Business Challenges

Many companies look to the cloud for new ways to innovate that allow for greater experimentation, customer engagement, and differentiation from competitors. However, the growth in cloud computing capabilities and services has driven more data into data centers where traditional IT security measures cannot reach. Realizing the full benefits of the cloud requires companies to:

• Prevent cyberattacks and data breaches that can erode the business’s reputation, customer relationships, and future profits.
• Implement strong data controls in the cloud without complicating user workflows.

IT Challenges

Infrastructure and application security can be one of the most complex elements of IT operations. In the cloud, a high number of interconnected systems across a wide range of vendors makes it difficult to have good visibility into what's going on and what new threats may have been identified in the wild. Providing a robust security infrastructure depends on IT’s ability to:

• Support enhanced assessment and governance tasks, and enforce security baselines, to cover against a broad range of cloud threats.
• Identify optimizations to OS security configurations and spot potential security vulnerabilities at the OS and software level.
• Simplify security operations with consolidated views and management across the environment.

Solution

With Deep Security as a Service, we do a lot of the work for you. Meet and maintain compliance needs with a single tool that’s also PCI DSS Level 1 certified. Deep Security integrates protection into your DevOps practice with full API, scriptable components, or central UI, baking security into your AWS workloads. Automated application control, host-based IPS and container protection support continuous application change so security won’t slow you down. Whether you’re building the next new application or planning your datacenter migration to AWS, you need cloud security that won’t get in your way.
Better Together
Trend Micro Deep Security is optimized for AWS to seamlessly protect both cloud and hybrid environments and containers, ensuring you have a consistent security solution with proactive policies across physical, virtual and cloud environments. Trend Micro’s tight integration with AWS reduces cost and complexity, making it faster and easier for you to adhere to your part of the shared responsibility model.

Trend Micro is an AWS Security Competency Partner with automated security controls that integrate into operations and processes, providing a scalable, automated security solution that won’t slow you down. With support for AWS Security services like Amazon GuardDuty, Amazon Macie and AWS WAF, Trend Micro partners with AWS to give our customers the tools to transform their business.

Product Highlights

Meet your shared security responsibility
Deep Security augments AWS security controls to keep your workloads safe and help you meet compliance requirements.

Automate security across hybrid environments and containers
With powerful, automated security capabilities for hybrid environments, including the fastest host-based IPS, broad container protection and AWS API integrations, Deep Security is built to scale with your cloud projects no matter where they live.

Prevent breaches with proactive security
Instantly shield against zero-day vulnerabilities with virtual patching. Intrusion prevention (IPS) prevents breaches by blocking network intrusions and vulnerability exploitation. The lightweight Deep Security agent is optimized for AWS, ensuring instant protection your workloads without slowing you down.

Accelerate compliance and consolidate tools (PCI DSS, HIPAA, etc)
Deep Security accelerates compliance by augmenting AWS security with multiple capabilities that address key PCI DSS requirements – and you can manage it all in a single console vs trying to integrate and consolidate point products.

Scale cloud workloads and automate security processes
With host-based security, you prevent security bottlenecks when scaling and provide customized protection for workloads. Deep Security is also fully scriptable and integrated with cloud management tools such as AWS CloudFormation, AWS OpsWorks, Chef, Puppet, SaltStack, and Ansible.

Uncover suspicious changes
Get alerts when unplanned changes, intrusions, or advanced malware attacks, including ransomware are happening on your systems. Suspicious events are highlighted in the dashboard so you can quickly evaluate if there is a threat — without sorting through thousands of logs.

Lock down servers across hybrid environments even when workloads are elastic, giving you flexibility to use application control in the cloud without the management headaches.
Deep Security Manager

A centralized web-based management console where you create and manage security policies, get alerts, and take preventive actions to protect workloads. The Manager integrates with Active Directory and can connect to leading SIEMs like Splunk and SumoLogic. Web services API available.

Deep Security Relay


Deep Security Agent

The enforcement point for all Deep Security functionality, this lightweight agent only includes the rules and policies needed for each workload, minimizing footprint and performance impact. Using a heartbeat, the agent communicates with the Deep Security Manager, pushing event logs and various other data points about the instance.
Database for Deep Security
Contains all persistent information that Deep Security Manager needs to operate, such as configuration details and event log information for each instance with a Deep Security agent installed.

Technical Specifications

The security capabilities offered by Deep Security can be enhanced by the following AWS services:

• AWS CloudFormation
• Amazon CloudWatch
• AWS CloudTrail
• Amazon VPC

AWS Security Services Integrations

• Amazon GuardDuty
• Amazon Web Application Firewall
• Amazon Inspector
• Amazon Macie

3rd party SIEM integrations for improved visibility, management and analytics

• SumoLogic
• Splunk
• ArcSight
• Amazon SNS

Orchestration tool integrations to automatically bake security into the development lifecycle:

• Chef
• Puppet
• PowerShell
• Saltstack

Broadest range of kernel support across Linux, CentOS, CloudLinux, Debian, Oracle Linux, RedHat, Suse and Ubuntu.

Deep Security protects your Docker hosts and containers running on Linux distributions:

• Identify, find, and protect Docker hosts within your deployment through the use of badges and smart folders
• Shield Docker hosts and containers from vulnerabilities to protect them against known and zero-day exploits by virtually patching new found vulnerabilities
• Provide real-time anti-malware detection for the file systems used on Docker hosts and within the containers
• Assert the integrity of the Docker host for continuous compliance and to protect your deployment

To support DevOps workflows, Deep Security offers APIs to automate, monitor, and manage security throughout the release lifecycle.

• Use deployment scripts to add and protect computers
• Automatically assign policies by AWS instance tags
• Schedule Deep Security to perform tasks
• Automatically perform tasks when a computer is added or changed
• Access events with Amazon SNS