Next Generation SIP Threats

Kevin Isacks – VP Edge Products

What is Changing Around our UC/VOIP Networks?

Zero-Trust

- There are no security borders
- SIP opens new doors; every application must be secured
- The security stack must be re-architected for data & **voice**

Implications to Your Business

- Attacks are becoming increasingly sophisticated
- A single network element cannot handle them alone
- Real-time communications are not fully secured

Why is VoIP and UC Becoming More Insecure?

Shift from PSTN to IP transport

UC now exposed to IP hacking tools

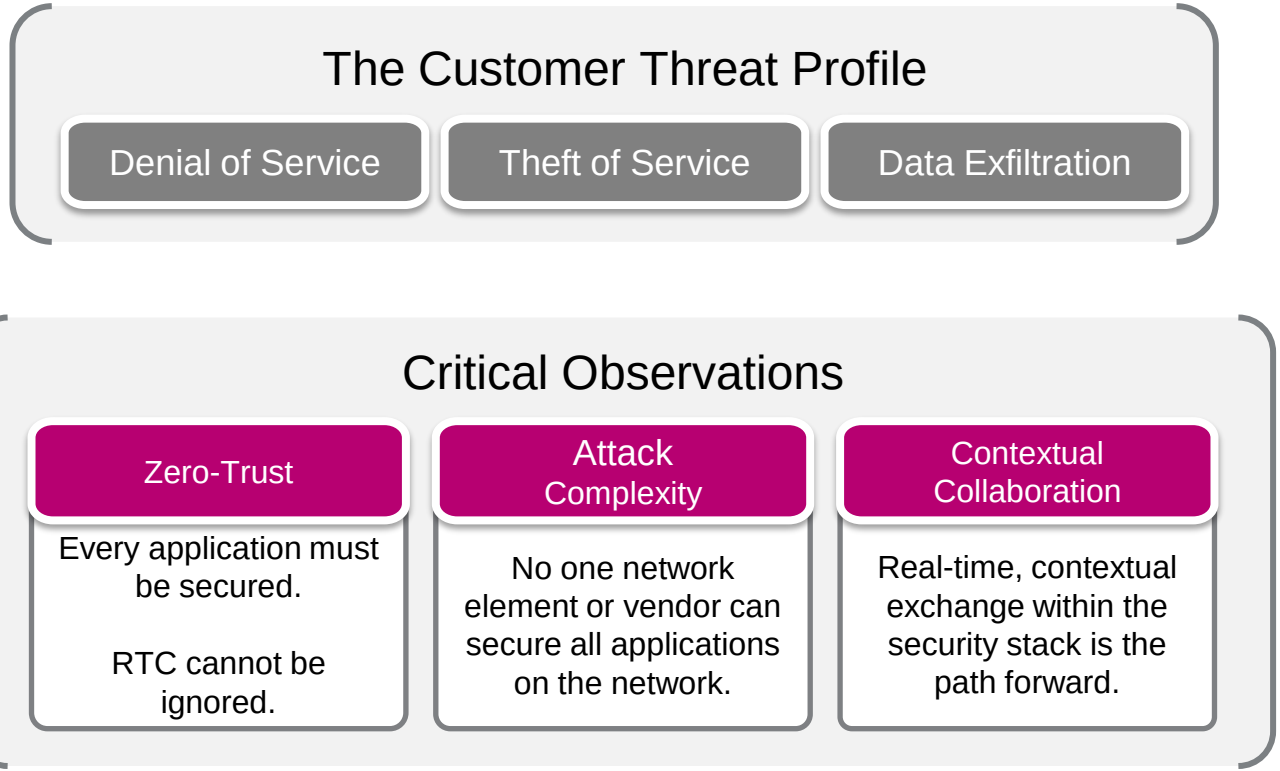
The application moves to the cloud

The surface area for attack increases

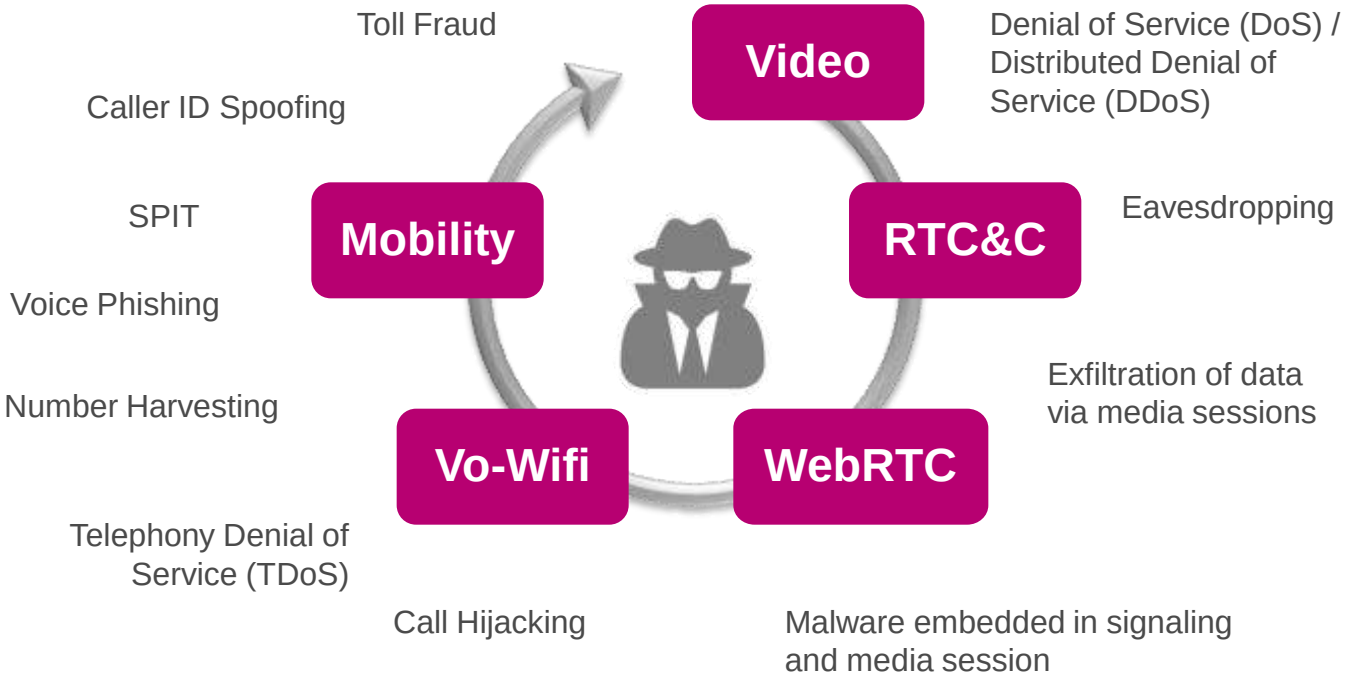
BYOD and Mobility

Endpoint control and access risks

The Drivers for a New Security Architecture



New Security Threats Against SIP Based Communications



Real world SIP attacks

"This novel data exfiltration technique using video marks an escalation in the conflict as ever more sophisticated attackers adopt the same tools that drive productivity and growth in the corporate world to steal its most sensitive assets." DARKReading

In Plain Sight: How Cyber Criminals Exfiltrate Data Via Video

Just like Fortune 500 companies, attackers are investing in sophisticated measures that let them fly beneath the radar of conventional security.

Kaushik Narayan
Co-founder and CTO at Skyhigh Networks

Cyber Threat Intelligence Shows Majority of Cybercrime is NOT Sophisticated

By Adam Meyer on January 20, 2017

"What cyber threat intelligence is showing us is that most threats simply exploit a series of well-documented vulnerabilities and other weak points to move along the path of least resistance – and the most profit." SECURITYWEEK

Hackers take veterinary office's phone system hostage

Business told to transfer $1,400 in bitcoins

WMUR9

http://www.wmur.com/article/hackers-take-veterinary-offices-phone-system-hostage/21992950

ribbon

SIP Attacks are are evolving – following typical data attack

- Find the weakest link
  - Devices are often not patched
  - Weak passwords
  - WebUI to control forward
- Many tools exist to attack a service
  - DDOS, fraud
  - Mr. SIP
  - SIP Vicious

Will a Firewall Keep Your RTC Network Secure?

Real-time Communications
With Traditional Firewall

Real-time Communications
With Comprehensive Security

RTC ports are not policed for bandwidth

- Theft of service implication: can pass more data than negotiated
- DoS implication: can flood downstream endpoints

RTC ports are not closed upon session termination; rely on inactivity

- Theft of service implication: can maintain a session longer than billed
- Service impact: call transfer and one-way audio flows may be broken

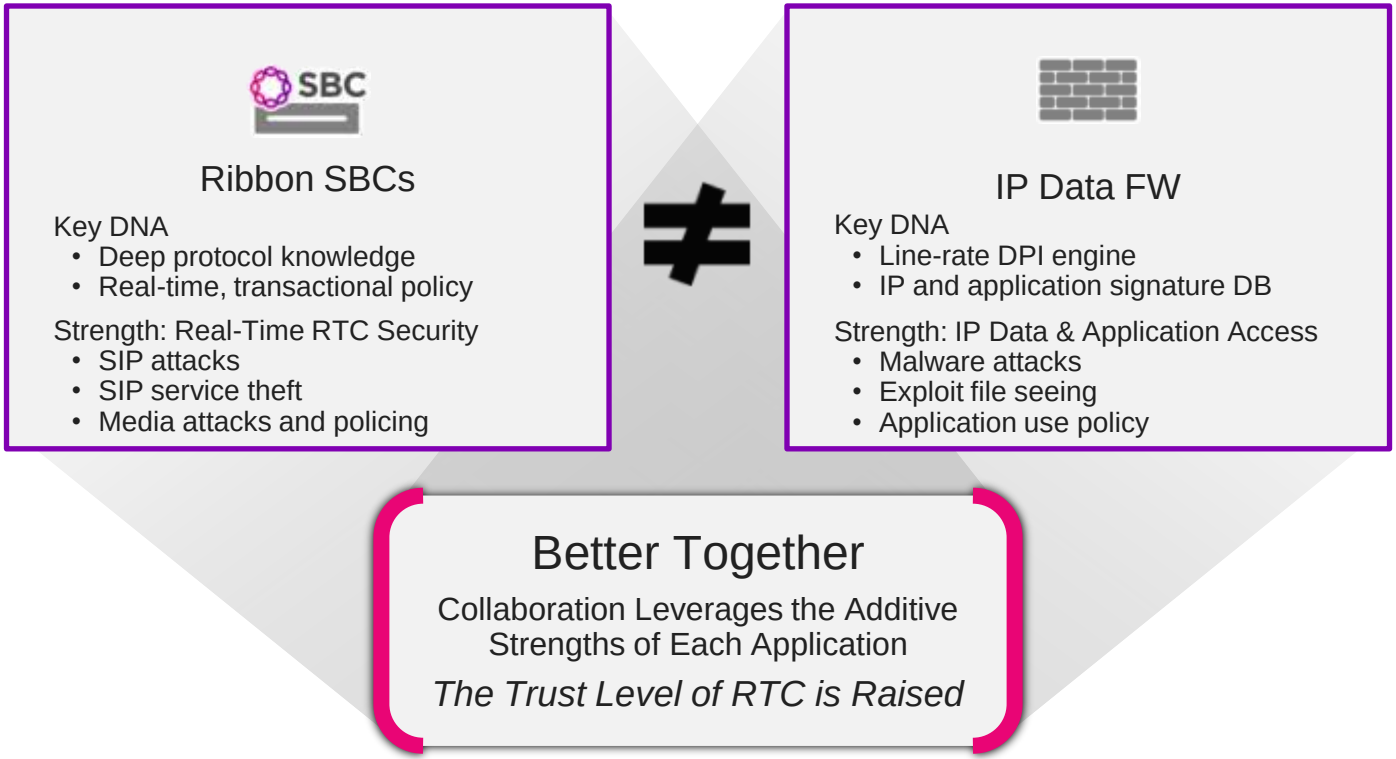
SIP parsing on a limited number of fields

- Perimeter breach: Can spoof a SIP call and trigger ALG to open ports
- Perimeter breach: Will pass unknown headers that can carry attack payloads
- DoS implication: can flood downstream endpoints with protocol errors

RTC flows over non-UDP protocol are not supported

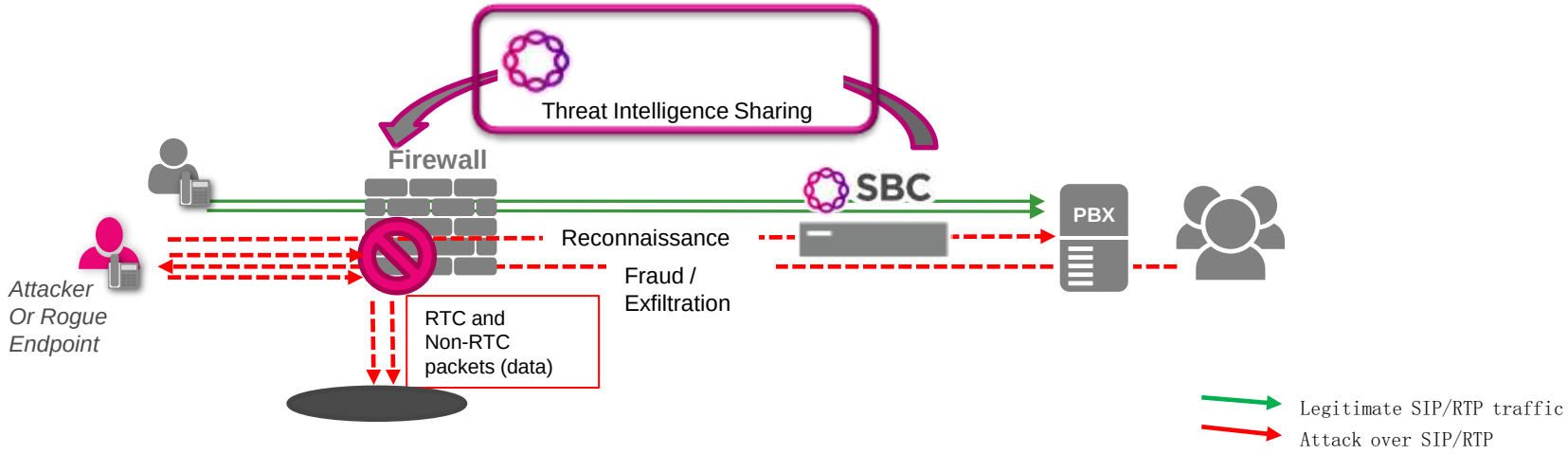
- Service Impact: TCP is used for multiple services (file xfer, conference ctrl, …)

Enabling the NGFW++



Securing Networks Together

SBC + Firewall

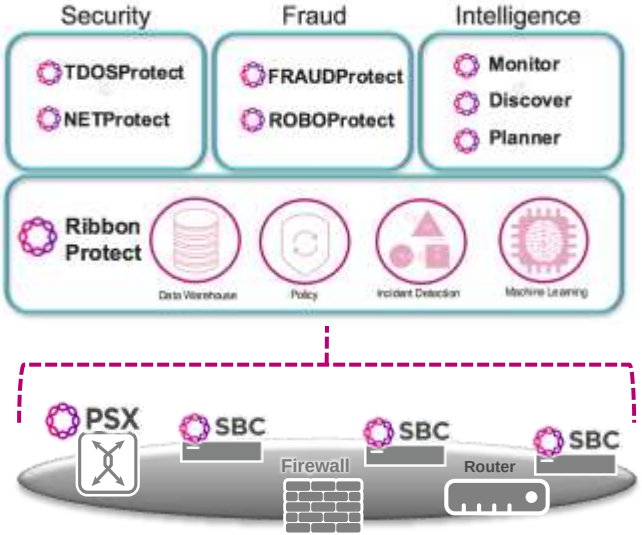


- DDOS prevention - Shared blacklist minimizes resources required
- Raise the security aperture - No wide open UDP port ranges
- Media policed for exfiltration only possible with transcoding
- Minimized firewall / SBC configuration issues by sharing Access Control Lists configuration
- Direct media to RTC endpoint now enforced by the firewall

How to Protect your SIP traffic

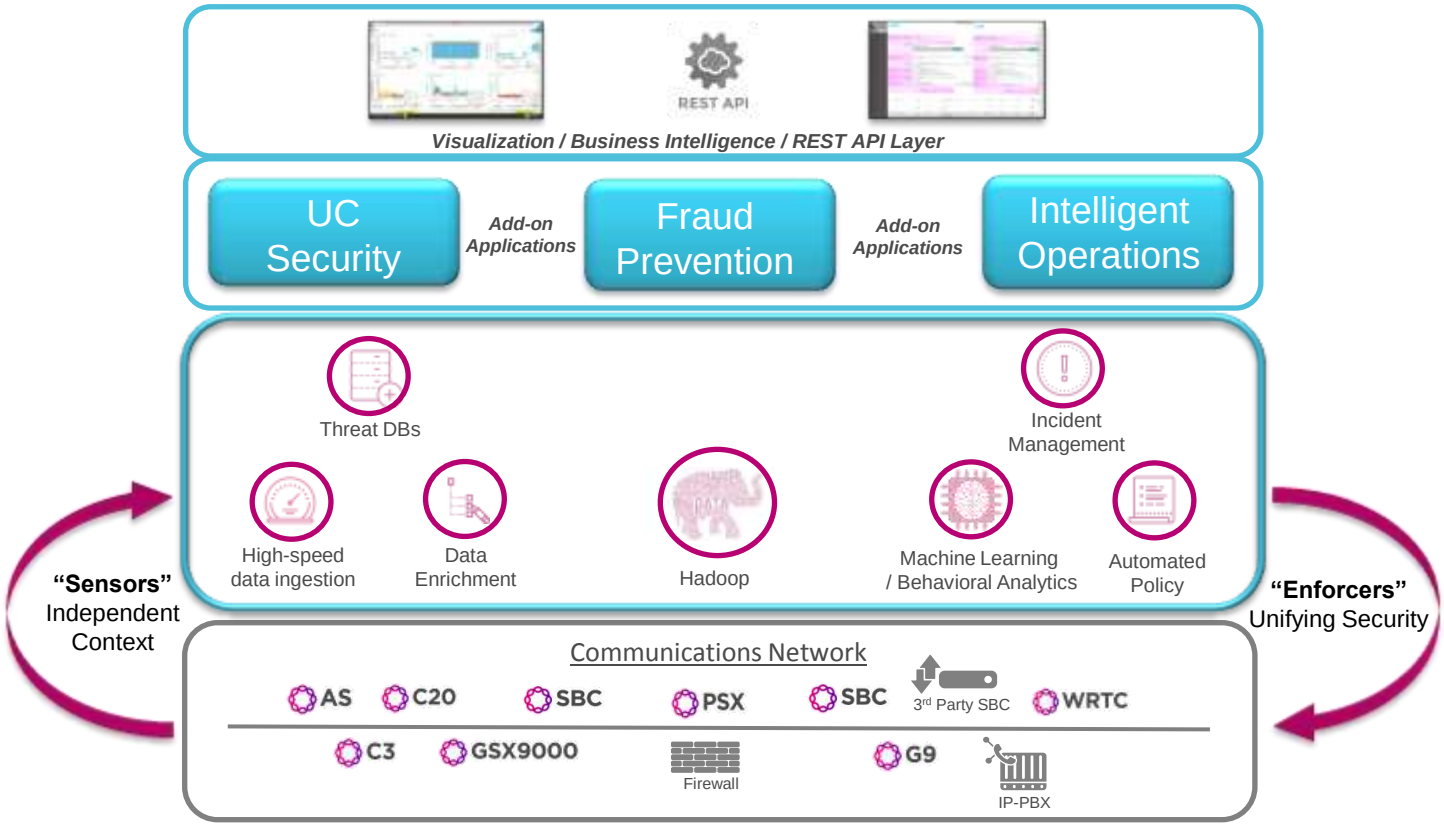
UC Security, Fraud Management and Intelligence

- Eliminates blind spots in your network security posture
  - *Data Aggregation from RTC network "Sensors"*
  - *Pinpoint security threats*
  - *Security policy disseminated across "Enforcers"*
- Fraud Management
  - *Identify suspicious/ abnormal call patterns, unusual call activity*
  - *Distinguish fraud from staff/customer usage*
  - *Network–wide automated alerting and/or blocking*
- Manage & optimize RTC to assure service quality
  - *Intelligent network wide view for operations*
  - *Proactively resolve issues before your end-users are affected*
  - *End-to-end SIP ladder diagrams*
  - *Capacity Planning*
- Wide range of use cases/applications
  - ***Security:** TDoS; toll fraud; robo-calling; threat intelligence sharing*
  - ***Operations:** Monitoring; troubleshooting, reporting, capacity planning*

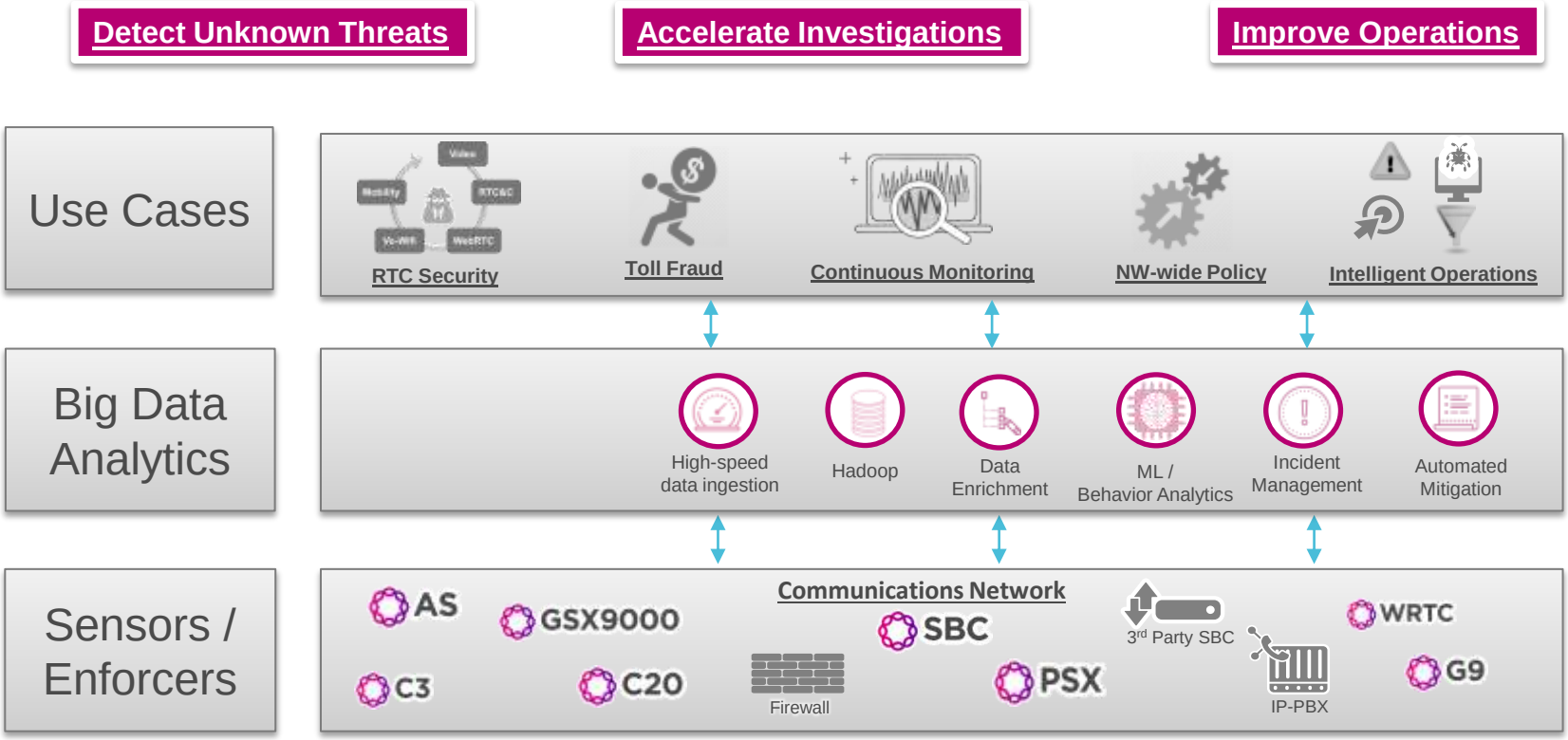


UC Security and Intelligent NW Operations Platform

Architecture

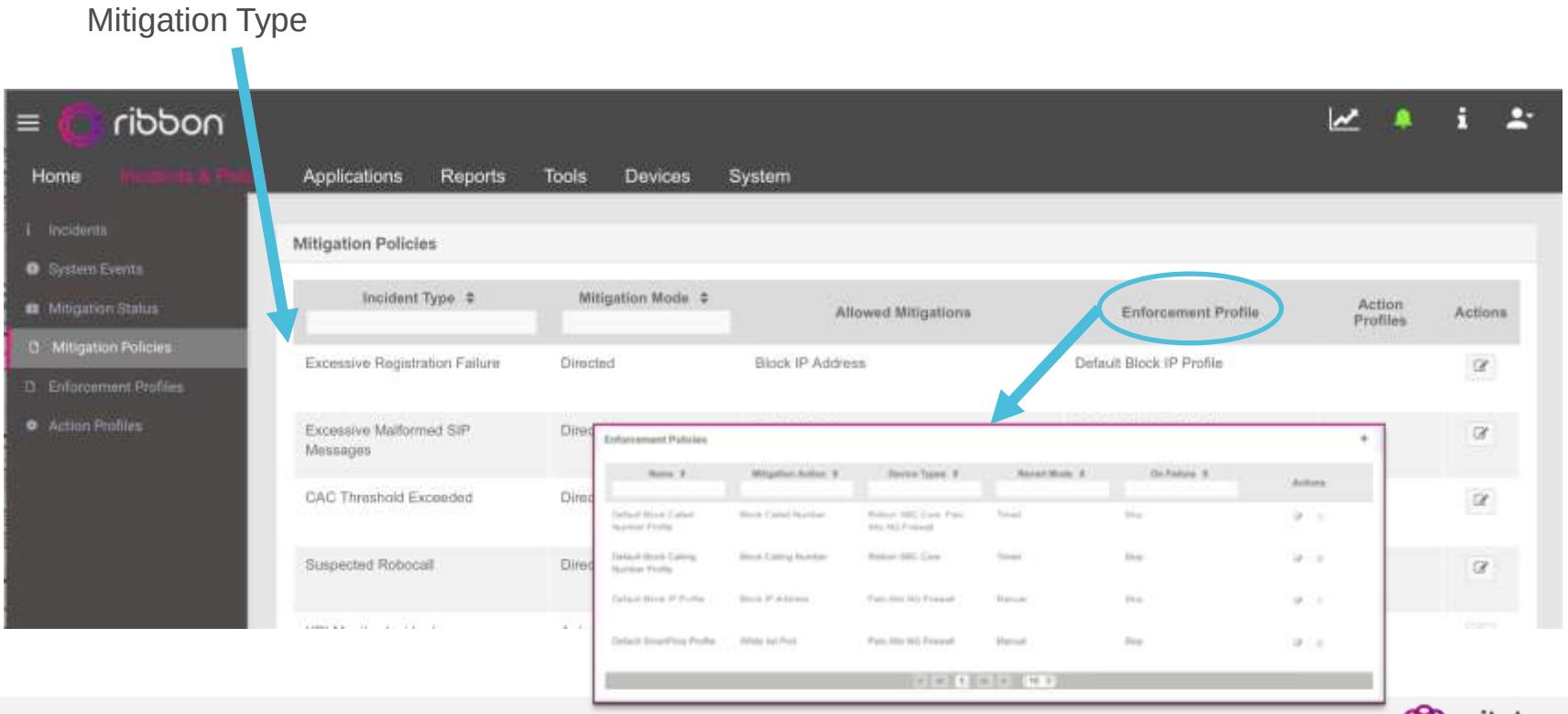


Identifying the Threats



Securing Real-time Communications

Mitigation - Automatically apply policy to blocks rogue calling patterns



Monitoring of Network Performance

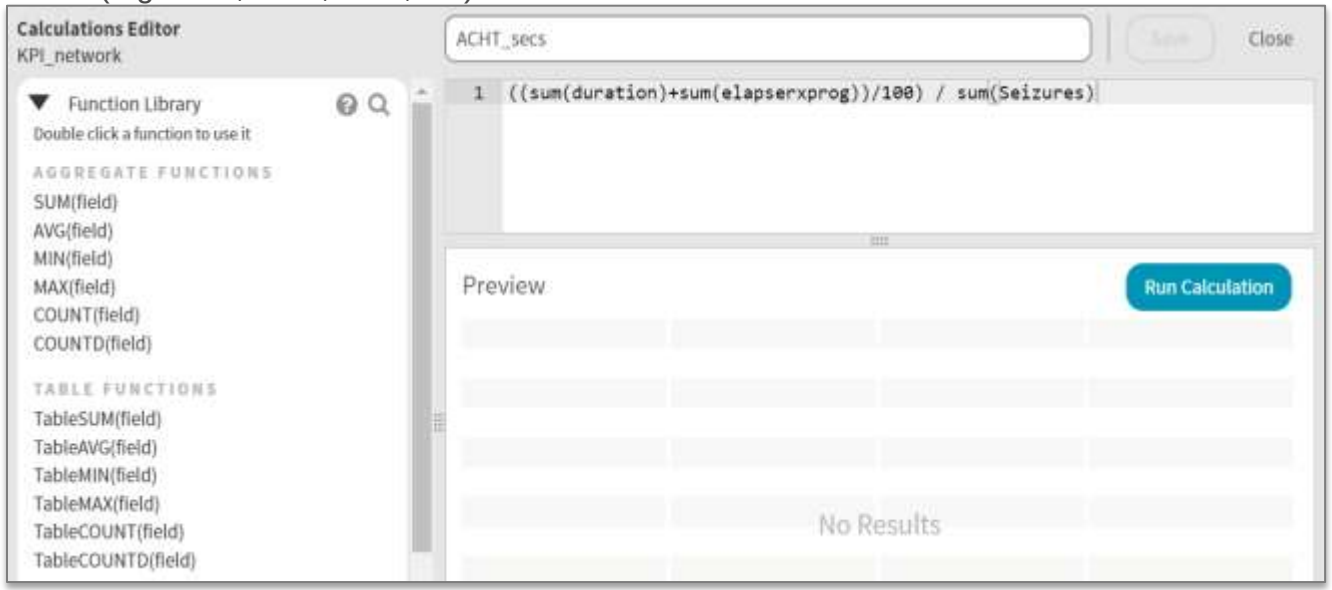
- Correlation of collected data points from performance metrics, CDRs, packets, faults, logs and alarms.
- Trending analysis to provide early visibility into service quality issues and identify abnormal peaks
- Schedule and automated sending of reports by e-mail, text message, SCP or SFTP.
- Export results and reports for sharing with support teams, network partners and other contingents as needed.
- Share the dashboards as static or interactive with others to view or integrate within your web application.

Monitoring of Network Performance

Customizable dashboards

Predefined KPIs

(e.g MOS, NER, ASR, etc)



Securing Real-time Communications

How it is Done

1. ***Behavioral Analytics***
2. ***Incident Reporting***
3. ***Mitigation***

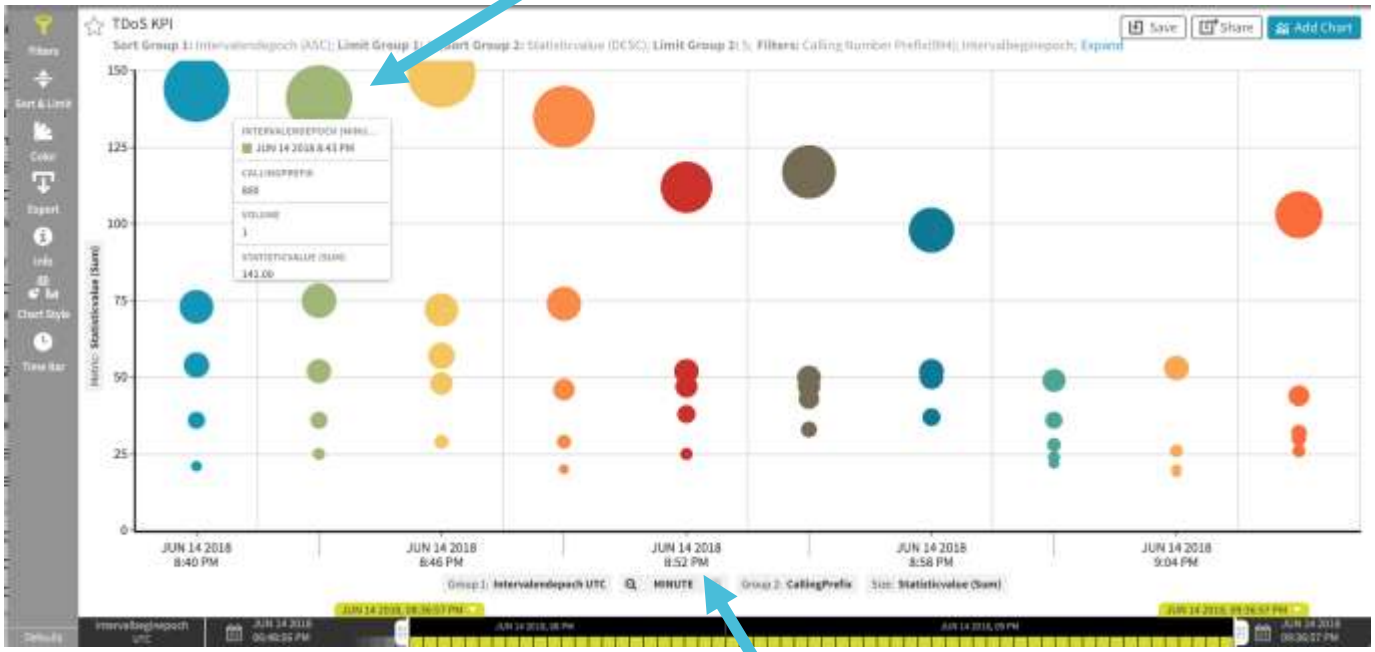
Communication Network Behavioral analytics

Activity profiles determines whether communications network activity is during working or non-working hours.

Online-learning (adapting to changes in user behavior over time)

- when normal behavior changes over time due to things such as business growth or seasonal activity, online learning adapts the model to reflect the current “normal” baseline.

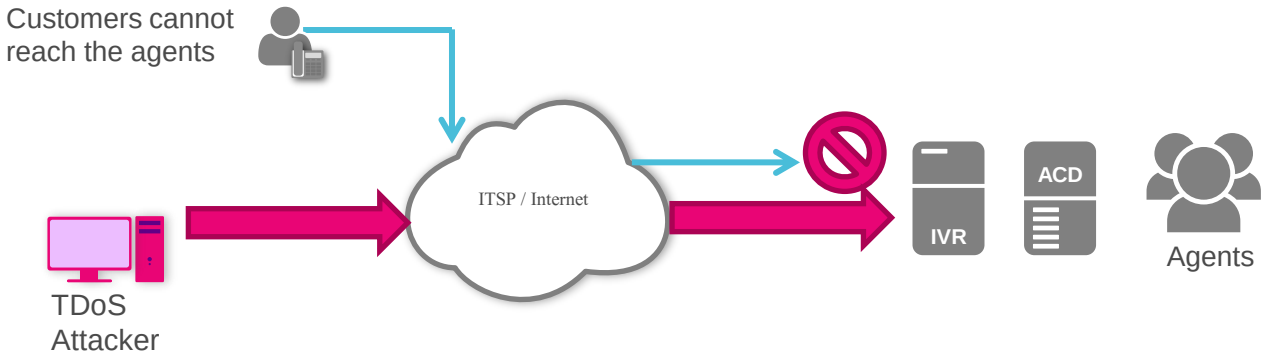
Usage Pattern Recognition



Time Segment Drill Down capabilities

TDoS - Telephony Denial of Service

- Telephony denial of service attacks (TDoS) are increasing in severity and frequency
- Unauthorized users flood the system with bogus access requests and prevent legitimate users from accessing the system
- Keeping these calls active for long duration, the attacker prevents voice network resources from being used by legitimate callers

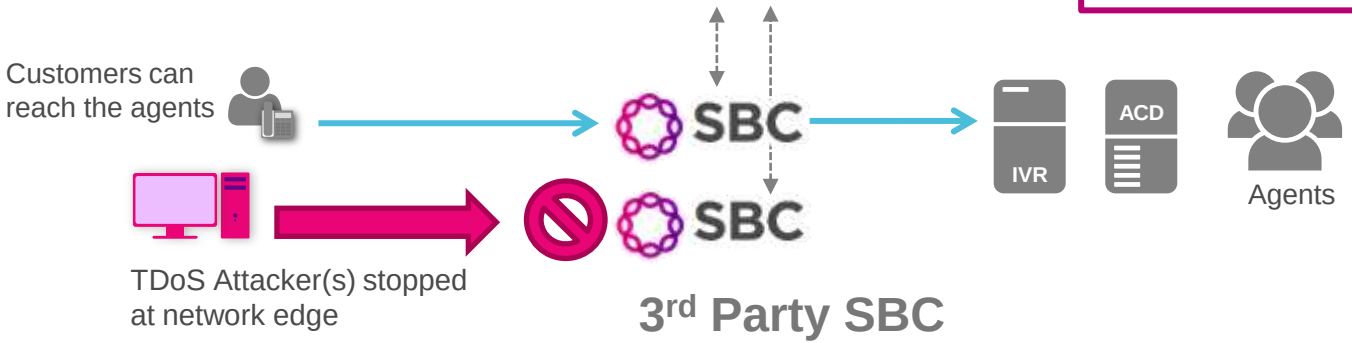


Use Case – TDOS

Severity	Message	Souce	Destination	Actor	Confidence Score	Date	Time	Action
Critical	192.168.12.37 ip address black listed for malformed SIP packets	192.168.12.37	10.10.40.17	192.168.12.37	90	05/09/17	9:47:52 AM	Completed
Critical	172.16.98.4 ip address black listed for excessive bandwidth violations	172.16.98.4	10.10.40.17	172.16.98.4	90	05/10/17	11:12:42 AM	Completed
High	978 614 8510 Possible TDoS excessive SIP registration violation	978 614 8510		978 614 8510	70	05/11/17	3:19:07 AM	Pending
High	192.168.12.37 ip address abnormal high volume activity	192.168.12.37	10.10.40.17	192.168.12.37	70	05/11/17	5:21:16 PM	N/A
Med	978 614 8510 automatic drop known Robo number	978 614 8510		978 614 8510	90	05/11/17	7:41:32 PM	Completed

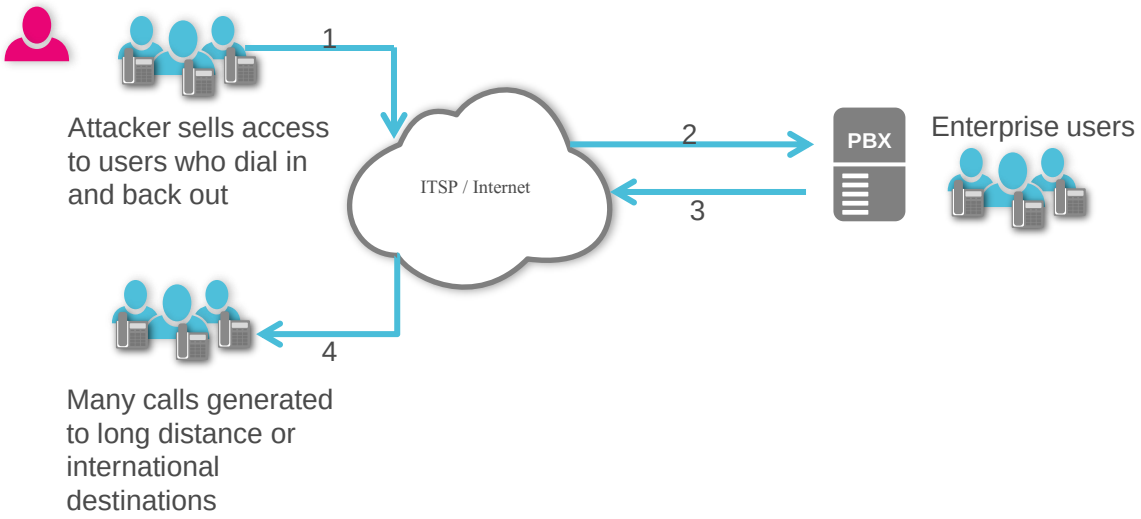
- Advanced algorithms to siphon out unwanted, disruptive calls from your communications networks and applications
- Detect calling anomalies based on metrics such as CAC by Calling number
- Automatically alerts on and blocks rogue calling patterns throughout the entire network

Alerts and Notifications:
NOC/SOC or Ops-Desk



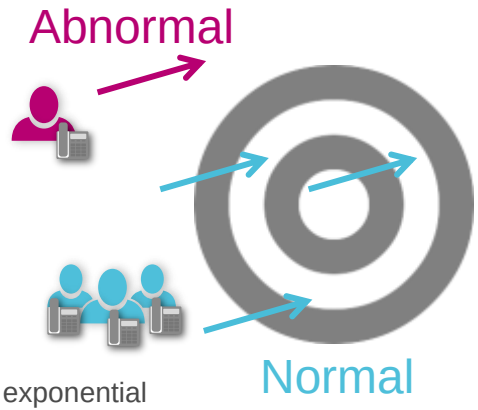
SIP Fraud Management:
Example: Dial-Through Fraud (DTF)

The idea is to exploit an IP PBX and find a way to take an inbound call and hair-pin out to an international number



SIP Fraud Management: Subscriber(s)/Target(s) Monitoring

- Subscriber (Caller #) and Target (Called #) Monitors
- Behavior Analytics model is created and maintained
  - Create a traffic profile for the subscriber/target
- Alert on calls outside the normal traffic profile; blocks activity



Protect tracks a daily exponential moving average (EMA) based upon call attempts, completed calls and minutes of use.

Subscriber (Or Caller #) Monitor

- Tracks individual metrics such as call attempts, call duration, calling number, called number, types of calls (Local, Long Distance, International) during working hours as well as non-working hours.

Targets (or Call-ed #) Monitor

- Tracks the activity of called numbers in the network.
- Called numbers are grouped by a configurable number of prefix digits