REDSHIFT NETWORKS

UCTM AND THE VoIP THREAT INTELLIGENCE NETWORK

Remote Worker Best Practices

SECURITY FOR REAL-TIME WEB CONFERENCING, VOICE OVER IP SERVICES AND OTHER UNIFIED COMMUNICATIONS APPLICATIONS

The movement to telecommuting has increased by 400 percent in the last decade with more than 4 million workers working remotely in the last 5 years. Remote workers typically make up 5 to 10 percent of the workforce. With the current global health issues, that online workforce has quickly grown beyond 80 percent to nearly 100 percent putting immense pressure on current infrastructure and security needs. One timely example is the 2020 World Health Organization Coronavirus Pandemic. Nearly every non-emergency worker, including business and academia now require their employees and students to digitally work from home to help contain the spread of the virus. Unfortunately, the Pandemic is not the only threat vector since many digital applications and processes like 5G are susceptible to malware, anomalous exploits and costly service theft.

Fortunately, RedShift is bridging the underlying security gap to help customers halt the spread of Unified Communication, 5G or Voice over IP-based threats to both enterprise workforces and their remote workers. CIOs and cybersecurity teams top priority is improving the security posture of the extended enterprise remote worker. Businesses, health care providers and schools require best-in-class cybersecurity for remote workers and students. This security level needs to mirror work processes and applications found inside any office or classroom. In short, users require constantly updated and stronger security mechanism at the dynamic 'remote edge' of the network.

> Real-time communication applications fall prey to malicious exploits and service theft operatives deploying new vulnerabilities and threat vectors.

CREATING A SUITABLE REMOTE WORKER SECURITY MOAT

Existing data-only applications are well managed and secured by today's standard data management and security practices including VPNs. Enterprises typically build strong authentication and encryption solutions for remote applications. After the initial remote authentication and encryption checks, traditional data applications are fortified with identity management systems, policy engines, next generation firewalls, IDS/IPS, SSL encryption, WAFs and other security mechanisms to keep the bad guys out. These data-centric security solutions are mature and in general, meet the basic needs of network managers.

In contrast, 5G, Voice and Unified Communication (UC) applications generally aren't yet fortified as well as data applications. Real-time communication applications like web-conferencing integrate voice, media and UC features. Malicious exploits and service theft operatives are deploying new vulnerabilities and threat vectors. New attack vectors appear weekly including:

- Robocalls – More than $9.5B of losses in 2019 in the US,
- Telecom Fraud – More than $30B of losses in 2019,
- VoIP Analytics – More than $15B loss in troubleshooting and SLA losses,
- Telephony DoS Attacks – Ransomware attacks with $50,000 loss per attack, and
- More than 40,000 additional VoIP Attack exploits – Many advanced persistent threats exist within the fabric of these communications networks.

> Application security needs to expand to include real-time low latency and QoS, deep packet inspection, ability to detect and manage VoIP endpoints and quarantine rouge endpoints, process SIP/TLS, SRTP encrypted traffic.

Communication networks traditionally secured by data application standards including physical or virtual separation from the rest of the network are exposed. They face a multitude of issues related to exposed threat vectors due to the convergence with data, especially with the rise of 4G/LTE and 5G.

Security and network administrators require real-time update services and new solutions to address the reliability and availability of enterprise assets, infrastructure, and endpoints for VoIP and UC services. Encryption is one answer used successfully to protect against Man-in-the-middle attacks (MITM). New real-time communications applications require further and much stronger voice/video-centric threat intelligent analytics to protect against advanced attacks that commonly plague VoIP/UC networks.

MOVING REMOTE REQUIRES NEW APPLICATION SECURITY MINDSET

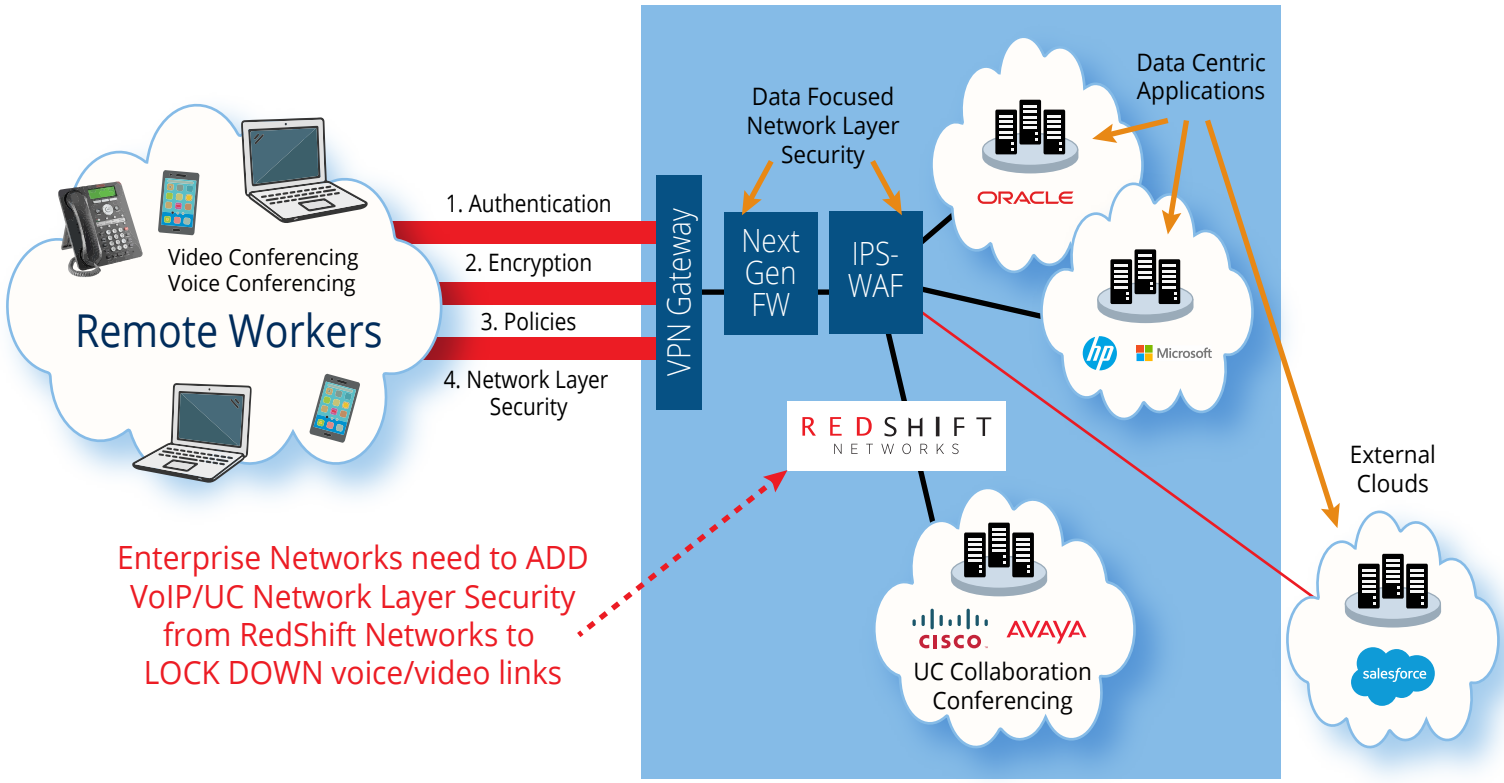
Corporations and their geographically dispersed workforces increasingly rely on modern real-time unified communication and collaboration platforms to improve remote workers productivity. Real-time application examples include Microsoft Workplace, Google Hangouts, Zoom, GoToMeeting, Cisco WebEx and Skype. Many services offer these real-time applications via public cloud UC services from vendors such as AWS/Azure or GCP, offered as on premise (OnPrem) software running in private environments or hosted in a co-location (CoLo) model.

Here's where the security model changes. Real-time VoIP/UC application security mandates a different set of requirements currently not adequately covered by other network devices or encryption.

New security for remote workers includes the ability to block advanced VoIP/UC security treats such as TDoS, voice phishing, robocalls, fuzzing, toll fraud, caller-ID poisoning, protocol fuzzing based attacks, signaling and media threats, data leakages using SIP tunnels, SIP scanners, conversation hijacking or snooping, number harvesting, illegal voicemail retrieval, and rogue applications to name just a few. Application

Remote Workers - Voice and Video Conferencing

Need UC/VoIP Network Layer Security with RedShift Networks UCTM Software



security needs to expand to include real-time low latency and QoS, deep packet inspection, ability to detect and manage VoIP endpoints and quarantine rouge endpoints, process SIP/TLS, SRTP encrypted traffic. RedShift Networks Unified Communication Threat Management (UCTM) software and services deliver a secure environment for managing the real-time network and application risks to secure the extended enterprise remote workforce including:

- Real time VoIP Security, Fraud detection and Analytics software,
- Real time Global SIP Threat Intelligence pushing out Signature and Blacklist updates
- Proactive Financial Risk Management, Cost Control and Security monitoring
- Enable multiple monitors with AI/ML for detection of voice Security attacks and Toll Fraud events
- Proactively Block threats in real-time via Auto Mitigation
- Insight and comprehensive visibility into the entire VoIP network
- Extensive reporting and call recording capabilities
- Ease of system and/or software installation as compared to other network products
- Intuitive and easy-to-navigate GUI interface, and Complement existing network elements (SBC, Soft Switch, Network Probes, CDR based fraud systems).

Work securely from any location with real-time applications using the patented advanced correlation engine technology from RedShift Networks.

We're ready to help your company seamlessly combine SIP Security, Powerful Analytics, and Fraud Detection for visibility into anomalous activities, enabling real-time threat mitigation and troubleshooting.

> Real-time VoIP/UC application security mandates a different set of requirements currently not adequately covered by other network devices or encryption.