REDSHIFT
NETWORKS
Secure Cloud Communication and Collaboration.

Unified Communications Threat Management (UCTM)

Secure Communications and Collaborations

Secure Cloud Communication and Collaboration.

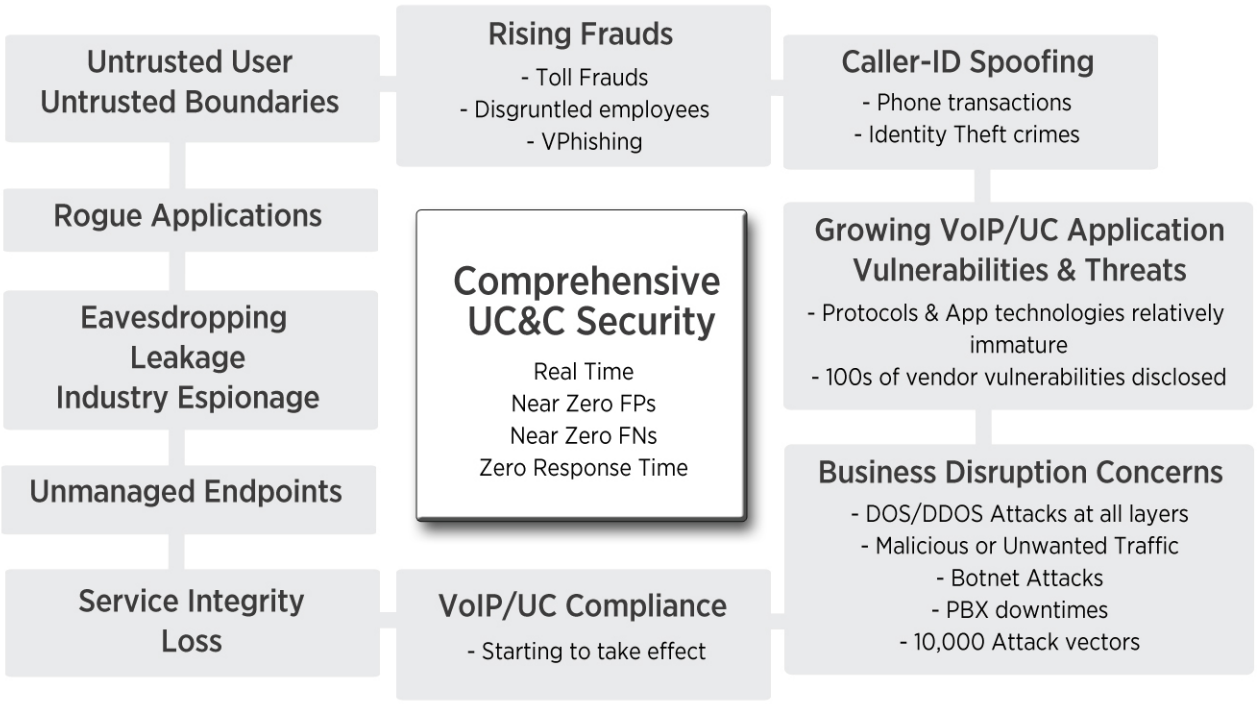
Unified Communications Threat Management (UCTM)

Secure Communications and Collaborations

Overview

The emergence of IP Voice, Video, Unified Communication and Collaborations (UC&C) technology and applications are causing a fundamental shift in the telecommunications industry. Traditional communication systems and applications running on legacy TDM networks are soon being replaced by their IP counterparts providing numerous benefits to businesses. The benefits ranging from low cost of operation, ability to quickly provision rich software enabled communication services, provide ease of manageability, usability and adaptability to business fluctuations while leveraging the benefits of open standards and its ecosystem.

Voice and UC solution vendors are making tremendous progress in tightly tying the operation of data applications (and UC services) with the IP-telephony features. This helps improve the overall employee connectivity and business productivity. The combination of these two previously separate worlds is being called “Unified Communications” (UC) when the integration happens at the end user desktop PC or “Communication-Enabled Business Processes” (CEBP) when the integration is within an enterprise application running on dedicated servers. As a result, rich services are now possible from anywhere, anytime and from any device, UC communication cloud services such as Presence and Collaboration being offered across any IP enabled device.



RedShift Networks

4000 Executive Parkway — Suite 290 — San Ramon, CA 94583 — USA
Phone +1 925 272 0100 +1 866 824 5775 (toll free) www.redshiftnetworks.com info@redshiftnetworks.com

Unified Communications Threat Management (UCTM)

Secure Communications and Collaborations

The stakeholders must understand that while IP Voice, Video, UC&C networks and applications present great promise, they also present unique security requirements that are different from conventional data applications. Due to real-time nature of communications combined with the complex interconnect involving many entities, the overall network complexity and threat vectors exposure is alarming.

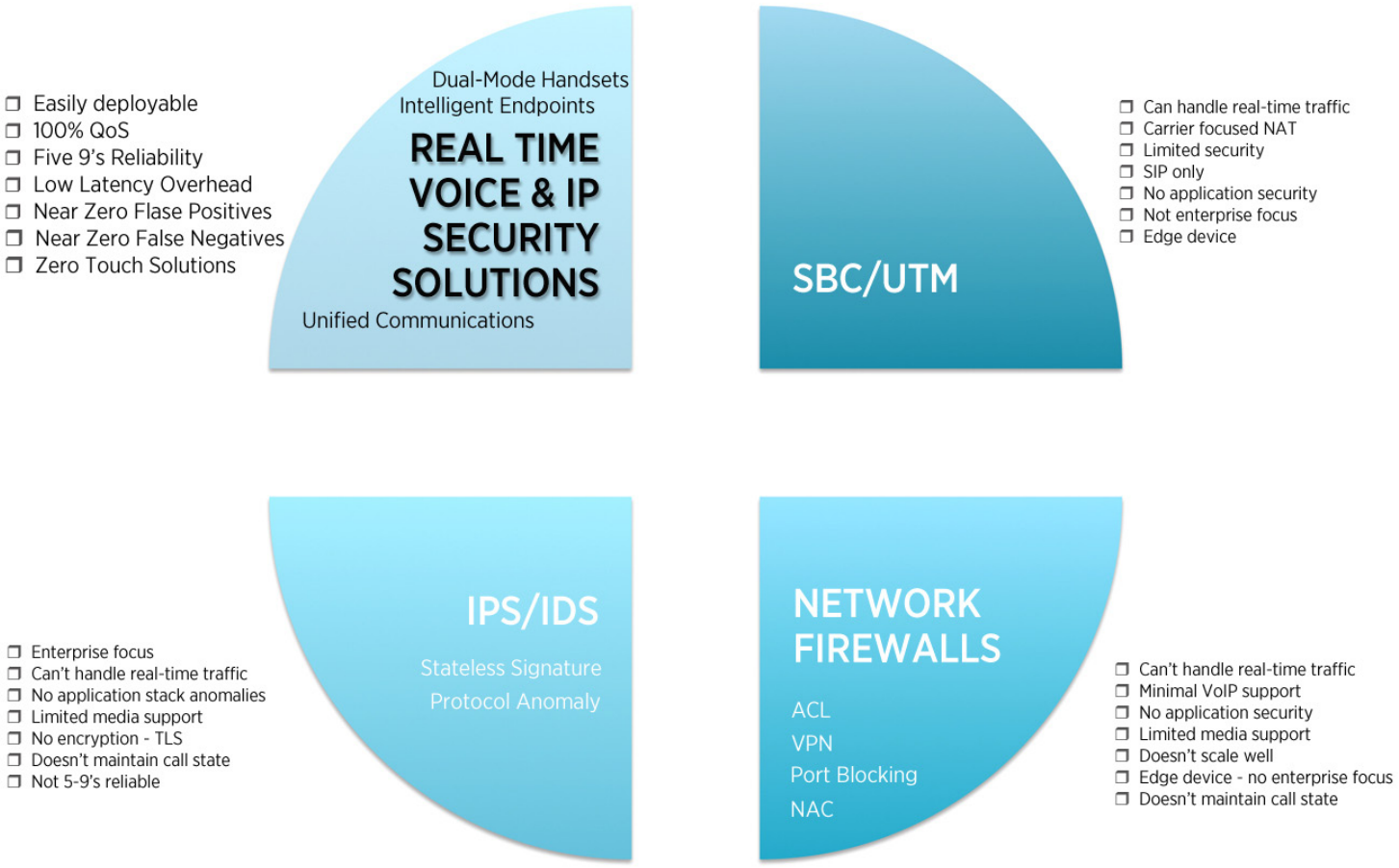
This above figure presents summary of potential risks to evaluate before massively deploying UC&C environments. The risks ranging from real time fraud detection mechanisms, rising vulnerabilities, control of rogue applications and users, meeting compliance requirements, protection against VOIP (and UC) infrastructure and application layer threats such as Voice/UC Denial-of-Service (VDOS/UC-DOS) attacks, SPAM over Internet Telephony (SPIT) attacks, Eavesdropping, Spoofing, Number Harvesting, Protocol anomaly or Fuzzing attacks, Signaling or Media threats, Toll Fraud etc.

Unified Communication Threat Management (UCTM) appliances are new product category. They are a highly specialized solution designed to provide complete protection, visibility and control for voice-, media-, unified communications and collaboration over-IP traffic. The solution offers a blended approach to security, ranging from well-known tools such as stateful inspection, protocol anomaly detection, and intrusion prevention applied to VOIP (and UC) protocols, to sophisticated application (and user-) aware learning and correlation techniques to provide a comprehensive security solution. UCTM appliances combine traditionally separate security services into a single device, providing complete control, visibility and protection to core UC&C infrastructure, servers, users and applications.

Why do you need UCTM?

Data applications are well managed and secured by today's standard data management and security practices. These data-centric security solutions are mature and in general meet the needs of network managers. However with new communication applications beginning to integrate voice, media and UC features, new vulnerabilities and threat vectors are emerging that have not been previously encountered. Communication networks that have traditionally been secured by physical or virtual separation from the rest of the network are now unexpectedly exposed to a multitude of issues related to the convergence with data. Security and network administrators need new tools to address the reliability and availability of enterprise assets, infrastructure, and endpoints of Unified Communication Services.

The paper identifies five distinctive properties for any solution to effectively address the VOIP and UC security requirements and deployment challenges.



Category I: Real-time requirements

- 5-9's reliability translating to only 5 minutes of downtime per year
- Low latency for signaling and media
- Stringent Quality-of-Service (QoS) jitter requirements
  - 100 µs for Media
  - 2 mSec for signaling

Category II: Security requirements

- Low tolerance to false-positives
- Low tolerance to false-negatives
- Call re-attempts are not acceptable
- Process encrypted traffic (SIP/TLS, SRTP)

Categoría III: Technology requirements

- Deep packet inspection capabilities from Layer 3 – Layer 7 VOIP and UC traffic
- Heterogeneous architecture comprising of both pro-active and reactive solution elements
- Need to maintain multiple levels of call state with adaptive behavioral learning of both UC application and VOIP endpoint
- Advance correlation of protocol state and security events across the different layers and security modules

Unified Communications Threat Management (UCTM)

Secure Communications and Collaborations

- » Comprehensively address VOIP, UC and CEBP application security threats
  - SIP/SCCP/H.323 protocol anomaly detection, IPS, Voice DOS and SPIT prevention, eavesdropping, toll fraud, number harvesting, MITM attacks etc.
- » UC-aware policy and incident management system

Category IV: Enterprise focus

- » Deeper interoperability requirements with disparate systems
- » Complex services spanning multiple protocols
- » One security solution – not a slapdash combination of several piecemeal solutions
- » Zero-touch deployment

Category V: UC and CEBP Communications focus

- » Tightly integrated with IP-PBX and other communication infrastructure elements – easy to deploy and manage
- » Easy integration with 3'rd party vendor solutions providing UC and SOA services (e.g. Microsoft, SAP, BEA, IBM)
- » Provide visibility to all VOIP and UC traffic
- » Provide control to all UC services, Applications and Assets

Current security solutions:

1. IDS/IPS vendors – Strong in enterprise focus (Category IV) but are not well suited to meet real-time communications requirements (Category I), possess high degree of false-positives (Category II) and lack technology elements (e.g. advanced call state correlation) required to address the complex blended threats that span multiple VOIP protocols (Category III). Conventional data security solutions also lack UC and CEBP communication focus (Category V).

2. UTM vendors – Solution properties are very similar to IDS/IPS vendors but lack best-of-breed solution and technology elements. Significantly lower price and more suited towards small-&-medium business (SMB) price sensitive segments. UTM devices are mired in performance related issues. They don't address – Category II, III and V.

3. SBC vendors – SBC solutions are very strong in Category I (real-time) and provide adequate security for carrier and edge (or border) protection deployments. They are however not enterprise focused and lack the necessary technology and solution elements required to provide adequate UC and CEBP application security (e.g. Categories III, IV and V).

4. Existing IP PBX players – Primarily focused on providing end-user Voice solutions and equipments. Strong in real-time, enterprise and UC focus (Category I, IV and V). However, providing security solutions is not their primary focus, (Category II and III).

In summary, conventional security solutions such as IDS/IPS appliances, Data firewalls, UTM and/or SBC vendors are not well suited to address the complex VOIP and UC application security requirements and deployment challenges.

The Growing Threats and Vulnerabilities

RedShift researchers have analyzed several thousand threats compiled from various sources, such as the VOIPSA group, CERT, BugTraq and other vulnerability postings from several IP-PBX vendors.

VoIP Fuzzing	Malformed Request (Protocol Fuzzing)	Malformed Protocol Messages	PROTOS Suite	Condenomicon Suite	Spirent ThreatEx	MuSecurity
Eavesdropping	Call Pattern Tracking	Number Harvesting	Conversation Eavesdropping and Analysis	Voicemail Reconstruction	TFTP Configuration File Sniffing	Conversation Reconstruction
VoIP Interception/ Modification	Call Blackholing	Conversation Alteration	Conversation Degrading	Conversation Hijacking	False Caller Identification	DTMF Alteration/ Recording
Service Abuse/ Integrity	Call Conference Abuse	Call Stealing (Toll Fraud)	Identity Theft	Registration Spoofing/Attacks	Misconfiguration of Endpoints	Premium Rate Service Fraud
Flood based Diruption of Service	Registration Flooding	User Call Flooding	Directory Service Flooding	DoS on Signaling	RTP DoS Attacks	Distributed DoS Attacks
Signaling or Media Manipulation	Fake Call Teardown Messages	Call Hijacking	Registration Removal/ Hijacking/ Addition	Wiretapping	SPIT	Key Logging/ DTMF Logging
OS Vulnerabilities	Cisco Call Manager Vulnerabilities	Avaya Communications Manager	Microsoft LCS/ OCS Server	Nortel	Alcatel Lucent	Siemens/NEC
VoIP Scanning & Enumeration Tools	Nessus	SIP-Scan	SIPp	Sivus	iWAR	SIPCrack
Data Threats	SQL Injection	Cross-Site Scripting	Malware	Viruses	Web Vulnerabilities	Buffer Overflows
UC Application Threats	UM - Message Waiting Indication (MWI) Attacks	UM - Manipulation of User Mailbox	UM - VoiceMail Retreval Threats	UM - QoS Degradation	Conference - Illegal Join/ Leave Conference Attacks	Conference - Moderation Functions Attacks

Unified Communications Threat Management (UCTM)

Secure Communications and Collaborations

The common observations are that the VOIP and UC deployments faces a variety of threats from different entry points and attack vectors ranging from exploiting weaknesses in networking layers, malware-infected endpoint, underlying OS vulnerability, protocol implementation vulnerabilities, voice denial-of-service and SPIT attacks, UC application layer attacks and/or device configuration weaknesses.

The above table categories the most important threat vector bucket categories along with specific attack incidents reported, tools publicly available or published articles.

1. IDS/IPS vendors – Provide good reactive protection for Data threats and OS vulnerabilities through signatures support. No pro-active protection. Do not provide any protection for the remaining bucket categories along with blended threats that touch data and voice elements, e.g click-2-call sequence initiated from a browser.

2. UTM vendors – Protection generally weaker than IDS/IPS

3. SBC vendors – Provide limited protection to VOIP scanning and enumeration attacks through basic NAT functionality and limited protection against flood-based disruption of service attacks. Do note provide adequate protection for the remaining attack categories.

4. Existing IP PBX players – Do not provide any security besides basic call policy management and enforcement.

UCTM – Next Generation Security Solution for Secure Communications and Collaborations

To address this growing challenge and the security issues specifically Redshift Networks has developed a product line that delivers:

1. “Protection” via a patent pending hybrid of both static threat identification and an adaptive and dynamic behavioral learning engine that identifies abnormal traffic in real time.

2. “Visibility” by analyzing, reporting on VoIP, UC and CEBP network traffic and sessions.

3. “Control” via a configurable Policy Enforcement engine that allows IT managers to automatically delay, throttle or block traffic determined to be undesirable.

RedShift Networks 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.

Unified Communications Threat Management (UCTM)

Secure Communications and Collaborations

RSN - “Hawk/Eagle/Falcon” Product Line

- ✓ Synchronous Flow Security Technology TM
- ✓ Patent Protected
- ✓ Dynamic real-stream inspection technology
- ✓ Proactive proprietary threat assessment architecture
- ✓ Advanced behavioral learning analytics (user and app)
- ✓ Portable software architecture
- ✓ Distributed architecture
- ✓ Immediate Market: UC Focused Enterprise

About RedShift Networks

RedShift Networks is a leader in securing Cloud based VoIP networks and provides the industry’s first complete security solutions developed for Unified Communications (UC). Since 2006, RedShift Networks has been solving the most difficult UC security challenges for service providers and enterprises with the company’s UCTM product portfolio. Deploying the Redshift Networks application service and network layer technology in the cloud ensures secure, reliable service performance.

RedShift Networks partners and worldwide customers are comprised of Communications Service Providers and enterprises including VoIP Carriers, Mobile Operators, MSOs and Hosted Service Providers.

For more information, visit RedShift Networks at www.redshiftnetworks.com

RedShift Networks

4000 Executive Parkway — Suite 290 — San Ramon, CA 94583 — USA
Phone +1 925 272 0100 +1 866 824 5775 (toll free) www.redshiftnetworks.com info@redshiftnetworks.com