A Trend Micro White Paper I **July 2013**

Why You Need a Smart Protection Strategy

» Organizations of today need a smart protection strategy.
Smart. Simple. Security that fits.

Table of Contents

INTRODUCTION

With over one third of the world's population now on the Internet[1] and new mobile, social and cloud technologies being adopted at an unprecedented rate, connecting, communicating and collaborating on a global basis has never been easier or more prevalent.

It's a technology evolution and a behavioral revolution. For the first time ever, mobile devices are outselling PCs[2]; organizations are embracing cloud technology for their corporate data and business applications. The unprecedented amounts of information generated by this new-age connectivity is being analyzed by organizations to empower critical decision-making, capture new market opportunities, reduce customer churn and generate operational efficiencies. Information - its availability, access and control - is considered a core strategic asset. And organizations know the value in securing and protecting it.

This environment of supercharged user connectivity and global information access brings with it the challenge of a much more complex IT landscape with unique support requirements. Hackers and cyber-thieves are adept at their trade and are well aware of the impact they can have on compromising personal or customer data, credit card information, and intellectual property. One new threat is created every second of every day. Over 90% of organizations have active malware, yet more than half are not aware of these intrusions.[3]

IT, security, and risk professionals must continually weigh the benefits of providing users with the information they have come to expect against the risk of exposing sensitive information.

Security Then

Today's security scenario is different from 10 years ago, when users were issued a company PC connected solely to the organization's network with access to a finite set of applications. Then, data center servers were physically in the company data center and securing the corporate information involved ensuring the corporate systems had the latest antivirus pattern file to protect them from the most recent broad-based attack.

Security Now

Three clear trends are emerging in the current IT environment.

Consumerization: With mobile devices outselling PCs and cloud-based applications being used to share information, consumerization is a reality. Users no longer have a one-to-one relationship with their company-issued device or the corporate applications and network. There is a sense of distinct urgency amongst consumers and corporations alike to find a way to protect information flowing in this anytime, anywhere, any device world.

Cloud and Virtualization: The move away from data centers towards a more agile IT environment with virtualization and the use of cloud-based computing is occurring in every organization. Cost and operational efficiencies are realized as organizations increasingly choose to use the cloud to host business applications for finance, HR, CRM and others. Gartner predicts that 71% of server workloads will be virtualized by 2016.[4] Again, this borderless IT world has revealed new information security and protection challenges.

Cyber Threats: The evolution of cyber threats to targeted attacks is having a dramatic impact on business. These social, sophisticated and stealthy attacks are costing organizations millions of dollars. A Ponemon Institute survey reported the

occurrence of 1.8 successful attacks per week for large organizations.[5] It is increasingly difficult to provide consistent, trustworthy protection against targeted attacks, given the new complexities of consumerization, cloud and virtualization. Perimeter security is not sufficient to defend against advanced cyber threats.

Current Security Strategies

A number of organizations have tried to bolster their traditional information security perimeter with additional security technologies to solve specific point problems. This strategy often introduces another level of security issues. For example, Mobile Device Management, which addresses the influx of personal devices into the office, requires yet another location to manage and monitor security. It does not provide the centralized visibility necessary to ensure effective information protection. As well, this model consumes valuable resource time to manage the many disparate technologies.

A SMART PROTECTION STRATEGY

Organizations recognize that information is a strategic commodity that must be protected no matter where it is or on what device or platform it traverses. They want an effective security solution that is easy to manage and deploy at low cost with the necessary flexibility to address their dynamic business world.

> ***"In today's challenging IT environment, organizations need to take a step back and look at security in a strategic, holistic way. With trends like consumerization, cloud and virtualization, and today's sophisticated targeted attacks, organizations need to stay ahead of the curve. Trend Micro's smart protection approach outlines a security strategy organizations can use to ensure they are one step ahead."***
>
> **- Jon Oltsik, Senior Principal Analyst, Enterprise Strategy Group, Inc.**

What organizations are looking for is *smart, simple, security that fits* - a **Smart Protection Strategy**.

SMART PROTECTION FOR INFORMATION

Information needs to be protected at all times, regardless of location and device. Smart protection begins with layered content security.

Layered

Smart protection for information requires layered content security with multiple lines of defense to properly secure information.

First Line of Defense – the end-user

In the past, IT had an easier time dealing with employees and all their activities. Users sent email, surfed the web, and created documents locally and on file servers as well as USB drives, almost exclusively using Windows and Microsoft applications. Securing access to the user's machine or device was sufficient protection. The current environment is one where users have multiple devices and are using cloud and collaboration applications to share information. Home is an extension of work and vice versa. As users mix devices and applications for home and work, user behavior creates more risk. One in five users is now risking corporate information by using a personal Dropbox account[6]. It is all too apparent that security today must be focused on the user, not the device. Devices are merely locations where user data can reside, and need to be treated as such. By achieving visibility across user activities and device usage, organizations can ensure complete end user protection.

Second Line of Defense – network infrastructure

In the past, the corporate network was comprised of routers that separated the internal from the external network; switches were dumb and only passed traffic. A defined IP range was used to manage the network. A traditional security perimeter was sufficient. Today, routers are not the main network definition point. Networks are being extended through VPN gateways and employees may not even be using the corporate network, but public networks that are available in many locations. Additionally, cloud infrastructures such as Amazon Web Services, and cloud-based applications such as Salesforce have extended the boundaries of the corporate network. Security today needs to be context aware, able to analyze complex network traffic, and understand the *who*, *what*, and *where* of network activity. It must monitor for potential external attacks, as well as for internal traffic generated from end users and servers. As well, it must be able to analyze content in real time and determine if it is legitimate or malicious.

Third Line of Defense – servers

Previously, data center servers were used to store and exchange data, such as a file server, mail server, document server or database server. They were static, and stayed inside the office or the physical data center, protected by perimeter network security. Virus protection to prevent infected files from being shared and transmitted through these servers was sufficient.

Now, servers are used much more in computing-related tasks, performing search and sorting, and correlating of various types of data. They analyze and report on business performance and operations providing critical insight vital to corporate strategy. A compromised server could mean a loss of millions of dollars. These servers are

dynamic - virtualized to move between different network segments and data centers. Instead of sitting inside the office or data center, they are sitting at the network edge, external-facing to provide web-based access to partners and customers. Increasingly, they are being relocated to the public cloud, such as Amazon, to address economies of scale.

Today's organizations need smart server protection that works across all servers: physical, virtual, private and public cloud servers alike. They need a security policy that can dynamically follow the servers, protect unpatched servers from vulnerabilities, conduct real-time monitoring and provide instant protection.

Interconnected

It's not enough to have standalone layers of protection. Each layer must be interconnected and work together. If an attack or compromise is detected at the network layer, all other layers need to be instantly aware of this new threat in order to have comprehensive protection.

> ***"Trend Micro is moving in the right direction, by consolidating products and suites. Each release builds in more, and the big picture is coming together. Trend Micro is bringing together all the right products into consolidated, cost-effective security solutions."***
>
> **- Ty Smallwood, Information Services Security Officer, Medical Center of Central Georgia**

Real-Time

Smart protection should also be in real-time, with security updates provided via the cloud instead of traditional desktop pattern updates. Updating protection used to be infrequent and could be managed by periodically updating pattern files and "Patch Tuesdays" to address vulnerabilities. This model is not enough to address the current and constant proliferation of threats to information. Organizations need big data techniques for analyzing huge amounts of global threat and vulnerability data and providing proactive security.

Transparent

Effective security should be as transparent as possible to users in order to minimize workflow interruption or possible performance issues. Similarly, administrators need to have full visibility across their organizations' information, from end user devices, all the way to their cloud and data center systems. This is important for security professionals to get a holistic view of their organization's information, and build and monitor policies from one place.

SIMPLE YET FLEXIBLE TO DEPLOY AND MANAGE

A smart protection strategy requires solutions that are simple yet flexible to deploy and manage. The disparate point solutions and perimeter security systems of the past introduce risk with their management challenges, maintenance expenses and limited visibility. Today's organizations need to simplify operations - with streamlined solutions that address the reality of the business world - doing more with ever-shrinking budgets and fewer resources.

Centralized

Centralized visibility and control of security status across multiple layers is necessary for easy, risk-free management. Administrators need to have a view of the overall organization's security health, and be alerted when key metrics move beyond an acceptable range. This reduces the time to resolve security issues in the organization and mitigates risk.

Automated

Introducing new virtual machines or cloud instances to the corporate data center is faster and easier than ever before. Constantly changing data center servers need to be automatically detected and protected on the corporate network, without IT intervention or even prior knowledge. This saves time, money, and allows the organization's security to change with the same fluidity as its data center.

Lightweight

Security that is lightweight - fast and easy to deploy and manage, with minimal impact on network and server efficiency - ultimately reduces the cost of ownership. Security that was built to secure physical systems may adversely affect the performance of virtual or cloud systems. Organizations need a security solution that is optimized to work efficiently and effectively within the environment that it secures, and is as lightweight as possible in each scenario.

> ***"Simplicity has been another appreciated result of the move to Trend Micro. We haven't had to do a lot since deploying Trend Micro security—the products just seem to run and work…we save time with Trend Micro for sure."***
>
> **- Bruce Jamieson, Network Systems Manager, A&W Food Services**

Flexible

Organizations also need a security solution with the flexibility to suit their unique requirements. Whether this means on-premise technology, or "as-a-service" hosted solutions, it must be delivered, packaged and priced to suit the organization's specific environment.

SECURITY THAT FITS AN EVOLVING ECOSYSTEM

Finally, a smart protection strategy requires security that fits an evolving IT ecosystem.

Open

Security solutions must be open to support evolving operating systems and platforms. Users work environments used to be dominated by Microsoft Windows and Office applications, hard-drive or network file storage and LAN-based or dial-up access. User environments now include a myriad of additional operating systems such as Apple iOS and Android, new social apps such as Facebook and LinkedIn, cloud-based storage options such as iCloud, as well as alternate network access points in the office, airport, home or the nearest coffee shop.

Data centers, previously on-site and comprised of physical Microsoft, Unix, and Linux servers, now involve virtualized servers, hosted in a private or public cloud.

Optimized

Solutions should not only be open to new technologies, but also be optimized to work seamlessly with complementary technologies in the corporate environment, across all end user activities, data center and cloud, and network. The ideal security solution should work efficiently within it.

> ***"We are definitely watching cloud computing as it evolves, public cloud services are still pretty new, but Trend Micro's in-the-cloud security has already introduced us to private clouds. That's our first step into the cloud, and we feel that Trend Micro solutions will ease the way as we introduce more cloud services to our employees and constituents."***
>
> **- Bryon Horn, IT Manager, City of Fresno**

Focused

Security needs to be independent to the application environment it works within, and agnostic to the technology it secures. Deep industry-specific functionality is best addressed with purpose-built technologies; an organization's security requirements should receive the same focused attention. The security vendor of choice is one that is solely focused and dedicated to security – not distracted by upselling adjacent technologies.

Innovative

IT security today sits in a rapidly evolving landscape involving the consumerization of IT, cloud & virtualization technologies and sophisticated cyber threats**.** Organizations need a security partner that provides solutions that address the issues of the day and that is constantly innovating to address tomorrow's environments and threats.

CONCLUSION

Change is constant for IT, security and risk professionals. They are exposed to multiple new and emerging technologies; they know the statistics and are constantly challenged with the fast pace of today's IT environment.

Gone are the days of perimeter security and Patch Tuesdays. Technology is redefining everything; the way work is conducted, the management of data center servers and the corporate network. Strong and growing trends such as the consumerization of IT, cloud & virtualization technologies and targeted, sophisticated cyber threats have introduced real challenges to the task of information security.

Organizations of today need a smart protection strategy. Organizations need smart, simple, security that fits.

REFERENCES

[1] Internet World Stats, Dec 2012

[2] Asymco.com, June 2012

[3] Trend Micro 2012 survey

[4] Gartner, Forecast Analysis: Data Center, May 2012

[5] 2012 Ponemon Study on costs of Cybercrime

[6] Global survey of 1300 enterprise customers; "Shadow IT in the Enterprise", Nasuni, 2012

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

TREND MICRO INC.
U.S. toll free: +1 800.228.5651
phone: +1 408.257.1500
fax: +1408.257.2003