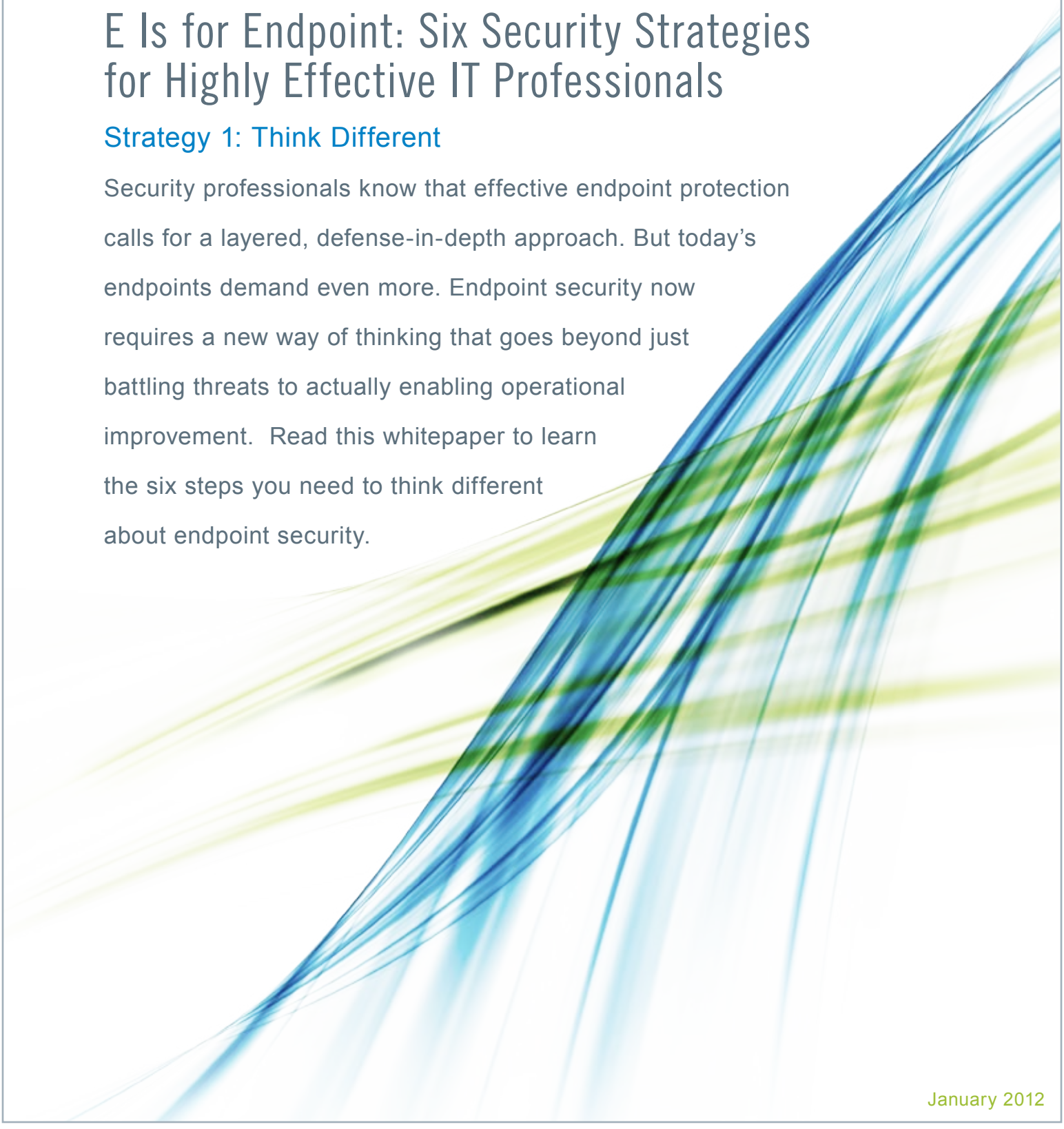
E Is for Endpoint: Six Security Strategies for Highly Effective IT Professionals

Strategy 1: Think Different

Security professionals know that effective endpoint protection calls for a layered, defense-in-depth approach. But today's endpoints demand even more. Endpoint security now requires a new way of thinking that goes beyond just battling threats to actually enabling operational improvement. Read this whitepaper to learn the six steps you need to think different about endpoint security.



January 2012

WP-EN-01-04-12

Overview

We all like the idea of a silver bullet—a single, simple solution to a complex problem. The notion dates to 18th-century France, where such rarified ammo was said to be the only force that could slay a werewolf. Security pros still face werewolves—the malware, spear phishing, click jacking, botnets and denial-of-service attacks that constantly threaten our organizations. But they recognize there's no silver bullet when it comes to information security.

For endpoint protection, however, some have clung to the vain hope that antivirus (AV) alone would do the trick. Others have come around to the need for a layered, defense-in-depth approach, but have sought to achieve it in a narrow fashion, that ultimately leaves their organization vulnerable.

The fact is that endpoint security remains a problem for many organizations. And the risks are only growing, as new forms of attack emerge and mobile business renders the endpoint more porous than ever.

It's time to think different about endpoint security. In particular, organizations today need to:

- Think about endpoint security as more than protecting against threats.
- Guard the data as well as the endpoint.
- Define a trust-based model for endpoint applications.
- Approach endpoint security from an enterprise-wide, operational perspective.

Changing Threats, Changing Needs

Despite ongoing investments in endpoint protection, threats and vulnerabilities remain. Two-thirds of organizations say their networks aren't more secure than they were a year ago.[1] Cybercrime—such as distributing viruses, illegally accessing data and stealing personal information—is now among the top four economic crimes and represents nearly one-quarter of all reported corporate fraud. Forty-eight percent of organizations that have experienced economic crime perceive the risk of cybercrime to be on the rise, and only 4 percent think it's decreasing.[2]

There are several reasons for this poor—and in some ways worsening—state of security:

Higher sophistication and volume of attacks—There's a lot of malware out there. In fact, one in every 14 downloads is malware.[3] Microsoft reports that Internet Explorer—probably not the most sophisticated piece of security software—alone blocks up to 5 million attacks per day.

More problematic is the shifting motivation for cybercriminals to create and disseminate malware. For instance, an underground "pay-per-install" industry is emerging in which hackers foster the proliferation of malware by charging for access. These perpetrators deploy more than 50 "families" of malware, including data-stealing Trojan horses, spam bots, denial-of-service bots and fake AV. To avoid AV detection, such malware is "repacked" every 11 days, on average.[4]

1. Ponemon Institute, "2012 State of the Endpoint"
2. PwC, Cybercrime: Protecting Against the Growing Threat, November 2011
3. Microsoft, The Technology of Socially Engineered Attack and Defense, May 2011
4. University of California, Berkeley, Measuring Pay Per Install: The Commoditization of Malware Distribution, August 2011

Proliferation of vulnerable third-party applications—There was a time when security professionals could rely on Windows Server Update Services (WSUS) for patch management. But today's organizations are stuffed full of third-party applications for which WSUS is useless. The numbers are pretty sobering:

- 66 percent of applications have known vulnerabilities.
- 78 percent of Web 2.0 applications support file transfer.
- 95 percent of organizations have social-networking applications installed.
- 28 percent of applications propagate malware.[5]

Lack of centrally defined and protected IT environments—Security professionals recognize the need for centralized management of IT operations, including security. But the organizations they work for often do not.

Only 41 percent of security professionals say non-IT executives support endpoint security operations. And only 35 percent have ample resources to minimize endpoint risk.[6] Similarly, only 36 percent report that executive leadership reviews cyber-risks at least once a year. And 15 percent never do.[7]

The fault doesn't lie solely with executive management. Only 12 percent of security professionals say that collaboration between IT operations and IT security is excellent, and 40 percent say that collaboration is poor or nonexistent.[8] Those are disappointing numbers, and the result almost surely is worse and less cost-effective endpoint security.

E Is for Endpoint: Six Security Strategies for Highly Effective IT Professionals

This document is part of a series of white papers designed to give IT professionals the knowledge and perspective they need to design, implement and maintain a truly effective defense-in-depth approach to endpoint security.

The complete series of papers, which will be published throughout 2012, address the following end-point security strategies:

- Strategy 1: Think Different
- Strategy 2: Back to Basics With Patch and Configuration Management
- Strategy 3: How to Check Unknown Apps at the Door
- Strategy 4: Enabling the Self-Defending Endpoint
- Strategy 5: Secrets to Reducing Complexity and Cost
- Strategy 6: How to Continuously Manage Compliance and Risk

5. Palo Alto Networks Application Survey 2009, 2010
6. Ponemon Institute, "2012 State of the Endpoint"
7. PwC, Cybercrime: Protecting Against the Growing Threat, Novovember 2011

Explosion of mobility and virtualization—Finally, the IT landscapes we're protecting are becoming ever more dispersed. Organizations are rapidly moving toward virtualized environments, through internal, external and hybrid cloud-computing schemes. Meanwhile, employees are increasingly mobile, accessing the network, transmitting data and storing data on a growing array of smart devices and removable media.

In fact, 42 percent of employees use their personal mobile devices in the workplace. Yet 42 percent of security professionals say their organization lacks an effort to secure those devices.[9]

What's more, 52 percent anticipate that virtualized environments will increase in the next 12 to 24 months. Yet 49 percent say no single department or function has responsibility for virtualization security. Likewise, 35 percent believe internal clouds will expand, and 56 percent expect third-party cloud computing to increase. Yet 41 percent say their organization lacks a cloud strategy.[10]

It's no wonder security professionals predict the greatest risks in 2012 will be remote employees, mobile devices, cloud computing, removable media and third-party applications.[11]

We're experiencing an underlying shift in the practices and expectations of organizations, and the users within them. Companies and employees increasingly believe that all data should be available on all devices, at all times. That's even becoming a competitive necessity as customers and partners expect organizations to serve up information anytime, anywhere.

The fundamentals of good security remain largely unchanged. But the context in which we exercise those fundamentals has shifted. It's time to think different.

Treat the Patient, Not the Disease

Physicians have always thought it was their job to fight diseases. But in recent years doctors have become aware that they can achieve more effective outcomes by treating the patient—the expectations, intentions, societal context and overall well-being of the individual.

The same concept applies to endpoint security. Security professionals have been taught to target threats. Block the threat, the thinking goes, and you have a secure environment. But that's no longer true. Even a defense-in-depth endpoint strategy, if merely threat-centric, ends up being a stack of AV layers searching for inbound attacks. It doesn't address the core configuration and vulnerability exposure of the endpoint itself.

Today, security professionals must think about endpoint security as more than protecting against threats. The best place to start is with patch and configuration management. Implemented effectively, these mechanisms can eliminate much of the attackable "surface area" of your endpoints.

8. Ponemon Institute, "2012 State of the Endpoint"
9. Ibid.
10. Ibid.
11. Ibid.

Deep Defense, Broad Protection

"Thinking different" about endpoint security must be built on a foundation of defense-in-depth. This approach goes beyond standalone technology to implementing layers of protection that deliver holistic security:

» **Patch and configuration management**—At the core of defense-in-depth are patch and configuration management. The goal is to ensure that operating-system and third-party vulnerabilities can't be exploited. This is among the most cost-effective security investments you can make.

» **Application whitelisting**—Surrounding patch and configuration management is application control in the form of whitelisting. It prevents any unknown or unwanted software—including known and unknown malware—from executing on your endpoints and servers. The key to effective whitelisting is built-in "intelligence" that lets you adapt to changing needs.

» **Data encryption**—Next comes data encryption, which protects the information that traverses and resides on your servers, networks and endpoints. One crucial aspect of data encryption is that it be applied to both hard drives and the removable devices and media that have proliferated in mobile environments.

» **Device control**—Effective device control enables you to centrally manage and enforce security policies around the use of removable devices such as USB drives and removable media such as DVDs. The goal is to prevent data loss and theft and to thwart malware intrusion.

Antivirus—The final layer of a complete defense-in-depth approach is antivirus (AV). Because AV is helpless against zero-day attacks, it's sometimes criticized as an inadequate security measure—and treated standalone, it is. But AV remains an important component of defense-in-depth.

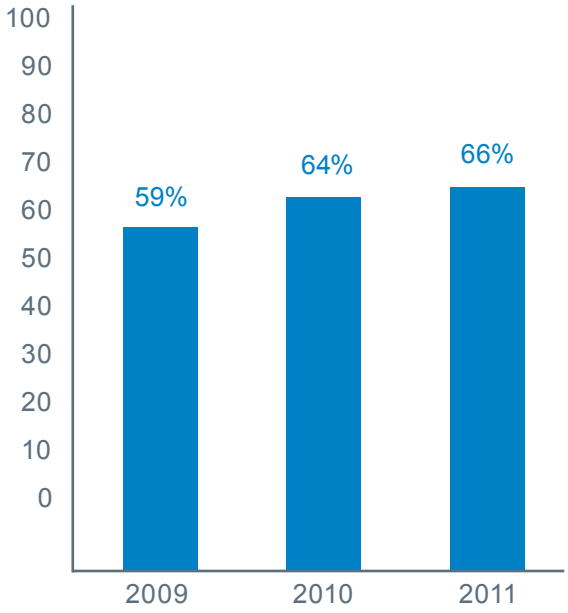
All layers of defense-in-depth must work in tandem to effectively reduce risk from the user, application and data security perspectives. With a single agent handling security at the endpoint, and a single console monitoring your security posture, you can achieve simplified management, lower total cost of ownership and stronger overall security.

In fact, patch and configuration management lie at the very heart of defense-in-depth. The key is to take a heterogeneous approach so you're covering all your operating systems and third-party applications. Bear in mind that many attacks target Web browsers and popular endpoint applications such as Adobe Acrobat and Apple QuickTime—not necessarily just the operating system.

Aberdeen Group recommends a four-step approach to patch management:

- **Assess**—Identify all assets, including platforms, operating systems, applications and network services. Scan these assets on a regular basis for vulnerabilities and patches.
- **Prioritize**—Maintain an inventory of assets and a database of remediation information. Prioritize the order of remediation in terms of risk, compliance and business value.
- **Remediate**—Model, stage and test remediation before deployment. Train administrators and users on vulnerability-management best practices.
- **Repeat**—Scan to verify the success of your last remediation. Report on it for audit and compliance. And continue to assess, prioritize and remediate on an ongoing basis. Note that this process is much more efficient if you deploy automated patch management.

Percentage of Respondent Answers That IT Network Security Is Not More Secure Or Are Unsure By Year



Source: Ponemon Institute, "2012 State of the Endpoint"

Despite ongoing investments in security, organizations don't perceive their IT networks to be more secure. In fact, perception of security is actually decreasing.

Last, don't forget configuration management. Gartner reports that 65 percent of endpoint risk can be attributed to misconfiguration. Concentrating on patching while ignoring configuration is like locking the door but not attaching it to the hinges. The solution is to centrally manage configurations for servers, workstations and laptops. Proactively enforce policy compliance and be vigilant about configuration drift. Stay on top of configuration drift by monitoring and reporting on noncompliance.

Continued »

Protect the Queen

Endpoints are the pawns on your IT chessboard. Defending them is necessary, but not sufficient to winning the game. The real crown jewel, the treasure you ultimately need to protect, is your data. This means endpoint security must not only fix vulnerabilities and thwart attacks, but also guard the information that traverses and resides on your endpoints.

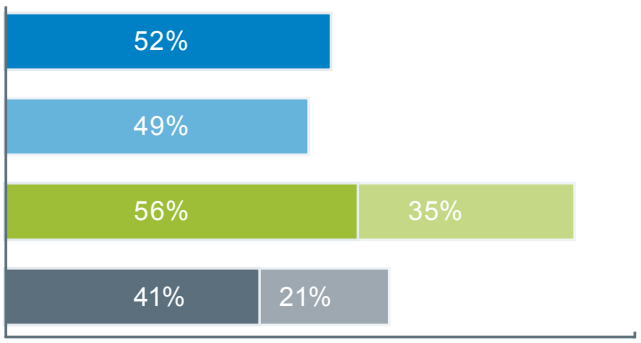
Data protection starts with full disk encryption (FDE). Without it, the simple loss or theft of a laptop—an unfortunately common occurrence—can completely expose your organization. Interestingly, research shows that while one-quarter of laptops are equipped with FDE, half of those laptops don't have FDE turned on. So something like 85 percent of all business laptops carry unencrypted data.

The solution is to enforce Federal Information Processing Standard (FIPS) 140-2 validated disk encryption, with encrypted swap and hibernation to protect data in all states. You can deploy user-transparent background encryption through single, pre-boot sign-on using Windows user ID and password. And, you can ease the administrative burden with network rollouts that requires no user involvement, as well as centralized monitoring and reporting.

Don't forget about removable media such as optical drives and memory sticks. Every day, those tiny devices are brought into your environment, along with any malicious payload the may be carrying. They're then shared among users, plugged into one laptop after another, and introduced to your network. At the end of the day, they often leave your premises, along with whatever corporate data has been transferred to them. Avoid blind spots: Encrypt all data placed on removable media.

FDE and device encryption don't need to be difficult. They don't have to involve full-blown data-loss prevention (DLP) with asset tagging and classification. Start by laying down a policy and procedure for basic—but global—protection of all corporate information.

Respondent Views On Security



Source: Ponemon Institute, "2012 State of the Endpoint"

While organizations overwhelmingly expect the use of cloud computing to increase, nearly half lack a cloud strategy or central management of cloud security.

Don't Bust the Trust

AV is based on a blacklisting model. Your AV vendor continually identifies new malware signatures and blocks them. That's an important, outermost layer of defense-in-depth. In fact, experts recommend deploying not one but two AV solutions. What one misses, the other might catch.

But even the best AV is useless against unknown threats. Your endpoints are vulnerable to "zero-day" attacks until your AV vendor identifies the threat and develops a fix. Bear in mind that AV vendors report finding millions of new pieces of malware every year—some as many as 60,000 new signatures per day.

What's needed is a trust-based model for endpoint applications, built on application whitelisting. While AV starts by letting in everything and then blocking what's bad, whitelisting starts by blocking everything and then letting in what's good.

Whitelisting is a mature, proven strategy, but it has always had the downside of locking down endpoints at the expense of flexibility. And when employees can't access and deploy the tools they need, their productivity can head south in a hurry.

The solution is "intelligent" whitelisting that essentially asks a series of simple questions before allowing an application to run. Is it a known bad? Is it a known good? Is it unwanted? Do I trust the vendor? Where did it come from? Is the user authorized to install it? And so on. This is actually a very lightweight approach that doesn't require a huge database of known bad and a long scanning delay. It gives you an automated means of making dynamic decisions about which applications should run—while delivering a rigorous layer to your endpoint security.

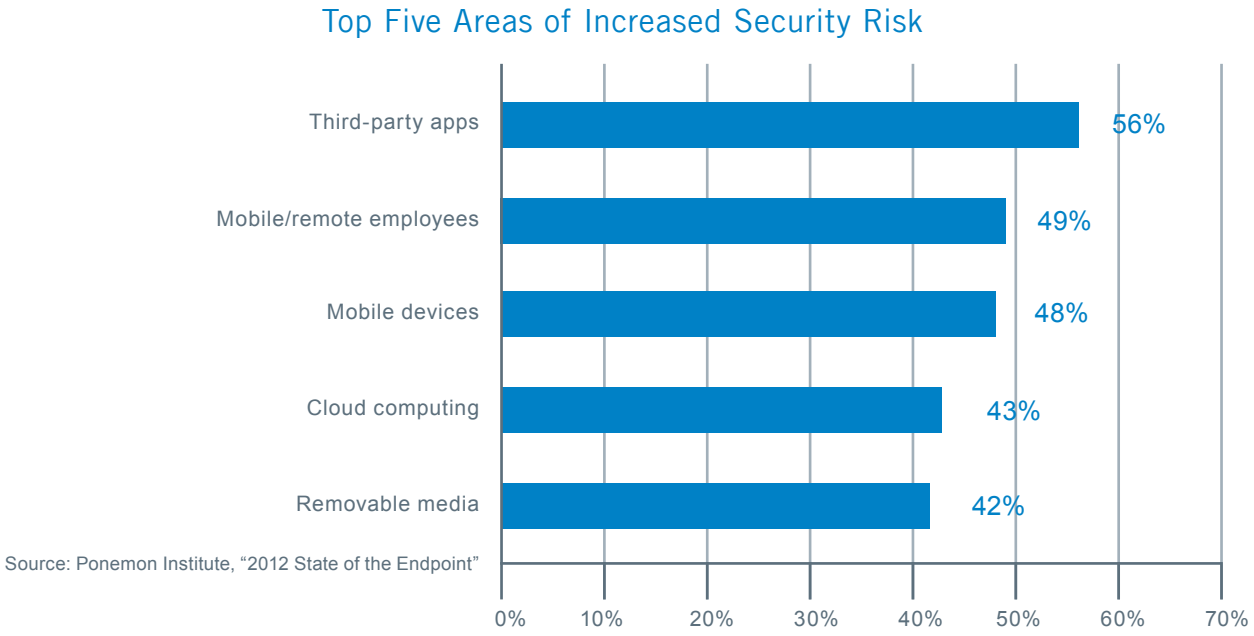
It's All About Your Operations

Finally, organizations need to begin approaching endpoint security from an operational perspective. Protection can't be an add-on to endpoints. Nor can it be treated in a standalone, siloed manner. Security and risk management must be part of daily endpoint management. And they should be a core component—and enabler—of operational performance.

To that end, defense-in-depth should include both security and operational aspects. Fragmented management, visibility and reporting will result in fragmented protection. It's interesting to note that while organizations cite third-party applications, mobile devices, removable media and cloud computing as their greatest risks, their investments in security don't always reflect that.[12] There's a disconnect between need and response.

The solution is an integrated security and management suite that provides a single security console and a unified security workflow. Many IT organizations have ended up with multiple security consoles to manage the various security technologies on their endpoints. An integrated suite delivers the

12. Ibid.



Security professionals cite issues around mobility and virtualization among the top-five security risks for 2012.

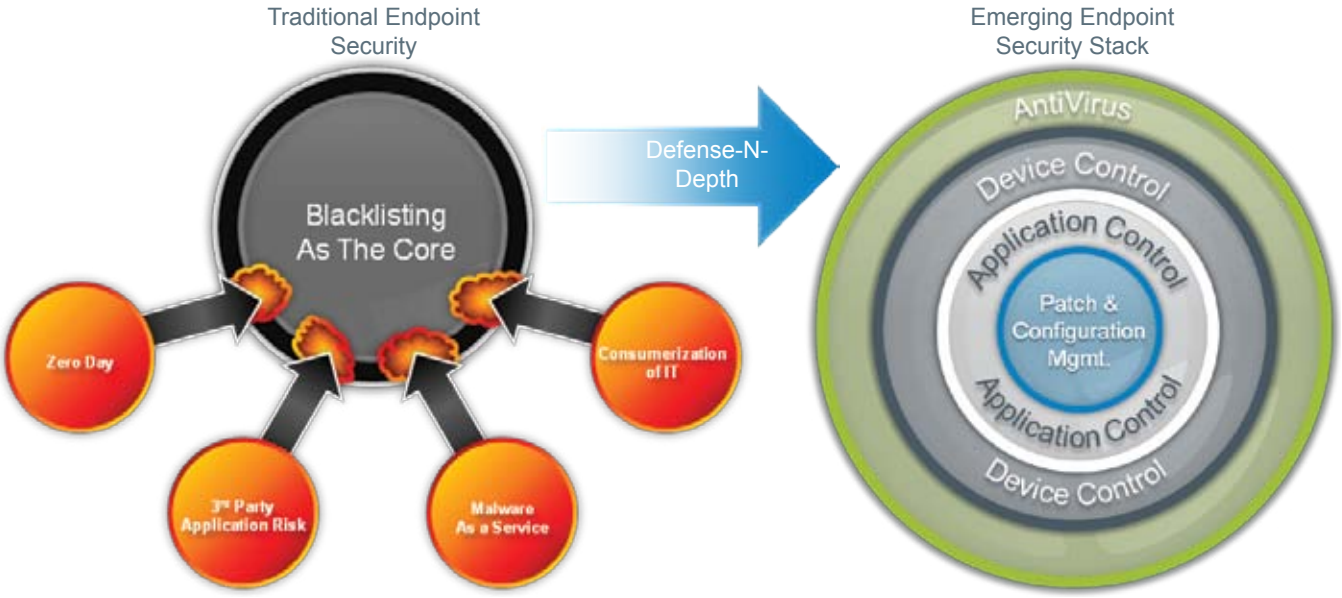
same functionality as individual applications, but it lets you control your environment from a single screen, without duplication of agents on every endpoint. It also gives you a single, accurate picture of your security posture. The result is better security, management and productivity, along with reduced total cost of ownership.

Ultimately, endpoint security should enable operational improvement. After all, you're not protecting data for the sake of protecting it. The reason you invest in endpoint security is to give users access to the information and tools they need, to improve the productivity and effectiveness of every employee while enabling your organization to compete and win in the marketplace.

Different Thinking, Different Results

By applying the concepts outlined in this white paper—thinking beyond threats, protecting your data, defining a trust-based model and approaching endpoint security from an operational perspective—you have the opportunity to change the outcomes of your security efforts and investments. Patch and configuration management, disk and device encryption, intelligent application whitelisting, and integrated, single-console security can deliver tangible benefits:

» **Reduced endpoint complexity**—Endpoints will continue to proliferate. The mechanisms for securing them should not. An integrated security suite makes not just protecting but also managing endpoints more efficient and more effective.



Traditional endpoint security places AV at the core—and leaves your organization vulnerable. A more effective approach is defense-in-depth, which layers protection to provide true security.

» **Lower cost**—A consolidated approach to patch management, whitelisting, device control and AV can reduce costs for blocking malware, remediating infections and managing endpoints. It can also avoid hidden costs for lost IT and user productivity.

» **Mitigated risk**—Effective endpoint security can reduce the risk of lawsuits and monetary damages. Encryption alone can give you "safe harbor" protection against reporting lost or stolen data.

» **Better and continuous compliance**—Centralized configuration management lets you monitor endpoints and ensure compliance. Single-console security ensures better visibility and a single source of truth.

» **Improved operational performance**—Ultimately, thinking different about endpoint security means more effective endpoint security. And that means better performance—for your IT operations, and for your entire enterprise.

One definition of insanity is doing the same thing over and over and expecting a different result—what many organizations have been doing with endpoint security. Another definition might be believing in silver bullets. The werewolves—the threats, vulnerabilities, attacks and risks—are still out there. But by thinking different, you have the chance to transform endpoint security into an opportunity for operational improvement and greater business success.

About Lumension Security, Inc.

Lumension Security, Inc., a global leader in endpoint management and security, develops, integrates and markets security software solutions that help businesses protect their vital information and manage critical risk across network and endpoint assets. Lumension enables more than 5,100 customers worldwide to achieve optimal security and IT success by delivering a proven and award-winning solution portfolio that includes Vulnerability Management, Endpoint Protection, Data Protection, Antivirus and Reporting and Compliance offerings. Lumension is known for providing world-class customer support and services 24x7, 365 days a year. Headquartered in Scottsdale, Arizona, Lumension has operations worldwide, including Virginia, Texas, Utah, Florida, Ireland, Luxembourg, the United Kingdom, Australia, and Singapore. Lumension: IT Secured. Success Optimized.™ More information can be found at www.lumension.com.

Lumension®
IT Secured. Success Optimized.™

Global Headquarters
8660 East Hartford Drive, Suite 300
Scottsdale, AZ 85255 USA
phone: +1.480.970.1025
fax: +1.480.970.6323