Trend Micro™

BEWERTUNG DES GARTNER "2019 MARKET GUIDE FOR CLOUD WORKLOAD PROTECTION PLATFORMS"

Nach eigener Einschätzung deckt Trend Micro alle 8 zentralen CWPP-Kontrollebenen ab. Darüber hinaus adressiert Trend Micro 4 der 6 zusätzlichen Evaluationskriterien vollständig und die verbliebenen 2 teilweise.

Durch den Übergang von der Private zur Public Cloud entsteht ein wachsender Bedarf an konsistenter Sichtbarkeit und Sicherheit über alle dynamischen Hybrid Cloud Workloads hinweg. Verfahren zur beschleunigten Bereitstellung wie DevOps treiben die Verbreitung von Microservice-Architekturen und Containern voran, die immer häufiger neben bestehenden On-Premise-, virtuellen und Cloud-Bereitstellungen eingesetzt werden. Die wachsende Zahl von Umgebungen in Hybrid und Multi-Clouds von Unternehmen führt aber auch zu vermehrten Risiken und einer vergrößerten Angriffsoberfläche. Moderne Workloads benötigen daher ebenso moderne Sicherheit, d.h. der Schutz muss bereits innerhalb der Software-Build-Pipeline beginnen und für die ganze Hybrid Cloud müssen konsistente Sicherheitskontrollen zur Laufzeit bereitgestellt werden.

Im "2019 Market Guide for Cloud Protection Platforms" schreibt Gartner:

"Die Anforderungen an den Schutz von virtuellen Maschinen, Containern und serverlosen Workloads in Public und Private Clouds entwickeln sich kontinuierlich weiter. Führende Sicherheits- und Risiko-Management-Anbieter müssen eine Strategie formulieren, um die einzigartigen und dynamischen Anforderungen an den Schutz von Hybrid Cloud Workloads zu adressieren."

Als einer der globalen Marktführer bei Cybersicherheitslösungen bietet Trend Micro umfassende Funktionalität für den Schutz von Server-Workloads. Neben einem breiten Spektrum von Betriebssystemen wird die Integration mit führenden Infrastrukturanbietern wie AWS, Google Cloud, Microsoft(r) Azure(tm) und VMware[r] unterstützt. Trend Micro ermöglicht außerdem den Schutz des gesamten Lebenszyklus von Containern in Build-Pipeline und Laufzeit-Umgebungen, inklusive Docker, Kubernetes und OpenShift.

"Es gibt acht Ebenen von CWPP-Kernkontrollen", so Gartner im "2019 Market Guide for Cloud Workload Protection Platforms".

Nach eigener Einschätzung adressiert Trend Micro mit seinen Lösungen alle 8 dieser zentralen Kontrollebenen.

GARTNER CWPP KERNFUNKTIONALITÄT, EBENE FÜR EBENE	TREND MICRO DEEP SECURITY
Härtung, Konfiguration und Schwachstellen-Management	✔
Netzwerk-Firewall, Sichtbarkeit und Mikrosegmentierung	✔
Gewährleistung der Systemintegrität	✔
Applikationskontrolle / Whitelisting	✔
Verhinderung von Exploits / Speicherschutz	✔
Server-Workload EDR, Verhaltensüberwachung und Threat Detection/ Response	✔
Host-basiertes IPS mit Schwachstellenabschirmung	✔
Anti-Malware-Scanning	✔

Außerdem empfiehlt Gartner, folgende Kriterien bei der Evaluation von Anbietern zu beachten. Nach eigener Einschätzung adressiert Trend Micro mit seiner Funktionalität 4 der 6 wesentlichen Evaluationskriterien.

GARTNER EVALUATIONSKRITERIEN FÜR CWPP-ANBIETER	TREND MICRO DEEP SECURITY
Unterstützung für unterschiedlichen Arten von Workloads	✔
Konsole und Integration	✔
Integration in die Endwicklungspipeline	✔
Flexible Lizenzierung	✔

Die verbliebenen 2 Evaluationskriterien werden teilweise adressiert:

GARTNER EVALUATIONSKRITERIEN FÜR CWPP-ANBIETER	TREND MICRO DEEP SECURITY
Verwendung von Analytik und Machine Learning	✔
Angrenzendes zum CWPP-Markt	✔

Nach Bewertung von Trend Micro werden die Evaluationskritierien auf folgende Weise adressiert:

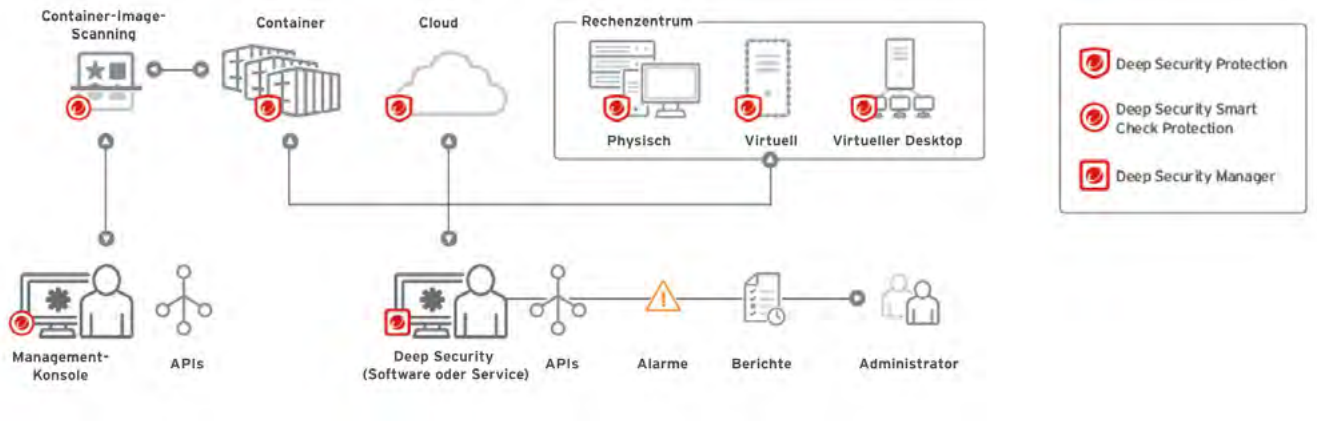
- ✔ Bereitstellung eines umfassenden Spektrums von Sicherheitskontrollen für unterschiedliche Arten von Workloads, breite Unterstützung von Plattformen und Betriebssystemen, nahtlose Integration in virtuelle und Cloud-Umgebungen, vollständiger Schutz von Container-Umgebungen sowie Schutz von Laufzeit-Applikationen für sichere Orchestration-as-a-Service und serverlose Umgebungen.
- ✔ Native Integration in führende Kundenumgebungen wie AWS, Azure, Google Cloud und VMware. Verfügbarkeit über App Stores und Marketplaces ermöglicht vereinfachte Beschaffung, konsolidierte Abrechnung und verbrauchsbasierte Preismodelle. Mithilfe unserer APIs können alle Sicherheitsaktivitäten über Skripte und CI/CD-Pipeline-Werkzeuge automatisiert werden. Die Konsole steht On-Premise sowie als cloudbasierter Service bereit.
- ✔ Schutz der Software-Entwicklungspipeline mit fortschrittlichem Image-Scanning zur Identifikation von Malware, Schwachstellen, vertraulichen Daten, IOCs und nicht konformen Inhalten. Integration mit führenden Pipeline- und DevOps-Werkzeugen wie Jenkins, Gitlab, Ansible, Chef, Puppet und weiteren mehr.
- ✔ Lizenzoptionen bieten Kunden Flexibilität beim Einkauf, zum Beispiel durch workload- oder containerbasierte Preismodelle sowie verbrauchsbasierte Preismodelle mit konsolidierter Abrechnung durch den IaaS Provider.
- ✔ Verbesserte Sicherheitskontrollen durch Einsatz von Analytics und Machine Learning. Bereitstellung von fortschrittlichen EDR-Funktionen für Sichtbarkeit und Erkennung, KI-gestütztem Anti-Malware-Schutz sowie gemeinsam genutzten Telemetriedaten und Bedrohungsinformationen für alle Trend Micro Lösungen.
- ✔ Breites Spektrum von Sicherheitsfunktionen, inklusive Log-Monitoring und Selbstschutz von Laufzeit-Applikationen, erweitert den Schutz über traditionelle CWPP-Kontrollen hinaus.

Eine vollständige Darstellung der Evaluationskriterien finden Sie im “2019 Market Guide for Cloud Workload Protection Platforms” von Gartner.

Gartner identifiziert zudem "andere wichtige CWPP-Markttrends".

Trend Micro adressiert diese Marktentwicklungen nach eigener Einschätzung durch:

- Bereitstellung eines breiten Spektrums fortschrittlicher, hostbasierter Sicherheitskontrollen, darunter Malware-Abwehr, Systemsicherheit und Netzwerkschutz. Nahtlose Integration in Cloud- und Rechenzentrumsumgebungen ermöglicht die automatisierte Durchsetzung von Sicherheitsregeln für bestehende oder neue Workloads. Eine einzige Lösung gewährleistet vollständige Sichtbarkeit der Umgebung.
- Fortschrittliche, hostbasierte Traffic Inspection und IPS schützen sowohl Nord-Süd- als auch Ost-West-Datenverkehr in Microservice-Architekturen.
- Beschleunigte Detection and Response für Server durch leistungsstarke, Workload-zentrierte Funktionen, darunter Erkennung von Indicators of Attack (IOAs) sowie Sperrung verdächtiger Applikationen und Prozesse. Trend Micro integriert sich mit führenden SIEM-Plattformen, um Telemetriedaten für das Threat Hunting auszuwerten, sowie auch mit SOAR-Werkzeugen für automatisierte Sicherheitsorchestrierung und Wiederherstellungsmaßnahmen.
- Schutz der Software-Build-Pipeline durch reibungsloses Image-Scanning. Integration in DevOps-Orchestrierungswerkzeuge sorgt dafür, dass Container ab dem Moment der Bereitstellung sicher sind.
- Schutz des gesamten Lebenszyklus für containerbasierte Applikationsarchitekturen. Fortlaufendes Image-Scanning in der Entwicklungspipeline und vollständiger Laufzeit-Schutz ermöglichen Sicherheit für unveränderliche Infrastrukturen.
- Bereitstellung von agentenlosem Schutz in Container-Umgebungen ohne Host-Zugriff über die Architektur sowie von Sicherheitskontrollen als privilegierte Container in Kubernetes-Umgebungen.
- Sicherheit von serverlosen Umgebungen mit Selbstschutz von Laufzeit-Applikationen. Durch Injektion von Code in die Applikation wird nahtloser Schutz erreicht, unabhängig vom Bereitstellungsort.



Trend Micro Container-Image-Scanning und Laufzeit-Workload-Schutz für Rechenzentren, Virtualisierung, Multi-Cloud und Container

Trend Micro™ Deep Security™ bietet mit einer einzigen Lösung umfassende Sicherheit und Sichtbarkeit für physische, virtuelle, Cloud- und Container-Umgebungen. Die umfangreichen APIs und Cloud-Templates von Deep Security ermöglichen ein automatisiertes Sicherheitsmanagement und die Integration in bestehende Sicherheits- und Entwicklungsabläufe für nahtlosen und konsistenten Schutz. Klicken Sie **hier**, um den "2019 Market Guide for Cloud Workload Protection Platforms" von Gartner zu lesen.

* Gartner "Market Guide for Cloud Workload Protection Platforms", Neil MacDonald, April 2019