NIAGARA NETWORKS

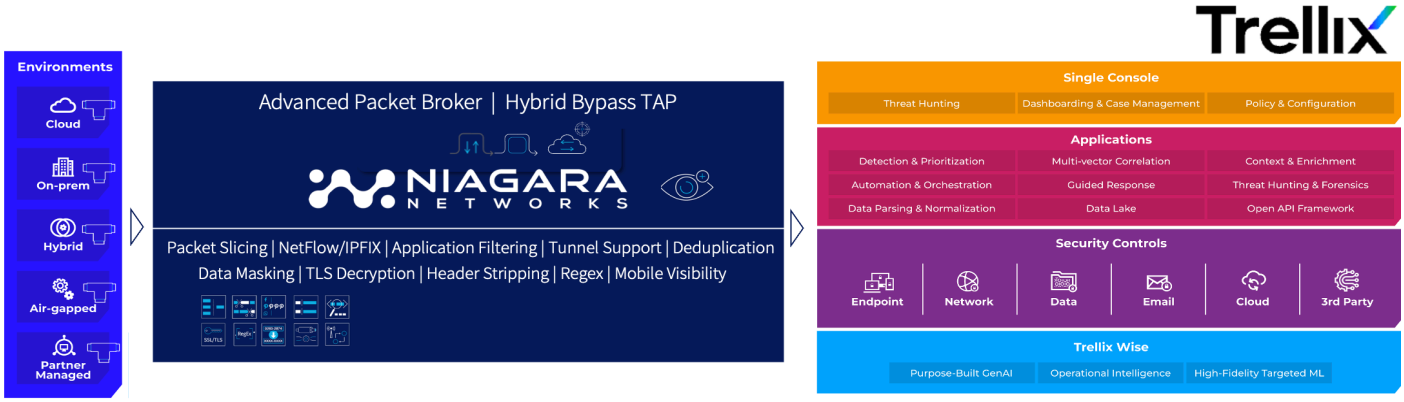
Trellix

## Solution Brief

# Trellix and Niagara Networks Empowering NetSecOps with Reliable Inline Security, Actionable Traffic Intelligence, and Advanced Threat Defense

## Introduction

The joint solution between Trellix® and Niagara Networks offers a best-of-breed security and visibility architecture. Together, we deliver resilient inline threat prevention, out-of-band monitoring, and comprehensive packet intelligence for enterprises, service providers, and government agencies operating across on-prem, cloud, and hybrid environments. By combining Trellix's world-class IPS, IDPS, NDR, DLP, and forensic capture technologies with Niagara's advanced packet brokers, Active Fail-Open (AFO) bypass, and SSL/TLS decryption, organizations gain end-to-end visibility, complete reliability, and compliance-ready operations.




## Challenges

Modern cyber threats are growing in scale and complexity, impacting enterprises, service providers, and government agencies alike:

- Encrypted traffic blind spots make it difficult for tools to detect hidden threats.
- Inline IPS/IDS deployments risk becoming single points of failure without proper bypass protection.
- Overloaded SOC/NOC tools struggle with duplicate packets, unnecessary payloads, and tunnel encapsulations.
- Hybrid and multi-cloud adoption requires consistent visibility across physical, virtual, and cloud environments.

To address these challenges across all verticals, organizations require a joint solution that delivers resilient inline deployments, intelligent traffic optimization, and scalable visibility — without compromising performance or compliance. By enabling actionable traffic intelligence and advanced threat defense, the solution empowers SecOps teams to effectively combat modern cyber threats across all network types and digital assets.

Creating a network visibility layer that routes packets without loss or performance degradation is critical.
Niagara Networks and Trellix have joined forces to address these challenges through an agile integration that delivers a unified, high-performance solution for comprehensive threat detection and traffic analysis across all network segments. This partnership provides a scalable, powerful platform that supports businesses of all types and networks of any size.

## Joint Solution Use Cases

- **Trellix IPS Inline Deployment with Niagara Packet Broker**
  Niagara Packet Brokers enable resilient inline delivery of network traffic to Trellix IPS, with policy-based filtering and optimization for accurate threat detection.

- **Trellix IDPS via SPAN/TAP Deployment with Niagara Packet Broker**
  Niagara's SPAN and TAP capabilities provide lossless access to production traffic, intelligently filtered and aggregated for Trellix IDS monitoring.

- **Niagara AFO Bypass Hardware with Trellix IPS**
  Carrier-grade Active Fail-Open (AFO) bypass hardware ensures uninterrupted IPS protection with sub-50ms heartbeat protection, supporting 1:1, 1+1, and n+1 redundancy.

- **Trellix NX / NDR Sensor Inline and SPAN/TAP Deployment**
  Niagara brokers distribute and balance traffic to Trellix NX/NDR sensors inline or out-of-band, with deduplication and tunnel termination for maximum detection accuracy.

- **Trellix Packet Capture (PX) SPAN/TAP Deployment**
  Niagara delivers high-fidelity, deduplicated traffic streams to Trellix PX appliances for packet capture and forensic analysis.

- **Niagara SSL/TLS Decryption for Trellix Tools**
  Niagara decrypts encrypted traffic and forwards it to inline or SPAN/TAP deployments of Trellix IPS, NX/NDR sensors, and DLP Monitor/Capture appliances. Supported scenarios include:
  > Active Inline Decryption
  > Passive Inline Decryption
  > Passive Out-of-Band Decryption

- **Packet/Flow Filtering & Deduplication**
  Niagara's advanced filtering and deduplication ensure Trellix IPS, NX/NDR, PX, and DLP tools receive only the most relevant, unique packets, reducing overload and false positives.

- **Scalability for Small, Medium & Large Networks**
  Niagara platforms scale seamlessly from 1G to 100G, meeting the needs of enterprises, service providers, and government agencies.

## Solution Value Proposition

Deployment architecture can be optimized to meet customer requirements and operational efficiency, whether through a modular approach or a fully integrated single-rack platform. With focused and optimized traffic flows from the Niagara Visibility platforms, Trellix threat detection operates as an agile cybersecurity solution, delivering a highly scalable, real-time threat detection and response platform with the following benefits:

### 360° Network Visibility

Network visibility for SecOps with Trellix anomaly detection, powered by machine learning and artificial intelligence, provides advanced security threat detection and automated investigation. This capability is further empowered by Niagara Networks' pervasive traffic intelligence and packet visibility, which capture all relevant traffic across digital assets and optimize intelligent traffic delivery to the Trellix security platform for comprehensive threat detection.

### Simplified and Scalable Deployments

The combination of Trellix and Niagara Networks solution makes for a perfect offering with a cost-effective business model and low TCO for midsize and large network deployments or remote locations at any rate and required micro-segmentation.

### Data Aggregation and Packet Intelligence

Security operations are improved through the efficient collection, aggregation, filtering, L2-7 packet parsing, and reduction of false positives achieved by intelligently removing data traffic duplicates delivered from network interception and aggregation points.

### Ability to inspect encrypted traffic

As an increasing share of network traffic is encrypted, effective threat detection becomes more challenging. The complementary TLS decryption capabilities are designed with a scalable, modular architecture to provide deep visibility and support uncompromising edge-to-edge security operations. The joint solution enhances SecOps by maintaining full compliance with privacy regulations while enabling thorough inspection of encrypted traffic. Advanced features such as data masking and payload slicing can be applied when required by the security architecture team, ensuring both strong threat detection and privacy preservation.

### Choosing the all-in-one platform for operational agility

Niagara Networks introduces a new generation of advanced network packet brokers built on an open platform that can host and manage security solutions directly on the appliance. This architecture enables hosting Trellix software in a highly efficient manner, making it ideal for remote sites. It delivers the full spectrum of visibility, network intelligence, and threat detection capabilities within a single appliance, enhanced by NFV-based virtual hosting.

## Deploying Trellix Threat Detection & Response Solution in conjunction with Niagara Advanced Network Visibility solution provides the following benefits:

- Ensure resiliency with always-on inline deployments protected by AFO bypass
- Achieve full visibility across physical, virtual, hybrid, and cloud environments.
- Optimize SOC/NOC operations by reducing duplicates (up to 50% of traffic), lowering false positives, and streamlining packet capture.
- Strengthen security posture with decrypted, filtered, and application-aware packet data delivered to Trellix tools for deeper inspection.
- Support compliance and privacy with payload stripping and selective forwarding to prevent unnecessary data exposure.
- Scale with confidence from 1G to 100G, supporting enterprises, service providers, and government agencies with both physical and virtual deployments.
- Future-proof operations by leveraging Niagara's modular platforms and Open Visibility hosting for Trellix's virtual sensors.

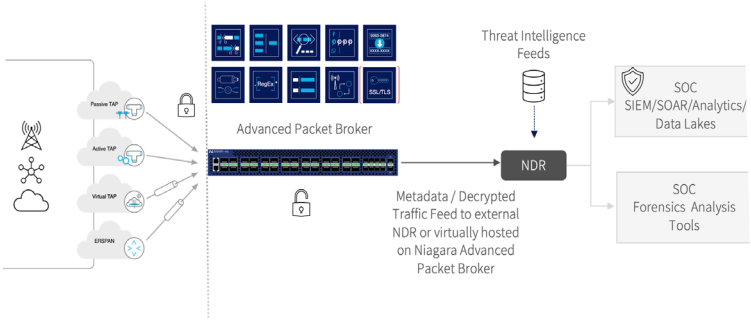
# NDR Integration Use Case

## Visibility > Optimization > Detection

Niagara Networks' advanced packet brokers serve as a bridge platform that can be deployed in either enterprise or service provider environments, providing extended visibility into private, public, and hybrid cloud networks. To efficiently collect and inspect the entire spectrum of digital assets, an intelligent network aggregation tier is required to gather the right sets of packet feeds for security tools. Strategic interception points within the network are tapped via physical or virtual TAPs, and the traffic is copied according to the defined network architecture policy. High-density aggregation is employed to scale the multiple TAP links and accommodate even more future needs, grooming all intercepted traffic to the Network Packet Broker solution.

Directing the right traffic at the required interface rates to the Trellix security stack enables effective threat detection, analysis, and response.

In addition, The Open Visibility solution can host the Trellix NDR virtually on a single appliance, leveraging hardware-accelerated traffic processing for enhanced performance. This includes advanced packet manipulation functions like header and payload slicing, masking, application filtering, metadata generation, tunnel termination (ERSPAN, GRE, NVGRE, VXLAN, GENEVE, etc.), selective TLS decryption, deduplication, and RegEx filtering to support sophisticated packet conditioning use cases.




Visibility into network traffic is the ultimate source of truth for the SOC

| Benefit | Description |
|---|---|
| Visibility | Complete packet, flow, and encrypted traffic visibility across hybrid networks. |
| Efficiency | Deduplication & header stripping cut false positives and reduce tool overload. |
| Security | TLS decryption and tunnel termination expose hidden threats to Trellix tools. |
| Compliance | Payload filtering and privacy-aware forwarding support regulatory requirements. |
| Scalability | Modular design scales from small enterprise to carrier-grade 100G deployments. |
| Agility | REST API automation enables orchestration with SOC/NOC workflows. |

## About Trellix

Trellix is a global company redefining the future of cybersecurity. The company's comprehensive, open and native cybersecurity platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through artificial intelligence, automation, and analytics to empower over 50,000 business and government customers with responsibly architected security. For more information please visit www.trellix.com.

## About Niagara Networks

Niagara Networks is a Silicon Valley-based company delivering high-performance, reliable network visibility and traffic delivery solutions for mission-critical environments. Our solutions empower Security and Network Operations Centers (SOC/NOC) with complete visibility and actionable intelligence across physical, virtual, and cloud networks. As a former division of Interface Masters, we provide all the building blocks for an advanced Visibility Layer, including packet brokers, bypass switches, network TAPs, and unified management software, offering a single pane of glass for simplified visibility infrastructure. For more information please visit: www.niagaranetworks.com.



48430 Lakeview Blvd,
Fremont, CA 94538, USA

www.niagaranetworks.com
info@niagaranetworks.com

Tel: +1 408 622 0354
Fax: +1 408 213 7529