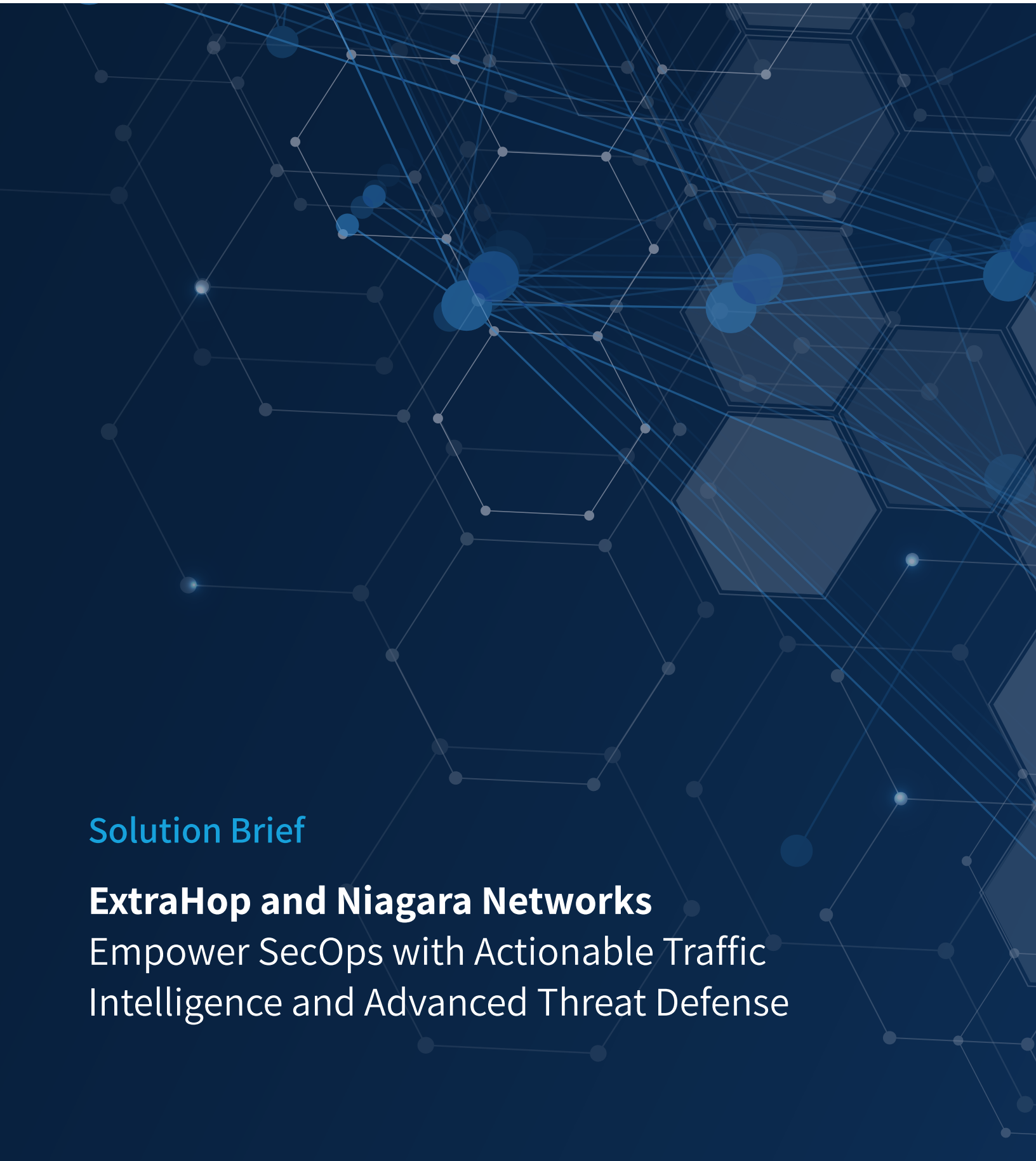


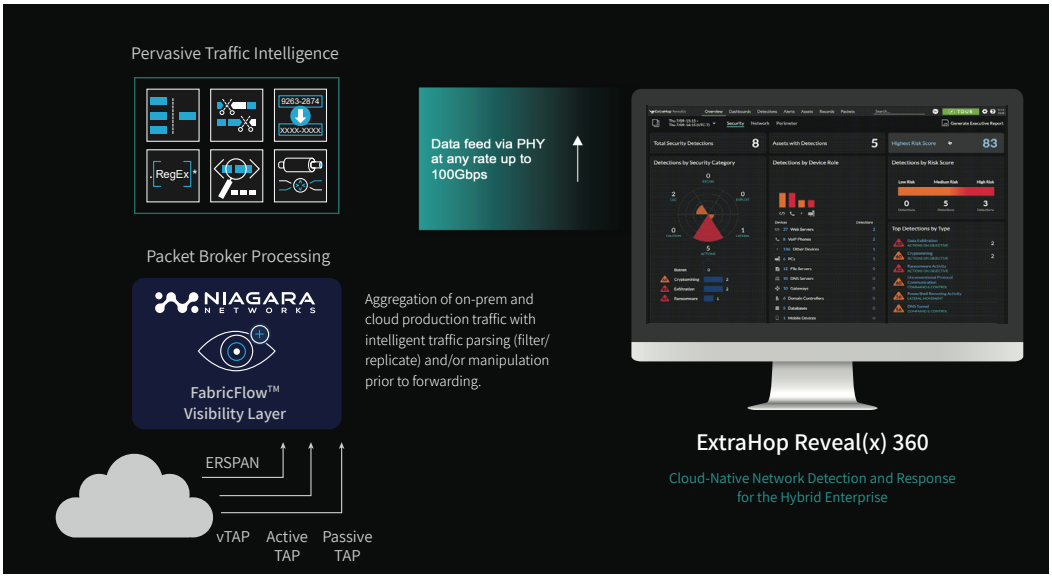
Solution Brief

ExtraHop and Niagara Networks

Empower SecOps with Actionable Traffic Intelligence and Advanced Threat Defense

Introduction

The joint solution between ExtraHop and Niagara Networks packet brokers offers the best-of-breed solution to maximize security posture by empowering consistency of network detection and response to threats across heterogeneous environments of on-prem and cloud networks.



Challenges

Modern cyber threats are more prolific and sophisticated than ever before, requiring both Enterprise Organizations and Service Providers to constantly re-evaluate their detection and incident response posture. Many traditional tools like Intrusion Detection and Prevention Systems have failed to rapidly adapt to the current threat landscape and suffer from traditional deployment methodologies that focus exclusively on traffic to and from the internet while leaving organizations blind to threats inside their enterprise, cloud, and hybrid environments. Network Detection and Response (NDR) with integrated IDS capabilities is designed to address these shortcomings.

The only way to get value from sophisticated network security tools and an ever-growing cybersecurity budget is to ensure that packets (malicious or otherwise) can't reach the large span of the enterprise domain without being analyzed.

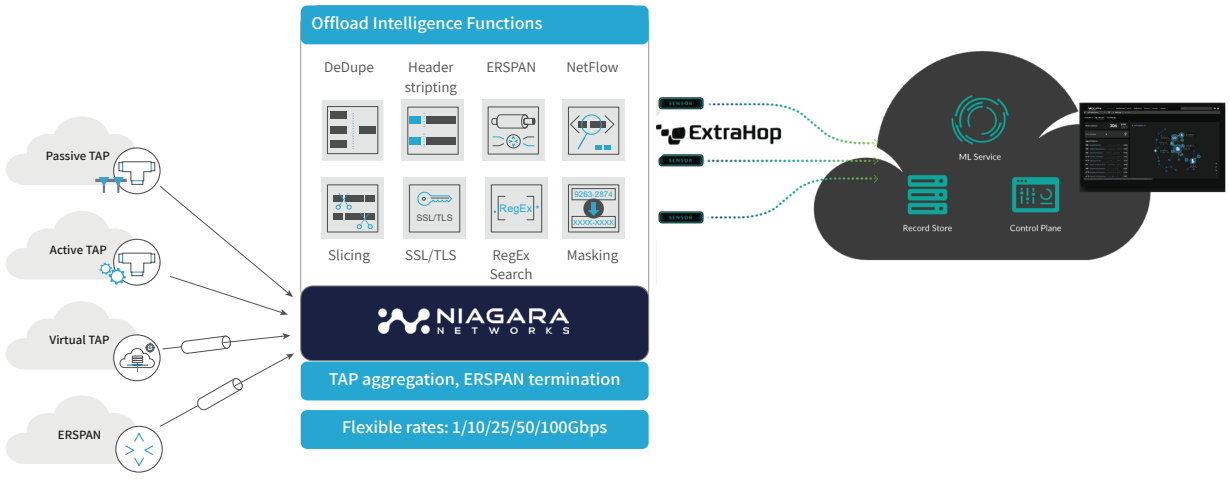
Creating a network visibility layer that properly routes packets without dropping them or negatively impacting performance is critical. Niagara Networks and ExtraHop has joined forces to solve these challenges, by creating an agile integration that enables a unified high-performance solution with full packet visibility and traffic analysis across all network segments. The partnership provides a scalable and powerful Network Detection & Response (NDR) solution to address the following challenges:

- Complex and long SecOps processes in detection and response to threats and intrusions across heterogenous environments of on-prem and cloud networks
- Traditional cybersecurity defenses lack the agility for rapid response against increasingly dynamic threats
- The enormous flood of data that can overwhelm a legacy security stack without effectiveness to separate signal from the noise

The joint solution enables deep visibility and regulation of the data traffic through multiple deployment scenarios and policy-based actionable threat detection and prevention through joint building blocks and holistic architecture that can be extended to state-of-the-art unified platform based on disaggregation, virtual hosting, service chaining in a multi-vendor security stack that can span a wide array of demarcation points of service.

Solution Benefits

Deployment architecture can be optimized for customer requirements and operational efficiency based on the modular approach or a highly integrated platform for a single rack solution offering.



With focused and optimized traffic flows from the Niagara Visibility platforms, the ExtraHop Reveal(x) platform operates as an agile cybersecurity solution to deliver a highly scalable real-time threat detection and response solution with the following benefits:

- 360° Network Visibility

360° network visibility to SecOps with ExtraHop Reveal(x) anomaly detections powered by machine learning for security threats and automated investigation, empowered by Niagara Networks' pervasive traffic intelligence and packet visibility that captures all traffic of interest from the entire digital assets and optimize intelligent traffic delivery to the ExtraHop Reveal(x) 360 platform for comprehensive threat detection.

- Simplified and Scalable Deployments

The combination of ExtraHop Reveal(x) and Niagara Networks solution makes it 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

Efficient data traffic collection, aggregation, filtering, L2-7 packet parsing and reduction of false positives for security operations by intelligent removal of data traffic duplicates, that are delivered from network interception and aggregation points.

- Ability to inspect encrypted traffic

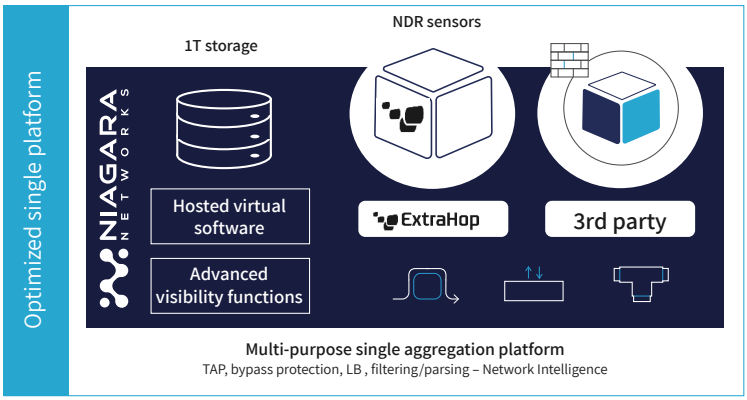
As an increasing amount of network traffic is encrypted, threat detection becomes harder. The complementary SSL/TLS decryption capabilities can be architected for a scalable and modular approach to enable deep visibility and effectiveness of uncompromised edge-to-edge security operations. A joint solution optimizes SecOps with full compliance with privacy regulations while enabling deep visibility and inspection of encrypted traffic, including decryption of MS active directory services and a wide spectrum of protocols including Kerberos, NTLM, LDAP/s, MS-RPC, WINRM, SMBv3, and WMI.

- ExtraHop Reveal(x) 360 Dashboard for actionable Visibility and Response

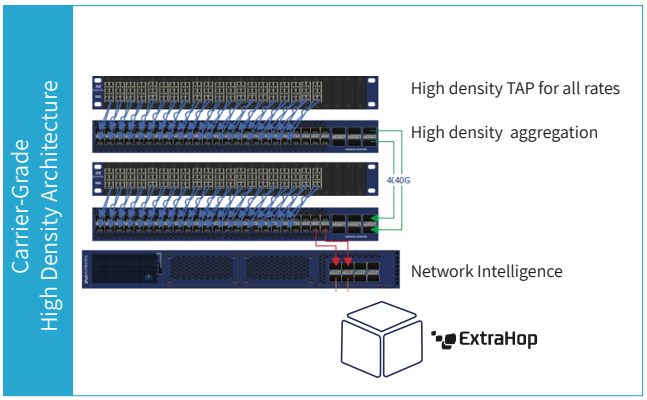
The precision and high fidelity of data optimization to ExtraHop Reveal(x) automatically generates the accurate attack visualizations that render to SOC the context it needs to quickly respond to cyber threats in seconds.

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

A new style of advanced network packet broker with an open platform that can host and manage the security solutions that run on it. Niagara Networks Open Visibility Platform can host ExtraHop virtual sensors– a highly efficient architecture that can fit remote sites with the entire range of visibility and network intelligence functions and threat detection in a single appliance with NFV virtual hosting capabilities.



Solution for remote sites



Solution for mid-size and large installations

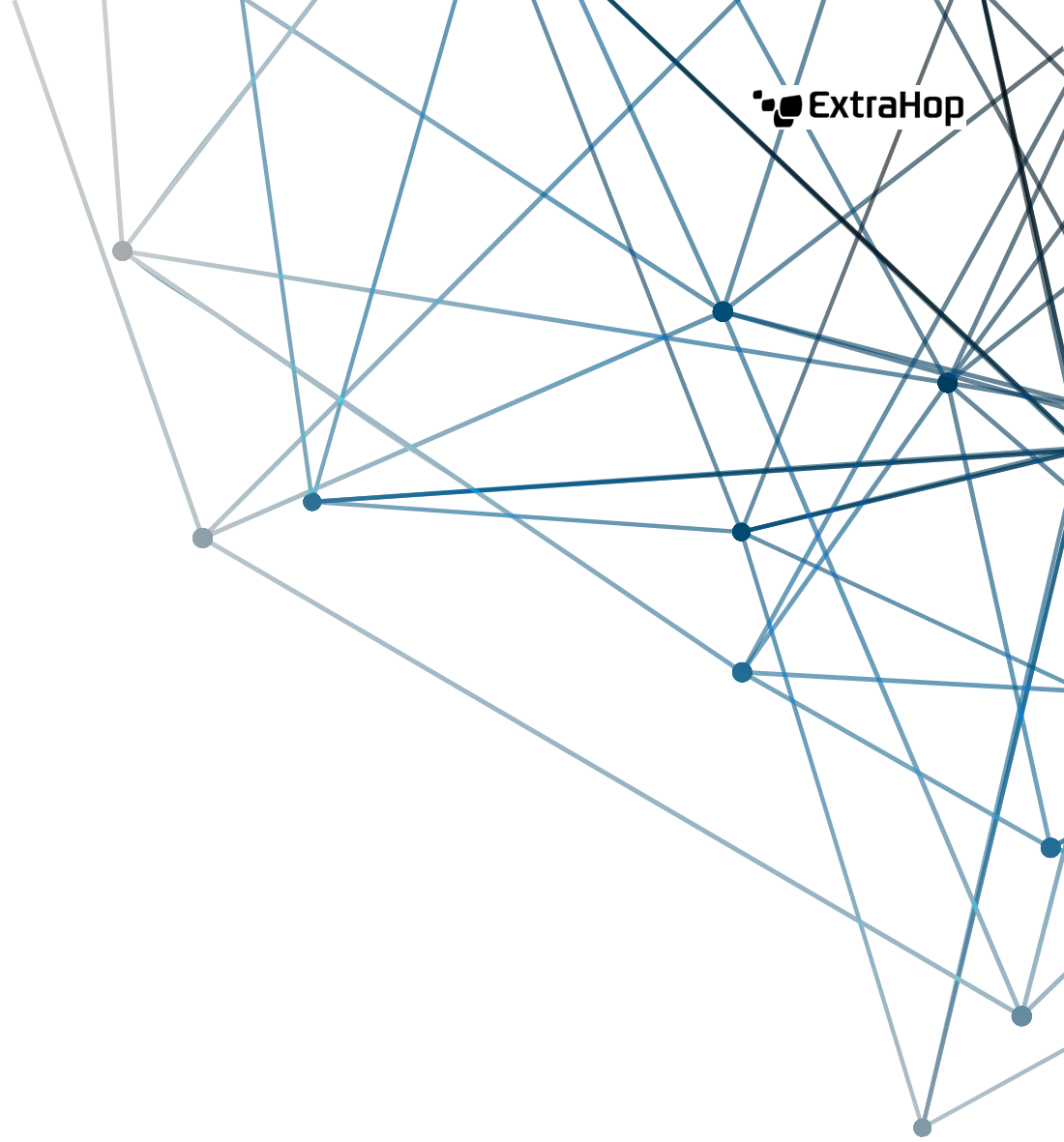
Integration Use Cases

Niagara Networks' advanced packet brokers serve as a bridge platform that can be deployed in an enterprise or service provider environment, with extended visibility to private, public, and hybrid cloud. To enable the efficient collection and inspection of the entire spectrum of the digital assets, an intelligent network aggregation tier is required to obtain the right sets of packet feeds to security tools. Strategic interception points in the network tapped via physical or virtual TAPs and copy the traffic per defined network architecture policy. High density aggregation deployed to scale the multiple TAP links to accommodate even more needs in the future by grooming all intercepted traffic to Network Packet Broker solution and enable highly efficient aggregation architecture that can be deployed and provisioned by Niagara's SDN-based software orchestration controller. The right traffic steered at the required interface rates to ExtraHop Reveal(x) architecture for threat detection, analysis, and response. Advanced and a highly integrated solution can enable the same workflow, but with a new state-of-the-art migration to the Niagara Networks Open Visibility Platform in the future.

The Open Visibility solution can host NDR sensors virtually on a single appliance with hardware-accelerated traffic processing, with including advanced packet manipulations functions such as header and payload slicing, masking, application filtering, metadata generation, overlay tunnel termination (ERSPAN, GENEVE, VXLAN, GRE, etc.) selective decryption, deduplication, and RegEx filtering for ultra-deep sophisticated packet conditioning use cases.

Deploying ExtraHop Reveal(x) NDR platform in conjunction with Niagara Networks Advanced Network Visibility solution provides the following benefits:

- Solves architectural complexity whilst creating clear segmentation, aggregation, and intelligent processing of network traffic to ExtraHop NDR
- Streamline Reveal(x) security analytics and advanced threat inspection and prevention
- Maximize tool efficiency and scale-optimization of traffic capacity and reduction of duplicated and non-relevant headers and payload to avoid false positives and processing overhead
- Attractive OPEX and CAPEX with optimized aggregation of TAP elements and operational simplicity
- Ultra-high granular view of packet flows from any TAP use case including Niagara's CloudRay virtual TAP solution
- Advanced header stripping for overlay and underlay protocols: ERSPAN, FabricPath, GENEVE, GRE, NVGRE, VXLAN, VLAN, VN tag, PPPoE, GTP, MPLS (GRE), MPLS (IP), MPLS (UDP), and many more packet and flow intelligence rules to streamline security operations
- Ability to intercept 100% of traffic at 1Gbps, 5Gbps, 10Gbps, 25Gbps, 40Gbps, 50Gbps and 100Gbps and any traversing communication protocols, including East-West traffic with a virtual TAPs
- Ability to migrate seamlessly to Niagara Networks Open Visibility Platform for Next-Gen virtual tools adaption and operational agility



About ExtraHop

ExtraHop was founded with a clear mission: to help organizations stop advanced threats with security that can't be undermined, outsmarted, or compromised. The company created a fundamentally new way to harness the power of network intelligence at the speed and scale of business. ExtraHop Reveal(x) 360 platform combines the power of cloud-scale AI with the simplicity of SaaS to defend against advanced threats like supply chain attacks, APTs, and zero days, providing security from core to cloud to edge. Cyberattackers can't hide on the network, but Reveal(x) can, giving security teams a secret weapon to detect threats, investigate incidents, and stop breaches fast—before they compromise your business.
For more information visit us at www.extra hop.com

About Niagara Networks

Niagara Networks provides high performance network visibility solutions for seamless administration of security solutions, performance management and network monitoring. Niagara Networks products provide advantages in terms of network operation expenses, downtime, and total cost of ownership. A former division of Interface Masters, Niagara Networks provides all the building blocks for an advanced Visibility Adaptation Layer at all data rates up to 100Gb, including TAPs, bypass elements, packet brokers and a unified management layer. Thanks to its integrated in-house capabilities and tailor-made development cycle, Niagara Networks are agile in responding to market trends and in meeting the customized needs of service providers, enterprise, data centers, and government agencies. For more information please visit us at 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