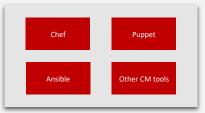
Deep Security



Pipeline Management

Deep Security Solution Components

APIs & Automation



- Works with industry leading pipeline managemen 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.

Centralized web-based delivered as software or software as a service (SaaS). REST API

Enforces the vironment'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 Delivers automated build-time and registry configuration details and image scanning with detection for malware, event log information for vulnerabilities, secrets, each workload with a Deep Security Agent

Delivers real-time protection from emerging threats by continuously evaluating and correlating global threat intelligence.

- 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

- 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
- Integration with Amazon SNS to facilitate monitoring activities and improve

XGenTM Security Capabilities

Malware Prevention

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

Network Security

- Protect against OS & application vulnerabilities
- Immediate, automated protection against zeroday vulnerabilities and exploits

System Security

- 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



- 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

