Trend Micro Cloud One

A security services platform for organizations building in the cloud

Key benefits

- Runtime protection for workloads (virtual, physical, cloud, and containers).
- Image scanning in your build pipeline.
- Security for cloud file and object storage services.
- Security for serverless functions, application programming interface (APIs), and applications.
- Cloud network layer Intrusion Prevention Service (IPS) security.
- Cloud security and compliance posture management.

Product overview

Trend Micro Cloud One provides visibility across your AWS services and threat protection across workloads, containers, file storage, serverless and more.
Trend Micro Cloud One enables you to secure your cloud infrastructure with clarity and simplicity. By considering your cloud projects and objectives holistically, Trend Micro Cloud One can provide powerful security, while you leverage all the benefits and efficiencies the cloud offers your business.

Simplify cloud security with an automated, flexible, and all-in-one security platform. Comprised of multiple services designed to meet specific cloud security needs, Trend Micro Cloud One gives you the flexibility to solve your challenges today, and the innovation to evolve with your cloud services in the future :

- Trend Micro Cloud One™ – Workload Security: Runtime protection for workloads (virtual, physical, cloud, and containers)
- 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

Product features

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 detection and protection across your physical, virtual, multi-cloud, and container environments with a single agent and platform.

Product features (continued)

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 General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), National Institute of Standards and Technology (NIST), Federal Risk and Authorization Management Program (FedRAMP), and more.

Detection and response Detection and response capabilities

Trend Micro Cloud One provides support and empowers incident response teams.

- Complement your protection with the advanced detection and response (EDR) 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 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 MDR services.

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

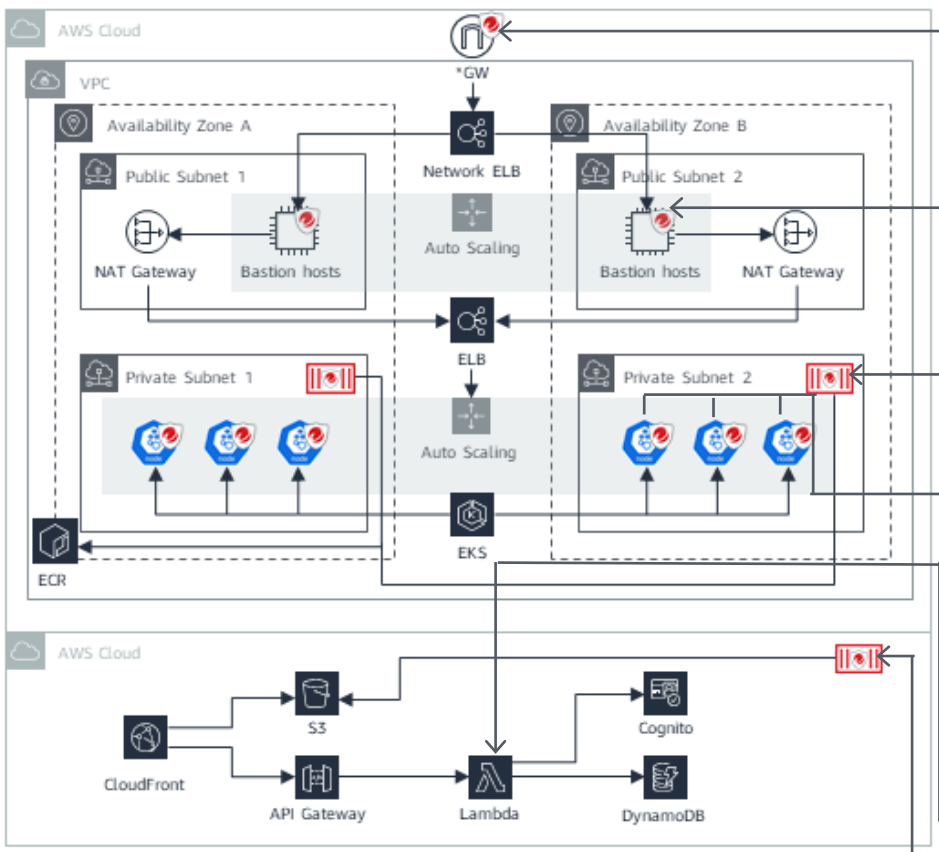
- **Application Control:** Blocks any executables and scripts that aren't identified as known good applications or DLLs from installing/executing.
- **Log Inspection:** Identifies and alerts unplanned changes, intrusions, or advanced malware attacks; including ransomware as it is happening on your systems.
- **File-integrity Monitoring:** Monitors files, libraries and services, 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.

How it works

Trend Micro Cloud One seamlessly defends your Amazon Elastic Compute Cloud (EC2) instances, AWS Lambda, AWS Fargate, containers, AWS Outposts, Amazon Simple Storage Service (S3) buckets, and your virtual private cloud (VPC) networking. With APIs and integrations into your toolchains, Trend Micro is security that won't slow you down. With anti-malware, virtual patching and IPS capabilities, protection for Linux workloads, and visibility and monitoring for unplanned or suspicious changes to your infrastructure or applications, we can help you gain immediate visibility into your environment and speed up your compliance requirements.



Cloud One Network Security
- Block malicious network traffic at the edge or transit gateway

Cloud One Workload Security
- Block Malicious File and Network traffic at each container host
- Detect suspicious activity
- Monitor system changes

Cloud One Container Security
- Detect vulnerable packages
- Detect compliance violations
- Detect misconfigured secrets
- In pipeline or registry before deployment

Cloud One Application Security
- Block Malicious File and Network traffic inside application code
- Provide developers with code level visibility to vulnerabilities

Cloud One File Security
- Detect and automatically remediate malicious content pushed to S3 buckets

Differentiators

- Cloud security simplified with Trend Micro Cloud One, a security services platform for organizations building in the cloud.
- Speed PCI-DSS and regulatory compliance with multiple security controls in one product.
- Defend against malware, and network threats with virtual patching, and Intrusion detection and prevention (IDS/IPS).

What are customers are saying

Silicon Overdrive

IT SERVICES AND SOFTWARE DEVELOPMENT

About Silicon Overdrive

Silicon Overdrive, established in 1995, helps customers to understand and uphold their portion of the shared responsibility model to ensure data and workloads are not at risk of being compromised. Based in South Africa, Silicon Overdrive provides IT managed services, support, and solutions.

TREND MICRO

About Trend Micro

As a global leader in cloud security, Trend Micro develops Internet content security and threat management solutions that make the world safe for businesses and consumers to exchange digital information.

Solution available in [AWS Marketplace]