Trend Micro™

DEEP SECURITY™

Complete security for container, cloud, and virtualized data center environments

Virtualization has already transformed the data center and now organizations are moving their workloads to the 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 you meet compliance requirements and have security across all of your workloads, whether physical, virtual, cloud, or containerized.

Trend Micro™ Deep Security™ 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.

BE POWERFUL
Protect against vulnerabilities, malware, and unauthorized change with the broadest range of security capabilities

GET STREAMLINED
Consistent protection and visibility, optimized for every part of your hybrid cloud

GO AUTOMATED
Connected security that can be integrated into Dev and Ops processes to ensure adoption

BUILD SECURE
Smart security controls that ensure you meet security and compliance requirements from the first build

SHIP FAST
Security that is connected through automation and integration in your continuous integration/ continuous deployment (CI/CD) pipeline

RUN ANYWHERE
Security that is optimized for the place that best suits your application

Key Business Issues

Automated protection
Automate security using a rich set of RESTful APIs and cloud templates to remove manual security processes and reduce operational costs.

Unified security
Deploy and consolidate security across your physical, virtual, multi-cloud, and containerized 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

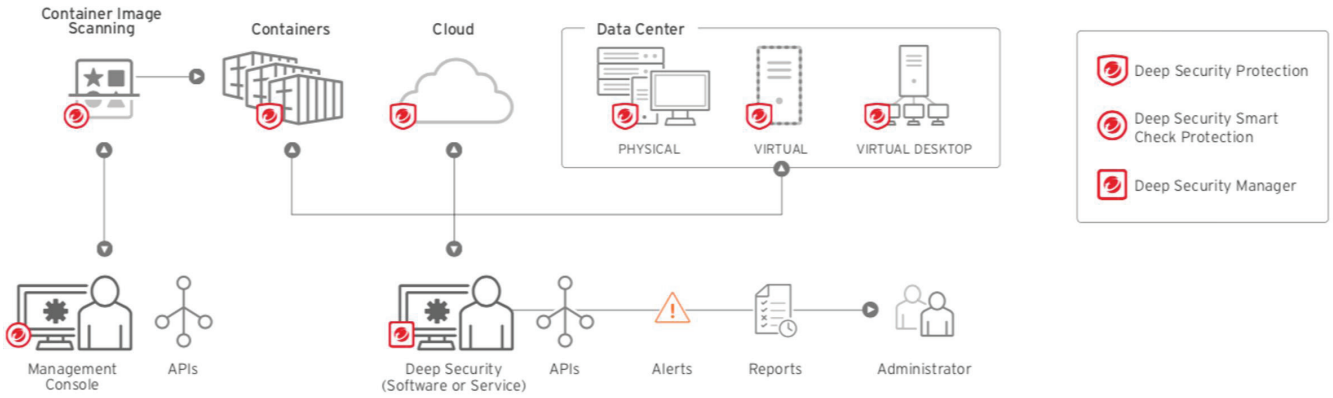
Deep Security delivers advanced runtime protection for containers. Layered security defends against attacks on the host, the container platform (Docker®), the orchestrator (Kubernetes®), the containers themselves, and even the containerized applications. Designed with a rich set of APIs, Deep Security allows IT Security to protect containers with automated processes for critical security controls. DevOps can leverage security as code by baking security into the CI/CD pipeline, reducing the friction that comes with applying security in rapidly changing and evolving infrastructures. With Trend Micro™ Deep Security™ Smart Check's build pipeline image scanning, Deep Security provides full protection across the container life cycle.

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. RESTful APIs allow for integrated security 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, enabling easy deployment and management of security across multiple environments through automatic policy management and in the case of VMware®, hypervisor-integrated agentless security. 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.



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 command and control (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 is limited, benefit from Trend Micro's Managed Detection and Response (MDR) service, providing these capabilities 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, the 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 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 Deep Security Smart Check'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 VMware 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 Deep Security Smart Check's build-time and registry scanning for policy compliance.

DEEP SECURITY DETECTION & 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 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 obfuscated, 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—and 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.
- ***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

sumologic | ANSIBLE | |

SWIMLANE | now | DEMISTO | splunk>

The Deep Security Scanner is a module that integrates with and protects SAP systems by integrating with the SAP NetWeaver® virus scan interface.

SAP Partner

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, 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 and 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.

Global Threat Intelligence

Deep Security integrates with the Smart Protection Network to deliver real-time protection from emerging threats by continuously evaluating and correlating global threat and reputation intelligence for websites, email sources, and files.

"Having a security partner like Trend Micro, that keeps up with modern technologies and advances 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

ZERO DAY INITIATIVE

Trend Micro ZDI disclosed 1,449 vulnerabilities in 2018. This powers unmatched timelines for virtual patches.

SYSTEM REQUIREMENTS (Software as a Service (SaaS), 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/11_3/on-premise/Get-Started/Install/system-requirements.html**

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/11_3/on-premise/Manage-Components/Software-Updates/compatibility.html**

DEEP SECURITY AS A SERVICE (DSaaS)

DSaaS gives you the proven protection of Deep Security without all the work. As a service deployment, we do the heavy lifting for you. We manage regular product and kernel updates, set up and maintain the security database, and administer the Deep Security manager. Our cloud-based security offering enables quick setup, and automates and simplifies security operations for cloud instances.

Key Benefits

- **Fast**: Start securing workloads in minutes
- **Cost-effective**: Usage-based pricing starting at $0.01/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 Marketplace to protect multi-cloud environments

Flexible pricing to meet cloud needs

DSaaS usage-based pricing:

AWS 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

POWERED BY XGEN™ SECURITY

Deep Security is part of the Trend Micro Hybrid Cloud Security solution, powered by XGen.

aws marketplace

Azure

Google Cloud

vmware

docker

kubernetes

Key certifications and alliances

- AWS Advanced Technology Partner
- AWS Container Competency Partner
- Common Criteria EAL 2+
- FIPS 140-2 validated
- ISO 27001
- PCI DSS
- 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