



Reining in Malware

2007: The year of the secure gateway

Table of Contents

The Business Case	3
“But I Already Have Gateway Security!”	4
New Threats Demand New Defenses	4
Toll on Assets and Resources	4
Balance Defense and Offense	5
The Appliance Advantage	5
Effective Armor	5
Efficient to Implement and Maintain	5
An Industry Best Practice	5
The McAfee Advantage: Leadership Without Compromises	6
Enterprise Expertise	6
Enterprise Manageability	6
Pure Security	7
The Year of the Secure Gateway	7

2007: The year of the secure gateway

Malware is good business. For malware developers. The year 2006 saw rapid evolution of malware technologies. Malware entrepreneurs figured out how to refine and speed attacks for maximum profitability, toxicity, and stealth. Their business models now precisely target theft of specific corporate and personal data and the distribution and installation of adware.

Reflecting operational maturity, malware development has moved from sporadic, independent activities to integrated, disciplined teams. Developers have embraced open-source development processes, created distribution paths through Web 2.0 sites such as MySpace and Wikipedia, and preyed on homogeneous enterprise systems. Their flexibility and innovation have made it very difficult to catch or constrain them. And their success has encouraged market entrants worldwide.

To combat malware’s escalation to big business, enterprises must update and expand gateway defenses to include multiple coordinated network and host-based protections, including anti-spyware, content filtering, anti-spam, and anti-virus. This mandate is based on two primary risk factors: more sophisticated, ubiquitous cyber-threats that jeopardize systems and confidential data, and an unsustainable, expensive toll on infrastructure and human assets.

The Business Case

Improved gateway security tools halt malware at the entrance to the enterprise and provide better visibility into and control over infrastructure usage. The results match today’s business priorities: more effective security with more predictable policy compliance and more efficient resource management. At a fair price.

Using the McAfee® tool for gauging reduced risk as a return on security investment (RRRoSI), deployment of a multi-function security gateway would generate a \$1 million risk reduction over three years (see Table 1). At a 10,000-system enterprise with \$25 million in IT assets, this risk reduction would yield

an improvement of roughly 4 percent in overall risk posture. Economically, the enterprise would reduce its risk enough in about eight months to justify a three-year investment.

Table 1: Calculation of RRRoSI for a multi-function security gateway

The calculation considers the impact of downtime on an organization, the number of events that would require updates or patches (a factor that drives complexity, cost, and risk), and the number of systems protected by the multi-function gateway to create a risk rating. The formula then calculates the security countermeasure by the impact on the systems it protects. In the case of a gateway, risk reduction includes expanded capabilities and expanded coverage for desktops, unmanaged systems, servers, and other assets. Projected costs reflect average pricing for an appropriately sized system. This calculation comes from a McAfee spreadsheet, publicly available upon request.

Cost of one hour of downtime to the enterprise	\$100,000
Number of hosts in the enterprise	10,000
Average annual number of patching events	12
Depreciation schedule (in months)	36
<hr/>	
Enterprise derived risk rating	54
Expected risk improvement	4 percent
<hr/>	
Asset exposure to risk	\$25,870,635
Risk	\$9,061,828
Projected risk reduction for Year One	\$342,933
Projected risk reduction through solution lifetime	\$1,028,798
Year One expected cost	\$150,000
Expected cost of projected solution (subsequent years)	\$30,000
Cost of projected solution	\$240,000
<hr/>	
Expected RRRoSI	8.3982 months to RRRoSI
	27.6018 months beyond RRRoSI

“But I Already Have Gateway Security!”

Why aren't existing protections sufficient? Because typical enterprise boundary protections, firewalls, anti-virus, and spam filters, have evolved alongside malware, but not quickly enough. They can't keep up with the diversity and volume of malware.

New Threats Demand New Defenses

Perhaps the biggest challenge for existing gateway protections is that most implementations are designed as individual point solutions, while malware is evolving across categories. By blending web, messaging, and script approaches, these hybrid threats avoid recognition by spam filters. They don't require access to desktop data, so they bypass traditional desktop anti-virus systems. All they need for activation is to be displayed by a browser.

Malware isn't just tied to incoming email. Malware developers now circumvent email protections by trapping innocent web users. “Drive-by” spyware is embedded in otherwise benign web sites, snaring unsuspecting visitors by obviating the need to “accept” an application. When employees visit a site, their inadvertent downloads allow attackers to install keystroke monitors and system backdoors to gain access to privileged information. Attackers can even target and take down (or worse, take over) unmanaged systems like network printers.

According to McAfee Avert Labs, the pace of malware development has skyrocketed since 2004, taking just two years to grow from 100,000 to 200,000 exploits. It took 18 years for the McAfee malware database to reach 100,000 malicious threats and just under two years to double to 200,000. At this rate, McAfee Avert researchers expect another 200,000 threats in the next two years.

Source: McAfee Avert Labs, July 2006

Another category of gateway weakness is simple age. In some cases, spam and anti-virus solutions use outdated filtering that is too slow and unsophisticated to catch today's threats. Many approaches don't even use streaming signature updates to match the pace of exploits. Developers are now adept at tweaking tried-and-true viruses to efficiently bypass these filters and distribute malware payloads like Trojans and adware. Proof that old solutions aren't sufficient: of the 4 million computers cleaned by the

Microsoft® Malicious Software Removal Tool, approximately 2 million of the computers (or about 50 percent of those with malware present) still contained at least one backdoor Trojan. (Source: Microsoft Security Intelligence Report, June 2006)

If allowed on the network and installed, these blended threats, virus variants, and Trojans can start accessing confidential information, corrupting data, slowing down systems, and propagating across the corporate network. These threats are expensive and risky to remediate—it is difficult to ensure that all dangerous code has been removed and all data sources are again trustworthy.

Toll on Assets and Resources

The second justification for increased gateway protections stems from the need to protect and optimize infrastructure availability. Spam, spyware, and network misuse place an onerous tax on business networks and storage resources, one that enterprises need to reduce by monitoring and restricting network usage. Many corporations also want to limit liability from inappropriate content viewed or stored on enterprise systems.

How bad is the problem? Resource consumption due to malware and misuse of Internet access has escalated so quickly that many organizations have been caught unprepared.

- According to McAfee Avert® Labs, in mid-October 2006, “image spam accounted for up to 40 percent of the total spam received, compared to less than 10 percent a year ago.” Image spam is doubly dangerous: it consumes three times the bandwidth of text spam and can harbor spyware within its files
- YouTube usage is much more expensive than music file sharing. Video clips are 20 times larger than audio files

Infrastructure assets and the employees who administer and restore them are precious and expensive. They should be protected and, better still, conserved for other business-critical purposes.

“URL filtering is but one of a few perimeter-based security technologies for protecting against malicious Internet content. It is the most widely deployed and the most necessary, but anti-virus and anti-spyware scanning of web traffic is becoming increasingly important.”

Source: Gartner Marketscope URL Filtering, March 2006

Balance Defense and Offense

Modern threats and Internet uses demand a two-pronged strategy—defend against external threats and enable and enforce internal policies.

- To protect against the threat of new blended malware, companies must proactively scan for malware on incoming communications. These protections should include web filtering, anti-spyware, anti-spam, and gateway anti-virus
- To reduce liability, enterprises must enable and enforce the right internal usage, processes, and policies for outgoing communications. They should automatically monitor and block access to inappropriate or unproductive content and restrict email distribution of confidential information

The Appliance Advantage

These protection and enforcement capabilities can be purchased as standalone solutions or in an integrated gateway appliance. Most companies have some level of desktop and gateway protections. They may argue, “Why is a new gateway appliance the right solution?” The answer involves both effectiveness and efficiency.

As of September 2006, McAfee Avert Labs has identified more than 800 attacks that are best stopped at the gateway.

Source: McAfee.com

Effective Armor

Multi-function gateway security appliances are appropriate because they concentrate key protections at the front door of the enterprise. They establish an easily controlled defense layer that fills coverage gaps (for example, for unmanaged or unprotected systems) and reinforces other security and business resources.

The gateway is the right place to halt incoming malware because it prevents exploits from reaching their target programs, whether web servers, PowerPoint and Word files, or browsers. The gateway is also the last hope for stopping outgoing information. It is uniquely effective against today’s risks. By including several types of scans, filters, and blocking, confidential information and risky behaviors can be discovered before damage is done.

The centralized appliance approach also improves security through better maintenance of protections. As an integrated

tool, it is simple to ensure vulnerability information and protections are always up to date—no rushing patches to desktop systems or performing hectic system audits when problems appear.

Efficient to Implement and Maintain

The other appliance advantage is efficiency. By integrating critical protections into a single product, on a single system, gateway appliances present the necessary tools within one installation instance. Startup is easy and fast, reducing a common source of errors.

Multi-function gateways also improve operational efficiency through streamlined reporting, maintenance, and management across defenses. Reporting, for internal requirements or external auditors, is much easier. Administrators gain a single view to help them aggressively monitor and maintain protections and efficiently scale performance. They can even manage remote systems at sites without local administrators.

For companies struggling to manage asset usage, gateways can provide visibility into network use to differentiate and manage appropriate and inappropriate use of infrastructure. With simple reports, gateway tools can present critical data that distinguishes types of use. Real data makes it easier to justify, establish, and monitor policies.

Once policies are clearly defined, automated controls and enforcement become straightforward. Specific sites (like MySpace or YouTube) can be blocked according to company policy, ensuring Internet use is appropriate and constructive. Proactive content filtering dynamically blocks sites known to harbor spyware and can be customized by specific categories to reflect corporate policies.

An Industry Best Practice

Analysts agree that gateway security should be central to every enterprise defense in depth strategy. IDC believes “corporations should consider spyware’s detection/removal as part of a comprehensive multi-layered strategy. Client-based anti-spyware software is important, but a complete solution should also include perimeter protection at the corporate gateway that prevents infection before spyware can reach the end user.” (Brian Burke, IDC, June 2006)

Gartner also validates the importance of updated gateway security:

- “We see the market quickly shifting toward Internet gateway malicious code management solutions that integrate “best of breed” antivirus, anti-spyware and URL filtering.” (Gartner Marketscope URL Filtering, March 2006)

- “The SMTP gateway is one of the effective locations for blocking malicious code from internal servers and users, although desktop protection is also required.” (Gartner Hype Cycle for Infrastructure Protection, July 2006)
- “Organizations should also use their gateway and network security devices to provide anti-spyware capabilities in the network, a strategy that has proved effective in the fight against viruses and spam.” (Gartner Hype Cycle for Cyberthreats September 2006)

The McAfee Advantage: Leadership Without Compromises

With these risks, rewards, and recommendations, integrated security gateways demand investment today. Why should enterprises choose a McAfee solution? In addition to meeting the previous functional requirements, McAfee Secure Internet Gateway has two distinct advantages: enterprise-leading protections and the integrated, extensible management of McAfee ePolicy Orchestrator® (ePO™).

Secure Internet Gateway is highly effective, scales extremely well, and has an intuitive user interface. Its excellent performance in our testing earned it a Network Testing Labs World Class Award for best Internet gateway. If you currently have a network firewall, you should consider adding this appliance as a mandatory next step in security protection.

Source: Network Testing Labs



Enterprise Expertise

McAfee has more than 17 years of non-stop monitoring and research into malicious code for enterprises. A many-million-node monitoring network supports Avert Labs researchers in 15 countries who have expertise spanning vulnerability detection to remediation to botnets. This breadth of insight helps McAfee detect, understand, and remediate new threats and endless malware variants in the wild—before they affect business. As threats blend and merge, this cross-category leadership pays off with accuracy and responsiveness that cannot be matched by point solutions.

At RPC, an oil and gas services company, McAfee Secure Internet Gateway keeps its users productive by blocking viruses, managing access to non-business sites and peer-to-peer file sharing, filtering content, and preventing inappropriate web usage.

Source: Tony Toth, Corporate Security Office, RPC

Unlike many solutions that sacrifice effectiveness in order to provide a broad spectrum of security coverage, the McAfee Secure Internet Gateway includes security features that lead in each of their respective categories and have been tested and proven under enterprise workloads. These features each win in head-to-head competitions against enterprise-scale threats, ensuring that customers are indeed obtaining best-of-breed effectiveness. McAfee has integrated these security features into one appliance, which makes them easier to buy, deploy, and maintain.

Enterprise Manageability

The second McAfee distinction is the extensible management built into the Secure Internet Gateway. It reflects the needs of some of the world’s largest and most security-conscious organizations:

- Real-time understanding of events can be the delta between safety and days of downtime
- Policies and regulations change frequently, demanding painful progress reporting
- Not all tools come from one vendor

The solution: unified, extensible management using McAfee ePO.

McAfee ePO presents an integrated, consistent view of real-time risks and status. Not only does it reflect the tools in the Secure Internet Gateway, views can include any McAfee product. It can even manage events for products from other companies, like Symantec. Administrators can see a convenient, comprehensive view of their protections, identify configuration and coverage gaps, and efficiently maintain their security postures in accordance with changing risks.

Pure Security

When you choose McAfee, you get much more than a point solution. McAfee is a pure security company with a comprehensive and careful portfolio of security risk management tools. Researchers, developers, and support teams offer security help every hour of every day. Every resource is applied to innovatively managing and mitigating security risk for customers.

No distractions. No compromises.

The Year of the Secure Gateway

The year 2007 may be a very profitable one for the malware industry. McAfee wants to rein in these profits by making it the year of the secure gateway. The threats and risks are real. These threats are manageable, using tools that deliver compelling risk reduction at a fair price. And industry analysts agree that security gateway appliances are part of the optimal solution to manage them:

- **Effective security.** Gateways block and filter evolving malware at the network edge, before it has a chance to disturb the enterprise. They efficiently integrate with and support desktop- and server-based protection to enable a defense-in-depth strategy
- **Efficient management.** The appliance approach integrates tools to make it easy and fast to implement, manage, and maintain appropriate protection and free up business assets

McAfee understands the reality of evolving threats, the increasing liabilities from data loss, and the need for high-value asset protection. With its leadership record, experience, and focus, McAfee is ready to help enterprises manage security risks at the perimeter and across the enterprise, even as the threats and regulations change.

Learn more about McAfee and the Secure Internet Gateway at www.mcafee.com. To calculate your own RRRoSI, start by reading the step-by-step guide, "Mastering Your Risk Reduction Through Security Investments," available on www.mcafee.com.