Deep Security

Pipeline Management

- Chef
- Puppet
- Ansible
- Other CM tools

- ✓ Works with industry leading pipeline management and deployment tools such as Jenkins, Chef, Puppet, Ansible, SaltStack, Kubernetes, and PowerShell.
- ✓ Rich set of RESTful APIs enabling seamless security integration into existing pipelines.

Deep Security Solution Components

Deep Security Manager (Software, Marketplace, or as a Service)	Deep Security Agent	Deep Security Virtual Appliance	Deep Security Relay	Deep Security Database	Deep Security Smart Check Scanner	Smart Protection Network Services
Centralized web-based management console delivered as software or software as a service (SaaS). REST API also available.	Enforces the environment's security policy via a small software component deployed on the workload being protected.	A single virtual appliance, built for VMware environments to provide both Guest and Network Introspection Services by integrating with the VMware NSX Platform.	Provides distributed updates of signatures and threat intelligence from the Trend Micro Active Update Servers to each Deep Security agent.	Contains all persistent information such as configuration details and event log information for each workload with a Deep Security Agent installed.	Delivers automated build-time and registry image scanning with detection for malware, vulnerabilities, secrets, and policy compliance.	Delivers real-time protection from emerging threats by continuously evaluating and correlating global threat intelligence.

APIs & Automation

- REST

- ✓ Extends visibility and protection of workloads into customer and partner environments.
- ✓ Automate discovery of workloads across cloud providers including AWS, Microsoft Azure, Google Cloud, and more.
- ✓ Standards based SOAP & REST interfaces can be used with any development environment e.g. Java, C#, C ++.NET, Python, Ruby, PHP, Perl and others.
- ✓ Designed for DevOps and automation to integrate security into your Continuous Integration Continuous Delivery (CI/CD) pipeline.
- ✓ Automate security deployment, policy management, health checks, and compliance reporting with Deep Security REST APIs.
- ✓ Comprehensive Automation Help Center providing best practices, code samples, SDK, and API documentation to enable security automation.

Event Management

- Splunk
- Sumo Logic
- IBM QRadar
- Other SIEM Providers

- ✓ Integrates with security information and event management (SIEM) tools to analyze telemetry data for advanced threat hunting and IOC sweeping.
- ✓ Connects with security orchestration, automation, and response (SOAR) tools for remediation and orchestration.
- ✓ Streamline threat and information sharing via security tools, infrastructure provider offerings, and Trend Micro Connected Threat Defense.
- ✓ Industry Standard Security Event Format supports CEF, LEEF 2.0 with secure delivery using TLS.
- ✓ Integration with Amazon SNS to facilitate monitoring activities and improve visibility.

XGen™ Security Capabilities

Malware Prevention

- Anti-Malware & Content Filtering
- Behavioral Analysis & Machine Learning
- Sandbox Analysis

- ✓ Detect & stop ransomware and crypto-mining
- ✓ Advanced machine learning and behavioral threat analysis

Network Security

- Intrusion Prevention
- Firewall
- Vulnerability Scanning

- ✓ Protect against OS & application vulnerabilities with virtual patching
- ✓ Immediate, automated protection against zero-day vulnerabilities and exploits

System Security

- Application Control
- Integrity Monitoring
- Log Inspection

- ✓ Track new software installs and changes
- ✓ Lock down malicious files
- ✓ Actionable intelligence from log files delivered through a single event
- ✓ Discover suspicious system changes

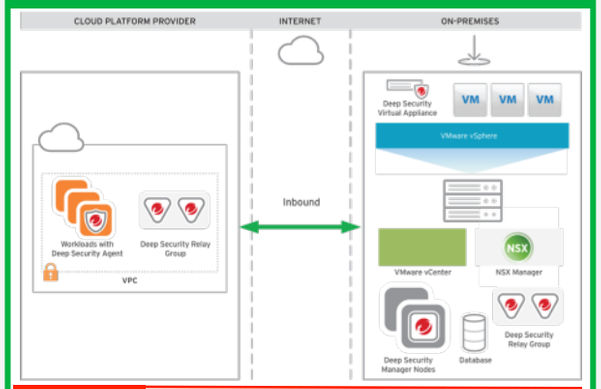
Detection & Response

- EDR
- XDR
- Managed XDR

- ✓ Advanced detection, response, and investigation capabilities (EDR), includes the ability to detect indicators of attack (IOAs) and lock down suspicious applications and processes.
- ✓ Detect and respond to threats across multiple layers (endpoints, network security, and server security) and gain greater context with XDR.
- ✓ The Managed XDR service collects, correlates, and prioritizes alerts and system information to determine a full root cause analysis. Our knowledgeable threat experts investigate on behalf of you and provide a full remediation plan.

Computing Environments Protected with Deep Security

Data Center + VMware



Solution Components

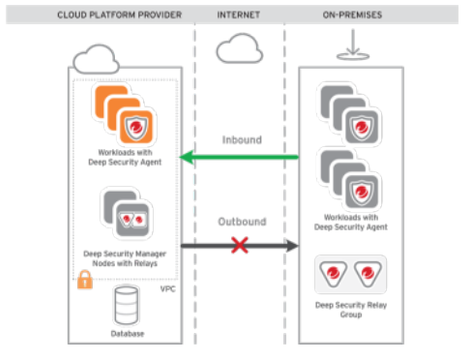
- Deploy Deep Security Manager on-premises i.e. close to your VMware vSphere virtualized environment.
- Deploy multi-node Manager setup for high availability and scalability.
- Use either MS SQL, Oracle DB, or PostgreSQL to store Deep Security data.
- Optionally use separate Deep Security Relay Groups for keeping update traffic local to each site i.e. Relay Group for cloud based workloads and separate Relay Group for On-Premises workloads.
- Use Deep Security VMware vSphere connector for vCenter to import your virtual machines into Deep Security and to provide continuous discovery.
- Use Deep Security Virtual Appliance to protect your virtualized environment and use Deep Security Agent on your virtual machines in the cloud.

Network Connectivity

- Establish a dedicated network connection from your on-premises to your public cloud provider.*
- Use Agent Initiated communication mode for Manager and Agent communication.
- Use Bi-Directional Communication mode for Manager and Deep Security Virtual Appliance communication.
- Allow Communication path from Deep Security Manager to VMware vCenter Server and NSX Manager.
- Allow Deep Security Manager, Deep Security Relays, Deep Security Virtual Appliance, and Deep Security Agent internet access for software and security updates.

* Alternately either use an IPSec (VPN) connectivity to connect On-Premises to your public cloud provider or make Deep Security Manager accessible over the Internet.

Cloud



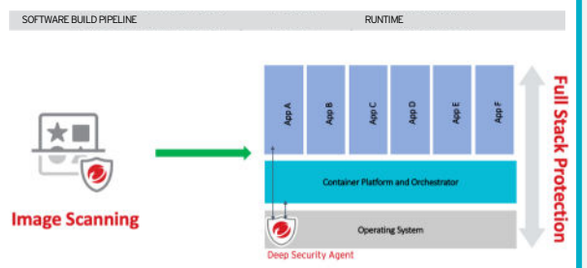
Solution Components

- 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.
- Use respective cloud vendor templates for quick start deployment.
- Deploy multi-node setup with co-located Deep Security Relays for high availability and scalability.
- Use cloud platform supported databases to store Deep Security data.
- Optionally use two Deep Security Relay Groups for keeping update traffic local to each site i.e. one Relay Group for cloud workloads and one Relay Group for On-Premises workloads.
- Use Deep Security cloud connectors to import your virtual machines into Deep Security and to provide continuous discovery.
- Combined benefit of security software-as-a-service (SaaS) with the convenience of consolidated cloud billing and usage-based pricing.

Network Connectivity

- Use Deep Security Manager nodes with Public DNS to make them accessible over the internet.
- Use Agent Initiated communication mode for Manager and Agent communication.
- Allow Deep Security Manager, Deep Security Relays, and Deep Security Agents internet access for software and security updates.
- No network access is required from Azure to On-premises.
- Use VPC/Network Security Group rules to allow required communication flow between components.

Build Pipeline & Containers



Solution Components

- Ensure full life cycle 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, IPS, and log inspection capabilities.
  - Protect runtime containers through container vulnerability shielding (via IPS), real-time malware protection, and east-west container traffic inspection.
  - Build pipeline scanning for malware, vulnerabilities, secrets and keys, and compliance violations
- 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.
- Designed with a rich set of APIs, Deep Security allows IT Security to protect containers with automated processes for critical security controls.

Trend Micro Deep Security is a fully automated solution that provides complete detection, investigation, and protection across the hybrid and multi-cloud infrastructure, securing workloads & applications no matter where they reside across virtual servers, public or private clouds, containers at runtime, or in the software build pipeline and across 1,000s of supported OS platforms.