Trellix

DATA SHEET

Trellix IPS+ For AWS

The IPS for AWS that goes way beyond signatures

Product Overview

Trellix IPS+ provides signature-based detection that protects vulnerable assets from exploit, and can stop DDoS, C2 callbacks, and more. It does so at a high speed and scale. It also includes the Trellix IVX dynamic analysis engine to provide signatureless detection (sandbox detonation) and behavioral analysis. Integration with AWS Gateway Load Balancer means Trellix IPS+ is easier to deploy, has higher availability, and scales up and down automatically as traffic changes.

Situation

Organizations are being driven by two powerful forces to reassess their choice of IPS: threats are getting worse, and migration to AWS.

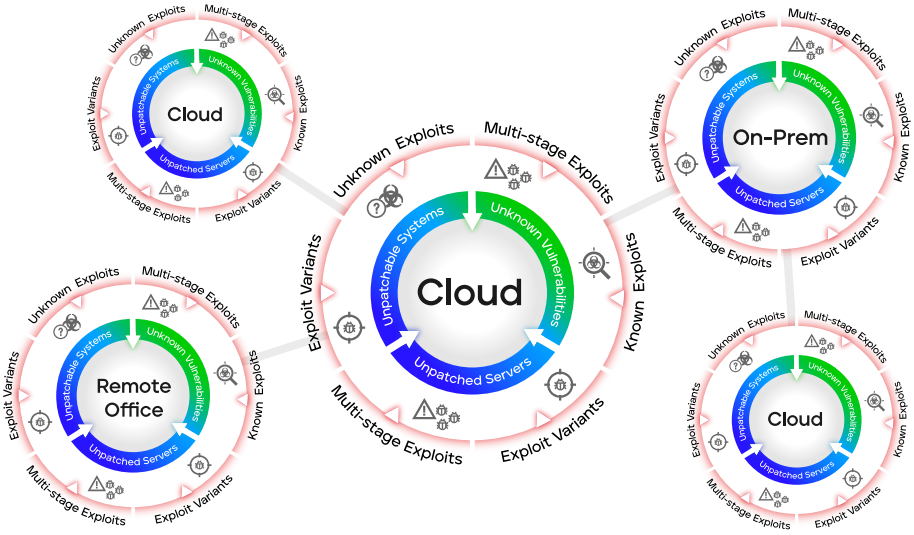
Attackers are flooding your organization with exploits to get past your defenses

The number of known vulnerabilities is soaring. In 2022, ethical hackers discovered 65,000 new vulnerabilities, a 21% increase over the prior year[1].

This has combined with an increased number of unpatchable legacy systems (no more patches being developed), as well as unpatched systems (IT can't keep up with installing patches, plus critical systems that organizations choose not to patch). According to one report, 58% of organizations run legacy systems that are no longer supported with patches[2].

Key Features

- Signature-based detections at speed and scale
- Includes Trellix IVX for signatureless detection (sandbox detonation)
- Behavioral analysis
- Virtual patching to protect unpatched systems
- High performance – 1Gbps per sensor, unlimited sensors
- Simplified deployment and management – no controllers or probes
- Integrated with AWS GWLB for auto-scaling and high availability
- North-South and East-West detection
- Unified policy management across all IPS+ sensors (AWS, other clouds, on-premises)
- Available as an AMI in the AWS Marketplace



A third ingredient is the increased use of exploit variants by attackers. By making minor changes to their code or their TTPs, new exploit variants escape detection by existing signatures. Finally, attackers are developing and deploying exploit variants at greater speed and scale, and the "waves" of exploits are crashing over organizations' defenses.

All of these factors have rendered traditional, signature-based IPS solutions inadequate to protect organizations today.

Securing AWS Workloads

Migrating to AWS means rethinking your cybersecurity needs. In the AWS Shared Responsibility Model[3], AWS is responsible for the security **of** the cloud, but you are responsible for security **in** the cloud. Intrusion prevention is one of your organization's responsibilities.

Inter-VM communication, and instant migration, replication, and backup of AWS workloads have combined to increase east-west traffic. Adding to the chaos, the flexibility provided by network virtualization makes these escalating traffic flows dynamic and unpredictable.

In the cloud, your workloads are dynamic and elastic, which means your attack surface is too, so your network defense needs to handle that. That means organizations want solutions that are less complicated, and easier to deploy and manage in a dynamic AWS environment. An IPS for AWS also needs to be high bandwidth, and to take advantage of AWS Load Balancer Gateway to auto-scale to ensure the IPS is never a bottleneck.

That makes migration to AWS the perfect time to re-examine your IPS requirements, to find a solution that can keep up with the threat landscape, and that isn't limited to signature-based detection.

Trellix IPS+ For AWS

We developed Trellix IPS+ For AWS to address these needs. Trellix offers superior detection, high performance, and reduced complexity.

Superior Detection

Trellix IPS+ For AWS includes the expected signature-based detection but goes beyond that to include multiple layers of signatureless detection. Trellix IPS+ For AWS provides:

- Multi-layered threat detection
  - Signature-based Detection – "Find known bad" – High speed analysis at scale
  - Signature-less Detection – "Find unknown bad" – Executes suspected malicious code in a safe environment (sandbox detonation)
  - Behavioral Analysis – "Reveal suspicious patterns" – Machine learning identifies characteristics similar to known bad behaviors
- Reconnaissance attack detection

- Virtual patching
- Proprietary/Custom Signatures (Snort, YARA)
- Static Network Rules/Blacklists
- Riskware detection
- Outbound file scanning
- Remote code execution detection

High Performance

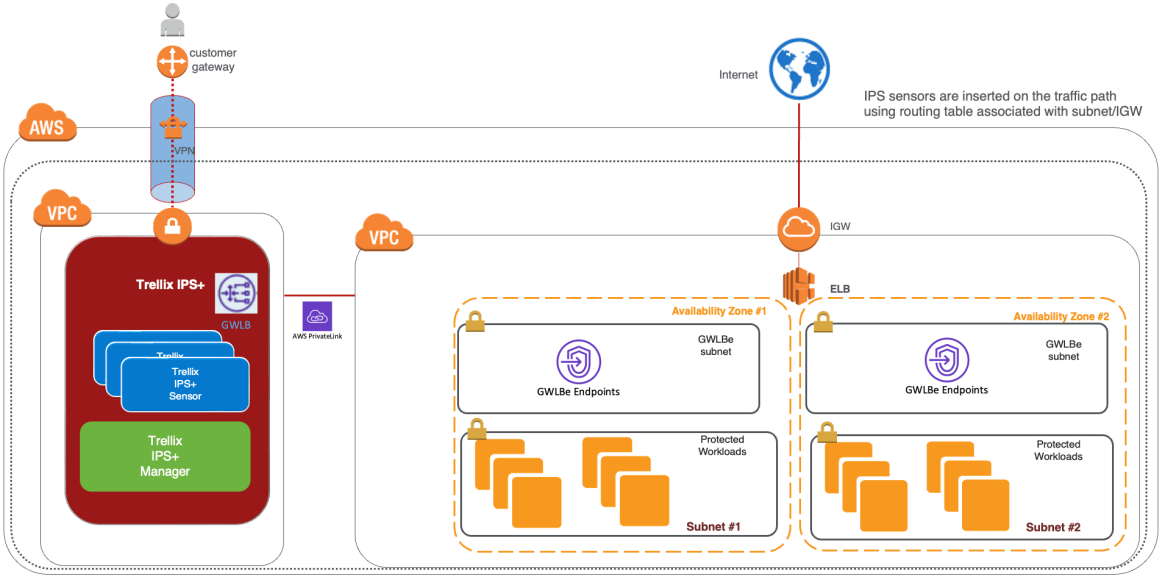
Trellix IPS+ has been designed to provide high speed and scale, so it won't become a network chokepoint.

- Throughput of 1Gbps per sensor; unlimited sensors
- Native integration with AWS Gateway Load Balancer provides automatic scale-up and scale down to adapt to elastic workloads
- Automatic load balancing across sensors ensures that performance is optimized

Reduced Operational Complexity

With the dynamic nature of AWS workloads, an IPS needs to be simple and streamlined.

- Fewer components and reduced complexity of deployment and management
- Single, unified policy manager and alerting for all sensors across all networks
- Generates telemetry for network forensics (Trellix Network Investigator)
- Integration with AWS Gateway Load Balancer for easy deployment and management, automatic scaling, and high availability
- High-precision verdicts for reduced alert fatigue
- High availability – a new controller instance is launched when an active controller becomes unavailable
- 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
- Standby controllers can be deployed for disaster recovery
- Streamlined workflows and analytics – includes advanced analytics and actionable workflows that correlate multiple IPS alerts into a single actionable event, enabling your administrators to quickly identify relevant information



Additional Features

Advanced Threat Prevention

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

Advanced Intrusion Prevention

- IP defragmentation and TCP stream reassembly
- Signatures: Trellix, user-defined, and open-source
- Host quarantine and rate limiting
- Inspection of virtual environments
- 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

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

Trellix Global Threat Intelligence

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

1. HackerOne "6th Annual Hacker-Powered Security Report", 2022
2. 0Patch, "Security Patching is Hard", 2018
3. https://aws.amazon.com/compliance/shared-responsibility-model/

Visit Trellix.com to learn more.

Trellix

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. 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, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.