Trellix Virtual Intrusion Prevention System

Complete threat detection and intrusion prevention for cloud networks

Key benefits

- Complete protection for private and public clouds (AWS, Azure, and OCI)
- Inline IPS/intrusion detection system (IDS) modes of operation
- True east-west traffic protection
- Uniform policy and management workflow
- Advanced inspection technologies protect against known and unknown threats
- High availability, disaster recovery, and load balancing for better performance
- Cloud license sharing for flexibility across private and public clouds
- Integrates with Trellix portfolio for device-to-cloud security
- Available at AWS Marketplace
- Available at Azure Marketplace

Overview

Trellix Virtual Intrusion Prevention System is a complete network threat detection and intrusion prevention system (IPS) built for the unique demands of private and public clouds. It quickly discovers and blocks sophisticated threats in cloud architectures with accuracy and simplicity, so you can protect your organization's workloads and restore compliance with confidence.

Our advanced technologies include signature-less detection, inline emulation, and signature-based vulnerability patching. In addition, streamlined workflows, support for autoscaling, flexible integration options, and simplified licensing allow your organization to easily manage and scale its security to meet existing and future needs.

Complete public cloud security

Public clouds offer convenience, cost savings, and the opportunity to shift infrastructure spending to an operational expense model. But they also introduce a new level of risk, where a vulnerability in publicly-accessible software could enable an attacker to puncture the cloud and exfiltrate sensitive information or accidentally expose customer data to other tenants using the same service. Trellix Virtual Intrusion Prevention System (vIPS) supports today's leading public cloud services, including Amazon Web Services (AWS), Microsoft Azure, and Oracle Cloud Infrastructure (OCI). It delivers complete threat visibility and protection for data passing through an internet gateway or server-to-server (east-west traffic).

Secure virtualized environments

Enterprises are rapidly adopting virtualized IT infrastructures, such as private and public clouds, where physical servers can simultaneously host multiple virtual machines (VMs) and virtualized workloads. The resulting inter-VM communication and instant migration, replication, and backup of these workloads have combined to dramatically increase east-west traffic inside private and public clouds, as well as software-defined data centers.

Adding to the chaos, the flexibility provided by network virtualization makes these escalating traffic flows dynamic and unpredictable. Trellix vIPS easily scales and adapts to keep up with constant changes and functions seamlessly with software-defined networking platforms that orchestrate these often short-lived VMs and workloads.

Agility in the private cloud

Trellix vIPS can be deployed as a virtual appliance on a VMware ESX server to protect virtual networks in a private cloud infrastructure. Available as an Open Virtualization Format image, the virtual appliance can inspect traffic between VMs on a particular ESX host and across different ESX hosts and physical networks.

Advanced threat prevention

Trellix vIPS is based on a next-generation inspection architecture designed to deliver deep inspection of virtual network traffic. It uses a combination of advanced inspection technologies—including full protocol analysis, threat reputation, behavior analysis, and advanced malware analysis—to detect and prevent known and unknown zero-day attacks on the network.

No single malware detection technology can prevent all attacks, which is why Trellix vIPS layers multiple signature and signature-less detection engines to help prevent unwanted malware from wreaking havoc in your clouds. It uses multiple inspection technologies, including inline emulation of browsers, JavaScript, Adobe files, botnet, malware callback detection, behavior-based distributed denial-of-service (DDoS) detection, and protection from advanced cross-site scripting and SQL injection attacks.

Trellix vIPS can also identify and block the stealthiest of files via integration with Trellix Intelligent Sandbox, where files are submitted for behavior analysis. It combines in-depth static code analysis, dynamic analysis (malware sandboxing), and machine learning to increase zero-day threat detection, including threats that use evasion techniques and ransomware. Trellix also provides native support for Snort signatures to detect and protect against malware.

Flexible cloud license sharing

Enterprise organizations often spread their IT resources and infrastructure across multiple clouds and platforms to support legacy applications, reduce dependency on a single vendor, and for system redundancy and cost savings. Licensing security solutions for virtualized environments can be complicated and expensive, as most vendors require the purchase of separate licenses for private and public clouds.

Trellix simplifies licensing and reduces costs through cloud license sharing, allowing your organization to share its Virtual Intrusion Prevention System licenses across a combination of public and private cloud platforms. Cloud license sharing provides flexibility and improves security by enabling your administrators to rapidly deliver east-west traffic protection and microsegmentation to virtual workloads wherever they reside, without the hassles of complex licensing and time-consuming procurement processes.

Streamlined workflows and analytics

Modern threats can generate large volumes of alerts, quickly outpacing a security operator's ability to prioritize and track them. If the response is too slow, real threats can slip by undetected. Trellix vIPS includes advanced analytics and actionable workflows that correlate multiple IPS alerts into a single actionable event, enabling your administrators to quickly identify relevant information. Integration with additional Trellix security solutions creates a truly comprehensive, connected network threat detection and mitigation platform.

Unified policy and management workflow

You can deploy vIPS as a virtual instance on VMware ESX servers and in AWS/Azure/OCI environments. This helps your administrators extend your on-premises security profile consistently across hybrid data centers as workloads shift to cloud platforms and manage them using a uniform management console and workflow. Trellix vIPS supports AWS Identity and Access Management, enabling your organization to easily and securely manage access to AWS services and resources based on permissions assigned to specific users and groups.

High availability, disaster recovery, and load balancing

Our vIPS automatically delivers uninterrupted control, protection, and performance via multiple methods. It provides high availability by proactively monitoring the environment. For example, a new controller instance is launched when an active controller becomes unavailable. In addition, a standby can be deployed for disaster recovery in AWS, Azure, and OCI environments.

Trellix vIPS also provides high availability for IPS sensors. If a sensor becomes unavailable, the auto-scaling capability automatically creates a new virtual IPS sensor for seamless, uninterrupted protection. And if network traffic increases, automatic load balancing across sensors ensures that performance is optimized. You can deploy additional sensors automatically to meet the required throughput performance.

Integrated security

Sophisticated attacks don't respect product boundaries and will quickly take advantage of any infrastructure gaps, especially between security products. Trellix vIPS seamlessly integrates across multiple security products and efficiently leverages data and workflows across solutions. This way, you get superior security and protection and an increased return on investment. Our vIPS integrates with many Trellix and third-party solutions to extend visibility, correlate threat information, and block malicious attacks.

Additional features

Advanced threat prevention

- Advanced malware protection
- Native inbound SSL inspection
- Microsoft 365 deep file inspection
- PDF JavaScript emulation engine (lightweight sandbox)
- Adobe Flash behavioral analysis engine
- Advanced evasion protection

Botnet and malware callback protection

- Domain name servers (DNS)/ domain generation algorithms (DGA)/fast flux callback detection
- DNS sinkholing
- Heuristic bot detection
- Multiple attack correlation
- Command and control database

Advanced intrusion prevention

- IP defragmentation and TCP stream reassembly
- Trellix, user-defined, and open-source signatures
- Host quarantine and rate limiting
- Inspection of virtual environments
- Denial-of-service (DoS) and DDoS prevention
- Allow/block lists in support of Structured Threat Information eXpression (STIX)
- Threshold and heuristic-based detection
- Host-based connection limiting
- Native support for Snort signatures
- Self-learning, profile-based detection

Trellix Global Threat Intelligence

- File reputation
- IP reputation
- URL/domain reputation
- Geolocation-based restricted access
- IP address-based access control

	Sensor type 1	Sensor type 2
Platform	VMware ESX	AWS Azure OCI
Virtual IPS sensor model	IPS-VM600	IPS-VM600-VSS
Type of virtual IPS deployment	Stand-alone	Distributed
AWS support	No	Yes
Azure support	No	Yes
OCI support	No	Yes
Number of logical CPUs	4	4
Memory required	8 GB	8 GB
Storage	8 GB	40 GB
Virtual sensor specifications		
Maximum throughput	Up to 1 Gbps	Up to 1 Gbps
Number of monitoring port pairs	3	1 (monitoring port, not a port pair)
Virtual interfaces (VIDS) per sensor	100	100
DoS profiles	300	300
Management port	Yes	Yes
Response port	No	No
Deployment modes	Inter-VM inspection, physical-to-VM inspection, physical-to-physical inspection, SPAN/inline port inspection	

To learn more about Trellix, visit trellix.com.

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