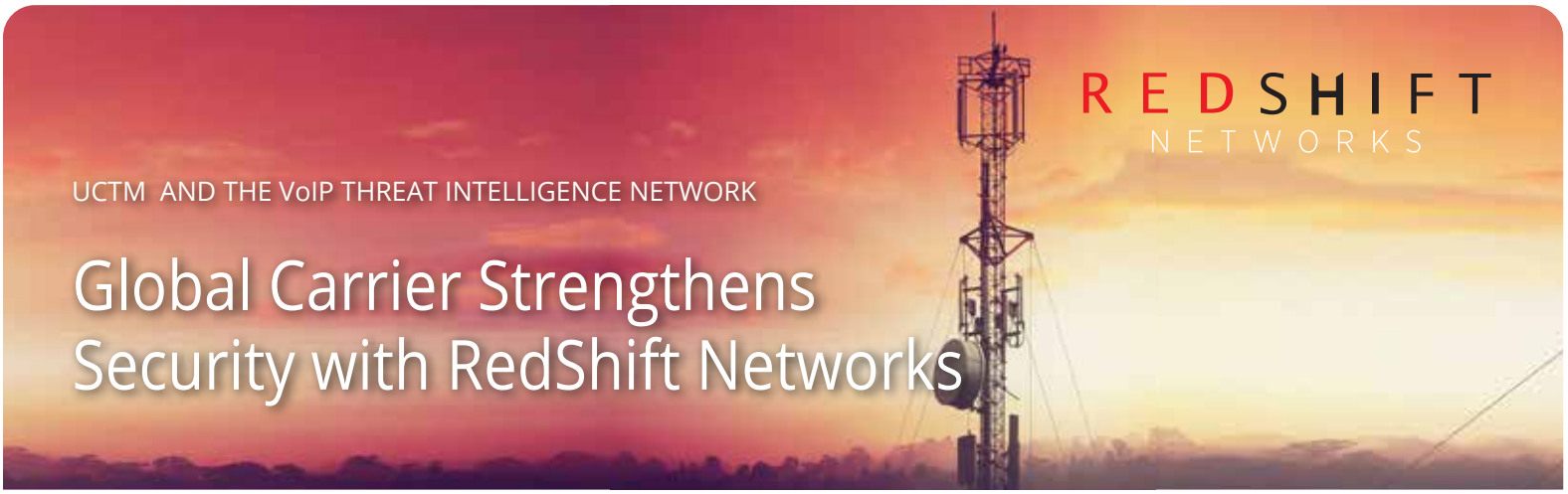


REDSHIFT NETWORKS

UCTM AND THE VoIP THREAT INTELLIGENCE NETWORK

Global Carrier Strengthens Security with RedShift Networks

ABOUT THE CUSTOMER

A global telecommunications carrier, considered one of the top 10 telecommunications companies in the world, is among the largest providers of telephone services – both fixed and mobile – within the United States and has a world wide footprint. The company owns and operates its own network. It offers telecom services to regional businesses and residential customers across the U.S.

THE PROBLEM

This telecommunications carrier was looking for assistance in achieving real-time visibility into voice call processing, unauthorized activities, and to mitigate threats hitting their core network. To that end, the carrier partnered with RedShift Networks to deploy high performance and highly scalable carrier class Unified Communications Threat Management (UCTM) platforms in its regional operations across peering nodes with other carriers, creating carrier-to-carrier interfaces where one telecom service provider passes voice traffic to/from another partner telecom service provider. This can often put a carrier at risk, with attacks potentially traveling from one carrier partner to the other.

This particular carrier was searching for a vendor partner that could provide VoIP/SIP Analytics, along with Security and Fraud Detections/Mitigation to protect against the risks inherent in peering nodes. That was when it discovered RedShift's high level of analytics insight, security protection, and fraud prevention – all major priorities for this carrier in its core Voice/Mobile services.

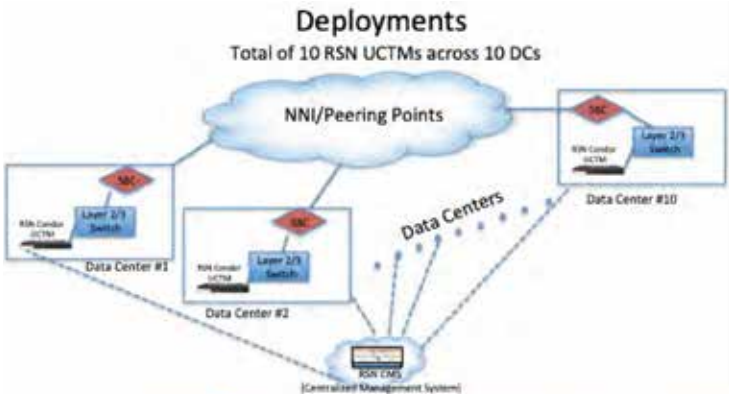
In general, global carriers currently lose $15 billion per year in misconfigurations and in troubleshooting network issues. They also face:

- More than $29 billion in fraudulent theft of telecom/UC services
- $2.5 million spent on every telecom distributed denial-of-service (DDoS) or TDoS attack
- $9.5 billion spent on robocalls

With all of this in mind, carriers cannot risk ignoring these threats – and this global carrier realized that it needed to heighten its security by partnering with RedShift.

In this case, the global telecommunications carrier estimated that they were losing $10M per year on unauthorized activity and threats to their network. The effects of this fraudulent activity resulted in downtime, loss of engineering resources, billing errors, and potential customer churn.

The immediate effect of implementing the RedShift security solution showed a reduction of 87% in the unauthorized activity and threats reported with a continuous ongoing improvement in downtime, engineering resource utilization, accounting, and customer satisfaction.



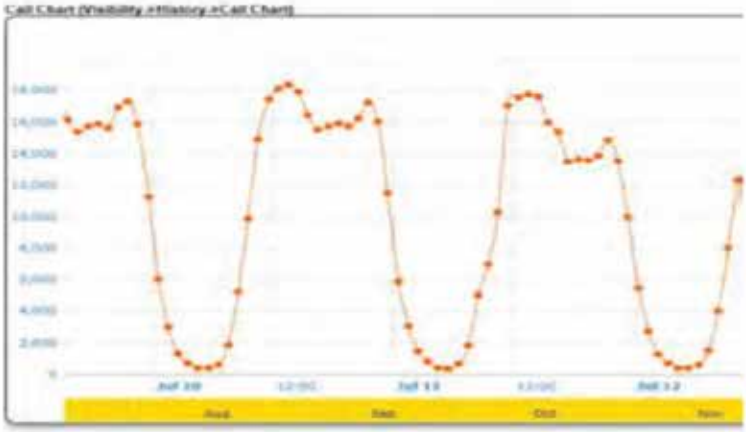
THE SOLUTION

This global carrier utilized RedShift Networks Condor UCTM platforms for deployment next to its Session Border Controllers (SBC) in TAP mode to connect to the Layer 2/3 switch. The Condor UCTM does a port mirror image and deep packet inspection on the peering traffic coming to and from the "outside" of the SBC, digesting all traffic to ensure security and mitigate risk.The carrier utilizes RSN UCTM to meet a variety of needs.

RedShift UCTM features used to solve this problem:

A. Explore Call History
Call History tool has over 50 parameters used to perform filtering for criteria such as Origin/Destination Phone numbers, Client/Server IP addresses, etc., with the ability to export call history in a CSV file and perform additional searches with that data outside of the UCTM. The solution also provides a FLOW/PCAP call file for analyzing networks, collecting and analyzing specific call evidence on call behavior, and provides visibility into the call flow.

B. Call Charts
Track SIP traffic behavior in a daily, weekly, monthly, and yearly time line to recognize trends.



Call Charts track SIP behavior to recognize trends.

C. Error Responses
Tracking specific SIP error and the IP response source was set up and very important to this carrier.

D. SIP Error Codes Charts
Notification of SIP errors causing major problems in the network with quick research - Root Cause Analysis (RCA) and resolution of the error was fundamental to the project.

E. Q850 Cause Codes Chart
In cases where a call is not an end-to-end VoIP call, Q850 cause code chart was used to identify non-IP networks.

F. ASR Groups/Links
ASR groups/links provide real-time monitoring of a segment or group of IP addresses between sent calls to answered/connected calls relevant for the carrier. RedShift UCTM monitors interconnection points (exchange traffic between carriers) in order to ensure the availability of the service, and service levels.

G. Average Call Duration (ACD)
ACD is one of the most complicated metrics to get for any traffic analyzer, and the behavior depends on the day of week, or even the month.

Call Duration is a complicated metric..

H. Reports and Scripts:
RedShift and the customer developed several customized reports and scripts based on specific customer needs.

NEXT PHASE OF DEPLOYMENT

- Enable the RedShift UCTM Security alerts and monitors and monitor
- Enable the RedShift UCTM Fraud alerts and monitors
- Implement mitigation of these threats via connections to Softswitch/IMS infrastructure and SBC

RedShift Networks helped this gobal carrier to achieve real-time visibility into voice call processing, unauthorized activities, and to mitigate threats hitting their core network.