

## MARKET ANALYSIS

### Worldwide Information Protection and Control (IPC) 2007–2011 Forecast and Analysis: Securing the World's New Currency

Brian E. Burke

Rose Ryan, J.D.

#### IDC OPINION

Information has become the world's new currency. The growing number of high-profile incidents in which customer records, confidential information, and intellectual property were leaked (or lost/stolen) has created an explosive demand for solutions that protect against the deliberate or inadvertent release of sensitive information. Moreover, numerous information-intensive government and industry regulations are requiring organizations to protect the integrity of customer and employee personal information and corporate digital assets. IDC believes that information protection and control (IPC) solutions will play a key role in protecting sensitive information and complying with privacy regulations. Addressing information protection and control is a complex challenge. The increasing use of corporate email, Web email, instant messaging (IM), peer to peer (P2P), and other channels for distributing data and the proliferation of mobile devices that allow employees to carry sensitive information outside the organization's boundaries make the control of information a substantial challenge. IDC believes IPC solutions are evolving to discover, protect, and control information contained in data in motion, data at rest, and data in use to help organizations of all sizes and vertical industries:

- Comply with government and industry regulations (Health Insurance Portability and Accountability Act [HIPAA], Gramm-Leach-Bliley Act [GLBA], Sarbanes-Oxley [SOX], Canada's Personal Information Protection and Electronic Documents Act [PIPEDA], European Union Data Protection Directive, Japan's Personal Information Privacy Act [PIPA], etc.)
- Prevent violations of corporate policy and best practices
- Stop the loss of intellectual property and proprietary information
- Prevent high-profile leaks of private information and customer records
- Preserve corporate brand image and reputation

## TABLE OF CONTENTS

	P
<b>In This Study</b>	<b>1</b>
Methodology .....	1
Information Protection and Control Market Definition .....	1
<b>Situation Overview</b>	<b>2</b>
Key Players in the Information Protection and Control Market .....	2
The Information Protection and Control Market in 2006 .....	4
Protecting Information: The World's New Currency .....	4
Internal Threat Environment .....	5
I Have Seen the Enemy, and He Is Us .....	5
Internal Versus External Threats .....	6
High-Profile Information Protection and Control Incidents .....	8
Government and Industry Regulations .....	10
Regulatory Impact .....	13
<b>Future Outlook</b>	<b>15</b>
The Future of Information Protection and Control.....	15
Encryption: Is It Finally the Year of Encryption? .....	15
Forecast and Assumptions .....	17
Information Protection and Control Forecast, 2007–2011 .....	17
Vendor Profiles .....	28
Aladdin Knowledge Systems .....	28
BorderWare .....	29
Clearswift.....	30
Code Green Networks .....	32
DigitalContainers .....	33
EMC (Authentica) .....	34
Entrust .....	35
Fidelis Security Systems .....	36
GTB Technologies.....	37
IronPort Systems (Acquired by Cisco).....	38
McAfee .....	39
MessageGate .....	40
MessageLabs .....	41
Mirapoint.....	42
Mobile Armor .....	44
MX Logic .....	44
Oakley Networks .....	45
Orchestria.....	46
PGP Corporation .....	46
PKWARE.....	48
PointSec.....	49
Postini.....	49
Proofpoint.....	51
Provilla.....	52
Reconnex .....	53

**TABLE OF CONTENTS — Continued**

	P
RSA .....	54
Secure Computing .....	54
Sendmail .....	55
Sigaba .....	57
SonicWALL .....	58
Sophos .....	59
SurfControl .....	60
Symantec .....	61
Tablus .....	63
Trend Micro .....	64
Tumbleweed Communications .....	65
Verdasys .....	67
Vericept .....	68
VeriSign .....	70
Voltage .....	71
Vontu .....	71
Websense .....	73
Workshare .....	74
ZixCorp .....	76
<b>Essential Guidance</b>	<b>77</b>
<b>Learn More</b>	<b>78</b>
Related Research .....	78
Methodology .....	78

## LIST OF TABLES

	P
1 Information Protection and Control Vendors by Market Segment .....	3
2 Examples of High-Profile Information Protection and Control Incidents .....	9
3 Key Regulations Driving Information Protection and Control.....	11
4 Worldwide Information Protection and Control Revenue by Segment, 2006–2011.....	17
5 Key Forecast Assumptions for the Worldwide Information Protection and Control Market, 2007–2011 .....	18

## LIST OF FIGURES

	P
1 Information Protection and Control Overview.....	2
2 Top 10 Threats to Enterprise Security .....	6
3 Origin of Most Serious Threats to Companies' IT Infrastructure by Company Size.....	7
4 Internal Threats to Companies' IT Infrastructure by Company Size, 2005 and 2006 .....	8
5 Affect of Privacy Regulation Requirements on Companies' Information Security and Staffing by Company Size.....	14
6 Existence of Company Policy for Notifying Customers When Their Private Data May Be at Risk .....	15
7 Companies' Planned Adoption of Security Technologies by Company Size .....	16
8 Worldwide Information Protection and Control Revenue by Segment, 2006–2011.....	18



## IN THIS STUDY

This study provides a top-down sizing of the information protection and control market in 2006 and a 2007–2011 forecast for this market. This study also includes profiles of leading IPC vendors and identifies the characteristics that vendors will need to be successful in the future.

---

## Methodology

See the Learn More section for a description of the forecasting and analysis methodology employed in this study.

In addition, please note the following:

- ☒ The information contained in this study was derived from the IDC Software Market Forecaster database as of April 19, 2007.
- ☒ All numbers in this document may not be exact due to rounding.
- ☒ For more information on IDC's software definitions and methodology, see *IDC's Software Taxonomy, 2007* (IDC #205437, February 2007).

---

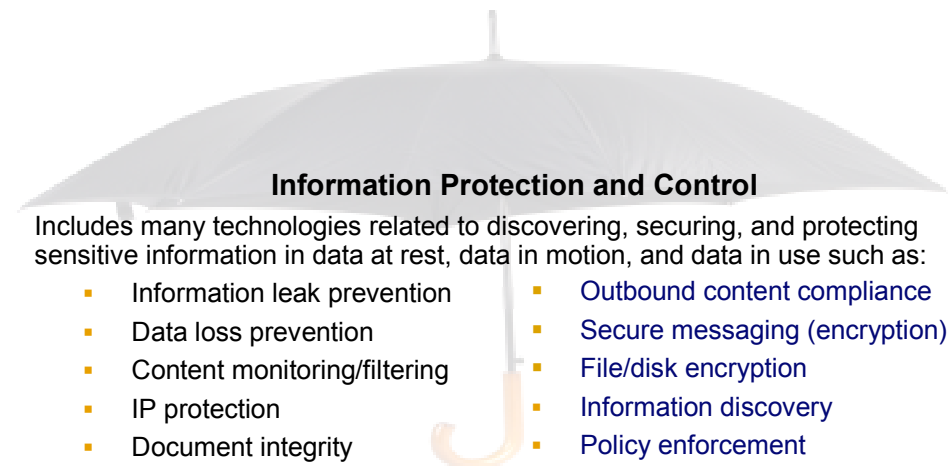
## Information Protection and Control Market Definition

Information protection and control includes solutions that discover, protect, and control sensitive information, as shown in Figure 1. IPC is a comprehensive solution that prevents sensitive customer data or company information from being distributed within or outside the enterprise in violation of regulatory or company policies. IPC includes the following technologies;

- ☒ **Data-in-motion IPC.** Data-in-motion IPC includes solutions that monitor, encrypt, filter, and block outbound content contained in email, instant messaging, peer to peer, file transfers, Web postings, and other types of messaging traffic.
- ☒ **Data-at-rest IPC.** Data-at-rest IPC includes solutions that discover, protect, and control information on desktops, laptops, file/storage servers, USB drives, and other types of data repositories.
- ☒ **Data-in-use IPC.** Data-in-use IPC includes solutions that protect and control information in use. These solutions are used to maintain the integrity of sensitive information such as contracts, term sheets, and other business-critical documents.

## FIGURE 1

### Information Protection and Control Overview



Source: IDC, 2007

## SITUATION OVERVIEW

### Key Players in the Information Protection and Control Market

Table 1 lists the key players in the IPC market.

**TABLE 1**

## Information Protection and Control Vendors by Market Segment

Data in Motion		Data at Rest	Data in Use
Aladdin Knowledge Systems	Provilla	EMC/RSA	Adobe
BorderWare	Reconnex	Entrust	DigitalContainers
Centennial	Secure Computing	GuardianEdge	Document Security Systems
Clearswift	Sendmail	Mobile Armor	EMC
Code Green Networks	Sigaba	Orchestria	Liquid Machines
Entrust	SonicWall	PGP	Oracle
Fidelis Security Systems	Sophos	PKWARE	Tablus
GTB Technologies	SurfControl	PointSec	Vericept
IronPort Systems	Symantec	Provilla	Vontu
McAfee	Tablus	Reconnex	Workshare
MessageGate	Trend Micro	SafeBoot	Websense
MessageLabs	Tumbleweed Communications	SafeNet	McAfee
Microsoft	Verdasys	Sigaba	
Mirapoint	Vericept	Tablus	
MX Logic	VeriSign	Utimaco	
Oakley Networks	Voltage	Verdasys	
Orchestria	Vontu	Vericept	
PGP	Websense	Vontu	
Postini	Workshare	Websense	
Proofpoint	ZixCorp	WinMagic	
		Workshare	

Source: IDC, 2007

## **The Information Protection and Control Market in 2006**

The demand for solutions that protect sensitive information was originally fueled by industries (financial services, banking, healthcare, etc.) that needed to comply with various government and industry regulations (HIPPA, GLB, SOX, etc.). In 2006, a series of high-profile incidents in which customer records, confidential information, and intellectual property were leaked (or lost/stolen) created an explosive demand for solutions outside of the heavily regulated industries.

### ***Protecting Information: The World's New Currency***

Protecting corporate intellectual property has rapidly moved up the priority list of many IT departments. Organizations of various industry and company sizes are extremely concerned with protecting patents, trademarks, brands, trade secrets, designs, architectures, copyrights, algorithms, software code, hardware schematics, inventions, business processes, and many other corporate assets. Gone are the days in which intellectual property and corporate secrets were kept safe in locked cabinets behind guarded doors. Today, nearly all corporate information exists in electronic form, accessible to almost any employee. Additionally, email has become the de facto filing system for much of this information, making it even more critical to protect the outbound flow of messages. The risks of inadvertent or deliberate disclosure of confidential information and intellectual property range from legal exposure to competitive disadvantage. Companies can risk losing serious dollars when design documents and source codes are posted to Internet message boards or emailed outside the organization. A privacy failure, even a merely perceived failure to protect customer data, can result in loss of consumer trust, affect customer retention, and cause significant damage to brand and company reputation.

A privacy failure, even a merely perceived failure to protect customer data, can result in loss of consumer trust, affect customer retention, and cause significant damage to brand and company reputation.

Organizations that manage patient health information, social security numbers, credit card numbers, and other types of personal data are being forced by government and industry regulations to implement security measures to address leakage of personal information. The loss of confidential personal information can materialize into compliance infractions, lawsuits from customers and/or patients, potential identity theft, and significant and often irreparable harm to an organization's credibility and reputation. The stakes are extremely high in online banking. Financial institutions must protect their consumers from fraud and identity theft, which run the gamut from authentication and securing private consumer data to making consumers whole in the event of a fraudulent loss. If consumers lose confidence in an institution's ability to adequately secure sensitive information, consumers will defect from both online banking and the institution. The same can be said for many other industries as well, especially retail, where customer trust and brand reputation are critical.

Many organizations are still struggling to understand the numerous regulations that potentially affect their organizations and what that means from a business perspective. In today's increasingly information-intensive businesses, technology is becoming a key part of strategic compliance initiatives to ensure sustainability of compliance-related processes and protection of sensitive information.

## Internal Threat Environment

### *I Have Seen the Enemy, and He Is Us*

Malicious code, spyware, and spam continue to be the most serious threat facing corporations today, but internal threats are rapidly climbing the priority list of enterprise security threats and now account for three of the top 10 most serious threats facing corporations today (see Figure 2):

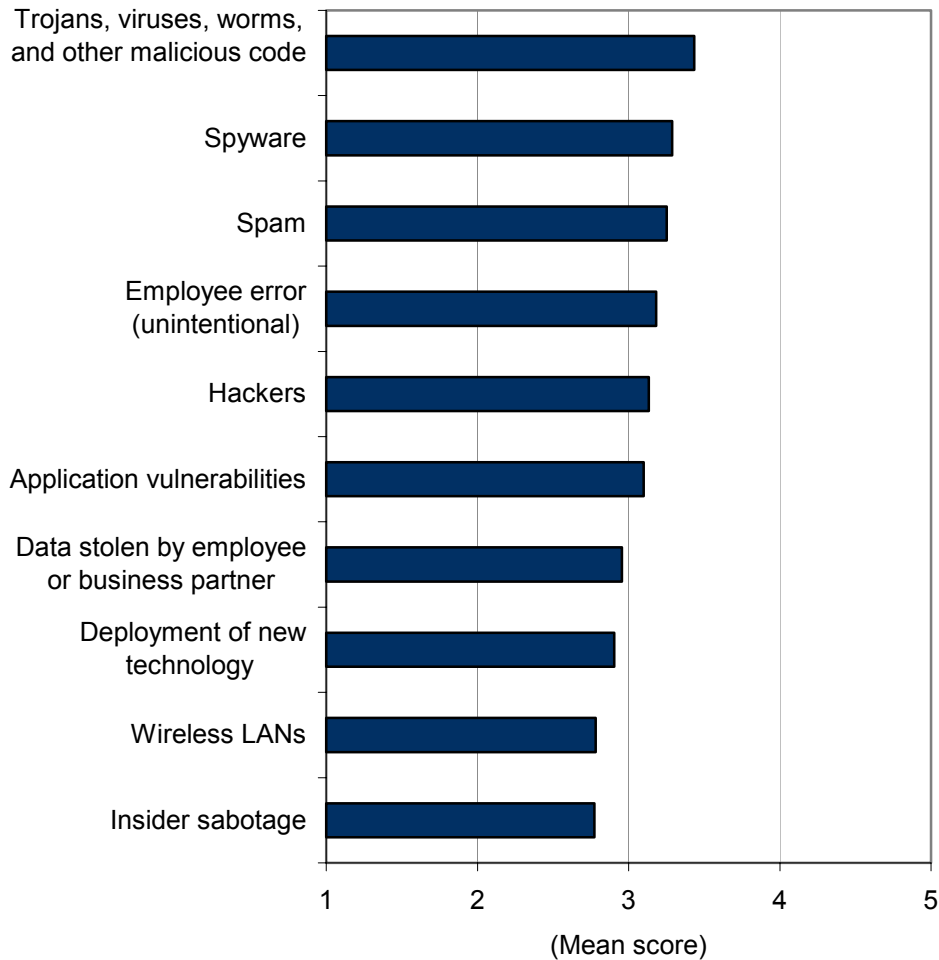
- ☒ Employee error ranks as the fourth-greatest threat to enterprise security. IDC believes the majority of information leaks and compliance violations come from employee error. Organizations are extremely concerned with employees inadvertently violating corporate policies and/or complying with government and industry regulations.
- ☒ Data stolen by an employee or a business partner ranks as the seventh-greatest threat to enterprise security. Although the majority of insider violations are inadvertent, IDC believes the most costly incidents are from malicious employees. IDC believes malicious action by a trusted source with access to corporate network resources and proprietary data will continue to rise up the priority list in organizations of all sizes.
- ☒ Insider sabotage ranks as the tenth-greatest threat to enterprise security. As with data stolen by an employee, insider sabotage by trusted employees poses a significant risk to organizations. Malicious employees facing financial hardship are increasingly looking for ways to use corporate information to commit fraud.

In all cases, organizations are facing a growing number of information leaks containing confidential data, proprietary information, or intellectual property from their employees.

Internal threats are rapidly climbing the priority list of enterprise security threats and now account for three of the top 10 most serious threats facing corporations today.

**FIGURE 2**

Top 10 Threats to Enterprise Security



n = 430

Note: Threat scores are based on a scale from 1 to 5, with 1 being no threat and 5 being a significant threat.

Source: IDC's Security Survey, 2006

***Internal Versus External Threats***

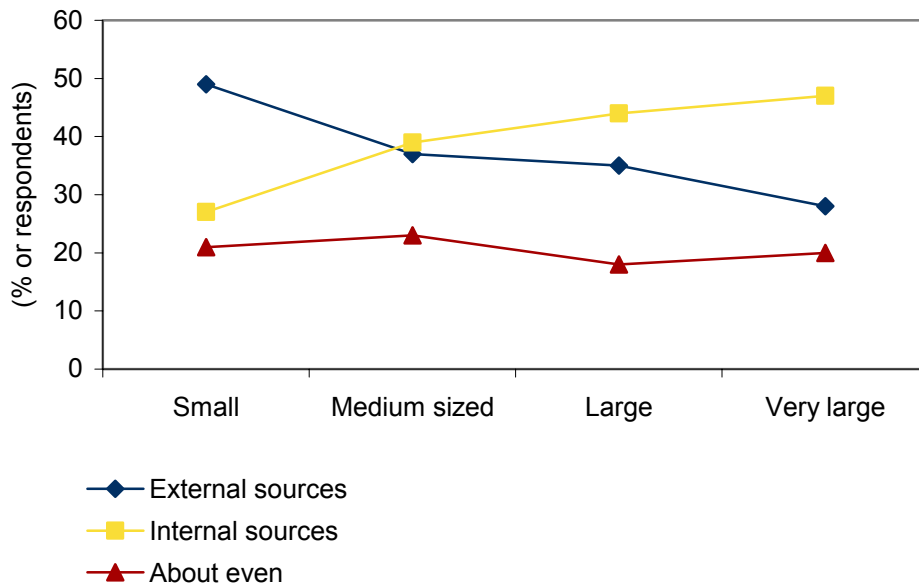
According to a 2006 IDC survey of 430 North American organizations, internal threats are much more of a concern in both large and very large enterprise environments, as shown in Figure 3. The growing concern with internal security threats comes as no surprise to IDC. In fact, the risks posed by internal threats are on the rise in organizations of all sizes, as shown in Figure 4. Our survey findings also showed that:

- ☒ 53% of very large organizations (10,000+ employees) and 41% of large organizations (1,000–9,999 employees) have terminated employees or contractors for internal security violations.
- ☒ 27% of very large organizations (10,000+ employees) and 11% of large organizations (1,000–9,999 employees) have prosecuted an employee for internal security violations.

**FIGURE 3**

Origin of Most Serious Threats to Companies' IT Infrastructure by Company Size

Q. Do you believe that the most serious threats to your company's enterprise IT infrastructure originate from internal or external sources?



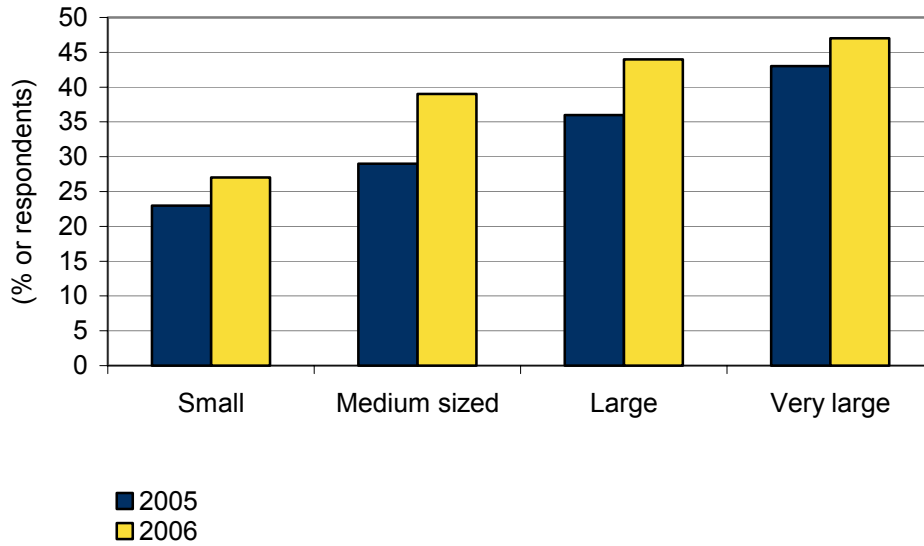
n = 430

Note: Company sizes are as follows: small (<100 employees), medium sized (100–999 employees), large (1,000–9,999 employees), and very large (10,000+ employees).

Source: IDC's Security Survey, 2006

**FIGURE 4**

Internal Threats to Companies' IT Infrastructure by Company Size, 2005 and 2006



n = 430

Note: Company sizes are as follows: small (<100 employees), medium sized (100–999 employees), large (1,000–9,999 employees), and very large (10,000+ employees).

Source: IDC's *Security Survey*, 2006

### High-Profile Information Protection and Control Incidents

There have been several high-profile incidents where customer records and/or confidential information have been leaked, as shown in Table 2.

**TABLE 2**

## Examples of High-Profile Information Protection and Control Incidents

Date	Location	Impact
1/18/2007	The TJX Companies Inc.; Framingham, Massachusetts	Customer data, including credit card numbers and other information related to customer transactions such as debit card, check, and merchandise return transactions and possibly also PIN numbers, was leaked from TJX's computer network. The leak affected an unknown number of TJX's customers, including its T.J. Maxx, Marshalls, HomeGoods, and A.J. Wright stores in the United States and Puerto Rico, and its Winners and HomeSense stores in Canada, and may involve customers in the United Kingdom and Ireland. In this event, numerous U.S. federal, state, and international data protection rules and regulations were violated.
1/4/2007	Cingular Wireless; Atlanta, Georgia	Cingular Wireless' latest Palm Treo 750 was leaked to the Web one week before the announcement date. A sales presentation that was supposed to be embargoed until the announcement date was leaked to the Internet by Engadget Mobile's Web site.
12/15/2006	Boeing Co.; Seattle, Washington	<p>A laptop with personal information, including the salaries, Social Security numbers, home addresses, phone numbers, and birth dates of about 382,000 retired and current company workers of the Boeing Co., was stolen. In this event, the laptop owner violated Boeing's policy and did not encrypt the sensitive data as company policy requires once it has been downloaded from a server. In a leaked email sent to Boeing's employees, Jim McNerney, Boeing's chairman, president, and chief executive, said that "This latest incident resulted from a clear violation of our data-protection policy." He also wrote that, "An employee, despite proper training, failed to comply with those requirements and as a result is being dismissed from the company."</p> <p>Boeing is violating numerous federal and state policies that mandate data protection and notifications. The company said that it will pay for credit monitoring for every person that was listed in the stolen database.</p>
12/13/2006	University of Texas at Dallas; Dallas, Texas	<p>The number of people affected was first thought to be 5,000, but is now increased to 6,000. Sensitive private information, including Social Security numbers of 5,000 students, faculty members, and staff might have been leaked when a computer system was hacked from the Internet.</p> <p>According to Texas SB 122, any person who conducts business in the state and owns or licenses computerized data that includes sensitive PI or maintains such computerized data is required to take reasonable measures to protect sensitive PI.</p>

**TABLE 2****Examples of High-Profile Information Protection and Control Incidents**

Date	Location	Impact
12/13/2006	UCLA; Los Angeles, California	<p>Social Security numbers, birth dates, home addresses, and contact information for about 800,000 names were leaked during a targeted attack on a UCLA database containing personal information on about 800,000 of the university's current and former students, faculty, and staff members, among others.</p> <p>The database included records for the university's current and former students, faculty, and staff — in some cases dating to the early 1990s. Others potentially affected included some applicants during the past five years who did not enroll at the university, as well as some parents of students or applicants who had applied for financial aid.</p> <p>Numerous regulations and California state laws were violated as a result of this incident. California's privacy bill SB 1386, a model for other state and federal regulations, requires proper notification; however, in this case, other state bills, such as AB 1950, were violated.</p>
2/18/2005	ChoicePoint Inc.; Alpharetta, Georgia	<p>Consumer data broker ChoicePoint, which acknowledged that the personal financial records of more than 163,000 consumers in its database had been compromised, will pay \$10 million in civil penalties and \$5 million in consumer redress to settle Federal Trade Commission charges that its security and record-handling procedures violated consumers' privacy rights and federal laws.</p>

Source: IDC, 2007

**Government and Industry Regulations**

Government and industry regulations remain a key driver for IPC implementations, as shown in Table 3. The increasingly complex environment of regulations and standards drives concerns about the accuracy and protection of an organization's data and information, not only with employees but also with customers, partners, and contractors. Organizations are faced with addressing compliance issues surrounding Sarbanes-Oxley, the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, FFIEC, PCI, and other federal regulations and guidelines, not only in the United States but globally. Further impetus for executives to push their organization to comply with these regulations includes personal liability and the threat of criminal and/or civil penalties. Civil prosecution can carry substantial financial penalties and damage a company's reputation with its customers.

Regulations governing privacy have been passed worldwide and vary from country to country. Organizations doing business internationally are struggling to cope with the effort to comply across borders. In the United States, complying with federal regulations that have recently come into effect is not as straightforward as executives

would have hoped because many of the laws by their nature are written with vague directives. The process of building best practices and industry standards is an ongoing one. The interpretation of federal regulations and the gradual building of industry standards will provide a framework from which companies can begin addressing both the concerns around sufficient security processes and the need for regulatory compliance. This has been a slow and often painful process for many organizations, which find themselves learning from the financial loss and public humiliation that often accompany noncompliant actions.

Privacy regulations in the United States are beginning to have a global reach, with many vendors in Europe and Asia opting to comply to facilitate business. As outlined, privacy regulations have surfaced worldwide, and the trend shows no signs of abating.

**TABLE 3**

Key Regulations Driving Information Protection and Control	
Regulation	Impact
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	HIPPA requires that to ensure privacy and confidentiality, all patient healthcare information be protected when electronically stored, maintained, or transmitted. It also mandates that each user be uniquely identified before being granted access to confidential information. It specifies that access to personal health information (PHI) be restricted to only those individuals who need access as part of their role.
Sarbanes-Oxley Act of 2002 (SOX)	In the wake of recent financial scandals, SOX requires public companies to validate the accuracy and integrity of their financial management. IDC believes this act will have long-term effects on federal securities regulation, corporate governance, and the regulation of auditors. SOX requires that businesses not only document and assess their internal controls but also control access to financial systems. Section 404 covers internal control activities during the creation of financial reports and points to compliance risks that can be addressed by IAM solutions.
Gramm-Leach-Bliley Act (GLBA)	GLBA mandates privacy and the protection of customer records maintained by financial institutions. These security requirements include access controls on customer information systems, encryption of electronic customer information, procedures to ensure that system modifications do not affect security, and monitoring systems to detect actual attacks or intrusions.
ISO 17799	ISO 17799 is a detailed security standard organized into 10 major sections: business continuity planning, system access control, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, computer and network management, asset classification and control, and security policy. The objective of ISO 17799:2005 is to provide a common basis and practical guideline for developing organizational security standards and effective security management practices.
IT Infrastructure Library (ITIL)	ITIL has seven sets of processes providing a framework for businesses in the following areas: service support, service delivery, planning to implement service management, ICT infrastructure management, applications management, security management, and business perspective.

**TABLE 3****Key Regulations Driving Information Protection and Control**

Regulation	Impact
Control Objectives for Information and Related Technology (CobiT)	CobiT was developed as a generally applicable and acceptable standard for good information technology security and control practices for management, users, auditors, and security practitioners. It was issued by the IT Governance Institute and now is in its third edition. CobiT contains 34 processes and provides the tools to assess and measure an organization's ability to deliver on those processes. It was originally published in 1996, with versions 2 and 3 appearing in 1998 and 2000, respectively. Version 4 has just been released.
Payment Card Industry (PCI) Data Security Standard	The PCI Data Security Standard was developed by MasterCard and Visa. It contains 12 requirements grouped into six areas: build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, monitor and test networks, and maintain an information security policy.
SB 1386	California's Information Protection Act requires companies to report security breaches involving private consumer information. Personal information is defined as Social Security number, driver's license or California ID card number, account number, or credit or debit card number in combination with a required security code, access code, or password that permits access to an individual's financial account.
Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)	Much like HIPAA, PIPEDA prohibits the collection, storage, and disclosure of personal information related to an individual without that person's explicit consent. Personal information is any factual or subjective information, recorded or not, about an identifiable individual. PIPEDA provides the individual with the right to know what is being collected and change the information if it is inaccurate. Interestingly enough, U.S. and U.K. businesses may also be bound by the rules protecting Canadian citizens' personal information.
European Union (EU) Data Protection Directive	Member countries are mandated to adopt standards for the collection, storage, and disclosure of personal data. This directive also outlines individuals' rights concerning their personal data. It is described as the most ambitious and stringent data privacy initiative, and the guidelines to ensure that data is transferred outside the EU only when it is adequately protected have extraterritorial implications for businesses. The U.S. Department of Commerce worked closely with the European Commission to develop a "safe harbor" framework to enable U.S. businesses to meet EU privacy regulations.
USA PATRIOT Act, Title III (anti-money laundering [AML] regulations)	Section 352 requires financial institutions to develop internal policies, procedures, and controls to guard against money laundering. Institutions are required to track and report suspicious activities and conduct regular independent audits to test AML programs. Additional rules designed to establish a customer identification program also came into effect recently and require financial institutions to document the methods they utilize to verify a customer's identity. A consortium of global financial institutions is looking to define business processes that can be shared among networked members and invoked using Web services and a service oriented architecture (SOA). AML has been identified as one of the key initiatives that would enable member firms to accomplish compliance at a lower cost.
Homeland Security Presidential Directive 12 (HSPD-12) (policy for a common identification standard for federal employees and contractors)	The primary objectives of HSPD-12 are the development and deployment of a federal government-wide common and reliable identification verification system that will be interoperative among all government agencies and serve as the basis for reciprocity between those agencies. In response to HSPD-12, the NIST Computer Security Division initiated the Personal Identity Verification (PIV) project and established the Federal Information Processing Standard (FIPS PUB 201).

Source: IDC, 2007

## ***Regulatory Impact***

Government and industry regulations are impacting the way organizations deal with information security and staffing in many different ways. Increased levels of network monitoring and reporting are very close to the top of the list of concerns, as shown in Figure 5. IDC believes this is clearly driven by the pressure government and industry regulations have placed on corporations to secure the use of their electronic communications. We expect the risk of compliance infractions and lawsuits from customers and/or patients to continue to force organizations to implement network monitoring and reporting technologies.

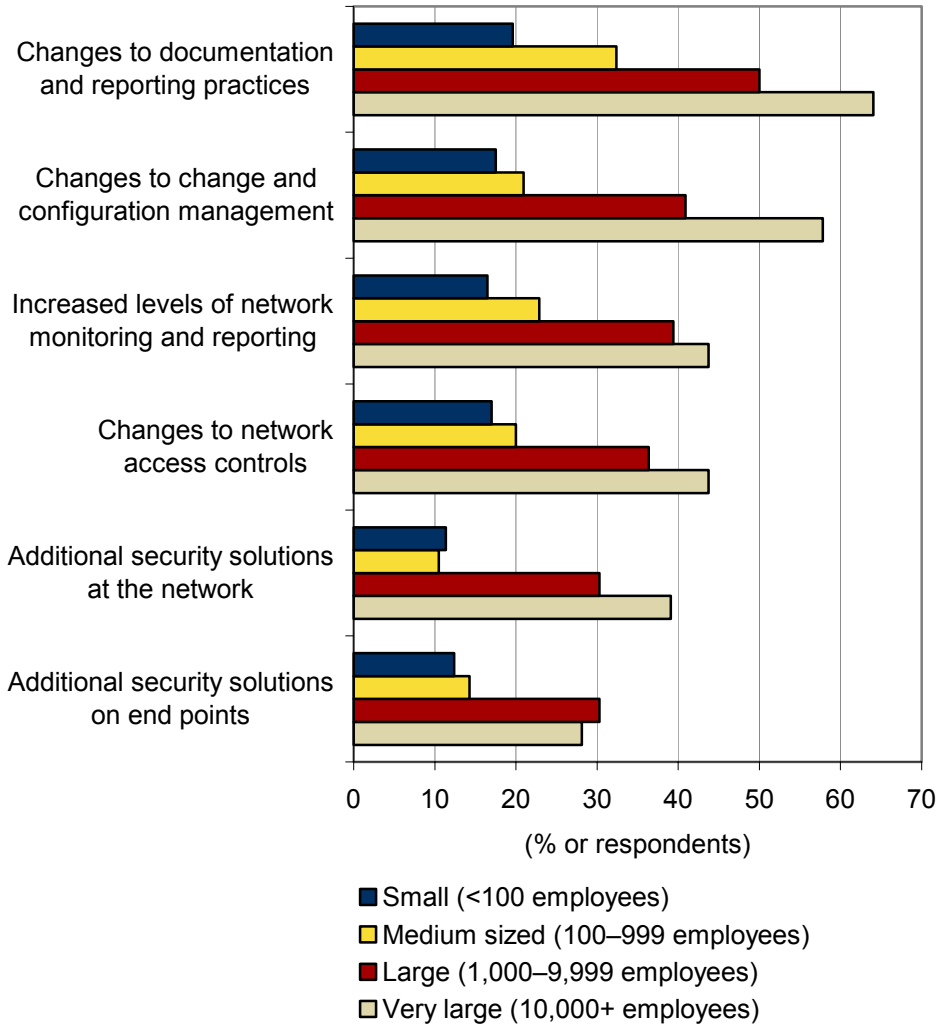
Our survey results also showed that the impact of regulations is having an effect on how organizations view endpoint security. We believe this is clear evidence of the need to secure data at rest on desktops, laptops, mobile devices, USB drives, and other types of data repositories.

Surprisingly, 48% of organizations still do not have a policy for notifying customers when their private data may be at risk, as shown in Figure 6. The state of California was a pioneer in adopting privacy laws that require organizations to notify California residents when the security of their personal information has been compromised. California's privacy laws reach far beyond the state's borders. As one of the largest economies in the world, most of the largest businesses in world work within the state and are therefore bound by its laws to some extent. Today, there are 35 states that have enacted data privacy laws across the United States, demanding that corporations and organizations conducting business in these states notify their residents of any security breaches and in certain states take proactive security measures to protect the customer information in their databases.

**FIGURE 5**

**Affect of Privacy Regulation Requirements on Companies' Information Security and Staffing by Company Size**

Q. *How have the requirements of privacy regulations affected information security and staffing in your organization?*



n = 430

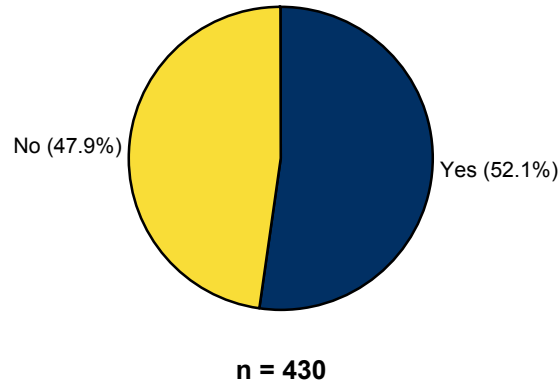
Note: Multiple responses were allowed.

Source: IDC's Security Survey, 2006

**FIGURE 6**

**Existence of Company Policy for Notifying Customers When Their Private Data May Be at Risk**

Q. Does your organization have a policy for notifying customers when their private data may be at risk?



Source: IDC's Security Survey, 2006

**FUTURE OUTLOOK**

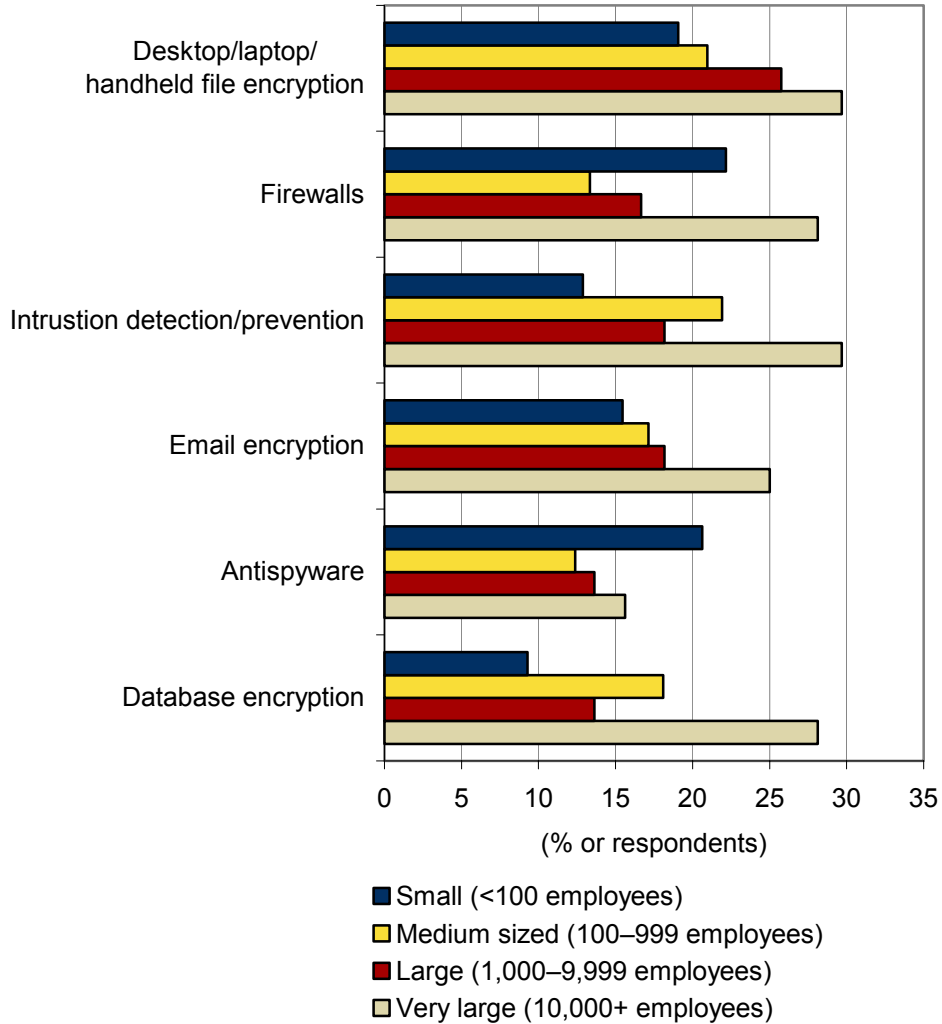
**The Future of Information Protection and Control**

***Encryption: Is It Finally the Year of Encryption?***

Figure 7 drills down into the point solutions that enterprises plan to deploy in 2007. Although firewalls, intrusion detection and prevention, and antivirus solutions usually dominate this answer, the 2006 survey had significantly different results. The product at the top of the list is desktop/laptop/handheld file encryption software. IDC speculates this is a result of regulatory compliance that requires stronger protection for specific information, and a result of all of the public data exposures. However, encryption is also a way to control sensitive data within the enterprise to ensure that only those with a need can access specific information. This result supports the growing concern regarding insider access. The high response rate for desktop encryption software doesn't appear to be an anomaly because encryption dominated the entire list, with email encryption second overall as the technology planned for deployment and database encryption third! All of this encryption appears to mean that organizations are going to get serious about exerting more control over their information.

**FIGURE 7**

Companies' Planned Adoption of Security Technologies by Company Size



n = 430

Note: Multiple responses were allowed.

Source: IDC's Security Survey, 2006

## Forecast and Assumptions

### *Information Protection and Control Forecast, 2007–2011*

IDC's estimate of the growth of the IPC market through 2011 is presented in Table 4 and Figure 8. IDC forecasts worldwide revenue for the IPC market to grow from \$765 million in 2006 to \$3.2 billion in 2011, representing a 33% compound annual growth rate (CAGR). Key forecast assumptions can be found in Table 5. Findings include:

- ☒ Data-in-motion IPC will grow from \$315 million in 2006 to \$1.3 billion in 2011, representing a 33% CAGR.
- ☒ Data-at-rest IPC will grow from \$300 million in 2006 to \$1.6 billion in 2011, representing a 40% CAGR.
- ☒ Data-in-use IPC will grow from \$150 million in 2006 to \$300 million in 2011, representing a 15% CAGR.

**TABLE 4**

Worldwide Information Protection and Control Revenue by Segment,  
2006–2011 (\$M)

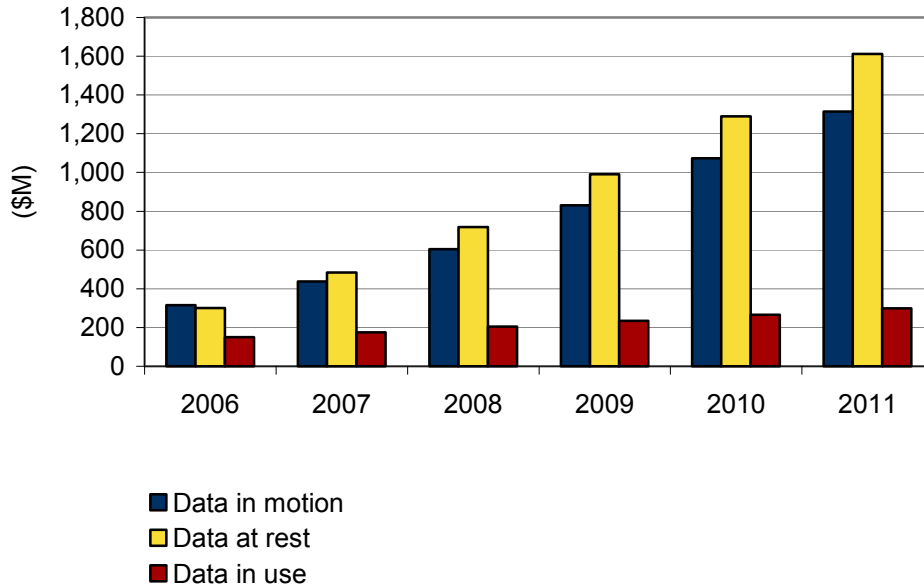
	2006	2007	2008	2009	2010	2011	2006–2011 CAGR (%)
Data in motion	315	437	605	830	1,073	1,314	33.1
Data at rest	300	483	719	990	1,290	1,612	40.0
Data in use	150	175	205	235	266	300	14.8
<b>Total</b>	<b>765</b>	<b>1,095</b>	<b>1,529</b>	<b>2,055</b>	<b>2,629</b>	<b>3,226</b>	<b>33.4</b>

Note: See Table 5 for key forecast assumptions.

Source: IDC, 2007

**FIGURE 8**

Worldwide Information Protection and Control Revenue by Segment, 2006–2011



Source: IDC, 2007

**TABLE 5**

Key Forecast Assumptions for the Worldwide Information Protection and Control Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
<b>Macroeconomics</b>				
IT governance and regulatory compliance	Compliance is still driving some IT spending, including Sarbanes-Oxley, Basel II, and HIPAA. We don't expect compliance spending to crowd out other IT initiatives; in fact, compliance record-keeping could spur initiatives in other areas as companies clean up their act. Increased attention to sound IT governance policies and compliance with regulatory requirements will drive an increased focus on storage and data management.	<b>Moderate.</b> Compliance and governance will have a positive impact on spending on infrastructure software that aids in the archiving, protection, and recovery of data. Compliance spending seems to be funding itself through better-run business operations.	↑	★★★★☆

**TABLE 5**

Key Forecast Assumptions for the Worldwide Information Protection and Control Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Economy	IDC assumes that worldwide and regional economic growth will be lower in 2007 compared with 2006. The United States will fall below 3%, Western Europe will be less than 2%, and Latin America, Eastern Europe, and Asia/Pacific outside of Japan will all drop. While Japan is expected by Consensus Economics to hit 1.8%, IDC analysts in Japan believe the country will beat expectations.	<b>Moderate.</b> The economy — in its stability but lower growth — is now a net-neutral influence on IT spending. It does seem able to withstand oil shocks and terrorism.	↔	★★★★☆
Profits	2007 profits will be far less than 2006's estimated 19% growth, according to Consensus Economics' October 2006 poll — in fact, at 4%. IDC expects that profits will be lower, but not <i>that</i> low.	<b>Moderate.</b> IT spending is almost to full strength as company profits have been good for a few years. With high profits, organizations increased IT spending. As profits fall, enterprises will now be looking for cost savings. Security and risk management initiatives could benefit as improved IT operations are used as a productivity multiplier.	↔	★★★★☆
Policy	Compliance with government regulations including Sarbanes-Oxley, GLBA, and HIPPA and industry standards such as PCI is driving increased spending on IT. Much of that spending has been on services, but expect enterprises to automate (with software) many compliance practices. Compliance record-keeping could spur initiatives in other areas as companies clean up their act.	<b>High.</b> Compliance initiatives are the major driver for the security and vulnerability market. As more regulations proliferate, it becomes more difficult to manage the process manually, so software solutions are required. Enforcing and maintaining compliance means that all SVM product submarkets benefit.	↑	★★★★☆

**TABLE 5**

Key Forecast Assumptions for the Worldwide Information Protection and Control Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
<b>Technology/service developments</b>				
Dynamic IT	IDC has identified the next style of computing — dynamic IT for dynamic enterprises — as a style that dramatically increases the effectiveness of IT. Within dynamic IT are a number of important subtrends — virtualization in the datacenter, data federation, software-as-a-service (SaaS) (see the software industry transformation row below), and composite and rule-based applications. IDC assumes the transition to dynamic IT will be slow and labored but will proceed nonetheless.	<b>Moderate.</b> Dynamic IT, by adding coherence to the enterprise usage of IT, would spur the market. However, confusing choices for enterprises and funding hurdles for new infrastructure will balance this impetus to market growth.	↔	★★★★☆
Killer apps	No "killer apps" or new technologies will come to drive overall industry growth in the same way Windows and office suites did in the 1980s or the Internet did in the late 1990s.	<b>Moderate.</b> With no "killer app," enterprises will work to improve the security of their existing infrastructure	↑	★★★★★
Convergence	Convergence is a complex phenomenon working at many levels — convergence of the telephone network and the Internet, of communications and IT technologies, of consumer and enterprise technologies, and even of storage, routing, and processing in the datacenter. Of these, perhaps the most overarching is the convergence of voice, video, and data communications. IDC assumes that this convergence is a permanent phenomenon and that it will pick up pace as the decade wears on. One measure is as follows: IDC expects that by 2009, there will be 1.5 billion users on the Internet and 3 billion users of the phone network, with 2.5 billion mobile users. The overlap will be significant.	<b>High.</b> The extension of IT product lines into consumer electronics adds to overall market opportunity for IT vendors and expands the definition of the market. A number of security start-ups hope to tap the consumer market. As technology expands, the requirements to manage risk will also grow. Expect to see new security solutions that attempt to manage the risk associated with converged networks.	↑	★★★☆☆

**TABLE 5**

Key Forecast Assumptions for the Worldwide Information Protection and Control Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Innovation	Vendors will continue security software, hardware, and services innovation at the same rate as in the past.	<b>Low.</b> The security market will not face bottlenecks from lack of new product development.	↔	★★★★☆
Enterprise workplace	Portal, collaboration, and content technologies will be applied in creative new ways to render "composite" applications, but more oriented toward specific user or user role needs rather than as a prepackaged set of business processes.	<b>High.</b> The broadening of the enterprise workplace has greatly increased risk, and IT organizations are trying to manage this new environment. This will eventually require more usage of policy, compliance, forensics, patching, and vulnerability assessment tools.	↑	★★★★★
Software industry transformation	The software industry is going through a major transformation, from basic architecture (SaaS) and the way software is written (composite applications) to the way software is delivered (software as services) and even funded (advertising based). IDC assumes that this transformation will take a decade, but that it will, when done, allow for much faster and more dynamic delivery of software functionality.	<b>Moderate.</b> The new software creation and delivery models should allow for a quantum increase in the ability to deliver and integrate new software functionality to information technology and communications (IT&C) systems. This should increase overall spending, even as it lowers costs.	↑	★★★★☆
Software security	Software is becoming much more dangerous. Hackers and others continue to find ways to misuse other people's software. Initially this was done by exploiting a vulnerability, but hackers are now finding ways to just miss appropriate software without a known vulnerability.	<b>High.</b> Inherent software vulnerabilities or intentional software exploits are a dangerous trend that requires remediation, during both software development and remediation after the fact. There is a growing awareness of the need to utilize software and application security tools during software development and deployment. Discovery, patching, and remediation remain important enterprise IT activities.	↑	★★★★★

**TABLE 5**

Key Forecast Assumptions for the Worldwide Information Protection and Control Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Storage management	Storage management functions such as virtualization, migration, policy-based classification, and data movement will continue to evolve to aid in managing increasing amounts of data.	<b>Moderate.</b> More intelligent and automated ways to manage data resident on storage makes tiered storage more effective but can also expand risks. The security of the storage level must be increased and managed.	↑	★★★★☆
Pervasive computing	This term refers to the proliferation of client devices and end-user or end-use devices at the network edge. IDC expects that by 2009, five times as many non-PC devices will be connected to networks as PCs — ranging from converged cell phones and networked entertainment and gaming devices, to automobiles, building automation systems, and industrial controllers. This doesn't even count RFID tags and sensors. IDC assumes that communicating client devices will proliferate at 5–10 times the rate of PCs installed. Devices will both converge (cells phones with more functionality) and diverge (single-use devices, such as RFID readers).	<b>Moderate.</b> The addition of billions of devices to the network edge will drive the need for more enterprise systems to deploy, manage, and make use of them. It will also shift the prevailing traffic from the center of the network outward to edge-inward, which will affect computing and communications architectures.	↑	★★★★☆
Modular IT/ risk aversion	Many firms remain cautious with regard to major IT investment/project implementation and have shifted to a more modular approach with longer periods of testing and slower rates of decision-making implementation.	<b>Moderate.</b> Overall demand will still fluctuate in the face of macroeconomic drivers/inhibitors, but the market should be less volatile. Large firms are taking a more long-term approach to IT than in previous years.	↔	★★★★☆
Storage management	Storage management functions such as virtualization, migration, policy-based classification, and data movement will continue to evolve to aid in managing increasing amounts of data.	<b>Moderate.</b> More intelligent and automated ways to manage data resident on storage helps mitigate the problem of a fixed quantity of human resources and allows users to leverage tiered storage more effectively.	↑	★★★★☆

**TABLE 5**

Key Forecast Assumptions for the Worldwide Information Protection and Control Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Security delivery model	Security software is more likely to be delivered as a service and/or a security appliance than bought as shrink-wrapped products.	<b>Moderate.</b> It will become more difficult to segment what is pure security software, what is inherent in a security appliance, and what is delivered as a software service. This has considerable impact on licensing and maintenance. Vendors like it because of the incremental revenue and hardware vendors like it because they can provide solutions not available to them, or they leverage their appliances to create a revenue stream.	↑	★★★★☆
Security threat environment	Software is becoming more rather than less vulnerable. Hackers and others continue to find ways to misuse other people's software. Initially this was done by exploiting a vulnerability, but hackers are now finding ways to just misappropriate software without a vulnerability.	<b>High.</b> The ability to bury malware within other software will become a dangerous trend that will lead to improved spyware software and increase the need for software and application security tools at software development and deployment. It will also increase the need for intrusion prevention software that enforces application execution. Although great for the security market, it could have a dampening impact on software in general.	↑	★★★★☆
Virtual machine software	Virtual machine software will cause a consolidation of physical machines and a proliferation of virtual machines.	<b>Moderate.</b> This will have no negative impact on operating systems images and may cause either some level of proliferation or an extension of the life expectancy, but without a related revenue growth.	↓	★★★★☆

**TABLE 5**

Key Forecast Assumptions for the Worldwide Information Protection and Control Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
<p>Launch of Windows Vista and Windows Longhorn Server</p>	<p>Windows Vista's broad launch in January 2007 will drive consumers to move to Windows Vista Home from Windows XP within days or weeks, but corporate adoption will follow a traditionally slower adoption ramp because of application compatibility testing, compliance testing, and IT and end-user training, and until a critical mass of Windows Vista-ready machines are within the installed base. Windows Longhorn Server, likewise, will be adopted on a timeline established by corporate IT practices, generally adopted as existing systems are retired and replaced or when net-new machines are deployed.</p>	<p><b>Moderate.</b> It will be "business as usual" for the Windows product shipments, with no significant "bump" of acquisitions or deployment immediately following the launch of Windows Vista or Windows Longhorn Server.</p>	<p>↔</p>	<p>★★★★★</p>
<p>Software complexity</p>	<p>Advances in standards and application infrastructure (such as SOA), while making it easier to build high-quality software, also add considerably to the complexity of resultant applications.</p>	<p><b>High.</b> Complexity can work to the advantage of a vendor that provides an application or tools that promise to reduce complexity. However, indiscriminant and uncoordinated development of standards can have the opposite effect. Complexity also works to the advantage of large vendors that provide a single "integrated" software stack and is one of the key forces driving industry consolidation.</p>	<p>↓</p>	<p>★★★☆☆</p>

**TABLE 5**

Key Forecast Assumptions for the Worldwide Information Protection and Control Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Standards	Standards provide recognition and approval of specifications regarding data and/or process. Standards will accelerate the use of technology.	<b>High.</b> Standards have the potential to affect a high degree of industry change. While standards curtail competition pertaining directly to the standard, they also foster competition in areas derivative to the standard. While standards are largely perceived to be a good thing, the indiscriminant creation of standards could lead to inconsistency, thereby undermining vendor credibility.	↑	★★★★☆
Consolidation	Consolidation will focus power in the hands of a small number of very large vendors.	<b>Moderate.</b> Consolidation is inevitable, but it is unclear whether consolidation is good or bad. Consolidation is good because it encourages broad-based vertical or horizontal integration, which tends to reduce perceived developer or end-user complexity. However, consolidation also can serve to reduce competition and therefore slow the pace of evolutionary market change. Consolidation is a relatively new phenomenon in the software industry, so while its effects are not yet well understood, industry change appears to be accelerating and innovation (Google) continues.	↔	★★★★☆☆

**TABLE 5**

Key Forecast Assumptions for the Worldwide Information Protection and Control Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
Enterprise workplace	Portal, collaboration, and content technologies will be applied in creative new ways to render "composite" applications, but more oriented toward specific user or user role needs rather than as a prepackaged set of business processes.	<b>High.</b> The enterprise workplace will offer a quick route to composite applications, which will be viewed by buyers as superior solution alternatives to old-fashioned "module" applications. The flexibility of "business integration on the glass" will drive buyers to switch budgets toward these types of efforts. Though underlying module prices may decrease (since users are only using pieces of those modules), the overall spend should increase and drive interest in this new class of offerings.	↑	★★★★☆☆
On-demand applications	The software industry is going through a major transformation, from basic architecture (SaaS) and the way software is written (composite applications) to the way software is delivered (software as services) and even funded (advertising based). IDC assumes that this transformation will take a decade, but that it will, when done, allow for much faster and more dynamic delivery of software functionality. Vendors offering infrastructureless applications, aka "on demand," will continue to garner share from license-only-oriented vendors, and this phenomena will spread to other applications beyond, for example, Web conferencing and sales automation.	<b>Moderate.</b> On-demand application specialists will force license-only suppliers to rethink their product delivery and licensing strategies and change their delivery to include on demand and offer new licensing options. Most application providers already offer "hosted" choices, so that is not a major impact. Though overall on demand may decrease prices at the outset of a new application sale, over the long run, it is not clear that vendors will recognize lower revenue, and the on-demand trends will reach new buyer audiences that could not afford classic license applications.	↑	★★★★☆☆

**TABLE 5**

Key Forecast Assumptions for the Worldwide Information Protection and Control Market, 2007–2011

Market Force	IDC Assumption	Impact	Accelerator/ Inhibitor/ Neutral	Certainty of Assumption
<b>Market characteristics</b>				
Hardware	Hardware markets continue to defy gravity and remained positive in 2006. IDC expects about the same performance in 2007, with pockets of both growth and decline. IDC assumes 6–7% growth in IT hardware spending (including network equipment sold to carriers and enterprises) in 2007.	<b>High.</b> Hardware spending, about 40% of total IT spending, drives spending as well in software and services.	↔	★★★★☆
Software	The software market will remain a mix of slow-and high-growth markets. Business-oriented software — collaboration, messaging, analytics, and business metrics — are higher growth than most infrastructure-related software, with the exception of security. IDC assumes worldwide software spending in 2007 will be 8%.	<b>Moderate.</b> Software spending, about 20% of total IT spending, can drive spending in hardware and in IT and business services.	↔	★★★☆☆
Services	IT services will grow, but at a muted rate as companies implement smaller, quicker-payback projects. Price declines are expected as offshore sourcing and blended models (offshore, near shore, onshore) increase. IDC expects worldwide IT services spending growth in 2007 of 6%.	<b>High.</b> IT services spending can affect the rate of overall solution adoption as well as the migration to dynamic IT. It accounts for about 40% of IT spending.	↔	★★★★☆
The Internet	Internet adoption is still going strong, especially in emerging economies. In the next four years, 500,000,000 new users will come online and commerce will double. By the end of 2006, over 50% of Internet households will be broadband. The hype around Web 2.0 is aiding awareness that the Internet economy is not dead.	<b>Moderate.</b> Analysts and pundits may underestimate the impact of the Internet because the "buzz" is gone, despite the hype over Web 2.0. It will be an enabler for both new markets and new business models.	↑	★★★★☆

Legend: ★☆☆☆☆ very low, ★★☆☆☆☆ low, ★★★☆☆ moderate, ★★★★☆☆ high, ★★★★★ very high

Source: IDC, March 2007

---

## **Vendor Profiles**

### ***Aladdin Knowledge Systems***

#### **Overview**

Aladdin eSafe is a proactive Web content security platform that provides strong security with the high capacity and reliability needed to effectively protect against known and unknown threats. eSafe reveals Web usage, threats, and abuse in real time, including real-time outbound and inbound threats containment; centralized content security threats assessment; Web usage monitoring, and granular policy enforcement. The product provides transparent deep-Web content inspection with effective speeds starting at 5 million fully inspected Web pages per hour. Using a combination of malicious code detection, proactive exploit prevention, and smart content policy enforcement, eSafe allows organizations to effectively control the usage of Internet applications within their enterprise.

#### **Information Protection and Control Products**

Aladdin offers the following IPC products:

- eSafe Gateway is an integrated Internet content security solution that inspects Web and email content (HTTP, FTP, POP3, and SMTP). Customers can separate SMTP inspection from other protocols for better performance.
- eSafe Mail is content security for email (SMTP), providing full email security as well as advanced protection against spam and phishing attacks. eSafe Mail can also be installed as a secure SMTP relay in an organization's DMZ.
- eSafe Web is a full content security solution for Web traffic, transparently inspecting HTTP and FTP protocols.
- eSafe Web SSL enables full content inspection of encrypted Web traffic as well as validation of HTTPS site certificates.
- eSafe AppliFilter protects against application-level threats and provides policy enforcement and control of all inbound and outbound communications, regardless of port.

All eSafe products can be delivered on purpose-built appliances or as a Virtual Appliance CD, which turns any server into an eSafe Content Security machine.

#### **Information Protection and Control Focus**

Aladdin eSafe addresses various layers of content security threats, preventing malicious content from activating and as a result creating an information leakage, and also preventing users from intentionally and unintentionally disclosing information or creating security breaches. Aladdin has developed technologies to identify and block zero-day unknown information-stealing malicious code, application and protocol layer vulnerability exploits, and phishing.

Policy enforcement is extremely important for IPC. eSafe can help organizations comply with the ISO 17799 standard as well as various regulations. eSafe allows organizations to enforce strict yet unobtrusive security policies identifying and limiting potential breaches such as usage of unauthorized instant messengers, limiting IM file transfers, preventing tunneling, or even using remote desktop applications to access home computers via a Web browser from the workplace.

eSafe identifies and blocks unauthorized communication patterns, including:

- Outbound spyware and related traffic protocols: spyware, adware, BHO, and ad-supported software
- Inbound spyware and related: browser hijackers, pop-installers, and drive-by spyware
- Instant messengers: chat and file transfer
- P2P applications, Skype
- Outbound tunneling
- Protocol enforcement (HTTP, HTTPS, HTTP WebDAV, etc.)
- Remote control/remote PC
- Inbound/outbound Internet worms and TCP exploits
- Outbound trojan and keylogger traffic
- Connections to anonymous proxies that are often used to bypass organizational security policy

URL filtering has long been associated with productivity, but it has significant IPC value. With a profile-based URL filtering and monitoring, eSafe can prevent or monitor user access to suspicious Web sites and site categories, intentionally or accidentally. The updating database includes 60 million sites in 60 categories.

One of the growing IPC issues is phishing. eSafe has a unique approach to this dire problem. Since phishing is usually a two-stage attack — a socially engineered bait email and a linked spoofed and malicious Web site — eSafe uses two-stage phishing prevention. The email phishing prevention not only blocks mass-phishing as spam but identifies and removes various phishing elements from the emails, and so renders them useless without causing any content problem for legitimate email, including mailing lists, newsletters, and nonspam commercial email. eSafe's Web site phishing protection blocks access to known phishing sites and protects from malicious content if access to the site is somehow gained.

## ***BorderWare***

### **Overview**

Founded in 1994, BorderWare Technologies Inc. provides messaging security solutions for enterprises and government. BorderWare has more than 6,000 customers with systems deployed at various military, intelligence, defense, and national security agencies and at corporations worldwide. Its headquarters are in Mississauga, Ontario.

## Information Protection and Control Products

BorderWare offers the following IPC products:

- ☒ SIPassure secures and enables SIP-based communication applications including VoIP, instant messaging, presence, and collaboration. It provides cost-effective solutions to extend the reach of converged communication applications to partners and customers in a secure way by addressing three key areas:
  - ☐ Service enablement and reliability
  - ☐ Network and application management
  - ☐ Network and application security
- ☒ BorderWare Security Network (BSN) goes beyond simple sender reputation to provide an all-encompassing view of the real-time behavior of an IP address by cross-referencing and analyzing data across multiple protocols. The BSN can detect potential spam sources by analyzing security probes against SMTP ports.
- ☒ MXtreme Mail Firewall is a comprehensive email security, privacy, and compliance solution that enables organizations to prevent inbound threats, control outbound content, and centrally manage an email infrastructure. MXtreme is a highly available email security system with message-level redundancy and on-demand clustering capability. It is built on the BorderWare Security Platform operating system, which is based on S-Core OS, a hardened operating system that provides the highest level of security demanded.

## Strategic Direction

For the past 11 years, BorderWare has been building comprehensive network security solutions for enterprises and government. Today, BorderWare's "application specific" firewalls set the benchmark for messaging security. The company's SteelGate Firewall+VPN, SIPassure SIP Firewall, and award-winning MXtreme Mail Firewall products protect mission-critical network resources in sensitive environments and are deployed by more than 8,000 customers in 65 countries. Over the years, BorderWare has developed affiliations and partnerships with some of the industry's most prominent companies in Internet infrastructure, security, and messaging, including 3Com, Cisco Systems, F5 Networks, Sun Microsystems, FaceTime Communications, Symantec/Brightmail, Research In Motion (RIM), Kaspersky Labs, and RSA Security.

## *Clearswift*

### Overview

Clearswift, the MIMESweeper company, is present in 15 countries worldwide, with headquarters in both the United States and the United Kingdom and sales offices in Germany, Spain, Japan, and Australia. Clearswift has over 17,000 customers and is a leading supplier of content security solutions for email, the Web, and IM.

Clearswift's products are designed from the ground up to ensure information protection and control. Its MIMESweeper products are policy based and filter all traffic, whether it is inbound, internal, or outbound. With content filtering features such as true file recognition, pattern matching, lexical analysis, and document finger printing, patient data, social security numbers, and credit card information are protected.

## Information Protection and Control Products

Clearswift offers the following IPC products:

- ☒ MIMESweeper Email Appliance is a preloaded appliance offering antivirus, antispam, antispysware, antiphishing, plug-and-play deployment, automated updates and easy management of both inbound and outbound filtering, and content compliance. It performs policy-driven email content security to help protect against loss of intellectual property and safeguard the privacy of organizations and individuals as electronic content is transferred within, out of, and around organizations.
- ☒ MIMESweeper for SMTP is a server-based email solution that protects organizations against inbound and outbound email threats, from spam and viruses to employee time wasting, circulation of pornography, breaches in confidentiality, legal liability, and IT resource misuse.
- ☒ MIMESweeper Email Managed Service is as a managed service; no software is installed in the customer environment. All the technology is located in three redundant datacenters that are automatically synchronized, updated, and managed by Clearswift's in-house technology. The service uses multiple antivirus products to scan messages for viruses and malicious content; these scanners are dynamically monitored by both Clearswift's automated watchdogs and 24-hour staff to ensure maximum performance and security.
- ☒ MIMESweeper for Exchange and MIMESweeper for Domino provide internal email security for organizations protecting against harassment and the advertent and inadvertent distribution of confidential information.
- ☒ MIMESweeper for Web brings policy-based content security to the HTTP gateway. MIMESweeper for Web analyzes Web content and blocks pages or files that are prohibited by an organization's security policy. It also provides policy-based content security for organizations that allow access to Web-based email and Web 2.0 applications such as social network sites, blogs, wikis, and chat rooms.
- ☒ The MIMESweeper Web Appliance is an enterprise-class Web security solution that covers all Web threats — inbound and outbound — in an appliance form factor and that includes built-in and integrated URL filtering, content filtering, antispysware, and antivirus components in an award-winning management GUI. This new policy-based Web security appliance delivers no-compromise bidirectional content security and that is easy to deploy and manage. This solution also helps control access to and manage the use of Web 2.0 tools such as social network sites, blogs, wikis, and chat rooms.
- ☒ MIMESweeper IM Enterprise Edition is an enterprise-class IM filtering solution that detects and stops malware such as viruses, worms, and spyware via Internet chat, from propagating through real-time Internet communication channels. It controls evasive peer-to-peer, file sharing, and anonymizer applications including Skype and offers comprehensive IM control. Its real-time filtering capabilities monitor, control, record, and manage inappropriate chat and legitimate IM conversation and apply policy to the transfer of information and documents. With MIMESweeper, IM Enterprise Edition organizations are able to prevent loss of confidential information via a wide range of real-time Internet communications channels.

## **Strategic Direction**

Clearswift secures content and protects against digital attacks by enforcing security policies that increase productivity, reduce IT costs, and create a safer business environment. Its goal is to provide total content security for data in motion (i.e., email, Web, and IM). Clearswift's core expertise lies in the content analysis and policy enforcement of email, Web, and IM content traveling into, across, and out of organizations. Clearswift enables organizations to protect themselves against digital attacks, meet legal and regulatory requirements, implement productivity-saving policies, and manage intellectual property passing within, into, and out of their network. MIMESweeper's content analysis engine allows organizations to filter inbound and outbound traffic according to a variety of attributes. Each email, IM conversation, Web page, and attachment that comes into or leaves a company's internal network is scanned and compared against the personalized policy to ensure that information exchange is appropriate.

Clearswift meets the overwhelming demands of the market to address regulatory and legal issues brought on by government statutes and compliance laws worldwide. Underpinning the strategic road map, Clearswift will provide content security solutions to the market on a range of platforms — software, managed services, and appliances — while remaining focused on helping organizations address the future of the rapidly changing Internet and email content security market with solutions that secure and enforce policy on both data in motion and data at rest.

## ***Code Green Networks***

### **Overview**

Headquartered in Santa Clara, California, Code Green Networks provides products that enable small and midsized companies and government organizations to mitigate the growing threat of having sensitive information leaked from the inside using digital technology.

### **Information Protection and Control Products**

Code Green offers the following IPC products:

- ☒ Content Inspection (CI) Appliance is connected at the network egress point and provides comprehensive data loss prevention solution in a box. It enables IT and security managers to monitor content flows in all of the most widely used TCP protocols including SMTP, FTP, HTTP, IM, and WebMail and discover data leaks and implement automated policies to prevent them. A role-based Web interface enables users to easily define protection policies and analyze incidents.
  
- ☒ Code Green's Deep Content Fingerprinting technology provides detection of protected unstructured information while Data Element Fingerprinting protects structured data. The CI Appliance includes an on-board mail transfer agent (MTA) to enable blocking enforcement of SMTP email. It interfaces to proxy servers with ICAP to enable blocking enforcement of WebMail, HTTP, HTTPS, and FTP. It also includes integrated, on-board encryption services provided by the Voltage Security Network to enable policy-based secure messaging.

- ☒ Content Inspection Agent helps IT and security managers protect sensitive data, both on and off the network, by preventing the transfer of files to or from unauthorized portable devices, such as USB memory sticks, providing complete visibility of device and file accesses and automatically encrypting data copied to approved devices.

### **Strategic Direction**

Code Green Network's appliance packaging and pricing enable customers to protect their sensitive information in a cost-effective manner. Code Green Networks products are sold and supported through a global network of business partners. Its customer base includes corporations and government agencies in Asia, North America, and Europe.

The founders of Code Green Networks, Sreekanth Ravi and Sudhakar Ravi, also founded SonicWALL (Nasdaq: SNWL), a leading provider of Internet security solutions, and took it public through a successful initial public offering. Code Green Networks' management team consists of experienced leaders from established, market-leading companies including Documentum, Business Objects, and Tumbleweed.

### ***DigitalContainers***

#### **Overview**

Headquartered in Fairfax, Virginia, DigitalContainers LLC owns patented solutions that support secure file and media delivery, tracking, authorization, certification, and communication of transactional data to trusted third parties across the Internet. Whether a Digital Container is distributed by email, by instant message, in a P2P network, by download from a Web site, or physically on a CD, the copyright protection and status/activity tracking gives the file its own security and commerce system. These patented processes support Secure Superdistribution, one of the most powerful ecommerce models on the Internet.

#### **Information Protection and Control Products**

DigitalContainers offers the following IPC products:

- ☒ Delivering Electronic Content technology is a system that allows "containerized" digital content — such as a song, video, or travel brochure — to be promoted, and the request fulfilled instantly from banner and flash advertising on any Web site or in an instant message or email.
- ☒ Regulating Access to Digital Content is a process in which access to digital content — such as text, video, and music — is based on completion of an authorization process to unlock or gain access to the protected object. Authorization may require payment information and/or other usage information before approval is granted.
- ☒ Tracking Electronic Content is a system whereby a secure digital content file persistently reports the identification of, and provides information about, any new user that attempts to access the content. With the granting of the Tracking Electronic Content patent, DigitalContainers has obtained what amounts to the "Superdistribution" patent for the Internet and distributed networks.

## **Strategic Direction**

DigitalContainers has patented symmetric key/token-based security technologies for use in digital rights management, peer-to-peer application development, ecommerce, and privacy compliance applications. Its systems are an important alternative to public key infrastructure because they are much simpler, less expensive to build and maintain, and more secure.

A Digital Container is an intelligent software package that provides an all-in-one security, management, and ecommerce system for files of any type and size as they travel over the Internet. These containers "wrap" the files in a secure digital shell that can only be opened with a "key" that can be as simple as a password, as unique as a fingerprint, or used in conjunction with a patented authorization process in which the container "talks" to remote authorization authorities.

A Digital Container includes the following self-contained features to create a persistent and comprehensive digital rights management system: file protection/encryption, tracking, authentication, and ecommerce system. This combination of features allows files and media to travel the Internet in a variety of ways yet be perpetually tracked, controlled, and audited by the content owners.

## ***EMC (Authentica)***

### **Overview**

EMC Corp. (NYSE: EMC) is a world leader in products, services, and solutions for information management and storage that help organizations extract the maximum value from their information, at the lowest total cost, across every point in the information life cycle.

### **Information Protection and Control Products**

EMC offers the following IPC products:

- ☒ EMC Documentum IRM Client for Adobe Acrobat is a flexible, secure document-sharing application that gives content owners total control over proprietary information. Organizations can dynamically control information by allowing content owners to decide who can view, copy, print, and forward documents and who cannot. Content owners can expire or revoke document access even after delivery outside of the corporate firewall.
- ☒ EMC Documentum IRM Client for E-Mail gives organizations control over email content, protecting content both during and after delivery — unlike traditional secure delivery solutions. Email and attachments are kept confidential and tamperproof no matter where they're distributed or stored. A detailed audit trail provides proof of compliance with corporate security policies and regulatory requirements.
- ☒ EMC Documentum IRM Client for Microsoft Office gives organizations a powerful tool for securely sharing and collaborating on sensitive Microsoft Office files including documents, spreadsheets, and presentations. Information is encrypted and persistently protected at rest, in transit, and even while it's being viewed by recipients.

- ☒ EMC Documentum IRM Client for RIM BlackBerry works in concert with EMC Documentum IRM Client for E-Mail to persistently encrypt and protect email that's pushed to a RIM BlackBerry device. Messages protected with IRM Client for RIM BlackBerry can be viewed but not forwarded or copied.
- ☒ EMC Documentum IRM Services for eRoom make it easy for distributed teams to collaborate securely without fear of information leaks. Protected folders and documents can be created within an eRoom and shared with partners and customers; content is protected even after it leaves the eRoom. Content managers define when and how documents may be used and track activity through a detailed audit trail. They can also expire outdated documents, ensuring that only the most current versions are available for use.

### **Strategic Direction**

EMC Corp. acquired Authentica on February 27, 2006. Authentica Secure Mail, Authentica Secure Mobile Mail, and Authentica Secure Documents products have been combined with EMC Documentum products. Authentica represents a natural extension to the EMC Documentum platform, which currently provides secure creation, tracking, and distribution of content within the Documentum environment. Authentica augments these industry-leading security capabilities and will allow Documentum and eRoom users to maintain the same control over and audit access to content distributed outside the Documentum environment, outside the corporate firewall, and over the Internet. Authentica has been a partner with EMC Documentum for several years, and this is a natural evolution of an already strong partnership.

### ***Entrust***

#### **Overview**

Entrust Inc., which is headquartered in Addison, Texas, is a global provider of security software. It was founded in 1994 as a spinout of Nortel Networks and went public in 1998. Entrust has approximately 1,650 customers in more than 65 countries.

#### **Information Protection and Control Products**

Entrust offers the following IPC products:

- ☒ Entrust's solutions help governments, enterprises, and financial services companies stop noncompliant behavior before it becomes a problem.
- ☒ Entrust Secure Messaging Solution and Entelligence Messaging Server offer real-time corporate and regulatory policy enforcement, including automatic protection of sensitive information at the boundary. It is an integrated suite of components that provides automatic content scanning of outbound email messages, centralized policy enforcement, and boundary-based email encryption.
- ☒ Entrust Entelligence Messaging Server is a server-based security gateway that makes it easier to communicate securely with external partners and customers. Messaging Server transparently manages email encryption functions and enforces corporate secure email policies enabling "end to end," "boundary only," and hybrid encryption architectures. Messaging Server supports multiple messaging platforms, delivery methods, and secure protocols to enable flexible and secure communications outside of the organization.

- ☒ Entrust Intelligence Group Share provides manageable network file share encryption for secure collaboration between teams and departments. Group Share provides automated, persistent encryption, policy-based access control, and centralized auditing of secured file access.
- ☒ Entrust TransactionGuard offers out-of-the-box, behavior-based fraud detection for Internet-based applications and seamlessly integrates with multifactor authentication solutions such as Entrust IdentityGuard for risk-based authentication. A fraud rule library is available as well as access to an Open Fraud Intelligence Network providing industry-based fraud rule feeds. Rapid deployment can be achieved with no changes to back-end applications.
- ☒ Entrust Intelligence Security Provider, Desktop Manager, and Email Plug-in provide "government strength" (FIPS, Common Criteria, NIST, and PKITS certified) email security down to the desktop environment — protecting email messages while they are in transit and while they are stored on the desktop.
- ☒ Entrust Intelligence Mobile Data Security Suite offers full-disk encryption for laptops and desktops. It also includes transparent on-the-fly encryption of removable media (USB, CD/DVD, etc.), PDAs and smartphones.

### **Strategic Direction**

In September of 2006, Entrust announced a strategic partnership with Vericept to deliver fully embedded email encryption functionality in a content monitoring and control solution. Under the terms of the agreement, Vericept has integrated the Entrust Intelligence Messaging Server encryption capability into Vericept's Protect product providing automatic encryption, compliance, and content control to both Vericept and Entrust customers. In addition, Entrust is a reseller partner of Vericept's data loss prevention solutions.

Entrust's software and services are deployed to ensure the privacy of electronic communications and transactions across corporate networks and the Internet, addressing functions such as identification, verification, privacy, and security. Entrust's software is used to authenticate users via passwords, smart cards, digital certificates, biometric devices, questions and answers, grid authentication, and hardware-based OTP tokens. Entrust IdentityGuard can be used to secure access to both consumer- and enterprise-based applications. Entrust is working to tie its products together to offer a seamless protection platform, and moving toward a single management interface, to solve the bigger story of protecting data. The company also offers services such as consulting, deployment, and managed security services.

### ***Fidelis Security Systems***

#### **Overview**

Since 2002, Fidelis Security Systems has been committed to giving organizations the power to protect their brand, intellectual property, and resources by stopping data leakage. The company's Extrusion Prevention System gives organizations the power to identify and stop data leakages before they occur. Based on patent-pending proprietary technology, the Fidelis Extrusion Prevention System, Fidelis XPS, solves data leakage challenges such as protecting intellectual property and identity information, assuring compliance with government and industry privacy regulations,

and managing insider use of the Internet. Fidelis Security Systems gives organizations the power to protect their brand, intellectual property, and resources by stopping data leakage. Fidelis is headquartered in Bethesda, Maryland.

### **Information Protection and Control Products**

Fidelis offers the following IPC products:

- ☒ The Fidelis Extrusion Prevention System, Fidelis XPS, identifies and stops data leakages before they occur. Organizations choose Fidelis XPS to solve their biggest data leakage challenges, protecting intellectual property and identity information, assuring compliance with government and industry privacy regulations, and managing insider use of the Internet. Fidelis XPS is a network appliance available in three configurations designed to address the most demanding network environments. In addition, a range of prebuilt policies for Digital Asset Protection, Privacy Compliance, and Insider Internet Management deliver out-of-the-box extrusion prevention specific to companies' business requirements.

### **Strategic Direction**

The latest version of Fidelis XPS includes new capabilities such as support for Internet content adaptation protocol, which allows Fidelis XPS to inspect, alert, and/or stop encrypted outbound Web traffic. Customers can now apply the same granular level of control they apply to non-encrypted traffic. Fidelis XPS also includes a prebuilt database of drug names to support HIPAA compliance. Customers can select from an expanded library of plug-and-play policies, avoiding time-consuming data registration and realizing fast deployment and a lower total cost of ownership. It offers expanded, robust support for unproxied instant messaging traffic as well as support for Microsoft Office 2007.

Fidelis continues to extend the coverage organizations can count on from Fidelis XPS. The system was designed to deliver a solution that would give customers the flexibility to either prevent or simply detect and alert on a policy-by-policy basis. The granularity of control built into Fidelis XPS to manage and monitor channels, attachments, file types, and specific content is what customers' complex environments and business policies demand.

## ***GTB Technologies***

### **Overview**

Based in Newport Beach, California, GTB Technologies designs, develops, and markets information leak prevention systems. The GTB Inspector protects against unauthorized transmission of confidential data from the network to the Internet. The solution is especially valuable to insurance, banks, financial, healthcare, universities, and high-tech companies.

### **Information Protection and Control Products**

GTB Technologies offers the following IPC products:

- ☒ GTB Inspector is an appliance that monitors all outbound traffic and physically blocks unauthorized data transmission attempts. Optionally, it can be configured

to detect and monitor breaches and alert security personnel rather than blocking transmission.

- ☒ GTB Data-at-Rest Manager (DARM) is a data discovery and search tool that scans the enterprise network for presence of the data of interest. It has two functions: discovery of exposed confidential data and data classification assistance. Confidential data is discovered with the same precision and performance of the GTB Inspector. GTB DARM scans any location on the network, including file servers, desktops and laptops, and removable media. GTB DARM is a separate product but it is capable of working together with GTB Inspector, sharing policies and data.

### **Strategic Direction**

GTB announced a partnership with 8e6 Technologies, a security company dedicated to Internet filtering and reporting, to deliver a new data leakage appliance within the rapidly growing data security market. Under terms of the agreement, 8e6 plans to integrate the new data leakage product into its existing Web filtering and reporting infrastructure to provide customers with a comprehensive solution that goes beyond simply tracking users' Web usage to include monitoring of all outbound Internet-based communication to determine whether employees are trying to send confidential information outside the company's network.

### ***IronPort Systems (Acquired by Cisco)***

#### **Overview**

IronPort Systems was founded in 2000 by pioneers in Internet messaging. With technical staff from companies such as Hotmail, eGroups, ListBot, and Yahoo!, IronPort's mission is to revolutionize Internet messaging. In 2004, IronPort reported \$43.7 million in total bookings. IronPort protects the messaging systems of over 2,000 organizations in 35 countries worldwide, including 8 of the top 10 ISPs.

On January 4, 2007, Cisco announced that it intends to acquire IronPort Systems Inc. for approximately \$830 million in cash and stock.

#### **Information Protection and Control Products**

IronPort offers the following IPC products:

- ☒ The IronPort C-Series email security appliances address the issues faced by corporations large and small by uniquely combining powerful performance with preventive and reactive security measures that are easy to deploy and manage. The IronPort C-Series delivers defense-in-depth security with its carrier-proven technology and the management capabilities required by companies of all sizes.

IronPort email security appliances protect internal servers from attacks and enable organizations to comply with HIPAA, GLB, SOX, and other regulatory compliance laws by applying filtering, encryption, and archiving policies on incoming and/or outgoing messages.

## **Strategic Direction**

IronPort Systems is a leading email security products provider for organizations ranging from small businesses to the Global 2000. The company has developed a family of email security appliances, the IronPort C-Series, as well as security modules and unique technologies that offer breakthrough performance, multilayer protection, and best-of-breed options. IronPort is driving new standards and providing innovative products for those faced with the monumental task of managing, protecting, and growing mission-critical email systems.

IDC sees great potential in integrating the email and Web security solutions from IronPort into the existing Cisco Self-Defending Network. Securing email, messaging, and other sorts of content is of primary concern to enterprises and other organizations. As email and messaging are leading Web applications and major sources of compliance violation, the IronPort acquisition is a natural extension to Cisco's security portfolio. The security products and technology from IronPort add a rich and complementary suite of messaging solutions to Cisco's industry-leading threat mitigation, confidential communications, policy control, and management solutions.

On November 1, 2006, IronPort Systems Inc., a leading Internet gateway security provider, announced its intended acquisition of PostX Corp. IronPort Systems also announced the introduction of major enhancements to its content scanning capability that, when combined with PostX technology, results in a robust and scalable solution to provide secure, encrypted email.

## ***McAfee***

### **Overview**

McAfee Inc., a leading dedicated security technology company, headquartered in Santa Clara, California, delivers proactive and proven solutions and services that secure systems and networks around the world. With its security expertise and commitment to innovation, McAfee empowers home users, businesses, the public sector, and service providers with the ability to block attacks, prevent disruptions, and continuously track and improve their security. Founded in 1989, McAfee held its initial public offering in 1992. The company has approximately 3,900 people currently under its employ. McAfee has worldwide offices in more than 35 countries with major operations across the United States, in India, and in the United Kingdom. Formerly Network Associates, the company changed its name to McAfee on July 1, 2004.

### **Information Protection and Control Products**

McAfee offers the following IPC products:

- McAfee Data Loss Prevention is a comprehensive solution offering complete visibility and control to instantly monitor and prevent confidential data loss at work, at home, and on the road. McAfee DLP protects enterprises from the risks of financial loss, brand damage, competitive disadvantage, lost customers, and noncompliance.

- ☒ McAfee Data Loss Prevention Host employs its logging and analysis server to deploy centrally managed policies, monitor real-time events, and generate reports. It allows customers to apply security policies to regulate and restrict how employees use and transfer sensitive data without interfering with normal business activities.
- ☒ McAfee Data Loss Prevention Gateway monitors and prevents data loss by analyzing traffic sent from the network. It stops data loss on systems without an agent including guest laptops, servers, non-Windows systems, and mobile devices. Data can be monitored, blocked, quarantined, or encrypted (via third-party service) based on granular security policies.

### **Strategic Direction**

In October 2006, McAfee moved into the IPC market with the acquisition of Onigma, an Israeli vendor of data-leak prevention software. This \$20 million cash acquisition advances McAfee's strategy of offering its enterprise customers a complete security risk management approach to managing security and compliance. In February 2007, McAfee officially launched McAfee Data Loss Prevention (DLP) Host, a comprehensive solution that prevents confidential data loss through malicious and unintentional means. McAfee DLP offers organizations full control and absolute visibility to data, leaving endpoints via email, instant messaging, printed documents, USB drives, CD-ROMs, and more

In April 2007, McAfee expanded its IPC protection to the gateway. The launch of McAfee Data Loss Prevention Gateway complements McAfee Data Loss Prevention Host by delivering multilayered protection that prevents data loss at the desktop and the gateway. McAfee DLP Gateway prevents data loss from guest laptops, non-Windows systems (e.g., Mac and Linux), servers, mobile devices, and all other agentless devices by blocking the transfer of confidential information at the gateway. The protection of agentless devices is growing in importance as corporations and government agencies are increasingly using mobile devices to access sensitive information on corporate networks.

### ***MessageGate***

#### **Overview**

MessageGate provides practical email governance software and services that help companies cope with threats, improve archival and retrieval activities, and ensure proper usage across a variety of industries. It originated from internal technology developed and implemented by Boeing Co. MessageGate spun out and established itself as an independent company in 2003.

#### **Information Control and Control Products**

MessageGate offers the following IPC products:

- ☒ MessageGate starts with an audit-led approach to governance with its MessageGate Activity Profile (MAP). This analysis creates a quick and inexpensive view of how organizations use email and the risks that rise from that

use. Recognizing these issues is imperative to implementing the right solution based on user needs.

- ☒ MessageGate Archive Categorization enables users to apply consistent email archiving policies before messages enter the archive. Classifying and categorizing email before it enters the storage network significantly streamlines the archival and retrieval process. MessageGate Archive Categorization can partition messages by category, enhance retrieval capabilities through policy-added metadata, and reduce archiving costs through the elimination of non-business email. 50–65% percent of email is non-business and does not need to be archived (alerts, newsletters, etc.).
- ☒ MessageGate Policy Enforcement prevents intentional and unintentional breaches while mitigating insider threats. The practical policy engine, numerous message dispositions, and policy-specific content enable companies to proactively manage their information flow and protect corporate secrets.
- ☒ MessageGate SenderConfirm covers most email governance issues caused by inadvertent or nonmalicious actions, which account for more than 90% of email misuse. Using predefined parameters and rules, SenderConfirm looks at the context and content of the message. If needed, it engages the sender. Any policy violations are displayed, providing an opportunity to stop the email before it is sent. This reduces risk by focusing on the easiest problem to solve — employee behavior. SenderConfirm builds organizational support and avoids employee embarrassment by providing an opportunity to stop email before it enters the system as a corporate record for IT review.

### **Strategic Direction**

MessageGate recently completed a comprehensive InfoWorld product review for its email governance platform, receiving a "very good" ranking of 8.6 out of a possible 10. According to review findings, MessageGate applies sophisticated email classification for message archiving as well as the ability to enforce usage policies within the live messaging stream. The platform applies categories based on policies and enhances retrieval by applying essential metadata to email records prior to archival. This drives retrieval costs down and optimizes existing archiving systems. The MessageGate platform also gained accolades for scalability. The component-based architecture scales based on customer needs, providing an attractive total cost of ownership and limited server requirements to process millions of emails per day. Additional components and features are also easily added, including MessageGate Activity Profile (MAP) services and SenderConfirm.

### ***MessageLabs***

#### **Overview**

MessageLabs provides a range of managed security services to protect, control, encrypt, and archive communications across email, Web, and instant messaging. MessageLabs currently protects more than 15,000 businesses worldwide, ranging from small business to Fortune 500, representing more than 6 million business end users across more than 80 countries. MessageLabs has regional headquarters in Gloucester,

United Kingdom; New York; and Sydney, Australia. The company has 400 employees across ten countries worldwide and was founded in 1999.

### **Information Protection and Control Products**

MessageLabs offers the following IPC products:

- Email Services defend organizations against email security threats, allowing clients to control email content and to secure communications in and out of their organization. Email Services includes:
  - Email Protect.** Multilayered antispam, antivirus, and antiphishing email services
  - Email Control.** Content control, image filtering, and advanced email management services
  - Email Secure.** Fully managed guaranteed boundary-to-boundary email encryption services
  - Email Recover.** Fully managed archiving service guaranteeing secure storage of corporate email
- Web Security Services provide Internet-level protect and control functionality to scan organizations' Web traffic for malicious code, spyware, adware, and phishing — at a low TCO. Sophisticated filtering can be achieved through control of user-level access to specific sites by category, MIME type, and file extension.
- Enterprise Instant Messenger Service is designed to optimize corporate IM use. The service eliminates risks and concerns arising from traditional instant messaging and file sharing offerings by providing secure communications, sophisticated administrative features, the ability to map existing enterprise hierarchical structures, IM logging capabilities, and interoperability with other consumer messaging networks.

### **Strategic Direction**

MessageLabs is focused on providing messaging security and management services to business. Delivered across a globally distributed platform at the Internet level, its fully managed services ensure the integrity of electronic communications, allowing clients to manage and reduce risk while securing their critical infrastructure and information. MessageLabs provides industry-leading services to guard against email threats such as viruses, spam, identity theft, and targeted blackmail campaigns, all of which jeopardize business continuity, regulatory compliance, reputation, and brand.

### ***Mirapoint***

#### **Overview**

Mirapoint provides comprehensive messaging and security solutions through purpose-built appliances designed to protect data networks. Mirapoint was founded in 1997 and has 230 employees headquartered in Sunnyvale, California. Mirapoint serves over 100 million mailboxes worldwide in the education, managed service provider, and enterprise verticals.

## Information Protection and Control Products

Mirapoint offers the following IPC products:

- ☒ The Mirapoint RazorGate appliance protects inbound and outbound emails through multilayered antivirus and antispam blocking in an easily deployed, easily managed appliance. Other features that protect emails include:
  - ☐ Outbound content filters that enable messages to be redirected, rejected, quarantined (for review by a compliance officer), or wiretapped (for archiving purposes)
  - ☐ Embedded policy engine that enforces recipient validation and recipient-based policies without querying the corporate directory inside the firewall for each message, therefore eliminating the need for firewall holes to the directory
  - ☐ Policy-based secure transmission of messages by requiring TLS on inbound and outbound connections
- ☒ Mirapoint Message Server appliance provides rich mail, calendaring, group scheduling, and address book, coupled with the inbound and outbound message protection provided by Mirapoint RazorGate. Other ways it protects messaging data include:
  - ☐ Fault tolerance built into the appliance hardware to minimize data loss as well as downtime
  - ☐ Policy-based enforcement of secure access from all types of clients (POP/IMAP, Web, mobile) using SSL and TLS
- ☒ Mirapoint Messaging Reporter (MMR) provides centralized logging and reporting for all devices — email security devices as well as mail servers — allowing administrators to mine data from any given period of time for up to 10 years. MMR's forensic capabilities trace messages quickly and effectively, indicating exactly what happens to every message traversing the system.
- ☒ The Mirapoint RazorSafe appliance, when functioning with the Mirapoint Message Server and RazorGate appliances, passively and discreetly copies email communications sent or received, including all header information, and indexes the messages and places them into a permanent archive. The message archive can be backed up securely to tape and then deleted from the originating journal mailbox.

## Strategic Direction

Mirapoint will continue to enrich its products to provide secure messaging from end to end (transmission, storage, access, archival, and policy-based administration). Mirapoint aims to build upon its content filtering capability with deep inspection of messages. Mirapoint will continue to grow and enhance its hybrid messaging solution, which enables companies to provide all employees with secure messaging functionality at a low total cost of ownership (TCO).

## ***Mobile Armor***

### **Overview**

Mobile Armor LLC is a Saint Louis, Missouri–based provider of enterprise mobile data security. Mobile Armor develops and markets the next-generation software suite that enables dynamic organizations to fully protect business, financial, and operating information and data.

### **Information Protection and Control Products**

Mobile Armor offers the following IPC products:

- ☒ MA Mobile Firewall Prevents unauthorized network access to mobile devices and keeps information secure from Internet vulnerabilities.
- ☒ MA Remote Network Integrated VPN solution is managed through the Mobile Armor PolicyServer, allowing secured communications between mobile devices.
- ☒ MA DataArmor Ensures device data security through strong authentication, advanced administration, and user-transparent data encryption.
- ☒ MA Virus Defense is a virus protection solution to protect against malicious virus attacks.

### **Strategic Direction**

With a data security system centered on its flagship PolicyServer software, Mobile Armor provides the ability to integrate its DataArmor full-disk strong encryption and preboot authentication security software with other security applications such as antivirus, firewall, and virtual private networking provided by Mobile Armor or others. Using an extensible, cross-platform client and enterprise scalable Web services–based architecture, Mobile Armor's security solutions enable rapid deployment of new and centralized security policies that are consistently and uniformly applied across the enterprise to all electronic devices such as servers, PDAs, desktops, laptops, tablet PCs, and smartphones.

## ***MX Logic***

### **Overview**

Founded in 2002 and headquartered in Englewood, Colorado, MX Logic Inc. is a managed security services provider of email and Web security services.

### **Information Protection and Control Products**

MX Logic offers the following IPC products:

- ☒ MX Logic Email Defense Service is a managed email security service that offers comprehensive protection against a wide range of email threats using a combination of proven spam filters, leading antivirus engines, fraud protection, content filtering, and email attack protection.

- ☒ MX Logic Web Defense Service is a Web security solution that effectively blocks quickly evolving Web threats, including spyware, viruses, and phishing attacks, while enabling greater control over unauthorized Web surfing by employees.

### **Strategic Direction**

MX Logic Inc. is a managed security services provider of email and Web security services. MX Logic strives to make the most user-friendly security solutions in the industry for enterprise-grade service and performance without enterprise-level complexity and cost. MX Logic's distinctions in 2006 include Security Products Guide's Global Excellence Customer Trust Award in Email Managed Service and *SC Magazine's* Award for Best Email Managed Service. MX Logic services are distributed through an extensive partner network.

### ***Oakley Networks***

#### **Overview**

Oakley Networks was founded in 2001 and is a privately held company backed by Kleiner Perkins Caufield & Byers, Duff Ackerman Goodrich, and Fidelity Ventures. The company has 180 employees and is headquartered in Salt Lake City, Utah.

#### **Information Protection and Control Products**

Oakley Networks offers the following IPC products:

- ☒ SureView is a host-based solution for exposing and eliminating insider threats at the desktop and a desktop product integrated with a complementary network appliance solution. By adding context and event correlation to behavioral visibility, SureView allows companies to make extremely targeted and informed decisions about remediation, ranging from simple user coaching and training to modifying or creating new business policies and procedures, even taking disciplinary actions including termination with documentation.
- ☒ CoreView is a network-based solution for insider threat mitigation that incorporates both comprehensive network traffic coverage and deep behavioral content analysis, capturing the entirety of packet-level activity for analysis and incident reconstruction and forensics. CoreView provides insight required to effectively expose and eliminate insider threats such as information exposure, data leakage, and improper business practices. CoreView scales to high-volume egress points and performs at wire speed for interdepartmental deployments.
- ☒ SureFind works behind the scene to silently and securely ensure confidential information is not compromised. SureFind will track any activity that has taken place, even if a new operating system has been installed, and tell customers whether the data located on a lost or stolen laptop has been exposed or compromised.

### **Strategic Direction**

Oakley Networks offers a network and host-based suite to provide enterprises with total visibility into the behavior of their users. Oakley Networks integrated solution gives enterprises the critical insight and Information they need to detect and eliminate

insider threats. Oakley Networks customers include Fortune 1000 enterprises and government customers.

## ***Orchestria***

### **Overview**

Founded in August 2000, Orchestria Corp. is headquartered in New York with additional sales offices in London; Boston; Washington, D.C.; Chicago; and Los Angeles. Orchestria helps organizations improve operational efficiency and eliminate risks in electronic communication by ensuring regulatory compliance, protecting intellectual property, and ensuring appropriate employee behavior. Its customers include many of the world's largest and most sophisticated corporations, such as Goldman Sachs, Bear Stearns, and Lehman Brothers.

### **Information Protection and Control Products**

Orchestria offers the following IPC products:

- ☒ Orchestria manages threats across all communication channels: email, instant messaging, BlackBerry-type devices, Webmail, and blogs. Additionally, Orchestria's technology is embedded in Bloomberg Professional, Instant Bloomberg, and leading archive providers.
- ☒ Orchestria's Active Policy Management approach detects policy violations in email and Web activity before the message is sent or the Web transaction is completed. Through Real-Time Prevention and Intelligent Review, Orchestria defines policies, accurately detects violations, and initiates the appropriate action.

### **Strategic Direction**

Orchestria helps organizations eliminate the risks in uncontrolled electronic communication by helping to prevent confidential data leakage, protecting intellectual property, encouraging appropriate employee behavior, and ensuring regulatory compliance. Orchestria controls threats across all electronic communication channels: email, instant messaging, BlackBerry-type devices, Webmail, and blogs. Additionally, Orchestria's technology is embedded in Bloomberg Professional, Instant Bloomberg, and leading archive providers. Orchestria's integration with leading archive vendors provides an unprecedented level of control for the full life of a message, from its creation through archive and retrieval.

Orchestria's family of control solutions is powered by intelligent policies that drive their core approach and take the risk out of business-critical electronic communication. Their technology works in real time to accurately detect policy violations in all electronic communication before the message is sent or the Web transaction is completed.

## ***PGP Corporation***

### **Overview**

Headquartered in Palo Alto, California, PGP Corporation is a global security software company focused on email and data encryption. PGP solutions are used by more than 80,000 enterprises, businesses, and governments worldwide. PGP solutions are utilized

by enterprises as part of a regulatory and audit compliance solution to protect confidential information, secure customer data, and safeguard companies' brands and reputations.

### **Information Protection and Control Products**

PGP offers the following IPC products:

- ☒ PGP Encryption Platform reduces the complexities of protecting business data by enabling organizations to deploy and manage multiple encryption applications cost-effectively from a single management console. Deployed with the first encryption application, the PGP Encryption Platform makes installing a separate or additional infrastructure unnecessary when the organization needs other encryption applications.
- ☒ PGP Whole Disk Encryption provides comprehensive, nonstop disk encryption, enabling quick, cost-effective protection for data on PCs, laptops, and removable media. The encrypted data is continuously safeguarded from unauthorized access, providing strong security for intellectual property, customer and partner data, and corporate brand equity.
- ☒ PGP Desktop Email delivers all the encryption functionality necessary for protecting an organization's email communications in a single solution. Secure email communications from the sender's email client to the recipient's is automatic, using centrally defined, policy-based encryption. PGP Desktop Email supports major email security standards and will interoperate seamlessly with most popular email security software solutions.
- ☒ PGP Universal Gateway Email is a standards-based enterprise gateway email encryption solution that offers centralized, automated key management, security policy enforcement, and secure Web-based message delivery options. The solution consistently secures confidential email and extends enterprise security policy to internal and external email users without requiring special training or client software.
- ☒ PGP NetShare enables collaborating teams to securely share sensitive files and folders on network shares. The encryption/decryption is performed transparently by PGP NetShare clients. Files remain protected during transport, backup, or copy operations and require no additional management or responsibilities for storage and network administrators.
- ☒ PGP Command Line enables organizations to automate protection of confidential information, securing it for local storage or transfer over the Internet. Integrating PGP Command Line into batch processes helps ensure compliance with corporate and regulatory information security mandates using the same PGP technology trusted to secure email communications and desktop storage.

## **Strategic Direction**

PGP Corporation announced record performance and results for 2006. PGP saw broad, balanced adoption of the PGP Encryption Platform around the world, with equal contributions from all PGP applications, including gateway messaging, endpoint messaging encryption, and full disk encryption.

The PGP Encryption Platform is the cornerstone of PGP product offerings. The PGP Encryption Platform provides a single, leveraged, and extensible architecture that reduces IT operational costs and eliminates duplicative tasks, systems, training, and support issues. The PGP Encryption Platform delivers an integrated encryption framework across the broadest range of encryption applications. The PGP Encryption Platform is deployed with the first PGP application installed to secure email, laptops, desktops, instant messaging, PDAs, IM, network storage, FTP, and bulk data transfers, or backups, enabling organizations to reap best-in-class encryption in phases or as business requirements emerge and evolve.

## ***PKWARE***

### **Overview**

PKWARE Inc. is a global software company providing ZIP solutions. The PKWARE solution has evolved over 20 years. PKWARE created PKZIP to simplify data exchange when limited bandwidth was the major issue. By allowing users to compress one or more large files within an electronic "container" that guards the files against corruption or interference, PKZIP entered the world of security.

### **Information Protection and Control Products**

PKWARE offers the following IPC products:

- ☒ SecureZIP ensures that information is protected throughout an organization as it is exchanged from platform to platform or at rest in electronic or physical storage. As a neutral format application, SecureZIP can be used to complement existing security investments.
  
- ☒ PartnerLink enables organizations to securely exchange information with partners outside corporate networks. Sponsor organizations can extend their security policies and best practices to an unlimited number of partners by offering them SecureZIP Partner, a free version of SecureZIP. This enables partners to securely send and receive information from their sponsors regardless of their computing platform and security infrastructure.

## **Strategic Direction**

PartnerLink helps address the escalating concern for protecting data in cross-enterprise exchanges. A specialized deployment of PKWARE's SecureZIP, which provides multiplatform file encryption and digital signature capabilities, PartnerLink provides a platform that enables the secure exchange of information between an enterprise and its customers, service providers, and suppliers — regardless of existing IT infrastructures.

PartnerLink is designed to overcome the implementation and interoperability obstacles faced by other data security tools, which have failed to facilitate the two-way secure exchange of data across diverse IT infrastructures. By providing one multiplatform conduit for businesses to freely share data with external partners and customers, PartnerLink overcomes complex and costly standardization procedures, lowers the cost and time of implementation and enables persistent data protection for files, whether in storage or transit.

## ***PointSec***

### **Overview**

Founded in 2000, Pointsec's North American headquarters are located in Lisle, Illinois. Its European headquarters are in Stockholm, Sweden. It also has offices in the Americas, Europe, and Asia. Pointsec protects PCs, laptops, PDAs, smartphones, and removable storage.

### **Information Protection and Control Products**

PointSec offers the following IPC products:

- ☒ Pointsec for PC offers full-disk encryption with access control. It is FIPS and Common Criteria certified, works with Linux or Windows, and is centrally managed.
- ☒ Pointsec Security for Mobile Platforms allows systemwide encryption with access control. Pointsec for mobile platforms provides encryption support not only for system memory but also for removable storage media such as flash cards and microdrives.

### **Strategic Direction**

Pointsec protects PCs, laptops, PDAs, smartphones, and removable storage and offers extensive certifications for mobile platforms. Its encryption works on PCs, laptops, removable media and wireless and handheld devices. It works easily with all Windows and Linux-based systems, and security can be customized with cards, tokens, and single sign-on to fit customer needs. Pointsec supports all the popular operating systems for PCs, PDAs, and smartphones as well as portable storage devices, providing file security for all stored information with hard drive encryption. Pointsec has also sold over 5,000,000 end point security licenses worldwide.

## ***Postini***

### **Overview**

Founded in 1999 and headquartered in Palo Alto, California, Postini customers include more than 35,000 businesses worldwide, across a wide range of industries.

## **Information Protection and Control Products**

Postini offers the following IPC products:

- ☒ Postini Email Security ensures email customers are protected from email-based external threats and junk mail. It blocks spam, viruses, phishing, and email threats and provides sophisticated message management and policy enforcement.
- ☒ Postini Web Security blocks spam, viruses, phishing, malware, and spyware from collecting information on users and prevents information leaks by blocking outbound data transmissions from spyware-infected desktops.
- ☒ Postini IM Security stops IM-borne threats from reaching the network and enables the monitoring and archiving of IM. Administrators can set IM access policies, control inbound and outbound IM file transfers, filter conversations for inappropriate or sensitive content, and archive IM sessions for future search and retrieval.
- ☒ Postini Policy Enforced TLS employs transport layer security to automatically encrypt email connections between businesses. Postini integrates strong TLS encryption with policy-based management so you can control and ensure which messages are delivered over encrypted connections.
- ☒ Postini Message Archiving provides a secure and effective way for companies to manage their email and IM archiving. It also provides compliance and management for archiving policies. Postini Message Archiving is an online search interface for email discovery and retrieval that simplifies ediscovery processes and reduces costs. Postini Message Archiving also includes personal archive functionality that provides end users and IT administrators a simple way to access archived email directly from desktops.
- ☒ Postini Message Encryption provides a secure and effective way for companies to encrypt their email communications with individual customers based on business policies. Consumers can retrieve the contents of encrypted email after authentication without requiring any extra software or complex digital certificates.

## **Strategic Direction**

Postini is a pioneer in the software-as-a-service approach to providing communications security and compliance and holds two fundamental patents in the space, with more patents pending. Their patented "stateless" architecture and redundant global datacenters are backed by certifications such as SAS 70 Type II, WebTrust, and the Department of Commerce/UE Safe Harbor. Postini continues to invest and innovate solutions that provide effective security and compliance across multiple communication channels and increase business productivity. The Postini Message Center is available in 14 languages, with service and support available 24 x 7 worldwide with proven 99.999% reliability. As an on-demand service, there is no software or hardware to buy, install, maintain, or upgrade. Administrators use standard Web browsers to manage the system, and users seamlessly continue to use their existing email, IM, and Web software. Postini serves over 35,000 businesses through direct and 1,700 business partners.

## ***Proofpoint***

### **Overview**

Proofpoint, founded in June 2002, is a privately held messaging security company headquartered in Cupertino, California. Investors include Benchmark Capital, Mohr-Davidow Ventures, Meritech Capital Partners, RRE Ventures, and Inventures Group. Proofpoint is especially strong in large enterprise deployments, with key customers including Kaiser Permanente, Hitachi Data Systems, Bank of America, Tyson Foods, and National Instruments.

### **Information Protection and Control Products**

Proofpoint offers the following IPC products:

- ☒ Proofpoint Messaging Security Gateway (appliance), Proofpoint Messaging Security Gateway — Virtual Edition (virtual appliance), and Proofpoint Protection Server (software) are Proofpoint's enterprise-class messaging security platforms. Proofpoint provides gateway protection from both inbound and outbound message-borne threats, with a wide variety of options including antispam, antivirus, zero-hour antivirus, structured and unstructured outbound content scanning, policy-based encryption, and multi-protocol IPC. Proofpoint offers a virtual appliance form factor, which offers all of the same antispam, antivirus, data privacy, and intellectual property leak prevention features found in Proofpoint's physical appliances in a virtual appliance for VMware's virtualization products.
- ☒ Proofpoint Regulatory Compliance helps organizations comply with a wide variety of data protection and privacy regulations including HIPAA and GLBA. This module monitors outbound messages for a wide variety of personal identifiers, private financial, and healthcare information, including credit card numbers, ABA routing numbers, social security numbers, and U.K. national insurance ID numbers as well as HIPAA "codesets," such as standard disease, drug, treatment, and diagnosis codes. A wide variety of disposition options are available, including blocking/quarantining messages that contain private information or automatically encrypting such messages before sending.
- ☒ Proofpoint Digital Asset Security protects against leaks of confidential information and intellectual property. Proofpoint's MLX machine learning technology is used to analyze and classify confidential documents and then monitors outbound message streams for that information. Messages can be blocked or otherwise disposed of with a wide variety of disposition options. More than 400 document types are supported, and new or proprietary document types can be added to the system. The product interfaces to filesystems, databases, content management systems (including EMC Documentum systems), and other external applications to enable automatic indexing of new or modified confidential information.
- ☒ Proofpoint Network Content Sentry is a separate appliance that extends Proofpoint's email-based outbound content security features to additional message streams including HTTP and FTP. The appliance can detect private and confidential information in Web-based email, blog postings, message board postings, and FTP transmissions, using the same policies defined in other Proofpoint modules.

- ☒ Proofpoint Secure Messaging incorporates identity-based encryption technology OEMed from Voltage Security to add policy-based encryption capabilities to a Proofpoint deployment. The product automatically and dynamically applies encryption or decryption to messages based on deep inspection of message contents and the organization's defined policies at the enterprise gateway. IBE technology eliminates the infrastructure, certificate, and key management overhead traditionally associated with encryption systems. Proofpoint also maintains technology partnerships with other leading secure messaging vendors, and its platform easily integrates with third-party encryption systems.

### **Strategic Direction**

Proofpoint continues to see strong adoption of its policy-driven email encryption solutions across the company's core enterprise, healthcare, financial services, university, and government markets. The Proofpoint Regulatory Compliance, Proofpoint Digital Asset Security, and Proofpoint Secure Messaging modules work together to add powerful, policy-driven encryption features to the Proofpoint Protection Server software and Proofpoint Messaging Security Gateway appliance.

IDC believes Proofpoint's Messaging Security Gateway Virtual Edition is an early example of a new form factor for security appliances that IDC expects to pick up steam over the next few years. A confluence of technologies has made it possible for the concept of a software appliance to move from just that — a concept — to a reality in the market. Without the impending widespread deployment of virtualization technology, software appliances would be nothing more than an interesting idea without a market to exploit. But once the majority of servers have a hypervisor layer in place, the infrastructure is in place to support multiple operating systems, each carrying one or more application workloads. This same many-to-one multiplexing of operating system images aboard servers also makes it possible to locate software appliance functionality aboard these same servers, leveraging otherwise unused capacity.

### ***Provilla***

#### **Overview**

Provilla Inc.'s flagship product, LeakProof, prevents information leakage of sensitive data by combining endpoint-based enforcement with fingerprinting technology called DataDN. Provilla is headquartered in Mountain View, California.

#### **Information Protection and Control Products**

Provilla offers the following IPC products:

- ☒ LeakProof is a solution for securing mobile devices and preventing internal security violations. It helps with information leak protection identity theft and compliance. LeakProof prevents data leaks without compromising legitimate communications through superior, content-aware endpoint enforcement of granular security policies.
- ☒ DataDNA Server is a dedicated network appliance, working in conjunction with LeakProof A/L Agents to identify and prevent data leakage violations.

## **Strategic Direction**

Provilla has an OEM agreement with Reconnex, a provider of network-based information monitoring and protection solutions, to provide its flagship LeakProof intelligent endpoint solution to Reconnex customers. As part of the agreement, Provilla LeakProof will be integrated with the Reconnex Information Protection System, offering complete protection for data in motion, data at rest, and data in use.

Provilla has also agreed to license the patented DataDNA technology and LeakProof agent to BigFix Inc. Comprehensive forensics and on-demand scanning of all confidential data throughout the organization provide powerful tools for addressing compliance regulations such as PCI, CA SB-1386, GLBA, and Sarbanes Oxley, enabling enterprises to determine if confidential, unencrypted data exists on laptops and desktops.

## ***Reconnex***

### **Overview**

Headquartered in Mountain View, California, Reconnex offers purpose-built appliance solutions that allow visibility into and protection over critical content on all ports and for all types of connections.

### **Information Protection and Control Products**

Reconnex offers the following IPC products:

- ☒ iGuard appliance provides a hardened, turnkey solution for information monitoring and protection to address privacy and protect intellectual property assets. Deployed at the network egress points, iGuard operates passively in tap mode with no impact on overall network performance.
- ☒ inSight console provides a centralized interface for managing all security policies as well as alerting and reporting. It supports multiple levels of access for multiple classes of users, ensuring usage flexibility. Through inSight, IT can configure and manage the iGuard appliance, including multisystem management across multiple devices.
- ☒ Reconnex 6.0 Endpoint Agent extends full discovery, monitoring, capture, and prevention capabilities to all enterprise endpoints, including mobile devices and removable media.

## **Strategic Direction**

Reconnex provides three stages of information protection: before it becomes a risk by discovering information at rest, during the transmission of information in motion, and after, by capturing network events related to information at rest and in motion to identify previously unknown risks. Today, Reconnex protects information assets for over one million users.

## ***RSA***

### **Overview**

Now part of EMC, RSA spent the better part of 2005 and early 2006 acquiring technology vendors such as PassMark and Cyota in an effort to broaden and strengthen market reach. RSA has long been the leader in the traditional hardware authentication token space, and its SecureID tokens are used by Fortune 2000 companies worldwide.

### **Information Protection and Control Products**

RSA offers the following IPC products:

- ☒ RSA BSAFE tools provide a complete portfolio of solutions for developers to meet the wide-ranging security goals of their applications. Architecting applications using the RSA BSAFE security tools allow customers to achieve a good, secure application design without greatly increasing development timelines or costs.
- ☒ RSA Enterprise Data Protection solutions provide comprehensive data security infrastructure and are designed to help companies implement appropriate information-centric security controls at every point in the information life cycle to ensure data is always protected without breaking existing data flows and business processes.

### **Strategic Direction**

With the purchase of RSA, EMC has inherited a diverse security portfolio. RSA has tremendous brand-name recognition in security circles and enjoys the reputation of providing top-of-the-line security technology. RSA is the premier provider of security solutions for business acceleration. As the chosen security partner of more than 90% of the Fortune 500, RSA helps the world's leading organizations succeed by solving their most complex and sensitive security challenges. In September 2006, after over 20 years providing leadership to the security industry, RSA Security joined forces with EMC Corp. and Network Intelligence to form the Security Division of EMC. Driving this merger is the recognition that customer needs have changed and traditional approaches to information security are no longer sufficient. Increasingly, what should be a company's most important company asset — information — is its greatest liability.

In response, RSA is ushering in a new information-centric approach to security that will empower leading companies worldwide to address these challenges and move ahead with the confidence to compete and win in today's marketplace. Fueling our mission is the passionate belief that security should be about lifting business limitations, not imposing them.

### ***Secure Computing***

#### **Overview**

Secure Computing Corp. (Nasdaq: SCUR), an enterprise gateway security company, delivers a set of solutions that help customers protect their critical Web, email, and network assets. Over half of the Fortune 50 and Fortune 500 companies are part of

the Secure Computing customer base of more than 19,000 global customers worldwide.

### **Information Protection and Control Products**

Secure Computing offers the following IPC products:

- ☒ Messaging Gateway Security provides administrators and compliance officers with control over defining policies and mapping them to specific business processes, monitoring and detecting violations, enforcing policy, and encrypting messages as necessary.

### **Strategic Direction**

In July 2006, Secure Computing acquired CipherTrust. The combined company will be positioned as a leader in the enterprise gateway appliances market, featuring a comprehensive, integrated, and unified portfolio of solutions — including unified threat management (UTM), messaging security, Web filtering, and identity management — with centralized policy and management capabilities. Together, these products will address network gateway and application gateway security for all of the major Internet protocols, including Web (HTTP and FTP), email (SMTP and POP), and instant messaging and identity-based access protection.

IDC believes the secure content management (SCM) market and threat management market are quickly evolving from standalone products to more comprehensive and integrated security solutions. IDC believes CipherTrust's messaging security complements Secure Computing's focus on unified threat management, Web filtering, and hardware authentication. With messaging increasingly viewed as a critical enterprise application, the ability to secure traffic at wire speeds is a critical business enabler. Moreover, CipherTrust's TrustedSource reputation technology, with its network of thousands of sensors throughout the Internet, will add a new element of sophistication and intelligence to existing UTM and SCM products.

### ***Sendmail***

#### **Overview**

Sendmail is a leading provider of policy-centric solutions for securing and authenticating business communications. Based on the world's first Internet Mail server, developed 25 years ago by Sendmail founder Eric Allman, Sendmail provides enterprises directory-driven, policy-based message processing to address both internal and external threats in a single, integrated platform. Large enterprises across 33 countries, including the majority of the Fortune 1000, rely on Sendmail to protect sensitive data and intellectual property, eliminate unwanted messages, and effectively manage their mail stream to maintain brand and shareholder value and comply with security and regulatory policies. Sendmail is headquartered in Emeryville, California, with offices and distributors in Europe, Asia, and North America.

## Information Protection and Control Products

Sendmail features a secure and open architecture designed to deliver information protection and control and ensure trusted messaging. Built on a flexible policy engine, Sendmail products provide control at any point within the message life cycle. The protection covers four strategic areas:

- ☒ **Clean Messaging.** Multiple options for spam, virus, and malware defense, including zero-hour protection, combined with solutions to defend targeted denial of service and directory harvesting attacks
- ☒ **Compliant Messaging.** Out-of-the-box policy to support regulatory and corporate compliance such as SOX, HIPAA, GLBA, EU Data Protection, and content filtering applied to inbound, outbound, and internal messaging
- ☒ **Secure Messaging.** Peer-to-peer and server-to-server policy-driven message encryption
- ☒ **Authenticated Messaging.** Support for all the leading sender/recipient domain validation technologies (DKIM, DK, SIDF, SPF) combined with IP reputation services

Sendmail offers the following IPC products/services:

- ☒ Sentrion is an enterprise-class, policy-driven security appliance (or soft appliance) that delivers real-time control over messaging to shield end users, safeguard the messaging infrastructure, protect content, and enable compliance. Sentrion provides advanced security capabilities to block spam and viruses and eliminate targeted attacks and fraud. The Sentrion appliance provides protection for both the inbound and the outbound message streams.
- ☒ Sentrion policy management lets businesses build and maintain a library of business rules for their entire enterprise. These rules can be quickly and easily applied to all email messages, whether inbound or outbound, helping to better manage and respond to ongoing email threats. Policies allow virtually any action to be taken on any message based on any condition, protecting organizations from the loss of intellectual property through email, as well as enforcing regulatory mandates or acceptable use policies on outgoing messages.
- ☒ Sendmail Encryption is a policy-based and fully automated clientless, encryption, decryption, and digital signing solution that integrates technology from Voltage Security and Sendmail for 360-degree management and security over business communications. Sendmail Encryption enables message encryption, decryption at the gateway without the complexity of certificates, Certificate Revocation Lists (CRLs), and other costly infrastructure. Sendmail Encryption is non-intrusive; all email traffic, whether encrypted or not, can be processed by antispam, antivirus, content filtering, and archiving solutions. Leveraging policies for privacy, Sendmail Encryption delivers HIPAA/SB1386 compliance to corporate messaging.

- ☒ The Sendmail Risk Assessment Service uncovers the security and compliance risks in outbound email based on a 48-hour analysis period. This unique service is key to determining the true compliance, security, and operational risks in email prior to initiating an education, enforcement, and blocking strategy.
- ☒ To correlate events from disparate applications within the messaging environment, Sendmail Auditor provides forensics and audit/compliance reporting. This includes reporting from all Sendmail products and applications like Exchange, Notes, and McAfee. The result is an integrated email auditing solution that provides the ability to quickly aggregate, retain, and mine log data for troubleshooting, forensics, governance, compliance, and advanced reporting.

### **Strategic Direction**

Sendmail continues to innovate to assist companies in securing the valuable assets that exist within their email infrastructure, from the business processes that email supports to the content delivered in email that represents the corporate memory of a company.

Sendmail announced enhancements to its IPC offerings with a number of significant product releases designed to support the growing need for bidirectional, policy-centric message processing and protection. To support the growing need for compliance and outbound message processing, the new releases provide built-in clientless encryption and policies for HIPAA and GLBA to prevent confidential information leakage from within.

## ***Sigaba***

### **Overview**

Sigaba is headquartered in San Mateo, California. Originally founded in 2000, Sigaba has offices in major cities across North America. Sigaba is privately held, with funding from Liberty Partners and Royal Wulff Ventures.

### **Information Protection and Control Products**

Sigaba offers the following IPC products:

- ☒ Sigaba Secure Email is a premier enterprise secure messaging solution for business, financial institutions, governments, healthcare, and other organizations with a compelling need to protect confidential information.
- ☒ Sigaba Secure Statements is a leading solution for creating, managing, and sending electronic statements for end-to-end secure document delivery. It addresses risks associated with sending financial statements and protected health information.
- ☒ Sigaba Secure IM is a secure instant messaging and presence solution built for the enterprise. Sigaba Secure IM allows corporate users to conduct secure multiuser conversations from their desktops and other platforms, enabling easy collaboration within and among workgroups, between enterprises, or across a business customer base.

- ☒ Sigaba Secure Messaging for Mobile Devices is a leading enterprise secure messaging solution that enables users of mobile devices, such as PDAs, to send and receive messages securely, from the beginning to the end of transmission.

### **Strategic Direction**

Sigaba solutions enable organizations to secure sensitive information in B2B, B2C, and B2G applications, while automatically enforcing the strictest compliance with industry, government, and regulatory requirements. SigabaNet, Sigaba's services oriented architecture, provides a framework for building custom secure applications. By separating authentication from encryption, Sigaba delivers message-level security and accurate, up-to-the-moment audit trails. Leveraging this platform, Sigaba has developed its award-winning messaging solutions — Sigaba Secure Email, Sigaba Secure Statements, Sigaba Secure Mobile Devices, and Sigaba Secure Instant Messaging — enabling financial services, government, and healthcare customers to meet the most demanding privacy requirements of GLBA, HIPAA, and SEC.

The company is a member of the Anti-Phishing Working Group (APWG), Financial Services Technology Consortium (FSTC), Organization for Advancement of Structured Information Standards (OASIS), and Liberty Alliance and is instrumental in making federated authentication a reality for governments and enterprises worldwide.

Sigaba's future direction is to extend its corporate policy creation, enforcement, and reporting capabilities for preventing leakage of intellectual property, confidential information, and customer privacy data.

### ***SonicWALL***

#### **Overview**

Founded in 1991, SonicWALL Inc. designs, develops, and manufactures network security, secure remote access, Web and email security, continuous data protection, and policy and management solutions. Offering appliance-based products as well as value-added subscription services, SonicWALL's comprehensive array of solutions provides enterprise-class Internet and data protection without any compromises.

#### **Information Protection and Control Products**

SonicWALL offers the following IPC products:

- ☒ SonicWALL's Email Security suite was introduced in 2006 after SonicWALL's acquisition of MailFrontier. The security suite delivers high-performance, easy-to-use inbound and outbound email threat protection for organizations of all sizes.
- ☒ SonicWALL Email Security 5.0 also enables organizations to address Sarbanes-Oxley, GLBA, HIPAA, and other compliance requirements by leveraging functionality, including:
  - ☐ Record ID matching (detect Social Security, credit card, and other predefined and custom records), predefined dictionaries (healthcare and financial), and predefined policies that complement powerful existing policy management and content filtering functionality to identify noncompliant messages

- ❑ Encryption routing using third-party products and built-in TLS encryption along with on- and off-box email archiving that extends existing remediation options such as log, block, route, copy to, or put in approval box
- ❑ Compliance reports that augment the existing reporting module and powerful email auditing functionality to provide a clear view of email traffic

### **Strategic Direction**

In early 2006, SonicWALL announced that it had acquired email security company MailFrontier Inc. for a consideration of approximately \$31 million in an all-cash transaction. The purchase of MailFrontier enables SonicWALL to bring powerful, easy-to-manage email security to channel partners and their end users as part of its end-to-end suite of secure content protection. MailFrontier's customers will benefit from the integration of SonicWALL's secure content management and unified threat management capabilities, while SonicWALL's distributed enterprise customers will have access to a further range of offerings for the midmarket.

The launch of the Email Security line of appliances reflects SonicWALL's commitment to enhancing the technology already in use with MailFrontier's 2,000-strong mid-enterprise customer base, and to making the technology widely available to an expanded user base at a highly competitive price point. Through its global network of 10,000 channel partners, SonicWALL's customers can now take advantage of richly featured email threat protection as part of the company's extended security suite comprising network security, business continuity, and secure content management.

## ***Sophos***

### **Overview**

Sophos is a trusted, global provider of integrated threat management solutions, protecting businesses against viruses and spam and enforcing corporate messaging policies. Over 35 million users in 150 countries are protected by Sophos technology.

### **Information Protection and Control Products**

Sophos offers the following IPC products:

- ☒ PureMessage for Unix is a secure email gateway solution providing integrated antivirus, antispam policy enforcement and powerful email management. It delivers reliable, proactive protection against inbound and outbound email-borne threats through a highly flexible and easy-to-use administrative interface through a combination of infrastructure, detection techniques, and an extensible message processing architecture.
- ☒ The PureMessage for Unix Extended Policy module addresses a broad set of security and mail filtering requirements with rich hierarchical policy controls, a database-driven quarantine, and hooks for third-party integration. The extended policy module allows policies to be configured for subgroups within an organization to reroute or tag messages based on message attributes for specific keywords, phrases, or patterns.

- ☒ The PureMessage Compliance Toolkit simplifies the challenge presented by regulatory compliance by enabling organizations to capture and contain compliance violations before they occur. It provides the tools to manage compliance quickly and effectively by implementing a lexicon of industry- and company-specific tests to identify potentially sensitive materials entering or leaving the network. These messages are routed to compliance quarantine for review through a compliance officer interface designed for managing, monitoring, and reporting on compliance policies.
- ☒ PureMessage Policy Router sends pristine, non-augmented messages to a third-party machine such as encryption and archiving servers on a selective basis according to the PureMessage policy. The Policy Router provides simple, seamless transfer of messages to another machine in their original state and condition, providing uncomplicated message routing using familiar policy rules.

### **Strategic Direction**

Sophos provides virus and spam solutions for organizations of any size, from large enterprises to small businesses. Sophos' strategic direction focuses on long-term cost-of-ownership reduction. The company's products are sold and supported through a global network of subsidiaries and partners in more than 150 countries. In addition, virus and spam experts based at Sophos' high-security research laboratories in the United Kingdom, the United States, Canada, and Australia carry out 24-hour analysis to ensure rapid response to any new threat anywhere in the world, irrespective of time zone.

Driven by mounting pressures to ensure a secure and low-cost infrastructure, Sophos will continue to focus on providing consolidated protection against security threats such as viruses, spam, and policy breaches.

### ***SurfControl***

#### **Overview**

SurfControl has 12 offices worldwide with headquarters in the United States and the United Kingdom and sales offices in France, Germany, Australia, China, and Singapore. SurfControl has more than 20,000 customers and is a leading supplier of unified threat management for email, Web, IM, P2P, mobile, and desktop protection.

#### **Information Protection and Control Products**

SurfControl offers the following IPC products:

- ☒ E-mail Filter for SMTP is a preconfigured product offering antivirus, antispyware, antiphishing, malicious URL link detection within emails, plug-and-play deployment, automated updates, and easy management of both inbound and outbound filtering and content compliance. It employs flexible and customizable policies to help protect against loss of intellectual property and safeguard the privacy of organizations and individuals as electronic content is transferred in, out, and around organizations. File attachments, archive files, and embedded file attachments are extracted and interrogated against each organization's compliance rule sets.

- ☒ SurfControl E-mail Filter for Exchange provides internal messaging security for organizations by protecting against inadvertent distribution of confidential information to unauthorized departments or individuals. In addition, E-mail Filter for Exchange also protects customers' safe and productive working environments by ensuring no offensive or harassing language, including inappropriate jokes sent within an organization.
- ☒ SurfControl RiskFilter — E-mail is a turnkey enterprise email security appliance. Quality content recognition, multilayered blended threat protection, antivirus technologies, and ease of use, combined with extensive reporting and analysis, provide the tools and flexibility to protect organizations from every form of harmful and inappropriate content in both inbound and outbound emails.
- ☒ SurfControl Enterprise Threat Shield enforces appropriate-use policies in real time at the endpoint. It proactively detects, prevents, and removes unapproved instant messaging applications, peer-to-peer applications, spyware applications, and games that can compromise confidentiality, data integrity, or operations. Enterprise Threat Shield's rules-based policy enforcement ensures that only approved users run the approved IM tool and only at approved times.

### **Strategic Direction**

SurfControl protects organizations with multiple layers of threat protection that filter inbound, outbound, and internal Internet traffic. SurfControl's Enterprise Protection Suite protects multiple threat vulnerability points — Web, email, IM, P2P, and mobile users, and endpoint protection — and is supported by SurfControl's worldwide Adaptive Threat Intelligence Service to provide customers with early detection of emerging threats, real-time updates, and continuous protection.

SurfControl's vision continues to become more relevant as threats increasingly blend multiple methods of transmission and extend into more Internet technologies. SurfControl will continue to provide customers with unified threat protection solutions that fit seamlessly into their enterprise security infrastructure and control threats before they jeopardize the network and the business.

## ***Symantec***

### **Overview**

Symantec is a United States-based company that was founded in 1982. The company held its initial public offering in June of 1989 and is headquartered in Cupertino, California. Employer to more than 14,000 people, Symantec has operations in more than 40 countries, including all over the United States as well as in Canada, New Zealand, Japan, and Australia.

### **Information Protection and Control Products**

Symantec offers the following IPC products:

- ☒ Enterprise Vault Symantec provides a software-based intelligent archiving platform that stores, manages, and enables discovery of corporate data from email systems, file server environments, instant messaging platforms, and

content management and collaboration systems. Enterprise Vault uses intelligent classification engines to manage data, improving a company's ability to retain and protect corporate information while reducing storage costs and simplifying management.

- ☒ Mail Security 8300 Series Symantec appliances feature integrated, antispam, antivirus, and content-filtering technologies that stop inbound and outbound email-borne threats from negatively impacting productivity and compromising security. The new Premium Content Control add-on subscription helps organizations manage risks associated with data leakage, regulatory compliance (HIPAA, GLBA, and PCI), and internal governance.
  
- ☒ Information Foundation 2007 delivers protection from risks to messaging and collaboration systems and helps reduce the cost of data retention and electronic discovery. The integrated product suite protects against data leakage, spam, and other unwanted content and provides centralized, multisource archiving and retention of information across the enterprise.

### **Strategic Direction**

Symantec for the past few years has competed in secure content markets and augmented those solutions with acquisitions. The new Symantec has organized itself around five operating segments: consumer products, security and data management, datacenter management, services, and other.

Symantec acquired IMlogic in January 2006. The acquisition of IMlogic signals that Symantec's two-year-old buying binge continues. In the past two years, Symantec has bought BindView Development, Brightmail, Liric, Sygate Technologies, TurnTide, WholeSecurity, and storage giant VERITAS Software. In October 2005, executives at Symantec said that the company planned to make six to eight acquisitions a year, with a major deal every 18 months. The merging of BindView's agentless technology with Symantec's complementary products created a solution that enables customers to meet the critical demands of their IT infrastructures. The combination of BindView's medium-sized company client base with Symantec's large enterprise focus will make Symantec the leader in the security and vulnerability management market in 2006.

In January 2007, Symantec Corp. announced it had signed a definitive agreement to acquire Altiris Inc., a leading provider of IT management software that enables businesses to manage and service network-based endpoints, from mobile devices, laptops, and desktops to servers and storage assets.

Specific to its acquisition of IMlogic, Symantec customers will eventually have the ability to secure the full life cycle of business-critical messages, including email and IM, and have a one-stop shop for compliance and hygiene. IMlogic was available via a service or as on-premises software, or via an appliance, and Symantec is committed to offering customers the same choices for its combined platform going forward, though full integration of the products will take some time (as a reference, Symantec set aside 12 months to integrate its larger acquisition of VERITAS/KVS with Symantec products). Symantec has a substantial customer base for its email appliance products and plans to offer customers the convenience of adding IM security on existing turnkey appliances (SBAS, 8000) "with the flip of a switch."

## **Tablus**

### **Overview**

Tablus, Inc. is a leading provider of comprehensive content loss prevention solutions. Founded in 2002, this Silicon Valley company's technology locates, monitors, and protects sensitive enterprise information from potential loss or misuse. By preventing such disclosures, Tablus helps organizations protect sensitive content, reduce legal and financial risk, preserve brand equity and competitive advantage, and prove regulatory compliance. Tablus is privately held, with Series "B" funding from Trident Capital and Menlo Ventures completed in October 2006.

### **Information Protection and Control Products**

Tablus offers the following IPC products:

- ☒ Tablus Content Sentinel discovers sensitive content stored on laptops, desktops and servers in large corporate environments. With its patent-pending ZettaScan Architecture, Content Sentinel brings the software to the data versus the data to the software. This distributed architecture utilizes unique temporary and permanent agents as well as grids to enable organizations to scan thousands of computers and very large data repositories in parallel, while virtually eliminating network impact and reducing scan time from months to hours.
- ☒ Tablus Content Alarm NW is a precise network monitoring and blocking solution. It continuously monitors, accurately detects, and blocks or quarantines the outbound transmission of confidential content via the network, supporting most network communications, not just email.
- ☒ Tablus Content Alarm DT provides visibility and control over confidential information in use on laptops and desktops, enabling organizations to monitor content activity for irregularities, alert users to at-risk processes, and ultimately stop the misuse of data before it happens.

### **Strategic Direction**

Tablus, Inc. provides comprehensive content loss prevention solutions to protect against the accidental loss or misuse of sensitive content. This includes personally identifiable information (PII), customer information, financial statements, or information governed by the Payment Card Industry (PCI) Standard, design specifications, and source code.

The complete Tablus Content Loss Prevention Suite enables enterprises to locate, monitor, and protect sensitive content from loss or misuse — regardless of whether it is at rest, in motion, or in use. This unique approach makes it possible to identify sensitive content stored or in transit anywhere on the network or in use on the desktop. It then manages that content in precise accordance with any number of policies. The complete Tablus suite enables organizations to comply with privacy regulations, reduce legal and financial risk, safeguard trade secrets, and protect customer data, corporate assets, and brand equity.

VeriSign will use the Tablus Content Sentinel solution as part of the VeriSign Payment Card Industry (PCI) onsite audit and scanning services practice. VeriSign is an authorized security assessor for PCI Compliance to assist merchants and service providers with required annual audits. The PCI Data Security Standard was created by major credit card companies to safeguard customer information. Visa, MasterCard, American Express, and other credit card associations mandate that merchants and service providers meet certain minimum standards of security when they store, process, and transmit cardholder data.

### ***Trend Micro***

#### **Overview**

Trend Micro Inc., which is headquartered in Tokyo, Japan, is a global leader and innovator in secure content and threat management. The company's products and services protect businesses and consumers from viruses, worms, spyware, spam, phishing, and other security threats. Since its inception in 1988, the company has established offices and representation in more than 30 countries. The company is traded on the Tokyo Stock Exchange (4704).

#### **Information Protection and Control Products**

Trend Micro offers the following IPC products:

- ☒ **InterScan Messaging Security.** Trend Micro InterScan Messaging Security solutions integrate antispam and antiphishing with antivirus and antispymware. Innovative techniques such as customer-specific reputation services and patent-pending image spam detection keep customers safe as threats evolve while predictive techniques such as zero-day protection, advanced heuristics, and behavior analysis block targeted attacks. This comprehensive email protection also provides flexible content filtering to enforce compliance and to prevent data leakage. This solution is offered in software, appliance, and hosted versions. With a highly scalable platform and centralized management for easy administration, the solution is optimized to block the full range of standalone, blended-threat, and customer-specific email attacks at the gateway
- ☒ **Trend Micro ScanMail** solutions deliver effective, high-performance mail server security — with antivirus and antispymware, as well as antispam and antiphishing. Innovative techniques — such as zero-day protection, image spam detection, and advanced heuristics — and optional threat management services keep customers safe even as threats evolve. Additionally, flexible content filtering can be utilized to enforce compliance and to prevent data leakage. Trend Micro ScanMail solutions are optimized for the email environments they secure (including Microsoft Exchange Server and IBM Lotus Domino) and integrate tightly with existing IT infrastructure to reduce IT impact, infrastructure, and management costs.
- ☒ **Instant Messaging Security for Microsoft Office Live Communication Server.** Trend Micro IM Security for Microsoft Office Live Communications Server (LCS) delivers protection from malicious code and inappropriate content. IM Security can be centrally managed and administered and runs with minimal performance impact

to LCS. Incident-based archives support quick and easy searches for content violations. Complete with instant notification through LCS and comprehensive real-time reporting, IM Security helps administrators deploy and maintain a virus-free IM environment with secure content. IM Security has the ability to filter inbound and outbound instant messages/files with predefined dictionaries (lexicons) or manually created content policies. IM Security policy is built with Active Directory integration so that organizations can create ethical walls between AD users or user groups. IM Security offers the ability to archive, block, and quarantine instant messages to assist in enterprise IM compliance management. IM Security also integrates with Live Communication archive server and is capable of indexing conversations based on content policies. Administrators can easily query an instant message conversation in its original format.

### **Strategic Direction**

Trend Micro provides multilayered security that protects gateways, servers, desktops, and mobile devices against malware and content security threats. As botnet attacks become more malicious and sophisticated, solutions such as Trend Micro's Botnet Identification Service will play an increasingly valuable role in protecting both consumer and enterprise environments. We expect botnet attacks to increase in volume, sophistication, and severity. IDC believes the Botnet Identification Service is an ideal solution to help ISPs identify and quarantine customers whose PCs have been infected.

Today, Trend Micro ScanMail for Microsoft Exchange, ScanMail for Lotus Domino, PortalProtect for Microsoft SharePoint Portal Server, and Windows SharePoint Services also provide internal messaging content compliance capabilities. Trend Micro InterScan Web Security Suite, with its URL filtering, Web-email scanning, antispymware, and "phone home" blocking capabilities, can also address further HTTP/FTP-based outbound compliance concerns. Trend Micro is committed to further development of compliance-related products and features across all of its products and believes that integration of these features and capabilities into existing products, where appropriate, is the best approach for easiest deployment, management, and lower total cost of ownership.

### ***Tumbleweed Communications***

#### **Overview**

Tumbleweed Communications Corp. was founded in 1993 and held its initial public offering in 1999. The company is a recognized leader in providing secure Internet communication software and appliances for enterprises and government customers of all sizes. Products include antispam, content filtering, email encryption, managed file transfer, and PKI validation. The company has over 300 employees around the world and is headquartered in Redwood City, California, with offices across the United States and Europe as well as in Hong Kong, Singapore, New Zealand, and Australia. Research and development is staffed out of three locations — Redwood City, California; Hurst, United Kingdom; and Sofia, Bulgaria. This includes Tumbleweed's 24x7 Message Protection Lab. The company is trusted by over 1,400 enterprise customers around the world that use Tumbleweed products to communicate securely with over 10,000 corporations and millions of end users.

## Information Protection and Control Products

Tumbleweed Communications offers the following IPC products:

- ☒ Tumbleweed MailGate Appliance offers comprehensive email security functionality in an easy-to-deploy, easy-to-manage appliance. IPC functionality includes:
  - ☐ Custom policy management for enforcement of corporate email policies and regulatory compliance
  - ☐ Deep content filtering for regulatory compliance and data leakage prevention
  - ☐ Encryption for secure, private communications of sensitive information
- ☒ Tumbleweed MailGate Desktop Manager allows for streamlined desktop-to-desktop encryption for internal corporate users. With the addition of Desktop Messenger, Tumbleweed extends its extensive line of secure messaging solutions to provide robust, easy-to-use encryption technology for sensitive internal emails.
- ☒ Tumbleweed MailGate Email Firewall offers comprehensive email security functionality in a flexible, configurable software form factor. IPC functionality includes:
  - ☐ Custom policy management for enforcement of corporate email policies and regulatory compliance
  - ☐ Deep content filtering and monitoring for regulatory compliance and data leakage prevention
  - ☐ Encryption for secure, private communications of sensitive information
- ☒ Tumbleweed MailGate Secure Messenger is an integrated email encryption server and an industry-leading solution for securing email communications for regulatory compliance and protection of sensitive information. IPC functionality includes:
  - ☐ Secure communications — an industry-leading set of encryption options, including:
    - ☒ S/MIME encryption for B2B and B2C secure messaging
    - ☒ SMG Certified S/MIME encryption for interoperable, cross-vendor B2B secure messaging
    - ☒ TLS encryption for enforceable relay-to-relay secure messaging to internal and external mail servers
    - ☒ OpenPGP encryption and digital signing for B2C secure messaging to individuals with PGP desktop software
    - ☒ A set of secure Web-based delivery mechanisms that provide universal B2C secure messaging

- ☒ Reporting and auditing for regulatory compliance
- ☒ Archive integration and content indexing for regulatory compliance
- ☒ Custom policy management for enforcement of corporate email policies and regulatory compliance, including templates for HIPAA, GLBA, and SOX
- ☒ Deep content filtering and monitoring for regulatory compliance and data leakage prevention

### **Strategic Direction**

Tumbleweed provides secure Internet communications solutions for enterprises and government customers of all sizes, allowing them to safely and efficiently leverage these communication channels to optimize and grow their business. Tumbleweed offers these security solutions in three comprehensive product suites: MailGate, SecureTransport, and Validation Authority. MailGate provides protection against spam, viruses, and attacks and enables policy-based message filtering, encryption, and routing. SecureTransport enables organizations to securely and reliably exchange data and files with their customers and partners over the Internet. Validation Authority is a world-leading solution for determining the validity of digital certificates.

### ***Verdasys***

#### **Overview**

Verdasys is headquartered in Waltham, Massachusetts, with sales offices in Boston, New York, San Francisco, London, Düsseldorf, and Tokyo. Verdasys solutions deliver centralized monitoring, audit, and control over the use of data where it is most at risk, providing information security.

Verdasys customers are leaders in banking, financial services, insurance, healthcare, entertainment, manufacturing, software, and other industries around the world.

#### **Information Protection and Control Products**

Verdasys offers the following IPC products:

- ☒ Verdasys' Digital Guardian is a data security solution for protecting and tracking the flow of critical data. A central server console deploys and monitors intelligent agents, Digital Guardian logs user data transactions and applies predefined rules to ensure that end users are using applications and data properly. It also assures that data is being used in accordance with established company best practices and government regulations (such as HIPAA and GLBA) for handling confidential and private information — all without modifying existing business processes.
- ☒ Adaptive E-Mail Encryption Module extends the comprehensive monitoring and control capabilities of the Digital Guardian solution by including the ability to perform, on the fly, automated, policy-based encryption of email attachments. The Adaptive E-Mail Encryption Module uses proven data encryption technology to selectively protect corporate data.

- ☒ Adaptive File Encryption Module uses data encryption technology to protect data without the need to modify existing business processes. Using the Adaptive File Encryption Module, companies can now flexibly apply encryption to protect proprietary and sensitive information in the form of files to bring them into compliance with corporate policies and regulations governing the use of such data.

### **Strategic Direction**

Verdasys' solutions protect proprietary and sensitive data and the integrity of the business processes essential to successfully conducting business on a global basis. Verdasys customers use Digital Guardian for comprehensive data loss prevention and corporate compliance. The Digital Guardian platform creates a secure virtual perimeter that assures that data is controlled by policy and monitored for accountability, establishing a community of trust between the data user, data owner, and data provider. Digital Guardian integrates content, context, and location awareness along with encryption and data level controls to reduce the risk of information loss or misuse. Verdasys solutions are in use by government agencies and by leaders in financial, pharmaceutical, insurance, healthcare, manufacturing, entertainment, and other industries around the world.

### ***Vericept***

#### **Overview**

Founded in 1999, with major operations in Waltham, Massachusetts, and Denver, Colorado, Vericept is a leading provider of comprehensive compliance and data loss prevention solutions. Key investors in the company include Sigma Partners, Sequel Venture Partners, William Blair, Visa International, and Globespan Capital Partners. Vericept's Data Loss Prevention Solution mitigates internal risk by providing enterprisewide discovery, classification, and prevention of the information exchanged inside and outside an organization. Vericept's patent-pending classification suite delivers a high degree of accuracy and low instance of false positive events. Vericept's technology is deployed in over 750 organizations worldwide, including many Fortune 500 companies. Vericept works with organizations in several different sectors, including financial services, retail, healthcare, energy, and government, to protect billions of pieces of communication every day.

#### **Information Protection and Control Products**

Vericept offers the following IPC products:

- ☒ **Vericept Monitor.** Based on a patent-pending classification suite, Vericept's Monitor solution analyzes all Internet-based communication and attachments including email, IM, P2P file sharing, chat rooms, blogs, Web postings, FTP, and Telnet for violations of a company's corporate governance, compliance, and acceptable use policies. Utilizing a suite of content detection technologies and over 70 predefined Risk Categories, Vericept Monitor helps gain visibility into the exact nature of an organization's data leakage problems, thereby enabling it to plan remedial action to protect the company's brand and reputation.

- ☒ **Vericept Protect.** Vericept Protect provides email control to defend against unauthorized loss of data. Protect uses Vericept Risk Categories, custom categories, or Content Analysis Description Language (CANDL) categories to develop email policies that control how information flows outside of the organization. Email communications and attachments are analyzed and can be automatically encrypted, blocked, or quarantined or initialize a self-compliance capability if violations of corporate and compliance policies are discovered. Email Self-Compliance sends the communication back and allows the sender to decide whether or not to continue sending while User Alerts inform the sender of the policy violation and the action of encryption, block, or quarantine that was taken. Vericept Protect encryption is embedded and powered by Entrust.
- ☒ **Vericept Discover.** Vericept Discover investigates data at rest to find violations residing in stored data on desktops, laptops, and file servers. Based on the Vericept classification suite, Discover analyzes data at rest utilizing the Vericept Risk Categories to identify and capture violations of the corporate and compliance policy and provide additional "proof positive" evidence. When a violation is identified, Vericept can automatically encrypt information to protect against unauthorized use.
- ☒ **Vericept Edge.** Vericept Edge controls information leakage on desktops and endpoints. Edge allows organizations to discover confidential data on laptops, desktops, and servers to determine all insider risk and infractions associated with confidential data loss and compliance violations. Preventing loss of confidential information at endpoints can be enforced by restricting print, save, copy, access, movement, and download of sensitive data to removable media or other drives whether connected or disconnected to the network. Other features include the ability to send user alerts or self-compliance messages to train on company policy and control content without impeding the flow of business. If a laptop is lost or stolen, Vericept Edge will monitor laptop inactivity to preempt possible violations.

### **Strategic Direction**

Vericept provides data loss prevention solutions that allow companies to discover, classify, and protect sensitive information in motion, at rest, and in use. Vericept's detection technology discovers sensitive information based on company policy while business operations continue in real-time. After discovery, Vericept classifies and protects critical information against unauthorized distribution, even when it is modified or reformatted. The Vericept solution allows companies to mitigate violations of regulatory compliance, intellectual property loss, and customer data loss, whether malicious or inadvertent. Classification is the key to controlling and preventing data breaches. Vericept provides precise and accurate classification available to protect sensitive information. Vericept's patent-pending classification suite scales effectively to large enterprise environments to minimize false positives and increase accuracy of sensitive data discovery. Vericept's strategy is to develop best-in-class enterprise security products to protect organizations from loss of sensitive data, resulting in compliance violations, loss of intellectual property, and customer data leakage.

In September of 2006, Vericept announced a strategic partnership with Entrust to deliver fully embedded email encryption functionality in a content monitoring and control solution. Under the terms of the agreement, Vericept will integrate the Entrust Entelligence Messaging Server encryption capability into Vericept's Protect product providing automatic encryption, compliance, and content control to both Vericept and Entrust customers. In addition, Entrust will become a reseller partner of Vericept's data loss prevention solutions. Vericept's data loss prevention solutions, combined with services and support, are focused on providing the tools to those responsible for maintaining information security of corporate data.

## ***VeriSign***

### **Overview**

VeriSign Inc. (Nasdaq: VRSN) operates digital infrastructure that enables and protects billions of interactions every day across the world's voice and data networks. VeriSign offers solutions that help companies to deliver integrated marketing campaigns and mobile content across the three screens of personal computers, mobile phones, and television sets. VeriSign's solutions help organizations deliver emerging services such as mobile banking, voice over Internet Protocol (VoIP), and video over broadband. VeriSign provides layered security solutions that protect an organization's consumers, brand, Web site, and network. VeriSign's digital certificates protect over 750,000 Web servers.

### **Information Protection and Control Products**

VeriSign offers the following IPC products:

- ☒ VeriSign Security Risk Profiling Service enables customers to generate a risk score for organizations that includes threats, vulnerabilities, network access policies, and financial impacts. Simulation tools show how changes in the environment will affect risk and compliance with internal and external policies and regulations. Best-of-breed technology, threat intelligence, and structured processes are employed to help customers make better business decisions about their information security programs.
- ☒ VeriSign Vulnerability Management Service provides a full range of services designed to identify vulnerabilities at the network, host, and application levels to reduce the exposure of critical systems to external and internal attacks. VeriSign's information security analysts leverage automatic and manual vulnerability assessment tests.
- ☒ VeriSign Phishing Response Service, part of the VeriSign Anti-Phishing Solution, allows customers to quickly shut down sites and document exposure. VeriSign helps defend against future attacks and monitor customer brands worldwide.

### **Strategic Direction**

VeriSign is now focused solely on delivering security services, as the decline in pure sales product revenue indicates. The vendor bills itself as a "provider of intelligent infrastructure services for Internet and telecommunications networks" and recently announced that Charles Schwab has selected VeriSign to provide a full set of online security services for its clients. Under the terms of the agreement, Charles Schwab

will deploy VeriSign Identity Protection (VIP) Fraud Detection and Authentication services to secure client log-in and transaction information. Additionally, Charles Schwab plans to become an anchor tenant of the VIP Fraud Intelligence and Shared Authentication Network. The VIP Shared Authentication Network is already supported by PayPal, eBay, and Yahoo!.

Outsourcing security to services vendors is now a routine, acceptable practice. With the potential uptake in the consumer market, this approach should retain its appeal as a sound delivery system.

## ***Voltage***

### **Overview**

Voltage Security Inc., an enterprise security company, offers secure business communication and data protection solutions. Voltage was founded in 2002 and is headquartered in Palo Alto, California.

### **Information Protection and Control Products**

Voltage offers the following IPC products:

- ☒ Voltage SecureMail addresses the critical need to secure email communications through a comprehensive email encryption solution. SecureMail delivers a policy-based push solution that leverages the power of identity-based encryption to automatically manage keys.
- ☒ Voltage Data Protection System delivers a centrally managed key management system that enables enterprises to ensure sensitive data is encrypted as it is collected, transmitted, and stored.

### **Strategic Direction**

Based on the Voltage Enterprise Privacy Management platform, Voltage provides scalable enterprise key management and encryption capabilities for securing data throughout the enterprise. Voltage provides solutions for secure communication and data at rest to leading financial services, healthcare, government, and pharmaceutical companies.

## ***Vontu***

### **Overview**

Founded in December 2001 and headquartered in San Francisco, California, Vontu is a leader in data loss prevention software. Vontu's product suite, Vontu 7, helps businesses discover and protect confidential data at rest, monitor and prevent data in motion from wrongful disclosure, control data at the endpoint, and automatically enforce data loss prevention policies. Vontu is proven to scale and meet the needs of global organizations across industries and government markets.

## Information Protection and Control Products

Vontu offers the following IPC products:

- ☒ Vontu Discover identifies unsecured confidential data at rest exposed on open file shares, Web servers, and individual desktops and laptops.
- ☒ Vontu Protect secures confidential data at rest and has the ability to automatically quarantine or copy sensitive files. Vontu Protect also helps organizations enforce access control and encryption policies to stop inadvertent or malicious data loss by unauthorized employees. The combination of Vontu Discover and Vontu Protect allows customers to secure their confidential customer data, intellectual property, and classified information to reduce risk and ensure workforce compliance — on an ongoing basis.
- ☒ Vontu Network Monitor inspects all network communications for confidential data, accurately detects policy violations, and precisely qualifies and quantifies the risk of data loss, such as intellectual property or customer data.
- ☒ Vontu Network Prevent proactively stops data security violations of data in motion over email, Web communications, and file transfer protocols. Vontu Prevent blocks email and Web communications that contain confidential data, including email, Web, secure Web (HTTP over SSL), and file transfers (FTP).
- ☒ Vontu Endpoint Monitor is a content-aware, enterprise-class endpoint DLP product that is fully integrated with DLP capabilities for data in motion and data at rest. Using the same detection and policy enforcement as the Vontu network-based products, a new, agent-based product, Vontu Endpoint Monitor, delivers visibility and control over confidential data copied to removable media like USB storage drives, or downloaded to local drives in violation of security policies. The Vontu 7 multitier architecture scales to support tens of thousands of endpoints, while ensuring stability and manageability.
- ☒ Vontu Enforce is a central management platform that enables organizations to build, deploy, and automatically enforce consistent data loss prevention policies across Vontu Discover, Vontu Protect, Vontu Network Monitor, Vontu Network Prevent, and Vontu Endpoint Monitor.

## Strategic Direction

Vontu nearly doubled its workforce in 2006 and raised an additional \$10 million in venture capital from existing investors Venrock Associates, Benchmark Capital, U.S. Venture Partners, and Performance Equity Management LLC. Vontu offers proven solutions for data security initiatives that combine process, people, and technology to protect company confidential data. Vontu's expertise comes from working with industry leaders across verticals that have partnered with Vontu to build solutions for such issues as data privacy compliance, including PCI DSS requirements, as well as intellectual property protection, and laptop theft.

Vontu's strategy is to bring together the best team and solutions to help enterprises and government agencies prevent the loss of confidential data. Vontu's product road map is focused on innovations that protect data at rest, prevent inadvertent and

malicious data loss, and enforce confidential data policies. As risks evolve, Vontu will continue to invest in advanced detection algorithms, additional threat coverage, and proactive enforcement actions that involve the employee population in the secure handling of confidential data. Vontu's go-to-market strategy is to increase its market-leading position in the Fortune 1000 and extend its customer base in the federal, midmarket, and international markets through direct and channel sales programs as well as strategic alliances with technology and consulting companies.

## ***Websense***

### **Overview**

Founded in 1994, Websense Inc. (Nasdaq: WBSN) is a total content security vendor with global leadership spanning inbound and outbound content threat prevention and risk management. Websense continues to gain momentum and is a recognized leader in the content security market. The company has offices around the world, with over 25 million seats under subscription worldwide across all industries, ranging in size from small organizations to large, multinational corporations.

### **Information Protection and Control Products**

Websense offers the following IPC products:

- ☒ Websense Content Protection Suite v5.1 is the next-generation IPC product delivered from Websense after its acquisition and integration of PortAuthority technologies. Content Protection Suite v5.1 is a fully integrated and centrally managed information protection and control solution that protects organizations from information leaks and data loss, both at the perimeter and inside the organization, by discovering the location of sensitive data inside the network, monitoring the data as it attempts to travel inside or outside the organization, and protecting the data, with policy-based controls that align to business processes.

Content Protection Suite provides protection for data at rest, data in use, and data in motion with advanced controls for sensitive information distributed over a wide range of communication channels, including outgoing email, Web email, internal email, and messaging applications; networked printing; FTP; and textual data on any protocol. The combination of identification, classification, and patented, content-aware technologies (i.e., knowledge of the data itself, not just the file) and policy-based enforcement and robust reporting provides superior content security in an easy-to-manage solution. Content Protection Suite provides organizations with the ability to effectively identify and mitigate risk from information leaks and enforce regulatory and corporate policies in real time.

- ☒ Websense Enterprise and Web Security Suite are recognized as the industry-leading content security solutions designed to provide protection, control, and governance for the usage of the Web and other prevalent network applications and protocols, including instant messaging, peer to peer, streaming media, and many others. The solutions protect organizations from known and new inbound Web-based threats. Built with Websense ThreatSeeker technology, Websense Web Security Suite protects against spyware, malicious mobile code, phishing attacks, bots, and other threats. It also blocks spyware and keylogger backchannel communications from reaching their host servers. In addition,

Websense Web Security Suite offers the Websense Web Protection Services that help protect organizations' Web sites, brands, and Web servers. Outbound control and governance is provided by granular user/group, IP address, or workstation policies governing access to Web sites or network applications. The solution is supported with reputation and real-time classification technologies and resources that feed into databases that are automatically updated for customers in real time. Currently, there over 100 million Web sites with 90 corresponding categories, 2 million applications with over 50 corresponding categories, and over 100 protocols with 15 corresponding categories.

### **Strategic Direction**

On January 9, 2007, Websense Inc. finalized its acquisition of PortAuthority Technologies after a previously announced OEM relationship. Since the close of the acquisition, Websense has already released a new, integrated version of the PortAuthority solution, Websense Content Protection Suite 5.1. Websense is unique in its delivery of a dedicated IPC solution with a broad global footprint, increased marketing and development resources, global channel partner network, and a broader portfolio of complementary content security solutions.

Websense content intelligence, including all aspects of data itself, sets Websense apart from other vendors in this space. Websense technology exceeds basic threat-focused security solutions and enables organizations to discover and remediate broken business processes, implementing controls over where users go and how they get there, and what information they can send or use, all from a unified policy architecture.

Content Protection Suite is a logical extension to Websense's existing inbound content-based threat prevention solutions. It extends Websense's ability to effectively control unwanted outbound dissemination of sensitive and confidential information, such as personnel records and corporate trade secrets. With a low total cost of ownership and high return on investment, Content Protection Suite helps organizations secure their most sensitive assets, adhere to regulatory requirements, and maintain a competitive advantage.

### ***Workshare***

#### **Overview**

Workshare, an information security company, delivers secure content compliance solutions to more than 6,000 organizations worldwide. Workshare solutions uniquely combine policy enforcement, management control, and user education to ensure safe information exchange without business disruption. Its products include Workshare Protect and Workshare TRACE!, a suite of data-motion, data-at-rest, and data-at-use IPC products, and Workshare Professional, a data-in-use product focused on high-value business documents. Workshare's customer base spans small to large organizations in every industry segment, with more than 62% of the Fortune 1000 and 85% of the ProServices 250. More than 1 million professionals in 65 countries use Workshare software. The company has offices in San Francisco; New York; Chicago; Atlanta; Dallas; Washington, D.C.; London; Frankfurt; Paris; and Sydney.

## Information Protection and Control Products

Workshare offers the following IPC products:

- ☒ **Workshare Protect Enterprise Suite.** Workshare Protect Enterprise Suite, the security industry's first unified endpoint and network-level outbound content security solution, dramatically reduces the leakage of privacy, financial, and confidential information over multiple channels and file types. The Protect Enterprise Suite consists of the Workshare Protect client, Workshare Network Protect, Workshare Policy Manager, Workshare Trace, and the Workshare Ready SDK, and extensions:
  - ❑ **Workshare Protect client.** Workshare's client allows for the creation and management of content security policy and educates users as it enforces this policy. Working both online and offline, Protect client removes risky content, converts information to appropriate formats, and applies content rights. Rather than simply stopping business, Protect's rich client warns and educates users in real time about sensitive information and, if authorized, lets them decide how to treat the content. The Protect client covers email, data in use, removable media, and other endpoint channels such as wireless. The Protect client can be deployed standalone on an individual user's PC, or in conjunction with either or both Network Protect and the Workshare Policy Manager.
  - ❑ **Workshare Network Protect.** Workshare's new network channel gateways provide IT security staff with visibility and policy enforcement into content leaving the organization via network channels such as HTTP and SMTP. By deploying Network Protect, organizations can provide a robust last line of audit and control on outbound network traffic.
  - ❑ **Workshare Policy Manager.** Workshare's enhanced policy management offering provides a centralized policy management console for the creation and distribution of outbound content policy for both Protect client and Network Protect deployments. In addition, the Policy Manager delivers complete reporting and robust incident management into activity and incidents at both endpoints and network egress points and offers prepackaged, customizable policy packs.
  - ❑ **TRACE!.** A free set of document security tools, TRACE! Endpoint and TRACE! Network analyze files and provide alerts to violations of regulations as well as inside-out breaches of information security. The product performs on demand or batch assessment of files in folders and email and on Web sites and automatically updates as legislation and regulations change.
  - ❑ **Workshare Ready SDK and Extensions.** Through the Ready Partner Program, technology partners can bundle their product and service offerings with Workshare. These partnerships establish best-of-breed integrations through joint development and testing. The Ready Partner program also enables vendors to build their own integrations with Workshare products to enhance their own product offerings. Current Workshare Ready extensions allow for the application of third party IPC actions such as Encrypt, apply

document rights, delivery certification, and others. Partners include PGP, Secured Email, Utimaco, Secure Computing, Microsoft, and others.

- ☒ **Workshare Professional.** Working in line with Microsoft Office, and integrated with email and document management systems, Workshare Professional is a complete document integrity solution designed to provide data-in-use accuracy, security, and compliance for critical business documents such as term sheets, regulatory filings, contracts, and product documentation. Workshare Professional provides accurate and efficient document review control automatically across email, document repositories, and Microsoft Windows SharePoint. Features and benefits of Workshare Professional include fast and accurate multiparty document review and comparison, elimination of version/master proliferation and confusion, extended and secured document control over email and portals, PDF conversion anywhere and on email send, and discovery and removal of hidden data and visible content leaks. The Workshare Professional Suite includes content security for data in motion and data at rest by embedding the Workshare Protect client and working with other Workshare Protect products and Workshare Ready extensions.
  
- ☒ **The Workshare Compare Service** is software-as-a-service offering that dramatically improves team productivity and workflow processes for creating, editing, and reviewing documents. The Compare Service has been designed from the ground up to be integrated into Web and enterprise applications for easy and accurate document comparison.

### **Strategic Direction**

The Workshare architecture addresses the top issues underlying regulatory compliance. It simplifies the effort to pinpoint the appropriate level of security for each content component. It allows organizations to set data protection levels appropriate to the sensitivity of the information, to the user's level of risk, and the risk of the channel being used. Through third-party action application, it can also protect and/or limit content access to only those who should be using it. The architecture provides the enterprise the means for managing its entire range of content protection capabilities. It enables enterprises to establish policies that facilitate broad — but controlled — exchange of attachments or documents, keeping company-confidential data inside the company.

Workshare's multiple deployment options allow the organization to address client, client/server, and gateway outbound content compliance needs. Moreover, Workshare's ability to address threats associated with outbound content compliance applies not only to email but also to instant messaging, peer to peer, file transfers, removable and mobile media, Web postings, and other types of messaging traffic. The ability to protect confidential information and sensitive data across multiple protocols is quickly becoming a business-critical mission for enterprises of all sizes.

### ***ZixCorp***

#### **Overview**

Headquartered in Dallas, Texas, ZixCorp (Nasdaq: ZIXI) provides ecommunication services that protect, manage, and deliver sensitive information to enterprises and consumers in healthcare, finance, insurance, and government.

## **Information Protection and Control Products**

ZixCorp offers the following IPC products:

- ☒ ESecureservices enable policy-driven email encryption, content filtering, and send-to-anyone capability, while ZixCorp's eHealth service improves patient care, reduces costs, and improves efficiency through an eprescribing solution.
- ☒ PocketScript, an eprescribing solution, brings big benefits. Deployed through a handheld device or a secure Web site, PocketScript enables users to generate prescriptions with immediate point-of-care access to patient and formulary data.

## **Strategic Direction**

ZixCorp provides email encryption services for privacy and regulatory compliance. ZixCorp's network allows seamless encrypted email delivery to healthcare organizations, financial institutions, and government agencies. ZixCorp supports five encrypted email delivery mechanisms: S/MIME, TLS, OpenPGP, secure portal, and "push" delivery.

ZixCorp's PocketScript eprescribing service provides clinical decision support at the point of care with real-time access to patient-level eligibility, formulary, and copay information to aid prescribers in selecting the most cost-effective prescription based on the member's benefits. Deployed through a secure wireless PDA or secure Web site, PocketScript reduces costs, improves patient safety and convenience, and enhances physician practice efficiency. PocketScript enables users to order and deliver prescriptions electronically to the patient's preferred pharmacy. The system also provides comprehensive drug-to-drug and drug-to-allergy interaction alerts based on patient-specific medication history, and it maintains a comprehensive drug reference guide to assist in prescribing decisions. PocketScript is certified with RxHub, SureScripts, and Per Se to enable end-to-end prescribing and is further recognized as a SureScripts GoldRx solution provider.

## **ESSENTIAL GUIDANCE**

IDC believes that information protection and control will be a major area of investment over the next five years. There are many different items converging, which leads IDC to this decision. Most of them have been discussed in this document. The bottom line is that IPC is needed to protect sensitive information. Moreover, an ever-growing list of government and industry standards and regulations are forcing organizations of all sizes and vertical markets to deploy and use such solutions. We expect to see more examples of high-profile incidents in which customer records, confidential information, and intellectual property are leaked. This will continue to fuel the demand for IPC solutions that monitor, secure/encrypt, filter, and block sensitive information contained in data at rest, data in motion, and data in use.

Organizations must move from a reactive compliance stance to proactive and cost-effective information protection and control. Enterprises must go beyond the minimum requirements of regulatory compliance to internal policy compliance at a higher level of assurance. The ability to perform automated checks in advance of auditing, to report on a regular basis, and to monitor employees and discern behavior patterns to stop malicious and noncompliant actions before they occur requires that steps be

taken to achieve proactive and effective cost management. IDC believes IPC is the answer to this problem.

## LEARN MORE

---

### Related Research

- ☒ *TJX Incident Highlights the Need for Information Protection and Control (IPC)* (IDC #ICUS20627807, March 2007)
- ☒ *Worldwide Mobile Device Security 2007–2011 Forecast* (IDC #206072, March 2007)
- ☒ *IDC's Software Taxonomy, 2007* (IDC #205437, February 2007)
- ☒ *Enterprise Security Survey, 2006: The Rise of the Insider Threat* (IDC #204807, December 2006)
- ☒ *Worldwide Security and Vulnerability Management Software 2006–2010 Forecast and Analysis: Managing Security Knowledge and Control* (IDC #204693, December 2006)
- ☒ *Worldwide Secure Content Management 2006–2010 Forecast Update and 2005 Vendor Shares: The Convergence of Secure Content and Threat Management* (IDC #203550, September 2006)
- ☒ *Worldwide Security Compliance and Control 2006–2010 Forecast and Analysis: Going Beyond Compliance to Proactive Risk Management* (IDC #203350, September 2006)

### Methodology

The IDC software market sizing and forecasts are presented in terms of packaged software revenue. IDC uses the term *packaged software* to distinguish commercially available software from custom software, not to imply that the software must be shrink-wrapped or otherwise provided via physical media. Packaged software is programs or codesets of any type commercially available through sale, lease, rental, or as a service. Packaged software revenue typically includes fees for initial and continued right-to-use packaged software licenses. These fees may include, as part of the license contract, access to product support and/or other services that are inseparable from the right-to-use license fee structure, or this support may be priced separately. Upgrades may be included in the continuing right of use or may be priced separately. All of the above are counted by IDC as packaged software revenue.

Packaged software revenue *excludes* service revenue derived from training, consulting, and system integration that is separate (or unbundled) from the right-to-use license but does include the implicit value of software included in a service that offers software functionality by a different pricing scheme. It is the total packaged

software revenue that is further allocated to markets, geographic areas, and operating environments.

The software revenue forecasts presented in this study represent IDC's best estimates and projections based on the following:

- Reported and observed trends and financial activity in 2006 as of the end of January 2007, including reported revenue data for public companies trading on North American stock exchanges (1Q06–3Q06 in nearly all cases, plus 4Q06 where available)
- Additional modeling to fill in any information gaps using a top-down/market-level approach to estimate overall 2006 market sizing
- Bottom-up regional forecast growth rates provided by IDC analysts in each geographic region

Bottom-up/company-level data collection began in March 2007, with in-depth vendor surveys and analysis to develop detailed 2006 company models by market, geographic region, and operating environment. This activity will form the basis of vendor share, updated forecast, and competitive analysis studies that will appear later in the year.

---

## Copyright Notice

This IDC research document was published as part of an IDC continuous intelligence service, providing written research, analyst interactions, telebriefings, and conferences. Visit [www.idc.com](http://www.idc.com) to learn more about IDC subscription and consulting services. To view a list of IDC offices worldwide, visit [www.idc.com/offices](http://www.idc.com/offices). Please contact the IDC Hotline at 800.343.4952, ext. 7988 (or +1.508.988.7988) or [sales@idc.com](mailto:sales@idc.com) for information on applying the price of this document toward the purchase of an IDC service or for information on additional copies or Web rights.

Copyright 2007 IDC. Reproduction is forbidden unless authorized. All rights reserved.

---

**Published Under Services:** Secure Content and Threat Management Products; Security and Vulnerability Management Software; Secure Content Management