40 Ways to Use Splunk in Financial Services

Duncan Ash, AVP Global Financial Services

Haider Al-Seaidy, Financial Services Technical Lead

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only, and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

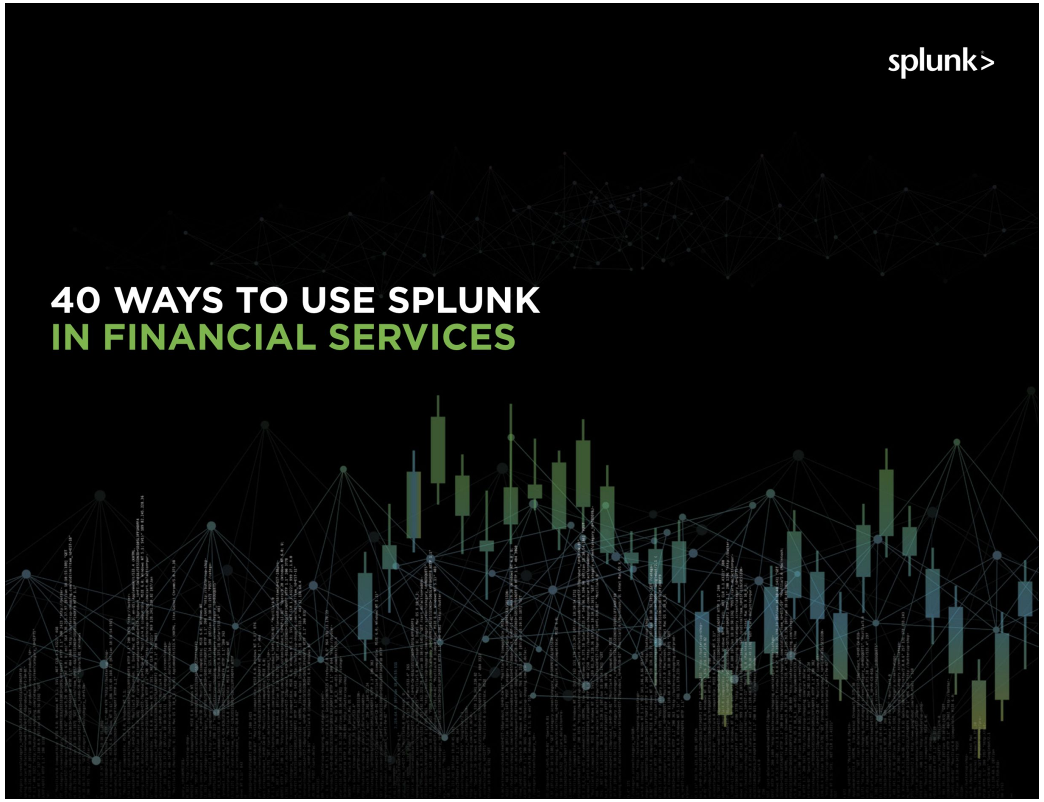
Agenda

40 Solutions – Is that all?

Featured Use Cases:

- **Trading**
- **Branch Banking and ATMs**

Fantastic Assets and Where to Find Them



splunk>

40 WAYS TO USE SPLUNK
IN FINANCIAL SERVICES

Splunk for Financial Services

Splunk is best known in Security and IT Operations

Customers are using us for a multitude of use-cases

Examples from the real-world:

- Banking and Insurance
- Trading and Risk
- IT Operations
- Security and Financial Crime
- Supervision and Compliance

LOW-LATENCY TRADING OPERATIONS

LOW-LATENCY TRADING OPERATIONS

The business challenge:

Participants in low-latency trading are operating at the highest extremes of technical performance. Their requirements push hardware, software, networks and people to their limits. Anything below the fastest performance with the highest reliability will result in missed opportunities, lost trades and potential trading losses. A few nanoseconds can be the difference between a good day and a disaster.

Participants need to develop, monitor and optimize algorithms for low-latency strategies. Often, a firm will have hundreds of different models that can be deployed in an instant, depending on the type of instrument being traded, the venue where it is traded and the market conditions on the day. It is essential to have the best possible algorithm in production at any given point in time.

Participants also must understand and manage the different "circuits" — private networks between their data centers and the different trading venues. Many trading venues allow for a co-location strategy (placing a server at the venue), and those need to be managed and optimized to deliver the lowest possible latency (compared to other co-located servers) and 100 percent availability.

They also need to monitor the performance of each venue: how they perform technically but also how well they fill orders — for example, what proportion of attempted trades are executed. High "fill rates" are essential in order to maintain a client's business; it is common for a client to take its business elsewhere if performance is not up to the expected level.

Participants need to monitor and optimize information from algorithms, PC-based systems, networks, FPGA-based execution systems and APIs, all of which need to perform well together in order to deliver the desired performance.

Splunk's approach:

Many participants in low-latency trading use Splunk within their trading operations. Most use it to monitor their trading infrastructure; measure the performance of the various networks, venues and algorithms; and report anomalies.

Developers are using Splunk's DevOps capabilities extensively, inserting meta-tags into the trading algorithms so that they can measure the effectiveness of an algorithm and correlate the performance against the market conditions, venue and instrument.

Splunk is able to take a time-series view of events and correlate across thousands of concurrent events, highlighting previously unseen insights to traders and algorithm developers. These insights are used to refine the algorithms and drive new strategies.

Algorithm developers frequently have to test new strategies against historical data, and due to the frequency of trades, the associated data can be large. It is common to analyze data sets of 50TB or more, which requires a scalable platform. Fortunately, the horizontal scalability of Splunk facilitates this kind of analysis. In fact, Splunk's largest customers index more than 5 petabytes of data per day.

The value of being able to stop an attack before it becomes an incident is hard to quantify in monetary terms, but it is of clear value to any organization.

In a security environment, it is necessary to have multiple tools and services — there is no single product that does everything. Splunk acts as the nerve center for security operations and is able to bring in data from any system and monitor all of your systems and operations in real time. Splunk Phantom handles the orchestration and automation of security events, making sure that critical issues are responded to promptly.

There are clear benefits associated with being efficient in security operations, being able to react quickly and being able to minimize time spent chasing false positives. Splunk allows firms to manage those operations while maintaining excellent service levels.

Security posture dashboards aggregate and prioritize notable events from across your ecosystem of security tools to help analysts respond with all of the context they need, or automate responses where appropriate.

> "The success of a Security Operations Center starts and ends with knowing what is inside of your network. As hackers become increasingly sophisticated, that level of visibility is often challenging, especially when you are consuming more than 20 different security data sources like we are. Since implementing Splunk Enterprise Security as the brain in our security nerve center, we have found Splunk to be the right solution to quickly and effectively create and implement security analytics across a wide array of data sources and security use cases."

Tim Callahan, Senior Vice President, Chief Global Security Officer at Aflac

Read more about Splunk at Aflac.

FINANCIAL SERVICES SECURITY

Trading

Splunk the end-to-end trading environment

Trading Operations

Every aspect of trading needs to run at 100%, all the time

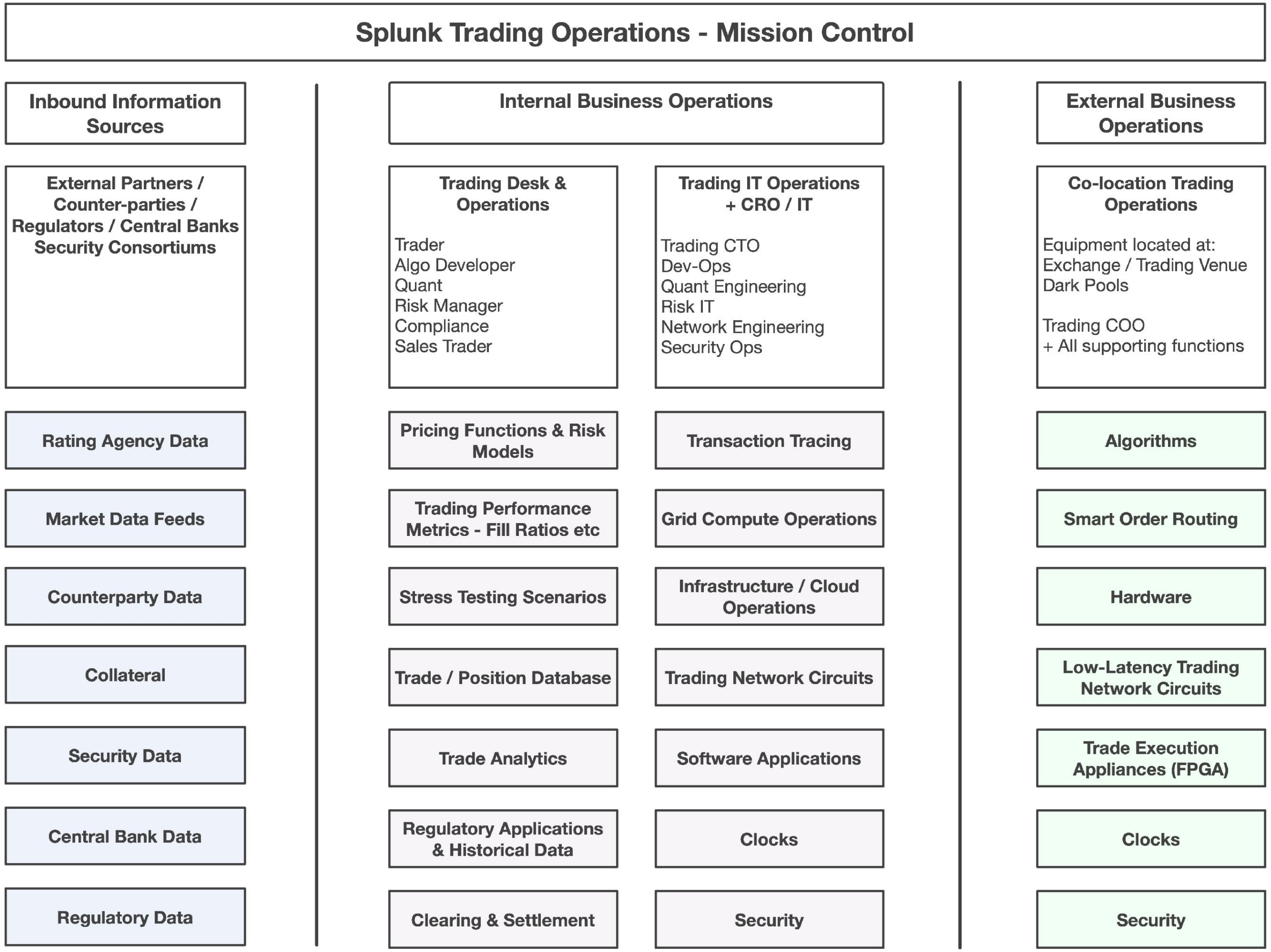
Trading Operations are highly complex and demanding

Thousands of systems and moving parts – internal and external

Timing is everything

If something blinks for 1 millisecond, there are consequences

Multiple Aspects of Trading Need Splunk



Splunk Trading Operations - Mission Control

Inbound Information Sources

External Partners / Counter-parties / Regulators / Central Banks Security Consortiums

- Rating Agency Data
- Market Data Feeds
- Counterparty Data
- Collateral
- Security Data
- Central Bank Data
- Regulatory Data

Internal Business Operations

Trading Desk & Operations

Trader
Algo Developer
Quant
Risk Manager
Compliance
Sales Trader

- Pricing Functions & Risk Models
- Trading Performance Metrics - Fill Ratios etc
- Stress Testing Scenarios
- Trade / Position Database
- Trade Analytics
- Regulatory Applications & Historical Data
- Clearing & Settlement

Trading IT Operations + CRO / IT

Trading CTO
Dev-Ops
Quant Engineering
Risk IT
Network Engineering
Security Ops

- Transaction Tracing
- Grid Compute Operations
- Infrastructure / Cloud Operations
- Trading Network Circuits
- Software Applications
- Clocks
- Security

External Business Operations

Co-location Trading Operations

Equipment located at:
Exchange / Trading Venue
Dark Pools

Trading COO
+ All supporting functions

- Algorithms
- Smart Order Routing
- Hardware
- Low-Latency Trading Network Circuits
- Trade Execution Appliances (FPGA)
- Clocks
- Security

Demo

Branch Banking and ATMs

Cost efficient operations, lower fraud, tighter security

Branch and ATM Operations:

Managing cost, security, and financial crime

Branches have changed for good

Branches are now either an automated experience, or a sales channel for high-value products and services

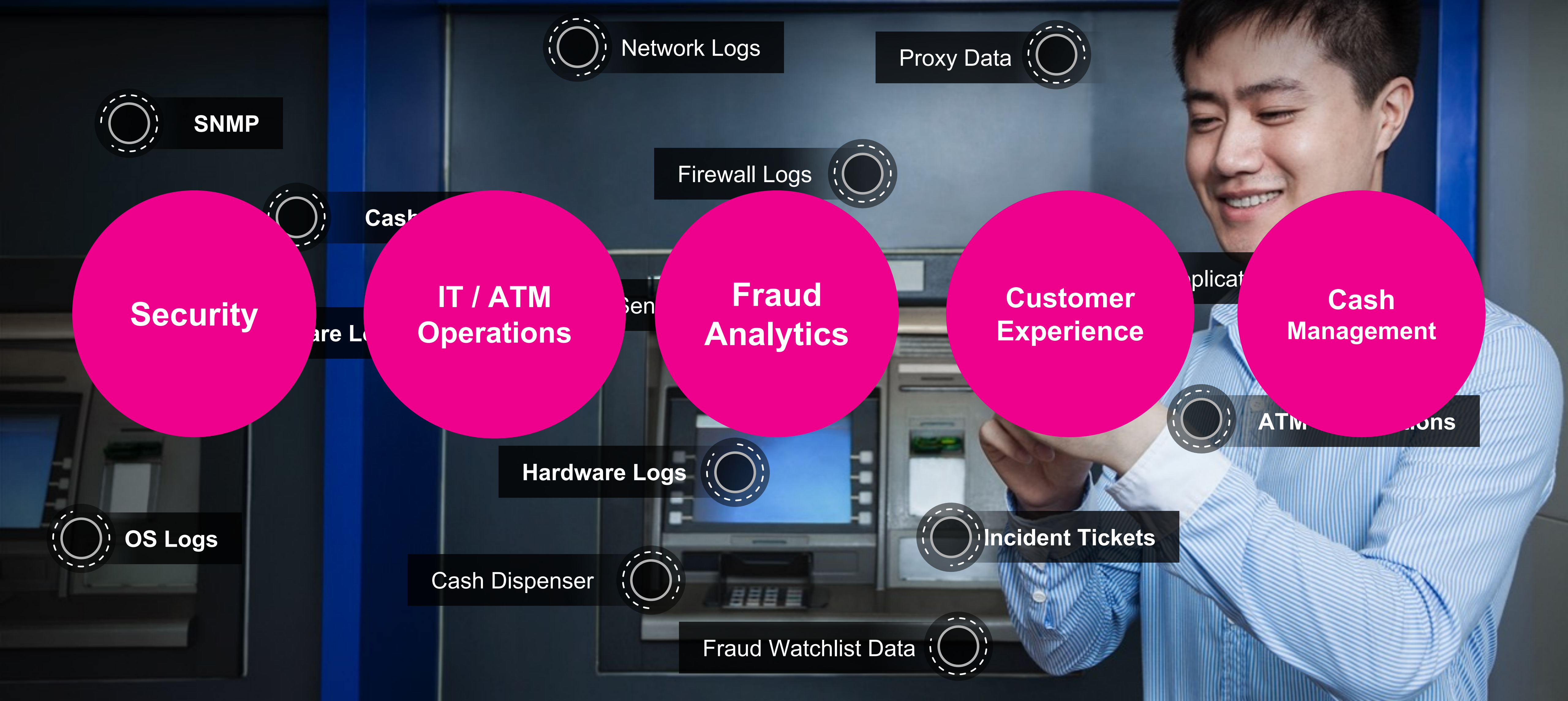
ATM and IDM hardware needs to perform flawlessly

If only it was easy to run the ATM network…

The Evolution of Bank Branches

ATM – Same Data, Multiple Times the Value

Delivering a secure and reliable network brings together a diversity of real-time data sources



Network Logs

Proxy Data

SNMP

Firewall Logs

Cash

Security

IT / ATM Operations

are L

Sen

Fraud Analytics

Customer Experience

plicat

Cash Management

ATM

ons

Hardware Logs

OS Logs

Incident Tickets

Cash Dispenser

Fraud Watchlist Data

ATM Applications

Web Services

Sensors

Social Media

Energy Meters

Tracing

UX / UI

APM

Networks

Databases

Servers

Storage

Security

Transactions

Firewall

GPS Location

Fraud

Online Services

SNMP

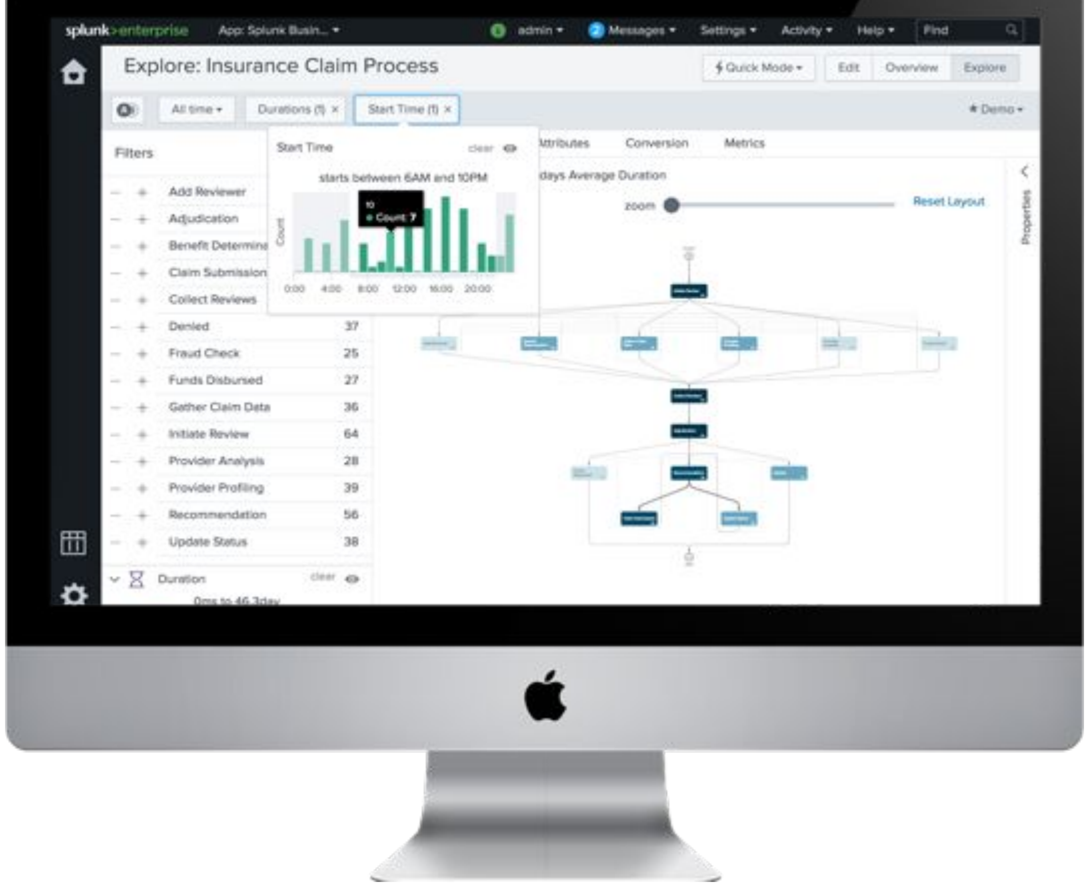
Clickstreams

Mobile Tops Up

Containers

splunk>

TURN DATA INTO DOING



Explore: Insurance Claim Process

Filters

Add Reviewer	
Adjudication	
Benefit Determina	
Claim Submission	
Collect Reviews	
Denied	37
Fraud Check	25
Funds Disbursed	27
Gather Claim Data	36
Initiate Review	64
Provider Analysis	28
Provider Profiling	39
Recommendation	56
Update Status	38

Duration clear

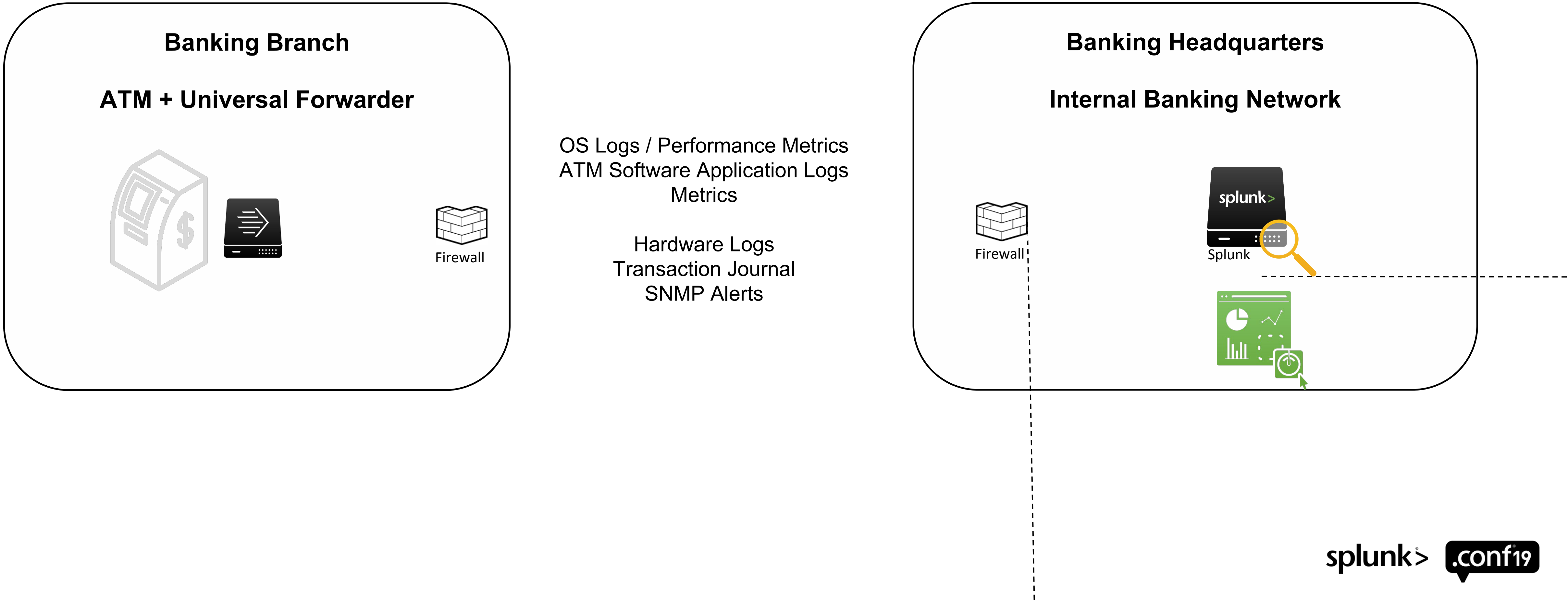
0ms to 46.3day

- Centralized Granular Data
- Real Time Analytics
- Reduce ATM maintenance costs
- Optimize ATM availability
- Continuous Threat Remediation
- Reactive to Proactive Maintenance
- Better Cash Management
- Fraud Reduction
- Improved Customer Experience

splunk> .conf19

The Universal Forwarder

Stream Data | Guaranteed Delivery | Load Balancing | Bandwidth Throttling | Buffering



Banking Branch

ATM + Universal Forwarder

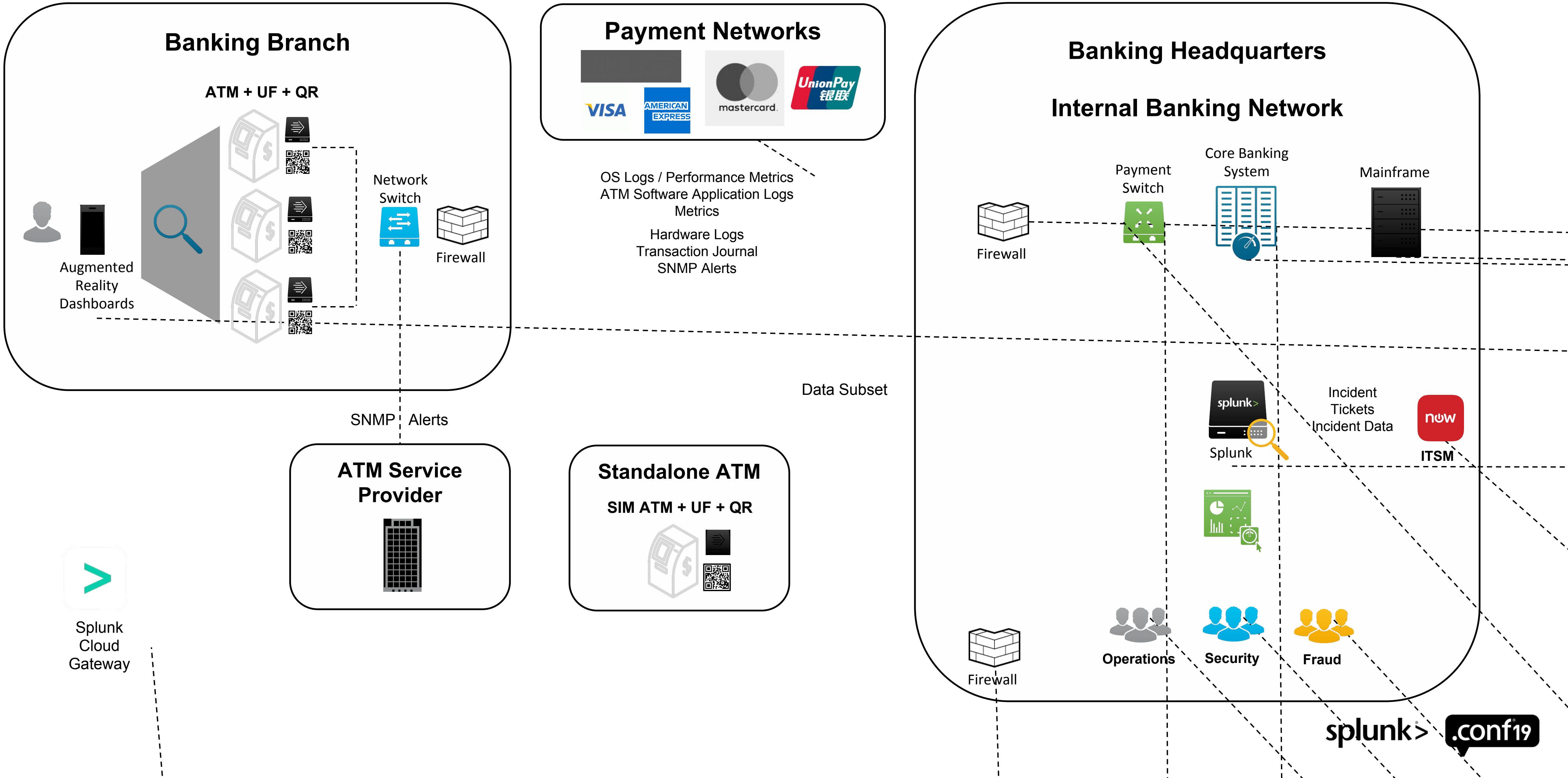
OS Logs / Performance Metrics
ATM Software Application Logs
Metrics

Hardware Logs
Transaction Journal
SNMP Alerts

Banking Headquarters

Internal Banking Network

High Level ATM Solution Architecture



Banking Branch

ATM + UF + QR

Augmented Reality Dashboards

Network Switch

Firewall

Payment Networks

OS Logs / Performance Metrics
ATM Software Application Logs
Metrics

Hardware Logs
Transaction Journal
SNMP Alerts

Data Subset

SNMP Alerts

ATM Service Provider

Standalone ATM

SIM ATM + UF + QR

Splunk Cloud Gateway

Banking Headquarters

Internal Banking Network

Firewall

Payment Switch

Core Banking System

Mainframe

Splunk

Incident Tickets
Incident Data

ITSM

Operations

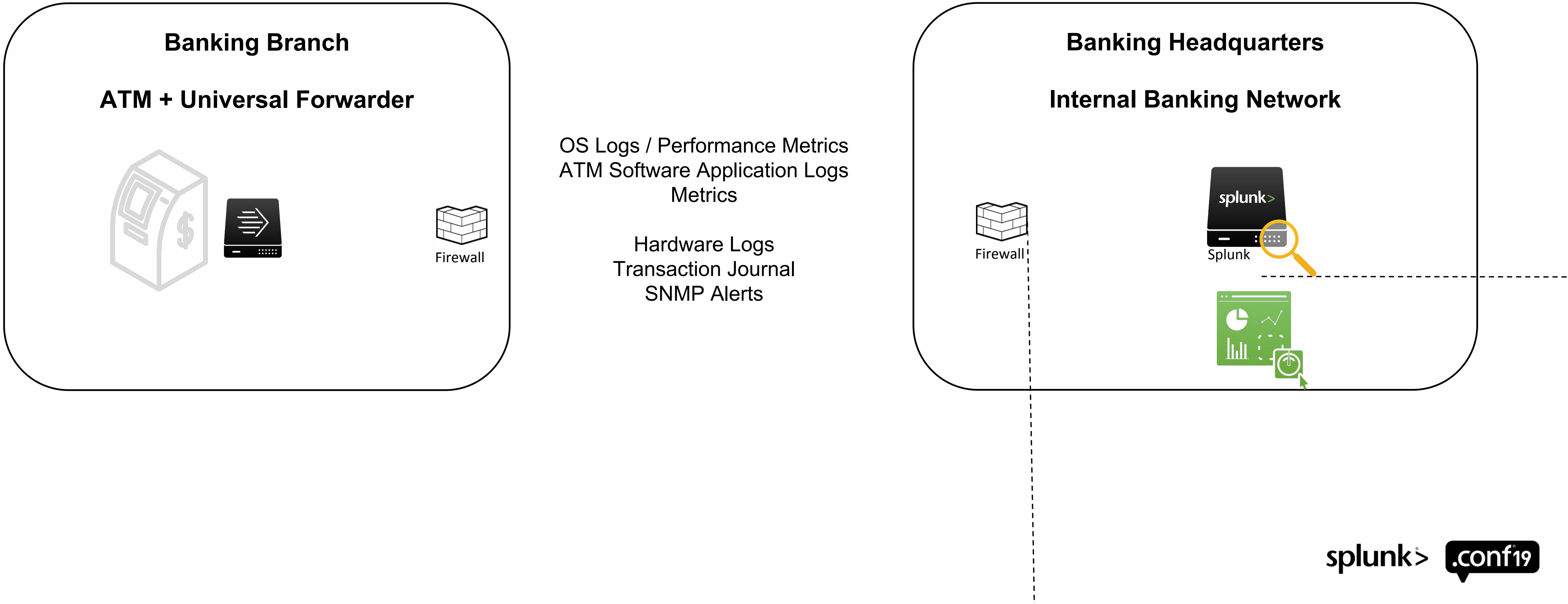
Security

Fraud

Firewall

The Universal Forwarder

Stream Data | Guaranteed Delivery | Load Balancing | Bandwidth Throttling | Buffering



Banking Branch

ATM + Universal Forwarder

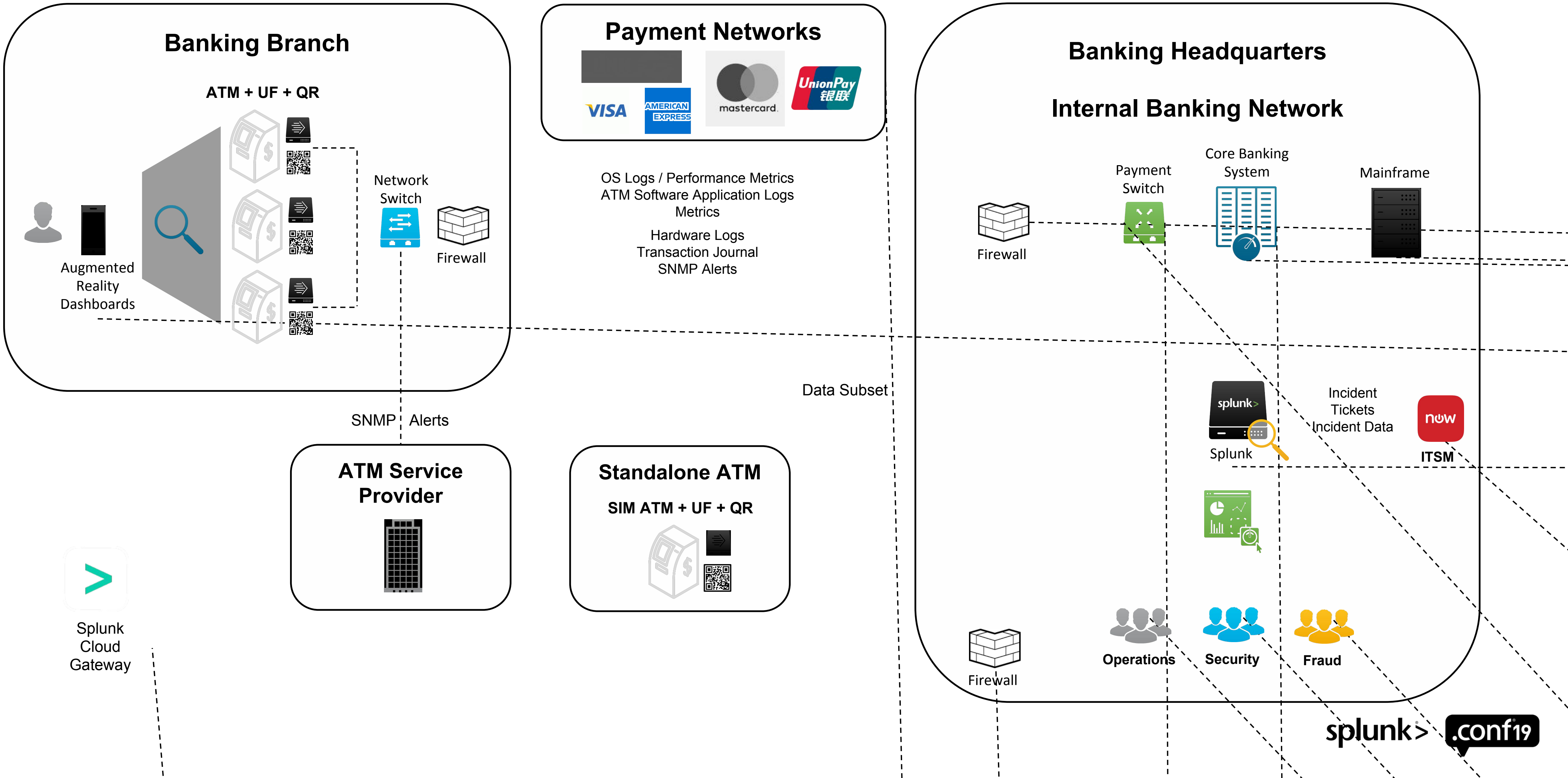
OS Logs / Performance Metrics
ATM Software Application Logs
Metrics

Hardware Logs
Transaction Journal
SNMP Alerts

Banking Headquarters

Internal Banking Network

High Level ATM Solution Architecture



Banking Branch

ATM + UF + QR

Augmented Reality Dashboards

Network Switch

Firewall

Payment Networks

OS Logs / Performance Metrics
ATM Software Application Logs
Metrics

Hardware Logs
Transaction Journal
SNMP Alerts

Data Subset

SNMP Alerts

ATM Service Provider

Standalone ATM

SIM ATM + UF + QR

Splunk Cloud Gateway

Banking Headquarters

Internal Banking Network

Firewall

Payment Switch

Core Banking System

Mainframe

Splunk

Incident Tickets
Incident Data

ITSM

Operations

Security

Fraud

Firewall

Demo

Fantastic Assets and Where to Find Them

Check out our thought leadership and connect with experts

Assets for Financial Services

Book: 40 Ways to Use Splunk in Financial Services

- Pick up your copy here today at our booth in the source=*pavilion
- Download the ebook on splunk.com
- Demo’s can be arranged for customers and partners on request

App: Splunk Essentials for Financial Services

- This toolkit is available on Splunkbase.

Our source of truth, for all customer stories and thought leadership: **Splunk.com**

.conf19

splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION