

Trend Micro

CLOUD ONE™ – WORKLOAD SECURITY

Runtime security for physical, virtual, cloud, and container workloads

The data center is undergoing a tremendous transformation. Organizations are now moving their server workloads to the cloud, and even leveraging containers and serverless in their cloud-native application architectures. There are many advantages of hybrid cloud computing, however, it also comes with new risks and threats. Your organization must ensure compliance requirements are met, and that you have security across all of your workloads: Physical servers, virtual, cloud, or container.

Trend Micro Cloud One™ – Workload Security provides comprehensive security in a single solution that is purpose-built for server, cloud, and container environments. Workload Security allows for consistent security, regardless of the workload. It also provides a rich set of application programming interfaces (APIs), so security can be automated and won't impact your teams.

AUTOMATED

Security as code lets your DevOps teams bake security into their build pipeline to release continuously and frequently. With built-in automation, including automated discovery and deployment, quick-start templates, and our Automation Center, secure your environment and meet compliance requirements quickly.

FLEXIBLE

Builder's choice. Security for your hybrid cloud, multi-cloud, and multi-service environments, as well as protection for any vintage of application delivery—with broad platform support.

ALL-IN-ONE SOLUTION

One platform that has the breadth, depth, and innovation required to meet and manage your cloud security needs today, and in the future.

Key Business Issues

• Automated protection

Save time and resources with automated security policy across your hybrid environments, such as data center and cloud, as you migrate or create new workloads.

• Unified security

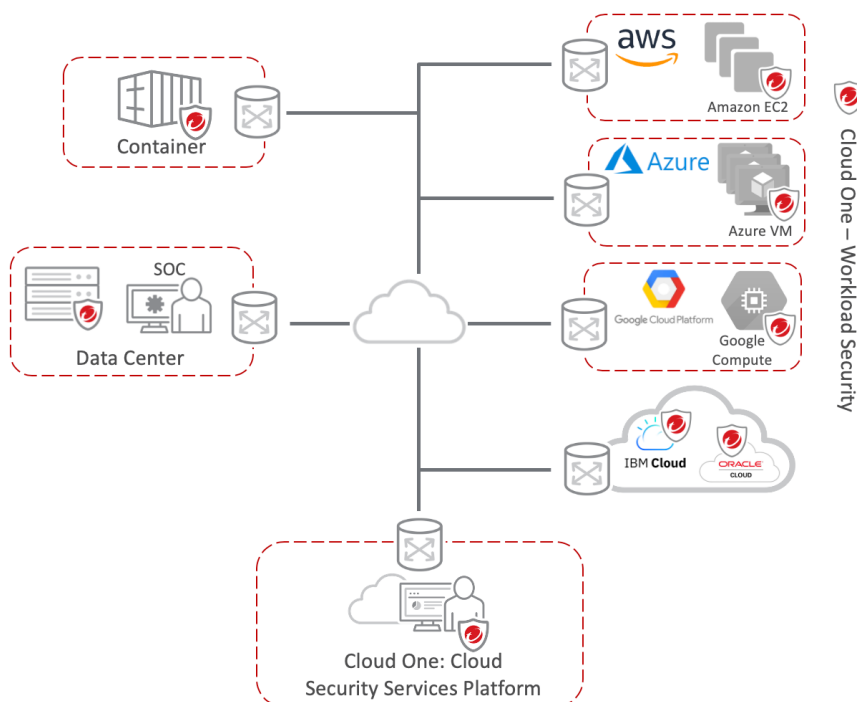
Deploy and consolidate security across your physical, virtual, multi-cloud, and container environments with a single agent and platform.

• Security for the CI/CD pipeline

API-first, developer-friendly tools to help you ensure that security controls are baked into DevOps processes.

• Accelerated compliance

Demonstrate compliance with a number of regulatory requirements, including GDPR, PCI DSS, HIPAA, NIST, FedRAMP, and more.

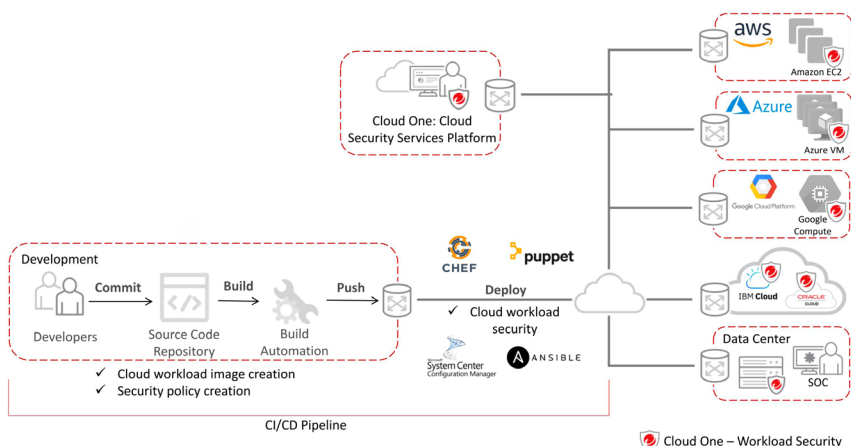
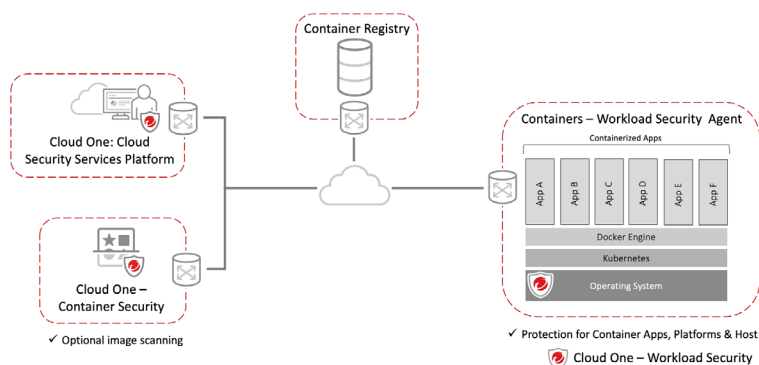


TRUSTED HYBRID CLOUD SECURITY

Full Life Cycle Container Security

Workload Security delivers advanced runtime protection for containers. Layered security defends against attacks on the host, container platform (Docker®), orchestrator (Kubernetes®), containers themselves, and even containerized applications. Designed with a rich set of APIs, Workload Security allows IT Security to protect containers with automated processes for critical security controls.

DevOps can leverage security as code by baking security into the application development pipeline, reducing the friction that comes with applying security in rapidly changing and evolving infrastructures. Complementing container runtime security, Trend Micro Cloud One™ - Container Security looks for vulnerabilities, malware, secrets, and compliance in your build pipeline.

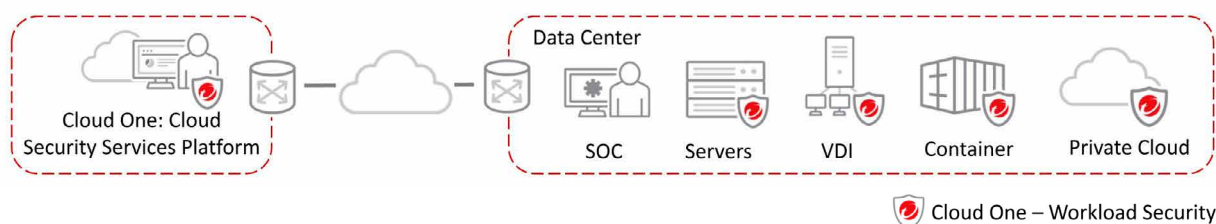


Automated Cloud Security

Workload Security works seamlessly to secure dynamic jobs in the cloud, with automated discovery of workloads across cloud providers, such as AWS™, Microsoft® Azure™, and Google Cloud™. Workload Security's single management console enables unified visibility over all of your workloads and automated protection across a multi-cloud environment with consistent, context-aware policies. Deployment scripts and RESTful APIs enable integrated security with your existing toolset for automated security deployment, policy management, health checks, compliance reporting, and more.

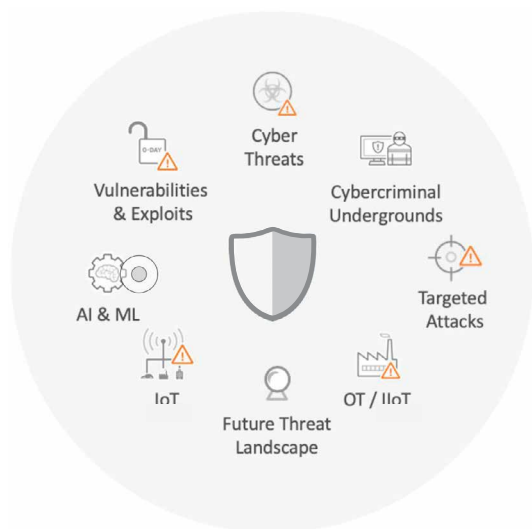
Virtualization and Data Center Security

Workload Security brings advanced protection to physical and virtual servers, enabling easy deployment and management of security across multiple environments through automatic policy management. Workload Security protects virtual desktops and servers against zero-day malware, including ransomware, cryptocurrency mining attacks, and network-based attacks, while minimizing operational impact from resource inefficiencies and emergency patching.



Security fueled by leading global threat research

Our 15 global research centers and 450 internal researchers networked across the world have visibility into the entire global 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.



Scope

We continually analyze and identify new malware, ransomware, malicious URLs, command and control (C&C) locations, and domains that could be used in attacks.

Thanks to the Zero Day Initiative™, the largest bug bounty program in the world, we can identify and disclose new vulnerabilities across a wide range of platforms.

KEY ADVANTAGES

Advanced Threat Protection

- Protect your critical servers and applications with advanced security controls, such as an intrusion prevention system (IPS), integrity monitoring, machine learning, and application control.
- Detect and block threats in real time, with minimal performance impact.
- Detect and block unauthorized software execution with multi-platform application control.
- Shield known and unknown vulnerabilities in web, enterprise applications, and operating systems through an IPS.
- Send alerts and trigger proactive prevention upon the detection of suspicious or malicious activity.
- Secure end-of-support systems with virtual patches delivered through an IPS, ensuring legacy systems stay protected from existing and future threats.
- Track website credibility and protect users from infected sites with web reputation threat intelligence from Trend Micro's global domain-reputation database.
- Identify and block botnet and targeted attack C&C communications.
- Secure against the latest threats using threat intelligence from Trend Micro™ Smart Protection Network™, powered by Trend Micro's market-leading threat research.

Support and Empower Incident Response Teams: Detection and Response

Enable EDR capabilities across servers and cloud workloads with [Trend Micro XDR](#).

- Sweep for indicators of compromise (IoC) or hunt for indicators of attack (IoA) for more comprehensive protection.
- Detect server, cloud workload, and container platform (Docker, Kubernetes) attacks for better visibility.
- Run a root cause analysis for Linux® and Windows® servers, understand the execution profile of an attack (including associated MITRE ATT&CK TTPs), and identify the scope of impact.
- Combine with other Trend Micro solutions for endpoint, email, and network to give you correlated detection and integrated investigation and response.
- Integrate via API with leading SIEM platforms, as well as with SOAR tools for security orchestration.
- Augment your internal teams with Trend Micro threat experts to provide full threat monitoring, identification and analysis through our 24/7 managed detection and response (MDR) service via [Trend Micro™ Managed XDR](#).

Unified Security for the Hybrid Cloud

- Cloud and data center connectors automatically discover workloads running in your hybrid cloud environments for full visibility and automated policy management.
- Eliminate the cost of deploying multiple point solutions and achieve consistent security across physical, virtualized, cloud, and container environments with a lightweight, single agent and management console.
- Ensure security at multiple layers of your container environments, including protection for the host, container platform (Docker) and orchestrator (Kubernetes), the containers themselves, as well as the containerized applications.
 - Secure your container host with the same advanced host-based controls applied across your physical, virtual machine (VM), and cloud workloads.
 - Monitor for changes and attacks on Docker and Kubernetes platforms with integrity monitoring and log inspection capabilities.
 - Protect runtime containers through container vulnerability shielding (via IPS), real-time malware protection, and east-west container traffic inspection.
- Enforce security early in the pipeline using Container Security's advanced build-time image and registry scanning, complementing Workload Security's runtime capabilities for protection across the container life cycle.

Automate and Streamline Security

- Automate security deployment, policy management, health checks, and compliance reporting with Workload Security REST APIs.
- Reduce management costs by automating repetitive and resource-intensive security tasks, reducing false-positive security alerts, and enabling a workflow for security incident response.
- Significantly reduce the complexity of managing file-integrity monitoring with cloud-based event whitelisting and trusted events.
- Match security to your policy needs so fewer resources need to be dedicated to specific security controls.
- Simplify administration with centralized management across Trend Micro security products. Centralized reporting of multiple security controls reduces the challenge of creating reports for individual products.
- Connect security with your existing environment and DevOps tools with integration for leading SIEM, security management, orchestration, monitoring, pipeline, and IT service management tools.

Achieve Cost-Effective Compliance

- Address major compliance requirements for the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), and more, with one integrated and cost-effective solution.
- Provide detailed audit reports that document prevented attacks and compliance policy status.
- Reduce the preparation time and effort required to support audits.
- Support internal compliance initiatives to increase visibility of internal network activity.
- Help consolidate tools for meeting compliance requirements with enhanced file-integrity monitoring capabilities.
- Enforce compliance across the development pipeline with Container Security's build-time and registry scanning for policy compliance.

“Having a security partner like Trend Micro, that keeps up with modern technologies and advanced threats in real time, gives me confidence that my workloads can be protected at any time—even as architectures shift”

Jason Cradit
Senior Director of Technology, TRC

Key Benefits

- **Fast:** Start securing workloads in minutes
- **Cost effective:** Annual subscription and usage-based pricing starting at \$0.01/hour
- **Simple:** Multiple security controls in a single product
- **Saves time:** We manage and update the product so you can focus on your business
- **Proven:** Protects thousands of customers and millions of servers globally
- **Flexible:** Purchase and procure through AWS and Azure Marketplaces

DETECTION AND PROTECTION CAPABILITIES

Network security tools detect and stop network attacks and protect vulnerable applications and servers

- **Host-Based Intrusion Prevention:**
Detects and blocks network-based exploits of known vulnerabilities in popular applications and operating systems using IPS rules.
- **Firewall:**
Host-based firewall protects endpoints on the network using stateful inspection.
- **Vulnerability Scanning:**
Performs a scan for known network-based vulnerabilities in the operating system and applications.

System security tools lockdown systems and detect suspicious activity

- **Application Control:**
Blocks any executables and scripts that aren't identified as known-good applications or DLLs from installing/executing.
- **Log Inspection:**
Identifies and alerts unplanned changes, intrusions, or advanced malware attacks; including ransomware as it is happening on your systems.
- **File-Integrity Monitoring:**
Monitors files, libraries and services, and etc. for changes. To monitor a secure configuration, a baseline is created that represents the secure configuration. When changes from this desired state are detected, details are logged and alerts can be issued to stakeholders.

Malware prevention stops malware and targeted attacks

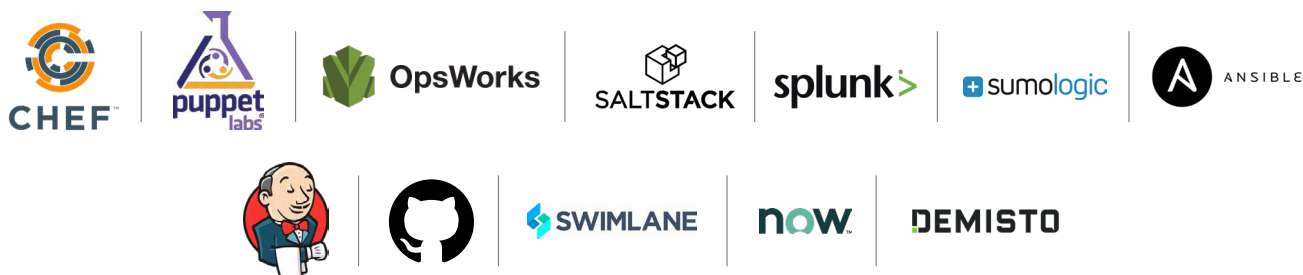
- **Anti-Malware:**
 - i. File Reputation—blocks known-bad files using our anti-malware signatures.
 - ii. Variant Protection—looks for obscure, polymorphic, or variants of malware by using fragments of previously seen malware and detection algorithms.
- **Behavioral Analysis:**
Examines an unknown item as it loads and looks for suspicious behavior in the operating system, applications, and scripts, as well as how they interact, in order to block them.
- **Machine Learning:**
Analyzes unknown files and zero-day threats using machine learning algorithms to determine if the file is malicious.
- **Web Reputation:**
Blocks known-bad URLs and websites.

BUILT FOR SECURITY IN THE CLOUD

Workload Security is optimized for leading cloud providers' infrastructures, including support of the most common operating systems:



Compatibility with configuration, event, and orchestration tools:



CERTIFICATION FOR CLOUD SERVICE PROVIDERS (CSPs)

Trend Micro's CSP partner program is a global validation program designed for CSPs to prove interoperability with industry-leading cloud security solutions from Trend Micro.

ARCHITECTURE AND SUPPORTED PLATFORMS

Workload Security is a software service (SaaS) hosted by Trend Micro in the cloud, which means we do the heavy lifting for you. We manage regular product and kernel updates, set up and maintain the security database, and administer the management platform. Our cloud-based security offering enables quick set-up, as well as automates and simplifies security operations for cloud instances.

Workload Security Agent

Enforces the environment's security policy (application control, anti-malware, IPS, firewall, integrity monitoring, and log inspection) via a small software component deployed on the server or VM being protected (can be automatically deployed with leading operational management tools like Chef, Puppet®, Ansible, Microsoft® SCCM, and AWS OpsWorks).

- As Trend Micro is constantly supporting new operating systems and versions, please refer to the following URL for the complete list, including Microsoft® Windows, Linux, Solaris™, AIX®, and Docker containers:

<https://cloudone.trendmicro.com/docs/workload-security/system-requirements/>

NOTE: For software installation, please refer to the Trend Micro™ Deep Security™ Software, which provides similar functionality and is available to install and manage in your own data center or cloud.

Flexible pricing to meet cloud needs

SaaS usage-based pricing:

AMAZON EC2® INSTANCE SIZE	MICROSOFT AZURE VIRTUAL MACHINE	HOURLY PRICE (USD)
Micro, small, medium	1 Core: A0, A1, D1	\$0.01
Large	2 cores: A2, D2, D11, G1	\$0.03
XLarge and above	4+ cores: A3-A11, D3-D4, D12-D14, G2-G5, D3, D4, D12-D14, G2-G5	\$0.06

Workload Security is part of Trend Micro Cloud One™, a security services platform for organizations building in the cloud, which also includes:

- Trend Micro Cloud One™ – Container Security:**
Image scanning in your build pipeline
- Trend Micro Cloud One™ – File Storage Security:**
Security for cloud file and object storage services
- Trend Micro Cloud One™ – Application Security:**
Security for serverless functions, APIs, and applications
- Trend Micro Cloud One™ – Network Security:**
Cloud network layer IPS security
- Trend Micro Cloud One™ – Conformity:**
Cloud security and compliance posture management



Trend Micro ZDI disclosed 1,045 vulnerabilities in 2019. This powers unmatched timeliness for virtual patches.



Key Certifications, Compliance, and Alliances

- AWS Advanced Technology Partner
- AWS Container Competency Partner
- ISO 27001
- PCI DSS
- GDPR
- HP Business Partnership
- Microsoft Application Development Gold Partner
- Microsoft Certified Partnership
- Virtualization by VMware
- VMware Cloud on AWS Partner
- VMware Global Partner of the Year



Securing Your Connected World

©2020 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, Deep Security, Smart Protection Network, Trend Micro Cloud One, Deep Discovery are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [DS02_Cloud_One_Workload_Security_200618US]

For details about what personal information we collect and why, please see our Privacy Notice on our website at: <https://www.trendmicro.com/privacy>