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

TREND MICRO MEETS 23 OF 26 CORE CAPABILITIES AND ARCHITECTURAL CONSIDERATIONS

With the rise of private and public cloud adoption, there is a fast-moving shift from traditional signature-based end-user security to a much more tactful and strategic approach to protecting hybrid and multi-cloud servers and workloads. As the requirements for cloud services and container use cases increase, so too does the attack surface that InfoSec and DevOps teams must address as a unified security posture to keep the business safe from harm.

Gartner states:

"Cloud Workload Protection Platform offerings address the unique requirements of server workload protection in modern, hybrid data centre 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."

As a global leader in cybersecurity solutions, we deliver unique server workload protection capabilities, support for a broad number of OSes including Windows®, Linux® and Unix®, integration with VMWare®, AWS, Microsoft® Azure™ and its latest product releases, which include native application control as well as Docker host and image scanning protection for containers.

Gartner identifies a core set of capabilities in their 2018 Market Guide for Cloud Workload Protection Platforms for hybrid cloud workload protection. Trend Micro has determined we meet eight of ten capabilities:

GARTNER CORE CWPP CAPABILITIES	TREND MICRO DEEP SECURITY
Hardening, configuration and vulnerability scanning	✓
Workload segmentation, traffic visibility and optional network traffic encryption	✓
System integrity monitoring/management	✓
Application control	✓
Exploit prevention and memory protection	✓
IaaS data-at-rest encryption	
Server EDR for behavioral monitoring	✓
Host IPS including vulnerability-facing HIPS	✓
Deception	
Signature-based antivirus	✓

Additionally, when assessing cloud workload protection solutions, Gartner suggests key architectural considerations that buyers should evaluate. Trend Micro has determined we address 15 of 16 considerations:

GARTNER'S CWPP KEY ARCHITECTURAL CONSIDERATIONS	TREND MICRO DEEP SECURITY
Support for hybrid cloud environments	✓
Server OSs supported	✓
Container support	✓
Full API enablement	✓
Explicit SDL integration	✓
Impact on runtime performance	✓
"Agentless" protection	✓
Native integration and support for leading virtualization and cloud providers	✓
Management console capabilities	✓
Compliance reporting	
Ability to securely bootstrap	✓
Machine learning	✓
Pricing model flexibility	✓
Auditing and logging	✓
Threat intelligence and community intelligence	✓

Gartner suggests five buyer recommendations to address security and compliance risks inherent in public cloud environments.

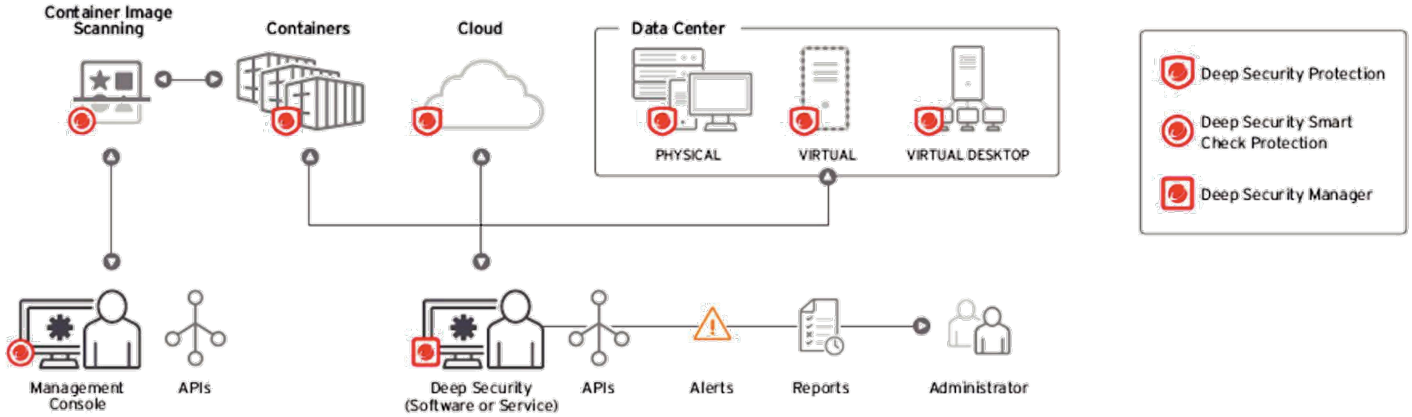
Trend Micro addresses those key recommendations by:

- Providing seamless integration with leading environments (VMware®, AWS, Azure) and high-performance security with actionable insights from a cross-generational set of security capabilities, including anti-malware, network (IPS, Firewall), and system security (integrity monitoring, application control, log inspection). Identifying security issues (malware and vulnerabilities) prior to deployment, with container image scanning that integrates directly with your DevOps CI/CD pipeline.

- Delivering complete visibility and protection of workloads across all environments – physical, virtual machines, cloud and containers (both runtime and pre-deployment) – enabling automated policies on existing or spun-up instances, helping to remove security gaps and ease compliance risks. Offering the broadest support for platforms including Microsoft, Linux and legacy OSes.

SOMA IT

- Automating discovery and deployment of security controls leveraging API-level integration specific to each environment that works in conjunction with leading DevOps orchestration tools like Chef, Puppet, and SaltStack.
- Protecting cloud workloads and Docker hosts to ensure that only supporting applications you whitelist with application control are allowed to run on your host
- Integrating security for DevOps with more developer-friendly environments and tools, including API integrations and the ability to protect developer-focused architectures, and environments such AWS, Azure, or Google Cloud, as well as Docker image scanning for earlier detection of vulnerabilities and malware.



Trend Micro container image and host protection, and data centre and multi-cloud server workload security

Our cloud workload protection increases visibility and speed of response to sophisticated attacks through a connected enterprise threat defence, providing protection against the known and unknown, while allowing the business to focus on their day-to-day operations with the assurance of a trusted security solution.

SOMA IT proudly partnering with Trend Micro; to tailor your cyber-security strategy, talk to SOMA IT today
www.somait.com.au | 1300 131 559 | info@somait.com.au

*Gartner "Market Guide for Cloud Workload Protection Platforms," by Neil MacDonald; March 26, 2018.