

## Gartner Secure Web Gateway Magic Quadrant – 2008

Gartner published their second SWG (Secure Web Gateway) Magic Quadrant in September 2008. The first SWG was published in 2007. This document looks at their comments on Clearswift's Web security products and makes general observations from Clearswift's perspective on the results. Note: Sophos were in the last MQ but were dropped from this release.

The MQ results were:

### Challengers:

- IronPort (Cisco)
- Trend Micro
- ScanSafe
- McAfee
- Websense
- MessageLabs

### Niche Players:

- Barracuda Networks
- ContentKeeper Technologies
- CA
- Webroot
- Clearswift
- 8e6 Technologies (now Marshal)
- Cymphonix
- Marshall
- CP Secure

### Leaders:

- Secure Computing (now McAfee)
- Blue Coat Systems

### Visionaries:

- Aladdin Knowledge Systems
- Finjan
- Mi5 Networks
- FaceTime Communications

As with 2007's version Blue Coat and Secure Computing (now part of McAfee) are placed in the top right sector. Given that the only apparent difference in what Secure Computing delivers to customers versus our Web Appliance is their native FTP handling the reasoning behind their position may be down to the extensive joint programs they have run with Gartner! Blue Coat is a logical choice but to get a solution as complete as the one we offer (admittedly only for web browsing) would be very expensive. Blue Coat WAN optimization is however attractive to certain types and sizes of business but the complexity it introduces in its use, plus the integration required with other web security tools produces a very expensive solution with a high TCO, and they do no native document analysis or data leakage/loss control except through partners like Code Green.

In this SWG we make the top 10 (out of 20) along the completeness of vision and 17<sup>th</sup> on the ability to execute. I could go into Gartner's criteria on what a Secure Web Gateway should be but to be brief lets me say that the ability to execute simply reflects our need to grow share in this space, our company size and our US customer base - as Gartner are US centric in their approach to this market. Increasing our completeness of vision is to do with us handling non-browser based web applications like Skype and IM clients therefore offering more than our port 80/HTTP and port 443/HTTPS scanning. However our design brief was not to do everything web but ensure safe web browsing which we deliver brilliantly. If we were simply an organisation of say IronPort's size we would be top right, by right. Gartner is not truly comparing like with like and doing a somewhat slanted comparison.

## This is what Gartner said about Clearswift:

### Clearswift

#### Strengths

- Clearswift is a veteran secure e-mail vendor with a high profile in Europe, the Middle East and Africa (EMEA). It has integrated a proxy-based SWG into its e-mail security appliances and software.
- Its browser-based management interface provides a clean logical interface for policy development that is easy to use, even for nontechnical users. E-mail and the Web are managed in the same console. Multiple devices can be managed from any machine, and configuration is gradually implemented as users end their browsing sessions.
- Policy development for DLP is one of the best in this market and several policy constructs – that is, Sarbanes-Oxley Act (SOX), Gramm-Leach-Bliley Act (GLBA), Payment Card Industry (PCI) Security Standard, Securities and Exchange Commission, accounting terms and stock market terms – are included. The same policy can apply to Web and e-mail, and it is possible to intercept and copy/archive Web mail and IM traffic that triggers DLP policy.
- Clearswift offers good reporting capability. All machines in a cluster are capable of local or consolidated reporting. Reports are active and include a hyperlink drill-down of details.
- Malware filtering is provided by Kaspersky and Sunbelt. It is augmented with some in-house preconfigured, policy-based code analysis.
- MIMESweeper Web is capable of SSL certificate validation, decryption and inspection.
- URL categorization is provided by the Websense database.
- Overall, Clearswift's primary advantage is its integration with its e-mail solutions and the provision of DLP across both channels, making it a good choice for existing e-mail customers or EMEA buyers looking for both solutions from the same vendor.

#### Strengths Commentary:

- Bullet one supports our integration strategy behind email and web (common console, common engines etc.) which is one of the major points of differentiation in what we offer the market – a real strength.
- Bullet two supports the design of our intuitive UI, common policy console. In fact if policy is changed it is effected almost immediately it is applied, not 'gradually implemented' as stated here.
- Bullet three - the content inspection and DLP message has got through 'one of the best in the market' I would argue that it is still 'the best'. And Blue Coat offers none! This is also a vital sales message as our ability through content filtering to monitor and control the collaborative nature of today's web is an essential capability for all organizations.
- Bullet four is accurate our reporting is good and getting better but note our consolidated reporting is still limited to a common threat report currently, although this will broaden.
- Bullet five malware underplays our capabilities. For instance we control web scripts and stop malicious clipboard data theft while most of our competitors do not. Simply using MIMESweeper to de-compose web traffic has in tests made the anti-malware engine twice as effective at finding malware, and Gartner still don't recognise the Heuristic capabilities within Kaspersky which in independent tests outperforms all the other well known vendors.
- The final bullet is actually a warm recommendation we offer real benefits (not necessarily the ones Gartner scores on) like consolidated management; dual malware protection and we do both web and email to the same high standard.

So even though we do not get out of the 'niche' segment, our niche is we do web browsing protection really, really well and our DLP and content is not just a nice to have and is recognized by Gartner as being very important.

What's more we can offer customers that in email too, reducing their administration costs, simplifying their security yet providing them with leading technology all-round. Which is exactly our differentiation with customers in the first place, and why customers buy our products in preference to others. What we secure, we secure with excellence.

### Cautions Commentary:

#### Cautions

- Clearswift remains an EMEA brand and does not enjoy significant brand recognition in North America. Its market share in the SWG market is minimal, and its growth rate is well below the SWG market growth rate.
  - Malware detection is primarily limited to signatures and only in HTTP/S traffic. The proxy cannot isolate or clean infected machines.
  - URL-filtering policy options do not include advanced features such as time of day, bandwidth or quotas.
  - Application control is limited to blocking URL destinations (and/or streaming protocols) and file type blocking. It cannot filter or manage evasive applications, such as Skype.
  - MIMESweeper Web does not support in-line/bridge mode deployments, ICAP or Web Cache Communication Protocol (WCCP). Active configurations require Layer 4 load balancing or static proxy auto-configuration (PAC) file settings.
- Bullet one. The US centric bit coming out. Obviously we do not disagree with this, but we do have the web and email technology to change that and grow our US market share.
  - Bullet two. This is inaccurate. As I've already mentioned there are heuristics and a lot of anti-malware prevention capabilities in the Kaspersky, Sunbelt and MIMESweeper combination. True we do not clean infected machines. We do however report on infected users/machines so a proper remediation is able to take place and we stop spyware 'call-homes'. Automated agentless cleaning is just as likely to damage the user's machine which is why we do not offer this auto-spyware cleaning feature.
  - Bullet three **was true** - but since February 2009 we have simply the best Time of Day; and Quota features available in any product. Bandwidth control where you limit bandwidth usage by user is not something we get a lot of demand for, however we could offer this in future if demand is there. Content security however is essential.
  - Bullet four is accurate we are not designed to manage evasive web based applications and to be frank a lot of the others claim some capability but don't really do a very good job of it, apart from FaceTime.
  - Bullet five is true. In line/bridge mode would mean that we sniff all web/network traffic, which was not our design purpose. Our design purpose was to control web browsing not all web-based applications and their clients. ICAP is a red herring as we do not need to pass traffic out to other applications like Blue Coat for anti-virus, or any other type of non- Blue Coat filtering. We simply don't need ICAP as we provide a complete solution!

### In Summary:

*Yes customers read Gartner but they do not follow it slavishly. From a Sales perspective we really just need to get the messages across that we have at least as good a product as Secure Computing's - in fact its better in every respect apart from handling native FTP. There are really no excuses to not be selling lots of Clearswift Web Appliances'.*