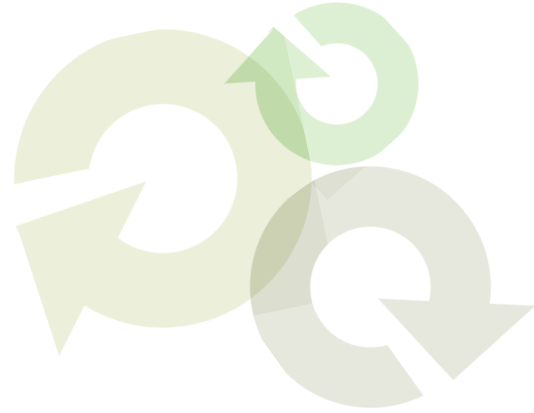




WhitePaper:



**Reshaping Your Endpoint
Security Strategy**



Reshaping Your Endpoint Security Strategy

Reshaping Your Endpoint Security Strategy

Abstract: Business as usual when it comes to managing and securing endpoints is no longer affordable. Not just because of tight budgets and shrinking IT staff, but because threats are changing. During the past 15 years, organizations have built up defensive barriers for the servers and databases that house their most sensitive data. But today's polymorphic threats aren't restricted to the data center. These modern threats have moved downstream, to endpoints outside the protective cocoon of the data center, providing hackers an on-ramp to your network.

So why don't endpoints receive the same attention as the critical business systems in the data center? A multitude of reasons: it is too time consuming to patch these endpoints, there is a lack of visibility to know that endpoints don't match corporate-defined configuration policies, or the current antivirus solutions are slow, bloated, and impedes business productivity. The business of managing and securing endpoints is in serious need of an overhaul. The singular approach of using a cookie-cutter, one-size-fits-all antimalware program to keep your endpoints safe isn't good enough anymore. You can no longer count on antivirus and antispymware programs that were written for Windows 95 to successfully defend against modern threats. Nor can you afford solutions that require too much time, money, and IT staff to get the job done. Too many of the tools available are lacking. They lack depth and comprehensive protection. They lack the automation needed to be efficient. They lack the visibility and control necessary to be effective. And, they lack results for the dollars invested. These critical IT operations require solutions that are architected for today. Solutions that take a new look at modern technology, modern threats, and modern business reality.

*This document is
provided strictly as a guide.
No guarantees can be
provided or expected.*

Security and Operations Must Meet To Find and Fix the Gaps

Because hackers have moved their attention from the data center, perimeter-only protection at the endpoint leaves you exposed. Many security teams continue to believe that properly configured routers, firewalls, and antivirus software are the keys to good endpoint protection. Though presenting a hardened Internet-facing exterior seems more cost effective (as there are fewer machines to protect and manage), when threats bypass the perimeter, subsequent downtime and cleanup costs can quickly outpace any savings realized by this narrow focus. Threats are bypassing the perimeter protection with increasing regularity, in part due to the rising popularity of virtual private network (VPN) software. Once a threat is



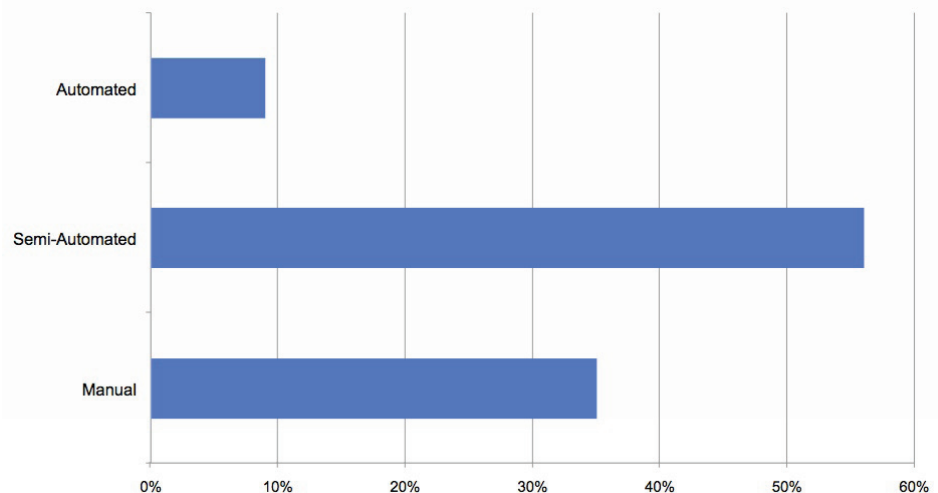
WhitePaper:

Reshaping Your Endpoint Security Strategy

in-house it has little difficulty locating and infecting unpatched or misconfigured machines. Why do endpoints remain a significant hole in corporate security strategies? The primary reason is that in many organizations, once the security team has established perimeter-based protections, the ongoing maintenance -- system updates, signature updates, and mitigation of problems found at the endpoint -- are then the responsibility of the IT operations team. Security may use one set of technologies to find gaps while IT operations uses another set of technologies to close them. This separation of duties might be required for audit purposes, but the lack of integration and automation between these tasks is wasting hours of IT staff time and leaving gaps in system security. Ignoring the importance of an automated, repeatable, and measurable process for finding and fixing gaps in your system security is an ill-advised long-term strategy. It is essentially an invitation to hackers to infiltrate your network and compromise your sensitive data.

And these inefficiencies and gaps continue to occur because IT executives typically don't have visibility into the operational processes required to properly manage and maintain the security of endpoints. The tools the operations teams must work with to manage and mitigate threats often include older-generation, bloated AV software; and a combination of manual and semi-automated processes to update, patch and properly configure their systems.

Are Your Current Processes Manual, Semi-Automated, or Automated?



90% of survey respondents admit that their current configuration management processes are either manual or only semi-automated, using a combination of tools and scripts to maintain the environment. Source: Security Survey conducted from over 435 IT operations and security specialists.

This document is provided strictly as a guide. No guarantees can be provided or expected.



What Are the Endpoints You Are Trying to Manage and Secure?

They Include Your Physical Machines, Of Course

The physical machines that are the endpoints in your centrally-managed network include your servers, your desktop machines, and your laptops. These systems represent the vast majority of machines in your network and it is critically important they are protected. Laptops, which are frequently disconnected from the network, present unique challenges because they are not readily visible nor are they easy to manage. All parts of these physical machines must be considered, including any removable storage devices such as external hard drives or USB drives. This includes software applications that are persistent on the endpoints. Protection and management of endpoints must include identifying and patching third-party applications which often present a large attack surface due to their quantity and diversity.

But Don't Forget About Your Virtual Machines

A virtual image is not a physical, real machine but rather a software environment (usually an operating system) designed to emulate a real machine. A virtual image can run programs just like a physical machine. The physical machine used to host the virtual image can often support multiple virtual images.

Virtual images can be either online or offline. A virtual machine that is online and running is ideally treated exactly the same as a physical machine. This means it should automatically be provided with the same protections as your physical machines.

Offline virtual images, however, present a greater challenge. They are virtual images that aren't powered on when scans, updates, and other preventive measures are being performed. These virtual images may be powered on for only a few hours or days a month and then powered off until they are needed again the next month. It is critically important to ensure that these systems are protected the same as a physical machine so that when they are brought online they don't expose your network to risk.

*This document is
provided strictly as a guide.
No guarantees can be
provided or expected.*



Reshaping Your Endpoint Security Strategy

The Problems with Today's Approach

There are two main problems with today's traditional approach to endpoint security:

- *It depends on bulky, slow, and outdated tools*
- *It depends on a single strategy*

The Commoditization of Antivirus

Many companies provide malware (antivirus + antispyware + anti-rootkit) detection software. They all pretty much detect the same threats using the same detection criteria. So at this point the things that differentiate the good from the bad are not so much what they do, but how they go about it. Some things to consider include:

- *Are they heavy or light on system resources? How much CPU do they consume? How much RAM?*
- *How big of a footprint do they leave? Do they require a lot of disk space? What is the size of the .dat file or signature file?*
- *What does it take to install and manage the program and/or its agents to make sure it's running properly? How many agents are required to successfully defend against all malware threats?*
- *Is it fast or slow? What is its scan time?*
- *How stable, how accurate, and how effective is the product?*

Unfortunately, in many cases the answers to these questions are not good. The "leaders" of this multi-billion-dollar industry have provided us with products that are buggy, bloated, and broken. They have not produced products whose sole purpose is to provide a lean, mean, endpoint security machine. Rather, they have clumsily bolted together the engines of older-generation technologies and called it a day.

Current Antimalware Tools Are Not Good Enough

Even if a particular tool is light on resources and easy to manage, chances are it's still not good enough. Many of the established antispyware, antivirus, anti-whatever programs available today depend strictly on signature files to block malware. This makes these tools obsolete. The turn-around time required to identify new threats, update the signature files, and push the updated files to the endpoints is not fast enough to prevent threats that can pop out of nowhere. They can't respond quick enough to be effective. They don't possess the intelligence to detect threats that aren't conveniently listed in their signature file.

This document is provided strictly as a guide. No guarantees can be provided or expected.



WhitePaper:

Reshaping Your Endpoint Security Strategy

Another part of the problem is the sheer number of signatures that are required. With new threats arriving almost daily, the number of signatures used by antimalware programs is huge. There can be anywhere from 500,000 to nearly one million signatures. Yes that's right, nearly one million distinct signatures. That doesn't mean there are one million known threats. Rather, there are many variants of the same threat that all require a unique signature in order to be blocked. Authors of malicious software understand how the system works and use polymorphic code to modify the malicious code so that it no longer matches the original threat. Some easy math can show that the number of signatures that must be tracked will soon grow out of hand, if it hasn't already done so. Relying solely on a signature blocking strategy that doesn't scale is doomed to failure.

In addition to using polymorphic code to obfuscate and hide their threats, malware authors are creating new threats that often blur the distinction between traditional threat categories, causing additional problems. A virus that masquerades as a worm may not be detected by traditional antivirus software. And the malware may not reside in just one file, it may actually move around to many different files.

Which brings up yet another problem: the old defenses also don't go far enough. If they are able to eventually locate and eliminate an infection, for many that's the end. Just as important, however, is the ability to stick around and clean up all the dirt and sludge left behind by an infection. Often it's the remnants found in registry keys, browser objects, DNS entries, and assorted dummy files that can continue to plague a machine and slow its performance.

The upshot is that these issues have rendered the old defenses useless. Threats are getting through because the defenses are outdated, outmanned, and don't utilize the latest detection techniques, including:

- *Exact signature matching*
- *Heuristics (pattern matching)*
- *Behavior detection (behavior matching)*
- *Whitelisting and blacklisting*

A Single Strategy Is Not Enough

Even with the best available antimalware tools, it is clear that this single-pronged strategy does not go nearly far enough. The tools target only one facet of the problem. They are only reactive and do nothing to proactively prevent bad things from happening. To amass an effective endpoint security strategy there are additional critical-to-perform tasks that must be utilized in conjunction with

*This document is
provided strictly as a guide.
No guarantees can be
provided or expected.*



Reshaping Your Endpoint Security Strategy

antimalware tools. Just as a good general will use multiple tactics when engaging the enemy, good administrators must employ both proactive and reactive measures when protecting their endpoints from harm.

Take a Proactive Approach

A proactive approach provides the defense in depth that helps to prevent threats from finding their way onto your endpoints in the first place. There are three primary legs to a proactive approach:

- *Properly configure your endpoints*
- *Properly patch your endpoints*
- *Utilize real-time protection software*

Properly Configure Your Endpoints

Misconfigured endpoints are one of the main causes of system downtime and exposure to threats and misuse. In fact, studies have shown that up to two-thirds of vulnerabilities are a result of system configuration errors. And it only takes a relatively small percentage of misconfigured endpoints—usually those with nonstandard settings that allow the user too much control—to generate a large number of virus and spyware incidents. The ability to detect and correct configuration errors is therefore a critical component for successfully managing and protecting endpoints. A security configuration management program is a must in order to proactively manage your critical system and security configuration attributes in an automated, repeatable, and auditable manner. You need to understand, check, assess, audit, and enforce policy checks on the endpoints in your network.

What will a security configuration management program help you achieve? By ensuring your endpoints are properly configured it will seal cracks in your defensive armor. For example, it will:

- *Make sure that passwords used to gain access to the endpoint are complex and not easily guessed*
- *Set a minimum password length and a maximum password age*
- *Prevent password guessing programs from working by setting account lockout thresholds to proper levels*
- *Verify that there are no open shares on the endpoint that a hacker can use to gain a foothold on the machine*
- *Require a personal firewall to be enabled*

This document is provided strictly as a guide. No guarantees can be provided or expected.



WhitePaper:

Reshaping Your Endpoint Security Strategy

- *Dictate that all guest accounts are disabled*
- *Record all policy check enforcements that are performed on a machine*
- *... and much, much more.*

Configuring the endpoints once in accordance with a corporate policy is not good enough. You can't simply "set it and forget it." Endpoints must be constantly monitored for changes and reported on. A comprehensive view into the security state of the entire network is required in order to properly assess potential risk to the organization. Vulnerabilities gain a foothold when there is no consistent means of measuring the condition or state of endpoints on the network. As a result, a gap develops between an organization's documented security policies and the true state of individual endpoints on the network. This gap leaves organizations exposed to multiple risks such as downtime from system failure, introduction of security vulnerabilities, and insider security threats.

Organizations that gain visibility and control over configuration settings of their endpoints are also well-positioned to always be ready for the next audit event, whether it is an audit against internal policies or external regulations. A clear and direct mapping of configuration controls to policies and regulations streamlines compliance costs and results in measurable improvements in security.

Properly Patch Your Endpoints

Keeping your endpoints up-to-date with the latest security patches is critically important for keeping them secure. By patching your endpoints, you eliminate many of the vulnerabilities that hackers use to gain access to your system and to facilitate the spread of infection. The goal here is to consistently patch the operating systems and the programs running on your endpoints in order to secure them against known vulnerabilities.

And a properly patched endpoint has other benefits. In addition to providing security, patching an endpoint will:

- *Improve its performance*
- *Increase its reliability*
- *Eliminate known bugs*

The application of patches is one of those critical-to-perform vulnerability management tasks that must be performed in a timely manner. Machines that are unpatched for even a few days or weeks present a risk. According to a recent report, up to 90 percent of security breaches could be prevented by simply keeping machines up-to-date with the appropriate patches (2008 Data

*This document is
provided strictly as a guide.
No guarantees can be
provided or expected.*



WhitePaper:

Reshaping Your Endpoint Security Strategy

Breach Investigations Report, Verizon Business RISK Team). And yet consider the Conficker worm known as Downadup. By January, 2009, it was estimated to have infected more than 9 million machines, even though the patch that plugged the vulnerability (MS08-067) was available in October, 2008.

So what is preventing the patches from being deployed on time? There are many reasons, including:

- *The sheer volume of patches issued each year*
- *The large number of machines that must be patched*
- *The diversity of operating systems and application software*
- *The testing that must be done*
- *The distribution of the patches without affecting the users of the machines*

Patch management is indeed a complex and time-consuming issue. Using a patch management program that simplifies and automates the process is therefore a must. The primary objectives of a patch management program should be to:

- *Scan your machines for patches defined in a patch policy*
- *Report on patches that are missing from those machines*
- *Acquire the patches that are deemed safe for deployment*
- *Perform test deployments to validate the safety of the patches*
- *Deploy approved patches to all required machines in the network*
- *Generate administrative reports that clearly identify the patch status of the machines*

Utilize Real-Time Protection Software

Real-time protection software actively monitors for attempts to install malware on a machine. It is a constant sentry against attempts to sabotage the machine and stops the intrusion from occurring, all in real-time. Real-time protection operates by watching for changes to specific security configuration settings and values. Attempts to change security settings and values are often an indication that some sort of malware is trying to install itself on the machine. If a change is detected it can respond immediately. Depending on how it is configured it may ask the user what to do, or it may simply change the setting back to the original value.

This document is provided strictly as a guide. No guarantees can be provided or expected.



WhitePaper:

Reshaping Your Endpoint Security Strategy

Add a Reactive Approach, Too

The reactive approach until recently was the primary method for deterring threats. In today's environment it is still necessary, but rather than your first resort it should be used as your last layer of defense. A reactive approach is what you must use if trouble finds its way to the endpoints in your network. You must have tools that identify malware lurking on your endpoints and then eliminate it.

But the tools you use cannot be yesterday's technology, they must be state-of-the-art. They should be invisible to the user. They must be purpose-built programs that are:

- *Fast and efficient*
- *Easy on system resources such as CPU, RAM, and disk space*
- *Simple to install and manage*
- *Stable, accurate, and effective*

They must also use advanced, next-generation detection technologies, such as:

- *Exact signature matching*
- *Heuristics (pattern matching)*
- *Behavior Detection (behavior matching)*
- *Whitelisting and blacklisting*

Endpoint Security is a Big Deal!

Still not convinced? Consider this:

- *In 2007 it was determined there were 6,437 new vulnerability disclosures, an average of 124 per week¹*
- *In 2007 there were nearly 410,000 new examples of malware, including viruses, worms, back doors, key loggers, trojans, spyware and rootkits¹*
- *(¹July, 2008 Aberdeen Group – Vulnerability Management Report- Assess, Prioritize, Remediate, Repeat)*

The numbers are mind-boggling and rather scary. Anyone with a stake in the health and well-being of an organization had best pay attention or risk placing their endpoints (and perhaps their jobs) in jeopardy.

How do you go about protecting your endpoints (and yourself)? By:

- *Properly configuring your endpoints*
- *Properly patching your endpoints*

This document is provided strictly as a guide. No guarantees can be provided or expected.



WhitePaper:

Reshaping Your Endpoint Security Strategy

- *Utilizing real-time protection software*
- *Detecting and eliminating trouble that finds its way to your endpoints*

The tools you use to accomplish these tasks must be designed to effectively perform all of the critical IT operational tasks. They must be efficient, provide high performance, provide comprehensive detection and remediation, and yet be simple to use. And they must be able to let you measure the effectiveness of your solution. In the final analysis, unless you can prove your endpoints are indeed secure, they're not.

*This document is
provided strictly as a guide.
No guarantees can be
provided or expected.*