

# Trend Micro™ Vulnerability Shielding

## The Patch Management Challenge

Today's enterprises are bombarded by sophisticated exploits such as Duqu and Conflicker which target vulnerabilities in the systems that enterprises rely on most. Countless software vulnerabilities leave the door open to data-stealing malware and other attacks. And IT teams can't keep up—it's virtually impossible to download, test, and deploy patches for all critical vulnerabilities before they are exploited. At the same time, emergency patching causes unacceptable downtime, overhead, and costs; virtualization creates additional operational challenges; PCI regulations mandate patching within 30 days; and zero-day attacks strike with increasing frequency. Given these challenges, there has never been a more urgent need for a virtual patching solution that complements existing patch management processes by shielding known and unknown vulnerabilities.

## Where are you most vulnerable?

Enterprises need to shield known and unknown vulnerabilities in a broad range of critical applications and systems that are being targeted by cybercriminals.

**Enterprise Applications:** Each year thousands of critical software flaw vulnerabilities are reported in operating systems, databases, servers, and other applications. Patching these vulnerabilities can be disruptive and time consuming, requiring systems to be rebooted and impacting service level agreements. Even when a patch is available, it can take weeks or even months before the patch can be fully deployed.

**Legacy Web Applications:** The majority of records that are breached are the result of SQL Injection attacks on web applications. Web applications are particularly vulnerable because they're inherently open and accessible to attackers. In addition, content and functionality is increasingly complex and programmers are often untrained in secure software development practices. Perimeter security won't shield these systems and it can be difficult to locate and assign the custom development resources necessary to fix the code.

**Unsupported Operating Systems and Applications:** Patches are no longer developed or issued for older operating systems and applications that have reached their end-of-life, such as Oracle 10.1 and Solaris 8. Often, the time and cost required to migrate to a newer version is simply too high, and organizations need a more immediate, cost-effective solution. When support for Windows 2000 ended July 2010, virtual patching became the only cost-effective way to ensure continued protection for these and other unsupported systems.

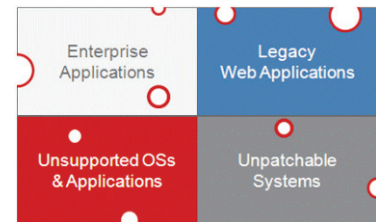
**Unpatchable Systems:** Systems such as point-of-sale devices, kiosks and medical or other embedded devices are often considered unpatchable. Often, low-bandwidth connections with remote locations make deploying large patches prohibitively time consuming or expensive. At other times, regulations or service level agreement uptime requirements may preclude systems from being patched.

## Key Drivers

- Microsoft Tuesday
- PCI 6.1: Security Patches
- Oracle patching
- Virtualization

“ Only 27% rate their patch management process as being effective.”

## Information Week





## Trend Micro Deep Security for Vulnerability Shielding

Trend Micro Deep Security shields vulnerabilities in critical systems until a patch is available and deployed or in place of a future patch that may never materialize. Either way, you get a timely, cost-effective complement to traditional patching processes that can significantly lower costs, reduce disruptions, and give you greater control over the scheduling of patches. Designed to provide comprehensive protection for all servers—physical, virtual, and cloud—as well as some endpoints, Deep Security can be deployed as an agent on a physical or virtual machine, or as a virtual appliance on a VMware ESX server to protect guest VMs.

### KEY FEATURES & BENEFITS

- **Intrusion Detection and Prevention (IDS/IPS)** rules shield known vulnerabilities from being exploited. Deep Security includes out-of-the-box vulnerability protection for over 100 applications, including database, web, email and FTP servers. In addition, IDS/IPS rules also provide zero-day protection for known vulnerabilities that have not been issued a patch, and unknown vulnerabilities.
- **Recommendation scanning** streamlines security update management by automatically scanning systems to recommend which rules need to be deployed to protect a given system. Deep Security scans the system to identify which IDS/IPS rules need to be deployed to optimize protection—based on the OS version, service pack, patch level, and installed applications. Deep Security also automatically recommends when rules can be removed to minimize resource impact.
- **Security updates** from a dedicated team of security experts continuously monitor multiple sources of vulnerability disclosure information to identify and correlate new relevant threats and vulnerabilities. Trend Micro also receives vulnerability information from Microsoft in advance of their monthly security bulletins, making it possible to anticipate emerging threats and provide more timely protection.
- **Web application protection rules** defend against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities, shielding these vulnerabilities until code fixes are completed. Security rules enforce protocol conformance and use heuristic analysis to identify malicious activity.
- **Enterprise-grade, bi-directional, and stateful firewall** allows communications over ports and protocols necessary for correct server operation, and blocks all other ports and protocols. This reduces the risk of unauthorized access to the server.
- **Protection for physical, virtualized and cloud computing environments** ensures that vulnerabilities are shielded, no matter how the hosts are deployed. In addition to providing guest-based protection, Deep Security leverages VMware APIs to provide virtualization-aware protection, maximizing deployment flexibility.

## Choose the Right Solution for Vulnerability Shielding

With over 20 years of security experience, Trend Micro is a leader providing virtual patching solutions. With security that fits your enterprise, we help you maximize protection while minimizing complexity.

For more information, please visit [www.trendmicro.com/virtualpatching](http://www.trendmicro.com/virtualpatching)

### Spotlight on Conficker

Deep Security customers were protected against attacks that targeted critical vulnerabilities discovered in Microsoft Windows 2000, Windows XP, and Windows Server 2003 (MS08-067) the same day the vulnerability was announced, and weeks before the first Conficker exploits.

### Vulnerability Shielding for Desktops

Trend Micro Intrusion Defense Firewall shields vulnerabilities in Windows desktops and laptops, and seamlessly plugs into the Trend Micro OfficeScan console for unified management.

“Deep Security protects our healthcare system by proactively shielding vulnerabilities in Electronic Health Record web applications and operating systems from targeted attacks until patches can be deployed.”

**Bill Gillis**

Beth Israel Deaconess  
Medical Center

