Trellix

DATA SHEET

Trellix Intrusion Prevention System

Comprehensive, intelligent, advanced threat protection

Key benefits

- Quickly detects and blocks threats to protect applications and data
- High-performance, scalable solution for dynamic environments
- Centralized management for visibility and control
- Advanced detection, including signature-less malware analysis
- Inbound and outbound SSL decryption to inspect network traffic
- High availability and disaster recovery protection
- Virtual appliances also available
- Integrates with Trellix solution portfolio for device-to-cloud security

Miercom CERTIFIED SECURE

Trellix Intrusion Prevention System (IPS) is a next-generation intrusion detection and prevention system (IDPS) that discovers and blocks sophisticated malware threats across the network. It uses advanced detection and emulation techniques, moving beyond traditional pattern matching to defend against stealthy attacks with a high degree of accuracy.

To meet the needs of demanding networks, IPS can scale to more than 30 Gbps with a single device—and up to 100 Gbps when stacked. The integrated Trellix solution portfolio streamlines security operations by combining real-time Trellix Global Threat Intelligence (GTI) feeds with rich contextual data about users, devices, and applications for fast, accurate responses to network-borne attacks.

Protection against today's stealthy threats

Trellix IPS combines intelligent threat prevention with intuitive security management to improve detection accuracy and streamline security operations. Your network faces advanced attacks that can evade traditional detection methods—which is why our IPS layers multiple signature and signature-less detection engines to help prevent unwanted malware from wreaking havoc on your network. It performs deep inspection of network traffic using a combination of advanced technologies, including full protocol analysis, threat reputation, and behavior analysis to detect and protect against malware callbacks, denial-of-service (DoS), zero-day attacks, and other advanced threats.

Integrated security

Trellix IPS integrates with Trellix Intelligent Sandbox, which combines in-depth static code analysis, dynamic analysis (malware sandboxing), and machine learning to detect zero-day threats, including threats that use evasion techniques and ransomware.

Our IPS also combines file reputation from Trellix GTI and offers integration with Trellix ePO and Enterprise Security Manager for real-time correlation of network events across all relevant sources. The combined solution incorporates device details, user information, endpoint security posture, vulnerability assessments, and other rich information to help your organization better understand threat severity and business risk factors.

Performance and availability

Trellix IPS offers the best of both worlds—security and high performance. It combines a single-pass, protocol-based inspection architecture with purpose-built, carrier-class hardware to achieve real-world inspection up to 100 Gbps. Its efficient architecture preserves performance regardless of security settings, outperforming other IPS solutions that can experience up to a 50% reduction in throughput with security-over-performance policies.

Our IPS also provides active-active and active-passive modes with stateful failover, enabling you to meet high availability service-level agreements while avoiding the bottlenecks of slower performing appliances or over-burdened stand-alone solutions.

Scalable hardware provides investment protection

Trellix NS7500 and NS9500 series appliances offer flexibility so you can buy what you need now, and easily scale throughput as needed via a software license. You can also add more capacity by stacking multiple NS9500 appliances.

Visibility and control

Make informed decisions about the applications and protocols on your network. Trellix IPS was the first IDPS solution to combine advanced threat prevention and application awareness into a single security decision engine. We correlate threat activity with application usage, including Layer 7 visibility of more than 2,000 applications and protocols. This enables you to make more informed decisions about which applications you allow on your network.

In addition to application identification, our IPS provides user and device visibility. It prioritizes risky hosts and users, including active botnets, through the identification of anomalous network behavior.

Intelligent, scalable security management

Make the most of your security investment through intelligent network security management. IPS Manager provides scalable web-based management from two to several hundred network security appliances. It offers intuitive, progressive disclosure workflows that guide administrators to relevant alerts, along with easy-to-use security dashboards that automatically prioritize events based on alert severity and relevancy.

Additional features

Advanced threat prevention

- Inbound Secure Sockets Layer (SSL) decryption supports Diffie-Hellman and Elliptic-Curve Diffie-Hellman ciphers using an agent-based, shared key solution with no impact on sensor performance (patent pending for NS-series)
- Outbound SSL decryption (NS-series)
- Gateway Antimalware Emulation engine
- PDF JavaScript emulation engine
- Adobe Flash behavioral analysis engine
- Microsoft Office Deep File Inspection engine
- Advanced evasion protection
- Mobile threat reputation and cloud analysis

Botnet and malware callback protection

- DNS/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
- Native support for Snort signatures (NS-series)
- Allow list/block list enhancements in support of Structured Threat Information eXpression (Trellix NS-series)
- Host quarantine and rate limiting
- Inspection of virtual environments
- Integration with Trellix Intelligent Sandbox
- HTTP response decompression support

DoS and DDoS prevention

- Threshold and heuristic-based detection
- Host-based connection limiting
- Self-learning, profile-based detection

Trellix GTI

- File, IP, and URL reputation
- Application and protocol reputation
- Geo-location
- Allow listing based on Trellix GTI categories

High availability

- Active-active and active-passive with stateful failover
- External fail open (active)
- Built-in fail open

Protocol tunneling support

- IPv6
- V4-in-V4, V4-in-V6, V6-in-V4, and V6-in-V6 tunnels
- MPLS
- GRE
- Q-in-Q Double VLAN

IPS Manager

- Tiered management (up to 1,000 sensors)
- User authentication (RADIUS and LDAP)
- Automated failover and fail back
- Disaster recovery of critical configuration data
- Centralized, hierarchical policy management
- Memory dashboard details memory utilization by device

To learn more about Trellix, visit trellix.com.

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

About Trellix
Trellix is a global company redefining the future of cybersecurity. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix's security experts, along with an extensive partner ecosystem, accelerate technology innovation through machine learning and automation to empower over 40,000 business and government customers.