Solution Brief

# High Speed Network Traffic Decryption for Advanced Threat Detection & Response

## Array Networks and Stamus Networks Joint Solution Brief

## CHALLENGES

Nearly all network traffic is encrypted today, making the job of security monitoring significantly more difficult as threats are hidden inside the encrypted traffic flow. While encryption offers enhanced security and privacy to the end user, it raises serious issues for enterprise security teams tasked with protecting the organization and ensuring that relevant legal and regulatory requirements are met.

Striking the correct balance between security and privacy in the enterprise is challenging, which can require visibility into at least some portion of the encrypted traffic.

Innovative network security companies have responded by developing techniques to identify malicious activity in encrypted traffic without having to decrypt the flows.

### Solution Highlights

Monitor encrypted traffic payload for improved threat detection and response

Response-ready and high-fidelity detection

Extensive incident context and evidence

Decrypts across all TCP ports up to 200 Gbps

Automatically adjusts the cipher suite selection

### Solution Benefits

Deep visibility into all network traffic

Uncover weak attack signals

Eliminate alert fatigue

Accelerate incident response

Leverage rich network telemetry for central AI analytics

Maintain integrity of privacy and compliance initiatives

These techniques include heuristics around encrypted session fingerprinting using techniques such as JA4 and anomaly detection using artificial intelligence and machine learning. But even with these techniques in place, the network-based threat detection systems will miss some threats.

But even with these techniques in place, the network-based threat detection systems will miss some threats.

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

## THE NETWORK SECURITY MONITORING IMPERATIVE

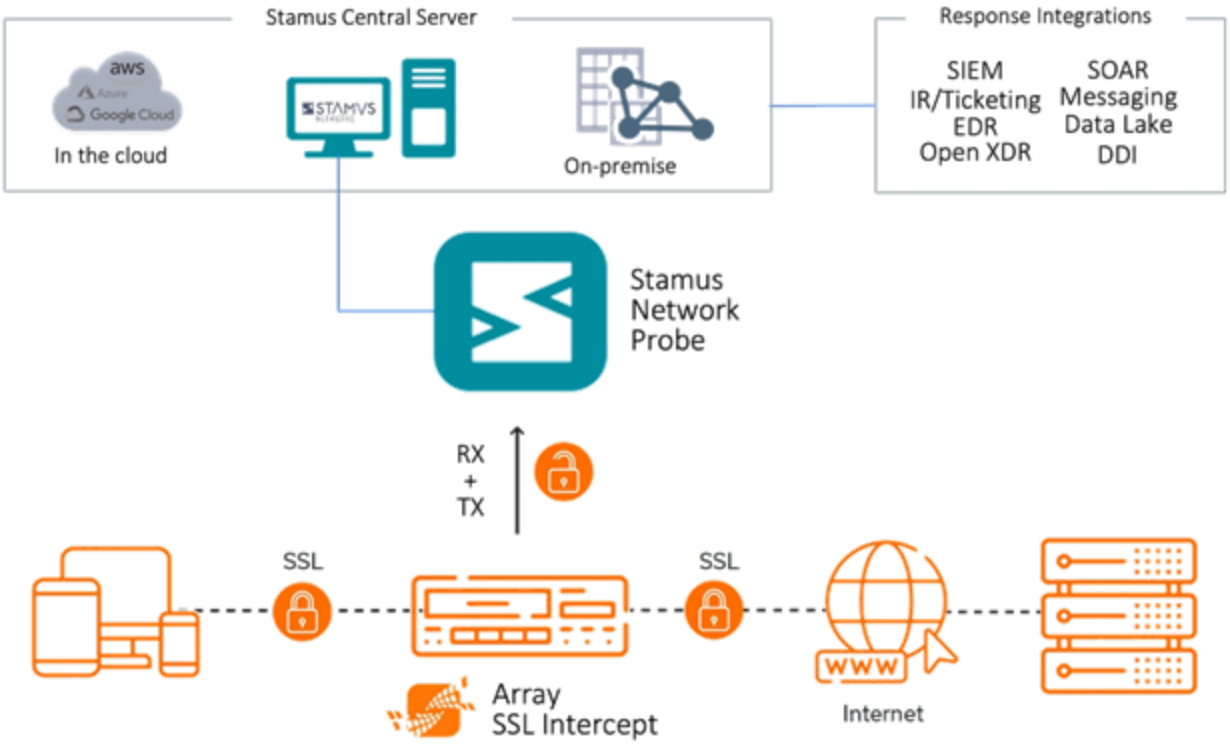
The rapid proliferation of IoT devices, network devices, and cloud infrastructure has drastically expanded the attack surface for organizations across all industries. As these attack surfaces change, organizations must adapt the way they monitor them. The growing reality is that endpoint-based security 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 Array SSL Intercept decrypts SSL traffic and then sends the unencrypted data to the Stamus Security Platform for inspection.

The Array SSL Intercept (SSLi) is a best-in-class encryption/decryption technology that acts as a proxy to decrypt SSL/TLS traffic, sends a copy of the bidirectional traffic over a single connection to the Stamus Network Probe for inspection, and then re-encrypts the traffic before it is forwarded to its destination.




Array's whitelisting ensures that sensitive information to and from trusted sites is not decrypted, and web classification helps ensure that banking, healthcare and other regulated information is processed appropriately.

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.

The combination of SSLi and SSP offers a complete solution to a historically difficult problem and provides security teams with unprecedented visibility into threats facing their organization.

## 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
- Monitor encrypted traffic for improved detection and response
- Decrypt traffic across all TCP ports using dynamic port Inspection at line rates up to 200 Gbps connections
- Provides decryption for protocols such as SMTP and POP3

- SSL/TLS proxy adjusts the cipher suite selection for encryption
- Support for multiple Stamus Network Probes with a single Array SSL Intercept instance

## SOLUTION BENEFITS

- **Deep visibility** – The Array SSL Intercept removes the SSL/TLS blind spots, allowing the Stamus Security Platform to uncover threats that might otherwise be hidden by encryption.
- **No endpoint agent required** – Other NDR decryption solutions require agents to be installed on endpoints to decrypt traffic flows.
- **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. Leverage the industry's richest network telemetry for centralized AI analytics
- **Empower threat hunters** – through a powerful guided threat hunting user interface in SSP
- **Ease of use** - Both the Array SSL Intercept and the Stamus Security Platform are easy to install, configure and integrate with other elements of your security tech stack.
- **Maintain integrity of privacy and compliance initiatives** – with flexible decryption rules and policies the Array SSL Intercept organizations can easily create granular policies to selectively decrypt traffic to meet their business needs (Example: "Do not decrypt financial or banking traffic going out of the business")

## 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