


A background image showing a laptop on a desk with a speedometer overlay, suggesting performance or security metrics.

Trend Micro OfficeScan 10 with File Reputation

Part of Trend Micro Enterprise Security. 

 A Revolutionary New
Approach to Enterprise
Endpoint Security

A Trend Micro White Paper | March 2009

I. DRAMATIC RISE IN THREATS

The number of threats being propagated by cybercriminals is growing at an alarming rate. The number of unique threats processed per hour has skyrocketed from 205 in 2007 to 799 in 2008—almost a 400% increase. This has been documented by TrendLabs, Trend Micro's global network of research, service and support centers committed to constant threat surveillance and attack prevention. For several years, TrendLabs has been monitoring the astounding increase in the number of unique malware samples per hour and the results are eye-opening.

This increase in volume has been fueled by the evolution of common business enablers, such as universal web access and the dependence on the Internet for business-critical communications. To capitalize on an increasingly available target, the malware industry has become sophisticated, well-organized, and profitable. Nowhere is this felt more in the enterprise than at the endpoint.

Cybercriminals realize that traditional endpoint security approaches cannot keep up with an extremely high volume of threats, opening a window of vulnerability to exploit. Enterprises are struggling with larger and more frequent pattern updates and users are becoming increasingly frustrated with the demands of bigger endpoint security that leaves endpoints with fewer resources at their disposal. These issues combine to form a perfect storm—an ideal environment that is ripe for targeted attacks and data-stealing malware.

The time is right to rethink endpoint security and question assumptions on how endpoint protection should be delivered. More frequent updates and larger signatures are not the answer. IT Administrators yearn to be freed from the chains of increasingly complex endpoint security solutions that require more and more time to manage. End users long to work without fear of their endpoint security solution staging an all-out coup on the limited CPU and memory resources on their devices.

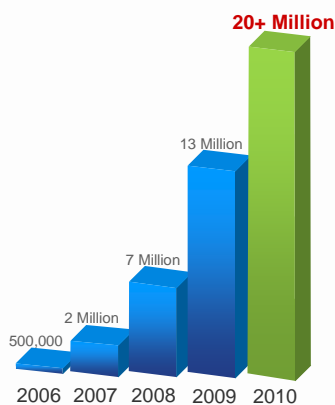


Figure 1: The Dramatic Increase in Unique Malware Samples¹

With OfficeScan 10, Trend Micro introduces a revolutionary new way to defeat the volume of today's threats—File Reputation moves the burden of protection off the endpoint and into the cloud. This white paper describes this new technology and how it provides more effective protection for enterprise endpoints, while reducing management complexity for administrators and resource utilization for end users.

II. COMPLEXITY INCREASES THE RISKS OF SECURITY

For the past several years, the enterprise endpoint security market has run amok with feature envy. As new threats emerged, new features were either purchased or developed to counter them. As each new technology took the market by storm, most vendors struggled to keep up with a rising number of acquisitions, resulting in increasingly expansive product offerings. But long after the dust has settled, the question remains, “Are enterprise endpoints more secure?”

With so many point products and so many tactical features at their disposal, enterprises can easily find themselves overwhelmed by the complexity of their solutions. In fact, the complexity of many traditional solutions is more of a concern for enterprises than the threats they were designed to address.



Figure 2: Biggest IT Security Challenges²

For many enterprises, the complexity of endpoint security surfaces in the daily challenge to manage and deploy an increasing number of pattern file updates for thousands of endpoints. Factors such as increasingly mobile endpoints, complex network infrastructures, and the increasing frequency of pattern updates all work to further challenge security—actually countering the effectiveness of an otherwise strong defense.

Addressing the growing volume of threats consumes more and more endpoint resources, resulting in end users becoming increasingly frustrated with slow machines. According to IDC, there has been an increase in “complaints from corporate users and consumers that, ‘Security is eating my machine. It takes forever to boot. AV scans make work impossible. Background security tasks always slow down application and web access.’” As a result, end users are less productive as they either walk away from their useless computer in frustration or spend their time searching terms such as “disable antivirus”.

Trend Micro realizes that complexity is as big a challenge as effective protection. As a result, Trend Micro Enterprise Security strongly asserts that immediate protection must be accompanied by less complexity. Otherwise, the advantages of increased security will be nullified by the productivity lost. Achieving this balance is what makes the Trend Micro approach to endpoint security unique.

III. THE NEED FOR A NEW APPROACH

Current endpoint security relies on file-based threat handling with patterns (or definitions) delivered in batches from security vendors to endpoint security solutions on a scheduled basis. Whenever a new update is received, the security software on the computer reloads a new batch of pattern definitions to the hard disc and into memory. Any time a new malware risk emerges, this pattern needs to be updated again and reloaded on the user's computer to ensure continued protection. The time it takes to update represents a gap in the computer's security.

As attacks hit faster and faster, the volume of threats represents a new type of security risk. The process of constantly updating can impact server and workstation performance and network bandwidth usage, as well as the critical time it takes to deliver quality protection.

To effectively combat this extreme volume of threats, Trend Micro has pioneered a new approach designed to immunize the threat of malware volume. Leveraging a revolutionary new technology and architecture, Trend Micro is able to remove the bulk of malware signature storage from the endpoint and move it into the cloud. By offloading the burden of malware signatures, Trend Micro provides immediate protection against an ever-increasing future volume of security risks.

IV. FILE REPUTATION

Traditional malware scanning identifies infected files by comparing several hash values of the file content with a list of hash values stored in a pattern file. If a file is marked suspect in the first pass of hash comparison, the scan engine employs a multi-phase approach to further drill down on it. In all of today's conventional endpoint security solutions, this pattern file is located on the endpoint and has to be distributed regularly to provide protection against the latest threats.

Trend Micro breaks that paradigm. Our new File Reputation decouples the pattern file from the local scan engine and conducts pattern file lookups over the network to a Smart Scan Server. That Smart Scan Server may reside on the customer premises or even on the Internet. This in-the-cloud approach alleviates the challenge of deploying a large number of pattern files to hundreds or thousands of endpoints. With Trend Micro's new approach, as soon as the pattern is updated on the Smart Scan Server, protection is immediately available to all clients leveraging that scan server. File Reputation addresses today's enterprise endpoint security challenges by providing shorter time to protect while assuring less complexity.

"Trend Micro is shifting the burden of anti-malware signature scanning from customer endpoints into Trend's Smart Protection Network. This dramatic move is mandated with the realization that 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



COMPONENTS OF THE ARCHITECTURE

Smart Client

The central scanning component of Trend Micro's endpoint security solution is the Smart Client. Comparable to the scan engine in traditional content scanning, the Smart Client interacts with Smart Scan Servers to determine with certainty whether a file is infected or not and what action is to take on that file.

Smart Query Filter

A component of the Smart Client, Smart Query Filter is designed to prevent the Smart Client from querying the Scan Server for every single file that needs to be scanned. The Smart Query Filter leverages complex mathematical models to determine—with a high degree of accuracy—whether the file scanned can be found in the actual pattern file. Due primarily to its principles of operation, the Smart Query Filter does not generate false negatives and only a small number of false positives. If a file is not “whitelisted” by the Smart Query Filter, the local signature cache is queried to find the signature for this file. For offline scenarios where no Smart Scan Server can be queried, the Smart Query Filter references an “index” of the pattern file, allowing it to determine whether any given file is NOT in the pattern file on the Smart Scan Server.

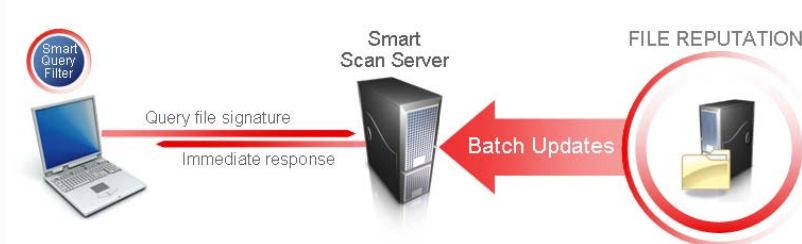


Figure 3: Scan Server Flowchart

Smart Scan Server

The Smart Scan Server resides on the customer network for easy access to endpoints. This minimizes gateway network traffic and reduces the latency of cloud pattern lookups. The Smart Scan Server receives and immediately stores pattern files from Trend Micro. If necessary, the Smart Scan Server also signals updates to the client's Smart Query Filters which take place on the next Smart Client query. Generally, the Smart Scan Server is the only component of the solution that receives frequent updates. Having only one central component to update increasingly often is much easier and significantly faster than deploying patterns to all individual endpoints.

V. RETHINKING ENDPOINT SECURITY

RETHINKING THREATS

In the past months, the number of threats has increased exponentially. The risk of enterprises being impacted by new malware has grown significantly. While releasing patterns in a higher frequency alleviates the problem for centralized sites such as gateways and mail-servers, it does not solve the problem for enterprise endpoints. The window of exposure for individual endpoints is difficult to close, due to the time and effort needed to increase the frequency of deploying protection to the clients.

RETHINKING PATTERN MANAGEMENT

Managing patterns in distributed enterprise environments is a key challenge for security administrators. Not only does a non-consistent pattern deployment mean additional risk for the individual clients, it also makes a realistic risk assessment impossible. In enterprises of all sizes, administrators struggle to maintain the same pattern level across the endpoint population. But increased mobility and rapid pattern releases worsen their ability to address threats. In today's threat environment, malware protection is no longer about being able to block every single threat; it is more realistic to aim at providing the best possible protection using a set of powerful risk-management tools.

The need to deploy patterns to thousands or tens of thousands of individual endpoints represents a significant burden for an enterprise. The difficulty of ensuring that all endpoints are updated—whether they are on the local network or connected to the internet while roaming—makes it particularly challenging to maintain consistent policy and pattern levels.

File Reputation technology instantly provides identical protection to all endpoints, ensuring faster time to protection, delivering consistent protection, and facilitating risk-management. This reduces the complexity of managing—and risk-managing—an ever increasing number of pattern deployments while increasing the quality of protection.

RETHINKING ENDPOINT RESOURCE CONSUMPTION

Keeping pattern files at the endpoint consumes a significant amount of resources, especially memory. For today's traditional security solutions to provide real-time on-access protection capabilities on the endpoint, they have to integrate with the Operating Systems at the kernel level. For on-demand or scheduled scanning capabilities and powerful, automated clean-up, each and every pattern file has to be loaded not only into the kernel-mode driver but onto user-mode components as well.

Despite continuous optimization of its file format, pattern files have grown significantly over the past 24 months. In fact, over the past years, the industry average has shown a 241% growth³ in the size of pattern files. And they will continue to grow in the coming months to address the ever accelerating rate of malware availability. Given limited endpoint resources, larger pattern files are simply not sustainable. The concept of hosting pattern files on the endpoint is destined to fail in the near future.

Trend Micro's File Reputation technology is much leaner than traditional approaches. Only the Smart Query Filter index—as well as the occasional updated pattern file for highly complex malware—resides on the endpoint. Using cloud-based patterns significantly reduces the amount of resources taken away from the system and applications on the endpoint, freeing up memory and accelerating the system's overall performance. The result is a better user experience is better and a corresponding increase in productivity.

Ultimately, if end users do not notice significant delays from their endpoint protection, they are more likely to keep existing protection in place, facilitating policy enforcement. Endpoints using File Reputation are more

“Trend's level of integration and cooperation between the different levels, products, and services is highly developed. For example, it using its cloud-based approach to reduce threat management scanning at the endpoint level. This reduces the footprint of the endpoint security client. This can extend the useful life of older PCs that are bedeviled by the resource requirements of new security suits. It also has the potential to reduce user complaints to the help desk about new security software slowing down their old hardware.”

IDC, August 2008



likely to experience better, more consistent protection because end users are no longer encouraged to disable endpoint security to reclaim performance. By reducing the size and frequency of signature file downloads on the endpoint, File Reputation frees up endpoint resources, improving performance, stability, and user productivity.

By streamlining network-wide implementation with the ability to identify and manage endpoint security on every computer regardless of location or connectivity, File Reputation makes security management easier while saving costs for the business. With less frequent, lighter-weight updates on the endpoint, File Reputation reduces the burden of ongoing signature file management and deployment. And because the File Reputation blocks most threats at the source based on reputation, administrators spend less time and money cleaning threats on endpoints.

By maintaining a predictable resource utilization schedule, File Reputation can also reduce overall capital expenses. For example, as the number of threats increases over the coming years, endpoints using File Reputation will experience no unexpected hike in the minimum system resources required for security. So enterprises always have updated protection without deploying unexpected endpoint refreshes.

RETHINKING BANDWIDTH REQUIREMENTS

Deploying patterns to thousands of endpoints requires large amounts of network bandwidth, increasing steadily with the acceleration of pattern releases. When assessing this bandwidth savings of File Reputation, it is important to understand that to achieve the same level of protection—especially the same rapid time to protection—patterns must be deployed to individual endpoints in much shorter cycles than they are today. File Reputation accomplishes this relative speed by transferring the pattern only once, to the Smart Scan Server. This saves a tremendous amount of network traffic, which would have otherwise been consumed deploying that same pattern to thousands of endpoints.

VI. JOIN THE ENDPOINT SECURITY REVOLUTION TODAY!

OfficeScan 10 is the right choice for medium and large enterprises. The revolutionary new File Reputation frees your endpoints from the resource drain and frees your administrators from the burden of deploying and managing an ever increasing stream of pattern files. So regardless of whether your endpoints are in an airport, a hotel, a home office, or within your corporate network, they'll get immediate protection with less complexity.

Learn new ways to rethink your endpoint security. www.trendmicro.com/RethinkEndpointSecurity.
Or speak to your local Trend Micro sales representative at +1-877-21-TREND.

¹ AV-Test. "Considerably more viruses, worms and other malware than ever." Data compiled by Andreas Marx (listed in articles in the AV-Test news archive 11 January 2008). Retrieved from: <http://www.av-test.org/index.php?menu=2&sub=Newsarchiv&lang=0>

² InformationWeek Analytics. "2008 InformationWeek Strategic Security Survey." Mike Fratto. June 2008.

³ Trend Micro internal benchmark tests.