REDSHIFT NETWORKS

Secure Cloud Communication and Collaboration.

Cloud Security Solutions

Cloud Operator Challenges

VoIP Cloud operators and hosted service providers offer business customers a great many new benefits, most notably: improved cost performance, access to enhanced Unified Communication services, ease of management, and investment protection. Unified Communication is a key component of these benefits that grants business of all sizes access to scalable and flexible communications services and applications. However, Cloud service operators hold an increased concentration of client service information and resources within their operations that pose added security risk.

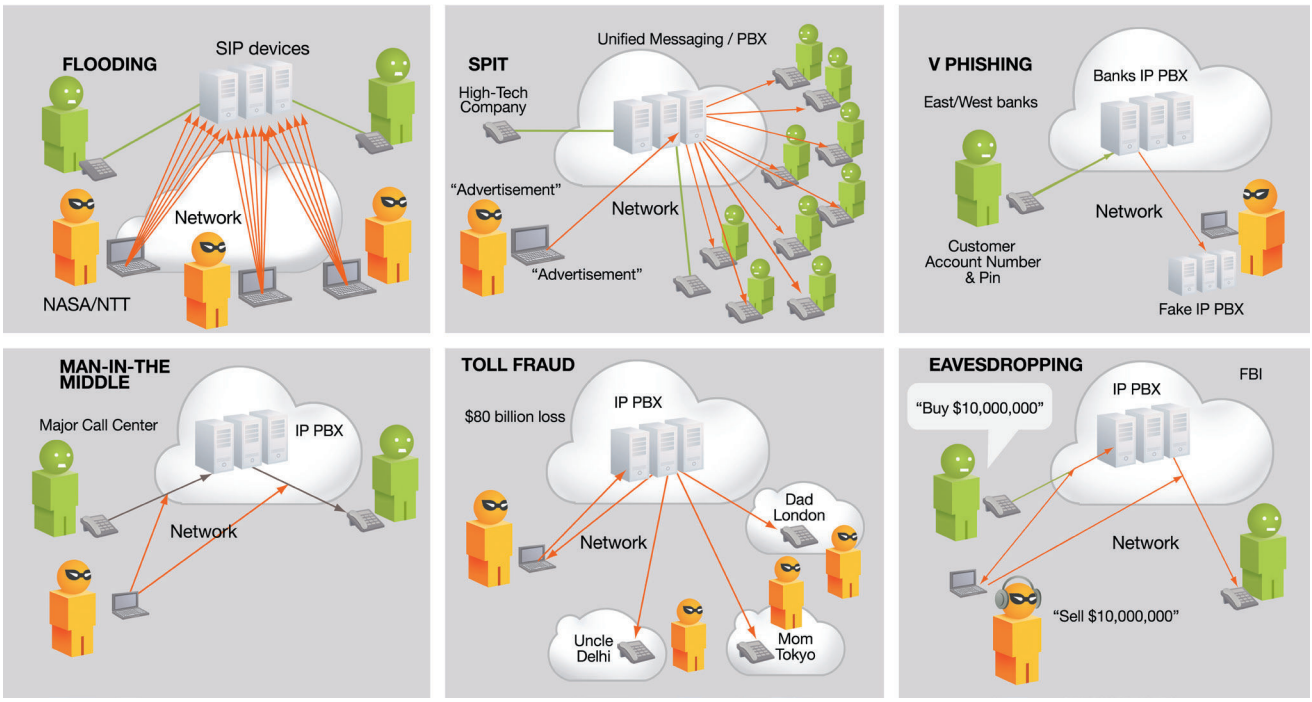

Figure 1: Cloud Security Vulnerabilities

Cloud Operator Requirements

Service and reliability are key components of business grade Unified Communication delivery. Customers expect Cloud operators to deliver comparable availability and security, as was found in premises based PBX, voice mail, and network services. While Cloud operators are able to deliver flexible and scalable service solutions, customers relinquish much of the control of the system to the operator.

Unified Communications is based on a collection of open standards and technologies leveraging IP networking and data infrastructure. Delivering Cloud-based services requires that the provider must consider the security impact of managing valuable and sensitive customer communications in an environment that has proven vulnerable to compromise. Cloud service providers have previously invested in specialized security solutions to protect email, web services, and databases. Hosting Unified Communication services present Cloud operators with a significant new set of risks.

REDSHIFT NETWORKS

Secure Cloud Communication and Collaboration.

- If a communication port or relay is opened, even for a few seconds, the system is exposed to a VoIP Denial of Service - a severe form of attack that prevents subscribers from access to the network and effectively shuts down the service.
- Weak authentication at a customer endpoint can be exploited for toll fraud. Billing and call management systems can be compromised, so shielding the attack from detection for hours or days allow the attacker to steal expensive international calling services.
- Protocol injection in media or signaling streams can be used by savvy network attackers to access confidential information contained in voice mail, customer directories, or other databases used to store subscriber information. This technique is also used by cyber attackers to eavesdrop on calls.

UC Cloud operators must implement comprehensive and manageable security policies that encompass all cyber threat models including: access control, anti-virus, and disaster recovery planning. These policies coupled with authentication schemes, password protections, and encryption requirements will aid in protection, but are far from comprehensive.

Basic security policies strengthen VoIP provider defenses, but without the added ability to monitor, enhance, and enforce security protections on a 24/7 basis, the network will remain highly vulnerable to today's UC cyber threat techniques and the losses to Cloud providers can be cataclysmic.

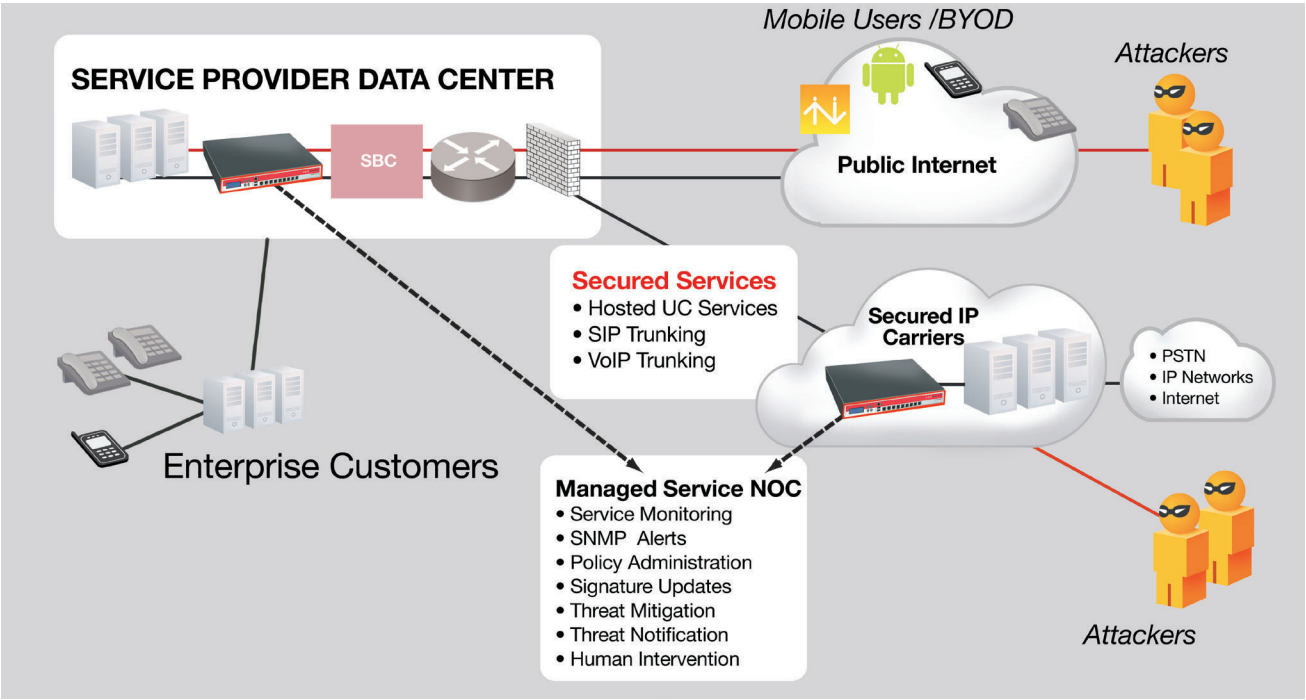

Figure 2: Critical secure points

RedShift Networks Cloud Security Solutions

To address this growing security challenge, RedShift Networks has developed a product line that delivers:

- "Protection" via a patented hybrid of both static threat identification and an adaptive dynamic behavioral learning engine that identifies abnormal traffic in real-time
- "Visibility" by analyzing, reporting on VoIP, UC and CEBP network traffic and sessions
- "Control" via a configurable Policy Enforcement engine that allows IT managers to automatically delay, throttle or block traffic determined to be undesirable

RedShift Networks UCTM does this without sacrificing performance and employee productivity. RedShift Networks Security Appliances provide a point of integration, visibility, control and protection for enterprise Unified Communication applications.

RedShift Networks - "Hawk/Eagle/Falcon" Product Line

- Synchronous Flow Security Technology ™
- Patent protected
- Dynamic real-stream inspection technology
- Proactive proprietary threat assessment architecture
- Advanced behavioral learning analytics (user and app)
- Portable software architecture
- Distributed architecture

RedShift Networks - 4000 Executive Parkway - Suite 290 - San Ramon, CA 94583 - U.S.A.
Voice +1 (925) 272-0100 - +1 866 824 5775 (toll free) - www.redshiftnetworks.com - info@redshiftnetworks.com