Trend Micro

WHY SERVER AND CLOUD WORKLOAD SECURITY IS DIFFERENT

Threats target servers and cloud workloads differently, and therefore require a different blend of defenses. In the past few years, attacks leveraging vulnerabilities, like Apache Struts 2 and Heartbleed, have specifically targeted workloads. While endpoint products can run on a server operating system, they don't address the way servers or cloud workloads are deployed or attacked. Here are the main reasons 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™ Deep Security™ provides a range of automation and visibility (Smart Folders) functionalities to ensure that security gets configured and deployed automatically when new workloads are instantiated.

Agentless Anti-malware in Virtualized Environments

Deep Security's 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)*

Hybrid Cloud Security

Most large enterprises manage their workloads across a hybrid, multicloud environment that spans across physical and virtual data centers, public clouds, and containers. Deep Security provides consistent protection for all of these environments through a single agent and management console. For VMware NSX® environments, Deep Security can also transparently enforce security with agentless protection.

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 during the DevOps software pipeline. Deep Security provides security for the software build pipeline with container image scanning for malware, vulnerabilities, secrets, and compliance validation. In addition, Deep Security runtime workload protection secures the container application, container platform (e.g. Docker® and Kubernetes®), container traffic, and host operating system.

> "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."
>
> Gartner,
> *"Market Guide for Cloud Workload Protection Platforms"*,
> April 2019, Neil Macdonald

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. Deep Security scales alongside the workloads enabling Trend Micro to provide a consumption-pricing model option for Deep Security through AWS and Azure marketplaces. Security is licensed based on the number of protected hosts per hour, this means you only pay for how much you use and enjoy the bonus of consolidated billing from the cloud provider.

Application Programming Interfaces (APIs) and Automation

With Deep Security, customers can automate manual processes with security that integrates into the continuous integration/continuous delivery (CI/CD) pipeline using APIs to enable security management, deployment, and monitoring within the pipeline and at runtime. Trend Micro's Automation Center provides development and operations teams with a searchable portal of best practices, script samples, software development kits (SDKs), API reference, and documentation to help customers automate manual processes and simplify implementation of security in their pipelines. In addition to API integration, Deep Security has built-in automation with event-based tasks. These tasks can be used with the VMware vCenter® integration to automatically protect new workloads or workloads being migrated via VMware vSphere® vMotion®.

Widespread use of Linux® on Workloads

A substantial portion of workloads are based on Linux. Deep Security 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®.

Virtual Patching and Lateral Movement Detection

Virtual patching and lateral movement detection are critical for detecting and blocking operating system and application vulnerabilities. Deep Security has strong virtual patching capabilities, which are powered by Trend Micro's industry-leading threat research and a rich ruleset. The same engine also provides visibility and detection for lateral movement exiting protected workloads.

File Integrity Monitoring and Application Control

Deep Security 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 endpoint detection and response (EDR)-style detection alerts. On modern server operating system platforms, detection and alerts occur in real time. With application control, Deep Security provides full visibility and control of host executables and can quickly lockdown applications and servers on both Windows and Linux.

Log Inspection

Deep Security has a log inspection capability that functions as a specialized EDR 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 security information and event management (SIEM) products. The Deep Security log inspection module is able to collect and correlate events across Windows, Linux, Solaris, web servers, SSHD, Samba, Microsoft® FTP, as well as custom application log events and more.

> "Even though some of the same capabilities may be leveraged across a vendor's EPP and CWPP offerings, they are different offerings. Example differences include CWPP requirements such as full programmability of the platform and the importance of application control, microsegmentation, and cloud platform integration. CWPP differences also include the critical need to support Linux and Linux containers with continuous delivery (CI/CD) scanning in a DevSecOps environment."
>
> Gartner,
> *"Market Guide for Cloud Workload Protection Platforms"*,
> April 2019, Neil Macdonald

ADDITIONAL RESOURCE

- **Gartner Research:** *2019 Market Guide for Cloud Workload Protection Platforms*

TREND MICRO™

Securing Your Connected World

[Doc01_Why_Server_Security_Different_190917US]