Trend Micro™

ASSESSMENT OF GARTNER'S 2019 MARKET GUIDE FOR CLOUD WORKLOAD PROTECTION PLATFORMS

Trend Micro has assessed that we deliver on all 8 CWPP core control layers, and fully address 4 of 6 additional evaluation criteria while partially meeting the remaining 2 criteria

As organizations transition to the private and public cloud, there is an increased need for consistent visibility and security across these dynamic hybrid cloud workloads. The rise of rapid development practices such as DevOps is also driving adoption of new microservices architectures and containers alongside existing on-premises, virtual, and cloud deployments. As the number of environments spanning an organization's hybrid and multi-cloud increase, so too does the risk and attack surface. Modern workloads require modernized security, with protection that begins during the software build pipeline and delivers consistent security controls across the hybrid cloud at runtime.

In the 2019 Market Guide for Cloud Workload Protection Platforms, Gartner states:

"Protection requirements for securing virtual machine, container, and serverless workloads in public and private clouds continue to evolve rapidly. Security and risk management leaders should develop a strategy for addressing the unique and dynamic requirements for protecting hybrid cloud workloads."

A global leader in cybersecurity solutions, Trend Micro delivers comprehensive server workload protection capabilities, with support for a broad range of OSes and integration into leading infrastructure providers such as AWS, Google Cloud, Microsoft® Azure™, and VMware®, as well as full lifecycle container security for build pipeline and runtime environments including Docker, Kubernetes, and OpenShift.

According to Gartner "There are eight layers of CWPP core controls." As outlined in their 2019 Market Guide for Cloud Workload Protection Platforms for hybrid cloud workload protection.

Trend Micro has assessed and found that our solution meets all of these 8 core control layers:

GARTNER CORE CWPP CONTROLS , LAYER BY LAYER	TREND MICRO DEEP SECURITY
Hardening, configuration, and vulnerability management	✔
Network firewalling, visibility, and microsegmentation	✔
System integrity assurance	✔
Application control/whitelisting	✔
Exploit prevention/memory protection	✔
Server workload EDR, behavioral monitoring, and threat detection/response	✔
Host-based IPS with vulnerability shielding	✔
Anti-malware scanning	✔

Additionally, Gartner suggests the following "Evaluation Criteria" to consider when evaluating vendors.
Trend Micro has assessed that our capabilities address 4 of the 6 main evaluation criteria:

GARTNER'S CWPP VENDOR EVALUATION CRITERIA	TREND MICRO DEEP SECURITY
Diversity of Workload Types Supported	✔
Console and Integrations	✔
Integration Into the Development Pipeline	✔
Licensing Flexibility	✔

While also partially addressing the 2 remaining evaluation criteria:

GARTNER'S CWPP VENDOR EVALUATION CRITERIA	TREND MICRO DEEP SECURITY
Use of Analytics and Machine Learning	✔
Other CWPP Market Adjacencies	✔

Trend Micro has assessed that we address this evaluation criteria by:

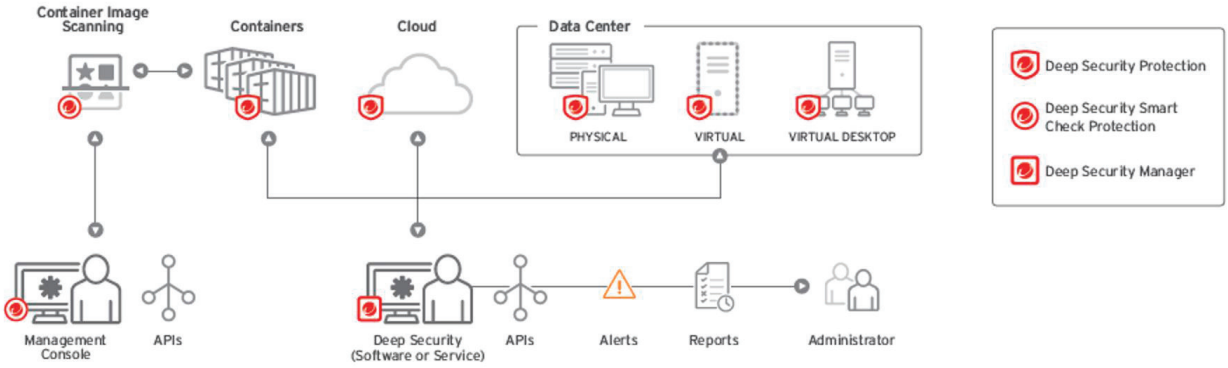
- ✔ Providing a comprehensive set of security controls across a diverse range of workload types, with broad platform and OS support, seamless integration into cloud and virtualization environments, full-stack protection for container environments, and runtime application self-protection to secure orchestration-as-a-service and serverless environments.
- ✔ Native integration into leading customer environments such as AWS, Azure, Google Cloud, and VMware, and availability via app stores and marketplaces for easy procurement, consolidated billing, and usage-based pricing. Our rich set of APIs allow for automation of all security activities through scripts and CI/CD pipeline tools, with the console available both on-premise and as a cloud-based service.
- ✔ Securing the software development pipeline with advanced image scanning for malware, vulnerabilities, secrets, IOCs, and non-compliant content, leveraging integration with leading pipeline and DevOps tools such as Jenkins, Gitlab, Ansible, Chef, Puppet, and more.
- ✔ Flexible licensing options allowing customers to purchase however they want, including workload-based pricing, consumption pricing based with consolidated billing through IaaS providers, and container host-based pricing.
- ✔ Enhancing security controls through application of analytics and machine learning, delivering advanced EDR visibility and detection capabilities, AI-powered anti-malware protection, and shared telemetry and threat intelligence across Trend Micro solutions.
- ✔ Delivering a broad range of security capabilities, including log monitoring and runtime application self-protection to extend protection beyond traditional CWPP controls.

For the full breakdown of the "Evaluation Criteria" refer to Gartner's 2019 Market Guide for Cloud Workload Protection Platforms.

Gartner also notes "Other key CWPP market trends".

Trend Micro has assessed that we deliver on those key market trends by:

- Providing a broad range of advanced host-based security controls such as malware prevention, system security, and network protection, as well as seamless integration into cloud and datacenter environments to enable automated application of security policy on existing or newly deployed workloads, with complete visibility from a single solution.
- Delivering advanced host-based IPS and traffic inspection to secure both north-south and lateral east-west traffic for microservices architectures.
- Accelerating server detection and response with powerful workload-centric capabilities such as the ability to detect indicators of attack (IOAs) and lock down suspicious applications and processes. Trend Micro integrates with leading SIEM platforms to analyze telemetry data for advanced threat hunting as well as SOAR tools for automated security orchestration and remediation action.
- Securing the software build pipeline with frictionless image scanning integrated into DevOps orchestration tools to ensure containers are secured from the moment they are deployed.
- Full lifecycle protection for container-based application architectures, with continuous image scanning during the development pipeline and full-stack runtime protection to ensure and enable protection for immutable infrastructures.
- Enabling agentless protection in container environments without host access through the architecture and deployment of security controls as a privileged container within Kubernetes environments.
- Protecting serverless environments with runtime application self-protection, via code injected into the application for seamless protection wherever it is deployed.



Trend Micro container image scanning and workload runtime protection for the data center, virtualization, multi-cloud and containers

Per Trend Micro™, Deep Security™ provides comprehensive security and visibility across container, cloud, virtual, and physical environments from a single solution. Deep Security's rich set of APIs and cloud templates enable automated security management and integration into existing security and development workflows for consistent and frictionless protection..

Click **here** to read the 2019 Gartner Market Guide for Cloud Workload Protection Platforms

* Gartner "Market Guide for Cloud Workload Protection Platforms," by Neil MacDonald; April 8, 2019.

Gartner Disclaimer: Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

TREND MICRO™

Securing Your Connected World