DATASHEET

Trend Micro™

MOBILE SECURITY SOLUTIONS

Protect Android™ and iOS devices from malware, malicious applications, and credential attacks with next-generation security

Mobile security is a critical part of a multi-layered security strategy, particularly in today's age of remote work and diverse resources. Even your savviest employees can mistakenly click on a malicious link or download a malicious app, thus exposing your enterprise to a cyberattack. The mobile security solution offerings from Trend Micro provide next-generation malware prevention, centralized visibility, advanced risk telemetry, and the ability to protect corporate data. For clients looking for a hosted option, the new Trend Micro Apex One™ Mobile Security solution provides software as a service (SaaS)-based functionality. For clients who prefer to stay on-premises, Trend Micro Mobile Security continues to provide highly-effective protection that can be managed directly in the client environment.

KEY FEATURES

- **Centralized Management and Policy Enforcement:** Streamlines administration with a single view for enterprise users, supporting device location tracking and inventory management in addition to providing single-click deployment of data protection policies.
- **Visibility:** Offers instant summary views of compliance, inventory, protection, and the health of all devices. Mobile Security also provides visibility into the number, types, and configuration of devices that are accessing corporate resources.
- **Threat Prevention and Detection:** Leverages our leading malware and phishing protection, powered by the Trend Micro™ Smart Protection Network™, to identify access to malicious code and websites.
- **Mobile Application Reputation Service (MARS):** Identifies and blocks apps that pose a security, privacy, and vulnerability risk by correlating installed app data against the MARS database of known malicious applications.
- **Integration with Mobile Device Management Solutions:** Enables IT to remotely enroll, provision, and de-provision devices with corporate network settings like VPN, Microsoft Exchange ActiveSync, and wi-fi. Microsoft Intune API integration is also available via Trend Micro Apex One™ Mobile Security.
- **Advanced Risk Telemetry:** Risk data can be pulled from devices to allow for threat detection and response as well as continuous risk assessment of devices and users.

WHAT MOBILE SECURITY CAN DO FOR YOU

Detects and blocks advanced threats

- Identifies ransomware and other types of zero-day malware using pre-execution machine learning
- Shares threat information with other security layers to guard against persistent and targeted attacks
- Blocks access to malicious and phishing websites, preventing access to malicious code access and potential data leaks
- Allows IT to assess the use of risky mobile apps based on up-to-the-minute data from the cloud-based Trend Micro™ Mobile App Reputation™ service
- Integrates with leading mobile device management (MDM) solutions to provide easy removal of apps identified as malicious or having potential risks

Reduces Cost and Complexity

- Streamlines management of mobile security, app management, and data protection in a single solution
- Simplifies deployment by leveraging either a SaaS-based architecture (Trend Micro Apex One Mobile Security) or the Trend Micro™ Cloud Communication Server (Trend Micro™ Mobile Security Enterprise); an optional cloud-based service that automates communications and reduces complexity of deployment
- Reduces operational costs with centralized visibility and control of all endpoint security

Improves Visibility and Control

- Enables IT teams to track, monitor, and manage mobile devices, apps, and data through a single console
- Provides visibility on the number, types, and configuration of devices accessing corporate resources, whether they have enrolled or not
- Determines risks of devices and identities by correlating mobile telemetry with endpoint, network, email, and directory services

COMPARISON TABLE: MOBILE SECURITY

FEATURE	TREND MICRO MOBILE SECURITY (ON-PREMISES)	TREND MICRO APEX ONE MOBILE SECURITY (SAAS)
Centralized Management	Yes, via Trend Micro Apex Central™	Yes, via Trend Micro Vision One™ console
Protection: Known Threats	Yes	Yes
Protection: Machine Learning	Yes	Yes
Protection: Unknown URL Protection	Yes	Yes
Protection: Malicious SSL Certificate	Yes	Yes
Out-of-Date OS Notification	Yes	Yes
OS Vulnerability Mapping	Yes	Yes
Integration with Mobile Device Management Solutions	Yes	Yes, with Microsoft Intune
Mobile Application Reputation System (MARS)	Yes	Yes
Advanced Risk Telemetry for Zero Trust Applications	-	Yes
Purchase Method	Via Subscription License (or Suite)	Via Trend Micro Credits

TREND MICRO™

Securing Your Connected World

DATASHEET

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 container.

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

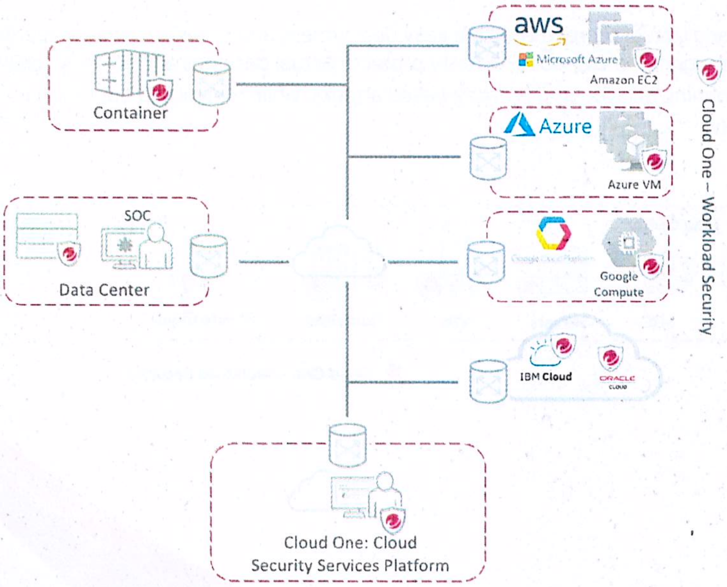
Security as code lets your DevOps teams bake security into their build pipeline to release continuously and frequently. With built-in automation, including automated discovery and deployment, quick-start templates, and our Automation Center, secure your environment and meet compliance requirements quickly.

FLEXIBLE

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

ALL-IN-ONE SOLUTION

Unified detection and protection capabilities in one platform, with the breadth, depth, and innovation required to meet your cloud security needs today and in the future.



Key Business Issues

✓ Automated protection

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

✓ Unified security

Deploy and consolidate detection and protection across your physical, virtual, multi-cloud, and container 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

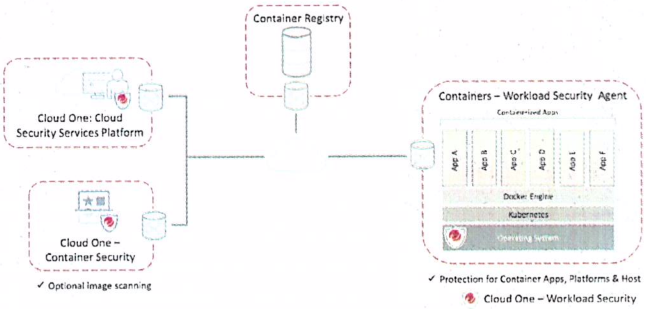
Demonstrate compliance with a number of regulatory requirements, including GDPR, PCI DSS, HIPAA, NIST, FedRAMP, and more.

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.

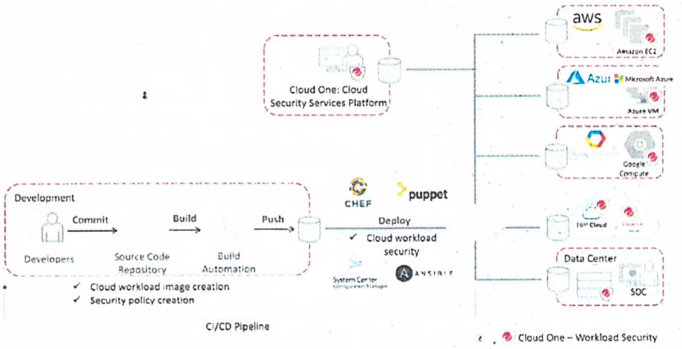
DevOps can leverage security as code by baking security into the application development pipeline, reducing the friction that comes with applying security in rapidly changing and evolving infrastructures. Complementing container runtime security, Trend Micro Cloud One™ - Container Security looks for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


Container Registry
Cloud One: Cloud Security Services Platform
Cloud One – Container Security
✓ Optional image scanning
Containers – Workload Security Agent
Containerized Apps
App A
App B
App C
App D
App E
App F
Docker Engine
Kubernetes
Operating System
✓ Protection for Container Apps, Platforms & Host
Cloud One – Workload Security

Automated Cloud Security

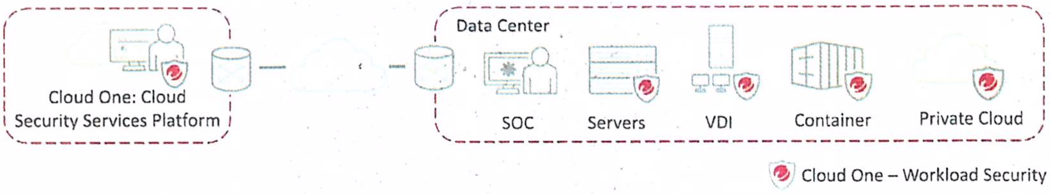
Workload Security works seamlessly to secure dynamic jobs in the cloud, with automated discovery of workloads across cloud providers, such as AWS, Microsoft Azure™, and Google Cloud Platform™.

The 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.


Cloud One: Cloud Security Services Platform
aws
Amazon EC2
Azure
Microsoft Azure
Azure VM
Google Compute
IBM Cloud
Data Center
SOC
Development
Commit
Build
Push
Developers
Source Code Repository
Build Automation
✓ Cloud workload image creation
✓ Security policy creation
CHEF
puppet
Deploy
✓ Cloud workload security
System Center Configuration Manager
ANSIBLE
CI/CD Pipeline
Cloud One – Workload Security

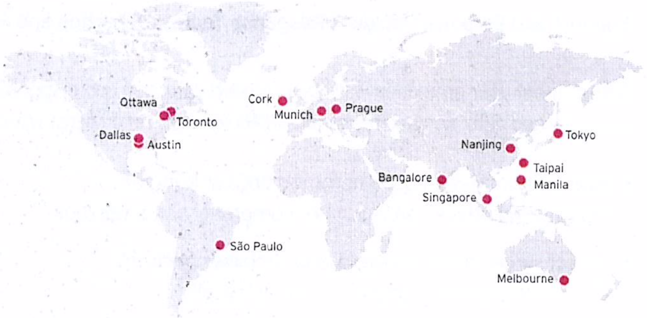
Virtualization and Datacenter Security

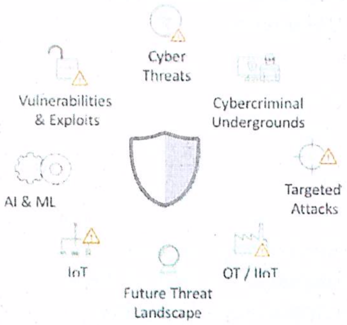
Workload Security brings advanced protection to physical and virtual servers, enabling easy deployment and management of security across multiple environments through automatic policy management. Workload Security protects virtual desktops and servers against zero-day malware, including ransomware, cryptocurrency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


Cloud One: Cloud Security Services Platform
Data Center
SOC
Servers
VDI
Container
Private Cloud
Cloud One – Workload Security

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™**, the 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.
- 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

Complement your protection with the extended detection and response (XDR) capabilities of Trend Micro Vision One™ or take advantage of our managed detection and response (MDR) service, Trend Micro™ Managed 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 Microsoft Windows servers, understand the execution profile of an attack (including associated MITRE ATT&CK tactics, techniques, and procedures [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 security information and event management (SIEM) platforms, as well as with security orchestration, automation, and response (SOAR) tools.
- Augment your internal teams with Trend Micro threat experts to provide full threat monitoring, identification, and analysis through our 24/7 Managed XDR services.

Unified 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, and container 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, 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 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 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.

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

*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 set up, 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 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.

Key Benefits

- **Fast:** Start securing workloads in minutes
- **Cost effective:** Annual subscription and usage-based pricing starting at $0.06/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

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™ - 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 | Google Cloud | Microsoft Azure | vmware

- 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

FORRESTER

Trend Micro named a leader with highest score in the current offering and strategy categories in The Forrester Wave™: Cloud Workload Security, Q4 2019

> "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 ZDI disclosed 60% of the gloal vulnerabilities in 2020. This powers unmatched timeliness for virtual patches.

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

[DS03_Cloud_One_Workload_Security_210610US]