March 2021

Security 101: Virtual Patching

How virtual patching helps protect enterprises.

As an enterprise's online infrastructures become more complex — from their decentralization to the adoption of cloud, mobile, and internet-of-things (IoT) technologies — patch management has become an even more time-consuming and resource-intensive task.

However, delaying or deferring the application of patches can be risky. In 2019, 60% of breaches were due to unapplied security patches. Data breaches could result in millions of dollars in financial losses, not to mention the hefty fines paid to authorities.

Besides data breaches, there's also the looming threat of ransomware and targeted campaigns abusing unpatched vulnerabilities. And as the Covid-19 pandemic forced organizations to shift to remote work, the need to patch vulnerabilities in technologies used in this setup (such as VPN) is also heightened. In 2020, the VPN flaw CVE-2019-11510 already had nearly 800,000 detections despite being a relatively new vulnerability.

What makes patching a challenge for enterprises?

Here are some of the challenges that organizations face when implementing a vulnerability and patch management policy:

- **Business continuity.** While regularly installing updates is a good practice, many organizations find the patching process so slow, disruptive, and costly that some opt to postpone it (or do away with it altogether) to avoid operational downtime.
- **Amount of vulnerabilities to patch.** This is especially true for organizations that constantly upgrade their IT infrastructures, as they have to patch an increasing number of vulnerabilities. Based on our data, which included input from more than 3,500 independent researchers who contribute to our Zero Day Initiative (ZDI) program, discovered and reported vulnerabilities increased by 40% from 2019 to 2020.
- **Limited visibility.** Larger online infrastructures involve more complex update processes. This could be further complicated by a fragmented IT infrastructure, usually composed of different operating system or application versions, that are sometimes also distributed geographically.
- **Frequency of patch cycles.** This can make patching difficult to manage efficiently, especially when it's hard to determine which vulnerabilities are the most relevant or critical.
- **Legacy and unpatchable systems.** Patches may no longer be issued to systems and applications that have already reached their end of life or support, even if they're still used to run mission-critical operations. Embedded systems, like those in point-of-sale terminals, IoT devices, and industrial control systems, often have software or components that cannot be patched.

What happens to unpatched IT infrastructures?

Once a vulnerability is disclosed, reported, or discovered, it is a race against time for enterprises. For cybercriminals and threat actors, it's an opportunity. An average organization, for instance, reportedly takes around 69 days to patch a critical vulnerability in its application. Businesses in the U.K. took an average of 60 days to determine that they've been breached.

This window of exposure leaves unpatched systems susceptible to threats. In January 2020, threat actors launched attacks against unpatched servers to install ransomware, putting networks of over 80,000 companies at risk.

How does virtual patching help?

Virtual patching — or vulnerability shielding — acts as a safety measure against threats that exploit known and unknown vulnerabilities. Virtual patching works by implementing layers of security policies and rules that prevent and intercept an exploit from taking network paths to and from a vulnerability.

A good virtual patching solution should be multilayered. This includes capabilities that inspect and block malicious activity from business-critical traffic; detect and prevent intrusions; thwart attacks on web-facing applications; and adaptably deploy on physical, virtual, or cloud environments.

Here's how virtual patching augments an organization's existing security technologies as well as vulnerability and patch management policies:

- **Buys additional time.** Virtual patching gives security teams the time needed to assess the vulnerability and test and apply the necessary and permanent patches. For in-house applications, virtual patching provides time for developers and programmers to fix flaws in their code.
- **Avoids unnecessary downtime.** Virtual patching provides enterprises more freedom to enforce their patch management policies on their own schedule. This mitigates the potential revenue loss caused by unplanned or superfluous disruptions in business operations.
- **Improves regulatory compliance.** Virtual patching helps organizations meet timeliness requirements, such as those imposed by the EU General Data Protection Regulation (GDPR) and Payment Card Industry (PCI).
- **Provides an additional layer of security.** Virtual patching provides security controls to components in the IT infrastructures for which patches are no longer issued (e.g., legacy systems and end-of-support OSs like Windows Server 2008) or are prohibitively costly to patch.
- **Provides flexibility.** Virtual patching reduces the need to roll out workarounds or emergency patches. It eases the task, for instance, of gauging specific points in the network that require patching (or if a patch needs to be applied to all systems).

Trend Micro Cloud One™ is a security services platform for cloud builders, equipped with the broadest and deepest solutions that are designed to meet cloud security needs both today and in the future. From cloud migration projects to cloud-native application delivery and even cloud center-of-excellence-driven objectives, Trend Micro Cloud One delivers automated, flexible, and all-in-one security.

The Trend Micro Apex One™ security solution's virtual patching delivers the timeliest vulnerability protection across a variety of endpoints, including point-of-sale (PoS), internet of things (IoT) devices, and systems with end-of-support (EoS) operating systems.

The Trend Micro Network One™ provides virtual patching and extensive zero-day protection against network-exploitable vulnerabilities via Digital Vaccine® filters. The Trend Micro Network One™ solution provides detection, in-depth analysis, and proactive response to attacks using exploits and other similar threats through specialized engines, customized sandboxing, and seamless correlation across the entire attack lifecycle, allowing it to detect threats even without any engine or pattern update.

Securing Your Connected World

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.