Trend Micro™

BEURTEILUNG DES GARTNER MARKET GUIDE FOR CLOUD WORKLOAD PROTECTION PLATFORMS

23 VON 26 KERNFUNKTIONALITÄTEN UND ARCHITEKTURKRITERIEN DURCH TREND MICRO ABGEDECKT

Durch die wachsende Nutzung von Private und Public Clouds verlagert sich der Schwerpunkt im Bereich IT-Sicherheit: Weg vom traditionellen, signaturbasierten Endanwenderschutz und hin zu einem strategischeren Ansatz, mit dem die Sicherheit von hybriden und Multi-Cloud-Servern sowie Workloads gewährleistet werden kann. Steigende Anforderungen an die Nutzung von Cloud-Services und Containern führen zu einer Vergrößerung der Angriffsfläche. Um Unternehmen auch weiterhin vor folgenschweren Angriffen schützen zu können, müssen sich InfoSec- und DevOps-Teams der Herausforderung mit einem einheitlichen Sicherheitsansatz stellen.

Im **2018 Market Guide for Cloud Workload Protection Platforms***, schreibt Gartner:

"Cloud Workload Protection Platform offerings address the unique requirements of server workload protection in modern, hybrid data center architectures that span on-premises, physical and virtual machines (VMs), and multiple public cloud infrastructure as a service (IaaS) environments. In addition, support for protecting container-based application architectures is becoming a mandatory requirement."

Als einer der weltweit führenden Anbieter von Cybersicherheitslösungen bietet Trend Micro herausragende Funktionen zum Schutz von Server-Workloads, Unterstützung für eine ganze Reihe von Betriebssystemen (darunter Windows®, Linux® und Unix®) sowie nahtlose Integration in VMWare®, AWS und Microsoft® Azure™, inklusive nativer Applikationskontrollen und Schutz für Container durch Docker-Host- und Image-Scanning.

Im 2018 Market Guide for Cloud Workload Protection identifiziert Gartner eine Reihe von Kernfunktionalitäten für den Workload-Schutz in der Hybrid Cloud. Nach eigener Analyse deckt Trend Micro acht der zehn Funktionalitäten ab:

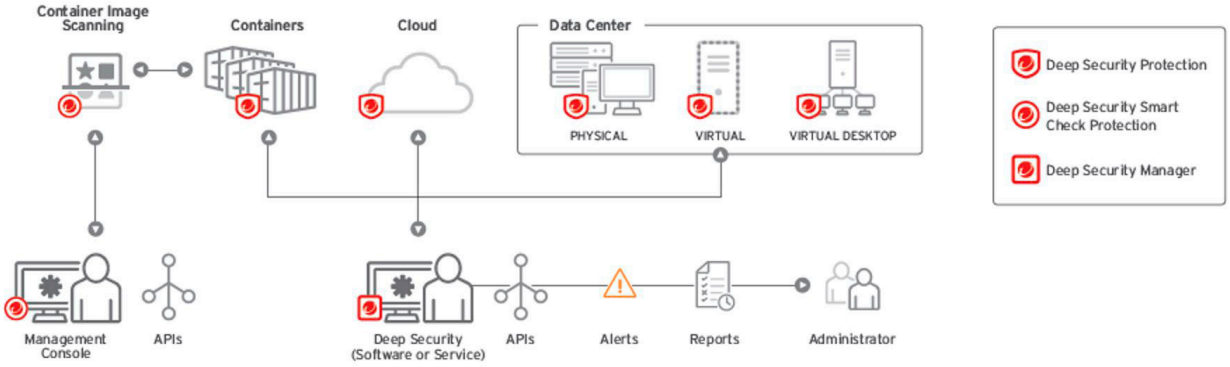
GARTNER CWPP-KERNFUNKTIONALITÄTEN	TREND MICRO DEEP SECURITY
Härtung, Scanning von Konfigurationen und Schwachstellen	✓
Workload-Segmentierung, Sichtbarkeit des Datenverkehrs und optionale Verschlüsselung des Netzwerkdatenverkehrs	✓
Monitoring und Management der Systemintegrität	✓
Applikationskontrolle	✓
Exploit-Verhinderung und Speicherschutz	✓
IaaS Data-at-Rest-Schutz	
Server EDR für Verhaltensüberwachung	✓
Host IPS inklusive schwachstellenorientiertem HIPS	✓
Täuschung (Deception)	
Signaturbasiertes Anti-Virus	✓

Bei der Evaluierung von Sicherheitslösungen für Cloud-Workloads sollten Käufer laut Gartner zudem wichtige Architekturaspekte bedenken. Nach eigener Analyse deckt Trend Micro 15 der 16 von Gartner aufgestellten Kriterien ab.

GARTNER ARCHITEKTURKRITERIEN FÜR CWPP	TREND MICRO DEEP SECURITY
Unterstützung für hybride Cloud-Umgebungen	✓
Server-Betriebssysteme unterstützt	✓
Container-Support	✓
Vollständige API-Fähigkeiten	✓
Explizite SDL-Integration	✓
Auswirkungen auf Laufzeit-Performance	✓
Agentenloser Schutz	✓
Native Integration und Support für führende Virtualisierungs- und Cloud-Provider	✓
Funktionalität der Managementkonsole	✓
Konsole-as-a-Service	✓
Compliance-Reporting	
Möglichkeit für sicheren Bootstrap	✓
Machine Learning	✓
Flexibles Preismodell	✓
Auditing und Logging	✓
Bedrohungsinformationen und Community-Intelligenz	✓

Gartner formuliert fünf Empfehlungen, anhand derer Käufer die inhärenten Sicherheits- und Compliance-Risiken von Public-Cloud-Umgebungen adressieren können. Trend Micro deckt die zentralen Empfehlungen ab durch:

- ✓ Nahtlose Integration mit führenden Umgebungen (VMware®, AWS, Azure) und leistungsstarke Sicherheit. Sofort umsetzbare Erkenntnisse zu Bedrohungen durch eine generationenübergreifende Kombination von Sicherheitstechnologien, inklusive Anti-Malware, Netzwerk- (IPS, Firewall) und Systemsicherheit (Integritätsüberwachung, Applikationskontrolle, Log-Inspektion). Identifikation von Sicherheitsproblemen (Malware und Schwachstellen) vor der Bereitstellung durch Container-Image-Scanning, das sich direkt in die DevOps CI/CD-Pipeline integriert.
- ✓ Vollständige Sichtbarkeit und Schutz für Workloads über alle Umgebungen hinweg, inklusive physischer und virtueller Maschinen, der Cloud und Containern (sowohl zur Laufzeit als auch vor der Bereitstellung). Unterstützung automatisierter Richtlinien für bestehende und anlaufende Instanzen, wodurch Sicherheitslücken geschlossen und Compliance-Risiken vermieden werden. Breiter Support für Betriebssysteme, inklusive Microsoft, Linux und Legacy-Betriebssystemen.
- ✓ Automatisierte Erkennung sowie Bereitstellung von Sicherheitskontrollen mittels Integration auf API-Ebene, spezifisch angepasst für jede Umgebung. Zusammenarbeit mit führenden DevOps-Orchestrierungswerkzeugen wie Chef, Puppet und SaltStack.
- ✓ Schutz von Cloud-Workloads und Docker Hosts gewährleistet, dass nur Applikationen auf dem Host ausgeführt werden können, die auf der Whitelist der Applikationskontrolle stehen.
- ✓ Integrierte Sicherheit für DevOps mit entwicklerfreundlichen Umgebungen und Werkzeugen (inklusive API-Integrationen und Unterstützung entwicklerorientierter Architekturen) sowie Unterstützung von AWS, Azure, Google Cloud und anderen Umgebungen. Docker-Image-Scanning für frühzeitige Erkennung von Schwachstellen und Malware.



Trend Micro Image- und Host-Schutz sowie Workload-Sicherheit für Rechenzentren und Multi-Cloud-Server

Trend Micro Cloud-Workload-Sicherheit steigert die Sichtbarkeit komplexer Angriffe und beschleunigt die Reaktion durch eine vernetzte, unternehmensweite Bedrohungsabwehr. Mit unseren bewährten Sicherheitslösungen schützen sich Unternehmen wirksam vor bekannten und unbekannten Angriffen, sodass sie sich wieder ganz auf ihr Kerngeschäft konzentrieren können.

Lesen Sie **hier** den 2018 Gartner Market Guide for Cloud Workload Protection Platforms

* Gartner „Market Guide for Cloud Workload Protection Platforms", Neil MacDonald, 26.März 2018.

Gartner Haftungsausschluss: Gartner spricht keine Empfehlung für die in seinen Forschungspublikationen beschriebenen Anbieter, Produkte oder Dienstleistungen aus und rät Technologienutzern nicht, nur die Anbieter mit den höchsten Bewertungen zu wählen. Die Forschungspublikationen von Gartner enthalten Meinungen der Forschungsorganisation von Gartner und sollten nicht als Tatsachenfeststellung ausgelegt werden. Gartner lehnt in Bezug auf diese Forschungsergebnisse jegliche Gewährleistung ab, weder ausdrücklich noch stillschweigend, und auch nicht hinsichtlich der Marktgängigkeit oder Eignung für einen bestimmten Zweck.

TREND MICRO™

Securing Your Connected World