Solution Brief

Network Visibility, Advanced Threat Detection, and Automated Response

SentinelOne and Stamus Networks Joint Solution Brief

Market Challenges

The increasing complexity of IT environments, fueled by IoT, cloud, and BYOD, has exposed significant gaps in endpoint-only security. Many organizations struggle to achieve comprehensive visibility and threat detection, particularly in agentless environments like IoT/OT networks, BYOD settings, or cloud infrastructure.

Challenges remain. These environments present unique obstacles to traditional security controls. Enterprises need solutions that offer visibility and threat detection in these agentless spaces.

NDR solutions that analyze network traffic to uncover serious threats and unauthorized activity in these environments are a vital countermeasures.

Joint Solution Highlights

Provides real-time visibility into all network activity

Trigger automated endpoint disconnection in response to network-detected threats

Delivers rich network security telemetry to SentinelOne Singularity Data Lake

Multi-source threat detection with SentinelOne Singularity XDR

Integration Benefits

Detect and respond to threats faster

Reduce the risk of breaches

Improve operational efficiency

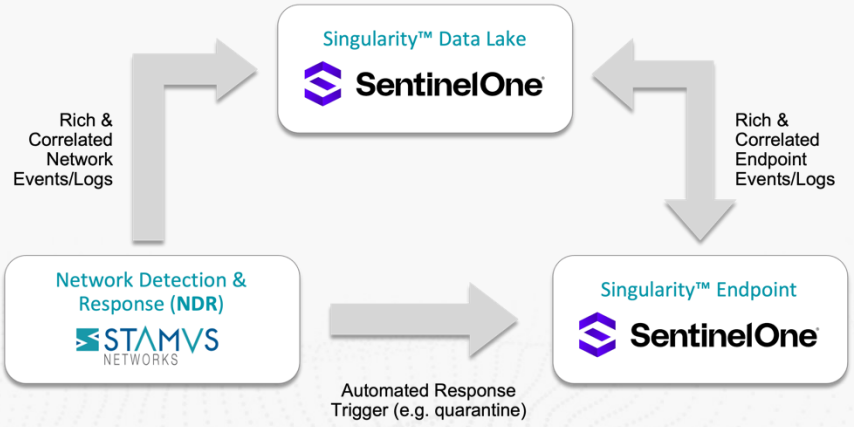
Enhance security posture

JOINT SOLUTION

The integration of Stamus Networks and SentinelOne empowers defenders with a more complete approach to threat detection and response.

The SentinelOne Singularity Platform – powered by SentinelOne Singularity Data Lake – ingests critical telemetry from both SentinelOne native solutions such as Singularity Endpoint and third-party security tools such as the Stamus Security Platform (SSP). Security Operations practitioners can contextually visualize and automatically respond to high-value security alerts with a single cloud-scale repository.

The Stamus Security Platform (SSP) is an open and transparent network detection and response solution (NDR) that delivers actionable network visibility and powerful multi-layered threat detection. SSP provides real-time network monitoring, detection, and automated response to thwart serious threats and unauthorized activity.



The SOC visibility triad with network + endpoint detection and response threat and evidentiary data feeding into the Singularity Data Lake for centralized correlation and analysis

SSP supports use cases like malware/ransomware detection, unauthorized activity tracking, shadow IT discovery, and threat hunting. It integrates with EDR, XDR, SIEM, SOAR, IR, and other systems, delivering a source of rich network security telemetry and enabling automated response to threats.

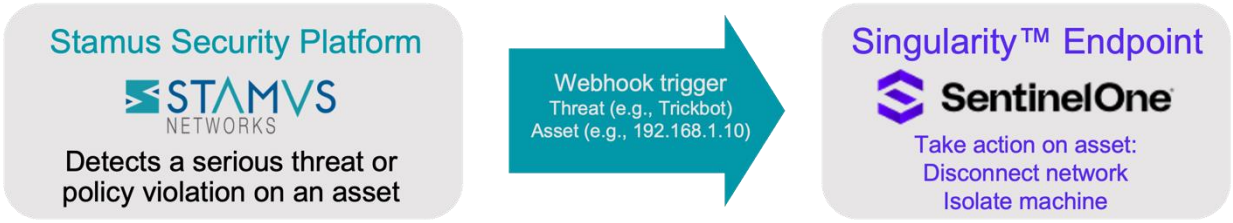
Stamus Network Probes and the Stamus Central Server may be deployed on premise, in the cloud, or in hybrid environments, giving enterprises maximum visibility and complete control over data residency.

INDIVIDUAL USE CASES

Here, we will offer real-world examples of how this joint solution can be used to address specific security challenges:

Network Detection with Automated Endpoint Quarantine

Stamus Security Platform's Declarations of Compromise™ (DoC™) identify serious and imminent threats with extreme accuracy. These ultra-high-confidence events identify threats on an asset and can be used to trigger a fully automated response. In this use case, the DoC integrates with SentinelOne Singularity Endpoint – using a webhook message – to notify the endpoint user and disconnect the endpoint involved in the threat detection. A similar detection called Declaration of Policy Violation™ or DoPV™ applies the same confident 'declaration' to a set of organization-specific policies and can also be used to disconnect an endpoint.



By leveraging the Stamus Security Platform's automated response, security teams can significantly enhance their efficiency and effectiveness in responding to threats.

Network Data Telemetry for More Comprehensive XDR

Stamus Security Platform (SSP) analyzes real-time network traffic, uses multiple mechanisms to detect threats, gathers metadata, then sends logs to Singularity Data Lake for use in its extended detection and response (XDR) application. Stamus Security Platform records all protocol transactions and generates verbose flow records. These are maintained independently as well as automatically correlated with the security events and included in the event logs. Users of Singularity Platform then can apply Purple AI for advanced analytics.

This integration enables threat hunters, incident responders and other security practitioners who use Singularity Platform to derive valuable insights from the rich network data provided by SSP to more effectively do their job.

KEY BENEFITS

The following are the primary benefits of the SentinelOne-Stamus Networks solution:

- **Detect and respond to threats faster** - by providing a more complete view of both network and endpoint security landscape, Singularity Platform enables faster threat detection and more effective incident response.
- **Reduce the risk of breaches** - the combination of NDR and endpoint data allows for more comprehensive threat identification and prioritization, reducing the risk of security breaches.
- **Improve operational efficiency** - by automating repetitive tasks and centralizing security data, Singularity frees up valuable time for analysts to focus on higher-level activities.
- **Enhance security posture** – Singularity Platform's AI-powered analytics and customizable dashboards provide valuable insights into network security trends, enabling organizations to proactively identify and mitigate risks.

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

 SN-JSB-S1-092024-1