REDSHIFT NETWORKS

Secure Cloud Communication and Collaboration.

Telecom Carrier Solutions

Telecom Operator Challenges

The revenue and service opportunities being realized as a result of the transition of telecom operators into IP service providers, whether fixed, mobile, cable (MSO) or wholesale providers, are compelling. The migration from minutes of usage models to application-based services is allowing providers to increase their value, while leveraging the benefits of rapid new service deployment. VoIP services, video collaboration, and mobility are now the primary revenue drivers for carriers. Newer data-centric architectures like IMS and LTE have been designed to enable carriers to deliver flexibility and operational improvements necessary to provide these services. At the same time carriers are now faced with evolutionary challenges. In the past, telecom carriers have been regarded for security and for five-nines reliability. The architecture of the PSTNs (public switched telephone networks), were closed and for the most part proprietary, unlike those of present day IP systems where security for real time services like VoIP is not inherent.

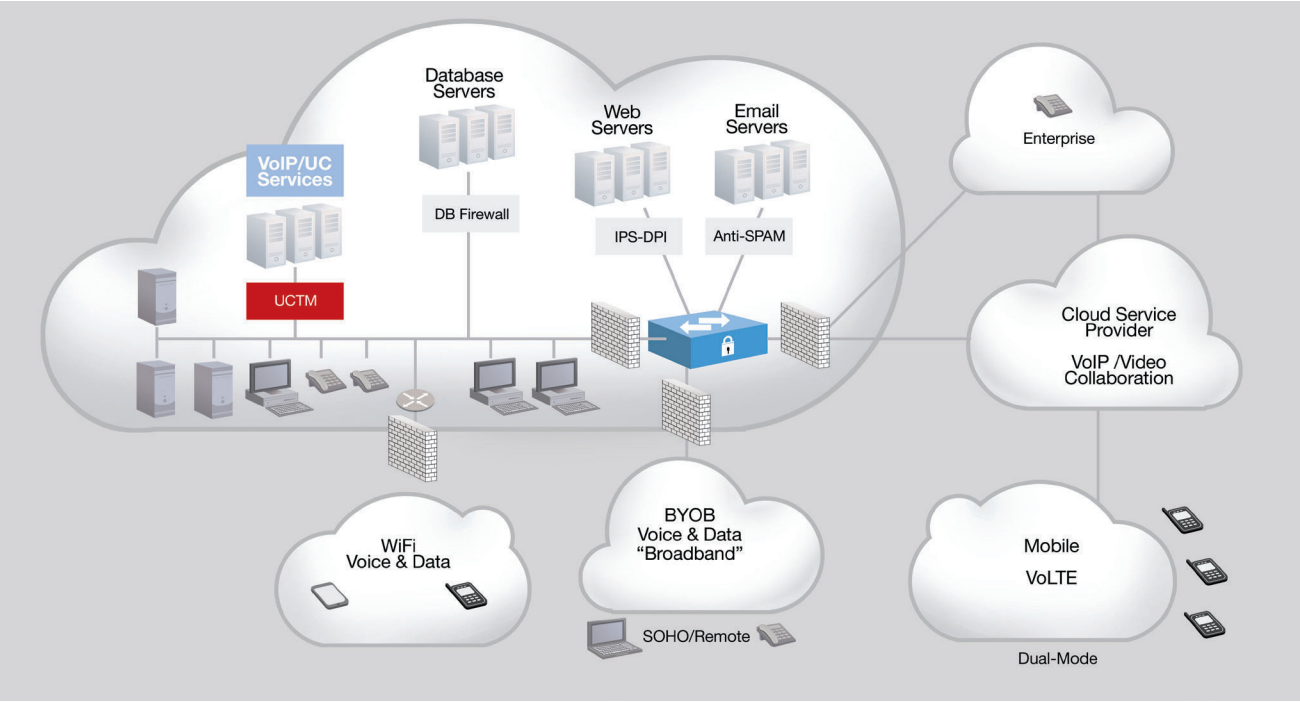

Figure 1: VoIP Service Protection in Carrier Networks

Telecom Operator Requirements

Customers expect their communications services to be secure, relying on service providers to insure the security of the network and its components from end to end.
The specialized requirements of VoIP security are often an afterthought. VoIP system implementation is seemingly ad hoc and based on customer demand / revenue requirements.
At the same time, operators are increasingly faced with an expanding set of vulnerability to attack in terms of number and severity, as Unified Communications concentrated within the service provider networks become high value targets for cyber crime.

Organized cyber criminals and malicious hackers have traditionally targeted data services and applications. However, a growing number of threats have emerged specifically targeting VoIP service components such as user endpoints, Softswitches, IP-PBX, SIP services, network directories, and user databases. The volume and frequency of VoIP & Unified Communication threats and the losses a successful attack can incur require that operators address VoIP & UC security today. To wait for new network service components, when facing potentially large revenue losses and erosion of customer confidence and loyalty would be catastrophic.

REDSHIFT NETWORKS

Secure Cloud Communication and Collaboration.

Toll Fraud and Denial of Service (DoS/DDoS) attacks have proven to present significant threats to all operators. These attack models can only be accurately detected through visibility into endpoint actions, signaling and media protocols, and through applications awareness. By correlating these events, with an in-depth understanding of service behaviors, loss due to compromised software elements and unauthorized access can be quickly averted while also reducing false positives and negatives that occur when security devices have only a limited view of the network and its operation.

A comprehensive detection, management and control solution are a must to address the core components of the telecom carrier network, as well as upstream and downstream behaviors, traffic, signaling, call states, and endpoint security.

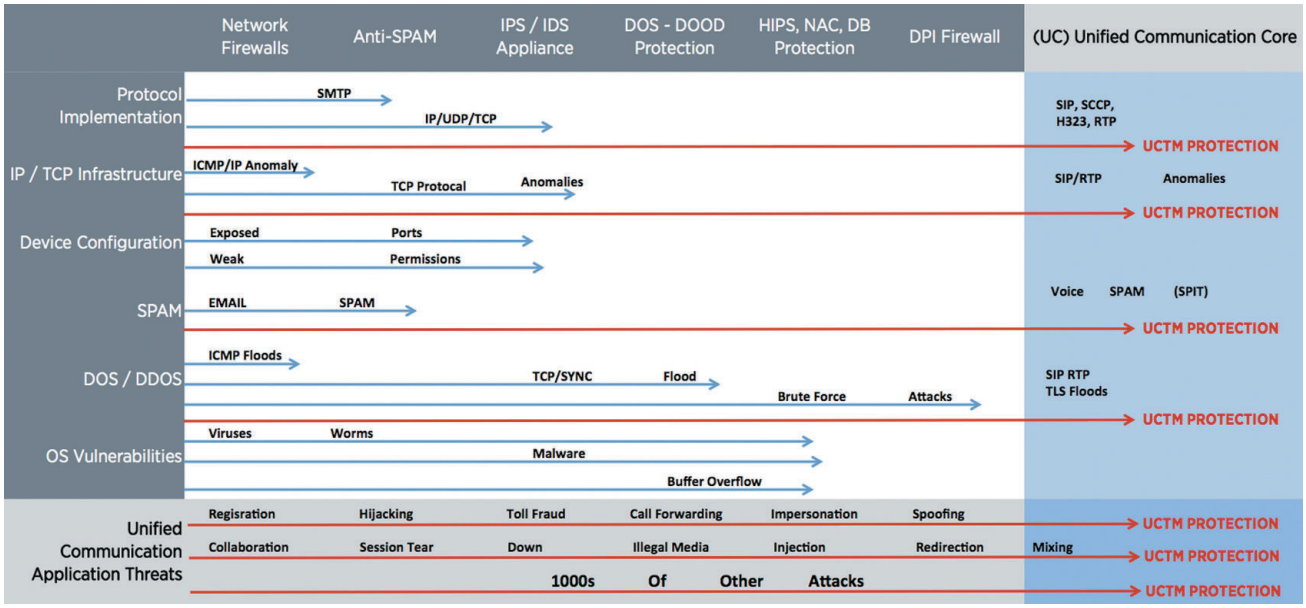

Figure 2: Unified Communications Threat Management - VoIP creates new security requirements.

RedShift Networks Telecom Carrier UCTM Solutions

- Visibility, control and protection of core elements such as Softswitch, applications servers, and directories
- VoIP & UC state monitoring and traffic analytics
- Security across signaling, media, and applications layer - layer 3 to layer 7
- Advanced behavioral learning algorithms
- UC & Collaboration application-aware security
- Attack detection, prevention, remediation and reporting

RedShift Networks core infrastructure UCTM solution monitors and manages the security of network elements and traffic from an appliance-based integrated system.

- As a purpose-built and patented technology solution RedShift Networks UCTM is able to detect and prevent a broad range of threats
- The solution incorporates over 40,000 threat signatures and an adaptive dynamic behavioral learning engine that identifies abnormal traffic in real time
- Proactive analysis and policy implementation enable operators to identify and mitigate threats as quickly as possible while reducing false positives and negatives
- Carriers can take advantage of automatic updates sourced from RedShift Networks global network of threat detection devices as attack models continue to evolve both at the global and regional level
- With a full product line that scales from enterprise to the largest carrier network, operators can deploy a comprehensive, integrated UC security solution, all from a single vendor

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
- High availability functionality for robust global VoIP Cloud Networks (Hawk/Eagle)

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