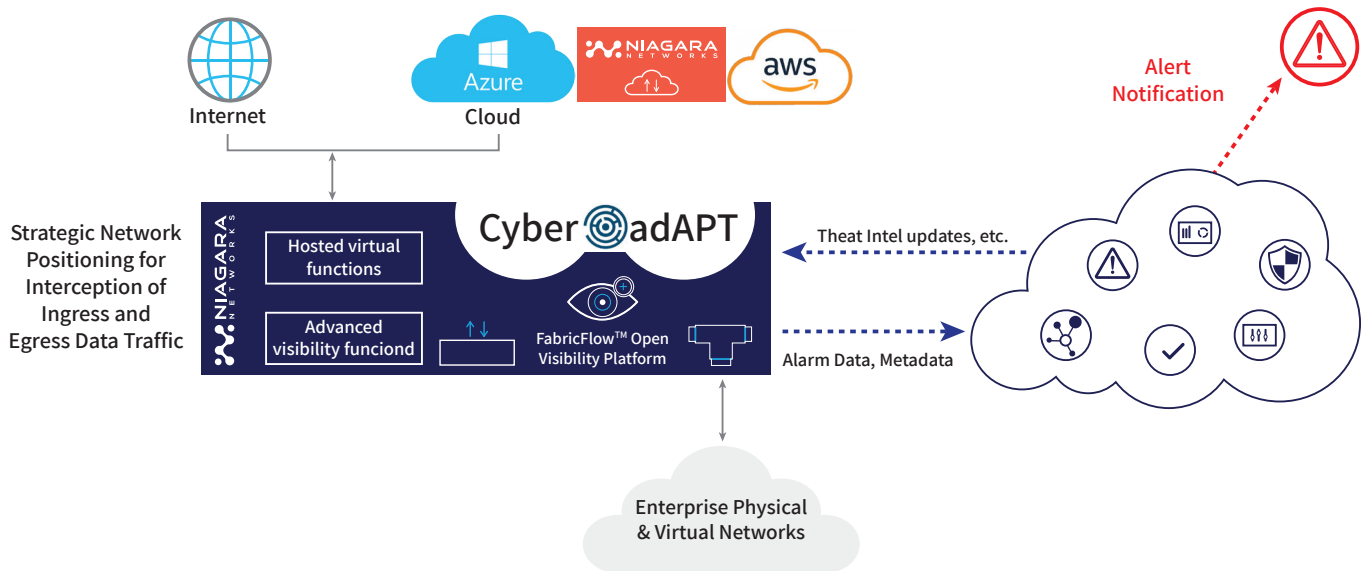# NIAGARA NETWORKS

Cyber adAPT

Solution Brief

Niagara Networks & Cyber adAPT

Niagara Networks and Cyber adAPT Deliver Integrated High-Performance Network-Based Cybersecurity

Introduction

Cyber adAPT and Niagara Networks have combined several of their unique technologies into a high- performance, cost-optimized, network-based threat detection solution that provides advanced cyber security protection for all traffic traversing the Niagara Networks' visibility fabric. Leveraging Niagara Network's Open Visibility Platform™, Cyber adAPT has added its patent-pending Optimized Packet Inspection® technology coupled with sophisticated threat intelligence to create a powerful, cost-effective cyber security solution. The combined solution identifies malicious traffic early and provides the option to automatically block this traffic before any damage is done.

Cyber adAPT and Niagara Networks empower SecOps
with actionable traffic intelligence and threat defense solution
across heterogeneous environments of on-prem and cloud networks

Challenges

Today's need for advanced cyber security protection is paramount. Cyber risk is one of the top threats facing businesses across the globe. Many Enterprises are especially vulnerable to a wide variety of cyber-attacks due, in many cases, to a shortage of existing cybersecurity measures, as well as the lack of awareness of how vulnerable their Enterprise is to attack. This situation makes the risk of digital assets loss so much greater. The impact of any attack can be significant ranging from ransomed data to the theft of valuable information including Intellectual Property. .

Enterprises are exposed to many types of cyber threats

Malware

Ransomware

Exploit

Malware- installs malicious files inadvertently downloaded by users:

- Slowing computer or web browser speed
- Causing device to freeze or crash
- Stolen sensitive information

Ransomware- encrypts company data and demands ransom be paid:

- Permanent loss of company data
- Shutdown of company operations
- Financial loss

Exploit- take advantage of security flaws in software applications:

- All software has vulnerabilities
- Are a method for attackers to deliver malware, run code, or steal sensitive data
- Constantly being discovered and require vigilant patching to fix

In order to establish a strong cybersecurity stance, enterprises must adopt solutions that take into account the limitations of their existing security resources, which may be limited by financial, human, or technical factors. To minimize risk, enterprises require security solutions that are simple to manage, cost-effective, and do not require in-house cybersecurity expertise. In the event of a cyber-attack, these solutions must quickly identify affected assets, reduce the mean time to remediation, and if necessary, block the attack BEFORE any damage is done.

Many challenges exist that make it difficult for the majority of Enterprises to incorporate the appropriate level of cyber security stack. These include:

1. High cost and complexity requiring, in many cases, dedicated resources from both the Enterprise and the solution provider.

2. The need for multiple, physical boxes or virtual instances to perform all the necessary cyber security functions driving cost and negatively impacting network performance.

3. The requirement for large levels of compute resources to provide sufficient detection capability for the amount of traffic entering and leaving the Enterprise.

4. The burden placed on individuals in the Enterprise to constantly maintain a current level of cyber security and manually deal with attacks as they occur.

The Niagara Networks and Cyber adAPT joint solution addresses these challenges by delivering a fully integrated, unified single-box solution that works as follows:

| All Enterprise traffic flows through the Niagara Packet Broker (NPB) | Leveraging the NPB and TAP functions duplicate traffic is forwarded to the OVP environment | OPI© technology slicing is enabled leveraging Niagara and Cyber adAPT technology | OPI© technology detection then analyzes the appropriate traffic to identify malicious activity | When necessary, the OPI© technology Detection Engine initiates a block of the malicious traffic leveraging the NPB capabilities |

The combined solution results in 10X threat detection performance at significantly lower cost than typical NDR/NTD solutions. Key drivers for the lower cost include:

Single Box Solution– A fully integrated solution requiring no additional external hardware and connections to enable a cost-effective business model and low TCO for midsize and large network deployments or remote locations at any rate and required micro-segmentation. This significantly reduces the hardware footprint and complexity of installation driving the lowest possible cost compared to typical NDR/NTD solutions.

360° network visibility- Anomaly detection across the entire 360° attack surface, powered by Cyber adAPT's NTD toolkit for non-intrusive automated, and contextual information that categorizes the risk and urgency of the threat, empowered by Niagara Network's converged packet broker solution for comprehensive deep flow data visibility that captures all traffic of interest from the entire digital assets and optimizes intelligent traffic delivery to the Cyber adAPT NTD platform.

High Performance Detection- OPI® technology typically requires 10X less compute resources than competing solutions. This means that all Enterprise traffic can still be monitored leaving available resources for other tasks in a common OVP environment further driving down costs.

Zero Touch Needed by the End User– As a fully integrated solution, everything works immediately from turn up. All network threat detection functions are fully automated including maintaining the very latest threat intelligence as well as blocking malicious traffic when required.

Flexible Deployment Options– The joint solution can be deployed on any Niagara platform that supports OVP in both physical and virtual implementations across private and public clouds. If multiple NPB deployments are needed, the joint solution can run across multiple OVP environments and act as a single entity cluster.

No additional Software at the Enterprise– The joint solution does not require additional software to be deployed at any of the Enterprise locations avoiding installation and maintenance challenges and complementing existing cyber security solutions that are deployed.

About Cyber adAPT

Cyber adAPT NTD secures every segment of the digital enterprise, finding greater numbers of attacks more quickly than competing solutions. The Cyber adAPT NTD threat detection solution monitors 100% of network traffic in real-time, without an impact on network performance. cyberadapt.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 niagaranetworks.com.

NIAGARA NETWORKS

48430 Lakeview Blvd
Fremont, CA 94538, USA

www.niagaranetworks.com
info@niagaranetworks.com

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