TREND MICRO™

Virtual Patching in Mixed Environments: How It Works to Protect You

A TrendLabs℠ Primer

Vulnerabilities in Web applications, servers, and endpoints can pose significant threats to organizations if hackers use them to gain entry into enterprise networks. The fact that vulnerabilities are commonly used to facilitate attacks reveals how security gaps can lead to serious consequences such as loss of critical data and, subsequently, devastating financial losses.[1]

Microsoft's decision to end its support for Windows® Server® 2003 and XP increased risks associated with malware infections and data breaches due to vulnerability exploitation caused by the nonissuance of security patches. Hackers are aware of this and will focus more on attacking exposed systems.

Despite this, a Trend Micro survey revealed that only 35% of businesses have migrated away from Windows Server 2003 while two-thirds of those planning to do so expect to only in the next six months. Even more surprising, an Enterprise Strategy Group (ESG) revealed that 25% of enterprises will continue to indefinitely use Windows Server 2003 even without vendor support and maintenance.[2]

As many enterprises face the challenge of keeping systems secure and continuously patched, hackers see an obvious attack vector. A single compromised server can make an entire network vulnerable to attacks, data loss, and malware infections. Inadequate and untimely protection can also make complying with regulations such as Payment Card Industry Data Security Standard (PCI DSS) 3.0 and others impossible.

Common IT security challenges organizations face

While IT security and operations teams face several challenges when dealing with data center and cloud deployments, some key examples include:

- Untimely release of patches for vulnerable systems
- Continued use of unsupported and unpatchable systems and applications
- Inconsistent patch cycles and infrequent release of emergency patches
- Business continuity interruptions

---

1 Trend Micro. (19 May 2015). *TrendLabs Security Intelligence Blog.* "[1Q 2015 Security Roundup] Bad Ads and Zero Days: Reemerging Threats Challenge Trust in Supply Chains and Best Practices." Last accessed on 19 August 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/1q-2015-security-roundup-bad-ads-and-zero-days-reemerging-threats-challenge-trust-in-supply-chains-and-best-practices/.

2 Jon Oltsik, Sr. (11 May 2015). *BrightTALK.* "Staying Secure After Microsoft Windows Server 2003 Reaches End of Life." Last accessed on 19 August 2015, https://www.brighttalk.com/webcast/1506/154857.

- Patch rollbacks and intentional delays

In a recent Protiviti survey, CIOs and IT directors gave patch management and vulnerability scanning a rating of only 6.9 in terms of importance as a security priority on a scale of 1 to 10. They instead gave utmost importance to issues such as advanced threat detection and incident response.[3] This challenge is further compounded by the increasing volume of significant attacks on organizations. In 2014, we saw two of the biggest vulnerabilities to date—Shellshock and Heartbleed.[4, 5] These vulnerabilities remained unpatched for years without issue until it was discovered that they could put many open source applications that have always been seen as secure at risk.

Heartbleed, in existence since 2011, in fact, affected 5% of selected top-level domains (TLDs) based on a scan of the top 1 million websites conducted in April 2014.[6] Around 6,000 mobile apps that access Heartbleed-vulnerable servers could also be affected.[7] Shellshock, in existence since 1989, meanwhile, was exploited in September 2014. This incident led to a plethora of attacks.

Enterprises will almost always have unpatched vulnerabilities in systems and applications at any given point in time. These could be due to time and resource issues, a lag between when a vulnerability is discovered and a patch for it is issued, the unavailability of patches for systems and applications that have reached their end of life (EOL), and other reasons.

There is a way to protect against vulnerabilities while minimizing the amount of time, effort, and resources required to do so—virtual patching.

---

3 Protivity. (2015). "Today's Enterprise—Cyberthreats Lurk Amid Major Transformation: Assessing the Results of Protivity's 2015 IT Priorities Survey." Last accessed on 19 August 2015, http://www.protiviti.com/en-US/Documents/Surveys/2015-IT-Priorities-Survey-Protiviti.pdf.

4 TrendLabs. (2015). *Trend Micro Security News.* "Magnified Losses, Amplified Need for Cyber Attack Preparedness." Last accessed on 19 August 2015, http://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/magnified-losses-amplified-need-for-cyber-attack-preparedness.

5 Pawan Kinger. (8 April 2014). *TrendLabs Security Intelligence Blog.* "Skipping a Heartbeat: The Analysis of the Heartbleed OpenSSL Vulnerability." Last accessed on 19 August 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/skipping-a-heartbeat-the-analysis-of-the-heartbleed-openssl-vulnerability/.

6 Maxim Goncharov. (10 April 2014). *TrendLabs Security Intelligence Blog.* "Heartbleed Vulnerability Affects 5% of Select Top-Level Domains from Top 1M." Last accessed on 19 August 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/heartbleed-vulnerability-affects-5-of-top-1-million-websites/.

7 Veo Zhang. (15 April 2014). *TrendLabs Security Intelligence Blog.* "Bundled OpenSSL Library Also Makes Apps and Android 4.1.1 Vulnerable to Heartbleed." Last accessed on 19 August 2015, http://blog.trendmicro.com/trendlabs-security-intelligence/bundled-openssl-library-also-makes-apps-and-android-411-vulnerable-to-heartbleed/.

What is virtual patching?

Virtual patching or vulnerability shielding provides the same functionality as software patches by implementing protective network controls that can shield vulnerable servers from attacks. This approach enables security controls to "virtually" mend vulnerabilities found at the network layer, preventing them from being exploited while enterprises wait for vendors to release patches that they can then apply. It works on the premise that exploits take identifiable network paths to and from application vulnerabilities, making it possible to manipulate and protect vulnerable servers without actually patching exploitable systems.

Effective virtual patching solutions control communications with target software. Host-based solutions are ideal, as perimeter solutions cannot provide effective protective mechanisms for each individual server, which is especially important in virtual and cloud-based deployments. The following technologies work together to deliver vulnerability protection:

- **Intrusion detection and prevention systems (IDS/IPS):** To protect unpatched network-facing systems, applications, and servers, this technology leverages smart rules and out-of-the-box vulnerability protection. Self-learning rules and comprehensive network behavior analysis makes it possible for these to:
    - Provide zero-day protection for known vulnerabilities for which patches have yet to be issued
    - Block exploits to unknown vulnerabilities by examining all incoming and outgoing traffic for protocol deviations, policy violations, and attack signals
    - Defend against Structured Query Language (SQL) injection, cross-site scripting (XSS), and other Web application vulnerability exploits
- **Multilayer firewalls:** To detect threats lying deep inside networks and prevent denial-of-service (DoS) attacks, virtual patching leverages enterprise-grade, bidirectional stateful firewalls that:
    - Decrease the possibility of attacks against physical, virtual, and cloud-based servers with fine-grained filtering, design policies per network, and location awareness across IP-based protocols and frame types
    - Detect reconnaissance scans

- **Recommendation scanning:** This capability automatically recommends which rules need to be deployed in order to optimize protection based on OS version, service pack, patch level, and installed applications, as well as which rules can be removed to minimize resource use. It also can be set to automatically and periodically rescan servers to ensure that there are no protection gaps.

Virtual patching can either be integrated with traditional patch management solutions to protect critical systems until patches are deployed or be used as a permanent shield for unsupported and unpatchable systems.

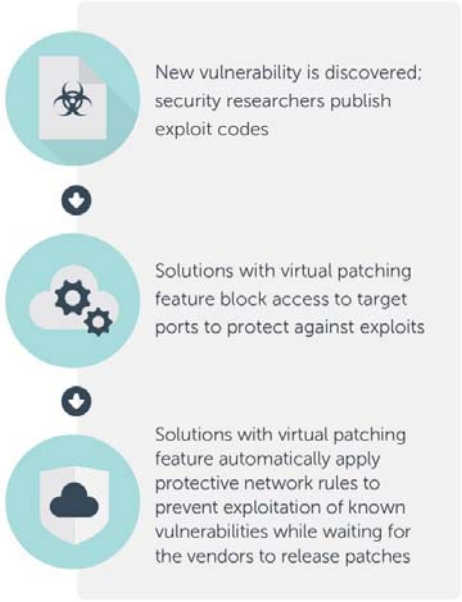
Additional host-based security controls can also play a critical role in protection. These should ideally be available in the same security platform. Examples include:

- Integrity monitoring to ensure that unplanned or suspicious changes are flagged
- Anti-malware with Web reputation controls to protect against malicious software, including viruses, spyware, worms, and Trojans

Virtual patching responsiveness

One of the major patching issues is the significant delay between when a patch is released and when it is deployed across pertinent systems. Virtual patching protects organizations during this period of vulnerability. It prevents possible exploitation while businesses wait for patches to be deployed to affected systems. The following table and figure show how solutions with virtual patching such as Trend Micro™ Deep Security protect organizations against possible exploit attacks against known vulnerabilities.[8]

Vulnerability	Time / Date vulnerability was disclosed	Date patch was released	Date first attack was reported	Average amount of time that passed between patch release and deployment
Heartbleed	7 April 2014	7 April 2014	8 April 2014	30 days
Shellshock	24 September 2014	24 September 2014	25 September 2014	30 days
POODLE	14 October 2014	14 October 2014	(Unknown)	30 days
FREAK	4 March 2015	4 March 2015	(Unknown)	30 days



> "The reality is that making software free from vulnerabilities is difficult and expensive, if not completely impossible. For every thousand lines of code, you can expect to find 15 to 50 errors of some kind. Maybe you can get that error rate down for truly critical applications like space exploration, but that adds time and money to the cost of software development."
>
> —Raimund Genes, Trend Micro CTO

[8] Trend Micro. (2015). *Trend Micro Deep Security Platform.* Last accessed on 19 August 2015, http://www.trendmicro.com/us/enterprise/cloud-solutions/deep-security/.

Organizations often take up to 30 days before being able to deploy patches to systems and applications. It may take them months or even years, meanwhile, to update more complex business applications and systems. As such, even if vendors immediately release patches, enterprises still suffer windows of exposure to attacks due to patch deployment delays.

Maximizing virtual patching benefits

Attackers often exploit vulnerabilities to infiltrate target networks. Old and new vulnerabilities are both fair game due mostly to the absence of patches for new ones and the reliability and effectiveness of older ones. Timely patching is expensive and could be prone to errors when deployed without testing in network environments. These also open networks up to zero-day exploits and other threats.

Threats unpatched vulnerabilities pose:

- Critical data exposure
- Security measure compromise
- Network and system compromise
- Financial loss
- Reputation damage

Virtual patching protects against software, Web application, and server vulnerabilities from exploit attacks. It addresses the challenge that comes with the continuous influx of high-profile vulnerabilities and critical updates. It also allows organizations to manage complex patching and vulnerability management challenges despite ongoing infrastructure changes brought about by virtualization and cloud adoption.

Effective virtual patching solutions should work across environments comprising:

- Virtual and physical servers
- Cloud workloads
- Endpoints for users

Utilizing virtual patching as a complement to standard patching, organizations can not only mitigate the risks that come with exploits but also minimize operational and financial problems related to standard patching.

Regardless of how well organizations keep up with standard patching tasks, to be adequately protected, they should employ host-based security technologies with virtual patching capabilities. Trend Micro Deep Security and Trend Micro Vulnerability Protection, part of the Trend Micro Smart Protection Suites, help protect applications, servers, and endpoints against

the risks that unpatched vulnerabilities and zero-day exploits pose while minimizing operational impact.[9]

Consider the POODLE attack, which leveraged a 15-year-old vulnerability found in Secure Sockets Layer (SSL) version 3.0.[10] It took the vendor 15 days to release a patch but it took less than 24 hours for Trend Micro to release and protect customers via a virtual patch for servers and endpoints alike. The same is true for FREAK, which has been present for many years. It took its vendor around 35 days to release a patched. But it took Trend Micro less than 24 hours to protect our customers via a virtual patch. Through virtual patching via the use of IDSs/IPSs, enterprises were quickly and painlessly secured from exploits for recent vulnerabilities such as POODLE and FREAK as well as other notable threats such as Heartbleed and Shellshock.

Even the large number of enterprises still using platforms that have already reached their EOL such as Windows Server 2003 and XP can rapidly and consistently stay protected from exploits that take advantage of the fact that Microsoft no longer issues patches for these. Trend Micro Deep Security's automated security also protects both virtual and cloud environments, ensuring that as organizations move to the cloud, they can use a single solution to consistently protect them.

---

9 Trend Micro. (2015). *Trend Micro Vulnerability Protection.* Last accessed on 19 August 2015, http://www.trendmicro.com/us/enterprise/product-security/vulnerability-protection/.

10 TrendLabs. (15 October 2014). *Trend Micro Security News.* "What to Do as Experts Reveal 'POODLE' Attack on Flawed SSL 3.0." Last accessed on 19 August 2015, http://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/what-to-do-as-experts-reveal-poodle-attack-on-flawed-ssl-3-0.

Conclusion

In sum, enterprises are at risk of vulnerability exploitation and are often challenged to keep up with standard patching, especially against major vulnerabilities such as Shellshock and Heartbleed. Even with standard patching, enterprises still suffer windows of exposure. It does not help that a large number of enterprises still use outdated applications such as Windows Server 2003 and XP.

Fortunately, Trend Micro solutions have virtual patching capabilities that can shield organizations against vulnerability exploits either until patches for them are deployed or indefinitely, as in cases where patches will no longer be made available. Enterprises that want to keep vulnerabilities in their systems and applications from being exploited can turn to virtual patching for quick-to-deploy and easy-to-manage solutions.

For more details on how virtual patching works, visit the Trend Micro Virtual Patching page. Arm yourself with the latest information on vulnerabilities as well with the help of the Trend Micro Threat Encyclopedia.

TREND MICRO™

Trend Micro Incorporated, 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 Trend Micro™ Smart Protection Network™ infrastructure, our industry-leading cloud-computing security technology, products and services stop threats where they emerge, on the Internet, and are supported by 1,000+ threat intelligence experts around the globe. For additional information, visit www.trendmicro.com.