Trend Micro™

DEEP SECURITY™ SOFTWARE

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

Virtualization has already transformed the data center and now, organizations are moving their workloads to cloud and container 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 containers.

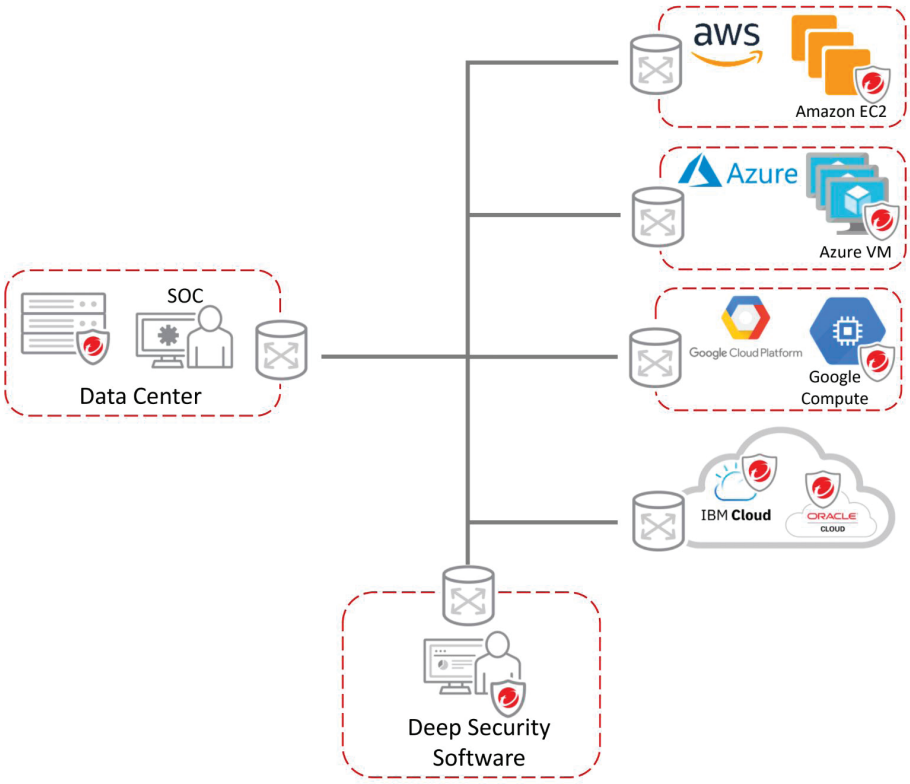
Trend Micro™ Deep Security™ software provides comprehensive security in a single solution that is purpose-built for virtual, cloud, and container environments. Deep Security allows for consistent security, regardless of the workload. It also provides a rich set of application programming interfaces (APIs), 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.



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.

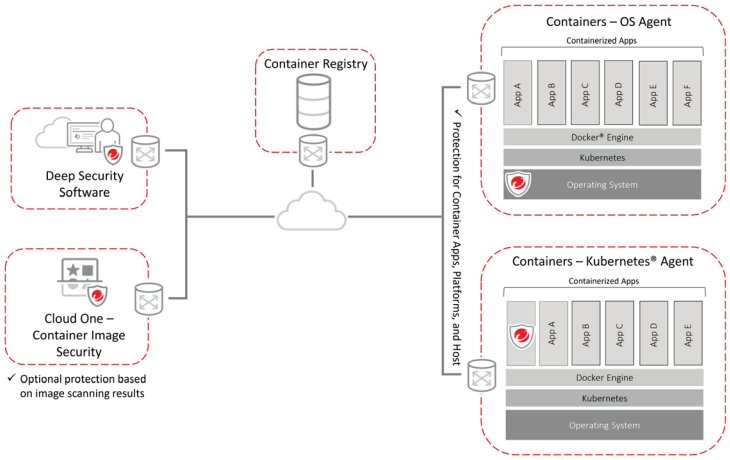
- **Accelerate compliance**

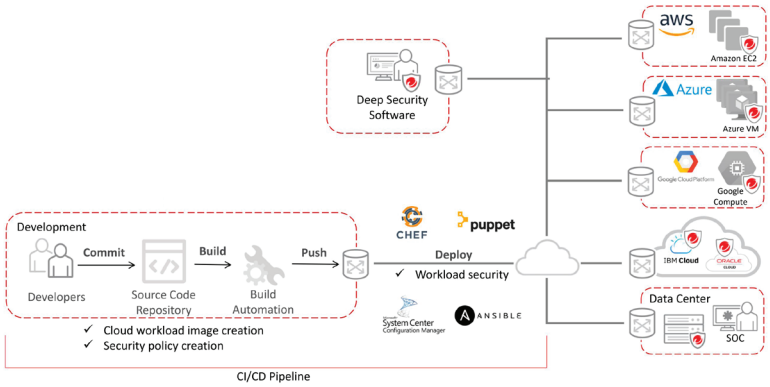
Demonstrate compliance with a number of regulatory requirements, including GDPR, PCI DSS, HIPAA, NIST, FedRAMP, and more.

TRUSTED HYBRID CLOUD SECURITY

Full Life Cycle Container Security

Deep Security delivers advanced runtime protection for containers. Layered security defends against attacks on the host, container platform (Docker®), orchestrator (Kubernetes®), containers themselves, and even the containerized applications. Designed with a rich set of APIs, Deep 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, Deep Security's container image scanning capabilities look for vulnerabilities, malware, secrets, and compliance in your build pipeline.



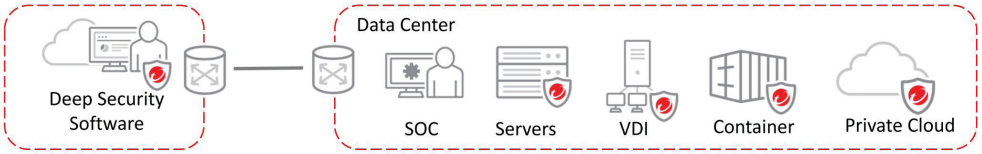


Automated Cloud Security

Deep Security works seamlessly to secure dynamic workloads in the cloud, with automated discovery of workloads across cloud providers, including AWS™, Microsoft® Azure™, Google Cloud™, and more. Deep 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 security to be integrated with your existing toolset for automated security deployment, policy management, health checks, compliance reporting, and more.

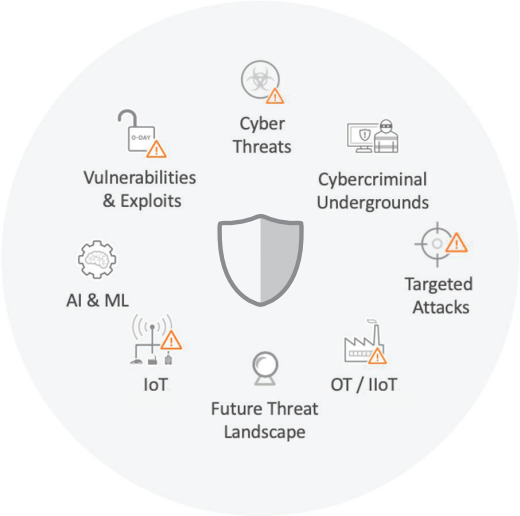
Virtualization and Data Center Security

Deep Security brings advanced protection to physical and virtual servers. Through automatic policy management, and in the case of VMware NSX-V® and VMware NSX-T™ hypervisor-integrated agentless security, Deep Security enables easy deployment and management of security across multiple environments. Deep 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, including an intrusion prevention system (IPS), integrity monitoring, machine learning, application control, and more.
- 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.
- Advanced threat detection and remediation of suspicious objects through sandbox analysis.
- Send alerts and trigger proactive prevention upon the detection of suspicious or malicious activity.
- Secure end-of-support systems with virtual patches delivered via 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 the Trend Micro™ Smart Protection Network™, powered by Trend Micro's market-leading threat research.

Support and Empower Incident Response Teams

- Support incident response with server endpoint detection and response (EDR) capabilities, including monitoring for indicators of attack and blocking of suspicious applications and processes.
- Integrate Deep Security with your security information and event management (SIEM) to analyze telemetry data for advanced threat hunting, indicators of compromise (IOC) sweeping, and security orchestration, automation and response (SOAR) tools for remediation and orchestration.
- When resources or time to investigate and remediate threats is limited, our MDR service, Trend Micro Managed XDR, includes many of these functions as a managed service.

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), orchestrator (Kubernetes), container itself, 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 objects 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 Trend Micro Cloud One™ – Container Image Security's advanced build-time and registry scanning, complementing Deep Security's runtime capabilities for protection across the container life cycle.
- Leverage Trend Micro's tight integration with leading cloud vendors, such as AWS, Azure, and Google Cloud, for unified visibility and protection across your multi-cloud environment.
- Enable service providers to offer customers a secure public cloud, isolated from other tenants via a multi-tenant architecture.
- Extend the benefits of microsegmentation in the software-defined data center and leverage Deep Security's integration with NSX-V to automatically detect and apply context-based policies.

Automate and Streamline Security

- Automate security deployment, policy management, health checks, and compliance reporting with Deep 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 security 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.
- Leverage proven technology certified to Common Criteria EAL 2 and FIPS 140-2 validated.
- Enforce compliance across the development pipeline with Container Image Scanning'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

System Requirements (Manager, Virtual Appliance, and Agents)

- Deep Security is available as a service and all management components are hosted and maintained by Trend Micro.
- Deep Security is also available as a software or a virtual appliance to run in your data center or cloud. System requirements are available at the following URL:

https://help.deepsecurity.trendmicro.com/12_0/on-premise/Get-Started/Install/system-requirements.html

Available as software as a service (SaaS)

- Trend Micro Cloud One™ – Workload Security is a SaaS offering with nearly identical functionality as Deep Security, but hosted by Trend Micro in the cloud—meaning 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 and automates and simplifies security operations for cloud instances. For more information visit our Workload Security page.

Supported Platforms (For Agent)

- 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://help.deepsecurity.trendmicro.com/12_0/on-premise/Manage-Components/Software-Updates/compatibility.html

DEEP SECURITY DETECTION AND PROTECTION CAPABILITIES

Network security tools detect and stop network attacks and shield 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.
- ***Web Reputation:***
  Blocks known-bad URLs and websites.
- ***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, services, and more for changes. In order 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.
- ***Sandbox Analysis:***
  Suspicious objects can be sent to the Trend Micro™ Deep Discovery™ network sandbox for detonation and extensive analysis to determine if it is malicious. A confirmation and rapid response update is then provided back to Deep Security for the appropriate response.

BUILT FOR SECURITY IN THE CLOUD

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

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)

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

Deep 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).

Deep Security Manager

Powerful, centralized management console: Role-based administration and multi-level policy inheritance allows for granular control. Task-automating features, such as recommendation scan, event tagging, and event-based tasks, simplify ongoing security administration. Multi-tenant architecture enables isolation of individual tenant policies and delegation of security management to tenant administrators.

Deep Security Virtual Appliance

Transparently enforces security policies on VMware vSphere® VMs. For VMware NSX® environments, this provides agentless anti-malware, web reputation, IPS, integrity monitoring, and firewall protection. A combined mode can be used where the virtual appliance is used for agentless anti-malware and integrity monitoring, and an agent for IPS, application control, firewall, web reputation, and log inspection.

Flexible pricing to meet cloud needs

- Protects thousands of customers and millions of servers globally
- Purchase and procure through AWS Marketplace or bring your own license to the Azure Marketplace
- Cost-effective, 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

Deep Security is part of the Trend Micro Hybrid Cloud Security solutions, which includes Trend Micro Cloud One™, a cloud security services platform, consisting of:

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

ZERO DAY INITIATIVE

Trend Micro ZDI detected 1449 vulnerabilities in 2018. This powers unmatched timeliness for virtual patches.

aws

Google Cloud

Azure

vmware®

Key Certifications and Alliances

- AWS Advanced Technology Partner
- AWS Container Competency Partner
- Common Criteria EAL 2+
- FIPS 140-2 validated
- HP Business Partnership
- Microsoft Application Development Gold Partner
- Microsoft Certified Partnership
- SAP Certified (NW-VSI 2.0 and HANA)
- VCE Vblock Validated
- Virtualization by VMware
- VMware Cloud on AWS Partner
- VMware Global Partner of the Year

TREND MICRO™

Securing Your Connected World