HOW VIRTUAL PATCHING HELPS PROTECT ENTERPRISES

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

VULNERABILITIES: AN ORGANIZATION'S WEAK SPOTS

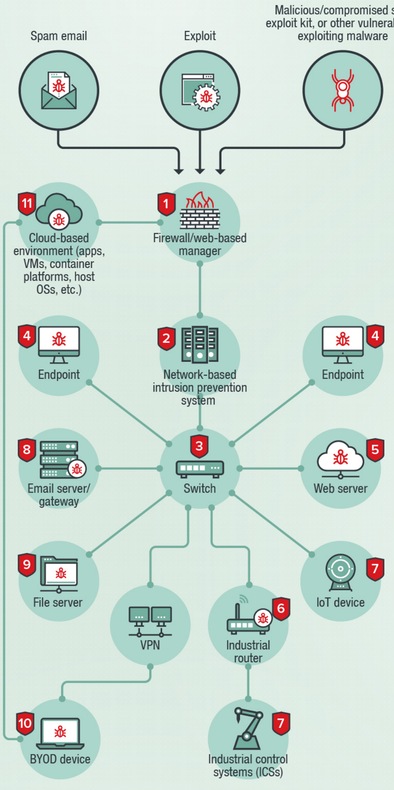
Discovered and reported vulnerabilities increased by **40%** from 2019 to 2020.

33% of zero-day vulnerabilities disclosed via the Zero Day Initiative (ZDI) in 2020 were related to industrial control systems.

64% of Microsoft advisories published by ZDI in 2020 were Windows-related.

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 from business-critical traffic; detect and prevent intrusions; thwart attacks on web-facing applications; and adaptably deploy on physical, virtual, or cloud environments.



1. Keeps track of sessions and prevents the creation of unauthorized connections, preventing attackers from accessing resources connected to it
2. Protects against threats that can let in attacks that could compromise vulnerable network- and internet-facing components
3. Further hardens the switch's security by preventing threats from exploiting vulnerabilities that can let attackers access or modify the switch's console, or laterally move to systems and servers connected to it
4. Prevents threats from exploiting vulnerabilities in endpoints and installed applications
5. Prevents threats from exploiting vulnerabilities in web servers and stopping them from spreading to endpoints and other servers
6. Blocks threats from exploiting vulnerabilities that can lead to unauthorized router configuration changes or abuse as a doorway into industrial control systems
7. Defend against threats that exploit vulnerabilities in IoT devices and IIoT systems, whether connected to the host or network
8. Prevents vulnerability-exploiting malware and malicious traffic from reaching email clients
9. Prevents threats from exploiting vulnerabilities that can affect the accessibility, integrity, and performance of file servers and the content stored in them
10. Blocks threats from exploiting vulnerabilities in BYOD systems
11. Shield exploitable vulnerabilities in cloud-based environments (e.g., servers, VMs, applications, containers)

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

The Trend Micro™ Deep Security solution provides virtual patching that protects cloud workloads, servers, and containers from threats that exploit network-based vulnerabilities in critical applications, operating systems (Linux kernels, AIX, Solaris, and Windows including those in end-of-support status), and platforms like Docker and Kubernetes.

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™ TippingPoint® Threat Protection System provides virtual patching and extensive zero-day protection against network-exploitable vulnerabilities via Digital Vaccine® filters.

The Trend Micro™ Deep Discovery™ 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.

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