Cloud UC
GRANULAR CONTROL OF REAL-TIME APPLICATION LATENCY, APP DELIVERY AND SECURITY

THE PROBLEM

Service providers and Enterprises are both accelerating their migration to popular growing Unified Communications/Collaboration and Security cloud services. Cloud-based voice services including enterprise call centers are among the most used UC (Unified Communications) and UCaaS (Unified Communications as a Service) offerings globally. UCaaS global market size, including enterprise use and communication service provider (CSP) revenue, is expected to grow from USD $15.8 billion in 2019 to USD $24.8 billion by 2024, at a Compound Annual Growth Rate (CAGR) of 9.5%.

CSP Cloud services promise Enterprise buyers both operational and capital savings including:

- No hardware to deploy
- Lower annual license fees for customers
- Reduced IT operational costs
- Easily remotely managed

Health issues and increased enterprise requirements for remote working, including the COVID-19 Pandemic, only further the promised benefits of a seamless deployment in the cloud.

Existing cloud-based security solutions do not address the threat vectors related to real time UC/Collaboration applications. Real time cloud security involves:

- Non-blocking application inspection with analytics correlations
- Preventing robocalls, VoIP threats, DDoS and TDoS with a real-time threat service
- Eliminating more than 40,000 different real time threats from “bad actors” at multiple application layers based on traffic analysis
- Advanced threat protection globally in real-time with a virtual, software or cloud-based solution

THE OPPORTUNITY

The cloud offering is an ideal solution for quickly addressing regulatory demands based on vertical industries for Government, privacy (GDPR) and others. The cloud based security services including enterprise call centers are among the most used UCaaS offering, RedShift built the world’s first new cloud security platform as a service and work stream collaboration ecosystem. Existing data centric focused cloud security solutions don’t address the unique network and application layer security challenges and requirements of cloud and on premise based Unified Communications, Collaboration, and IMS/5G infrastructures. Real time layer security requires application cloud security solutions should be session aware, application aware and user aware.

THE SOLUTION

To address cloud communication security weaknesses within every competitor who focus on solely on multi-tenant SaaS offerings with an inherently weaker shared security model.

The RedShift Networks Cloud UTCM solution’s 24×7 approach for enterprises and CSPs mirrors the needs of all popular UCaaS offerings paralleling well-established data security standards. Real-time apps require:

- UCaaS desktop applications
- Distributed contact centers, communications eMeeting solutions – to address ever evolving global threats
- Email with voice mail and unified messaging – to Secure over 40,000 VoIP/Video threats
- IMS/5G, Voice, Video Conferencing, Contact Center and IMS/5G infrastructures – for detailed network layer real time applications and networks
- VoIP, Video and Contact Center – to provide ‘eyes on the glass’ of entire voice/video network flows
- Remote worker proactive risk management, cost control and security – for rapid response to address real time network issues
- Voice and video security & network management expertise – with voice and video security & network management expertise
- Compliance reporting – to Secure over 40,000 VoIP/Video threats
- Fraud: IRSF, Wangiri Fraud, Call Forwarding, Financial dashboards, Call short stopping – for detailed network layer real time applications and networks
- Access Controls: Registration integrity checks, Authentication at UC Layer, Authorizations, Segmentation, UC eMessaging solutions – to address ever evolving global threats
- Security: – to Secure over 40,000 VoIP/Video threats
- Service providers and Enterprises are both accelerating their migration to popular growing Unified Communications/Collaboration and Security cloud services. Cloud-based voice services including enterprise call centers are among the most used UC (Unified Communications) and UCaaS (Unified Communications as a Service) offerings globally. UCaaS global market size, including enterprise use and communication service provider (CSP) revenue, is expected to grow from USD $15.8 billion in 2019 to USD $24.8 billion by 2024, at a Compound Annual Growth Rate (CAGR) of 9.5%.

THE PROBLEM

THE OPPORTUNITY

THE SOLUTION

BENEFITS
RedShift Networks Cloud UTCM solution can be applied on enterprise end-user applications and networks.

THE OPPORTUNITY

Many existing network providers are quickly adding cloud-based security and analytics capabilities including Zscaler, Cisco, Exabeam, ForcePoint and others. To protect users against the increasing number of sophisticated cyberattacks, there is a growing need for end-to-end holistic security products contributing to the growth of “Real-Time Cloud Communications” security gateway protection within the $5 billion secure web gateway ecosystem. Existing data centric focused cloud security solutions don't address the unique network and application layer security challenges and requirements of cloud and on premise based Unified Communications, Collaboration, Telephony, Video Conferencing, Voice Conferencing, Contact Center and IMS/5G infrastructures. Real time application cloud security solutions should be session aware, application aware and user aware.
THE SOLUTION

To address cloud communication security weaknesses within every popular UCaaS offering, RedShift built the world’s first new cloud security offering for CSPs and leverage within Enterprises using UCaaS solutions.

Both the RedShift Networks Cloud UCTM and on-prem solutions deliver:

• Powerful real-time actionable communication analytics
• Always updated threat intelligence applied automatically against more than 40,000 unique real time threats
• Centralized management system customizable and differentiated from competitors who focus on solely on multi-tenant SaaS offerings with an inherently weaker shared security model
• Remote worker proactive risk management, cost control and security monitoring
• Lower Capex and Opex costs using a virtualized multi-instance architecture with CSPs providing each customer with their own dedicated software and powerful analytics dashboard instance

RedShift Networks Cloud UCTM allows any threat detected anywhere in the cloud to be immediately blocked for all customers.
To see real-time attack origins, go to http://voip-attacks.redshiftnetworks.com.

The globally distributed cloud combined with CONDOR research labs allows for 0-day vulnerability identification, signatures, threat intelligence and blacklists rolled out as part of subscription service. As part of its patent-approved UC-aware and cloud native proxy architecture it performs real-time inspections for all incoming and outgoing traffic with fine-grain policies enforced. The four main functionalities include:

- **Access Controls**: Registration integrity checks, Authentication at UC Layer, Authorizations, Segmentation, UC ACLs, Policy, Endpoint integrity checks, compliance

- **Security**: IDS/IPS, UC Firewall, Threat Intelligence, Anomaly Detection, Zero Day Signatures, TDOS, Robocalls, SPIT, DLP, SQL injections

- **Fraud**: IRSF, Wangiri Fraud, Call Forwarding, Financial dashboards, Call short stopping

- **Analytics**: Troubleshooting, SIP error codes, MOS, Codecs, PCAP files, SIP Call ladder diagrams

The cloud offering is an ideal solution for quickly addressing regulatory demands based on vertical industries for Voice and video compliance on specific standards – Healthcare (HIPAA), Financial Services (GLBA/SOX), Government, privacy (GDPR) and others.
CSPs can leverage RedShift Networks Cloud UCTM infrastructure to offer “VoIP/UC Security and Analytics” Managed Services to their enterprise customers without investing heavily in infrastructure equipment and more rapidly launch new services to address ever evolving customer demands.

**MVSS Delivery Methods**

Multi-Tenant

**Hosted Multi-tenant Virtual UCTM System in NOC/SOC or RSN Cloud**

**Hosted Virtual UCTM System with CMS Multi-tenant in NOC/SOC or RSN Cloud**

**UCTM Cloud for CSP Managed Services Offerings**

**BENEFITS**

RedShift Networks Cloud UCTM solution’s 24x7 approach for enterprises and CSPs mirrors the needs of all popular UCaaS offerings paralleling well-established data security standards. Real-time apps require:

- **Security** – to Secure over 40,000 VoIP/Video threats
- **Analytics** – for detailed network layer real time applications and networks
- **Monitoring** – to provide ‘eyes on the glass’ of entire voice/video network flows
- **Tech support** – with voice and video security & network management expertise
- **15-minute SLA** – for rapid response to address real time network issues
- **Real-time threat updates** – to address ever evolving global threats
- **Compliance reporting** – for financial, healthcare, retail, government and other regulatory requirements

RedShift Networks Cloud UCTM solution can be applied on enterprise end-user applications and networks including:

- **Premise-based and Cloud-based voice and telephony enterprise infrastructure**
- **Unified Communications and Collaboration applications**
- **eMeeting solutions** – audio conferencing, video conferencing and web conferencing
- **eMessaging solutions** – email with voice mail and unified messaging
- **Virtual Desktop Infrastructure (VDI)** – UCaaS desktop applications
- **Communications-enabled applications** – Distributed contact centers, communications platform as a service and work stream collaboration

©2020 RedShift Networks. All rights reserved.