# Niagara Networks and Endace

NIAGARA NETWORKS

## Accelerate incident response and simplify network architecture with enterprise-wide visibility and continuous network packet capture.

The dynamic nature and complexity of today's modern networks make it critical for SecOps and NetOps teams to have visibility into all the activity happening across the network so they can manage performance, monitor network reliability and protect the network from security threats. Blind spots and vulnerabilities in your infrastructure can severely impact business productivity and security. Combining Niagara Networks visibility solutions with Endace's scalable, high-speed network recording gives SecOps and NetOps teams unparalleled visibility into network activity and provides the evidence analysts need to quickly and effectively identify and remediate network performance and security issues.

Niagara Networks provides the building blocks for an advanced visibility adaptation layer including TAPs, bypass switches, advanced network packet brokers and a unified management layer. This complete network visibility toolkit enables NetOps and SecOps teams easily and efficiently manage multiple security tools, enabling scale and flexibility while reducing operational expense and downtime.

EndaceProbe™ Analytics Platforms capture, index and store network traffic with 100% accuracy while simultaneously providing hosting for a wide variety of network security and performance monitoring applications in Application Dock™, the EndaceProbe's built-in hosting environment.

Customers can extend their network and security monitoring capability by deploying instances of virtual applications anywhere they have EndaceProbes deployed. Hosted solutions, from partners including Cisco, Darktrace, Palo Alto Networks, Fortinet and many others, can analyze real-time traffic at full line-rate for real-time detection or analyze recorded Network History for powerful back-in-time investigation.

The ability to deploy solutions quickly onto a common hardware platform lets customers expand and adapt their monitoring infrastructure to meet new emerging threats or monitoring needs and scale as network speeds and loads increase.

## Confidently Accelerate Investigations

The ability to monitor, record, and analyze large amounts of network traffic across the enterprise or service provider network typically requires multiple network analyzers placed separately in different networks.

By connecting Niagara Networks Advanced Packet Brokers to EndaceProbe™ Analytics Platforms, traffic on different segments of the network can be easily aggregated, filtered, deduplicated, decrypted, and delivered to EndaceProbes for recording, inspection, and analysis by hosted applications. The joint solution can scale and deliver for the most demanding network security operations.

The Niagara Networks visibility toolkit can also mirror or bypass traffic in the event of a network failure, to ensure that EndaceProbes can capture and investigate network traffic seamlessly without interruption.

SecOps or NetOps analysts can drill down in context of alerts, threat indicators or performance issues to analyze the related full packet data in EndaceVision. The EndaceProbe's Pivot-to-Vision API uses the IP address and time range of the trigger event to focus the analyst directly on relevant incident data. EndaceVision, lets them dissect, review and extract the relevant traffic from weeks or months of Network History recorded on the network. EndaceVision enables analysis to microsecond level detail with views filtered by Application, IP, Protocol, Top Talkers and many other parameters, providing rapid insights and enabling accurate conclusions.

Being able to get directly to the related packets with a single click lets security analysts rapidly establish the root cause of issues they are investigating and conduct efficient threat hunting across the network. They can respond quickly to threats, dramatically reducing the time to resolve critical incidents and minimizing the risk of security threats escalating to become more serious breaches.

### PRODUCTS

**Niagara Networks Advanced Hybrid Packet Broker**

**Niagara Networks TAPs**

**EndaceProbe Analytics Platform**

### BENEFITS

- Eliminate blind spots in physical, virtual and cloud networks to increase the overall 360 degree security posture
- Ultra-high resolution view of traffic intelligence - including TLS 1.3 encrypted data flows
- Scalable traffic optimization supports terabytes of aggregation capacity, filtering, deduplication, allowing traffic to be directed to where it's needed in the right format
- Streamlined investigation workflows from other tools your SecOps or NetOps teams use.
- One-click access to full definitive packet evidence, accelerates investigation and remediation and enables accurate reconstruction of events.
- Reduced threat exposure through greater analyst productivity and faster incident investigation.
- Definitive evidence trail with an accurate record of all relevant packets.

© Copyright Endace Technology Limited, 2023. All rights reserved. Information in this data sheet may be subject to change.

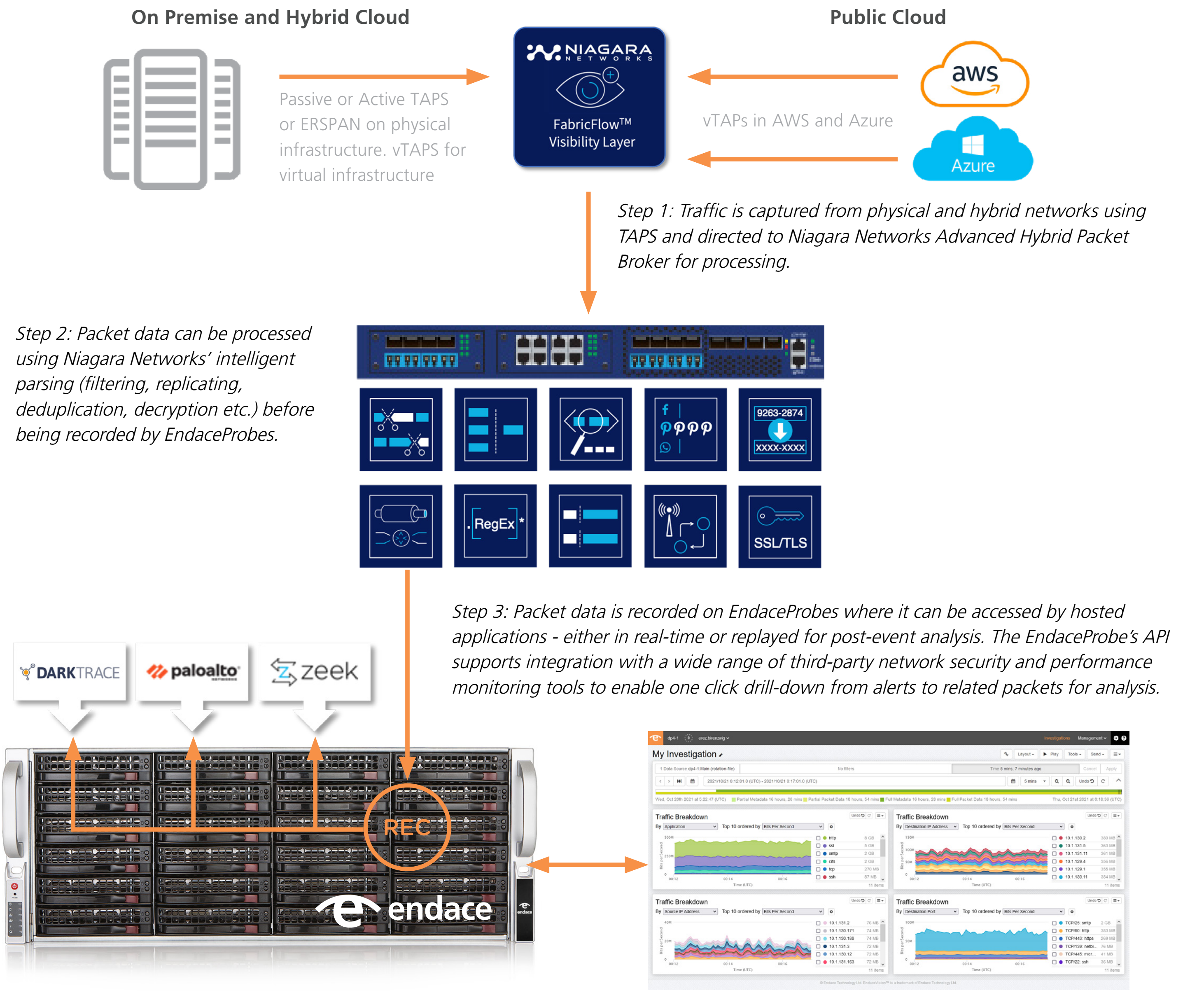
## Conclusion

Combining Niagara Networks visibility solutions with the EndaceProbe's 100% accurate Network History delivers network wide security analytics and always-on recording. This provides definitive evidence that gives SecOps and NetOps teams the time and accurate forensic data they need to investigate and resolve even the most complex investigations.

Combining the two technologies lets security teams respond to alerts faster and investigate threats with more confidence across both their physical and cloud environments. Decryption of traffic before it is recorded gives SecOps teams visibility into threats that might otherwise be hidden in encrypted traffic.

Additionally, by hosting third-party analytics tools in the EndaceProbe's Application Dock hosting environment, customers can extend their monitoring coverage without additional hardware deployments, enabling them to reduce cost by leveraging EndaceProbe hardware to extend traffic monitoring and analysis capability.

## How it Works



*Step 1: Traffic is captured from physical and hybrid networks using TAPS and directed to Niagara Networks Advanced Hybrid Packet Broker for processing.*

*Step 2: Packet data can be processed using Niagara Networks' intelligent parsing (filtering, replicating, deduplication, decryption etc.) before being recorded by EndaceProbes.*

*Step 3: Packet data is recorded on EndaceProbes where it can be accessed by hosted applications - either in real-time or replayed for post-event analysis. The EndaceProbe's API supports integration with a wide range of third-party network security and performance monitoring tools to enable one click drill-down from alerts to related packets for analysis.*

For more information on the Endace portfolio of products, visit: endace.com/products

For further information, email: info@endace.com

Endace™, the Endace logo, Provenance™ and DAG™ are registered trademarks in New Zealand and/or other countries of Endace Technology Limited. Other trademarks used may be the property of their respective holders. Use of the Endace products described in this document is subject to the Endace Terms of Trade and the Endace End User License Agreement (EULA).

© Copyright Endace Technology Limited, 2023. All rights reserved. Information in this data sheet may be subject to change.