Trend Micro Deep Security™

Proactive, host-based cloud security for seamless scaling and easy automation.

TREND MICRO

TREND MICRO DEEP SECURITY

The security you want.
The agility you need.

Host-based Intrusion Prevention and Detection (IPS/IDS)
Prevents exploitation of vulnerabilities like Shellshock and proactively protects workloads by inspecting network packets and dropping malicious or suspicious traffic.

Anti-malware (with Content filtering)
Protect Windows and Linux workloads from increasingly complex malware. Powered by the Trend Micro™ Smart Protection Network and consistently rated the best performing anti-virus solution by AV-TEST, we identify and remove malware and blacklist domains.

Firewall
This bi-directional host-based firewall helps you log and audit traffic for compliance reporting at the workload level, even for shortlived instances. This extra layer of instance-level protection limits communication to only the ports and protocols necessary.
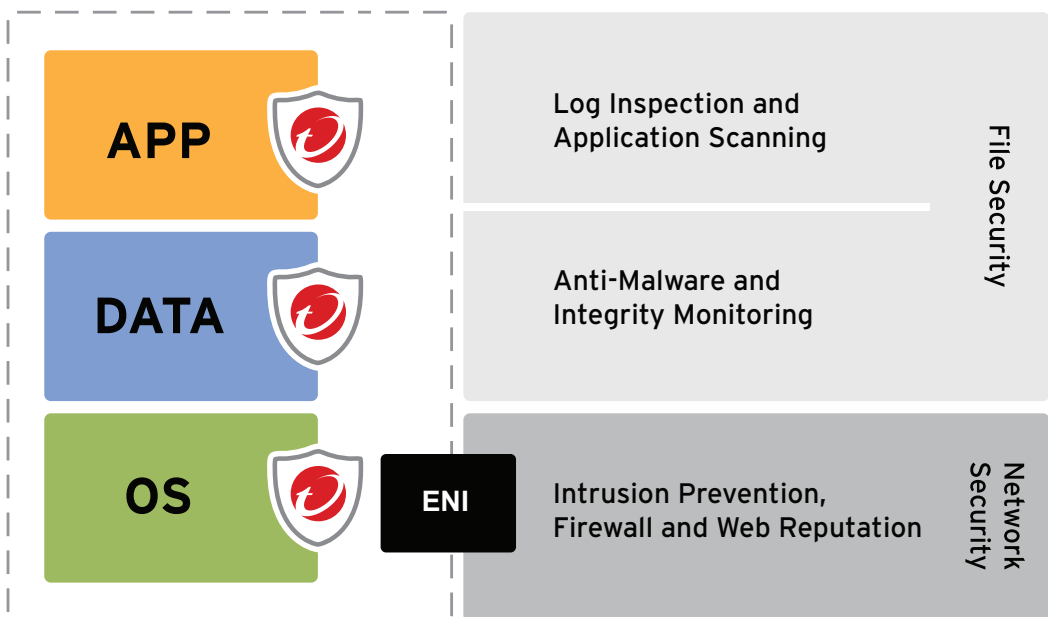
Integrity Monitoring
Host-based monitoring alerts you to unauthorized or out-of-policy changes across files, ports, registries, and more. Can also help meet compliance file and system monitoring requirements.

Log Inspection
Highlight potential security events in log entries from a variety of sources. It can also forward suspicious events to your SIEM or centralized logging server for correlation, reporting and archiving.

HOW IT PROTECTS

Deep Security provides comprehensive protection for your AWS workloads. It protects applications and data with a wide range of host-based security controls.

APP — Log Inspection and Application Scanning
DATA — Anti-Malware and Integrity Monitoring
OS — ENI — Intrusion Prevention, Firewall and Web Reputation

File Security
Network Security

REFERENCE ARCHITECTURE FOR HYBRID ENVIRONMENTS (AWS + ON PREMISE DATA CENTER)

AWS

Account A

AWS Region A
VPC — IGW
Public Subnet — Instances
Private Subnet — Instances
VPC- A

Public Subnet
Elastic LoadBalancer
SSL Pass-through for heartbeat listener

Security Group
Deep Security Manager Nodes with Co-located Deep Security Relay

Elastic IP
Remote Desktop Gateway
VPC NAT Gateway
Instances

Private Subnet
Security Group
Deep Security Manager Database
Instances
Availability Zone
Services VPC

AWS Region B
VPC — IGW
Public Subnet — Instances
Private Subnet — Instances
VPC- C

Account B

AWS Region C
VPC — IGW
Public Subnet — Instances
Private Subnet — Instances
VPC- D

VPC — IGW
Public Subnet — Instances
Private Subnet — Instances
VPC- B

AWS Direct Connect

Data Center

Non-Virtualized Workloads
Windows Hosts | Sun Solaris Hosts | HP-UX Hosts | AIX Hosts

Relay Group Data Center
Deep Security Relay 1 | Deep Security Relay 2

Virtualized Workloads
Windows VM | Linux VM

Network Communication Flows

From Solution Components (Outgoing – Internet)

80/443 — SMART Protection Network
Purpose: To provide Deep Security Agent access to Trend Micro Web Reputation and File Reputation Services (Optional, with a locally installed Smart Protection Server)

80/443 — Trend Micro Download Center & License Servers
Purpose: To provide Deep Security Manager access to license update server and to download software packages from Trend Micro Download center.

80/443 — Active Update Servers
Purpose: To provide Deep Security Relay access to Trend Micro Active Update servers to get new pattern and engine files and security updates.

From Solution Components (Incoming – Internal)

4120
Purpose: To provide Deep Security Agents access to the Deep Security Manager for heartbeat via the AWS Elastic Load Balancer (ELB).

4122
Purpose: To provide Deep Security Agents access to Deep Security Relays to get security updates and fetch plug-ins via the AWS Elastic Load Balancer (ELB).

443
Purpose: To provide Deep Security Relay access to the Deep Security Manager to download agent software plug-ins via the AWS Elastic Load Balancer (ELB).

1433
Purpose: To provide Deep Security Manager access to AWS RDS database for its data and configuration storage.

Admins — 443
Purpose: To provide Security Administrators access to the Deep Security Manager web console via the AWS Elastic Load Balancer (ELB).

DEEP SECURITY COMPONENTS

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. Web services API available.

Deep Security Relay
The Deep Security relay provides updates of signatures and threat intelligence from the Trend Micro Global Update Server to each Deep Security agent.

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.

DOWNLOAD THIS POSTER
www.trendmicro.com/aws