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 unified security across all of your workloads such as physical servers, virtual, cloud, or containers.

Trend Micro Cloud One™ – Workload Security provides comprehensive detection and protection 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

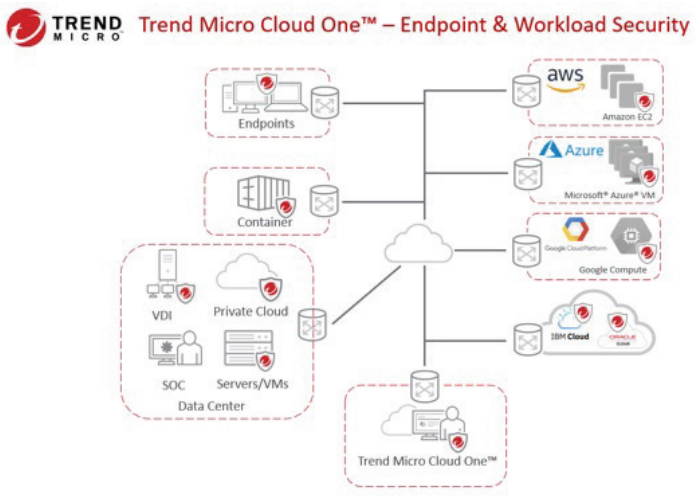
Security as code lets your DevOps teams bake security into their build pipeline to release continuously and frequently. With built-in automation, including automated discovery and deployment, quick-start templates, and our Automation Center, secure your environment and meet compliance requirements quickly.

## FLEXIBLE

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

## BETTER TOGETHER

Adopt the Trend Micro Cloud One™ – Endpoint Security service alongside Workload Security to protect user endpoints, servers and cloud workloads using a single platform, and with unified management and role-based access control. Eliminates the cost and complexity of deploying multiple point solutions while achieving specialized security optimized for your diverse endpoints and workloads.




## Key Business Issues

**Automated protection**

Save time and resources with automated security policies, deployments, health checks, and compliance reporting across your hybrid environments, such as data center and cloud, as you migrate or create new workloads.

**Complete security**

Deploy and consolidate detection and protection across your physical, virtual, multi-cloud, container, and user endpoint environments with a single agent.

**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**

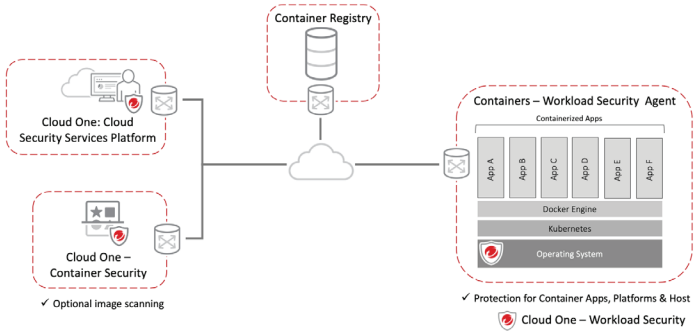
Demonstrate compliance with several regulatory requirements, including GDPR, PCI DSS, HIPAA, NIST, FedRAMP, and more.

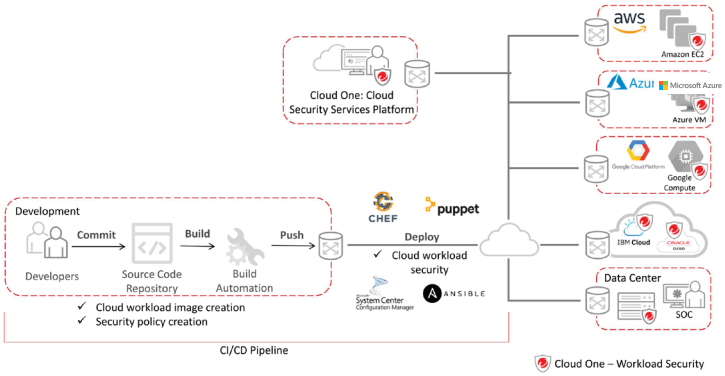
### Full Life Cycle Container Security

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.



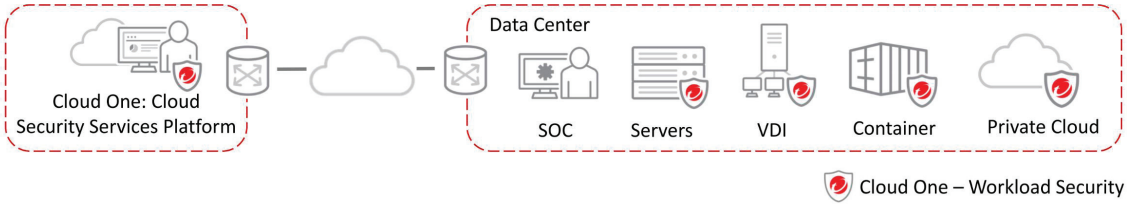

### Automated Cloud Security

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 Platform™ (GCP).

The single management console enables unified visibility over all 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 Datacenter 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 more than 10,000 independent researchers internationally 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 **Trend Micro™ Zero Day Initiative™ (ZDI)**, the global market leader in vulnerability disclosure, we can identify and responsibly disclose new vulnerabilities while helping our solutions discover threats sooner across a wide range of applications and platforms.

## KEY ADVANTAGES

### Advanced Threat Protection

- 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.
- Multi-platform application control to detect and block unauthorized software execution.
- 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.
- Inspect, detect, and prevent malicious payloads sent via Transport Layer Security (TLS) without the need of managing certificates and keys.
- 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.
- Market-leading threat research and threat intelligence from Trend Micro™ Smart Protection Network™ enables better security against the latest threats.

### Support and Empower Incident Response Teams: Detection and Response

Get the XDR advantage with integrated EDR capabilities designed for server, cloud workloads, and user endpoints, leveraging Trend Micro Vision One™.

- Receive prioritized, actionable alerts, and comprehensive incident views
- Investigate root cause and execution profile across Linux and Microsoft Windows endpoint and server attacks, uncovering their scope and initiating direct response
- Hunt for threats via multiple methods—from powerful queries to simple text search—to proactively pinpoint tactics or techniques and validate suspicious activity in your environment
- Continuously search for newly discovered IoCs via Trend Micro's automated intelligence or custom intelligence sweeping
- Leverage Trend Micro Vision One for enhanced and correlated detection, investigation, and response across security layers, including email, network, cloud, workloads, and more
- Integrate via API with SIEM platforms and SOAR tools
- Augment your teams with 24/7/365 managed detection and response (MDR) service

### Complete Security for the Hybrid Cloud

- Cloud and datacenter 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, container, and user endpoint environments with a lightweight, single agent and management console.
- Enforce security early in the pipeline using advanced build-time image and registry scanning from Container Security, complementing the runtime capabilities of Workload Security for protection across the container life cycle.
- 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.

### Achieve Cost-Effective Compliance

- Address major compliance requirements for the GDPR, PCI DSS, HIPAA, NIST, 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.

### Automate and Streamline Security

- Automate security deployment, policy management, healthchecks, 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 safelisting and trusted events.
- Match security to your policy needs to minimize the resources 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.

## DETECTION AND PROTECTION CAPABILITIES

### Network security tools detect and stop network attacks to 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 lock down 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, 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, 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.

**SAP Scanner*:**
Enables anti-malware scanning for Netweaver through the SAP Virus Scan Interface (VSI).

**SAP® Certified**
Integration with SAP NetWeaver®

**TLS Inspection:**
Inspects SSL/TLS content for threats and prevents attacks without having to manage keys and certificates, increasing security posture, and providing better protection.

*The SAP Scanner requires specialized functionality that must be purchased separately from your Workload Security license.

## BUILT FOR SECURITY IN THE CLOUD

Workload Security is optimized for leading cloud providers' infrastructures, including support for many operating systems, examples include:

Linux | Windows | SUSE | redhat | CentOS | ubuntu

Compatibility with configuration, event, and orchestration tools:

CHEF | puppet labs | OpsWorks | SALTSTACK | splunk> | sumologic | ANSIBLE

SWIMLANE | now | DEMISTO

## CERTIFICATION FOR CLOUD SERVICE PROVIDERS (CSPs)

Our 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 software as a service (SaaS) hosted by Trend Micro in the cloud, which means additional value from new capabilities and security functionality are delivered continuously. 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 setup, local and regional flexibility as well as automates and simplifies security operations for cloud instances.

Workload Security Agent enforces the platform's detection and protection policy (application control, anti-malware, IPS, firewall, integrity monitoring, and log inspection) via a small software component deployed on the endpoint, server, or VM being protected. This can be automatically deployed with leading operational management tools like Chef, Puppet, Ansible, Microsoft System Center Configuration Manager, 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 Windows, Linux, Solaris™, AIX, and Docker containers: **https://cloudone.trendmicro.com/docs/workload-security/system-requirements/**

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.

For more information about Workload Security's local and regional flexibility, please refer to the following URL about Trend Micro's Cloud One Regional Data Centers: **https://www.trendmicro.com/en_sg/business/technologies/regional-data-centers.html**

### Key Benefits

- **Fast:** Start securing workloads in minutes
- **Cost effective:** Annual subscription and usage-based pricing starting at $0.045/hour
- **Simple:** Multiple security controls in a single service
- **Saves time:** We manage and update the product so you can focus on your business
- **Proven:** Protects thousands of customers and millions of servers and endpoints globally
- **Flexible:** Purchase and procure through AWS and Azure Marketplaces

NIST

GDPR

HIPAA

PCI

**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™ – Endpoint Security:** Agent-based security for your endpoints
- **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 Cloud One™ – Open Source Security by Snyk:** Visibility and monitoring of open source risks

## KEY CERTIFICATIONS, COMPLIANCE, AND ALLIANCES

- AWS Advanced Technology Partner
- AWS Container Competency Partner
- ISO 27001/ISO 27014/ISO 27017
- PCI DSS
- GDPR
- HP Business Partnership
- Microsoft Certified Partnership
- SOC 2
- Virtualization by VMware
- VMware Cloud on AWS Partner
- VMware Global Partner of the Year
- Microsoft Application Development Gold Partner

## TRUSTED EXPERTISE

IDC *Analyze the Future*

Trend Micro ranked #1 in IDC's Worldwide Hybrid Cloud Workload Security Market Shares report

MITRE ENGENUITY ATT&CK® EVALUATIONS Enterprise WIZARD SPIDER & SANDWORM PARTICIPANT 2022

#1 performer in Linux, with 100% of attacks against the Linux host detected and prevented

"Trend Micro Cloud One - Workload Security checked all the boxes across cybersecurity and DevOps"

Mario Mendoza
Team Lead, Cyber Security Architecture and Engagement Blackbaud

ZERO DAY INITIATIVE

Trend Micro's Zero Day Initiative™ (ZDI) released advisories for 1,604 vulnerabilities in 2021, 10% higher than in the previous year.

Source: Navigating New Frontiers, March 2022

For more information on compliance, certifications, and audit reports, please visit the Trend Micro Cloud One Trust Center.

MITRE ENGENUITY
A Foundation for Public Good

MITRE Engenuity™ ATT&CK Evaluation Results with Workload Security

FORRESTER®

Learn more about the Projected Total Economic Impact™ of the Trend Micro Cloud One™ Security Services Platform

TREND MICRO™
Securing Your Connected World



[DS04_Cloud_One_Workload_Security_220630US]