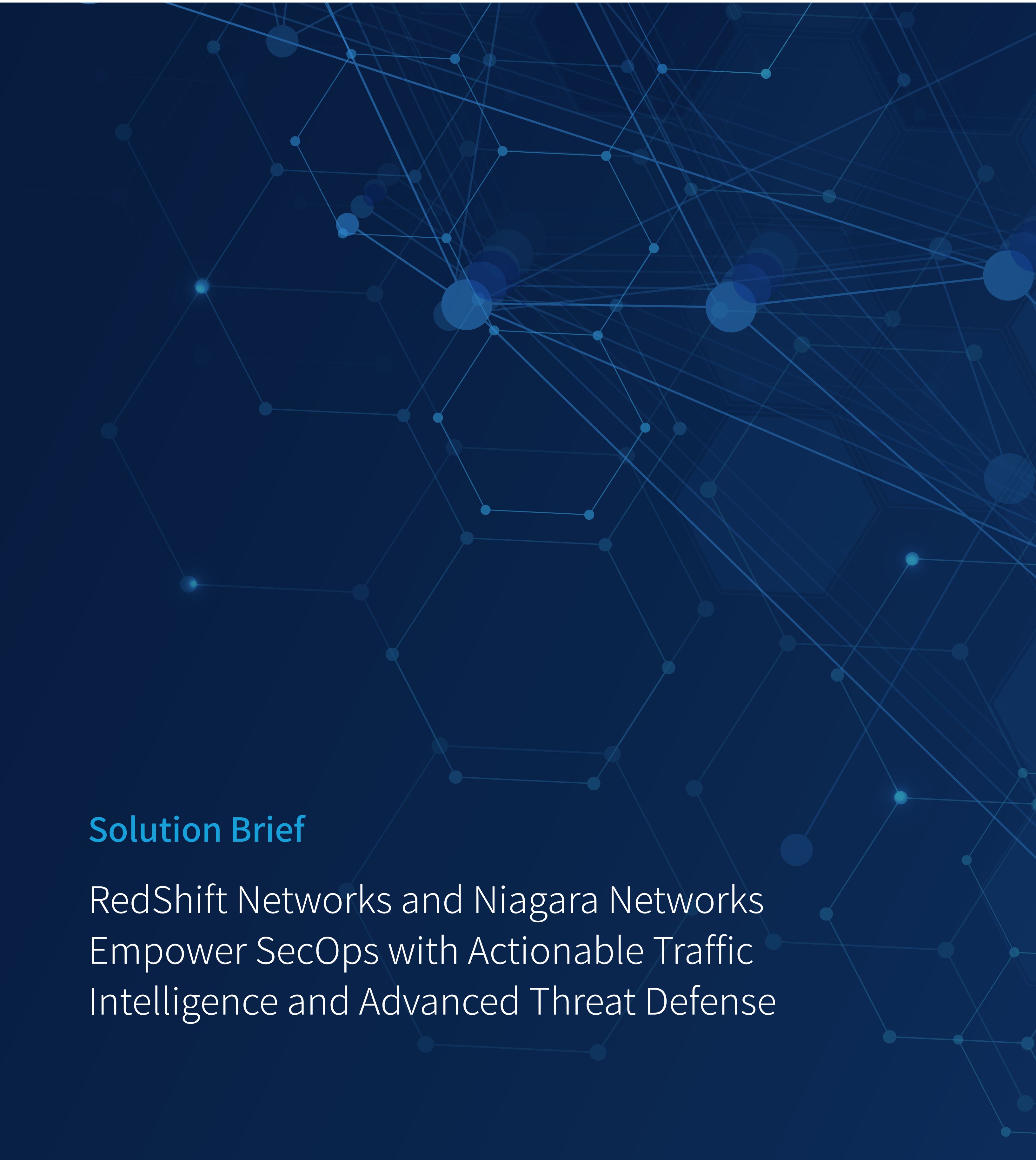
NIAGARA NETWORKS

REDSHIFT NETWORKS

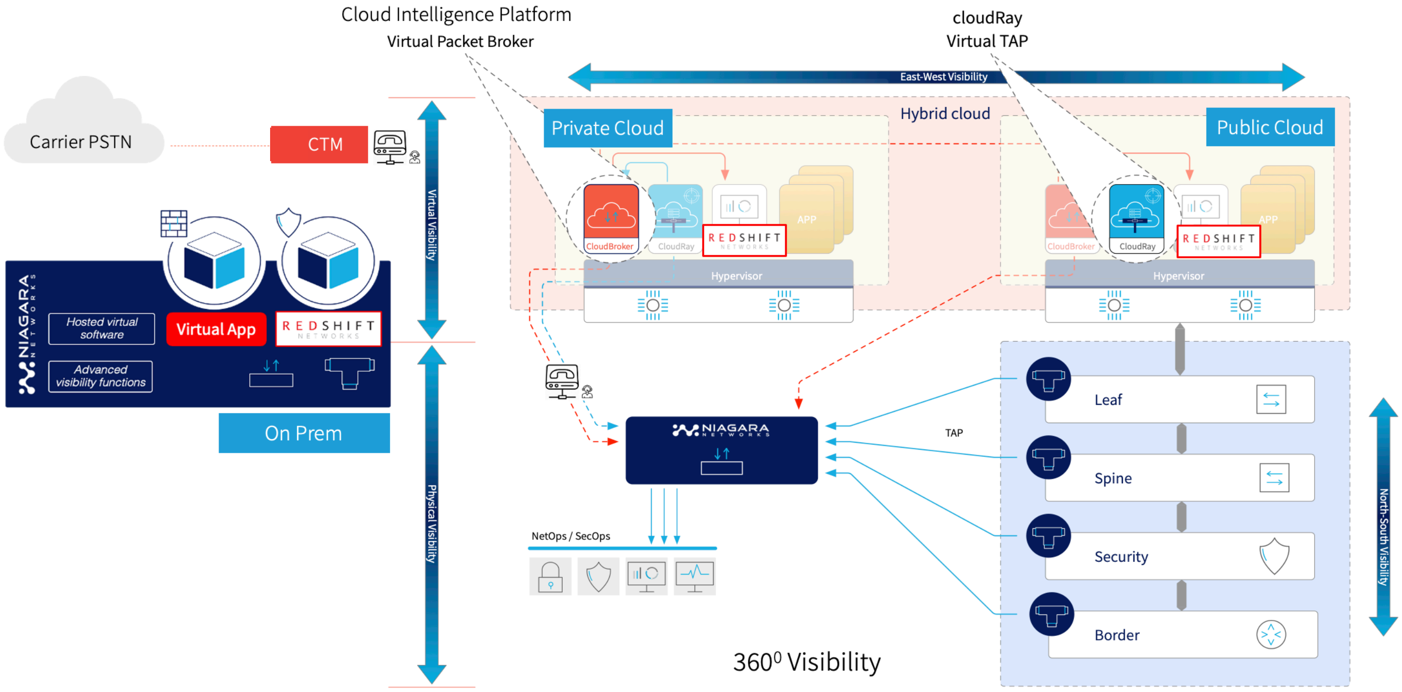


Solution Brief

RedShift Networks and Niagara Networks Empower SecOps with Actionable Traffic Intelligence and Advanced Threat Defense

Introduction

The integrated solution between RedShift Networks real-time IP voice security and fraud protection software 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. This is now even more true with the emergence of AI-driven attacks. RedShift Networks' real-time Communications Threat Management (CTM) platform 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 RedShift Networks have joined forces to solve these challenges, by creating an agile integration that enables a unified high-performance solution with full IP voice packet visibility and traffic analysis across all network segments. The partnership provides a scalable and powerful Communications Threat Management (CTM) service to address the following challenges:

- Traditional next-gen firewalls lack the thorough understanding of voice protocols to effectively monitor traffic without impacting the quality of IP voice
- Without access to a continuously updated, real-time, global voice network threat intelligence database, perimeter devices do not have sufficient visibility to detect and block IP voice threats
- Attackers are now leveraging artificial intelligence (AI) to devise and deliver sophisticated attacks that are not detected without global IP voice threat intelligence and specialized
- Administrators lack a single pane of glass to correlate IP voice security and fraud events in real-time and provide reporting for investigation and compliance
- Mobile phone spam, number spoofing and related social engineering attacks that lack call authentication are having a direct impact on enterprise security
- SecOps teams are challenged to detect, investigate and respond to a wide range of IP voice threats, including social engineering, across a distributed enterprise
- Data overload can overwhelm a legacy security stack, making it ineffective at separating signal from noise

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 RedShift Networks CTM and Mobile Call Assurance service operates as an agile cybersecurity platform to deliver a highly scalable real-time threat detection and response solution with the following benefits:

360° Network Visibility

Network visibility to SecOps with RedShift Networks anomaly detection powered by machine learning and artificial intelligence 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 RedShift CTM platform for comprehensive IP voice threat detection.

Simplified and Scalable Deployments

The combination of RedShift Networks 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

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 uncompromisable edge-to-edge security operations. The 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.

Dashboard for actionable Visibility and Response

The precision and high fidelity of data optimization of RedShift Networks' service automatically generates the accurate attack visualizations that render to a SOC the context needed 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 RedShift Networks software in 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.

Deploying RedShift Networks CTM service in conjunction with Niagara Networks Advanced Network Visibility solution provides the following benefits:

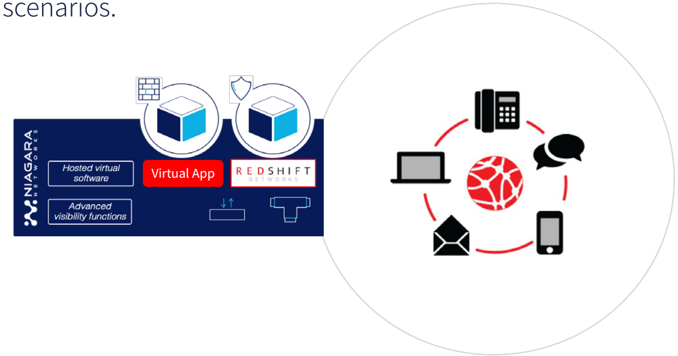
- Solves architectural complexity whilst creating clear segmentation, aggregation, and intelligent processing of IP voice traffic to RedShift Networks (CTM) at 100Gbps near wire-speed packet processing
- Streamline RedShift Networks (CTM) real-time security analytics and advanced threat inspection and 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
- Ultra-high granular view of packet flows from any TAP use case including Niagara's CloudRay virtual TAP solution and cloud packet broker functions via Niagara Networks' Cloud Intelligence Platform (CIP)
- 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 to Niagara Networks Open Visibility Platform for NextGen virtual tools adaption and operational agility

Integration Use Case

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 copy the traffic 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 or tunneling it to Niagara Networks' Cloud Intelligence Platform (CIP). This enables a highly efficient aggregation architecture that can be deployed and provisioned using Niagara's SDN-based software orchestration controller.

Directing the right traffic at the required interface rates to the RedShift Networks architecture enables effective threat detection, analysis, and response. Advanced solutions can achieve the same workflow, but with a seamless migration to the Niagara Networks' Open Visibility Platform or the Cloud Broker virtualized environment in the future.

The Open Visibility solution can host the RedShift's CTM service 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 decryption, deduplication, and RegEx filtering to support sophisticated packet conditioning use cases. Niagara Networks' Cloud Intelligence Platform (CIP) solution provides a single, holistic platform that allows security, network, and application analysts working at different locations to access and analyze network traffic. This solution is particularly useful for organizations that have security tools and analysts located at various geographically dispersed sites and hybrid cloud scenarios.



About RedShift Networks

Headquartered in the San Francisco Bay Area, RedShift Networks delivers worldclass, real-time security and fraud protection with underlying analytics for IP voice networks. RedShift's single pane of glass Communication Threat Management (CTM) platform supports the STIR/SHAKEN framework for regulatory compliance and provides end-to-end visibility and automated mitigation against known and emerging IP voice threats, including Robocalls, Toll Fraud, TDoS and AI driven threats. Powered by a continuously updated global IP voice threat intelligence database, the highly scalable CTM and mobile device Call Assurance provides protection for Enterprise, Service Provider and Carrier managed voice networks worldwide.
For more information, please visit us at www.redshiftnetworks.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