Trend 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 your workloads, such as physical servers, virtual, cloud, or containers.

Trend 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. Secure your environment and meet compliance requirements quickly with built-in automation, including automated discovery and deployment, quick-start templates, and our Automation Center.

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 Cloud One™ – Endpoint Security service alongside Workload Security to protect user endpoints, servers, and cloud workloads using a single solution 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.

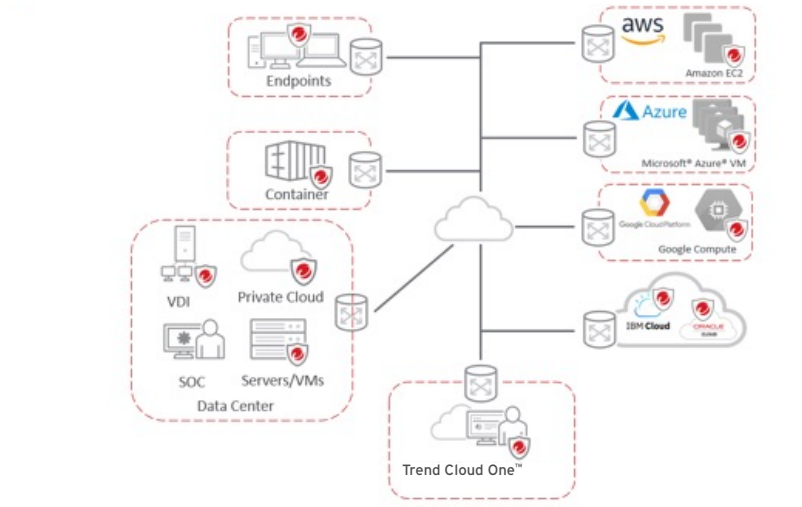
✔ Security for the CI/CD pipeline

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, and FedRAMP.

Trend Cloud One – Endpoint Security and Workload Security



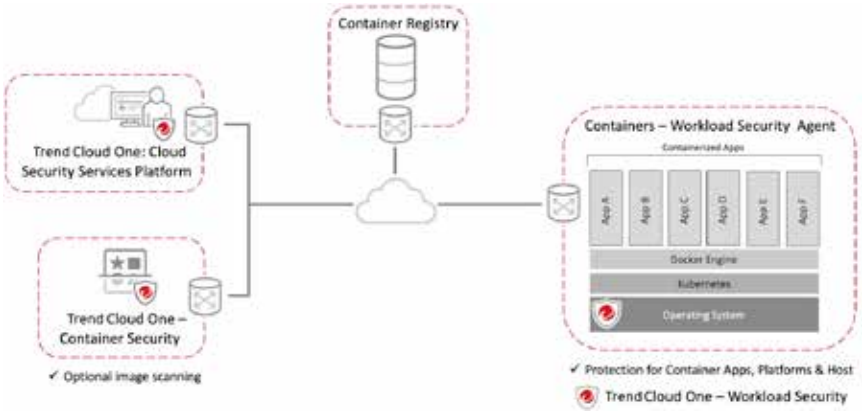
Trusted Hybrid Cloud Security

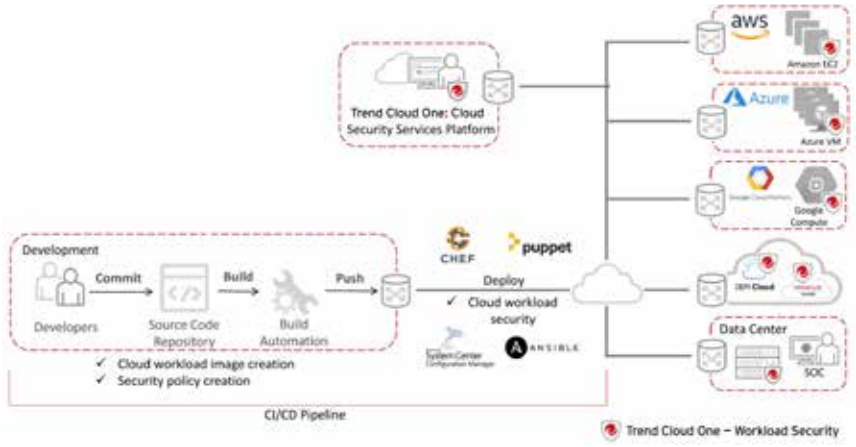
Full Lifecycle Container Security

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 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 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 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'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 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's automated intelligence or custom intelligence sweeping.**
- **Leverage Trend Vision One for enhanced and correlated detection, investigation, and response across security layers, including email, network, cloud, and workloads.**
- **Integrate via API with SIEM platforms and SOAR tools**
- **Augment your teams with 24/7 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 lifecycle.
- 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.

Workload Security is part of Trend Cloud One, a security services platform for cloud builders, which also includes:

- **Trend Micro™ Cloud Sentry:** Visibility of the threats in your AWS environment with quick, actionable insights in the context of your application
- **Trend Cloud One™ – Application Security:** Security for serverless functions, APIs, and applications
- **Trend Cloud One™ – Conformity:** Cloud security and compliance posture management
- **Trend Micro Cloud One™ – Container Security:** Automated image scanning in your build pipeline
- **Trend Cloud One™ – Endpoint Security:** Protection, detection, and response across endpoints, servers, and cloud workloads
- **Trend Cloud One™ – File Storage Security**: Security for cloud file and object storage services
- **Trend Cloud One™ – Network Security:** Cloud network layer IPS security
- **Trend Cloud One™ - Open Source Security by Snyk:** Visibility and monitoring of open source vulnerabilities and license risks

For more information, please visit **trendmicro.com**