Solution Brief

Intelligent Traffic Optimization and Aggregation for High Performance Threat Detection and Response

Array Networks and Stamus Networks Joint Solution Brief

CHALLENGES

High speed networks can be difficult to monitor cost-effectively with network detection and response (NDR) solutions due to the costs associated with deploying high capacity NDR sensors – those capable of monitoring 40 Gbps and 100 Gbps links, for example. Streaming video apps like Netflix and YouTube are contributing to these network traffic increases, especially on telcom networks. Not all traffic requires the same degree of security monitoring.

And in complex enterprise environments, deploying NDR sensors in all the right places can be challenging. For example, it may not be feasible to effectively mirror traffic from all network segments onto a single port for a single NDR sensor. And deploying multiple NDR sensors may be cost prohibitive.

Solution Highlights

- Filter traffic to monitor only high value packets
- Aggregate from multiple network taps or mirror ports to single probe
- Response-ready and high-fidelity detection
- Extensive incident context and evidence
- Traffic optimization at speeds up to 2 Tbps

Solution Benefits

- Enhanced visibility into all network traffic
- Improved threat detection
- Uncover weak attack signals
- Eliminate alert fatigue
- Accelerate incident response
- Leverage rich network telemetry for central AI analytics
- Reduce costs and improve scalability

This paper describes the powerful combination of a network traffic broker from Array Networks and network detection and response from Stamus Networks.

THE NETWORK SECURITY MONITORING IMPERATIVE

The rapid proliferation of IoT devices, network devices, and cloud infrastructure has drastically expanded the attack surface for organizations across all industries. As these attack surfaces change, organizations must adapt the way they monitor them. The growing reality is that endpoint-based security just can't handle many of these environments, leaving significant gaps in coverage. As a result, security teams are left grappling with the challenge of achieving visibility and threat detection in all areas of their organization.

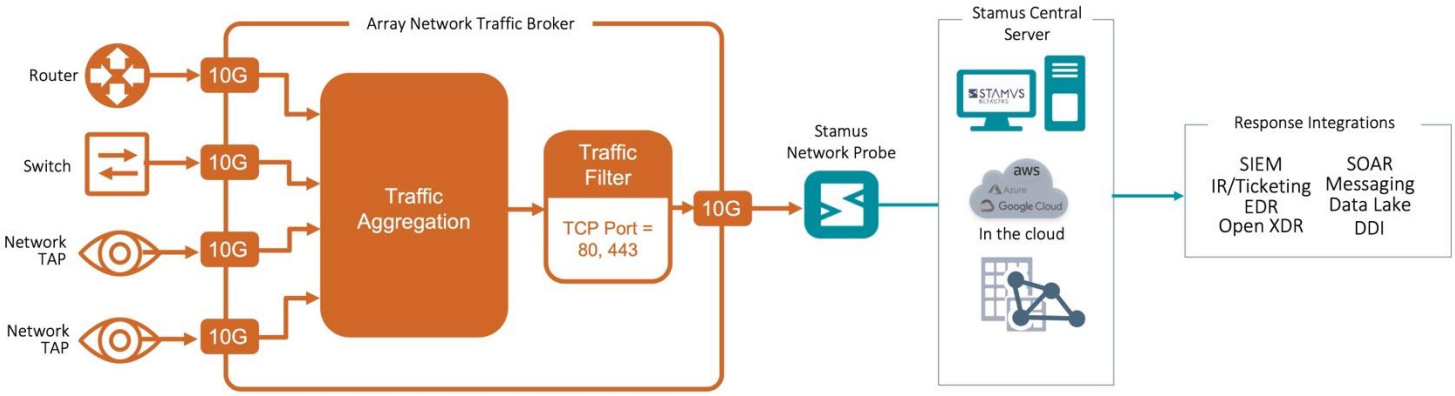
As such, mature enterprises tap into the inherent power of network traffic to uncover critical threats to their organizations. Network detection and response (NDR) systems use a combination of multiple detection technologies – such as machine learning-based anomaly detection, signatures, and IoC matching – to uncover serious threats and unauthorized activity to help security teams respond sooner.

JOINT SOLUTION OVERVIEW

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.

In large enterprise networks with high traffic volumes, the Array Network Traffic Broker (NTB) acts as an intelligent traffic management layer, capturing, filtering, and aggregating network traffic from various sources. It intelligently directs traffic to the Stamus Security Platform, ensuring optimal utilization of its threat detection capabilities.

The Stamus Security Platform leverages advanced threat detection techniques, including machine learning, behavioral analytics, and signature-based detection, to analyze network traffic and identify potential threats. These advanced threat detection capabilities enable it to identify sophisticated attacks, such as zero-day exploits and lateral movement, that may bypass traditional security solutions.



The combination of NTB and SSP offers a complete solution to a historically difficult problem and provides enterprise security teams with unprecedented visibility and enabling comprehensive threat detection and response across complex, multi-source network environments.

SOLUTION FEATURES

- Response-ready and high-fidelity threat notifications from machine learning, heuristics, signatures, and IoC matching and more – ideal for automated response
- Extensive incident context and evidence, including flow records, PCAPs, and extracted files
- Optimization to monitor only high-value security traffic
- Aggregate from multiple network taps to a single Stamus Network Probe
- Traffic optimization at network speeds up to 2 Tbps
- Discard unwanted traffic types - drop streaming services, discard encrypted traffic, or deliver encrypted handshake metrics and discard payloads
- Optionally deploy traffic broker inline with hardware bypass

SOLUTION BENEFITS

- **Enhanced visibility** – with intelligent traffic optimization from Array NTB, security teams can cost-effectively use Stamus Security Platform to monitor traffic high-performance environments such as data centers for east-west traffic.
- **Reduce costs** – with intelligent traffic aggregation from Array NTB, organizations can deploy fewer Stamus Network Probes comprehensive visibility into network activity, helping identify hidden threats and vulnerabilities.

- **Improved threat detection** – SSP's advanced threat detection capabilities, fed by optimized traffic from multiple sources through the NTB, ensure a high level of accuracy in identifying malicious activity, reducing false positives, and enabling faster response to genuine threats.
- **Scalability** – The joint solution can handle large volumes of network traffic, making it suitable for organizations of all sizes and ensuring effective threat detection even in complex network environments.
- **Operational efficiency** – The integration between the NTB and SSP streamlines security operations, reducing the complexity of managing multiple security tools and improving the efficiency of threat response.
- **Uncover even the weakest attack signals** – with SSP, you can leverage integrated detection algorithms, third-party threat intelligence and rulesets; and easily transform a threat hunt into custom detection logic.
- **Eliminate alert fatigue** - with the high-fidelity Declarations of Compromise™ and Declarations of Policy Violations™, you can be confident they are investigating real security events.
- **Accelerate incident response** - with extensive integrations into EDR, NAC, IPAM, SOAR, and other systems, SSP can automatically trigger an incident response.

ABOUT ARRAY NETWORKS

Array Networks, the network functions platform company, develops purpose-built systems for deploying virtual app delivery, networking and security functions with guaranteed performance. Headquartered in Silicon Valley, Array is poised to capitalize on explosive growth in the areas of virtualization, cloud and software-centric computing. Proven at over 7000 worldwide customer deployments, Array is recognized by leading analysts, enterprises, service providers and partners for next-generation technology that delivers agility at scale.

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.

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-ARRAY-NTB-092024-1