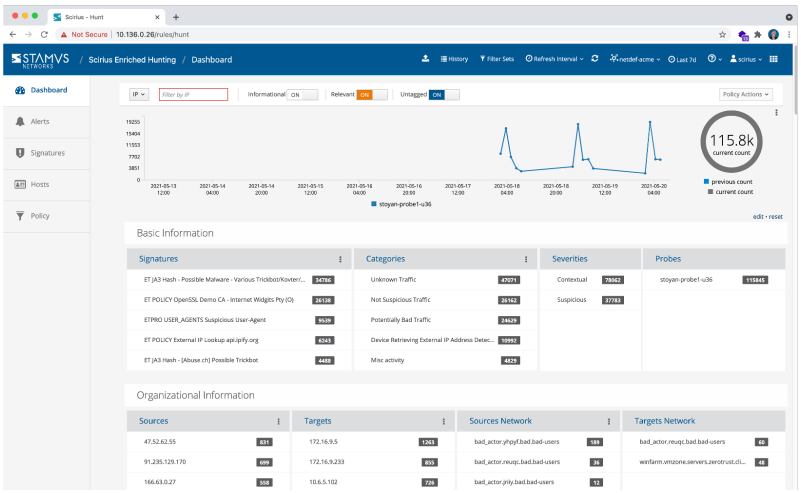
Datasheet

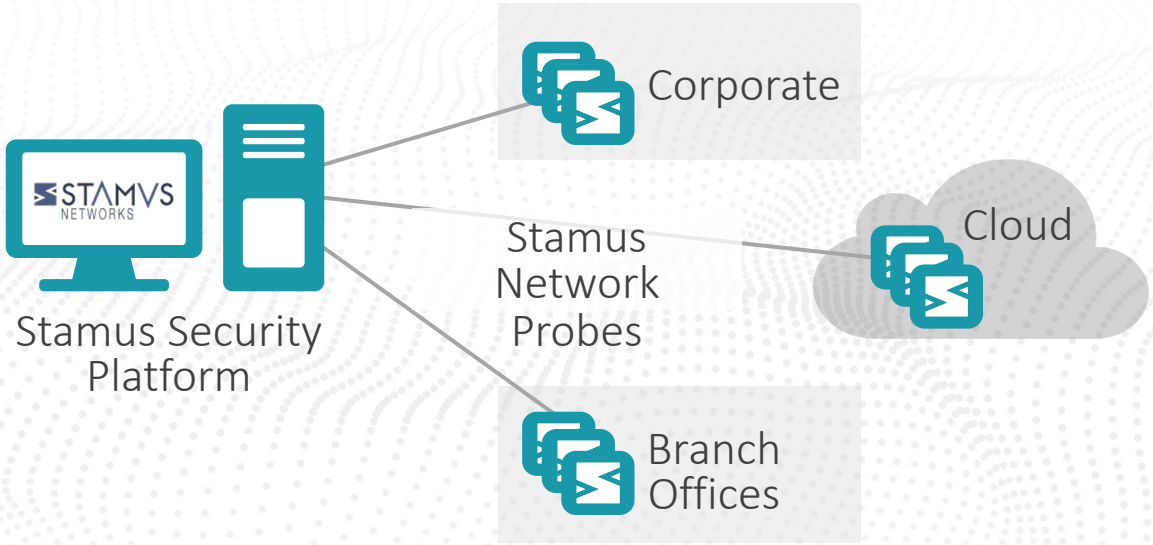
Stamus Network Detection (ND)

Stamus ND is a Suricata-based intrusion detection (IDS) and network security monitoring (NSM) system that delivers:

- Correlated IDS (signature-based) and NSM (protocol transaction logs) data
- Open interfaces for SIEM or log management system
- Native Splunk app
- Open third-party signatures and threat intel
- Tagging & classification for automated alert triage
- Integrated guided threat hunting



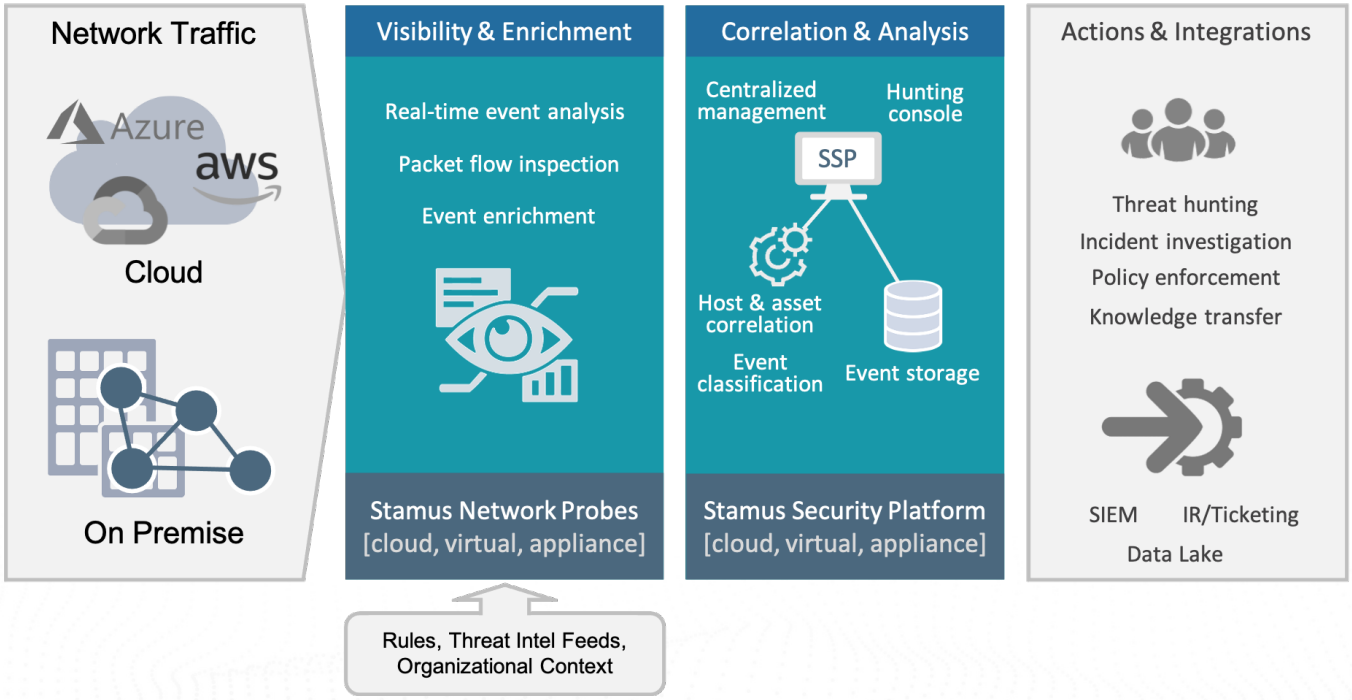
Stamus ND consists of two components: Stamus Network Probes and Stamus Security Platform. Each play a critical role in scaling the system. Stamus Security Platform and Stamus Network Probes can be deployed in private cloud, public cloud, on-premise, or hybrid environments.



STAMUS NETWORK PROBES

The probes may be deployed in the cloud, on premise or a combination of the two. Typically, multiple probes are connected to a network tap, packet broker, or span/mirror port in locations giving the system visibility into both north-south and east-west network traffic.

The function of the Stamus Network Probe is to inspect and analyze all traffic flows 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 Security Platform for additional analytics, processing and another layer of threat detection.



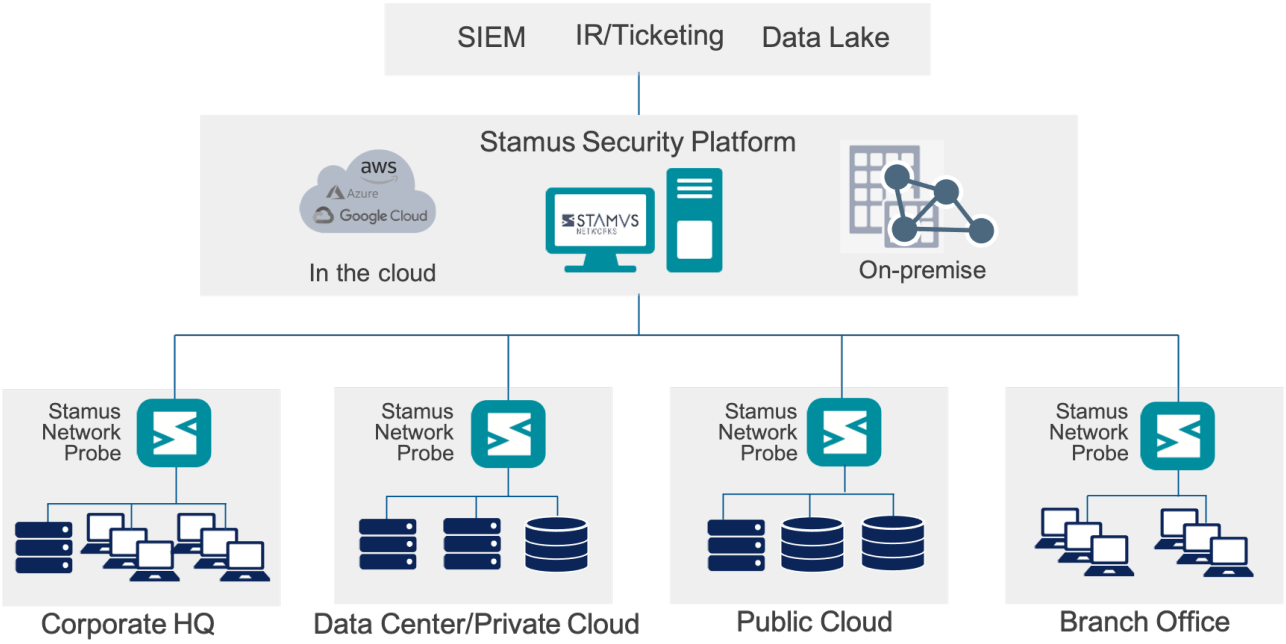
The probe is based on the Suricata engine which provides both network security monitoring (NSM) protocol transaction logs and intrusion detection (IDS) alerts.

The probes 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

* Stamus Networks appliances are required to monitor data rates above 10 Gbps

STAMUS SECURITY PLATFORM

Stamus Security Platform (SSP) provides the centralized management of the probes along with several other critical functions, including:



SSP consolidates event storage and provides the central integration point for the rest of your security tech stack, such as SIEM, data lake, or log management system

Consolidated event storage and central integration point for the rest of your security tech stack, such as SIEM, data lake, or log management system.

A guided threat hunting console for proactive threat hunting and incident investigation

Automated event triage - enabled by a tagging and classification workflow - to dramatically reduce the time spent by analysts reviewing security events

Extracting and organizing the data for networks, hosts, and users to bring the security event data to life, making sense out of it in the context of your organization

Management of third-party threat intelligence and rulesets that leverages the experience and organization-specific knowledge of your team

HOW STAMUS ND IMPROVES YOUR SECURITY

Security teams use Stamus ND for automated detection, proactive threat hunting, incident investigation and IT policy enforcement. Ultimately, the system helps 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.

Reduce alert fatigue – the system performs automated triage classification, tagging IDS alerts as either informational or important

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.

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 resources, 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.

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

See results immediately – Stamus ND 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 ND comes with an integrated guided threat hunting console that make the hunt both effective and efficient.

Integrated IDS and NSM Results		Multiple detection engines (rules, threat intelligence) coupled with protocol transaction flow data.
Open Interfaces		Open interfaces and extensive API for integration into SIEM, log management, and third-party threat intelligence.
Organizational Context		Your organization's network names, hostnames, and usernames are all included in alerts and flow logs
Built-in Guided Threat Hunting		Guided threat hunting interface with advanced pivoting on enriched data, event tagging and knowledge transfer workflow
It Just Works		Easy to install, integrate, configure, and operate. It just works - all the time.

BUILT BY OPEN-SOURCE SECURITY TECHNOLOGY EXPERTS

Stamus Networks' product development is led by Éric Leblond and Peter Manev. Both Éric and Peter are members of the Open Information Security Foundation executive team and developers on the Suricata project, the widely-deployed open-source intrusion detection and network security monitoring engine. The OISF is a non-profit organization created to build community and to support open-source security technologies like Suricata. Under the leadership of Éric and Peter, Stamus Networks applies its extensive Suricata and network expertise to develop our advanced network security solutions.

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

For more information, contact

KIPPEO
GET STARTED IN HOLISTIC SECURITY

https://kippeo.com
sales@kippeo.com

