Threats target servers and cloud workloads differently than endpoints (desktops, laptops, etc.), and therefore require a different blend of detection and prevention techniques. In the past few years, attacks and ransomware leveraging vulnerabilities, like Apache Struts 2 and Heartbleed, have specifically targeted workloads, containers, and container platforms. While endpoint products can run on a server operating system, they don’t address the way servers, cloud workloads, and containers are deployed or attacked.

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 Micro 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 Micro 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 are protected as soon as the vendor patch is available, and sometimes, even days before the vendor patch is released. In 2019, for the 11th year in a row, the ZDI was named Market Leader in Vulnerability Disclosures.

**Hybrid Cloud Security**

Most large enterprises manage their workloads across legacy servers, virtualized data centers, and newer services, such as containers, cloud file storage (e.g. Amazon Simple Storage Services (Amazon S3) buckets), and serverless applications. Enterprises also use multi- and hybrid cloud strategies to meet their business objectives. Trend Micro has the capability to offer leading security solutions for all of these customer scenarios across entire environments, including serverless functions and cloud file storage, in one powerful, SaaS-based solution—Trend Micro Cloud One™.

**Server Workloads Moving to Containers**

Containers are often very short lived at runtime, so it’s essential to protect them by “shifting left”, and providing security in the DevOps software pipeline. Trend Micro provides security for the software build pipeline with container image scanning for malware, vulnerabilities, secrets, and compliance validation. In addition, Trend Micro 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 Micro 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®.

Occasionally, we see enterprises using end user focused EPP offerings designed for desktops, laptops, and tablets on server workloads. These are ill-suited for the requirements of dynamic hybrid, multicloud workload protection. The risk profile and threat exposure of a server workload is markedly different than an end user facing system.”


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

- [IDC: Worldwide Hybrid Cloud Workload Security Market Shares, 2019](#)
- [The Forrester Wave™: Cloud Workload Security, Q4 2019](#)
- [2020 Gartner Market Guide for Cloud Workload Protection Platforms](#)
Support and Empower the SOC and Incident Response Teams

Trend Micro™ 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 Micro 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 Micro threat experts through our 24/7 managed detection and response (MDR) service via Trend Micro™ Managed XDR

Marketplace and Consumption-Based Licensing/Pricing

Cloud workload platforms are designed to scale dynamically, giving you the ability to painlessly support peak loads and scale back down during low or average demand. Trend Micro security scales alongside the workloads, enabling the ability to provide a consumption-pricing model through AWS and Azure marketplaces. Security is licensed based on the number of protected hosts per hour, meaning you only pay for how much you use—plus you get the bonus of consolidated billing from the cloud provider.

APIs and Security Automation

With Trend Micro, customers can automate manual processes with security that integrates into the CI/CD pipeline using APIs to enable security management, deployment, and monitoring within the pipeline and at runtime. Trend Micro’s Documentation Center provides development, IT operations, and security teams with a searchable portal of best practices, script samples, software development kits (SDKs), API references, and documentation to help customers automate manual processes and orchestrate responses. In addition to API integration, Trend Micro has built-in automation with event-based tasks.

Agentless Anti-malware and Vulnerability Protection in VMware Virtualized Environments*

Trend Micro agentless capabilities with VMware NSX® provide better security performance and scalability in your VMware environments with:

• Guest introspection (anti-malware and integrity monitoring)
• Network service insertion (intrusion prevention and web reputation)

File Integrity Monitoring and Application Control

Trend Micro 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 Micro provides full visibility and control of host executables and can quickly lockdown applications and servers on both Windows and Linux.

Log Inspection

Trend Micro 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 and make them visible in the product console and SIEM products. The Trend Micro 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.

*Note: Currently, the agentless capabilities are only available for Trend Micro™ Deep Security™ software, but will be available soon for Trend Micro Cloud One™ – Workload Security.