

A background image showing a person's hand pointing at a laptop screen. Overlaid on the image is a semi-transparent circular gauge with numerical markings from 0 to 7.0, suggesting a security or performance metric.

# Trend Micro Enterprise Security

Immediate Protection. Less Complexity. 

 Lower Security Risks  
and Costs by  
Minimizing the Time  
to Protection

*A Trend Micro White Paper | October 2008*

## I. INTRODUCTION

The enterprise threat landscape has dramatically changed with the proliferation of a new generation of content security threats. Today's cyber attacks harvest sensitive corporate data and expose companies to the risk of losing revenue, employee productivity, customer relationships, and market reputation. As the headlines prove, targeted threats are hitting companies faster and in larger quantities than they ever have before.

This white paper reviews the content security threat landscape and how it has evolved into a more dangerous environment, increasing the risks and costs for enterprises. This paper discusses how conventional content security approaches are inadequate at defending against today's threats and how a new paradigm is needed to provide sufficient protection. Enterprises need a solution that identifies risks immediately and creates better protection. At the same time, they need a solution that reduces the complexity in acquiring, deploying, and managing security.

Trend Micro Enterprise Security is a tightly integrated offering of content security products, services, and solutions for enterprises concerned about staying ahead of content security threats. At the core of these products and services is the Trend Micro Smart Protection Network, a newly introduced cloud-client architecture designed to provide fast protection with minimal network resources. Trend Micro Enterprise Security powered by our Smart Protection Network provides immediate protection with less complexity, offering lower business risks and costs to enterprises.

## II. ENTERPRISE CONTENT SECURITY THREATS

Cybercriminals are taking advantage of business' dependence on email and the web to attack enterprises and steal information and resources. Simple actions like opening an email attachment or clicking on a web link can result in lost confidential data, damaged infrastructure, or a ruined reputation.

The content security threat landscape has changed dramatically over the last few years. Spam is no longer just an annoyance and hackers are not simply creating malware for notoriety, Instead the focus has shifted to profiting from threats that steal data and resources. Profit-driven cybercriminals lurk behind most web threats, creating a new generation of spam and malware based on a powerful underground economy. To maximize profits, cybercriminals have become more sophisticated, delivering faster more insidious attacks. And finally, as content security threats have become more effective, they have dramatically increased in volume.

- **Content Security Threats Are Profit Driven.** According to a survey conducted by the Department of Justice, over 60 percent of businesses have been hit by cybercrime.[9] Enterprises are direct targets for cybercriminals, seeking to compromise data and resources on a larger scale. This has resulted in the rise of targeted attacks including data-stealing malware, botnet infections, ransom attacks, and other threats

designed to profit from the stolen data or resources of enterprises. Data breaches can subject an organization to legal fees and fines, not to mention negatively impacting consumer confidence. From January 2005 to September 2008, The Privacy Rights Clearinghouse reported over 245 million records of personal information had been breached. [8]

- **Increased Sophistication Confounds Conventional Security.** Cybercriminals no longer need to discover system and application vulnerabilities on their own. Instead, they can now use vulnerability information provided from security researchers to quickly craft exploit code to take advantage of these vulnerabilities. The time between the discovery of a vulnerability and the release of exploit code used to be measured in days or even weeks. Now 94 percent of exploit code that takes advantage of web browser vulnerabilities appears within a day.[3]

Cybercriminals are also increasing the sophistication of attacks by coordinating multiple components to successfully deliver a single attack, often delivering an email with a link to a malicious website or an email with an attachment that downloads malware and sends data over the web to the cybercriminal. These attacks can also combine seemingly innocuous code from multiple sources to deliver devastating results that are more targeted and difficult to detect. Increasingly, enterprises are being targeted with attacks designed to steal specific assets within the organization. In addition, threats—such as those that use a rootkit in which the system file is replaced—may result in a system infection that is so extensive that conventional uninstall or system cleaning approaches become useless. Content security threats must be stopped before they get a chance to infect the enterprise.

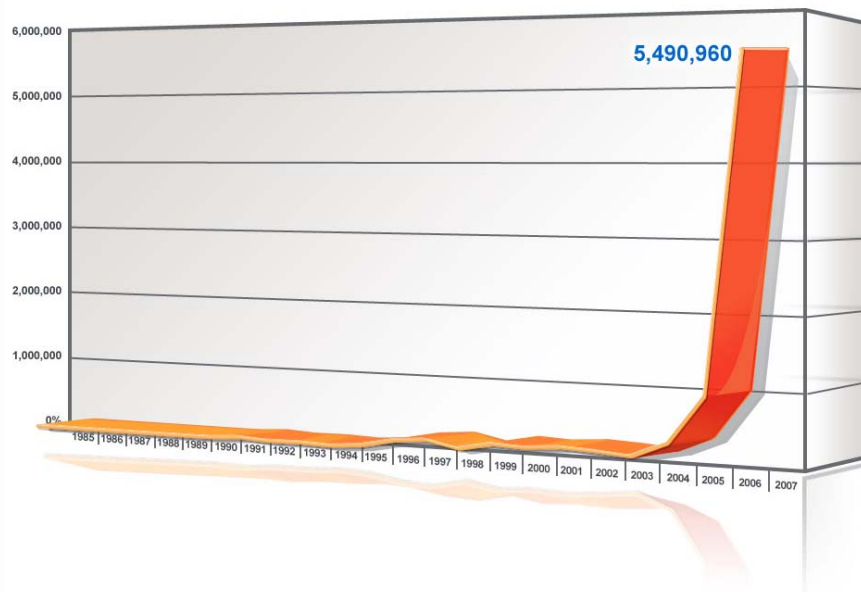


Figure 1: The Dramatic Increase in Unique Malware Samples [1]

- **The Volume of Threats Has Dramatically Increased.** Cyber crime has become its own industry with “Threat Kits” sold on the Internet, the resources of millions of computers stolen through botnets, and volumes of confidential data sold on the black market. The result is a dramatic increase in content security threats. Trend Micro research shows that spam now comprises up to 95 percent of all email and, according to AV-Test GmbH, security vendors collected 1,738 unique threat samples in all of 1988, which grew to 177,615 samples in 1998 and then to over 5 million by 2007. [1]

Historically, as cybercriminals have evolved their threat development skills, the security industry has responded in kind with new technologies to combat the new threats. Most recently, however, the explosion of new threats and the tendency to use combined threats has further complicated protection efforts. Conventional approaches are no longer sufficient to keep enterprises safe.

### III. CHALLENGES TO CREATING A DEFENSE

Enterprises are spending billions of dollars deploying “best-of-breed” security products, often layering multiple products, in an effort to create a solid defense against the next generation of content security threats. Plus, government and industry regulations and new technology trends increase complexity and cost. Here are several key factors that compound content security risks.

- **A Mobile Workforce.** There has been a considerable rise in the mobile workforce. Research firm IDC predicts that as many as 70 percent of all workers in the U.S. will be using mobile devices by 2011, and a survey conducted by Korn/Ferry International shows that 81 percent of the world’s business executives are already using mobiles.[2] IT organizations have to deal with an increasing mobile workforce as well as contractors and other temporary users. Enterprises need to protect these workers both on and off the network.
- **Web 2.0 and E-Commerce.** As Web 2.0 and e-commerce technologies increase the flexibility in accessing information and conducting business, they also open additional avenues for security breaches. Executives are all too familiar with security breaches that exposed private customer data of high-profile retailers, generating negative attention among customers, press, and legislators. Real-time protection is needed against data-stealing malware and other content security threats to protect organizations that have integrated these technologies into their business models.
- **Virtualization.** The Gartner Group determined that virtualization is the highest-impact issue changing infrastructure and operations through 2012.[5] According to InformationWeek Analytics, 90% percent of respondents said at least some portion of their network environment will be virtualized by 2010.[7] As enterprises rush to embrace the benefits of virtualization, it has become clear that security in a virtual-computing environment is different than in more traditional approaches and can add additional complexity if not included within a larger security solution framework.

- **Compliance and Other Industry Regulations.** Compliance is one of the top issues driving security expenditures. New rules have added concerns over patient records, customer data, and loss of intellectual property. One of the most effective ways enterprises are getting better business value from security is aligning security investments with business and compliance objectives. ,
- **Outsourcing, Partnering, and Customer Collaboration.** Today, business growth relies on sharing data with partners, suppliers, outsourcers, and through collaboration with customers. To be efficient and ultimately successful enterprises have opened their networks to third parties for joint collaboration, adding another layer of risk.
- **Ineffective Defense with a Patchwork of Point Products.** The new generation of content security challenges has resulted in a wide range of security products—many of them narrowly focused on one security issue. But instead of solving the problem, the resulting point-product sprawl makes it worse with constant deployment, administration, and support demands. Managing this complexity often poses greater problems than the threats themselves.

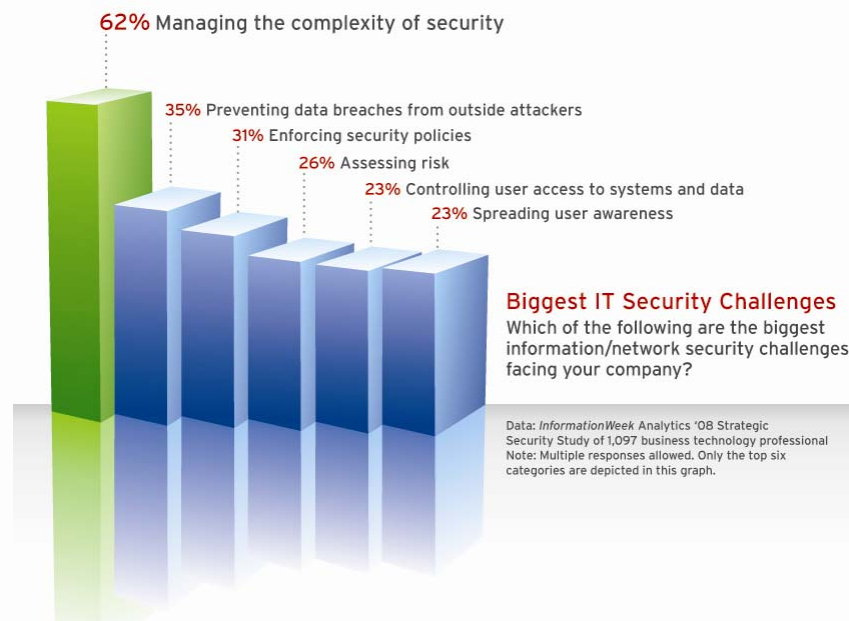


Figure 2: Biggest IT Security Challenges

These changes make mastering enterprise IT security more difficult today than it has ever been before. The 2008 InformationWeek Strategic Security Survey determined that the biggest security challenge is managing the complexity of security. This was followed by preventing breaches, enforcing security policies, assessing risk, controlling user access, and spreading user awareness. The study also found that 69 percent of businesses believe they are more vulnerable to risks this year than last year because of the increased sophistication of attacks.[6]

Enterprises need a solution that closes the window of vulnerability, while also reducing management complexity—this combination addresses all of the key enterprise security challenges.

## IV. NEED FOR A NEW PROTECTION PARADIGM

The enterprise risk profile has changed significantly. Just a few years ago it was relatively easy for enterprises to keep up with content security threats. The longer it took to deploy security, the more the risk grew, but enterprises had more time to implement a defense. Fast forward to 2008 and the risk profile includes significantly higher costs in a much shorter period of time. Cybercriminals are continuously releasing threat variants to get around security, increasing threat speed, and using threats like data-stealing malware, ransom attacks, and botnets. When it comes to protecting enterprises, time is more critical today than it has ever been before. Enterprises cannot risk delays when it comes to securing private data, business resources, and company reputation.

### ***TOO SLOW FOR AN EFFECTIVE DEFENSE***

Conventional security solutions cannot combat the new generation of faster, stealthier threats. Most security solutions rely on periodic pattern file downloads that cannot keep up with the volume and speed of today's threats. This reactive approach relies on the discovery of a threat, the creation of a threat signature, and the deployment of the pattern file. For endpoint protection, enterprises have to download pattern files across all of their clients. This entire process can take hours, if not days, creating a significant window of vulnerability. As more time elapses in identifying and resolving threats, risks and costs increase.

As the number of threats increase, so does the size of the pattern file that has to be downloaded. And scanning threats on the network increases infrastructure costs, such as bandwidth and storage. Downloading static pattern files to servers and clients is not only impractically slow in defending against the latest threats, but the security itself consumes considerable resources and impacts efficiency.

*“Trying to distribute thousands of attack signatures per day to millions of endpoints in a timely manner is not a viable approach. Trend Micro’s innovative strategy enhances its detection network to also prevent attacks from even reaching customer endpoints and enterprise networks.”*

Ogren Group, August 2008

Today's higher threat exposure causes enterprises using conventional content security products to significantly increase costs just to maintain a defense. However, in the future, conventional security solutions will not only be costly and risky, they will be completely unsustainable. Threats are expected to continue to increase exponentially. Pattern files will grow too large to provide an adequate defense and the time and infrastructure needed to deploy them will be impractical, if not impossible.

## ***TIME FOR CHANGE***

Conventional solutions provide an outdated approach to protection. The content security industry needs a new protection paradigm—a solution that minimizes security latency, closing the window of vulnerability. Enterprises need systems that can actively deal with evolving threats, seeing the trend before it happens and stopping the event from occurring. But an effective security solution has to be more than just fast. It must be tightly engineered to decrease the dependency on pattern file downloads and stop threats at their source, taking a load off the network.

Better protection should also be easier to manage. A common pain point for security executives is the level of complexity inherent in enterprise security and the time and resources required to keep an enterprise secure. Time is money. But the time it takes to protect the network can also impact more than the bottom line. Without a solid defense, content security threats can negatively impact brand reputation, customer satisfaction, and worker productivity. Enterprises cannot risk delays when it comes to securing private data, business resources, and company reputation. Enterprises need a better approach.

## **V. TREND MICRO ENTERPRISE SECURITY**

Trend Micro Enterprise Security is a tightly integrated offering of content security products, services, and solutions designed to help enterprises stay ahead of content security threats. To offer the best defense with proactive protection, Trend Micro believes there are two critical time challenges to address. First, it is critical to minimize the time it takes to protect the enterprise from new and unknown threats by tightening the time it takes to identify threats, create protection, and put that protection into place. Second, it should take less time to manage security with a better solution that minimizes complexity in addition to providing effective protection.

Trend Micro Enterprise Security addresses both of these content security time challenges and does so more effectively than any other security vendor in the marketplace by providing immediate protection with less complexity. First you get immediate protection that improves automatically—closing the window of vulnerability. Second, this tightly integrated security provides less complexity and minimizes the time it takes to acquire, deploy, and manage content security. Trend Micro Enterprise Security gets there first—before cybercrime can infiltrate businesses and impact resources.

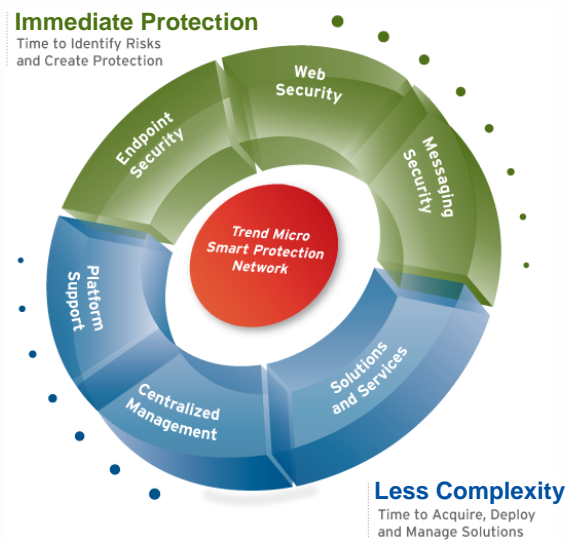


Figure 3: Trend Micro Enterprise Security Offers Immediate Protection with Less Complexity

## VI. TREND MICRO SMART PROTECTION NETWORK™

Trend Micro Enterprise Security is able to deliver immediate protection with less complexity because all solutions are powered by the unique Trend Micro Smart Protection Network. This innovative approach delivers security that is smarter than conventional methods—blocking the latest threats before they reach the organization to prevent threats from impacting networks and damaging businesses. The Smart Protection Network uses cloud-client architecture that combines in-the-cloud technology and light-weight client infrastructure to quickly and automatically protect information wherever and however an enterprise's employees connect—from home, within the company's network, or on the go.

Trend Micro starts by accessing threat intelligence with numerous sources of threat information around the globe, providing insight into the latest attacks whenever and wherever they strike. Trend Micro is uniquely positioned to provide automatic and immediate protection by instantaneously correlating threat data collected in real time through a global network of sensors. This threat information is analyzed using the global knowledge of over 1000 dedicated content security experts at TrendLabs<sup>SM</sup> locations worldwide. The results of the threat analysis are correlated in the cloud across three types of reputation databases—web, email, and file—which protects across all types of attack delivery mechanisms.

Smart Protection Network automatically coordinates information from in-the-cloud threat correlation, behavior analysis, feedback loops, and global threat intelligence to dynamically update the web, email, and file reputation databases. This up-to-the minute data is immediately available to the thin-client technologies in Trend Micro products at the customer site.

## **INTEGRATED REPUTATION DATABASES**

### *Web Reputation*

As a critical element of the Trend Micro Smart Protection Network, Trend Micro™ Web Reputation technology guards against web-based threats before they endanger a network or a user's PC. Web Reputation assigns a relative reputation score to domains and individual pages within these domains. This approach weighs several factors, including a website's age, frequent changes to the host server's location, and other factors that might indicate suspicious behavior. Web Reputation then conducts malware behavior analysis, monitoring network traffic to identify any malware activity originating from a domain or web page. Trend Micro Web Reputation also performs website content crawling and scanning to complement this analysis with a blacklist of previously known bad or infected sites. Access to malicious web pages is then blocked based on reputation ratings. To reduce false positives and increase accuracy, Trend Micro Web Reputation assigns reputations to specific pages or links, rather than an entire site, in cases where only portions of a legitimate site have been hacked.

### *Email Reputation*

Email is often the entry point of many web attacks. Trend Micro™ Email Reputation blocks up to 80 percent of email-based threats before these threats reach the network or the user's PC. Email Reputation validates IP addresses—or computer addresses—against both a reputation database of known spam sources and a dynamic service that can assess email sender reputation in real time. Reputation ratings are further refined through continuous analysis of the IP addresses' behavior, scope of activity, and prior history. Malicious or nuisance emails are blocked at the source based on the reputation of the sender's IP address. The breadth and depth of Trend Micro's email sensor network enables Email Reputation to detect bot-infected mail servers and downgrade their reputation quicker than competitive solutions. The reputation status is continually updated to ensure that a good reputation is restored when infected bots are cleaned, resuming delivery of legitimate email.

Threat information from Web Reputation is also leveraged to identify dangerous URLs embedded in emails. If Web Reputation determines that a web page contains malicious content, Trend Micro anti-spam will identify any email containing a link to that web page as spam.

### *File Reputation*

The Trend Micro Smart Protection Network also assesses the reputation of specific files, including files downloaded from websites and email attachments. Cybercriminals frequently move individual files with malicious content from one website to another to avoid detection. Web Reputation alone is not enough to track these threats in a Web 2.0 world. As cybercriminals move a malicious file from website to website, a reputation may not yet be assessed for each web page that contains this file, but the file's reputation will be triggered wherever the file is found. In addition, any file attached to an email is checked for malware, including viruses, spyware, and other dangerous code.

Trend Micro™ File Reputation checks the reputation of a file against an extensive database before permitting the user to download it to their system. To continually update the database in real time, File Reputation instigates a data crawl of each file hosted on a web page or attached to an email, as well as an assessment of each file's reputation.

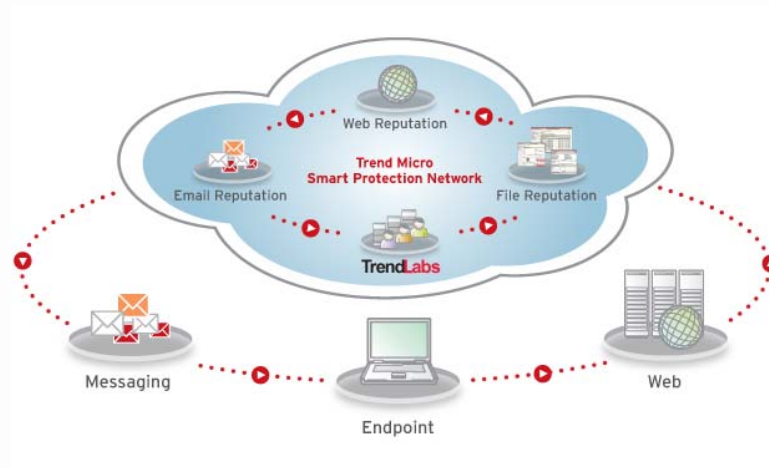


Figure 4: Smart Protection Network Diagram

## **CORRELATING THREAT INTELLIGENCE**

### *Across Reputation Databases*

All reputation databases are updated constantly and share data to provide significantly better protection than would be possible using any of these databases by itself. If any one attack element gets a bad reputation, it is automatically blocked across all threat delivery methods—providing immediate protection at every point of attack. This approach safeguards against all components of a content security threat—spam sources, embedded links, dangerous attachments, and malicious websites.

### *Using Behavior Analysis*

Not only do the reputation databases share threat intelligence, they also work together to determine if a threat is present. Although a single email or other component of a web threat may appear innocuous, several activities used in conjunction can create a malicious result. The Trend Micro Smart Protection Network uses behavioral analysis to correlate combinations of threat activities to determine if they are malicious. A holistic view—gained by examining the relationship between and across the different components of a potential threat—is required to determine if a threat is actually present.

Behavior Analysis is used to identify threats in three scenarios:

- **A Single Issue on One Protocol.** One example is an SMTP email attachment with a suspicious double extension, where the analysis is conducted on a single attachment sent over the SMTP protocol.
- **A Combination of Multiple Network Connections on the Same Protocol.** In this case, a downloader blended threat may contain individual files that appear to be innocent when downloaded, but together they form a malicious program. Investigating any of the individual files would not have discovered the threat. Only when analyzed together is the malicious result discovered.
- **Multiple Sessions across Different Protocols.** An email with a URL link may be sent to several recipients. Once users click on the link and land on the web page, an HTTP executable file downloads, infecting the user's PC. Here, a bad reputation is given to the file and then the reputation is extended to the web page, which is further extended to the email with the embedded URL to that web page. Looking at the email with the link is not enough. A holistic view of how all of these elements work together is needed to provide protection.

Information gathered from behavior analysis is distributed across all three threat databases, enabling the Smart Protection Network to block threats at all points of the attack. Whether using one product or a complete security solution from Trend Micro, enterprises can leverage the correlated information between the reputation databases. By correlating different threat components and continuously updating its threat databases, Trend Micro has the distinct advantage of responding in real time, providing immediate and automatic protection from email, web, and file-based threats.

### *Leveraging In-House Technologies*

Trend Micro is unique in owning all the security technologies used in this correlation process with a number of patent-pending technologies designed to protect customers from web threats. Trend Micro maintains the world's largest, most reliable reputation databases with over 5 billion dynamically rated websites, spam sources, and files every day.

### ***BENEFITS OF A CLOUD-CLIENT ARCHITECTURE***

With the Smart Protection Network, not only is threat information correlated, it is also delivered through a cloud-client architecture that enables enterprises to access this information much faster than traditional methods of protection. Conventional content security relies on pattern file updates which are not fast enough to keep an enterprise safe—particularly in today's threat environment. Cloud-client architecture is much faster because it houses threat intelligence in the cloud. Trend Micro can update the reputation databases in real time and enterprises can quickly access this information as needed—no longer waiting for periodic downloads of static pattern files to be protected.

Not only does this minimize security latency, but it also reduces the burden on the network. With Trend Micro's cloud-client architecture, more threat intelligence resides in the cloud. This means that content

security protection is less taxing on network and endpoint resources. This means that more of your critical computing resources can remain focused on other, non-security related business activities.

The cloud-client security model is the only approach today that will be able to scale as threats continue to increase. Security that relies on pattern files will not be sustainable. The pattern files will become too large for networks to download and distribute across clients and servers. A cloud-client architecture is needed to provide immediate protection, while also reducing network costs—regardless of the quantity of threats.

### **THREAT INTELLIGENCE FEEDBACK LOOPS**

Trend Micro is in a distinct position in the security industry—not only does Trend Micro have a vast global customer base, the threat information from those customers is leveraged to gather immediate threat intelligence. Each new threat identified via a single customer's routine reputation check becomes part of a feedback loop that will automatically update databases around the world, blocking any subsequent customer encounters of a given threat. These built-in feedback loops provide continuous communication between Trend Micro products and Trend Micro's threat research centers and technologies.

Threat information is also analyzed at TrendLabs—Trend Micro's global network of research, service, and support centers. TrendLabs has over 1000 dedicated content security threat experts located around the world, including the United States, the Philippines, Japan, France, Germany, and China. Multilingual staff members analyze global threats and respond in real time, providing 24/7 threat surveillance and attack prevention to detect, pre-empt, and eliminate attacks. Using a combination of technologies and data collection methods—including “honeypots,” web crawlers, customer and partner submissions, feedback loops, and TrendLabs threat research—Trend Micro proactively gains intelligence about the latest threats, to provide enterprises with immediate protection that improves automatically.

### **SCALE AND SCOPE**

The scale and scope of the Smart Protection Network is astounding. Other vendors are not able to offer their customers this level of protection against today's content security risks. Trend Micro is the only company that can deliver immediate protection through cloud-client technologies based on global threat insight.

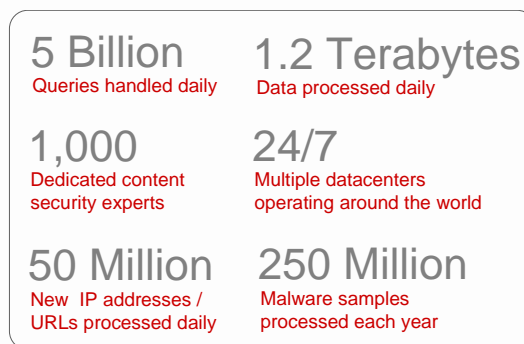


Figure 5: Smart Protection Network by the numbers

## VII. BENEFITS OF TREND MICRO ENTERPRISE SECURITY

### **COMPREHENSIVE CONTENT SECURITY**

Trend Micro Enterprise Security, powered by the Smart Protection Network, creates a unified defense throughout the network with web, messaging, and endpoints security. Trend Micro Enterprise Security delivers immediate protection against content security threats across the entire network with up-to-the-minute security. Trend Micro provides this same security and assurances to xSPs, ecommerce sites, and social networking sites—securing their digital assets and reputation, as well as the security of their site users' information.

Trend Micro protects every point of the network from the cloud to the gateway to desktop to handhelds, securing every attack vector, including email and compromised websites. This content security provides complete protection against any attack and a comprehensive platform for the integration of future information security technologies. Tightly integrated, centrally-managed security enables seamless inter-product collaboration to guard every network endpoint.

With Trend Micro, enterprises can avoid using a patchwork of narrowly focused security products and deploy an integrated content security solution across the network. A comprehensive defense across web, messaging, and endpoints blocks content security threats wherever they attack. Trend Micro Enterprise Security products and services minimize the time it takes to identify risks and secure your network.

### **REDUCED COMPLEXITY**

A better security solution will not only provide immediate protection, it will also provide less complexity, lowering costs. A proliferation of security point products has left many enterprises challenged with managing complexity and exposed with potential gaps in their security. Trend Micro solves these issues through a unified defense that simplifies security management. The Smart Protection Network is at the core, providing immediate, effective protection, and it has been built into flexible solutions that are easy to acquire, deploy, and manage.

Unlike conventional security, Trend Micro's cloud-client architecture in the Smart Protection Network reduces the complexity of deploying pattern files by housing threat intelligence in the cloud and blocking content security threats before they even reach the enterprise. The light-weight client architecture and fewer threats on the network take a load off infrastructure resources. With less burden on the network, costs and management requirements are reduced.

- **Holistic Solutions.** While many other security vendors are narrowly focused on securing specific points within the network infrastructure, Trend Micro Enterprise Security adopts a more comprehensive approach to content security. Trend Micro's international product development teams have designed complete content security solutions that combine integrated, best-of-breed technology with maximum flexibility. For example, Trend Micro's endpoint security combines web threat protection, device-level encryption, and

# TREND MICRO ENTERPRISE SECURITY

data leakage prevention tools with 24x7 expert analysis and support to provide a comprehensive security solution that earned a position in the leader's quadrant within Gartner's December, 2007 "Endpoint Protection Platforms Magic Quadrant" report.[4] Purchasing full solutions from Trend Micro, instead of single point products also offers less complexity by providing one point of purchase, maintenance, and support.

- **Flexible Platform Options.** The flexible platform support offered for Trend Micro Enterprise Security allows customers to select the solution that best fits their network environment. Trend Micro's enterprise solutions are offered on software supporting over 20 operating systems, Software as a Service, or SAAS, appliances, and software virtual appliances. These platform options optimize and integrate with enterprise network environments, making IT security more efficient.
- **Centralized Management.** In addition, centralized management across these solutions further simplifies configurations and reporting to make managing enterprise security easier and faster. Unlike the multi-vendor best-of-breed security in place at many enterprises, Trend Micro lowers Total Cost of Ownership by providing a comprehensive security solution with shared management tools and technologies that easily integrate into the existing IT infrastructure.
- **Vertical Market Support.** Trend Micro Enterprise Security also provides full threat protection for enterprises in every vertical market including industry solutions for financial services, healthcare, public sector, and manufacturing. Trend Micro helps to meet the privacy requirements of many industries with data leakage tools that secure against and educate about accidental and intentional transfer of critical digital information. Device-level encryption also secures enterprise data at rest, regardless of platform, providing additional security against device loss and theft. Vertical solutions integrate messaging, web, endpoint, ecommerce, and communication and collaboration security to offer a comprehensive approach to security management customized for specific industries.
- **Protects Evolving Business Models.** Trend Micro also understands the security requirements for new technologies trends, including protecting mobile workers, Web 2.0 technologies, virtualization, as well as other new and emerging technologies that will support businesses in the future. Trend Micro's cloud-client architecture delivers constantly-updated threat intelligence from minute zero and keeps roaming users protected from web threats when both on and off the network. These in-the-cloud technologies also protect against new threats emerging in the Web 2.0 environments. And this protection is provided with full virtualization support, including software virtual appliances for both messaging and web security.

All of this adds up to a uniquely cohesive framework of offerings that collaborate to provide the industry's best security with less complexity. Trend Micro recognizes the value of time, and will partner with organizations to save them time, allowing enterprises to focus on other high priority initiatives.

## VIII. WHY TREND MICRO

Singularly focused on content security since its founding 20 years ago, Trend Micro provides deep content security core competency and expertise. Trend Micro continues to provide innovation with the Smart Protection Network, correlating real-time data on new and unknown threats and delivering continuously updated protection.

With over one billion U.S. dollars in annual revenue, over 1,000 threat researchers—and over 4,000 employees—around the world, Trend Micro has the size, the speed, and the unique in-the-cloud core technology infrastructure required to handle today's enterprise security. No other security vendor can match the strengths Trend Micro offers enterprises. That is why thousands of enterprises around the globe continue to put their trust in Trend Micro.

*“This increasing scale simply breaks the old model as it demands constant signature updates, massive local pattern matching databases, and growing system resources. Trend Micro Smart Protection Network is a new type of security model that is spot on and a view of things to come for threat management.”*

**Enterprise Strategy Group**, July 2008

## IX. CONCLUSION

Enterprise content security is rapidly changing. As the speed of threats increases, so do risks and costs. Enterprises are looking for security that is scalable, manageable, and capable of reliably staying ahead of new threats. Trend Micro Enterprise Security minimizes the time to protect the enterprise from the latest threats, and gives IT professionals the time to proactively manage and optimize security throughout their enterprise.

Only Trend Micro offers the unique combination of immediate protection with less complexity. Powered by the unique Smart Protection Network, Trend Micro Enterprise Security delivers immediate protection that improves automatically, closing the window of vulnerability before damage is done. Trend Micro also dramatically reduces the time to acquire, deploy, and manage security. With Trend Micro Enterprise Security, enterprises minimize their time to protect, securing their customers, employees, data – and their business.

## X. REFERENCES

- [1] AV-Test. “Considerably more viruses, worms and other malware than ever.” Data compiled by Andreas Marx (listed in articles in the AV-Text news archive 11 January 2008). Retrieved from: <http://www.av-test.org/index.php?menue=2&sub=Newsarchiv&lang=0>
- [2] bMighty.com. “Experts Flag 10 Emerging IT Security Trends.” Mathew Schwartz. 27 September 2007. Retrieved from: <http://www.bmighty.com/security/showArticle.jhtml?articleID=202102359>

- [3] Enterprise Security Today. "Online Threats Materialize Faster, Study Shows." Jordan Robertson. 30 July 2008. Retrieved from: [http://www.enterprise-security-today.com/news/Online-Threats-Materializing-Faster/story.xhtml?story\\_id=103000ABOLCT](http://www.enterprise-security-today.com/news/Online-Threats-Materializing-Faster/story.xhtml?story_id=103000ABOLCT)
- [4] Gartner Group. "Magic Quadrant for Endpoint Protection Platforms." Peter Firstbrook, et al. 21 December 2007.
- [5] Gartner Group. "Virtualization Changes Virtually Everything." Phillip Dawson and Thomas J. Bittman. 28 March 2008.
- [6] InformationWeek Analytics. "2008 InformationWeek Strategic Security Survey." Mike Fratto. June 2008.
- [7] InformationWeek Analytics. "The New Sprawl: Managing Virtual Server Environments." Joe Hernick. April 2008
- [8] Privacy Rights Clearinghouse. "A Chronology of Data Breaches." Data from January 2005-September 2008. Retrieved from: <http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>
- [9] SC Magazine. "Report: 60 Percent of Businesses Hit by Cybercrime." Poremba, Sue Marquette (based on data from the Department of Justice). 18 September 2008. Retrieved from: <http://www.scmagazineus.com/Report-60-percent-of-businesses-hit-by-cybercrime/article/118195/>

©2008 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [WP01\_TMES\_081012US]