Datasheet

Why Cloud Workload Security is Different from Endpoint Security

Threats target servers and cloud workloads differently than endpoints (desktops, laptops, etc.), and therefore require a different blend of detection and prevention techniques. Servers and cloud workloads have a greater attack surface than endpoints and can expose critical data if not protected properly. In the past few years, attacks and ransomware leveraging vulnerabilities, like Log4J and Spring4Shell, have specifically targeted workloads, containers, and container platforms.

Hence the importance of automatically protecting new and existing workloads against both known and unknown threats.

Here are the main reasons servers/workloads require security that's built for them:

Workload discovery and auto scaling

Workloads are vulnerable from the moment they are instantiated. Trend Micro provides built-in workload discovery capabilities, integrating with Amazon Web Services (AWS), Microsoft® Azure™, Google Cloud Platform™, VMware®, and Microsoft® Active Directory®. Beyond discovery, Trend provides a range of automation and visibility (Smart Folders) functionalities to ensure that security gets configured and deployed automatically when new workloads are instantiated, even as a part of the build process or through your favorite deployment tools.

Virtual patching and lateral movement detection

Virtual patching (using host-based intrusion detection systems/intrusion prevention systems (IDS/IPS)) and lateral movement detection are critical for detecting and blocking operating system and application vulnerabilities. Trend has strong virtual patching capabilities, which are powered by its industry-leading threat research and a rich ruleset. Thanks to research provided by the Trend Micro™ Zero Day Initiative™ (ZDI), customers can be protected before the vendor patch is released. Since 2007, ZDI has been the Leader in Global Vulnerability Research and Discovery.

Hybrid cloud security

Most large enterprises manage their workloads across servers, virtualized data centers, and cloud. Enterprises also use multi- and hybrid cloud strategies to meet their business objectives. Trend has the capability to offer leading security solutions for all of these customer scenarios across entire environments in one powerful, SaaS-based solution—Trend Vision One – Endpoint Security™.

Server workloads moving to containers

Endpoint Security's runtime workload protection secures the container application, container platform, container network and traffic, as well as the host operating system.

Widespread use of Linux on workloads

A substantial portion of cloud workloads are based on Linux®. Trend has the broadest platform support that extends across current and legacy operating systems (Microsoft® Windows® and Linux), including extensive Linux builds and hundreds of Linux kernels, Solaris™, AIX®, and HP-UX®.

> “An end-user endpoint is regularly exposed to threats through email, websites, cloud services or USB drives. By contrast, threat actors target server workloads using software and configuration vulnerabilities, lateral movement, and stolen employee credentials. These differences in threat exposure create a need for distinct security requirements and protection strategies for end-user endpoints and server workloads”
>
> Gartner
>
> Prioritizing Security Controls for Enterprise Servers and End-User Endpoints (Evgeny Mirolyubov, Peter Firstbrook, January 2023)

Explore these additional industry resources featuring Trend Micro's workload protection solutions:

- **Trend is a leader in Gartner Magic Quadrant** for EPP since 2002. 19 times in a row
- **IDC: Ranked #1 for Cloud Workload Security Market Share** for the 5th consecutive year (2022)
- **A leader in the Forrester New Wave™:** Extended Detection and Response, Q4 2021
- **MITRE Engenuity ATT&CK (2022)** - #1 Performer in Linux protection, with 100% of attacks against the Linux host detected and prevented.

Support and empower the SOC and incident response teams

Trend Micro™ EDR/XDR enables detection and response capabilities across servers, cloud workloads, and container platforms by:

- Sweeping for indicators of compromise (IoC) or hunting for indicators of attack (IoA)
- Running a root cause analysis for Linux and Windows to understand the execution profile of an attack (including associated MITRE ATT&CK TTPs), and the scope of impact
- Combining other Trend solutions for endpoint, email, and network to give you correlated detection and investigation and response
- Integrating via an API with leading security information and event management (SIEM) platforms, as well as with security orchestration, automation, and response (SOAR) tools
- Augmenting your internal teams with Trend's threat experts through our 24/7 managed detection and response (MDR) service via Trend Micro™ Managed XDR

File integrity monitoring and application control

Trend detects changes to files, running services, ports, and critical system areas, like the Windows registry, that could indicate suspicious activity. Rulesets are provided to help detect server-related malicious activity and generate EDR-style detection alerts. On modern server operating system platforms, detection and alerts occur in real time. With application control, Trend provides full visibility and control of host executables and can quickly lockdown applications and servers on both Windows and Linux.

Log inspection

Trend has a log inspection capability that functions as a specialized EDR detection technique. Logs from the operating system and application are collected and analyzed, and log inspection rules identify important security events to make them visible in the product console and SIEM products. Trend's log inspection module is able to collect and correlate events across Windows, Linux, Solaris, web servers, SSHD, Samba, Microsoft® FTP, custom application log events, and more.

Trend provides server and workload security via:

Trend Vision One – Endpoint Security, leading endpoint security solution with EDR/XDR for endpoint, server, and cloud workload.

Trend Vision One cybersecurity platform

Earlier detection. Faster response. Reduced risk.

Simplifying and converging security operations start with a single platform. Trend Vision One supports diverse hybrid IT environments, automates and orchestrates workflows, and delivers expert cybersecurity services, so you can stop adversaries faster and take control of your cyber risks. Manage security holistically with comprehensive prevention, detection, and response capabilities powered by leading threat research and intelligence.

For details about what personal information we collect and why, please see our Privacy Notice on our website at: trendmicro.com/privacy