

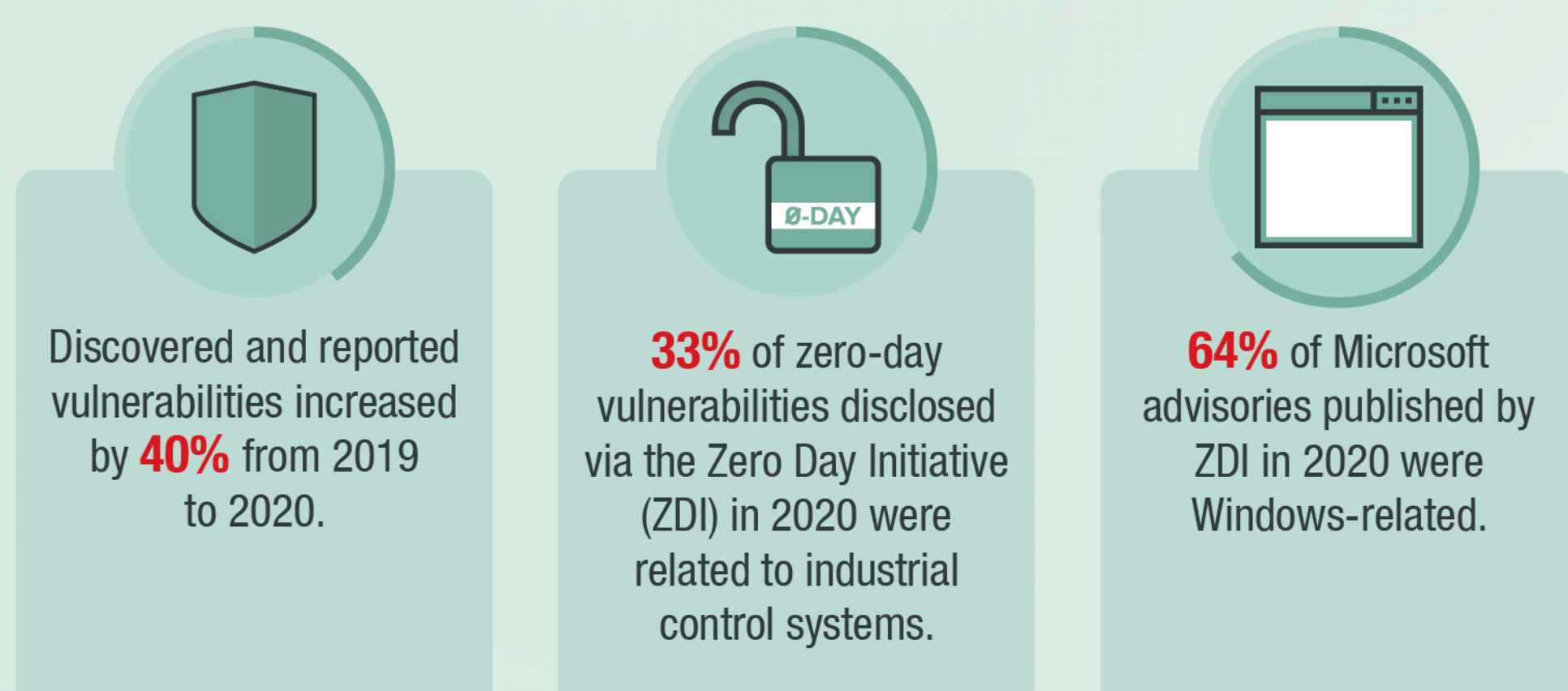
HOW

VIRTUAL PATCHING

HELPS PROTECT ENTERPRISES

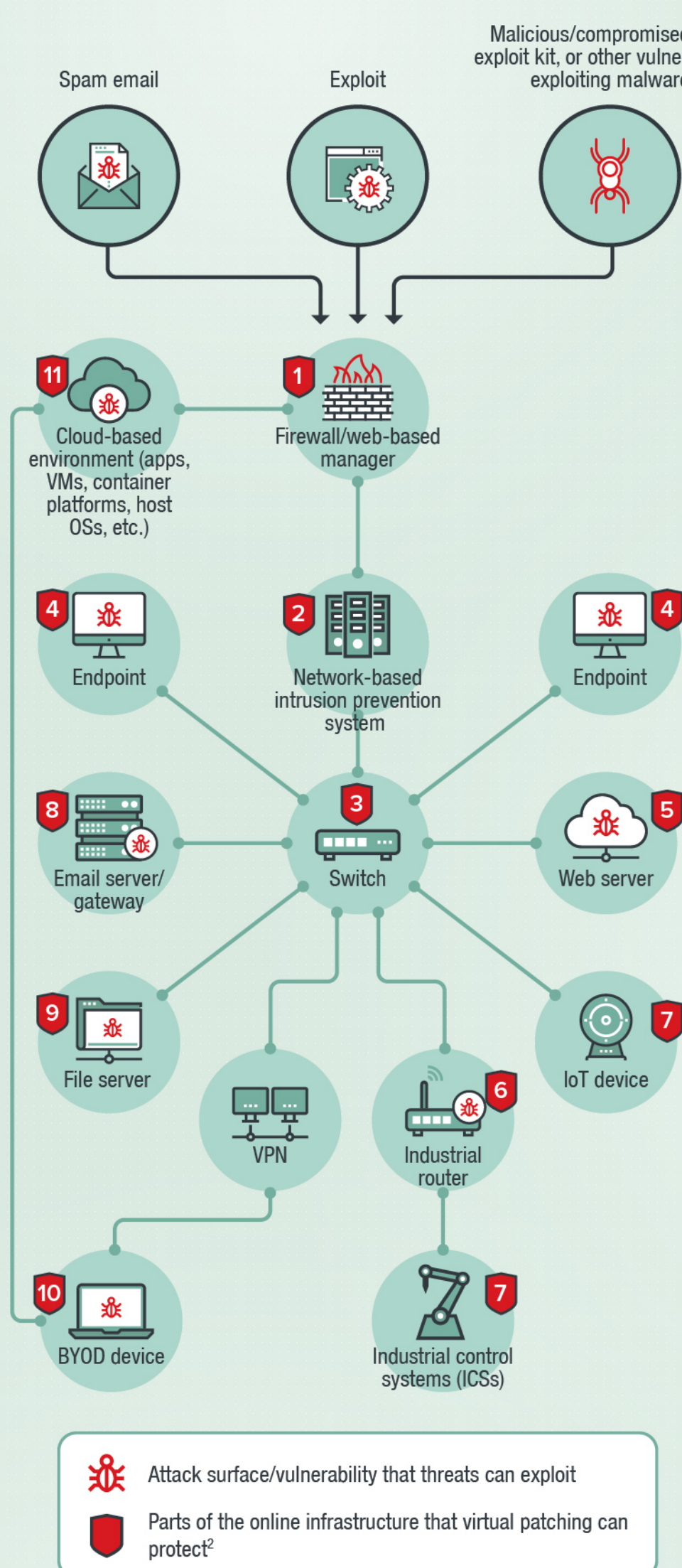
It only takes a single vulnerability for threats to infect, propagate, and laterally move within an enterprise's online infrastructure. While regularly updating them is a good practice, enforcing a vulnerability assessment and patch management policy remains a perennial challenge.

VULNERABILITIES: AN ORGANIZATION'S WEAK SPOTS



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.



- Keeps track of sessions and prevents the creation of unauthorized connections, preventing attackers from accessing resources connected to it
- Protects against threats that can let in attacks that could compromise vulnerable network- and internet-facing components
- 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
- Prevents threats from exploiting vulnerabilities in endpoints and installed applications
- Prevents threats from exploiting vulnerabilities in web servers and stopping them from spreading to endpoints and other servers
- Blocks threats from exploiting vulnerabilities that can lead to unauthorized router configuration changes or abuse as a doorway into industrial control systems
- Defend against threats that exploit vulnerabilities in IoT devices and IIoT systems, whether connected to the host or network
- Prevents vulnerability-exploiting malware and malicious traffic from reaching email clients
- Prevents threats from exploiting vulnerabilities that can affect the accessibility, integrity, and performance of file servers and the content stored in them
- Blocks threats from exploiting vulnerabilities in BYOD systems
- 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.

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™ 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.

