Trend Micro

DEEP SECURITY AS A SERVICE

Agile Security Built for the Cloud

Organizations are embracing the economic and operational benefits of cloud computing, turning to leading cloud providers including Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, and others. In the cloud, security is a shared responsibility. The cloud provider is responsible for the security of the physical and network infrastructure up to the hypervisor layer. It's up to you to protect what you put in the cloud—the workloads—including operating systems, service configuration, applications, and data.

Built on Trend Micro's industry-leading Hybrid Cloud Security solution, powered by XGen™, **Trend Micro™ Deep Security™ as a Service** is designed to augment cloud provider security with complete protection for cloud workloads. Deep Security provides a complete suite of security capabilities including intrusion detection and prevention, firewall, malware prevention with web reputation, predictive machine learning, sandbox analysis, integrity monitoring, log inspection, and multi-platform application control.

Deep Security as a Service 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 and Azure Marketplaces to protect multi-cloud environments

SIMPLIFY SECURITY MANAGEMENT

- Reduces resources needed for set up and management
- Simplifies purchasing and management with multiple security controls in one product
- Lowers management costs by automating repetitive and resource-intensive security tasks

PREVENT DATA BREACHES AND BUSINESS DISRUPTIONS

- Immediately protects against vulnerabilities like Shellshock, Heartbleed , or WannaCry
- Blocks malware, including ransomware, that attempts to evade detection
- Locks down servers so that no unauthorized applications can run
- Ensures cloud servers only communicate with expected systems and safe domains
- Detects and alerts you of suspicious or malicious activity

ACHIEVE COST-EFFECTIVE COMPLIANCE

- Addresses major compliance requirements for PCI DSS, as well as HIPAA, NIST, SANS, and SSAE 16 with one solution
- Provides detailed, auditable reports that document prevented attacks and policy compliance status
- Reduces the preparation time and effort required to support audits

KEY FEATURES

Intrusion detection and prevention

- Proactively protects against known and zero-day attacks by shielding known vulnerabilities
- Examines all incoming and outgoing traffic for protocol deviations, policy violations, or content that signals an attack
- Virtual patching helps compliance with major regulations like PCI DSS, HIPAA, etc.
- Defends against SQL injection, cross-site scripting, and other web application vulnerabilities
- Provides increased visibility into, or control over applications accessing the network

Malware prevention

- Protects your workloads against malicious software with advanced techniques like predictive machine learning
- Isolates malware to protect instances from sophisticated attacks, including ransomware
- Provides detection of suspicious activity or unauthorized changes and the ability to quarantine and recover quickly with behavioral monitoring
- Submits suspicious objects to Trend Micro™ Deep Discovery™ Analyzer for sandbox analysis

Multi-platform application control

- Increased visibility and protection for Windows and Linux servers
- Gives administrators the ability to lock down servers so that no new applications can run without being whitelisted
- Increases visibility into applications running on a given system and detecting and blocking unauthorized software, such as malicious attacks like ransomware
- Scans a server and determines what applications are currently on that machine
- Increases operational control and stability, allowing administrators to determine if new applications can be added and safely run

Integrity monitoring

- Monitors and tracks system changes and reports malicious and unexpected changes in real time
- Event tagging automatically replicates actions for similar events

Web reputation

- Integrates with Trend Micro™ Smart Protection Network™ to prevent communication with known Command and Control servers

Bidirectional firewall

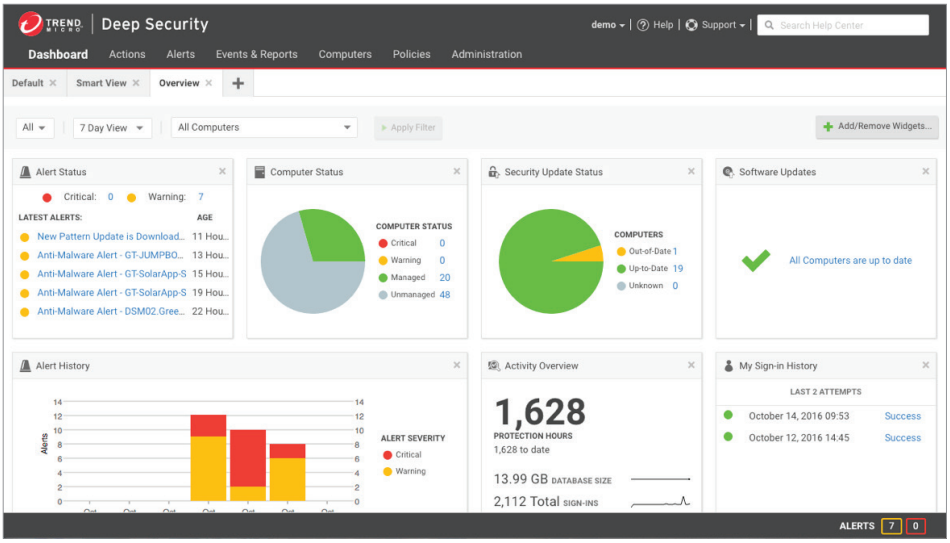
- Decreases the attack surface by creating a firewall perimeter to block attacks
- Limits communication to only the ports and protocols necessary
- Centrally manages server firewall policy, including templates for common server types

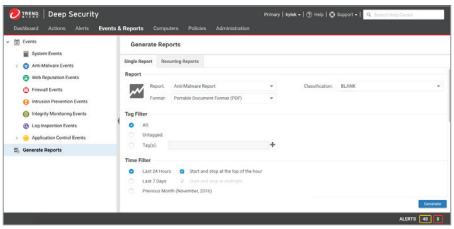
Log inspection

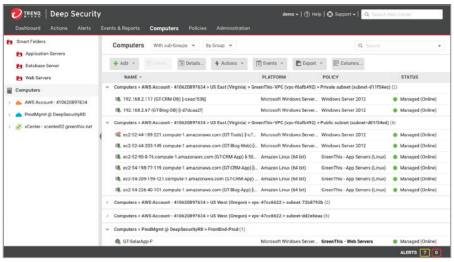
- Collects and analyzes operating system and application logs for suspicious behavior, security events, and administrative events
- Assists compliance (PCI DSS) by identifying of important security events
- Forwards events to SIEM system or centralized logging server for correlation, reporting, and archiving

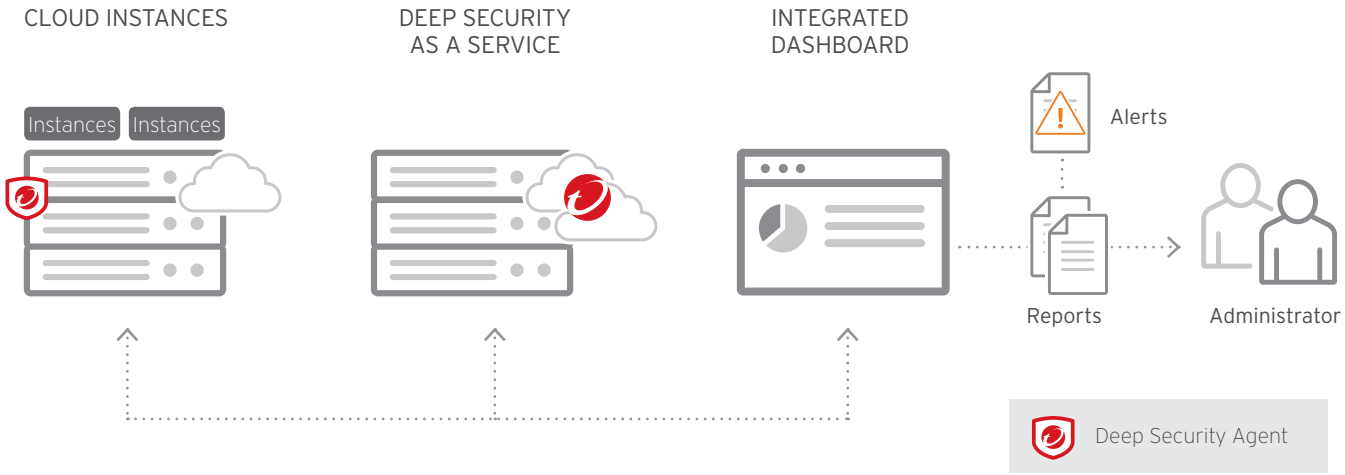
CLEAR CONTROL AT YOUR FINGERTIPS

- Enables policy-driven management and administration
- Customizable dashboard enables users to see the health of their security environment at a glance
- Customizable policy templates allow users to enable and disable security controls on the fly based on rules they assigned
- Provides immediate notification of events or activities that may require immediate attention (Logging Alert)









ELASTIC, SEAMLESS, AND STRESS-FREE

- Designed to seamlessly integrate with virtual, cloud, and container environments for fast and easy deployment
- Works with industry-leading cloud management tools such as Chef, Puppet, SaltStack, Ansible, and others
- The AutoSync feature detects new instances and provides detailed information that can be used to automatically set security policy without administrative intervention

BUILT FOR SECURITY IN THE CLOUD

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

Linux Windows SUSE redhat CentOS ubuntu

And compatibility with configuration management tools:

Chef puppet labs OpsWorks SALTSTACK ANSIBLE

Deep Security as a Service helps you resolve key business issues

Virtual patching
Shield vulnerabilities before they can be exploited and eliminate the operational pains of emergency patching, frequent patch cycles, and costly system downtime

Zero-day security
Protection against zero-day vulnerabilities while minimizing operational impact from resource inefficiencies and emergency patching

Compliance
Achieve and prove compliance with a number of regulatory requirements for PCI DSS, HIPAA, SANS, NIST, SSAE 16, and more

Integrated security
Shift from multiple point products to one trusted, complete security service

SUPPORTED PLATFORMS
• Microsoft Windows (32-bit/64-bit) • Amazon Linux AMI (32-bit/64-bit) • Ubuntu (64-bit) • CentOS 5, 6, 7 • Oracle Linux • Cloud Linux 5, 6 • Red Hat® Enterprise 5, 6, 7 (32-bit/64-bit) • SUSE® Enterprise 10, 11 (32-bit/64-bit)

Key certifications and alliances

- AWS SaaS Partner and Security Competency
- Microsoft Azure Certified Partner
- Level 1 PCI DSS Certified Service Provider
- PCI Suitability Testing for HIPS (NSS Labs)
- Certified Red Hat Ready

DEEP SECURITY AS A SERVICE FITS HOW YOU USE THE CLOUD

Pay only for what you use with **Trend Micro Deep Security as a Service**.
Get complete protection for your cloud workloads starting at only $0.01 per hour - with no long term commitments or minimum fees.

Flexible pricing to meet cloud needs:

Deep Security as a Service 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

Requires use of the Deep Security Cloud Connector (included). Price is $0.06/hour for unknown instance sizes.

AWS Marketplace:

Leverage the effortless deployment of Deep Security as a Service while keeping payments on your **AWS** bill.

Deep Security is available as software, as a service, or from the Marketplaces of leading Cloud providers like AWS and Azure.

POWERED BY XGEN™ SECURITY

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

Built for leading cloud providers

amazon web services | Partner Network
ADVANCED TECHNOLOGY PARTNER
SECURITY COMPETENCY

Microsoft Azure

vmware®

TREND MICRO™

Securing Your Journey to the Cloud