JOINT SOLUTION BRIEF

Secure VoIP and Cloud Communications with RedShift Networks and Gigamon

The Challenge

Voice over IP (VoIP), SIP and Unified Communications (UC) networks and services face a variety of threats – malware-infected endpoints, underlying operating system (OS) and protocol implementation vulnerabilities, voice denial-of- service (DoS), Robocalls/Spam over Internet telephony (SPIT) attacks and UC application-layer attacks and device configuration weaknesses. The challenge is to be able to see, detect, and mitigate these threats and intrusions.

Integrated Solution

Integrated with the Gigamon® Visibility and Analytics Fabric (inclusive of GigaVUE-HC and GigaVUE V series), the RedShift Networks Unified Communications Threat Management (UCTM) Platform – inclusive of Hawk, Eagle and Condor systems, virtualized UCTM software (vUCTM) and Cloud UCTM – accesses network traffic and detects anomalous VoIP traffic patterns to thwart cyberattacks and troubleshoot misconfigurations.

Joint Solution Benefits

- Comprehensive security solution developed for SIP-enabled services, such as VoIP, IMS, VoLTE, 5G, and UC/Collaborations applications.
- Intelligent session initiation protocol, real-time transport protocol (SIP/RTP) correlation helps the RedShift Networks UCTM proactively resolve voice communication security by addressing complex network transport issues in real-time.
- Enhanced visibility and easy access to traffic from physical, virtual and public cloud networks through the Gigamon Visibility and Analytics Fabric (VAF).
- SSL decryption by the VAF to avoid unnecessary processing by RedShift Networks UCTM while helping to ensure visibility into encrypted sessions.
- Aggregation, filtering and distribution of relevant traffic to RedShift Networks UCTM accelerates processing throughput.
- Coherent forwarding of SIP endpoint (subscriber or user) voice sessions to UCTM, whether native SIP and RTP or inside GTP user plane tunnels, for more effective analytics.

Introduction

UC, cloud and service providers must implement comprehensive and manageable security policies that encompass all cyber threat models, including: access control, antivirus and disaster recovery planning. While these basic security policies, coupled with authentication schemes, password protections and encryption requirements, help strengthen VoIP provider defenses, they are far from comprehensive. Without the added ability to monitor, enhance and enforce security protections on a 24/7 basis, the network remains vulnerable to today's UC/VoIP cyber threats.

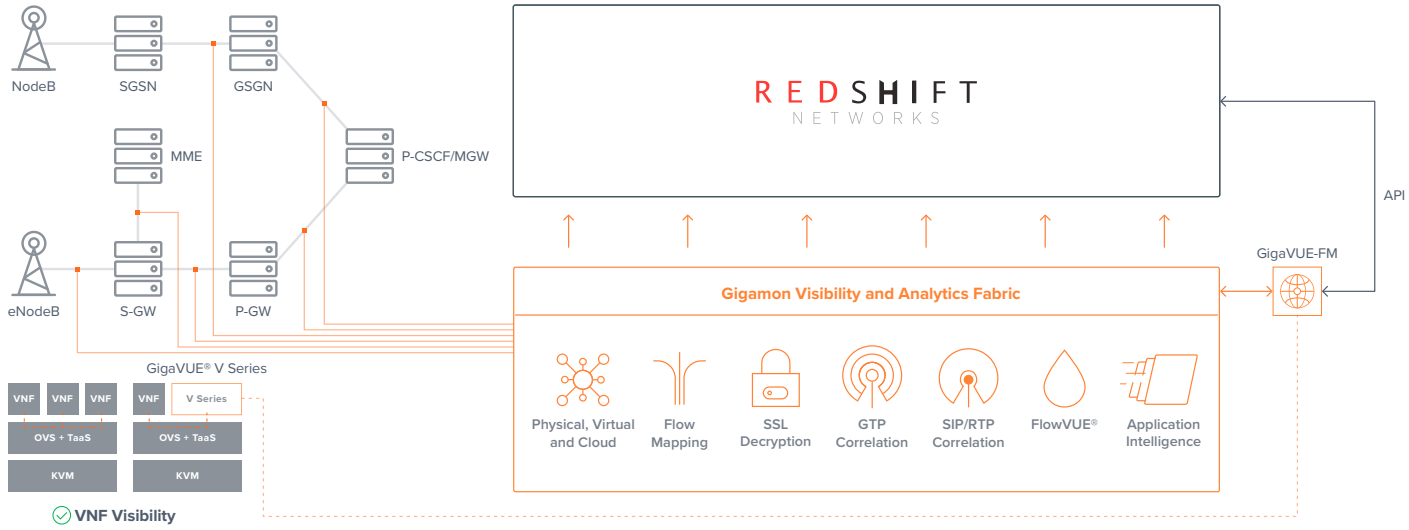
RedShift Networks UCTM Platform is a product portfolio — inclusive of Hawk, Eagle and Condor systems, v-UCTM software and UCTM Cloud — that are specifically designed for service provider, cloud and corporate enterprise environments. With its unique combination of VoIP security, fraud detection and threat intelligence analytics modules, RedShift UCTM helps detect anomalous VoIP activities and thwart cyberattacks, fraud and misconfigurations. Not only can its proactive behavioral learning capabilities assure accurate detection and reduce false alarms, it can also report and halt malicious traffic instantaneously, as well as provide deep visibility and analytics of SIP-based networks for use in determining threats and attacks.

The Gigamon and RedShift Networks Joint Solution

RedShift Networks UCTM offers a comprehensive security solution developed for
SIP-enabled services, such as VoIP, IMS, VoLTE, 5G, and UC/Collaboration applications/networks. Designed for seamless integration into hosted UC/Collaboration, VoIP, cable, fixed, wholesale and Voice over Long-Term Evolution (VoLTE) networks, they act as a central point for monitoring, detection and prevention of malicious VoIP attacks and anomalous traffic flows. With the ability to identify more than 40,000 different types of threats with its patented, service-aware Behavioral Learning Engine (BLE) and Deep Packet Inspection (DPI) functionality, RedShift delivers industry-leading VoIP protection from toll fraud, confidential information compromise, Robocalls and denial-of-service threats in a compact, easy to deploy, carrier-class platform.

RedShift Networks products are based on a high-performance proactive synchronous security design that protects VoIP/UC service delivery, including hosted Internet Protocol Private Branch Exchange (IP-PBX), SIP trunking, Integrated Services Digital Network Primary Rate Interface (ISDN-PRI) replacement and cloud-based UC. As a critical element of an overall security strategy, RedShift UCTM integrates within a network to provide advanced applications layer analytics, signaling layer analytics, stateful inspection and transition monitoring and real-time security policy enforcement.

Integrated with the Gigamon Visibility and Analytics Fabric (VAF), RedShift UCTM provides the necessary protection, visibility and control organizations need to communicate with confidence, knowing that their real-time IP voice, video and collaborative communications are secure and reliable for mission-critical carrier and enterprise use.



Key Gigamon solution features that augment the value of RedShift Networks technology deployments include:

- **Subscriber-aware media:** SIP/RTP correlation intelligently enables RedShift UCTM to resolve real-time communication security by addressing complex, real-time transport issues on the network and complex interoperability issues with the protocols themselves. GTP correlation further enables this for SIP messaging and VoIP traffic monitoring within mobile core networks.
- **Easy access to traffic from physical, virtual and public cloud networks:** The VAF manages and delivers all network traffic to RedShift UCTM, efficiently and in the correct format. To monitor east-west data center traffic and public cloud workloads, Gigamon taps virtual traffic and incorporates it into the Gigamon VAF for delivery to RedShift UCTM on the physical network. This eliminates blind spots and helps ensure that all traffic is monitored and analyzed together.
- **SSL/TLS decryption:** Real-time SSL decryption integration increases traffic visibility for RedShift UCTM.
- **Traffic filtering:** The Gigamon VAF sends specific traffic or sessions to RedShift UCTM so it does not become overloaded with irrelevant traffic – for example, HTTP, HTTPS or email – that would only be dropped at a later point. Filtering can be done based on the outer network layers, or based the application layer using **Application Intelligence**.
- **Aggregation to minimize tool port use:** The Gigamon VAF can aggregate links before sending them to RedShift UCTM to minimize the number of ports required. By tagging the traffic, the VAF helps ensure that the traffic source can be identified.
- **Load balancing to spread traffic across multiple devices:** When traffic flows are larger than a single tool can handle, the VAF can split the flow across multiple tools while helping to ensure sessions are kept together. This also facilitates incremental tool growth rather than rip-and-replace upgrades by allowing new devices to be added to those already connected.
- **Deduplication:** Pervasive visibility requires tapping or copying traffic from multiple points in the network, which in turn, means tools may see the same packet more than once. To avoid unnecessary packet processing overhead on RedShift UCTM, the Gigamon VAF removes duplicates.
- **Payload Slicing:** So the UCTM can more efficiently monitor and analyze the traffic on a continuous basis, the VAF can intelligently remove the payload content from RTP and SIP packets on a per packet or per flow basis, until an anomaly is detected.

For more information on Gigamon and RedShift Networks, visit:
www.gigamon.com and www.redshiftnetworks.com

Gigamon®
Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com