Datasheet

Stamus Security Platform

Actionable network visibility and threat detection

- Greater visibility and evidence
- More complete detection
- Response-ready Declarations of Compromise™
- Extensible threat intelligence
- Straightforward integrations
- Immediate results

Stamus Security Platform (SSP) is an open network detection and response solution that delivers actionable network visibility and threat detection.

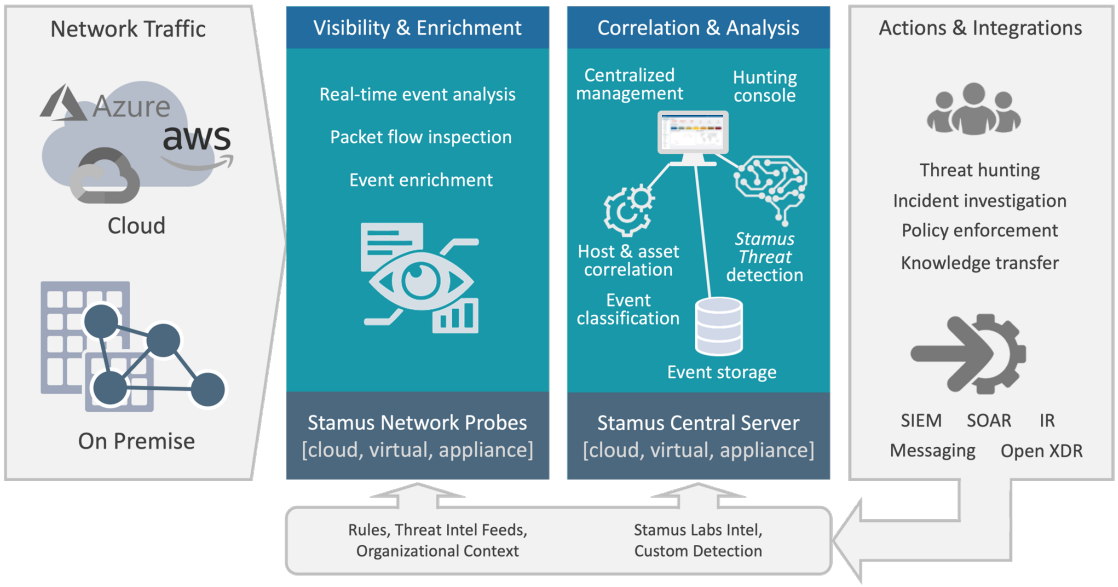
THE NETWORK DOES NOT LIE

In fact, the network holds the ground truth for an enterprise's security posture. Even as more organizations shift to cloud-based workloads, encrypted transmission, and remote workforces, nearly all cyber threats generate communications that can be observed on the network.

At Stamus Networks, we tap into the inherent power of network traffic to uncover every possible threat to your organization. We offer the best possible asset-oriented visibility and automated detection to help practitioners cut through the clutter and focus on only those serious and imminent threats.

SYSTEM ARCHITECTURE AND DEPLOYMENT

Stamus Security Platform consists of two components: Stamus Network Probe(s) and Stamus Central Server. Each play a critical role in scaling the system. Stamus Central Server and Stamus Network Probes can be deployed in private cloud, public cloud, on-premise, or hybrid environments.

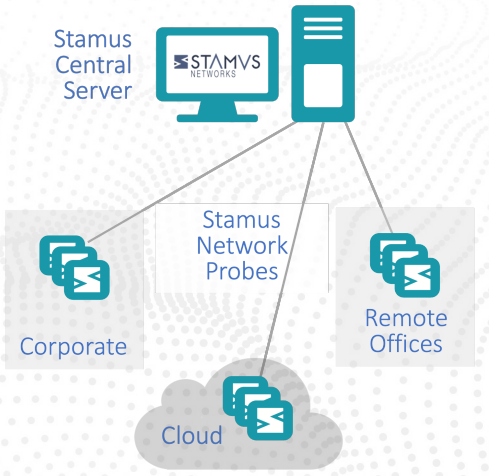


Stamus Network Probes

Stamus Network Probes inspect and analyze all network traffic to perform real-time threat detection, enrich the resulting events with extensive metadata, and capture network protocol transactions. The probe delivers all this data to the Stamus Central Server for additional analytics, processing and another layer of threat detection.

Stamus Central Server

Stamus Central Server provides the centralized management of the probes, third party threat intelligence and rulesets, consolidated event storage and a central integration point. It includes a additional layer of machine learning and algorithmic threat detection, along with automated event triage – enabled by tagging and classification. Finally, the Stamus Central Server provides a powerful threat hunting and incident investigation user interface.



SSP supports all combinations of physical, virtual, and cloud installations.

Both Stamus Network Probes and the Stamus Central Server are available as turnkey physical appliances (from Stamus Networks) or may be installed as a software image on bare metal hardware, virtual machines, public or private cloud

GREATER VISIBILITY AND EVIDENCE

Your next breach could be hiding in network blind spots.

Without a comprehensive view into network activity, these blind spots can provide a haven for malicious activity targeting your organization.

Stamus Security Platform (SSP) uncovers the subtle attack signals lurking in your network, notifies you of serious and imminent threats, provides a complete timeline for each host under attack, and delivers all the evidence you need in order to respond quickly and stop a breach before damage is done.

Examples of specific visibility offered by Stamus Security Platform include:

- **Minor policy violations** – using the extensive SSP policy filter toolkit, analysts can review and uncover unauthorized network activity, shadow IT, access control violations, improper configurations, and more.
- **Lateral movement** – with a dedicated set of lateral movement threat detections, SSP can help you spot an attack as it expands its foothold in your organization.
- **Encrypted traffic flows** – while SSP does not directly decrypt network traffic, the system examines the trail of evidence left during TLS handshake to identify anomalous activity and uses machine learning to detect command and control beacons, even in complex TLS environments.
- **Cloud workflows** – Stamus Network Probes can be deployed in your public and private cloud infrastructure to monitor network activity to, from, and between those systems. The Stamus Central Server correlates cloud, data center, and on-premise network activity to create a complete picture of your organization's security posture.
- **Host insights** – for every host it sees on the network, SSP builds an extensive record of activity. It tracks more than 50 data points for each host, including services running on the host, user activity, TLS fingerprints, device type, hostnames, user agents, file activity, etc. And SSP simultaneously maintains this activity for millions of hosts without requiring an endpoint agent.
- **Extensive supporting evidence** – for every security event it generates, SSP captures and presents a complete evidentiary log of associated activity, including protocol transactions, flows, packet captures (PCAPs), and extracted files along with a clear timeline of activity showing the progression of the various threats against a given asset.

MORE COMPLETE DETECTION

No single detection mechanism can uncover all the threats facing your organization.

Without access to multiple automated detection mechanisms, your security team could miss malware (including ransomware), botnets, advanced persistent threats, data exfiltration, remote access trojans, rootkits, social engineering, lateral movement, policy violations, phishing, and other threats.

Detecting these and other threats requires combining multiple mechanisms, some simple and others quite sophisticated. Each contributes to the system's ability to efficiently uncover threats and support an appropriate response. SSP currently employs the following detection mechanisms:

- **Explicit rules** – most efficient way to detect known threats
- **Machine learning** – good at detecting difficult patterns or abnormalities
- **Behavioral analytics** – efficient mechanism for identifying unauthorized activity
- **Stateful logic** – required for tracking the activities associated with an asset over time
- **Third party threat intelligence** – mechanism to leverage work of other threat researchers
- **Statistical anomalies** - efficient mechanism for identifying subtle behavioral changes

The combination of multiple detection techniques is much more effective than a single mechanism such as machine learning or explicit rules alone. In addition, these mechanisms allow SSP to generate a multi-dimensional stream of events that can be correlated and used for threat hunting and incident investigation.

The threat research team at Stamus Labs is continually developing new algorithms and intelligence to improve the SSP threat detection capability. SSP users receive threat intelligence updates daily and improved detection algorithms several times per year.

Example threats that can be identified using Stamus Security Platform's more complete threat detection

- Malware
- Ransomware
- Exploit kits
- Botnets
- Beacons
- Offensive tools
- Advanced persistent threats
- Data exfiltration
- Command and control
- Penetration tests
- Remote access trojans
- Rootkits
- Social engineering
- Lateral movement
- Shadow IT
- Policy violations
- Phishing
- Crypto mining

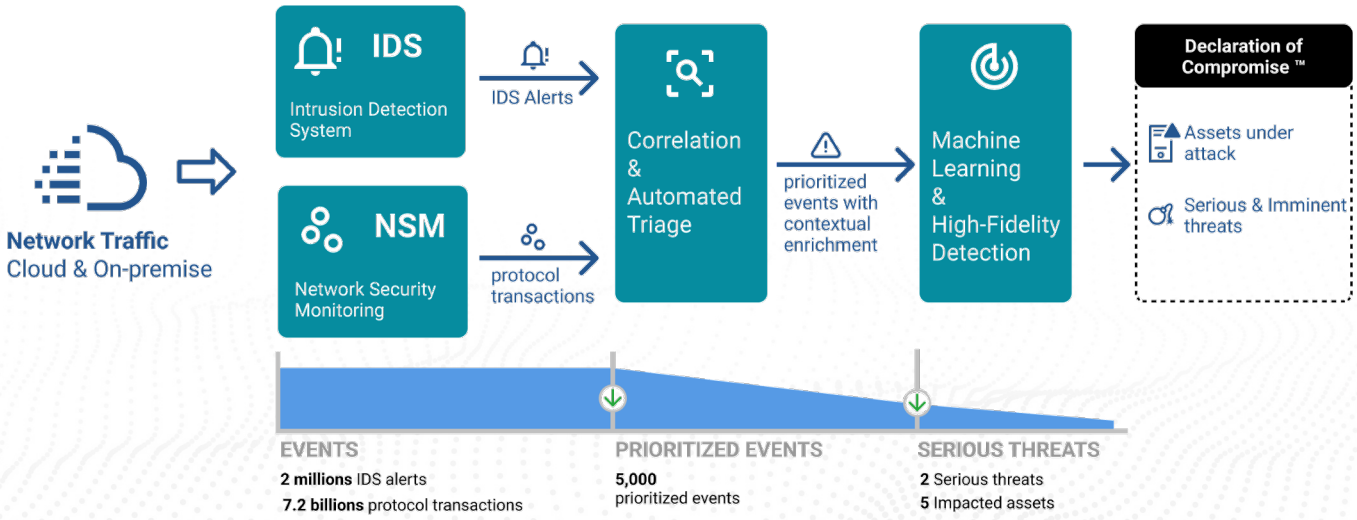
RESPONSE-READY DECLARATIONS OF COMPROMISE™

Security teams are overwhelmed with false positives and informational security events.

Without high-fidelity threat notifications that can be confidently used to trigger automated responses, security teams waste hours every day reviewing alerts and "suspicious activity". This creates alert fatigue which can desensitize security teams to real threats and prevents them from responding in a timely manner.

Stamus Security Platform performs the difficult work of automating event triage and identifying the most serious threats that need immediate attention. SSP applies an additional layer of algorithmic threat analytics to identify high-confidence threats to critical assets, map the advancement of those threats along the stages of the cyber kill chain, and serves as a "smoke alarm" to alert personnel or systems when a serious and imminent threat is discovered.

These "Declarations of Compromise" (DoCs) are an important output of an extensive automated triage process executed by SSP that gives security teams high-confidence notifications to trigger an immediate response. See illustration below.



DoC events may be viewed directly in the SSP user interface, or they may be used to automatically trigger a process in an integrated system. For example, a DoC can trigger a playbook in a security orchestration, automation, and response (SOAR) system, quarantine an endpoint via an endpoint detection and response (EDR) platform, or it may simply send a notification to a channel-based messaging app, such as Slack.

EXTENSIBLE THREAT INTELLIGENCE

Your network security vendor may not always know what's best for you.

Many network security solutions are closed systems. They do not allow you to take advantage of the myriad of third-party threat intelligence and detection algorithms that are created every day by specialized providers and your own team that has local knowledge. This forces security teams to rely on a single vendor to perform ongoing threat research and may not address the specific needs of your organization.

While Stamus Networks provides SSP users with a powerful set of industry-leading threat detection rules and IoC datasets, SSP allows you to take advantage of threat intelligence from other experts, including your internal or industry-specific threat research groups.

- **Third party threat intelligence** – with its IOC matching capability, SSP can ingest lists of known-bad IP addresses and domains from any source.
- **Third party rules** – because SSP uses the Suricata network security engine, SSP users can access the dozens of providers developing Suricata rulesets.
- **Custom DoC escalations** – when users uncover patterns of activity during a hunt or incident investigation for which they wish to explicitly identify, they may create custom Declarations of Compromise which may be applied to historic data or for future detection.

STRAIGHTFORWARD INTEGRATIONS

Network detection and response is not the only tool in your security technology stack.

While SSP includes a powerful native user interface, your team may wish to integrate your critical systems to simplify your security operations and automate your responses via security event and incident management (SIEM); security orchestration, automation, and response (SOAR) system; endpoint detection and response (EDR); extended detection and response (XDR), among others.

Stamus Security Platform supports four primary types of integrations with other elements of your tech stack:

- **Logging** - enriched event streams delivered to SIEM or data lake via syslog or TCP in JSON format
- **API** - evidence queries and configuration commands initiated by third party systems, such as a SIEM, SOAR, XDR, EDR, IR, with access to all SSP functions
- **Trigger** – a message or response signal initiated by a DoC event and delivered via webhook to SOAR, EDR, XDR, IR, ticketing, or messaging systems such as Slack or MS Teams.
- **Native Splunk app** - allows Splunk Enterprise and Cloud users to extract information and insights from both the Stamus Security Platform and open source Suricata sensors

IMMEDIATE RESULTS

Your network security system should be easy to deploy and begin working for you immediately.

Most network security systems are much more easily deployed than endpoint solutions such as EDR. This is because security teams can deploy network probes at just a few key junctions in the network and gain visibility into communications among all the endpoints in the organization. To get the same visibility with an endpoint system, security teams need to deploy an agent in every single system in their organization – a much more complicated logistical task. That said, some network security platforms need weeks or even months to train the system to detect anomalies.

With its multiple detection engines, the Stamus Security Platform can begin identifying malicious and unauthorized network activity within minutes of deployment. You cannot predict when you will be attacked, so deploying SSP ensures your defenses are in place as quickly as possible.

AVAILABLE IN TWO SIMPLE LICENSE TIERS

SSP is available in two functional license tiers – Stamus Network Detection (Stamus ND) and Stamus Network Detection and Response (Stamus NDR). See the table below for a high-level comparison.

	Stamus ND	Stamus NDR
Signature and reputation list-based threat detection	✓	✓
Flow and protocol-based data enrichment and event capture	✓	✓
Tagging and classification for auto event triage	✓	✓
Guided threat hunting	✓	✓
Machine learning and algorithmic detection engines		✓
Stamus threat intelligence and customizable detection		✓
Asset-oriented insights		✓
Declarations of Compromise™ | high-fidelity threat notifications		✓

System pricing is based on throughput. Annual licenses for Stamus Security Platform are based on the number of probes and their interface speeds. Probes are available with network interface speeds from 100 Mbps to 40 Gbps. The licenses include daily threat intelligence updates and regular software enhancements.

HOW STAMUS SECURITY PLATFORM IMPROVES YOUR SECURITY

Security teams use Stamus Security Platform for automated detection, proactive threat hunting, incident investigation and IT policy enforcement. Ultimately, the system helps both security (SecOps) and network (NetOps) operations teams:

Reduce your organization's risk – uncover known and unknown threats to critical assets from your cloud and on-premise networks.

Eliminate network blind spots – monitor north-south as well as east-west traffic with Stamus Network Probes at all critical points in your cloud and on-premise networks.

Eradicate alert fatigue – the system notifies incident response systems and personnel only when urgent and imminent threats are identified.

Reduce the workload of your SOC analysts – free your valuable staff, allowing them to focus on proactive security measures, rather than pouring through 1000s of alerts.

Dramatically accelerate incident response - quickly investigate potential issues with transparent, explainable results, backed up with extensive evidence.

See results immediately – Stamus Security Platform is easy to install, configure and integrate with other elements of your security tech stack.

Extend your capabilities – leverage third-party threat intelligence and rulesets; and easily transform a threat hunt into custom detection logic.

Uncover hidden threats – because even the most advanced system cannot automatically detect everything, Stamus Security Platform comes with an integrated guided threat hunting console that make the hunt both effective and efficient.

ABOUT STAMUS NETWORKS

Stamus Networks believes in a world where defenders are heroes, and a future where those they protect remain safe. As defenders face an onslaught of threats from well-funded adversaries, we relentlessly pursue solutions that make the defender's job easier and more impactful. A global provider of high-performance network-based threat detection and response systems, Stamus Networks helps enterprise security teams accelerate their response to critical threats with solutions that uncover serious and imminent risk from network activity. Our advanced network detection and response (NDR) solutions expose threats to critical assets and empower rapid response.

STAMUS NETWORKS

5 Avenue Ingres
75016 Paris
France

450 E 96th St. Suite 500
Indianapolis, IN 46240
United States

contact@stamus-networks.com
www.stamus-networks.com

