Trellix

Trellix Network Security

Effective protection against cyberbreaches for midsize to large organizations

Overview

Users

Trellix
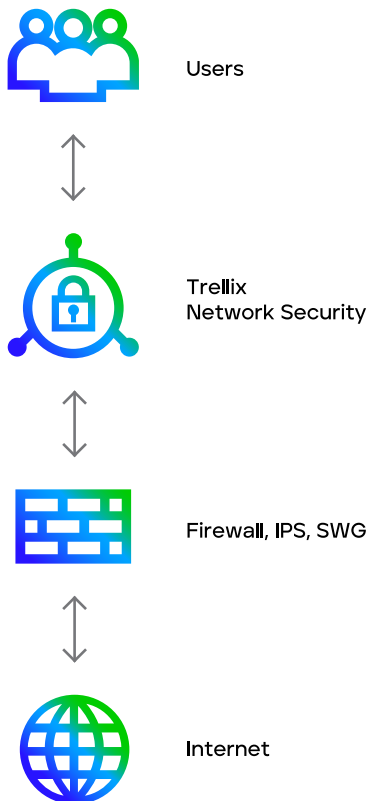Network Security

Firewall, IPS, SWG

Internet

Figure 1. Typical configuration of Network Security solutions

Trellix Network Security is an effective cyberthreat protection solution that helps your organization minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted, and other evasive attacks hiding in internet traffic. It facilitates efficient resolution of detected security incidents in minutes with concrete evidence, actionable intelligence, and response workflow integration.

With Network Security, your organization is effectively protected against today's threats, whether they:

- Exploit Microsoft Windows, Apple OS X operating systems, or application vulnerabilities
- Are directed at the headquarters or branch offices
- Are hidden in a large volume of inbound internet traffic that must be inspected in real time

At the core of Network Security are the Trellix Multi-Vector Virtual Execution (MVX) and dynamic machine learning and artificial intelligence (AI) technologies.

MVX is a signature-less, dynamic analysis engine that inspects suspicious network traffic to identify attacks that evade traditional signature- and policy-based defenses. Multiple machine learning, AI, and correlation engines represent a collection of contextual dynamic rules engines that detect and block malicious activity in real time and retroactively, based on the latest machine, attacker, and victim intelligence. Network Security also includes intrusion prevention system (IPS) technology to detect common attacks using conventional signature matching.

Trellix Network Security is available in a variety of form factors and deployments and performance options. It's typically placed in the path of internet traffic behind traditional network security appliances such as next-generation firewalls, IPS, and secure web gateways (SWGs) to detect both known and unknown attacks with high accuracy and few false positives, while facilitating an efficient response for each alert.

Technical advantages

Accurate and actionable threat detection and insights

Network Security uses multiple analysis techniques to detect attacks with high accuracy and a low rate of false alerts.

- The MVX engine detects zero-day, multiflow, and other evasive attacks with dynamic, signature-less analysis in a safe, virtual environment. It stops infection and compromise phases of the cyberattack kill chain by identifying never-before-seen exploits and malware.

- Multiple dynamic machine learning, AI, and correlation engines detect and block obfuscated, targeted, and other customized attacks with contextual, rule-based analysis from real-time insights gathered on the front lines from thousands of hours of incident response experience. Network Security stops the infection, compromise, and intrusion phases of the cyberattack kill chain by identifying malicious exploits, malware, phishing attacks, and command and control callbacks. It also extracts

and submits suspicious network traffic to the MVX engine for a definitive verdict analysis. In addition to client-side protection, engines support server-side detection, lateral movement detection, and detection of post-exploitation traffic.

- Alerts generated by Network Security include concrete real-time evidence to quickly respond to, prioritize, and contain targeted and newly discovered attacks. When operating in Evidence Collector mode, Network Security generates Layer 7 metadata, which is sent to Trellix Helix for analysis to provide further security context for your SOC team. In addition, detected threats can also be mapped to the MITRE ATT&CK framework for contextual evidence.

Detection

Capabilities	Benefits
Accurate detection of advanced, targeted, and other evasive attacks	Minimizes risk of costly cyberbreaches
Visibility and detection of post-breach lateral movement	Decreases time to detect post-breach activities and reduces attacker dwell time
Modular and scalable security architecture	Provides investment protection and supports business growth
Consistent level of protection for multi-OS environments and all internet access points	Creates a strong defense across the entire organization for all types of devices
Integrated, distributed, physical, virtual, on-premises, and cloud deployment options	Offers flexibility to align with organizational preferences and resources
Multivector correlation with email and content security	Provides visibility across a wider attack surface

Prevention

Capabilities	Benefits
Immediate blocking of attacks at line rates from 250 Mbps to 10 Gbps	Gives real-time protection against evasive attacks
Visibility into encrypted traffic	Delivers optional built-in TLS 1.3 decryption support on appliances without an additional license fee

Response

Capabilities	Benefits
Low rate of false alerts, riskware categorization, and mapping to MITRE ATT&CK framework	Reduces operational cost of triaging unreliable alerts
Pivot to investigation and alert validation, endpoint containment, and incident response	Automates and simplifies security workflows
Execution evidence and actionable threat intelligence	Accelerates prioritization and resolution of detected security incidents

Comprehensive visibility into suspicious lateral movements

Network Security includes the SmartVision advanced correlation and analytics engine that detects suspicious lateral internal network traffic across the entire network, from the data center to remote branch office locations. With more than 180 rules for lateral movement detection, SmartVision provides full kill-chain detection that targets east-west, server-facing deployments.

SmartVision also includes a machine learning framework with data-exfiltration detection, JA3 detection for identifying encrypted communication, web shell detection (visibility into attacks on web servers), and detection of malware lateral movement. It provides Layer 7 context around every real-time alert and maps adversarial techniques based on the MITRE ATT&CK framework.

Immediate and resilient protection

Network Security offers flexible deployment modes, including out-of-band monitoring via test access point (TAP)/switched port analyzer (SPAN), inline monitoring, or inline active blocking. Inline blocking mode automatically blocks inbound exploits and malware and outbound multiprotocol callbacks. In inline monitoring mode, your organization decides how to respond to generated alerts. In out-of-band prevention mode, Network Security issues TCP resets for out-of-band blocking of TCP or HTTP connections.

Selected models offer an active high-availability option to provide resilience in case of network or device failures.

Wide attack surface coverage

Network Security delivers a consistent level of protection for today's diverse network environments, providing:

- Support for most common Microsoft Windows, Apple Mac OS X, and Linux operating systems
- Analysis of over 160 different file types, including portable executables, active web content, archives, images, Java, Microsoft, and Adobe applications and multimedia
- Execution of suspicious network traffic against thousands of operating systems, service pack, IoT application type, and application version combinations
- Protection against advanced attacks and malware types that are difficult to detect via signatures: web shell uploads, existing web shells, ransomware, and cryptominers

Validated and prioritized alerts

In addition to detecting genuine attacks, MVX technology is also used to validate alerts detected by conventional signature-matching methods and to identify and prioritize critical threats. Your organization gets these efficiencies:

- IPS with MVX engine validation reduces the time required to triage signature-based detection that's traditionally prone to false alerts.
- Riskware categorization separates genuine breach attempts from undesirable but less malicious activity (such as adware and spyware) to prioritize alert response.

Response workflow integration

Network Security can be augmented in several ways to automate alert response workflows. For example:

- Trellix Central Management System correlates alerts from both Network Security and Trellix Email Security for a broader view of an attack and to set blocking rules that prevent the attack from spreading further.
- Trellix Network Forensics integrates with Network Security to provide detailed packet captures associated with an alert and enable in-depth investigations.
- Trellix Endpoint Security identifies, validates, and contains compromises detected by Network Security to simplify containment and remediation of affected endpoints.

Flexible deployment options

Network Security offers various deployment options to match your organization's needs and budget.

Integrated Network Security

Standalone, all-in-one hardware appliances with integrated MVX service secure an internet access point at a single site. Network Security is an easy-to-manage, clientless solution that deploys quickly without requiring rules, policies, or tuning.

Distributed Network Security

Extensible appliances with centrally shared MVX service secure internet access points within organizations using the following features and capabilities:

- **Network Smart Node** physical or virtual appliances analyze internet traffic to detect and block malicious traffic and submit suspicious activity over an encrypted connection to the MVX service for definitive verdict analysis.

- **MVX Smart Grid** on-premises, centrally located, elastic MVX service offers transparent scalability, built-in N+1 fault tolerance, and automated load balancing.

- **Trellix Cloud MVX** service subscription ensures privacy by analyzing traffic on the Network Smart Node; only suspicious objects are sent over an encrypted connection to the MVX service, where objects revealed as benign are discarded.

- **Protection options on-premises or in the cloud**, in addition to standalone and virtual appliances. Trellix offers Network Security in the public cloud with availability in both AWS and Azure.

Network Smart Nodes

Physical appliance

Cloud: AWS & Azure

Physical appliance (Remote site)

Virtual appliance (Remote site)

Central site
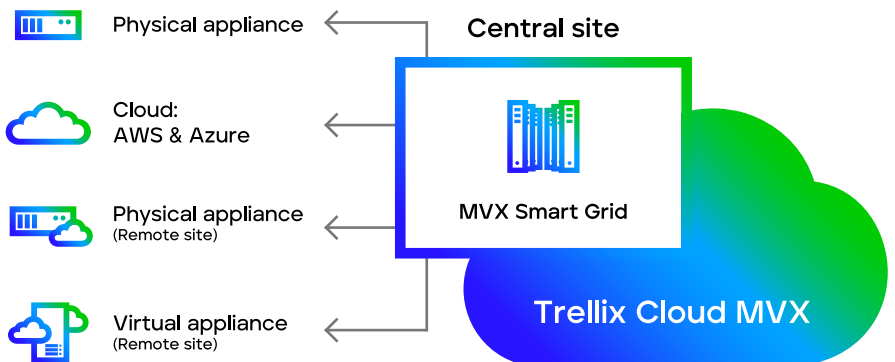
MVX Smart Grid

Trellix Cloud MVX

Figure 2. Distributed deployment models for Network Security

High performance and scalability

Trellix Network Security protects internet access points at line rate with performance options for a wide variety of branch and central office sizes.

The MVX Smart Grid and Trellix Cloud MVX scalable architecture allow the MVX service to support one Network Smart Node to thousands and scale seamlessly as needed.

MVX	Trellix analysis engines	IPS and riskware	Threat intellegence	SmartVision
Signatureless dynamic analysis engine	Intelligence-driven, rule-based analysis engines	Signature-based and non-critical malware engines	Correlation with Trellix and third-party threat data	Advanced engines that detect lateral attacker traffic

Figure 3. Modular components of Network Security

Response

Form factor	Performance
Integrated Network Security	50 Mbps to 5 Gbps
Physical Network Smart Node	50 Mbps to 10 Gbps
Virtual and public cloud Network Smart Node	50 Mbps to 8 Gbps

Business benefits

Designed to meet the needs of single-site and distributed multisite organizations, Trellix Network Security delivers several benefits.

Minimizes risk of cyberbreaches

Network Security is a highly effective cyberdefense solution that:

- Prevents intruders from breaking into an organization to steal valuable assets or disrupt business by stopping advanced, targeted, and other evasive attacks
- Stops attacks and contains intrusions faster with concrete evidence, actionable intelligence, inline blocking, and response workflow automation

- Eliminates weak points from an organization's cyberdefenses with consistent protection for various operating systems, application types, branches, and central sites

Short payback period

Network Security gives you a return on your investment in several ways:

- Focuses security team resources on real attacks to reduce operational expenses

- Optimizes capital spend with a shared MVX service and a large variety of performance points to right-size deployment to meet requirements

- Reduces future capital outlay with modular and extensible architecture

- Future-proofs security investment by scaling smoothly when the number of branches or the amount of internet traffic grows

- Protects existing investments by allowing cost-free migration from an integrated to a distributed deployment

Awards and certifications

The Network Security product portfolio has been awarded a number of industry and government awards and certifications:

- In 2022, Trellix received the Gold Globee Cyber Security Global Excellence Award for Network Detection and Response.

- In 2020, Trellix won first place in the Naval Information Warfare Systems Command (NAVWAR) Artificial Intelligence Cybersecurity Challenge.[1]

- In 2020 and 2021, KuppingerCole awarded Trellix the Leadership Compass for Network Detection and Response.[2]

- In 2020, Forrester recognized Trellix as a large vendor for Network Analysis and Visibility.[3]

- Network Security holds certifications including Common Criteria, FIPS 140-2, and SOC 2.

- Network Security has been a recipient of numerous awards from SANS Institute, SC magazine, CRN, and others.

- Network Security was the first security solution on the market to receive the US Department of Homeland Security SAFETY Act Certification.

1. Awarded to FireEye, now Trellix; U.S. Navy Office of Information, Naval Information Warfare Systems Command (NAVWAR) Awards FireEye First Place in Network Threat Detection Challenge, December 7, 2020

2. Awarded to FireEye, now Trellix; KuppingerCole, Leadership Compass Network Detection and Response, June 10, 2020

3. Recognition for FireEye, now Trellix; Forrester, Now Tech: Network Analysis and Visibility, Q2 2020, June 23, 2020

Trellix
6220 American Center Drive
San Jose, CA 95002
www.trellix.com

To learn more, visit trellix.com.

Trellix