

# 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.



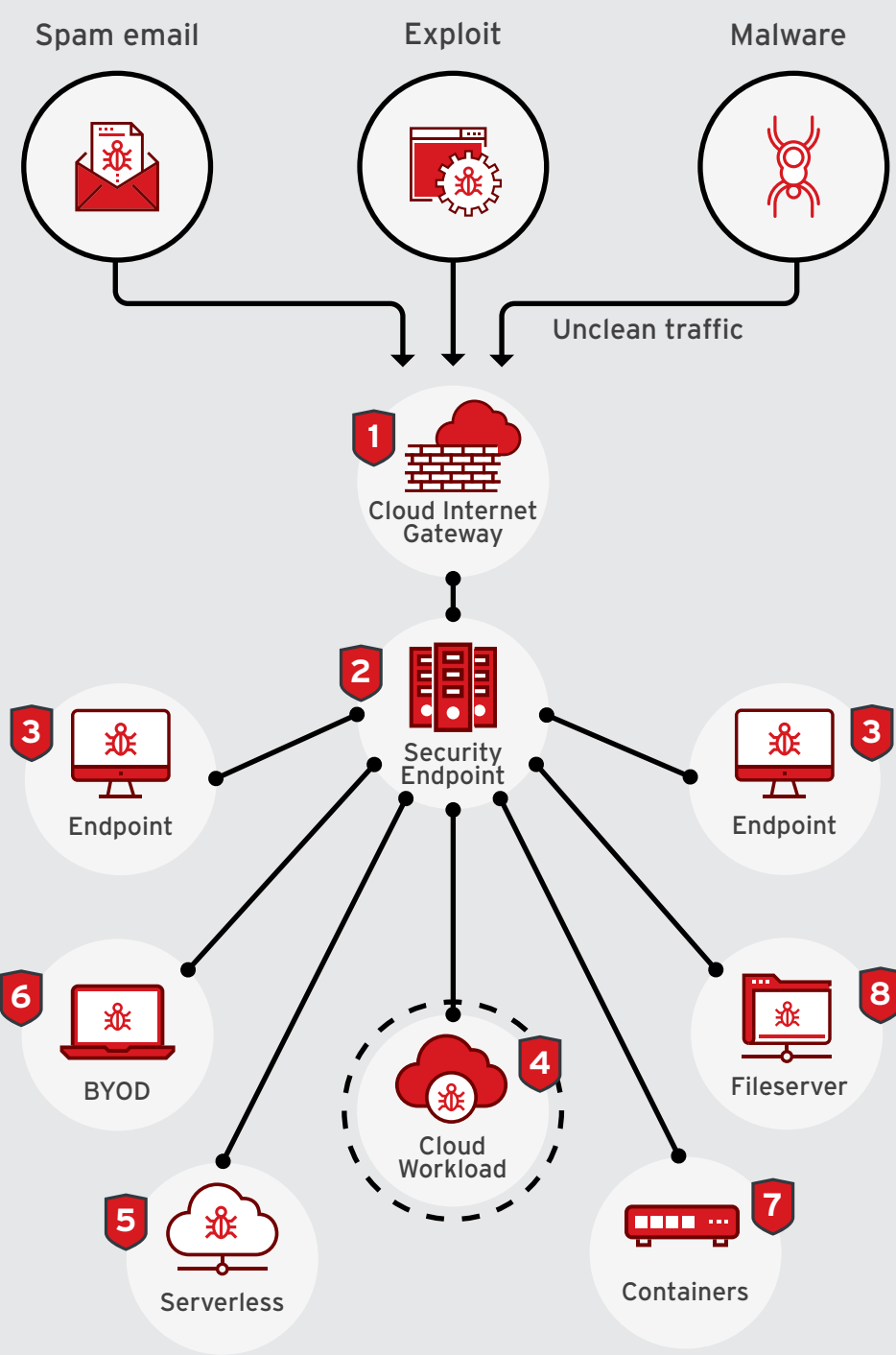
**36.5%** of zero-day vulnerabilities disclosed by Trend Micro™ Zero Day Initiative™ (ZDI) were related to industrial control systems (ICS).



**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.



### 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 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 Cloud One™ - Workload Security** provides automated protection against even unknown threats with techniques like machine learning and virtual patching. For enhanced network protection, **Trend 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.

