Securing a global investment fund using Splunk Cloud and Enterprise Security

Grant Slender | CISO & Head of Security, Cloud and Support

Simon O'Brien | Principal Sales Engineer

splunk> .conf19

Grant Slender
CISO & Head of Security, Cloud and Support | QIC

Simon O'Brien
Principal Sales Engineer | Splunk

splunk> .conf19

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.

Content Overview

Security, and some not-so-security focused content

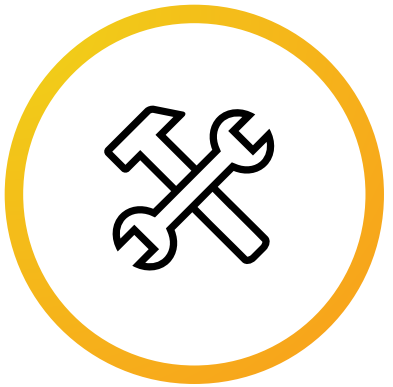
People

- Operational model
- Skills
- Services

Process

- Security journey
- Data onboarding
- Use case definition

Technology



- Splunk Cloud
- Enterprise Security
- Data sources

WE ARE A LONG-TERM SPECIALIST MANAGER IN ALTERNATIVES

A longstanding heritage with an established platform enabling us to become the visionary asset manager we are today.

- $80 billion in funds under management [1]
- Over 110 clients including government, pension plans, sovereign wealth funds, universities and insurers. Spanning Australia, Europe, UK, Asia, Middle East and US
- Established in 1991 by the Queensland Government to serve its long-term investment responsibilities
- Over 1000 employees with offices in Brisbane, Sydney, Melbourne, New York, Los Angeles, Cleveland, San Francisco, London and Copenhagen

- GLOBAL INFRASTRUCTURE
- GLOBAL REAL ESTATE
- GLOBAL PRIVATE CAPITAL
- GLOBAL LIQUID STRATEGIES
- GLOBAL MULTI-ASSET

[1] As at 30 June 2019. All figures in AUD.

QIC & Splunk

The Journey so far

splunk> .conf19

QIC's expectations and requirements

People

- 24x7 security capability
- Retention and skill gaps

Process

- Repeatable, consistent
- Good fit with our processes

Technology

- Integrated tooling
- Flexible and adaptable

QIC's expectations and requirements

People

- 24x7 security capability
- Retention and skill gaps

Process

- Repeatable, consistent
- Good fit with our processes

Technology

- Integrated tooling
- Flexible and adaptable

= SECURE!

The journey

How QIC came to use Splunk Enterprise Security in Splunk Cloud

SIEM on prem

The early days

Fully outsourced

A better option?

Splunk Cloud

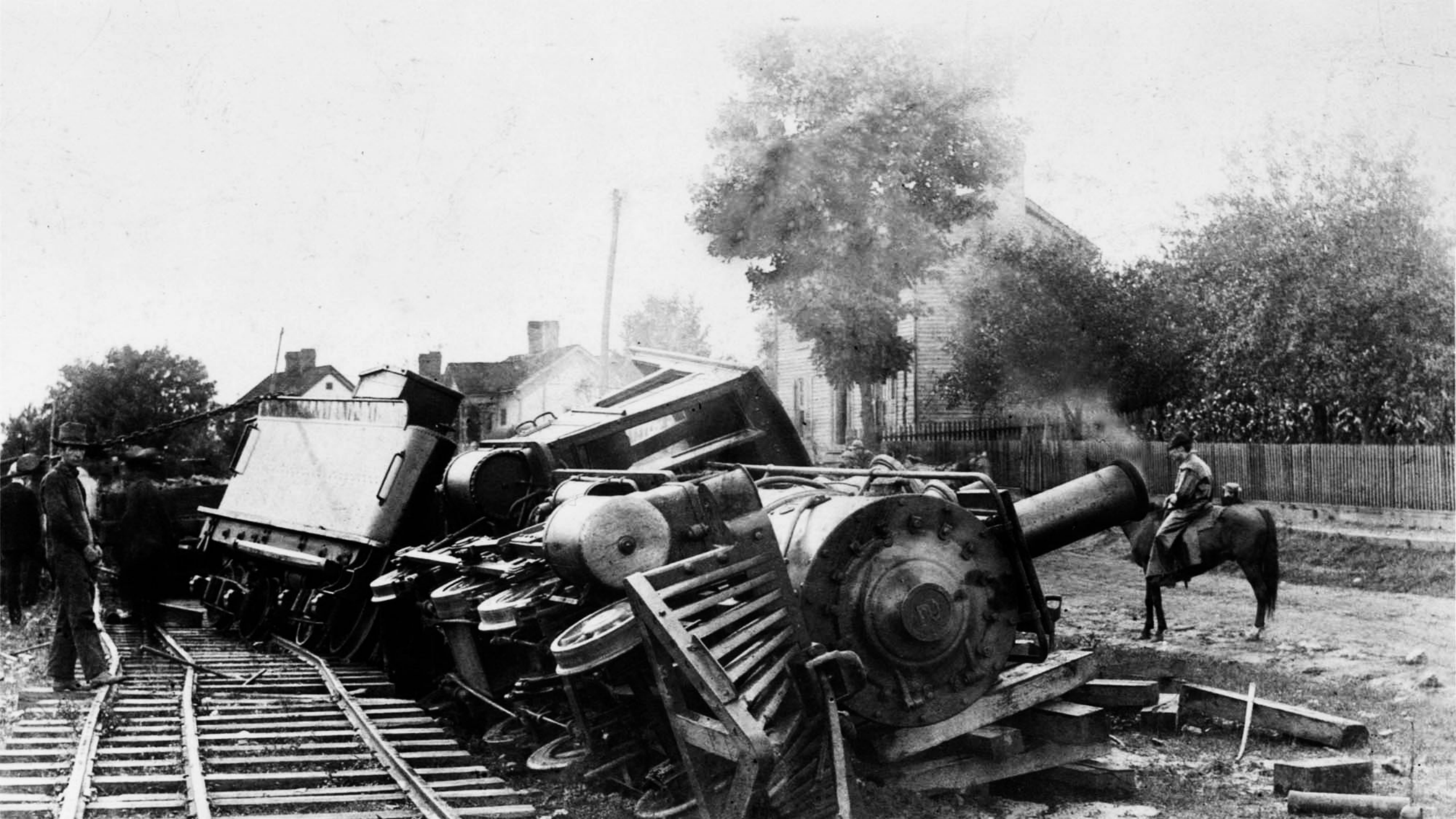
The goldilocks zone

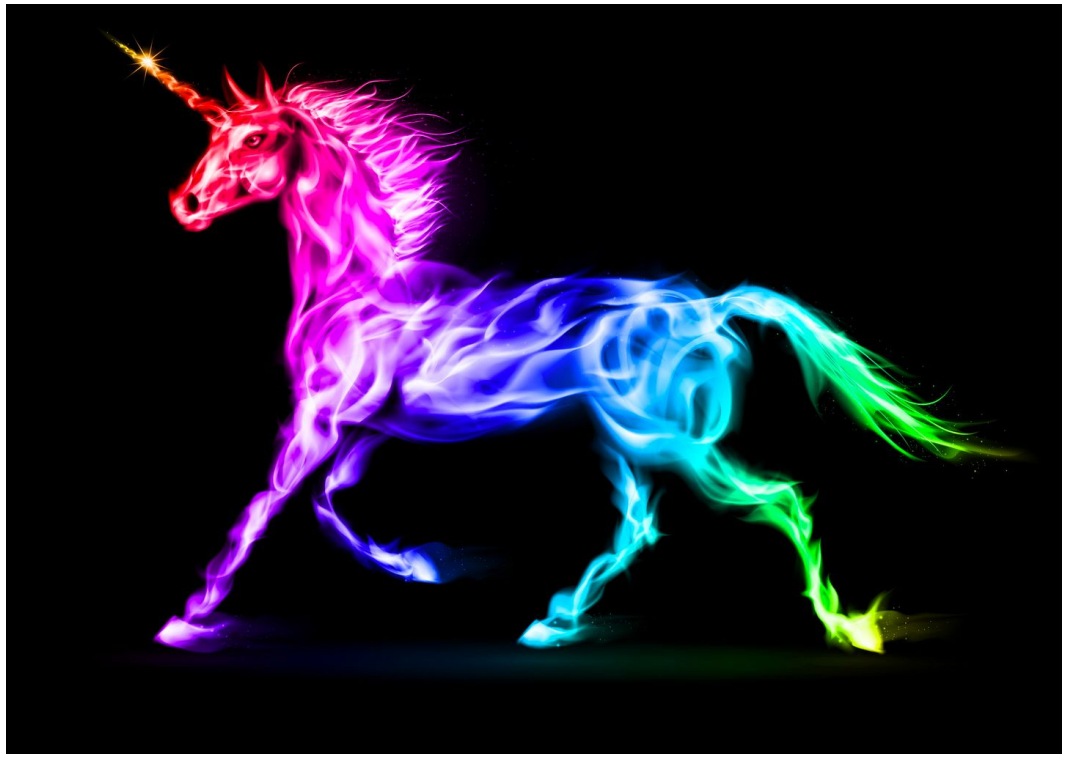
I think we have found our goldilocks architecture.”

Grant Slender

The operational model

splunk> .conf19





Operational Model

QIC personnel

Highly experienced professionals

Specialist 3rd parties

Splunk IT ops and security skillsets

External MSSP

Specialist security triage and support skillsets

Splunk Cloud

Splunk architecture, design and operations

splunk> cloud™

The benefits of Splunk as a service

Fastest time to value

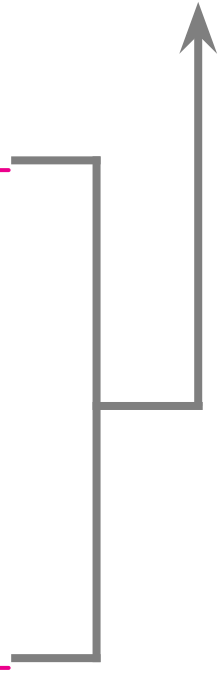
Eliminates infrastructure requirements

Maximizes value from limited resources

Managing Splunk Is More Than Just Software

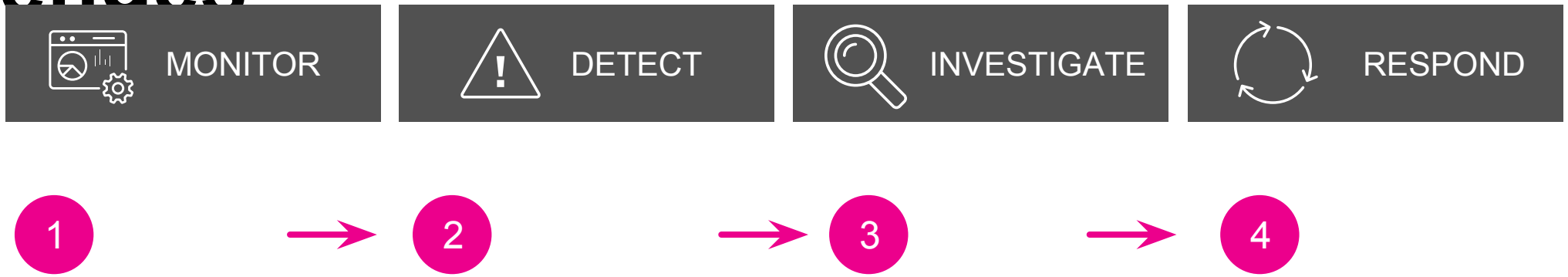
	Responsibility	Splunk Ent Deployed On-Premises	Splunk Cloud
Admin Tasks: One-time Setup	Purchase/rent HW	QIC	Splunk
	Rack and stack, cable, network all HW	QIC	Splunk
	Install Splunk	QIC	Splunk
	Install OS	QIC	Splunk
	Configure Splunk (create users, load apps, configure)	QIC	Splunk
	Configure indexes	QIC	Splunk
	Setup HA/clustering	QIC	Splunk
	Setup disaster and recovery	QIC	Splunk
	Configure forwarders	QIC	Joint
	Onboard data	QIC	QIC/MSSP
	Integrate with LDAP/AD	QIC	Joint
Admin Tasks: Ongoing	Scale up HW	QIC	Splunk
	Install Splunk patches / upgrades	QIC	Splunk
	Install OS patches / upgrades	QIC	Splunk
	Monitor deployment / health checks	QIC	Splunk
	Manage forwarders	QIC	QIC
	Create users / roles	QIC	QIC/MSSP
	Manage indexes	QIC	QIC/MSSP
	Onboard additional data	QIC	QIC/MSSP
	Load search head only apps	QIC	Splunk
	Load distributed apps	QIC	Splunk
	Load premium apps	QIC	Splunk
	Export data	QIC	Splunk
User Tasks	Search, alerts, reports, dashboards	QIC	MSSP/QIC/3rd Parties

Managing a Splunk deployment involves 12 on-going admin tasks, 8 of which are conducted by Splunk for a Cloud based deployment



splunk> .conf19

Splunk Enterprise Security Addresses Security Operations Challenges



KEY FEATURES

Splunk Enterprise Security™

SECURITY WORKFLOW Notable Event Framework	**EVENT CORRELATIONS** Search Management	**SECURITY ENRICHED CONTEXT** Asset, Identity Framework
THREAT INTELLIGENCE Threat Intel Framework	**RISK BASED ANALYTICS** Risk Scoring Framework	**ADAPTIVE RESPONSE** Adaptive Response Framework

Data onboarding process

splunk> .conf19

What Your Executives Want

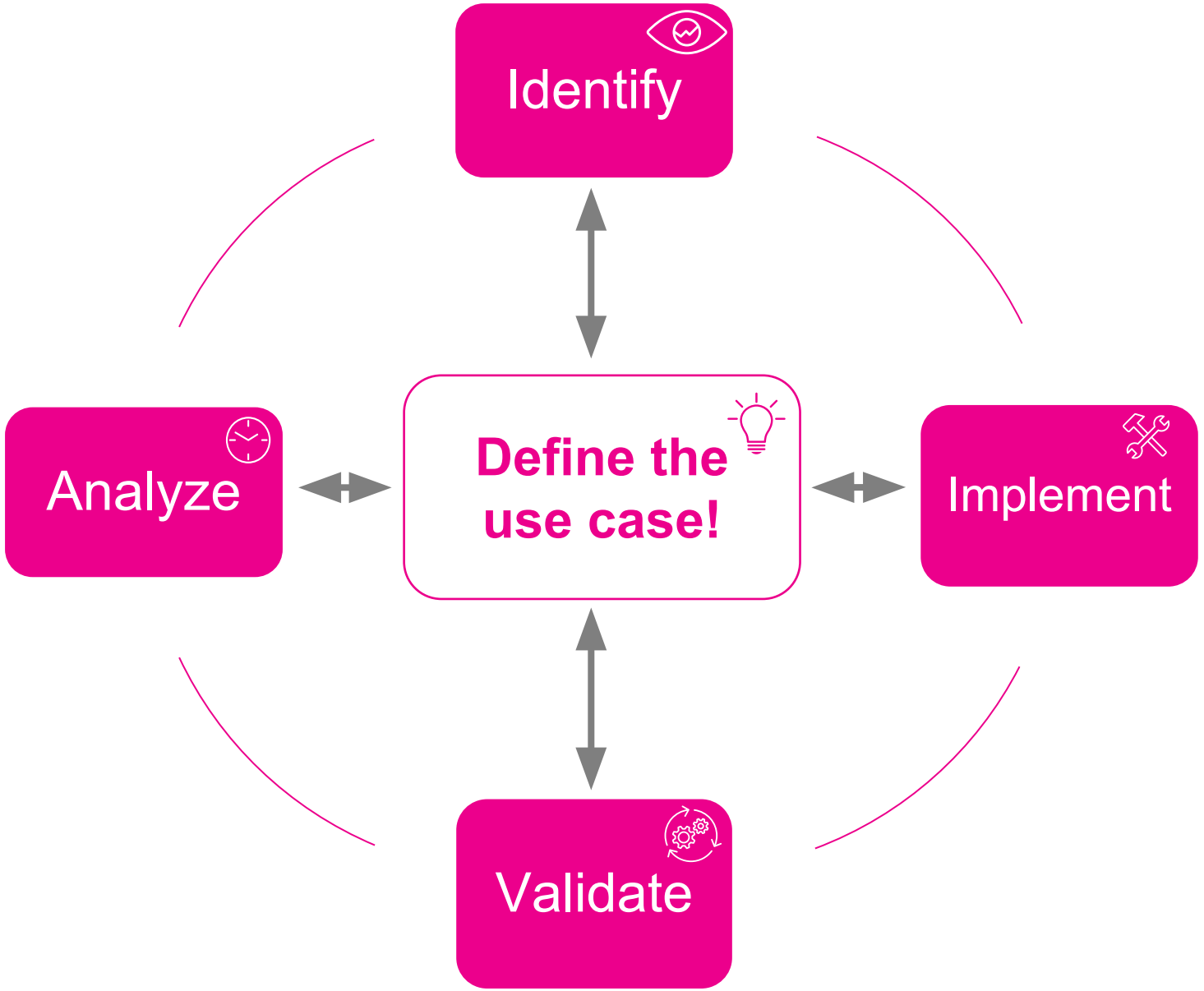
Splunk is not expensive. People are just lazy.”

Grant Slender

Don’t just throw data into Splunk. Define your use case first!”

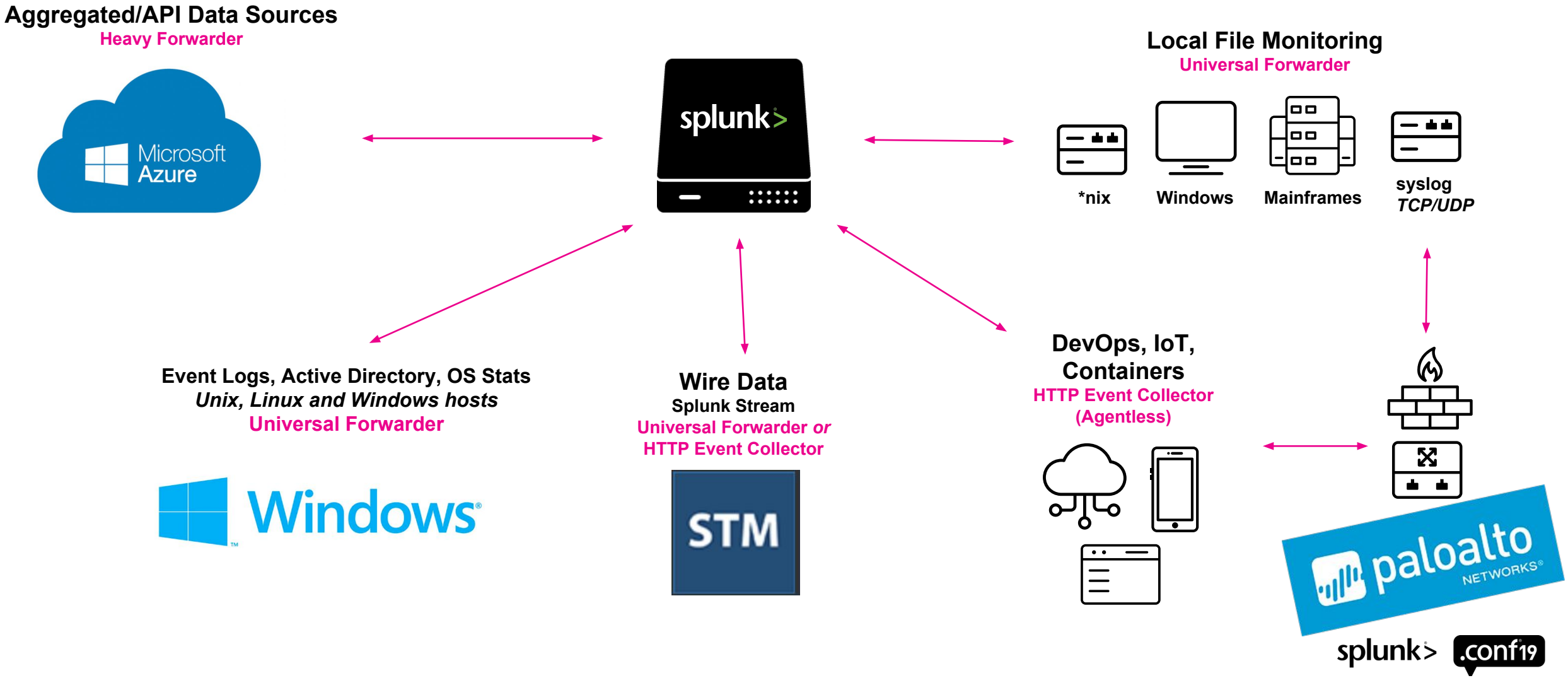
Grant Slender

Data onboarding process



What Can Splunk Ingest?

Agent-Less and Forwarder Approach for Flexibility and Optimization



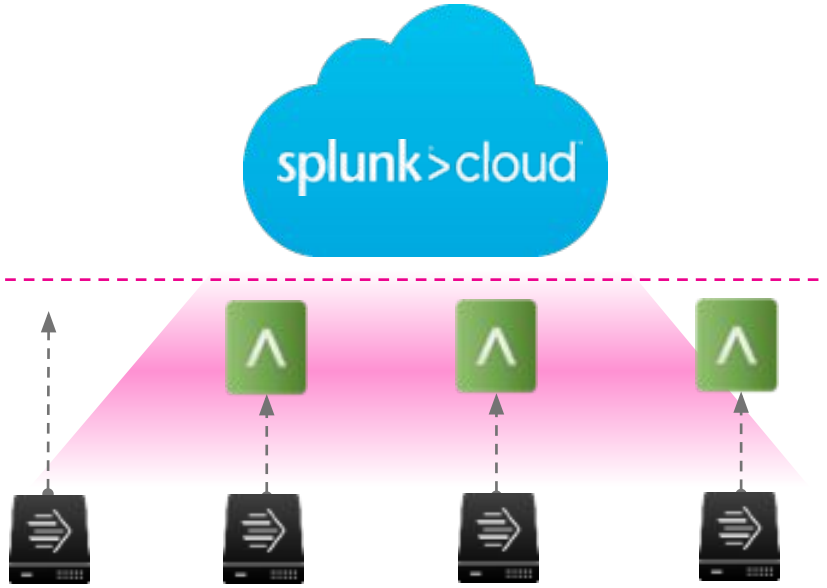
Use case overview

splunk> .conf19

Endpoint security posture improvements

Detection of brute force RDP connection attempts

- User working from home using a bridged connection to the Internet. UF deployed to ALL hosts.
- Target of brute force attacks from an IP in Europe.
- Attackers trying to authenticate to RDP with multiple usernames.
- WinEventLogs sent in almost real time from anywhere to Splunk allowed a use case to trigger an alert on the activity.
- The unusual activity prompted an investigation that helped uncover a misconfiguration on the endpoint firewall.



Custom threat intelligence

Provided through managed security services provider

- Custom TA deployed by SOC team to integrate threat feed into ES framework
- Mapped into Threat Framework to provide actionable insights to analysts based on trusted intel
- Generating hits against multiple data sources
- Tracking in excess of 9000 threats
- Has prompted action against vulnerability analysis

Most Active Threat Collections

threat_collection	search	sparkline
ip_intel	Source And Destination Matches	

Cisco device change monitoring

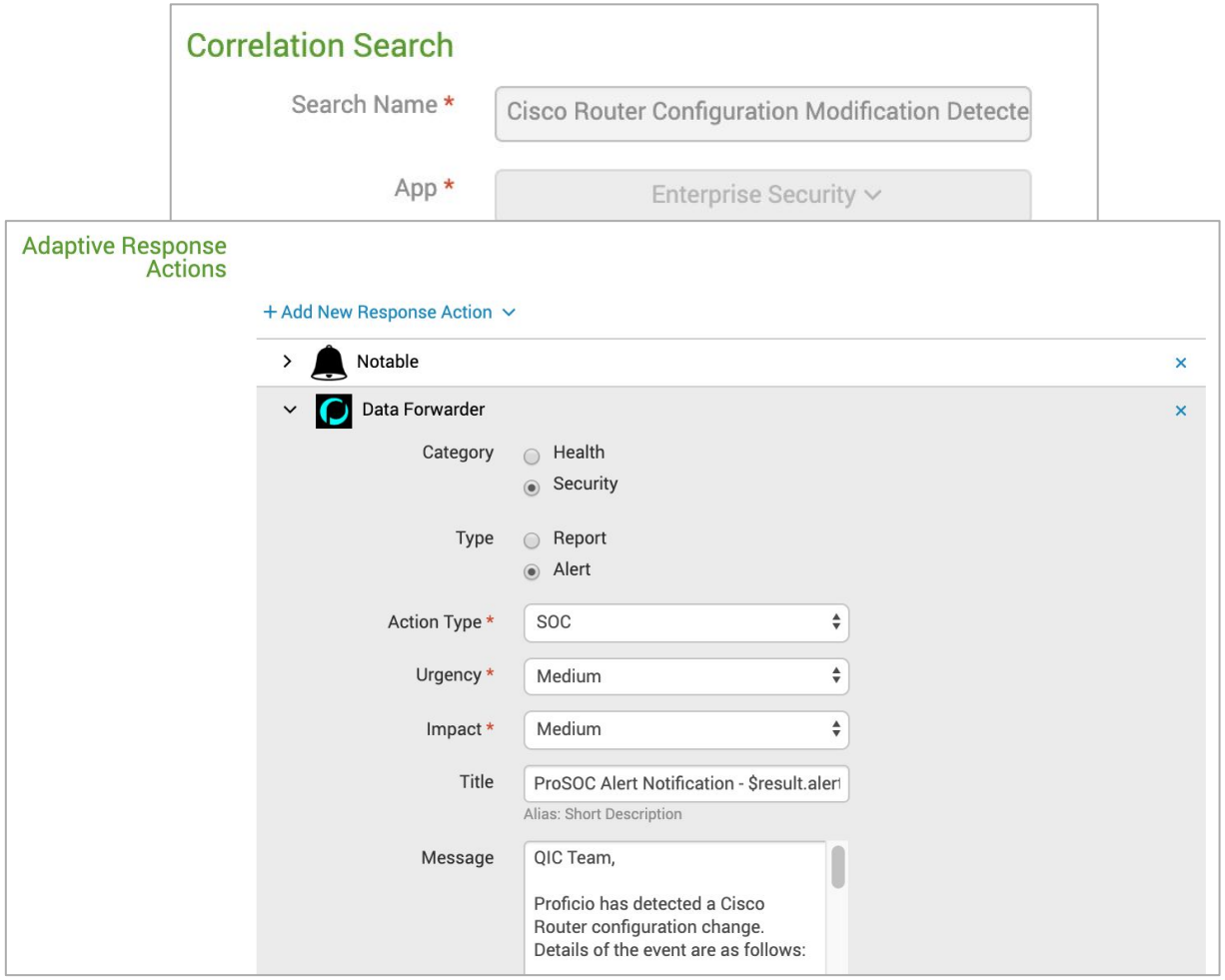
Detection of changes on critical devices

Notable deployed to identify changes to critical devices within the environment.

Custom notable developed and deployed through use case development process.

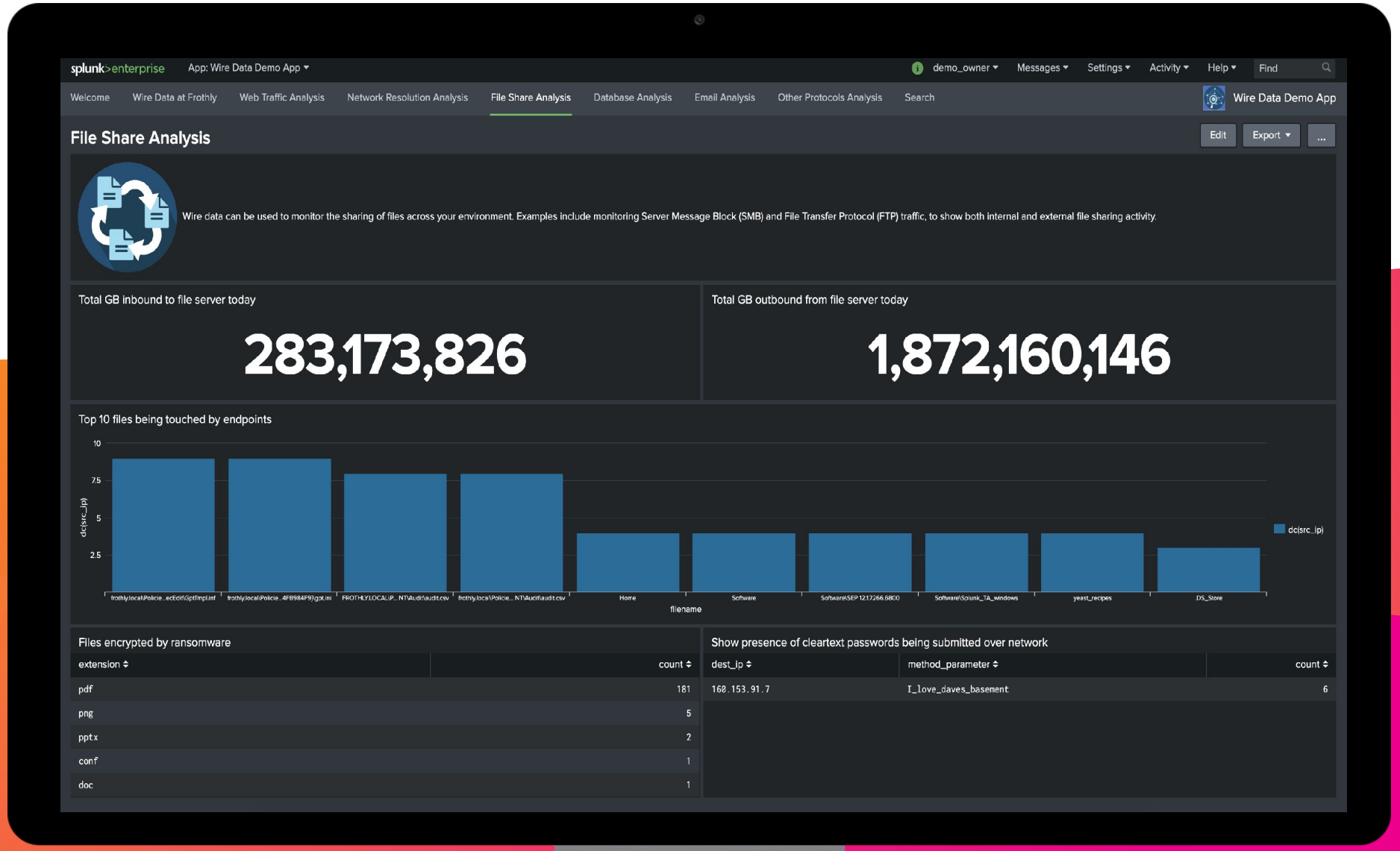
Adaptive response includes forwarding event to outsource SOC provider, via custom TA with actions.

Detected the cutover to new outsource network provider within short timeframe.



Business focussed outcomes

What we achieved outside the security world



The future

splunk> .conf19

The journey

How QIC came to use Splunk Enterprise Security in Splunk Cloud

SIEM on prem

The early days

Fully outsourced

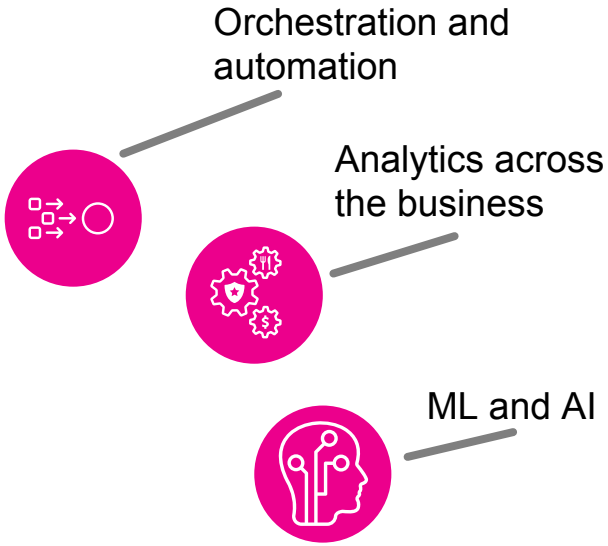
A better option?

Splunk Cloud

The goldilocks zone

The future

What next?



Key Takeaways

1. Consider the people, process and technology aspects of your organizational requirements

2. Define use cases and security visibility requirements first, then on board data!

3. Iterate. You (probably) won't get this all right the first time around!

Q&A

Grant Slender |
CISO & Head of Security, Cloud and Support |
QIC

Simon O'Brien |
Principal Sales Engineer | Splunk

splunk> .conf19

.conf19

splunk>

Thank You !

Go to the .conf19 mobile app to

RATE THIS SESSION