EXTENDING TRADITIONAL SECURITY TO VDI
ARE YOUR VIRTUALIZATION EFFORTS HURTING YOUR SECURITY?
Deploying Physical Endpoint Security to Virtual Desktops

Enterprises have adopted virtual desktop infrastructure (VDI) due to benefits such as increasing overall utilization, reducing management costs, and enhancing security.¹ Trend Micro surveyed enterprises worldwide in 2011 and found that the average VDI adoption rate was around 52 percent (see Figure 1).²

VDI also supports consumerization and bring-your-own-device (BYOD) strategies, as endpoint users can access applications and data on their desktops using any mobile device, resulting in better productivity.

The pressure from line-of-business (LOB) managers for IT departments to immediately deploy VDI forces the latter to treat security as a second priority. A study reported that cultural resistance among IT organizations, increased bandwidth requirements, and inability to work offline were some of the challenges related to VDI deployment.³ When push comes to shove, however, IT groups respond to the pressure by extending traditional security to virtual environments instead of evaluating security specifically designed for VDI to address the security and infrastructure needs of a virtual environment.

What force IT departments to migrate physical security to virtual desktops?

- **Immediate need of the mobile workforce:** Demand from the mobile workforce influences IT departments to give in to rushed VDI deployments. Aside from not modifying backup and software policies to avoid resource allocation issues, IT departments may also employ the same security policies and procedures to both physical and virtualized desktops or, worse, consider security too late in the deployment stage.

- **Unavoidable management of mixed environments:** Most enterprises are in the stage of mixing both physical and virtual endpoints in production. According to the previously cited Trend Micro study, 52 percent of companies worldwide have deployed or are piloting VDI. As such, IT departments end up using traditional endpoint security for virtual desktops as well.

- **Overall project’s financial intent:** Certain organizations’ place operation expense reduction as the end goal of their virtualization efforts. Instead of purchasing virtual-aware security software and/or tools, IT departments stick with traditional security to avoid perceived incremental costs.

*Extending traditional security to virtualized environments opens up networks to a plethora of security challenges and threats that can lead to business disruption or, worse, data leakage.*

---

Security Risks of Extending Traditional Security

One of the core benefits of implementing VDI is the ability to quickly generate a virtual desktop image instead of installing each instance from scratch. If IT departments simply extend traditional security to virtual desktops, duplicate images will inevitably update their security software or initiate full system scans at the same time, leading to a bandwidth problem known as “resource contention” or a “security storm.”

Common but improper work-arounds include randomizing or disabling antivirus scanning and updating. When IT administrators disable security functions at this level, they are, in effect, entrusting desktop security to network firewalls and intrusion detection systems (IDSs).

In such a situation, the unprecedented speed by which cybercriminals create malware—3.5 new threats every second—render virtual desktops vulnerable to attacks.

Unlike virtualized servers, virtual desktops comprise a broader attack surface because each instance is a potential entry point. User behaviors such as indiscriminately downloading programs and documents, surfing the Web, and clicking links do not help. Without protection for even a small amount of time, VM images can inadvertently introduce threats to corporate networks.

Zero-Day Exploits and the “Zero-Day Effect”

Zero-day exploits are deployed in the wild by cybercriminals or used in targeted attacks to exploit unpatched or unknown software vulnerabilities. Resource contention work-arounds that turn off protection or delay security force IT administrators to effectively face the same zero-day risks even if patches are already available and despite deploying security products.

Widely used applications from Microsoft, Adobe, and even Apple have all been found to carry software vulnerabilities that are crucial to cybercrime attacks because these allow automatic command execution.4

Customized Highly Targeted Attacks

Advanced persistent threats (APTs) target companies and organizations in order to steal confidential information. These campaigns frequently begin with social engineering attacks as mundane as sending out customized emails with exploit attachments.

After monitoring APTs for one month, Trend Micro found that the most exploited Microsoft Office software was Microsoft Word (see Figure 2).5 Furthermore, both relatively new (e.g., CVE-2012-0158)6 and old (e.g., CVE-2010-3333)7 vulnerabilities have been leveraged.

Exploits for vulnerabilities in Adobe Acrobat Reader and Flash Player have also been used in various APT campaigns such as LURID,8 SYKIPOT,9 and IXESHE.10

---

5 http://blog.trendmicro.com/snapshot-of-exploit-documents-for-april-2012/
6 http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0158
7 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3333
8 http://blog.trendmicro.com/trend-micro-exposes-lurid-apt/
9 http://blog.trendmicro.com/the-sykipot-campaign/
Responding to VDI Security Challenges with Agentless Security and Vulnerability Shielding

For enterprises to realize the benefits VDI offers, IT administrators must use security tools or implement policies that can respond to the unique security challenges and threats that exist in virtualized environments.

Enterprises that have begun virtualizing servers and foresee virtualization to be a core IT strategy should already consider extending server virtualization strategies to VDI. Specifically, VDI-aware security software that integrates well with hypervisors allows IT administrators to free up the space in each virtual desktop previously taken up by security agents.

Trend Micro™ Deep Security™, for instance, employs agentless technology through a lightweight driver in each virtual desktop used by the virtualization platform to orchestrate staggered security scans and updates instead of requiring a separate traditional security agent in each virtual desktop. This protects virtual desktops in the most optimal manner against the risks illustrated in the previous section while preserving virtual desktop resources. This agentless technology optimizes performance and increases VM density. Moreover, it does not need a traditional security agent in each VM, as it leverages the driver used in virtualization.

Furthermore, enterprises that use VM-aware security software such as Deep Security can also take advantage of vulnerability shielding, aka “virtual patching,” to address known patch management issues and, more specifically, the threat zero-days attacks pose.11 Plugging software holes with vulnerability shields at the network level enables enterprises to efficiently and proactively protect their networks even before a patch is developed by the affected software’s vendor.


Only extend traditional security to VDI if your security software can:

- Identify whether the agent is running on physical or virtual endpoints (i.e., a capability called “virtualization awareness”)
- Serialize scans and updates to prevent resource contention problems
TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TRENDDLABS™

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.

©2012 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.