Defense in Depth

Enterprise-Strength Protection for the Mid-size Business

A Trend Micro White Paper  I  August 2006
CONTENT

I. THE CHALLENGES OF SECURITY FOR THE MID-SIZE BUSINESS
   - Motive Shifting to Financial Gain.................................................................3
   - Increasingly Sophisticated and Rapid Attack................................................3
   - Perimeter-Based Defenses No Longer Adequate.............................................4
   - Spyware and Spam: Annoying, Expensive and Risky....................................4

II. SPYWARE: ANNOYING, PERVERSIVE—AND DANGEROUS..........................5

III. SPAM: EXPENSIVE JUNK MAIL.................................................................6

IV. VIRUSES, WORMS—AND MORE...............................................................7

V. CONTENT TRAFFIC REQUIRES CAREFUL SCRUTINY.....................................8

VI. MAKING SURE ALL USERS ARE ON THE SAME PAGE..............................10

VII. TREND MICRO: DEFENSE IN DEPTH FOR THE MID-SIZE BUSINESS
   - Gateway Protection......................................................................................11
     Trend Micro InterScan Gateway Security Appliance.....................................11
     Trend Micro InterScan VirusWall™ Software..............................................11
     Trend Micro Email Security Services..........................................................11
   - Client/Server Solutions and Network Access Control...............................12
     Trend Micro ScanMail Software................................................................12
     Trend Micro OfficeScan Software..............................................................12
     Trend Micro Network VirusWall Enforcer..................................................12

VIII. SUMMARY................................................................................................13
I. THE CHALLENGES OF SECURITY FOR THE MID-SIZE BUSINESS

Managing security for a mid-size business involves hard choices. You need to defend your organization against a complex barrage of threats that can degrade customer confidence and steal productivity by consuming time and network resources. Deploying basic desktop security software was once enough, but no longer. The proliferation of blended threats, spyware, phishing attacks, and pervasive Web-based threats requires more sophisticated defenses at every access point.

Yet investing time and money into disparate point solutions that provide inadequate security doesn’t solve the problem. What you need is a multilayered solution that you can count on to protect your assets, infrastructure and information, at an affordable price, from a vendor you can trust.

The security landscape has become more complicated in recent years making antivirus protection alone inadequate. A number of important recent trends affect security for the mid-size business.

**Motive Shifting to Financial Gain**

Everyone has heard stories of the lone hacker who unleashes a particularly destructive virus, then crowns about his accomplishment to fellow hackers. While such attacks often caused millions of dollars of damage and disrupted business operations dramatically, they did not directly benefit the hacker financially.

But today, hackers are motivated by making money, and the number of profit-motivated threats is skyrocketing, often engineered by organized crime. This shift has important implications for your business. Today, every mid-size business should expect profit-based attacks such as phishing and pharming schemes, theft of intellectual property or customer information—and plan for them.

“In 2005, the vast majority of threats were inspired by financial gain. These attackers prey on users with the intention of information theft. They invent tricks as modern-day con artists, with a worldwide field of millions serving as potential victims.”


**Increasingly Sophisticated and Rapid Attacks**

Paralleling the shift to profit-based attacks is the growing ability of threats to evade defenses as well as the pervasive availability of threat-building tools and sample code on the Internet. The mid-size business needs to step up to more robust and adaptable security solutions—or risk having one of these new custom threats penetrate its defenses and adversely affect operations.

Today’s hackers work at light speed. There used to be a time lag of months between the discovery of vulnerability and the first threat to exploit it, now the lag is measured in weeks, or even days. As an example, the Zotob worm set a disturbing world record in 2005 when it exploited a vulnerability in Microsoft Windows that had been published just five days previously!
**Perimeter-Based Defenses No Longer Adequate**

Defenses concentrated solely at the network perimeter assume that, if you can intercept threats there, the internal network is safe and secure. This strategy seeks to establish a well-defended perimeter as the principal barrier to threat penetration.

But thanks to remote workers and virtual private networks (VPNs), the perimeter is disintegrating. Today, threats can penetrate the enterprise at multiple entry points throughout the network architecture, in particular, through mobile devices such as laptops and mobile phones. To combat this trend, mid-sized businesses need a comprehensive multilayered defense that can intercept threats wherever they enter the corporate network.

**Spyware and Spam: Annoying, Expensive and Risky**

Both spyware and spam pose genuine security risks. Spam mail can serve as an entry point for the full range of malware. Spyware such as key-loggers can be part of attacks aimed at gaining access to private information such as credit card numbers and passwords. The most prudent approach is to assume that any piece of code on a computer that was installed without the knowledge and consent of a trusted IT professional is a threat, and a potentially serious one.

While very different in character, spam and spyware have one thing in common: They drain profits. Time spent removing spyware or deleting spam costs companies millions of dollars a year in IT support costs and unproductive employee time. This hurts the mid-size business’s bottom line. Many businesses find that they can justify the cost of enhanced security measures just by the productivity gains from eliminating spam and spyware.

Let's take a more detailed look at individual threat categories and how your mid-size business can effectively respond to them.
II. SPYWARE: ANNOYING, PERVASIVE—AND DANGEROUS

Spyware is pervasive. By one estimate, 67 percent of all business computers have some form of spyware installed. Most spyware enters the network through the so-called “drive-by download.” This breach occurs when a user visits a Web site and downloads and installs an application, unaware that it is infected. The application deposits its sinister payload into the user’s personal computer, then goes to work.

The most common spyware activity is gathering information—Web-browsing activity, credit card numbers, bank account information, computer license software keys, passwords—then transmitting it to the criminals via the Internet, so-called “phoning home.” Once the information is received, it can be used to drive a wide range of fraudulent money-making schemes. Their financial gain can come at the expense of your mid-size business, either directly through theft of money or intellectual property, or indirectly through diminished trust and brand loyalty when your customers suffer losses from a scheme using your company’s identity.

Spyware removal is labor intensive, and in fact can run to two or three hours per infected machine—a significant cost for your business. Clearly, stopping spyware before it takes root is the most cost-effective and safest approach for your mid-size business.

SPYWARE PROTECTION

The first line of protection against spyware should be deployed at the gateway to look for spyware activity in both directions. The gateway solution blocks access to URLs known to harbor spyware, scans incoming HTTP traffic for the presence of spyware in downloads, and intercepts “phone home” attempts. For additional protection, client-based security intercepts spyware that enters the network as remote users access the network over VPN, bypassing the Internet gateway.
III. SPAM: EXPENSIVE JUNK MAIL

What began as a trickle in the early days of email is now a flood. Spam—unsolicited, bulk messages sent through electronic messaging media—has become a productivity sink, a resource hog, and a security threat. While spam technically can plague any form of electronic messaging—instant messaging, search engine results, mobile phone messages, blogs—the largest vector is email. Spam constitutes a whopping 70 percent of all email traffic, and is estimated to grow to 78 percent by 2009².

The spammers are getting smarter. To avoid blacklists, today’s attackers hijack legitimate IP addresses to launch massive spam attacks. Some spammers have perfected directory harvest attacks, which steal whole blocks of addresses from a company’s mail server that can be used for spam blasts.

The overriding need is to block spam from entering your network in the first place. Once spam is inside the corporation’s walls, it can cause lost productivity and unleash attacks.

SPAM PROTECTION

An anti-spam filtering solution located at or before the gateway eliminates the bulk of incoming spam, reducing the risk of email-borne threats, boosting productivity, and conserving storage resources. An end-user quarantine capability enables users to manage their own spam, by presenting a view on the user’s PC of their quarantined mail. This feature relieves IT staff from the burden of quarantine management, enabling them to focus on more productive tasks.
IV. VIRUSES, WORMS—AND MORE

Despite the rise of other kinds of threats, mid-size businesses can’t afford to ignore malware. Trend Micro’s annual survey of threats shows that malware—viruses, worms, Trojans, rootkits and more—accounted for more than half of all threats in 2005. Without an effective defense, the enterprise faces the constant risk of an attack that can cripple operations and lead to substantial financial and other losses.

In the past, most threats entered the network as attachments to email sent using the Simple Mail Transfer Protocol (SMTP). Most businesses today have desktop antivirus solutions that also scan incoming SMTP email, so the danger from SMTP-borne malware has lessened in recent years.

However, that trend is being offset by the skyrocketing use of webmail through free services such as Hotmail, Gmail and Yahoo! Mail. Because it uses HTTP as a vehicle, not SMTP, webmail bypasses most antivirus solutions. As a result, webmail attachments can deliver threats directly to unprotected machines and thus gain access to the network.

In addition to webmail, modern networks are vulnerable to internal breaches in security. An unsuspecting employee can introduce a virus by connecting an infected laptop or other device, creating a direct path into the corporate network. Malware can also enter through mobile devices or removable media such as CDs and memory sticks.

MALWARE PROTECTION

The most effective multilayered defense against malware has solutions deployed at the gateway, mail server and desktop. A gateway solution that scans SMTP, FTP and HTTP traffic can block incoming malware before it enters the network. Mail server antivirus software provides a second line of defense, blocking and cleaning viruses carried as attachments in Microsoft Exchange or Lotus Notes. Desktop antivirus software blocks and cleans viruses that evade the gateway and mail server defenses, for example, remote users connected directly to the internet on broadband or dial-up.
V. CONTENT TRAFFIC REQUIRES CAREFUL SCRUTINY

Once you’ve protected your mid-size business against spyware, spam and malware, there is an additional danger to consider: the content of otherwise legitimate email and Web traffic.

Companies are required by multiple regulations* to protect the privacy of their customers. Therefore, an employee who sends out confidential information to the wrong person—intentionally or unintentionally—could subject the organization to fines, legal sanctions, lawsuits, and disastrous publicity.

Intellectual property can also make its way to unauthorized recipients as an innocent-looking email attachment. Imagine the damage to a mid-size business if blueprints, software source code or sensitive data were to be sent to a competitor or other entity by a disgruntled employee.

Incoming messages contain their own dangers. An employee who receives an email message containing hate speech, profanity or pornography can use that message as grounds for a lawsuit alleging a hostile work environment. At a minimum, such an action incurs substantial legal fees that most mid-size businesses can ill afford, and judgments can range in the millions.

A growing source of lost employee productivity comes from employees browsing Web content that is not related to work duties. Whether the target is a site with video games, sports scores, adult content, or on-line shopping, business efficiency suffers when employees use company resources and time for leisure activities.

MAIL CONTENT FILTERING
Effective mail content filtering at the gateway prevents objectionable material from entering your network. When an employee sends hate mail or other objectionable material to another person on the internal network, this traffic will not be intercepted by the gateway security device. An additional layer of defense is needed at the internal mail server to block inappropriate content from being sent and received internally.
WEB CONTENT FILTERING

A Web content filter at the internet gateway can block most offensive or pornographic content, yet also allow personal Web browsing during appropriate periods such as lunch breaks and after normal working hours. This solution improves productivity and business efficiency while limiting legal liability.

---

* Examples of privacy regulations include the Graham Leach Billey Act and the Healthcare Insurance Portability and Accountability Act (HIPPA) in the United States, the Data Protection Act in the United Kingdom, and the Personal Information Protection Law in Japan. See Trend Micro white paper "Regulatory Compliance Drives the Need for an Enterprise Security Framework" for a more detailed discussion of security and compliance.
VI. MAKING SURE ALL USERS ARE ON THE SAME PAGE

Once you’ve designed and deployed a comprehensive security solution for your mid-size business, you’re home free—or maybe not. As the workforce becomes more mobile and dispersed the risk increases that an unprotected laptop or remote PC will infect the network. Even if your own team is up to date with all security software and patches, a temporary staffer or partner employee can still be an unwitting entry point for malware or other threats. How do you ensure that every entry point is protected?

The answer is network access control (NAC), which prevents devices from connecting to the network unless they are fully compliant with all security software and application and operating systems patches.

NETWORK ACCESS CONTROL

An NAC solution scans for the most up-to-date security software and critical operating system patches. Noncompliant devices are immediately quarantined and automatically remediated.
VII. TREND MICRO: DEFENSE IN DEPTH FOR THE MID-SIZE BUSINESS

Mid-size businesses need enterprise-quality security, at an affordable price point, with a low administrative burden. Trend Micro offers a set of security solutions to implement a defense-in-depth strategy, protecting business from malware, spyware, spam and inappropriate content. Together, they constitute Defense in Depth: Trend Micro’s multilayered, industrial-strength solution specifically engineered for the needs of mid-size businesses.

GATEWAY PROTECTION

Widely regarded as a leader in gateway security, Trend Micro offers you the choice of hardware appliance, software or managed services protection:

 Emblem Trend Micro InterScan™ Gateway Security Appliance

Stop spyware, worms, viruses and phishing at the Internet gateway. It prevents spyware downloads, blocks access to malicious spyware sites, detects spyware activity on clients and triggers automatic cleanup operations. The InterScan Gateway Security Appliance also stops drive-by downloads by analyzing ActiveX and Java applets for threats and blocks access to suspicious spyware sites by filtering URLs in real time. The appliance is affordable and easy to deploy and administer. It serves mid-size businesses with up to 1,000 users, and can significantly lower your total cost of ownership.

 Emblem Trend Micro InterScan VirusWall™ software

Prevents viruses, spyware, spam, phishing and bot attacks from entering the network through vulnerable Internet gateway access points. It reduces unwanted email using a combination of signatures and heuristics to provide high detection rates and fewer false positives. By scanning unprotected protocols including SMTP, HTTP, FTP and POP3, InterScan VirusWall protects entry points exploited by attackers to carry malicious payloads. It’s the ideal way to preserve your investment in gateway hardware and features flexible per-seat licensing for up to 2,500 users.

 Emblem Trend Micro Email Security Services

Remove spam, viruses and other Internet threats carried in SMTP traffic before they penetrate your network, and stop denial of service (DOS) and directory harvest attacks (DHA) before they can take down your network. Backed by Trend Micro’s experts in gateway secure content management, Email Security Services help protect available Internet bandwidth and email performance while reducing onsite storage requirements. Email Security Services allow you to protect your business against email-borne threats and spam with a low initial investment of time and money.
CLIENT/SERVER SOLUTIONS AND NETWORK ACCESS CONTROL
As ideal complements to Trend Micro’s gateway protection, these client/server and network access control solutions add additional layers of coordinated security for your mid-size business:

**Trend Micro ScanMail™ software**
Guards against viruses, Trojans, worms and other malware hidden in email attachments. By filtering inbound/outbound SMTP connector-level traffic, it blocks threats before they can enter or leave the mail server. For additional security, ScanMail offers virus protection plus new anti-spam and advanced content-filtering technology. A centralized management console makes it easy to deploy group configurations, scan settings, notifications and automatic updates—across all mail servers. Trend Micro offers ScanMail for both Microsoft Exchange and IBM Lotus Domino environments.

**Trend Micro OfficeScan™ software**
Protects enterprise networks from viruses, Trojans, worms, hackers and network viruses, plus spyware and mixed threat attacks. As an integrated solution, it guards desktops, laptops and network servers, while the Web-based management console makes it easy to set coordinated security policy and deploy automatic updates on every client and server. By integrating with Trend Micro Network VirusWall Enforcer or any network admission control (NAC) architecture including Cisco Network Admission Control, OfficeScan can enforce policy on non-compliant computers, and then remedy, redirect, restrict, deny, or permit network access.

**Trend Micro Network VirusWall Enforcer appliance**
Protects against the fastest growing source of infection—the mobile and remote workforce. The Network VirusWall Enforcer appliance controls network access by ensuring devices—managed or unmanaged, local or remote—comply with corporate security policies, before they can access the network.

---

2 Source: The Radicati Group, Inc. 2006
VIII. SUMMARY

To be successful, the mid-size business must focus on its business, not protecting its network. At the same time, ignoring the dangers posed by spam, spyware, viruses and inappropriate content can spell disaster. The Trend Micro Defense in Depth solution outlined in this white paper offers the mid-size business an affordable, effective and efficient approach to multilayered security. And Defense in Depth is the best assurance that the mid-size business can keep its attention where it needs to be: on its products and services and, ultimately, its customers.

For more information, please see http://defense.trendmicro.com