



WHITE PAPER

Realizing Cost Benefits Through Perimeter-based Online Security





Introduction

Internet Security is on the front burner for many IT professionals and executives. Malware infections are increasing in frequency, severity and stealth. Spam is rapidly approaching 90% of all email traffic. Phishing attacks are becoming more sophisticated. And, the Internet has become an unwelcome workplace distraction, as employees use this valuable tool for non-work-related Web surfing, games, social networking, viral videos, and other unproductive activities, which not only consume time and bandwidth, but also expose the business to Web-borne threats.

Because there are real and indirect costs associated with Internet security threats, it stands to reason there are significant financial benefits to be gained by proactively stopping the threats before they impact corporate assets and employees. This white paper examines various methods of intercepting threats outside of the network, minimizing the negative impact on employee productivity, reclaiming network bandwidth, and mitigating legal liability risks.

Here There Be Tygers

Email has become a major communication medium, while the Internet is a core component in today's business environment as a primary customer, partner and vendor interface, and as an invaluable research and education tool. However, Internet access is also the lair of many with malicious intent. The goals of these "black hats" range from surreptitiously collecting demographic and usage information to corporate espionage, blackmail, fraud, and more.

Many organizations rely on solutions that detect and clean virus, spyware, and other infections on the network servers or individual desktops. While these solutions may be effective in the short term, they are also reactive, and can lead to a false sense of security. In order for desktop software to detect a virus, for instance, the virus must already have reached the computer, and therefore is already inside the corporate environment. Likewise, the virus detection program runs inside the operating system of the computer and thus the virus is already inside the operating environment before it can be detected. While detection and cleaning at this

Because there are real and indirect costs associated with Internet security threats, it stands to reason there are significant financial benefits to be gained by proactively stopping the threats before they impact corporate assets and employees.





level may work, there is also a risk that the damage has already been done without being detected.

With this in mind, moving detection and prevention mechanisms further up from the desktop can mitigate these risks. Perimeter appliances like firewalls and Unified Threat Management devices can be configured and maintained to detect various malware as it enters the corporate infrastructure, thus preventing the malicious code from getting to the servers or desktops and their operating system. Cleaning time and technical resources are thus minimized and good protection no longer depends on users maintaining virus updates on every machine or running regular scans.

The best option is to move the initial line of defense outside of the corporate infrastructure entirely. By subscribing to a managed service, email and Web traffic can be scanned for malicious threats *before* they reach the corporate network. This keeps the malware, and therefore the risks, a step further from individual machines and operating systems, allowing IT departments to greatly reduce the threats posed by spyware, worms, viruses and other malicious code.

By proactively stopping threats at a distance, organizations can realize a number of cost savings. Moving the initial processing outside of the corporate infrastructure to a managed service thus free the resources previously devoted to cleaning infected machines, which can be a time-consuming activity and often involves not only the individual user, but also a costly technical resource as well. Proactively eliminating threats before the desktop frees these human resources from reactive removal tasks and allows them to concentrate on more productive activities.

Below are several specific examples of threats and their associated costs. We'll also explore means to maximize security and reduce costs by using best security practices.

Locking the Corporate File Cabinet

There are many types and levels of security. No business would think of putting corporate assets into a building with no locks on the doors. Likewise, information security should be just as obvious. The key is to find the balance between the costs versus the risk brought on by insufficient

By subscribing to a managed service, email and Web traffic can be scanned for malicious threats before they reach the corporate network.

By proactively stopping threats at a distance, organizations can realize a number of cost savings.





protection. Do you trust that the lock on the door is enough? Do you need to add security cameras? Alarm systems? Guards? Or perhaps even more sophisticated methods of defense? In most cases, one line of defense is added to the previous one. This is true of online security as well. While each layer might add initial incremental costs, each layer of security greatly increases the effectiveness of the system as a whole and thus reduces risk further. There is no one-size-fits-all answer to how much security is right for a given organization, but the risks can be assessed universally.

Many of the threats to the corporate infrastructure are designed to extract individual or corporate information. Keyloggers and screen scrapers detect passwords, which allow cyber-criminals access to financial or other personal information through public Internet sites. Worms can penetrate even deeper into the network to expose files to the outside world. Unfortunately, the number of ways that information can be compromised is growing exponentially.

The costs of information exposure can be extremely expensive, both to the individual and the organization. According to *Consumer Reports 2006 State of the Net*, successful phishing attacks cost each victim \$850 and the U.S. at large a total of \$630 billion. Corporate information exposure can be more costly. For instance, an employee's computer at the Oregon Department of Revenue was infected by a keylogger, allowing over 2,200 state taxpayer IDs and other personal information outside the confines of the department. Those innocent taxpayers were thus susceptible to identity theft or other illicit activity at a yet-to-be-determined final cost.

The risk to any given organization cannot be fully quantified. Corporate reputation, legal liability, fines, and other costs can be added to any immediate financial losses. Again, there is also a real cost associated with detecting and removing infections after the fact. A small business IT consultant may charge a client \$150-\$200 to run a set of diagnostics and removal utilities on a single machine. An IT department in a large company may similarly bill a department for its services. In both cases, the infected machine is off-line for 30-90 minutes, if not longer, and the affected user loses productive work time. IT budgets for services or personnel are being put toward fixes instead of forward-looking projects.

While the reactive cost of cleaning virus or spyware infections from desktops or servers can be quantified, the full loss of productivity is more

Many of the threats to the corporate infrastructure are designed to extract individual or corporate information.

The costs of information exposure can be extremely expensive, both to the individual and the organization.





subjective. Early viruses were designed to get attention, mainly for the authors, but modern malware is engineered for stealth. Spyware, screen scrapers and keyloggers can collect data for days or weeks without detection, while networks of zombie computers, or botnets, can generate spam for months before any adverse effects are seen. Most spyware is detected when machine performance degrades to the point that the user actually notices it. By that point, the machine has most likely been compromised for a while and the slowdown has been slowly costing the employee ever-increasing amounts of productivity. Additionally, malware that generates network traffic can degrade the entire network, affecting the productivity of the organization as a whole. It is often the cumulative effect of multiple infections that tips the scales to the point that humans notice performance losses.

The effect of malware is real, as are the corporate costs. Stopping these threats should be a top priority for most IT departments today. Furthermore, blocking threats before they ever reach the corporate network should top the list of solutions, thus keeping the thieves further from the electronic file cabinet.

Keeping the Wolves at Bay

While some threats target information from individual machines or files, other threats are engineered to gain access to the corporate infrastructure. If keyloggers or screen scrapers steal external passwords, they can also be used to obtain corporate logins. Additional techniques use backdoors allow hackers to gain remote control of individual computers, which can therefore be enabled to commit any number of undesirable activities. Software vulnerabilities allow alternative mechanisms for exploitation. If a single instance of an individual phishing attack is estimated at \$850 and a single user can expose 2,200 individual data leaks, imagine what a cyber-intruder can do with full network access.

Keeping the intruders well away from corporate assets is the most cost effective way to deal with this sort of threat. Reacting after the fact can be prohibitively expensive. Consulting fees, data recovery and other forensic charges, legal fees and fines, and more are quantifiable costs while others are harder to pin down. Lost productivity reduces output. Poor press adversely affects the morale of employees, customers, and investors alike. The total cost can bring a company to its knees if a cyber-thief can expose confidential information or steal intellectual property.

The effect of malware is real, as are the corporate costs. Stopping these threats should be a top priority for most IT departments today.

If a single instance of an individual phishing attack is estimated at \$850 and a single user can expose 2,200 individual data leaks, imagine what a cyber-intruder can do with full network access.





Spam is More Than a Minor Annoyance

Reports from numerous organizations, including the MX Logic® Threat Center, place spam levels at an all time high, both in volume and percentage of total mail traffic. Spam can often peak at approximately 90% of all email traffic. If left unchecked, spam also comprises an ever-growing portion of total email cost to a company. As email has emerged as a core business component, optimizing these costs becomes more and more important.

The total cost incurred by email includes server hardware and software, server and desktop storage and processing resources, as well as both the LAN and WAN bandwidth needed to transmit it. As more spam reaches employee inboxes, the time to read, evaluate and delete messages takes valuable time away from each employee's day. Additionally, each piece of spam can include phishing or malware threats as well, increasing the risk to employee and organization alike. And if that organization is required to maintain or archive all electronic messages for internal or regulatory compliancy, up to 90% of an organization's long term email storage costs can be spent dealing with unsolicited mail.

As with all security, a multi-layered approach to controlling spam can be highly effective. By moving the spam detection and prevention layer outside the corporate infrastructure, an IT department can maximize its email systems. If junk mail never reaches the corporate servers, the savings compound for each user computer that each unwanted message would have touched. Using layered protection for email reduces not only Internet bandwidth usage, but also internal network bandwidth usage, firewall and mail server processing, and email storage requirements.

Bandwidth Recovery

Unfortunately, it's not just the outside world that can be costly. As the Internet has become a daily part of doing business, so has its temptations in the workplace. While employees are conducting business online, they are also shopping, checking sports scores, chatting with friends, downloading music and much more. Although individual companies have different philosophies or policies regarding acceptable Internet use, real savings can be realized by putting controls in place to optimize Internet activity.

Employee productivity is an obvious metric when it comes to Internet access control. There is an endless supply of Internet content that will

Reports from numerous organizations, including the MX Logic® Threat Center, place spam levels at an all time high, both in volume and percentage of total mail traffic.

By moving the spam detection and prevention layer outside the corporate infrastructure, an IT department can maximize its email systems.





draw people away from work-related activities, in some cases to the point of distraction. Monitoring or controlling that access gives management the ability to keep employees focused on the tasks at hand.

While employee productivity may not fall on the shoulders of an IT organization, controlling Internet access can also help optimize bandwidth usage as well. Internet radio stations are prevalent, and while popular with employees, this streaming media is a large and constant drain on Internet resources. Add the appeal of MP3 players and their associated downloads and the cumulative effect can be excessive. The ability to recover this wasted bandwidth and the associated infrastructure resources can ease the strain on IT budgets by delaying the need to purchase additional equipment or bandwidth.

Legal Liability

Internet and email activity also bring legal complications for businesses. Regulatory and workplace compliance rules may mandate certain filters be put in place to protect employees from sexual harassment or discrimination. Litigation can arise from hostile work environment issues that cause an employee to feel threatened or offended. The risk is real, but mitigating the risk from an IT perspective can be relatively simple.

While legal issues are complicated and cannot easily be resolved by good Internet policies, practices, or tools, best practice can put an organization on better legal standing. If, for instance, a company not only has a written Internet access policy, but actively enforces its policy through a content filter, the organization stands a much better chance of defending itself if audited or sued. Likewise, if emails are filtered for provocative or offensive content, the same applies. And the more a policy and its associated enforcement protects users, the more the organization protects itself. Policies and procedures of this nature are generally the purview of legal counsel, human resources, or compliance officers, but a good IT manager can also help to ensure that technology aspects are addressed.

The Managed Service Advantage

As there are cost savings from implementing best practices, one of the easiest and most effective ways to realize savings is to include a managed service in the security mix. A managed service sits outside of the corporate

Although individual companies have different philosophies or policies regarding acceptable Internet use, real savings can be realized by putting controls in place to optimize Internet activity.

While legal issues are complicated and cannot easily be resolved by good Internet policies, practices, or tools, best practice can put an organization on better legal standing.





infrastructure at the perimeter of the Internet. As such, it provides a security buffer that simply does not exist otherwise.

As discussed earlier, moving detection and prevention via a managed service outside of the corporate infrastructure keeps the threats from ever entering the corporate environment. Traffic can be scanned and analyzed for a wide variety of threats including virus, spam, phishing, trojans, and other malicious threats. Additionally, traffic can be scanned and analyzed for content to prevent confidential information, compliance violations, or offensive information from entering or leaving the organization.

The financial advantages of this additional layer vary on the threat. Savings from spam prevention, for instance, are relatively high. A managed service can stop or quarantine spam messages before they are sent, which, as mentioned, saves email-related bandwidth, server processing, desktop processing, and storage costs as well as employee time. The savings from blocking compliance-related email from leaving the network could be even higher should a violation be investigated.

There are additional advantages to a managed service besides the additional layer of protection. A managed service provides staff augmentation as well. A good managed service has a 24x7 staff monitoring traffic. Trends and problems can be recognized quickly and addressed in an expedited fashion. And since a managed service focuses on security, the monitoring is performed by experts in their fields, often a level of expertise that doesn't exist within a corporate IT department. This improves the overall security effectiveness of a company even further.

A managed service is also an expansion of the corporate architecture. As security resources are expanded into a managed service, that burden is removed from the corporate infrastructure, while threat-related maintenance issues, scalability concerns, and other administrative issues are lifted from the internal IT group. The managed service handles all upgrades, redundancy, and many other problems associated with a top tier data operation.

Since a managed service can focus solely on security issues, the level of effectiveness can also be increased by relying on the service's relationships with other organizations in the security community. MX Logic, for instance, is an active participant in the Messaging Anti-Abuse Working Group and the

As there are cost savings from implementing best practices, one of the easiest and most effective ways to realize savings is to include a managed service in the security mix.

Since a managed service can focus solely on security issues, the level of effectiveness can also be increased by relying on the service's relationships with other organizations in the security community.





Anti-Phishing Work Group, has relationships with anti-virus partners that allow high priority five-minute virus engine updates, and is a known entity to the various ISP and Real-time Blackhole List organizations. All of these relationships allow MX Logic to quickly recognize threats itself and through interactions with others, keep the most current viral signatures within its system, and respond quickly to messaging abuse issues.

Finally, a managed service offers painless implementation. There is no hardware or no software to install or maintain. There are few, if any, up front costs. Administration is performed remotely via the Web from anywhere, and there are no patches or upgrades to install. In many cases, there are no long term contracts – the service can be started or stopped if need be.

MX Logic Services

One of the simplest and most effective ways of adding a layer of protection is to include a managed service in the security mix. A managed service sits outside of the corporate infrastructure at the perimeter of the Internet. As such, it provides a security buffer that simply does not exist otherwise.

Email Security

For instance, when battling email threats like spam and viruses, a managed service like the MX Logic® Email Defense Service filters messages before they ever reach the corporate infrastructure. As up to 90% of all messages are spam or contain viruses, stopping these messages before they reach the corporate infrastructure means a 90% savings in email related bandwidth. The reduced message traffic also means reductions in mail server load and mail storage, for both local and archival purposes.

With the Email Defense Service filtering email, another set of virus filters operates without consuming server and desktop processing resources or adding latency to firewalls, routers, and other edge defenses. The Email Defense Service includes MX Logic's proprietary WormTraq® worm detection engine for protection against zero-hour worm attacks, and third-party virus protection from McAfee, Sophos, and Authentium. Additionally, because the managed service acts as a buffer, the corporate network is also protected from Directory Harvest Attacks (DHAs) and Denial of Service (DoS) attacks.

One of the simplest and most effective ways of adding a layer of protection is to include a managed service in the security mix.

When battling email threats like spam and viruses, a managed service like the MX Logic® Email Defense Service filters messages before they ever reach the corporate infrastructure.





Web Security

As with email security, Web protection can also be layered through a managed service. The MX Logic® Web Defense Service provides both threat protection and content control services at the network perimeter. By using the managed service, users are prevented from accessing phishing or spyware sources through a comprehensive set of known site lists, as well as dynamic site ratings. Files that are not from suspected malware sites are scanned for Trojans and viruses before ever reaching the corporate network, providing one more layer of detection and protection from threats. A further advantage of the Web Defense Service is its ability to also block spyware-infected machines from sending information back to the spyware developer. The service not only blocks the infected machine requests, but will also alert administrators so that corrective action can be taken, thus minimizing the risk of serious damage to the machine, the user, or the business.

The Web Defense Service also includes content-based controls that enable businesses to set and enforce Acceptable Use Policies. Administrators can block access to certain categories of websites, like pornography, gambling and sports for users or groups of users. More restrictive policies might also prevent access to news, music, or shopping as well, based on the needs of the business. Note that this also includes inadvertent access to inappropriate material that might happen through mistyped URLs, or even through ads and other embedded content on legitimate or approved sites.

24 Hour Threat Experts

A major value of a managed service is the addition of a staff of experts. The 24-hour MX Logic Threat Center, for instance, monitors email and Web traffic trends to provide up-to-the-minute detection rules, to react instantly to threats, to monitor other industry sources, and to provide a level of threat knowledge, experience and expertise that many small and medium-sized businesses are not able to provide themselves. MX Logic also delivers the highest level of virus and threat updates possible through partnerships with major anti-virus vendors as well as anti-spam, anti-phishing, and other anti-abuse groups.

The MX Logic® Web Defense Service provides both threat protection and content control services at the network perimeter.

A major value of a managed service is the addition of a staff of experts.





Enterprise Class Protection

Finally, many organizations cannot justify the expense for purchasing high-end equipment and software to protect their infrastructures. By using a managed service, those same organizations are able to have the benefits of sophisticated technology, redundant systems, 24 hour monitoring enjoyed by enterprise-level businesses. A managed service provider like MX Logic provides all of the protective advantages, but without the need to install, administer or maintain the hardware and software. The costs are spread across thousands of companies allowing each to gain all of the benefits of the most advanced systems while only paying only a small fraction of the cost.

Summary

Email, the Internet and other online tools are integral to businesses today, but expose those same businesses to a variety of threats. Recognizing the threats and cleaning up the effects are steps in solving the problems, but proactive approaches are more effective. Adding additional layers of security, particularly outside the network perimeter can maximize a company's ability to identify and stop Internet threats before they infect a machine, expose sensitive information, or consume valuable resources. A managed service is a simple, yet highly-effective method of adding a security buffer around a corporate infrastructure to provide a level of security that simply is not available otherwise. The cost savings can free budget for productive activities to move a company forward. And the peace of mind gained from putting in the best possible protection is priceless.

About MX Logic

MX Logic is a leading provider of managed email and Web security services that deliver enterprise-grade performance without enterprise-level complexity and cost. Our easy-to-use, award-winning services reduce risk and liability, lower overall IT costs, and increase productivity. MX Logic services are available through our industry-leading partner network. For more information, visit www.mxlogic.com.

By using a managed service, organizations are able to have the benefits of sophisticated technology, redundant systems, 24 hour monitoring enjoyed by enterprise-level businesses.

Adding additional layers of security, particularly outside the network perimeter can maximize a company's ability to identify and stop Internet threats before they infect a machine, expose sensitive information, or consume valuable resources.

More information:

MX Logic Sales Team
9781 S. Meridian Blvd. Suite 400
Englewood, CO 80112 USA
T: +1.877.MXLOGIC
F: +1.720.895.5757
E: sales@mxlogic.com
W: www.mxlogic.com