SECURITY 101: CLOUD-NATIVE VIRTUAL PATCHING

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. 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.

Trend Micro 2021 Annual Security Roundup: Navigating New Frontiers

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.
- **Number 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 the Trend Micro™ Zero Day Initiative™ (ZDI) program, discovered and reported vulnerabilities increased by 10% in 2021.
- **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.

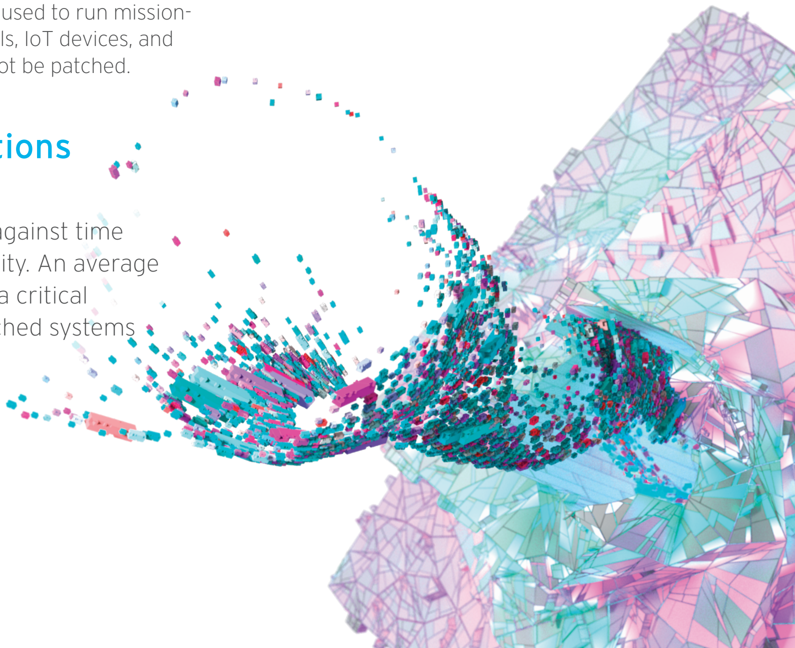
What happens to unpatched business applications and IT infrastructures?

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 60 days to patch a critical vulnerability in its application. This window of exposure leaves unpatched systems susceptible to threats.

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.

To secure new and existing workloads, Trend Micro Cloud One™ - Workload Security provides automated protection against even unknown threats like machine learning and virtual patching. For enhanced network protection, Trend Micro Cloud One™ - Network Security goes beyond traditional IPS capabilities with virtual patching and post-compromise detection and response.

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.



How does cloud-native virtual patching help?

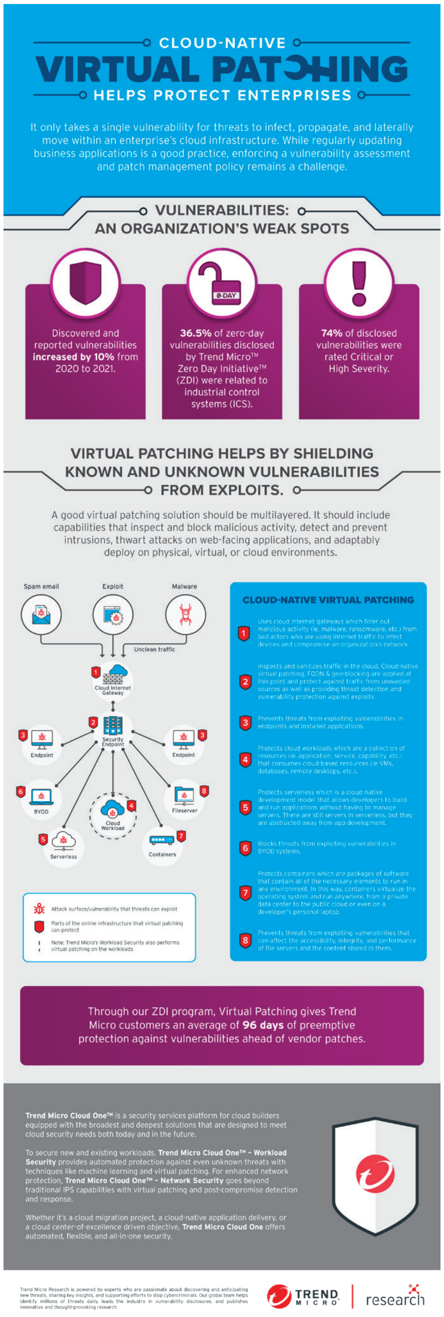
Virtual patching – or vulnerability shielding – acts as a safety measure against threats that exploit known and unknown vulnerabilities. Virtual patching works by implementing layers of security policies and rules that prevent and intercept an exploit from taking network paths to and from a vulnerability.

A good cloud-native 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 protect cloud networks, workloads and containers.

[Infographic: Minding Security Gaps: How Virtual Patching can Protect Businesses]

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

- **Prevents the risk of a successful breach or attack.** Virtual patching keeps your applications protected until a vendor-supplied patch is released or while the patch is being tested and applied.
- **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).
- **Customer-wide protection.** With cloud-native virtual patching, IT teams don't need to worry about maintaining the patching system itself. Cloud-native systems streamline the patching process allowing all their customers to be protected. Learn how virtual patching works and how it helps mitigate security and organizational risks in the infographic, "How Virtual Patching Helps Protect Enterprises."



CLOUD-NATIVE
VIRTUAL PATCHING
HELPS PROTECT ENTERPRISES

It only takes a single vulnerability for threats to infect, propagate, and laterally move within an enterprise's cloud infrastructure. While regularly updating business applications is a good practice, enforcing a vulnerability assessment and patch management policy remains a challenge.

VULNERABILITIES:
AN ORGANIZATION'S WEAK SPOTS

Discovered and reported vulnerabilities **increased by 10%** from 2020 to 2021.

36.5% of zero-day vulnerabilities disclosed by Trend Micro™ Zero Day Initiative™ (ZDI) were related to industrial control systems (ICS).

74% of disclosed vulnerabilities were rated Critical or High Severity.

VIRTUAL PATCHING HELPS BY SHIELDING KNOWN AND UNKNOWN VULNERABILITIES FROM EXPLOITS.

A good virtual patching solution should be multilayered. It should include capabilities that inspect and block malicious activity, detect and prevent intrusions, thwart attacks on web-facing applications, and adaptably deploy on physical, virtual, or cloud environments.

Attack surface/vulnerability that threats can exploit

Parts of the online infrastructure that virtual patching can protect

Note: Trend Micro's Workload Security also performs virtual patching on the workloads

CLOUD-NATIVE VIRTUAL PATCHING

1 Uses cloud internet gateways which filter out malicious activity (ie. malware, ransomware, etc.) from bad actors who are using internet traffic to infect devices and compromise an organization's network.

2 Inspects and sanitizes traffic in the cloud. Cloud-native virtual patching, FQDN & geo-blocking are applied at this point and protect against traffic from unwanted sources as well as providing threat detection and vulnerability protection against exploits.

3 Prevents threats from exploiting vulnerabilities in endpoints and installed applications.

4 Protects cloud workloads which are a collection of resources (ie. application, service, capability, etc.) that consumes cloud-based resources (ie VMs, databases, remote desktops, etc.).

5 Protects serverless which is a cloud-native development model that allows developers to build and run applications without having to manage servers. There are still servers in serverless, but they are abstracted away from app development.

6 Blocks threats from exploiting vulnerabilities in BYOD systems.

7 Protects containers which are packages of software that contain all of the necessary elements to run in any environment. In this way, containers virtualize the operating system and run anywhere, from a private data center to the public cloud or even on a developer's personal laptop.

8 Prevents threats from exploiting vulnerabilities that can affect the accessibility, integrity, and performance of file servers and the content stored in them.

Through our ZDI program, Virtual Patching gives Trend Micro customers an average of **96 days** of preemptive protection against vulnerabilities ahead of vendor patches.

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.

To secure new and existing workloads, **Trend Micro Cloud One™ - Workload Security** provides automated protection against even unknown threats with techniques like machine learning and virtual patching. For enhanced network protection, **Trend Micro Cloud One™ - Network Security** goes beyond traditional IPS capabilities with virtual patching and post-compromise detection and response.

Whether it's a cloud migration project, a cloud-native application delivery, or a cloud center-of-excellence driven objective, **Trend Micro Cloud One** offers automated, flexible, and all-in-one security.

Trend Micro Research is powered by experts who are passionate about discovering and anticipating new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative and thought-provoking research.

TREND MICRO | research

TREND MICRO™

Securing Your Connected World

[OP00_Security_101_Virtual_Patching_220621US]