Virtual Patching: Lower Security Risks and Costs

Trend Micro Deep Security

Hundreds of software vulnerabilities are exposed each month, and timely patching is expensive, prone to error and often impossible. Trend Micro virtual patching solutions deliver immediate protection while eliminating the operational pains of emergency patching, frequent patch cycles, and costly system downtime.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Patch Management Today</td>
<td>3</td>
</tr>
<tr>
<td>System Vulnerabilities Are Everywhere</td>
<td>5</td>
</tr>
<tr>
<td>A New Approach: Virtual Patching</td>
<td>8</td>
</tr>
<tr>
<td>How Deep Security Works</td>
<td>9</td>
</tr>
<tr>
<td>Why Trend Micro</td>
<td>11</td>
</tr>
<tr>
<td>Conclusion</td>
<td>12</td>
</tr>
<tr>
<td>References</td>
<td>13</td>
</tr>
</tbody>
</table>
INTRODUCTION

Patch management for vulnerability remediation can be a painful exercise for IT departments. If it were easy, patch release and deployment would be predictable events and vulnerabilities would be addressed within acceptable timeframes. Instead, emergency patches persist, IT staffs scramble to deploy them, and security officers brace themselves for the worst case—a data breach or unplanned system downtime. Beyond emergency patches, predictable events such as planning to maintain security for out-of-support (OOS) enterprise software pose an added challenge. For such systems, ongoing security patches cease, forcing IT operations to choose between expensive support contracts or accept the risk of exploits targeted at OOS systems with unpatchable vulnerabilities. And some systems are inherently difficult to patch such as point-of-sale devices, kiosks, and medical or other embedded devices. Yet these devices may be critical to the business.

This white paper reviews enterprise challenges with security patch management including risks to various areas of IT—security, compliance, operations, and budgets. It discusses how traditional approaches to remediating vulnerable systems can create new problems and provides a new model that keeps pace with the ever-increasing number of attack vectors.

Trend Micro Deep Security offers "virtual patching," which shields vulnerabilities in critical systems until an actual patch is available and deployed—or as permanent protection in the case of OOS or other unpatchable systems. Deep Security’s virtual patching lowers costs by preventing the need for emergency patching, frequent patch cycles, and system downtime as well as reducing the risk of breach disclosure expenses. It even avoids expensive support contracts for OOS systems by eliminating the need for customized patches and helping to extend the life of legacy systems and applications. Deep Security’s virtual patching mitigates risk across network topologies, platforms, and applications—including commonly targeted Web applications—and enables enterprises to maintain regulatory compliance, including necessary logging and reporting capabilities. Designed to provide comprehensive protection for all servers—physical, virtual, and cloud—as well as endpoints, Deep Security gives you 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.

PATCH MANAGEMENT TODAY

The primary goal of software patching is to keep operating systems and applications working smoothly and securely. For widely used systems such as Microsoft SQL Server or Windows 7, the process is relatively predictable, but life gets significantly more complex when older applications, custom development, and out-of-support operating systems enter the picture. Add budget constraints that restrict migrating away from OOS platforms or remediating supported platforms and a hacker community eager to exploit unpatched system vulnerabilities, and you have a situation ripe for disaster, or at least a nasty note from auditors.
COMPLEXITIES OF THE TYPICAL PATCH DEPLOYMENT PROCESS
The mere availability of a patch does not give IT a green light to deploy it across all business systems. Even the very predictable “Microsoft Patch Tuesday” releases are scrutinized every month by IT organizations to ensure that the risks are actually addressed without breaking existing applications. Typically, patch management follows a structured process that includes:

- Obtain the patch from a trusted party and check the integrity of both the patch and the patch source
- Test the patch to ensure the vulnerability is remediated and the patch will not break other applications
- Notify affected parties of any necessary scheduled downtime to apply the patch
- Deploy the patch to all affected systems
- Recheck operational efficiency of patched systems and remediate as required

The complexity and frequent time-critical nature of even predictable patching before a vulnerability is actually exploited is a significant burden on IT operations and consigns them to a state of reactivity and continuous catch-up. Against this backdrop, it is hardly surprising that almost one third of security survey respondents said their organization devotes a great deal of time and staff resources to patch management—the highest response across all IT security tasks listed. Yet only 22% found their patch management to be very effective. With the complexity of patch management, corners may be cut, risks may persist, and proactive IT projects may languish.

KNOWING THE RISKS: RISK WINDOW DURING THE TIME FROM VULNERABILITY DISCOVERY TO PATCH RELEASE PATCH DEPLOYMENT
The gap between discovering the vulnerability (or being notified of a critical security patch) and when appropriate patches are deployed to all production systems can extend for weeks or even months. The challenge is not getting easier over time, with the National Vulnerability Database reporting over 4,150 software vulnerabilities in 2011. The time it takes to test patches for these vulnerabilities and role them out to all applicable systems creates an extended risk window.

And security concerns over delays in patching systems are well founded. In 2011, malware was responsible for 95% of all data records stolen, and 94% of data breaches involved the confidentiality and integrity of servers. Attackers can repeatedly leverage the same system vulnerability and continue to get results as systems remain unpatched or unpatchable. Buying time to manage the window between when a vulnerability is discovered and a patch can be deployed, while still remaining secure, is a critical element in maintaining an adequate security posture.

REGULATORY COMPLIANCE
Regulatory compliance also impacts patch management. In addition to the specific timeliness requirements of the PCI regulations, periodic audits to ensure up-to-date patches on critical systems—ones that store or process regulated data—must be undertaken to comply with internal IT governance as well as many external data protection industry regulations.
REGULATORY COMPLIANCE
Beyond the predictable nature of “Patch Tuesday”—and its constant companion “Exploit Wednesday”—as well as regulatory compliance requirements, multiple additional factors must be borne in mind when implementing patch management programs:

- Emergency patches that must be applied immediately, with consequent downtime, overhead, and cost
- The operational challenge of patching virtualized systems and the rapid growth in the use of such systems
- Increasing frequency of zero-day attacks and attacks targeted at specific industries and platforms
- Ongoing consolidation of vendors and consequent disruption of patch development and distribution
- Growing use of “unpatchable” POS systems, ATMs, and embedded systems as a vector for malware delivery

SYSTEM VULNERABILITIES ARE EVERYWHERE

Patch management is both a solution and a source of frustration, so why do IT security policies continue to mandate timely and accurate patching of vulnerable systems? The answer is that, short of rewriting the original source code, patches are the most targeted way in which to remediate software vulnerabilities in specific operating systems and applications. However, there are also systems that are unpatchable either because they are OOS or non-typical systems. Whether patchable or unpatchable, 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
In 2011, 1,821 critical software flaw vulnerabilities (i.e., Common Vulnerabilities & Exposures (“CVE”; Score 7-10, high severity6) were reported in operating systems, databases, servers, and other applications, according to the US National Institute of Standards and Technology (NIST)7. This equals seven critical vulnerabilities per business day. 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 because of internal testing and the time required to deploy the patch across all applicable endpoints.

LEGACY WEB APPLICATIONS
Some vulnerabilities are caused by misconfigured systems, while others may be due to coding flaws in custom-built and legacy web applications. In the former case, manual intervention may be required; in the latter case, developers with the necessary subject matter expertise may not be available to fix the application, as was the case with Y2K and COBOL.

In large organizations (1000 employees and greater), web applications serve as a popular threat vector responsible for 54% of breaches in 20118. Web applications are particularly vulnerable
because they are inherently open and accessible to attackers. In addition, content and functionality are increasingly complex and programmers are often untrained in secure software development practices. Perimeter security will not shield these systems and it can be difficult to locate and assign the custom development resources necessary to fix the code.

**UNPATCHABLE SYSTEMS**

Unattended or embedded systems such as point-of-sale systems, kiosks and medical devices are often considered unpatchable despite significant levels of vulnerability. 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 such systems from being patched.

**UNSUPPORTED OPERATING SYSTEMS AND APPLICATIONS**

Clearly no software application will be supported in perpetuity; every IT manager has at some time received an End of Life (EOL) announcement, which specifies a date after which a particular program will be out-of-support (OOS) and no further patches will be issued except by special (and costly) individual agreements. 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.

**KNOWING THE RISKS: VULNERABILITIES ON UNSUPPORTED SYSTEMS**

Even with an organized end-of-life process, many organizations appear to be caught off guard or unprepared for the inevitability of OOS software. And those who do research the options find that those options often bring their own share of challenges. Ignoring the risks associated with the continued use of unpatched OOS systems is not wise for many reasons, not the least of which is that newer, supported platforms often share code with earlier releases. A new exploit on a supported platform can also affect an older OOS system that shares its code.

An OOS system that is still frequently used by organizations is Microsoft Windows 2000, which was designated OOS on July 13, 2010. Even a few Windows 2000 installations left “live” on a network can be exploited by savvy hackers who see Windows 2000 as an easy entry point long after Windows XP patches have been deployed. If operating system migration has not yet been completed, enterprises with these systems are at risk. As soon as the next Windows XP vulnerability is announced and a patch is released, the clock will start ticking until an exploit targets this same vulnerability on Windows 2000. And once the attacks start, they are unlikely to stop because there will be nothing there to stop them.

**The Perfect Storm - Windows 2000**

- Vulnerability announced for Windows XP
- Hackers start writing exploits based on this XP vulnerability
- Some exploits are successful before XP patch release
- Patched XP systems are protected, 2000 systems continue to be vulnerable and attacked indefinitely

**Undesirable Options for Addressing Out of Support (OOS) Systems**

- Ignoring the associated risks
- Eliminating these systems
- Purchasing custom support contracts
- Isolating them on the network
- Hardening systems
- Application whitelisting
KNOWING THE RISKS: VULNERABILITIES ON UNSUPPORTED SYSTEMS (CONT.)

UNDESIRABLE APPROACHES TO MANAGING THE RISKS

1. Custom Support Agreements for OOS Systems (continued)
   In the name of “customer service,” vendors may offer custom and extended support agreements for OOS software which entitle customers to emergency security patches. However, such agreements are frequently cost-prohibitive for all but the largest organizations; Windows 2000 Custom Support Agreements started at $50,000 per quarter\(^9\) in 2010, and these agreements tend to get more expensive over time as the operating system gets older. For example, OOS contracts for Windows NT v4 exceeded $1 million by 2009\(^10\). Not unsurprisingly, many enterprises find such costs to be unpalatable, driving them to find alternative methods to mitigate the risk or, in some cases, accept the risk of a potential compromise. Acquisitions bring their own complexity to the extended support contract. For example, when Oracle acquired Sun, Sun’s customers were required to renew their support contracts with Oracle to receive patches; a similar situation occurred when Oracle acquired middleware vendor BEA Systems.

2. Isolation
   One approach to managing risks associated with OOS software might be to make such systems hard for hackers to reach. Isolating these systems on separate networks or VLANs adds a layer of difficulty that hackers may decide is simply too much trouble. However, network isolation may not be practical for essential business systems, and therein lies the conundrum. Making OOS systems hard to reach adds a layer of security but may also prevent them from being used effectively, obviating the reason for retaining them in the first place.

3. System Hardening
   Hardening OOS systems (e.g., removing unnecessary services, user accounts) may appear to be an acceptable way to minimize risk. However, authorized users will still need access to these systems, so restricting user accounts alone may not be practical for business reasons. Hardening through removal of unnecessary services and ports is not trivial when business applications are designed to run on general-purpose operating systems with a variety of application services and ports (e.g. RPC ports, web services), and may break the application. Restricting application ports may also render stateful packet-filtering firewalls ineffective, since many applications dynamically allocate ports as needed.

4. Application Whitelisting
   Whitelisting OOS applications could potentially enable IT to be alerted if malware has affected and made changes to such an application, but does not remove the problem of dealing with such an event when identified. Using whitelisting to instead permit only the use of explicitly-authorized software on an OOS system is conceptually sound, but in practice would likely prove unmanageable; IT would need to update signatures for authorized executables and upload them into the whitelisting system every time one of those executables was patched.

While enterprises should plan for the eventual elimination of OOS systems, such plans are frequently dogged by budgetary constraints or technical limitations. Businesses need to be able to migrate away from OOS systems on their schedule while, in the meantime, effectively and inexpensively maintaining the security of these OOS systems.
A NEW APPROACH: VIRTUAL PATCHING

The dual challenge of vulnerability risks and patch management is clearly not being adequately met by traditional solutions. Trend Micro’s answer to the unwinnable challenge of patching unpatchable systems is Deep Security Virtual Patching, a non-disruptive “vulnerability shield” that protects systems during the risk window—and beyond.

DEEP SECURITY: A COST-EFFECTIVE COMPLEMENT TO PATCH MANAGEMENT

Trend Micro Deep Security shields vulnerabilities in critical systems until a patch is available and deployed, in place of a future patch that may never materialize, or to protect systems that are unpatchable. In each instance, enterprises get a timely, cost-effective complement to traditional patching processes that can significantly lower costs, reduce disruptions, and provide greater control over the scheduling of patches. Designed to provide comprehensive protection for all servers—physical, virtual, and cloud—as well as 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 virtual machines using agentless security. Deep Security coordinates several elements of the solution to provide virtual patching protection.

1. Intrusion Detection and Prevention (IDS / IPS)

If a hacker locates a vulnerability, he may try to exploit it. Deep Security Intrusion Detection and Prevention (IDS/IPS) rules shield against known vulnerabilities—for example those disclosed on Microsoft Patch Tuesday—from being exploited. The Deep Packet Inspection (DPI) engine leverages proprietary rules that protects network traffic in layers 2-7. These rules are used to protect unpatched, network-facing system resources and enterprise applications. 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 using smart rules that apply behavior analysis and self learning to block new threats.

Vulnerability shielding leverages the Deep Security IDS/IPS rules and requires updating when new vulnerabilities are announced. However, rather than relying on a new software patch for protection, the existing Deep Security engine is already at work, checking for updates to IDS/IPS rules and automatically applying them to applicable systems.

2. Recommendation Scanning

Recommendation scanning streamlines security update management by automatically recommending 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. In addition, as the server...
environment changes and patches are deployed, Deep Security automatically recommends which rules can be removed to minimize resource utilization.

3. **Security Updates**

Security updates from a dedicated team of security experts ensure the latest protection by continuously monitoring multiple sources of vulnerability disclosure information to identify and correlate new relevant threats and vulnerabilities. This includes more than 100 sources such as SANS, CERT, Bugtraq, VulnWatch, PacketStorm, and Securiteam. Trend Micro is also a member of Microsoft Active Protections Program receiving vulnerability information from Microsoft in advance of their monthly security bulletins. This makes it possible for Trend Micro to anticipate emerging threats and provide more timely protection. Trend Micro responds to advisories and security updates in addition to out-of-band security patches typically associated with zero day threats.

4. **Web Application 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.

5. **Enterprise-grade, Bi-directional, and Stateful Firewall**

An 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.

6. **Protection for Physical, Virtual, and Cloud Computing Environments**

Deep Security 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 agentless protection, maximizing deployment flexibility.

**HOW DEEP SECURITY WORKS**

Deep Security provides virtual patching through its vulnerability shielding capabilities outlined in the section above, but this is only one aspect of the protection it provides. This comprehensive server security platform delivers adaptive, highly efficient agentless and agent-based protection, including anti-malware, intrusion detection and prevention, firewall, web application protection, application control, integrity monitoring, and log inspection.


**DEEP SECURITY VIRTUAL APPLIANCE**

Deep Security can be provided as a dedicated security virtual appliance on VMware vSphere virtual machines. The virtual appliance integrates with vShield Endpoint and other VMware
APIs to offer agentless antimalware, file integrity monitoring, IDS/IPS, web application protection, application control, and firewall protection—while also coordinating with Deep Security Agent, if desired, for log inspection. Also the Deep Security Agent can be deployed on each physical or virtual server in lieu of using the dedicated virtual appliance / agentless security approach. Trend Micro customers have the flexibility to mix agentless and agent-based configurations to best secure their unique server environments.

**DEEP SECURITY AGENT**
The Deep Security Agent is a small software component that is deployed on the server or virtual machine being protected and which enforces the security policy. This is a single security agent that integrates all of the Deep Security modules being used, streamlining deployment and management.

For virtual patching, the Deep Security Agent integrates with the system’s network driver (stack) to evaluate network packets against Deep Security rules. Should the rules engine identify an exploit, the network connection is dropped to terminate and prevent the attack.

**DEEP SECURITY MANAGER**
The Deep Security Manager enables administrators to create security profiles and apply them to servers—across physical, virtual, and cloud server deployments. It has a centralized console for monitoring alerts and preventive actions taken in response to threats, and can be configured to automate or distribute security updates to servers on demand. The Manager can be used to generate reports to gain visibility into activity to meet compliance requirements. Event Tagging functionality streamlines the management of high-volume events and enables workflow of incident response.

**SECURITY CENTER**
The Security Center is a dedicated team of security experts who help customers stay ahead of the latest threats by rapidly developing and delivering security updates that address newly discovered vulnerabilities. The Security Center takes into careful consideration the large number of vulnerabilities (dating back over 10 years) and primarily focuses maintenance on vulnerabilities from 2006 to present. Considerations include system resource management, attack probability, and vulnerability age. While Deep Security does protect against some vulnerabilities dating as far back as 2001, Trend Micro’s position is to focus on the most relevant and current threat probabilities.

As there are a wide range of operating systems and applications in use within enterprises, Trend Micro focuses its protection on the operating systems and commonly used applications most relevant to its customers, based on analysis and on-going customer feedback. This includes out-of-box protection for over 100 applications.

Trend Micro Security Center has released 17,000+ rules to date. These rules provide network-based detection and prevention. This non-intrusive network IDS/IPS approach ensures critical systems and applications maintain operational availability goals while preventing attacks until patches can be deployed during scheduled patch maintenance, or in lieu of a patch when a patch is not available.
KNOWING THE RISKS: DEEP SECURITY VIRTUAL PATCHING IMMEDIATELY MITIGATES RISKS

1. **Microsoft Critical Vulnerability MS12-020: Remote Desktop Protocol Vulnerability**
   On Tuesday, March 13, 2012 (Patch Tuesday), Microsoft released the Security Update MS12-020. The vulnerability associated to this patch was rated as “critical” and affects all versions of Windows (servers and desktops) in which RDP service is “on.” The vulnerability could allow an attacker to install programs; view, change, or delete data; or create new accounts with full user rights. Also exploits could potentially act as worms because the vulnerability could enable unauthenticated, network-based exploits. With the security update, Microsoft stated that there was a high likelihood that attempts to exploit the vulnerability would occur in the following 30 days.

   **The Power of Virtual Patching: Deep Security Customers Automatically Shielded**
   As a member of the Microsoft Active Protections Program, Trend Micro received advance information about Vulnerability MS12-020, enabling the release of Deep Security Update DSRUI12-006 to protect against the vulnerability on the same day the Microsoft Security Update was announced, March 13, 2012. This Deep Security Update provided immediate vulnerability shielding against any exploits leveraging this vulnerability. Deep Security customers were instantly protected, allowing them to roll out the Windows patch during regularly scheduled maintenance and avoiding emergency patching and unscheduled downtime.

2. **Protection against 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 took advantage of these vulnerabilities.

WHY TREND MICRO

As the largest pure-play security provider with over 20 years of experience and the recognized leader in server\(^\text{12}\), virtualization\(^\text{13}\), and cloud security\(^\text{14}\), Trend Micro is uniquely positioned to help businesses make the most of virtualization and cloud computing. As part of this expertise, Trend Micro is a leading VMware security partner, providing Trend Micro Deep Security as the first partner solution designed specifically to:

- Integrate with vShield Endpoint APIs
- Integrate with other VMware APIs for network-level protection
- Deliver agentless anti-malware—available since 2010
- Deliver multiple agentless security options

Trend Micro provides a unique virtual patching solution that leverages the distinctive framework of Deep Security. Multiple security modules are offered in either agentless or agent-based
configurations for flexible deployment options—all on one security platform. Deep Security is the only solution that integrates this breadth of server security, enabling the coordinate of multiple security technologies for a highly-effective virtual patching solution.

CONCLUSION

Trend Micro Deep Security provides advanced protection for servers in the dynamic datacenter, whether physical, virtual or in the cloud. Deep Security combines antimalware, intrusion detection and prevention, firewall, integrity monitoring, web application protection, application control, and log inspection capabilities in a single, centrally managed software agent or with agentless security options for VMware virtual and cloud environments.

Deep Security enables IT operations to better manage systems and improve compliance by protecting vulnerable systems by extending the timeframe available to IT operations to deploy patches, or for Out-of-Support or unpatchable systems through protection in place of a patch. Deep Security protects confidential data and critical applications to help prevent data breaches and ensure business continuity, while enabling compliance with important standards and regulations such as PCI, FISMA and HIPAA. Whether implemented as software, virtual appliance, or in a hybrid approach, this solution equips enterprises to identify suspicious activity and behavior, and take proactive or preventive measures to ensure the security of the datacenter.

Used in conjunction with traditional patch management solutions, Trend Micro Deep Security adds an essential extra layer of protection for the enterprise’s most vulnerable systems.

FOR MORE INFORMATION ON DEEP SECURITY
Please call us at +1-877-21-TREND or visit http://www.trendmicro.com/deepsecurity.
REFERENCES


7 National Vulnerability Database. Data retrieved on April 17, 2012.


