

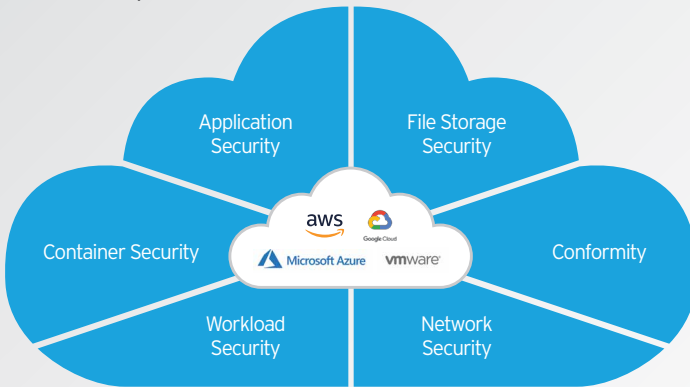
# SELLER CHEAT SHEET

## Trend Micro Cloud One™ - Workload Security



### WHAT IS TREND MICRO™ CLOUD ONE™?

A security services platform for organizations building in the cloud. Delivering the broadest and deepest offering in one solution, Cloud One enables customers to secure cloud infrastructure with simplicity. Providing support for all major cloud platforms and integration directly into DevOps processes and toolchain, Cloud One provides flexibility without slowing down business or application delivery.



### WHAT IS TREND MICRO CLOUD ONE - WORKLOAD SECURITY?

Workload Security provides a single service that is purpose-built for server, cloud, and container environments.

Security is automated with DevOps toolchain integration and a rich set of REST APIs, which facilitates deployment, policy management, health checks, and compliance reporting. Workload Security protects virtual desktops and servers against zero-day malware—including ransomware and network-based attacks—while minimizing operational impact from resource inefficiencies and emergency patching.



#### Target Customers

**Roles:**

- Info Sec, IT Security, Cloud Security, SOC teams

**Size of company:**

- Medium to very large companies

**Verticals:**

- Works well in all industries but strong customer base in healthcare, financial services, government, retail, telecom, high tech, transportation

[» See our customer success stories here](#)



#### Channel Spiffs

a. Meeting Spiff\*: Up to \$250 for every meeting created between Trend Micro and a new customer prospect

a. Sales Spiff: 5% of net to Trend Micro amount when closing an eligible Cloud One opportunity

\*Subject to partner eligibility and participation. Terms and conditions apply.

### WHAT PROBLEMS DOES WORKLOAD SECURITY SOLVE?



Problem

Not enough resources (staff, budget, time) to stay on top of security.



Solution

Automated protection across a multi-cloud environment with consistent, context-aware policies. DevOps toolchain integration with deployment scripts and RESTful APIs enable integrated security with existing toolsets for automated security deployment, policy management, health checks, compliance reporting, and more.



Problem

Too many single point solutions—which results in siloed security, making it difficult and expensive to manage.



Solution

One unified tool to consolidate security across physical, virtual, multi-cloud, and container environments with a single agent and platform.



Problem

Difficult to demonstrate compliance with a growing number of regulatory requirements.



Solution

Addresses major compliance requirements for GDPR, PCI DSS, HIPAA, and more, with one integrated and cost-effective solution. Provides detailed audit reports that document prevented attacks and compliance policy status.



Problem

Working with a complex and constantly evolving infrastructure, with multiple platforms, public and private cloud, containers, and physical servers.



Solution

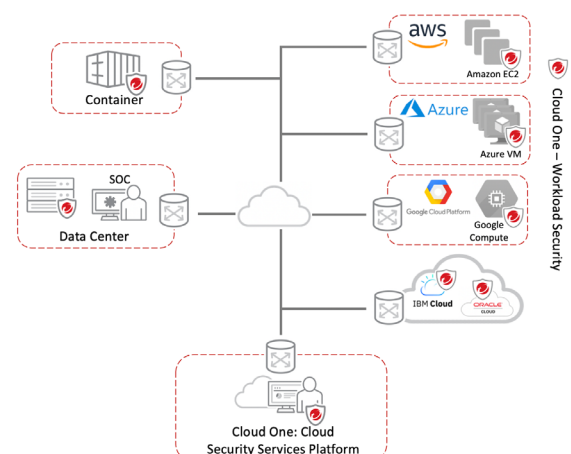
Seamlessly integrates with all the main public clouds, has a wide breath of integrations, supports an extensive list of Microsoft® Windows® and Linux® OSES (including end of support OSES), and protection/visibility across physical servers, virtual servers, and containers.

### DISCUSSION QUESTIONS

Investigative questions to discover hybrid cloud security needs and wants.

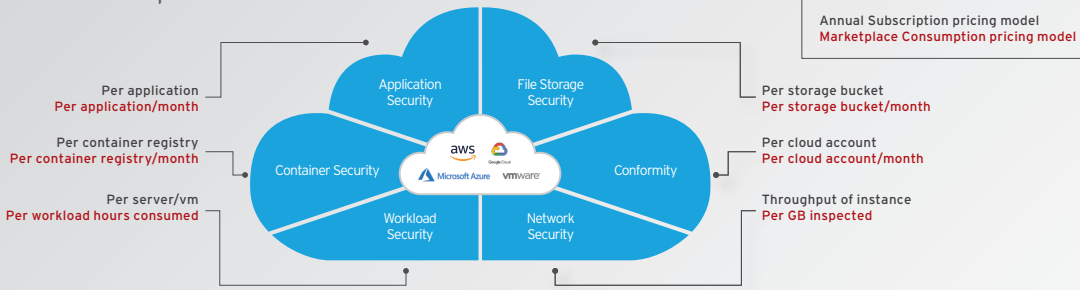
- What is your cloud strategy? Are you looking at multi-cloud or hybrid across your data center?
- How are you providing security for Linux kernels?
- Does your current solution auto scale up and down for dynamic cloud workload security?
- Are you implementing DevOps processes in your company?
- What cloud service providers are you using? AWS, Microsoft® Azure™, Google Cloud, VMware®?
- What tools do you currently have in your stack? (CHEF, Ansible, Puppet, Microsoft® SCCM)
- Do you have compliance or governance requirements in your environment?
- Are you utilizing Kubernetes® or Docker®?

### ARCHITECTURE DIAGRAM



# PRICING

High-level overview of the various pricing models for the 6 Cloud One services. For more details on the pricing for each service, please reference your regions most recent price list.



**Competitors**

## WHAT ARE THE KEY TREND MICRO COMPETITIVE DIFFERENTIATORS?

### 1. Depth of capabilities in a single solution

Protects against vulnerabilities, malware, and unauthorized changes with a wide range of powerful and intelligent capabilities.

- Depth of capabilities:**  
Intrusion prevention, anti-malware, machine learning, behavioral analysis, application control, integrity monitoring, web reputation, firewall, and log inspection.
- Secure EoS systems with virtual patches delivered through an IPS, ensuring legacy systems stay protected from existing and future threats.
- Detect and block unauthorized software execution with multi-platform application control.
- Advanced threat detection and remediation of suspicious objects through sandbox analysis.
- Shield known and unknown vulnerabilities in web, enterprise applications, and operating systems through an IPS.

### 2. Breadth of integrations

Connect security with existing environments and DevOps tools through integration for leading SIEM, security management, orchestration, monitoring, pipeline, and IT service management tools.

Cloud Vendors									
Container Platforms									
Operating Systems									
Automation and Orchestration Tools									

### 3. Global threat intelligence

Featuring 15 global research centers and 450 internal researchers,

Trend Micro has visibility into the entire threat landscape. With teams dedicated to cloud and cloud-native applications, we use our wealth of knowledge to strengthen our products and protect against current and future threats.



## ADDITIONAL RESOURCES

- [Cloud One - Workload Security Webpage](#)
- [Cloud One - Workload Security Datasheet](#)
- [Cloud One Customer Presentation](#)

## Need help selling Cloud One?

Contact your Channel Account Manager or email us at [perfectpartner@trendmicro.com](mailto:perfectpartner@trendmicro.com)