# Optimizing Splunk Enterprise on AWS

Accelerating Integration and Value Realization of Enterprise Intelligence

October 2018

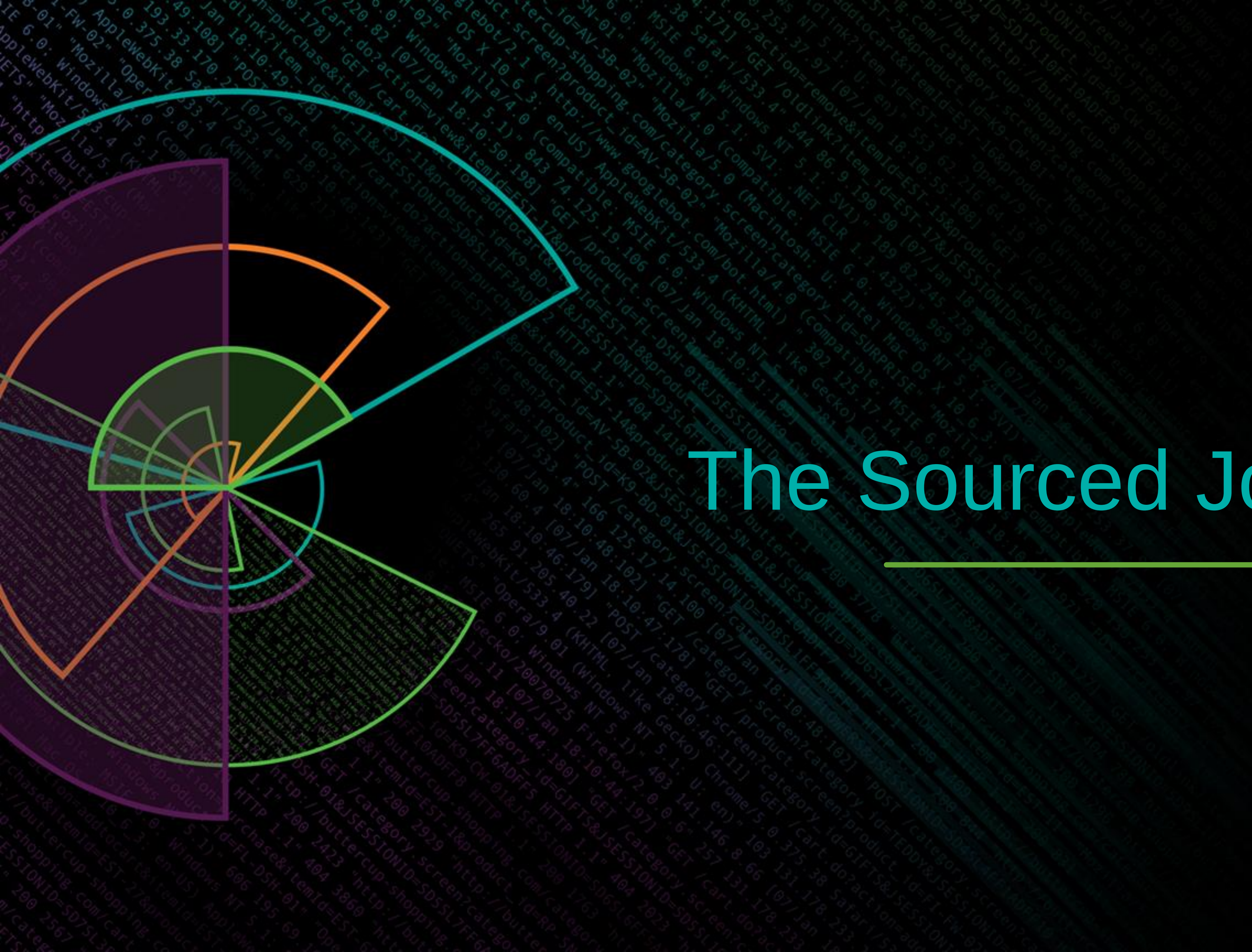
# Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. 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 functionality described or to include any such feature or functionality in a future release.

# Agenda

1. The Sourced Journey
2. The Challenge
3. The Solution
4. The Outcomes



# The Sourced Journey

# Your Presenters for the Day

Toronto based, knee-deep in AWS technologies and part of the Sourced Engineering team

**Jonathan Hodges**

Associate Systems Architect

https://www.linkedin.com/in/jonathan-hodges

**Daniel Barnett**

Associate Systems Architect

https://www.linkedin.com/in/danielrmbarnett

splunk> .conf18

# A Boutique Consultancy with a Global Reach

Sourced brings a unique perspective on cloud based on experience and innovation

Sourced Group founded in 2009 in Sydney, Australia

Specializing in Enterprise Cloud Transformation

Deep expertise in financial services, aviation, health and media

Proven delivery capability in AWS, GCP and Azure

# Our Solution Portfolio

Driving leading edge differentiation into IT

## SECURITY

Proactive & Reactive Controls | Encryption | Network Security | Identity & Access

## GOVERNANCE RISK & COMPLIANCE

Control Audits & Delivery | CCOE Transformation | Executive Cloud Governance | Program Delivery

### CLOUD TRANSFORMATION

- Cloud Strategy Delivery
- Business Case Development
- Organisational Change Management
- Workload Assessment
- Workload Migration Roadmap
- Cloud Platform Architecture

### DEVOPS

- Workload Architecture & Migration
- SDLC Enablement Via CI/CD
- Configuration Management
- Infrastructure as Code
- Automation

### DATA MANAGEMENT

- Big Data
- Database Migration
- Database Optimisation
- Data Warehouse
- Business Intelligence

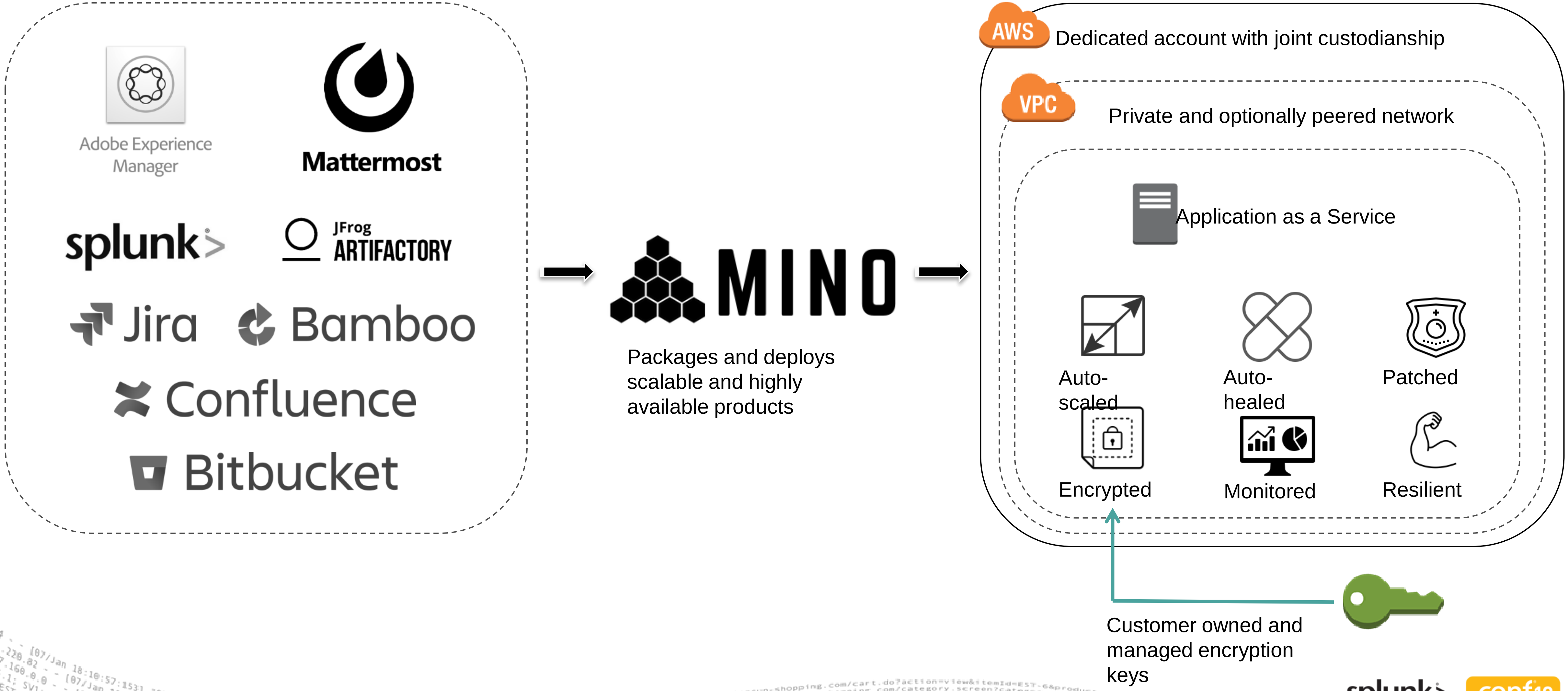
### ENGINEERED SaaS

- ChatOps
- Development Toolset
- Centralised Logging
- Content Management
- Next Generation Workspace

PLAN > BUILD > RUN

# Managed Services… with a Twist

We do the heavy lifting so our clients focus on business value that sets them apart from their competition



Packages and deploys scalable and highly available products

Dedicated account with joint custodianship

Private and optionally peered network

Application as a Service

Auto-scaled

Auto-healed

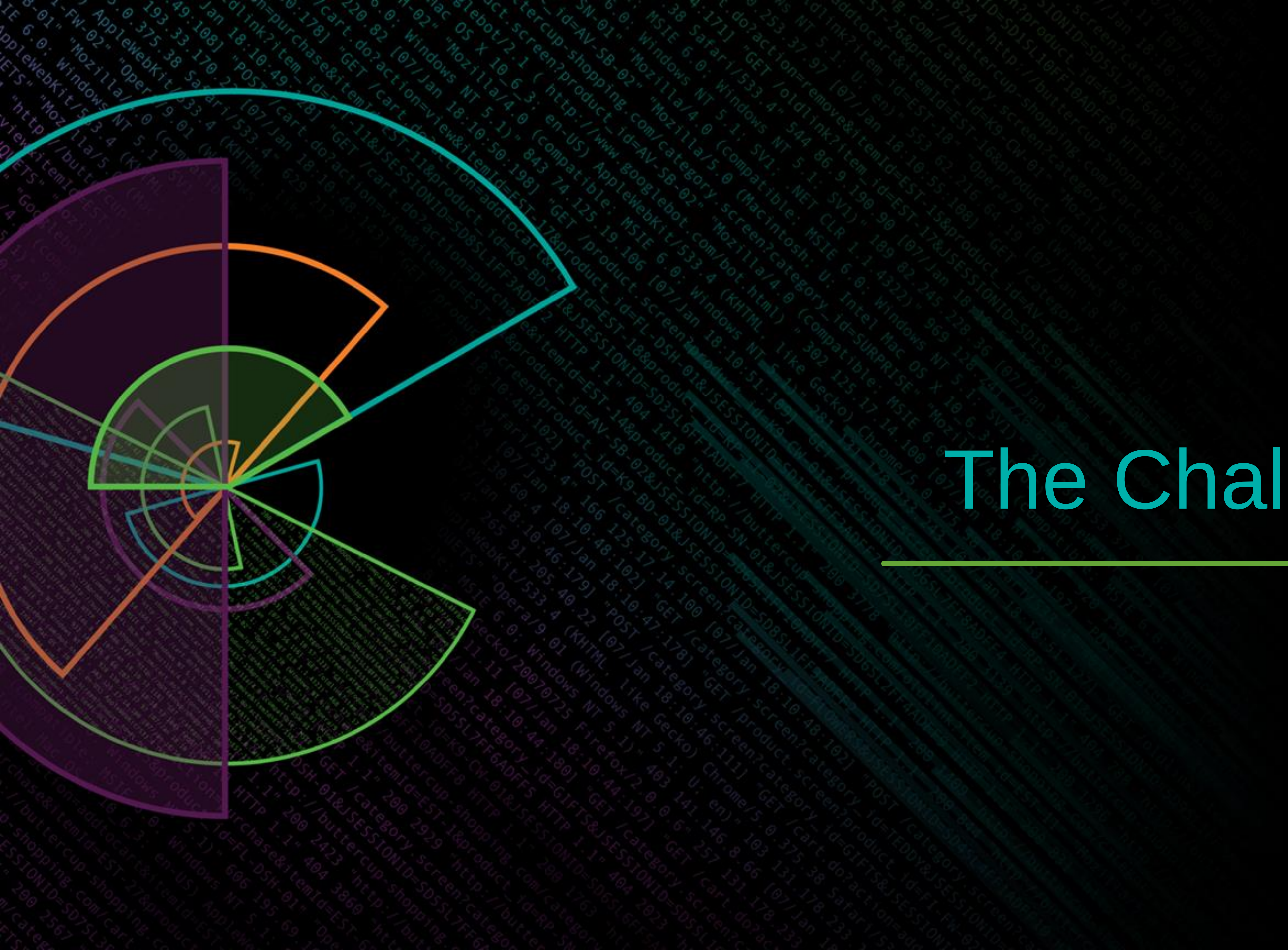
Patched

Encrypted

Monitored

Resilient

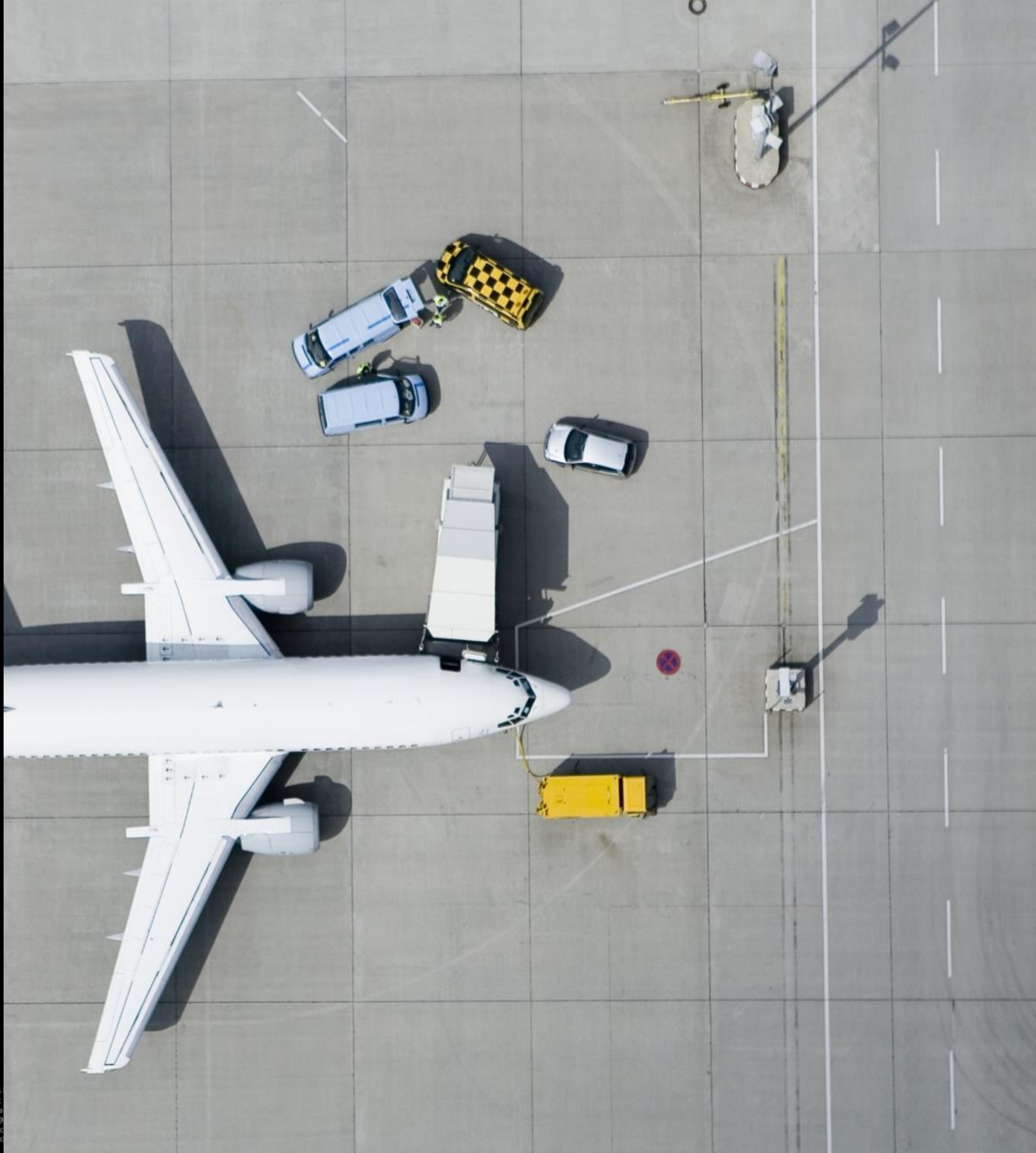
Customer owned and managed encryption keys



# The Challenge

# The Client

- Global airline based in Australia
- Over 1.6TB of daily data ingestion into Splunk
- Utilizing general purpose Splunk search capability, adding Enterprise Security (ES) and Splunk app for PCI Compliance
- Further growth and expansion expected as Splunk became the de-facto centralized logging platform for the enterprise



# A High Barrier of Entry

Deployment and operational challenges slow down integration and realization of business value

- Capital intensive when deployed on physical hardware
- High level of internal operational skills and experience required
- Eroded time to market value due to complex implementation effort
- Diversion of effort from Cloud transformations to building and maintaining supporting services
- Regulatory directives rendering traditional SaaS offerings non-viable

# The Requirements

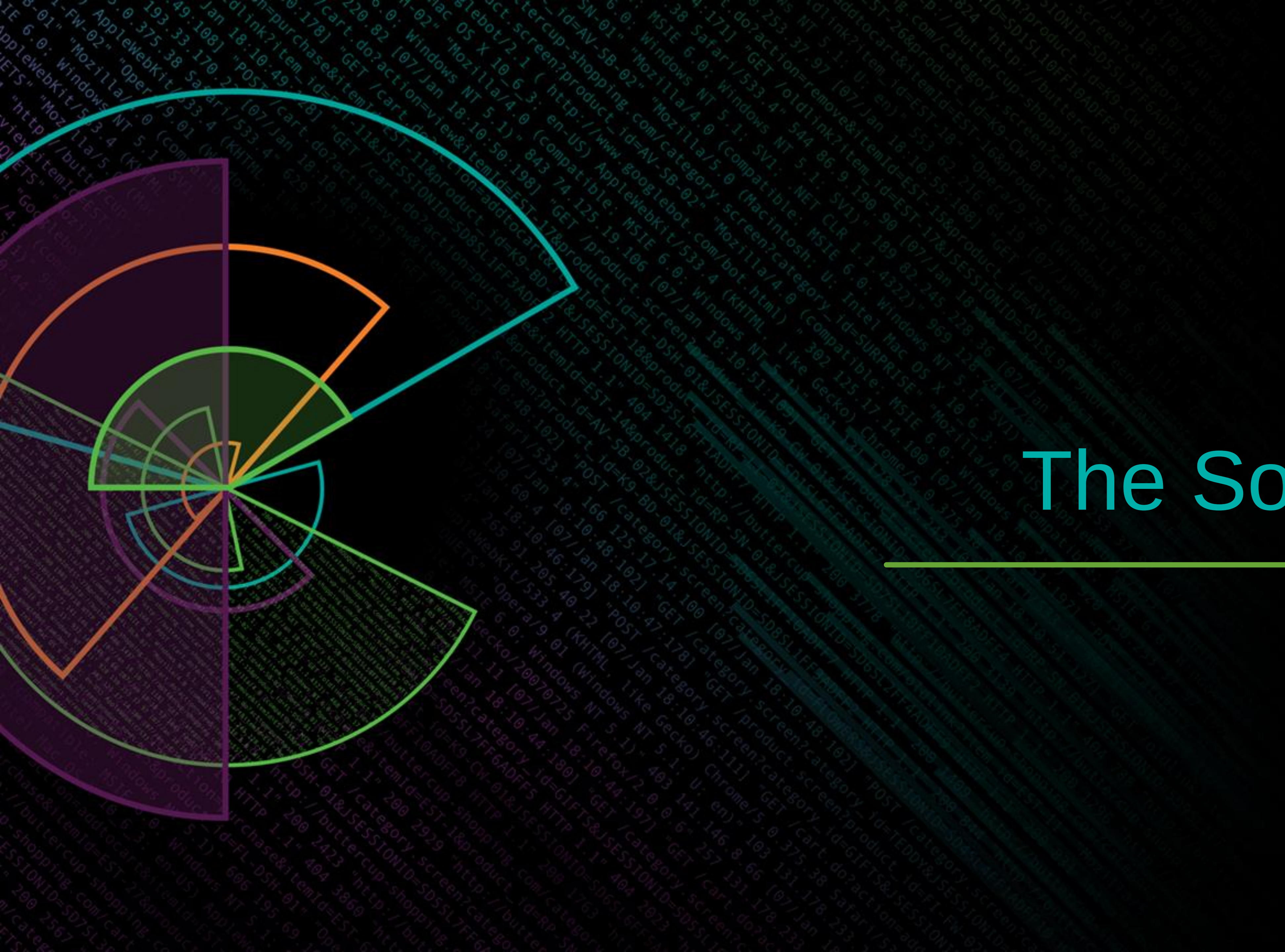
A set of non-negotiable core requirements were provided to our team to deliver

No outage during maintenance and patching periods

Reducing platform cost to allow for higher data ingestion rate

Ability to scale the platform depending on business growth

24x7 support to ensure highest possible platform availability



# The Solution

# The Requirements

A set of non-negotiable core requirements were provided to our team to deliver

No outage during maintenance and patching periods

Reducing platform cost to allow for higher data ingestion rate

Ability to scale the platform depending on business growth

24x7 support to ensure highest possible platform availability

# Outage-less Deployments

Minimizing risk in a crit-1 application deployment

No outage during maintenance and patching periods

- Ensuring no data loss of historical and ongoing operations
- Reducing synchronization time and impact
- Enabling data and functionality verification prior to release
- Simple rollback
- Zero impact to end-users

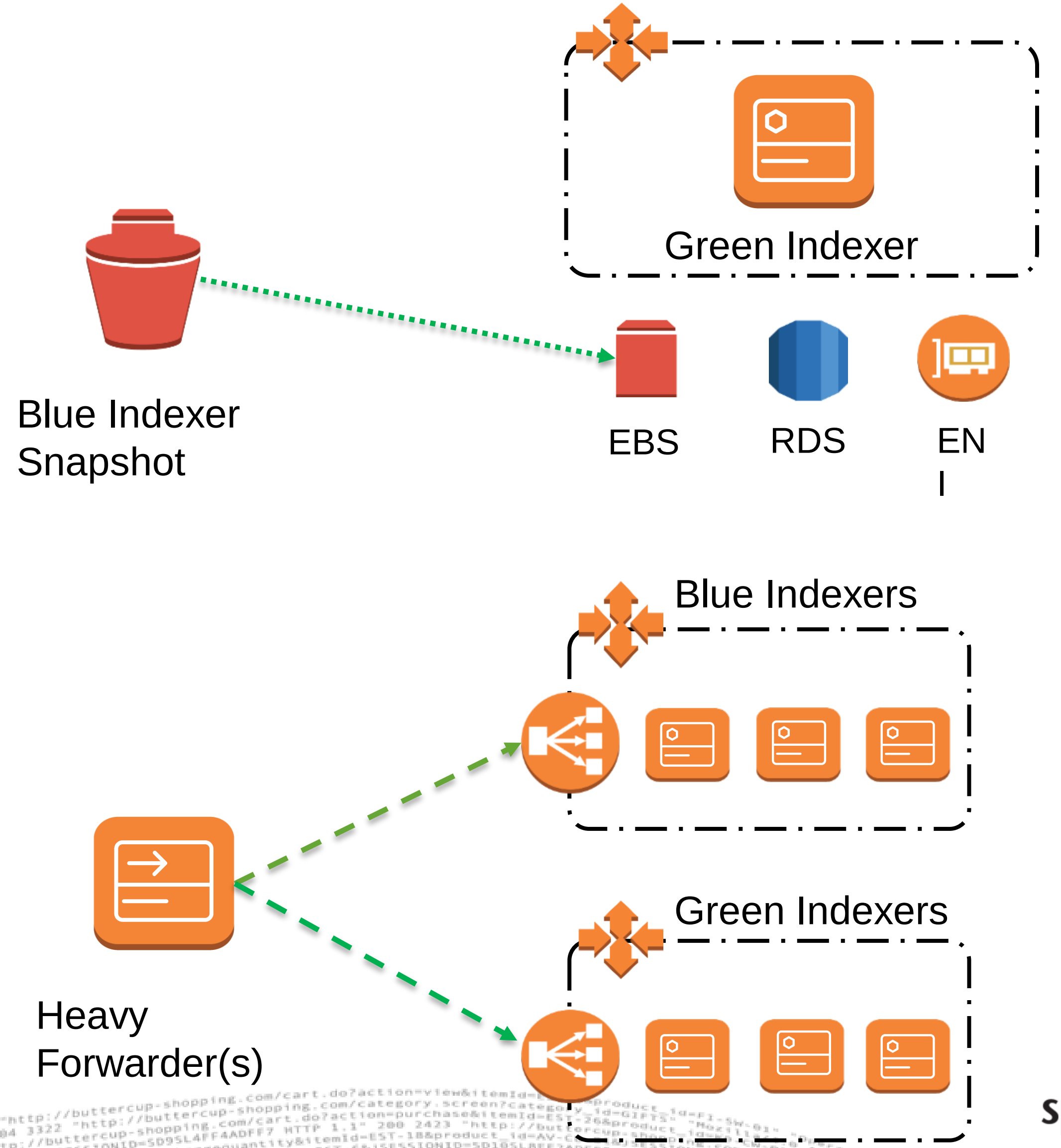
# Blue Green Deployment

Achieving data parity in blue green Splunk deployments

- Paralleled Architecture and Configurations
  - Backup/restore (Snapshotting)
  - Data baseline to limit sync activities

- Synchronously index new data
  - Splitting HF Traffic

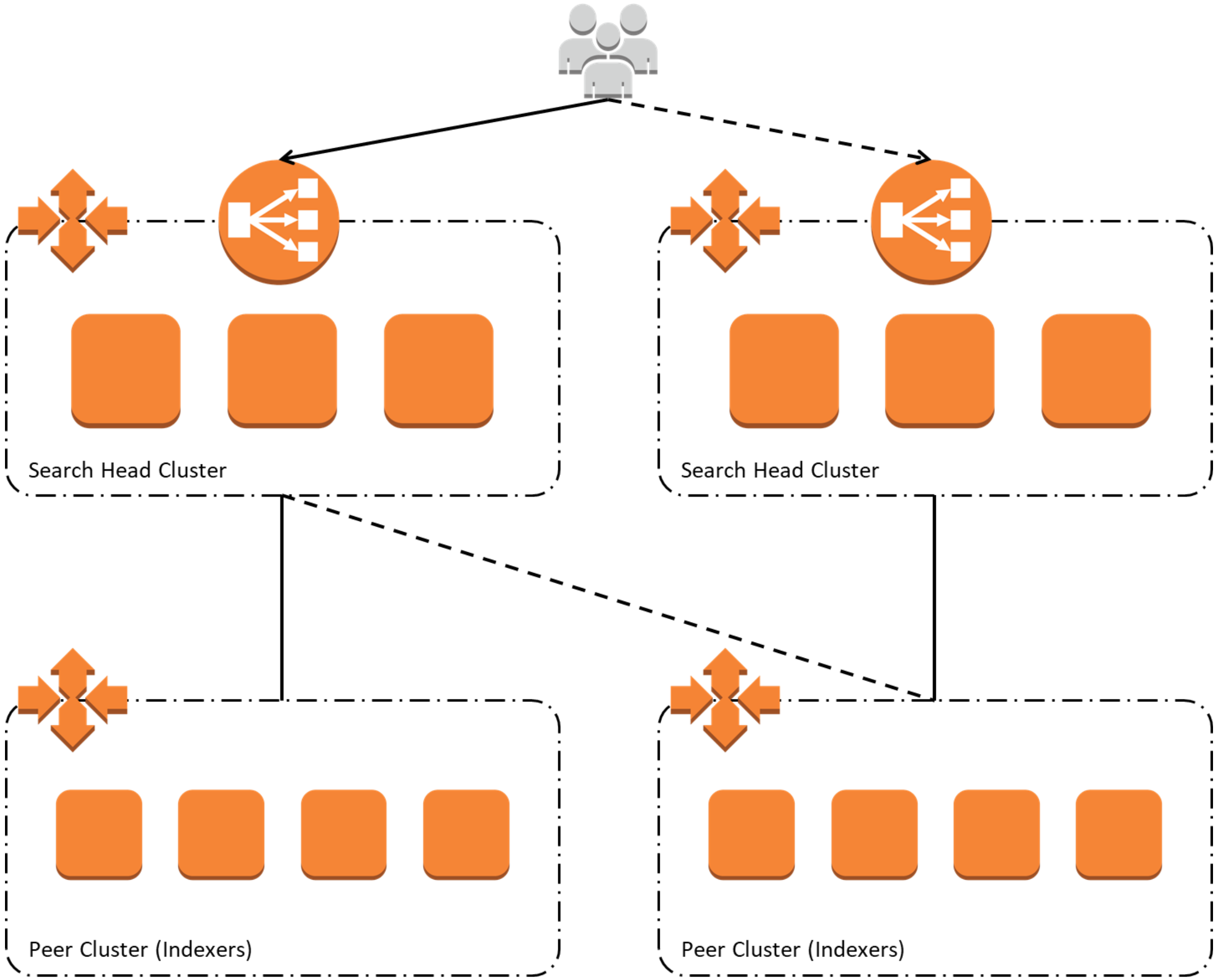
- Synchronize searches
  - Multi-Site Replication



# Blue Green Deployment

Splunk deployment UAT in isolation and release into production

- Testing in isolation
  - Load Balancing
  - Unique Endpoints
- Release
  - As simple as updating a DNS entry
  - Process identical in rollback activities
- End-user impact
  - Continuous service, continuous value



# The Requirements

A set of non-negotiable core requirements were provided to our team to deliver

No outage during maintenance and patching periods

Reducing platform cost to allow for higher data ingestion rate

Ability to scale the platform depending on business growth

24x7 support to ensure highest possible platform availability

# Indexer Storage

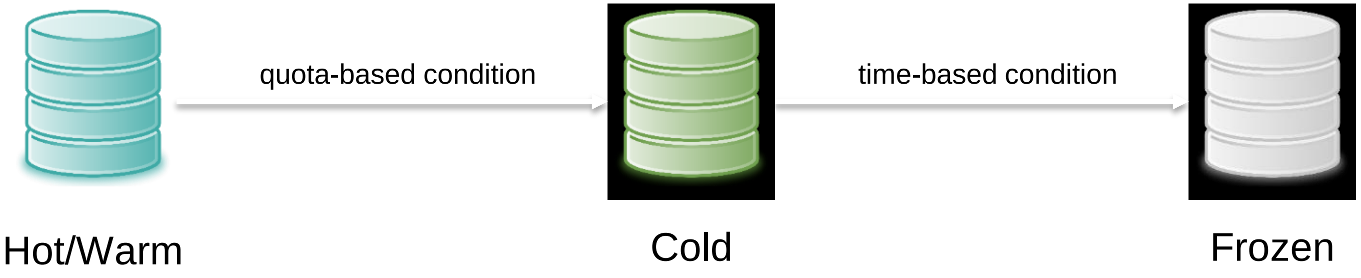
Mapping basic vendor requirements directly to AWS storage

Reducing platform cost to allow for higher data ingestion rate

- Daily indexing rate = 1.6 TB/day
- Retention period = 90 days (30 - hot/warm, 60 - cold)
- Indexed data = 1.6 x 90 = 144TB
- Sites = 2, Replication factor = 2
- Assumed compression of 20%
- 115.2 TB total storage
- io1 volume at 1,200 IOPS
- 4 Indexing nodes per site with 16 TB storage each

# Mapping Data to Storage Requirements

Chronological ordering of data with residence defined by quota and time based conditions



quota-based condition

time-based condition

### Hot/Warm

- Relatively low storage consumption
- <72 hours old
- High performance storage
- Low latency search for recent data
- Impacts end users' perception of the platform

### Cold

- Higher storage consumption
- Up to 60 days old
- Older data, less frequently queried
- Data is still searchable by end users

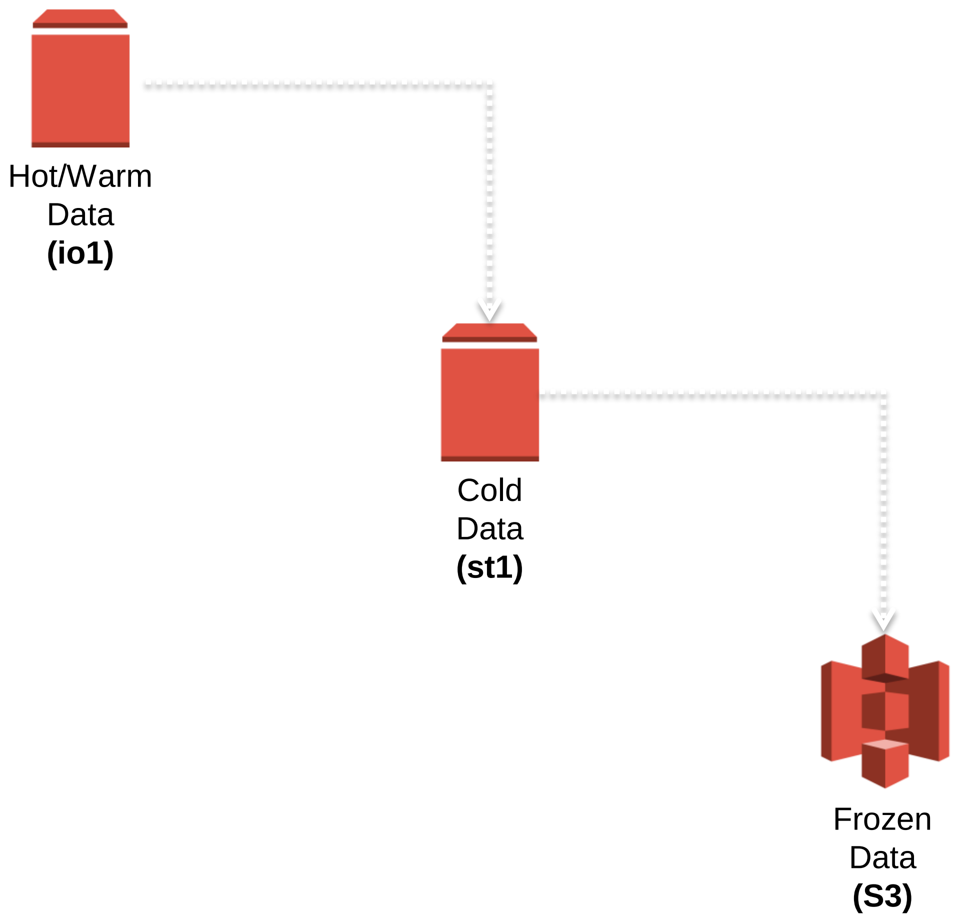
### Frozen

- Bulk of storage consumption
- Usually retained for a set period to meet regulatory compliance mandates
- Cost optimized storage for rarely accessed data

# Storage Optimization

Leveraging AWS storage options

- Leverage the data rolling mechanism native to Splunk to host data on different storage tiers
- Storage decisions are based on performance requirements related to business use cases
- Other AWS services such as Glacier can be leveraged for longer term and less expensive data archiving



Hot/Warm Data **(io1)**

Cold Data **(st1)**

Frozen Data **(S3)**

# Advanced EBS Patterns for Maximum Performance

Making use of various EBS configurations and features to drive performance and efficiency

## Optimizations

- Fall back to traditional disk configurations (RAID) to exploit disk performance characteristics
- A ‘free’ performance gain as disk is charged per GB not per volume but we get access to more IOPS
- Thin-provisioning of storage – true cloud computing model of pay for what you use
- Fallback to General Purpose volumes if their size will allow sufficient IOPS (be mindful of SLAs and exhausting burst credits for volumes < 1TB)

## Challenges

- Only works for some IO patterns scenarios – little performance improvement for sequential read/writes
- But introduces complexity of deployment and backups – can’t simply snapshot all disks in a RAID configuration
- Combination of AWS Step Functions, Lambda and SSM used to orchestrate consistent backup volume sets.
- Internal system ‘Chelydra’ commissioned to meet these backup management requirements

# Leveraging Convertible Reserved Instances

Advances in reserved instances offerings made it fiscally appealing with a low risk profile

- Convertible reservations provide reduced EC2 pricing with low risk
- Resale market for unused reservations
- Convertible instances exchangeable for deeper savings with pricing reductions
- Instance family and OS exchangeable with convertible reservations
- Maximize efficiency with 3 year standard reservations
- Roll reservations up or down as utilization increases
- Reduce TCO with no performance impact
- Reservations also available for RDS

# The Requirements

A set of non-negotiable core requirements were provided to our team to deliver

No outage during maintenance and patching periods

Reducing platform cost to allow for higher data ingestion rate

Ability to scale the platform depending on business growth

24x7 support to ensure highest possible platform availability

# Scaling the Clusters

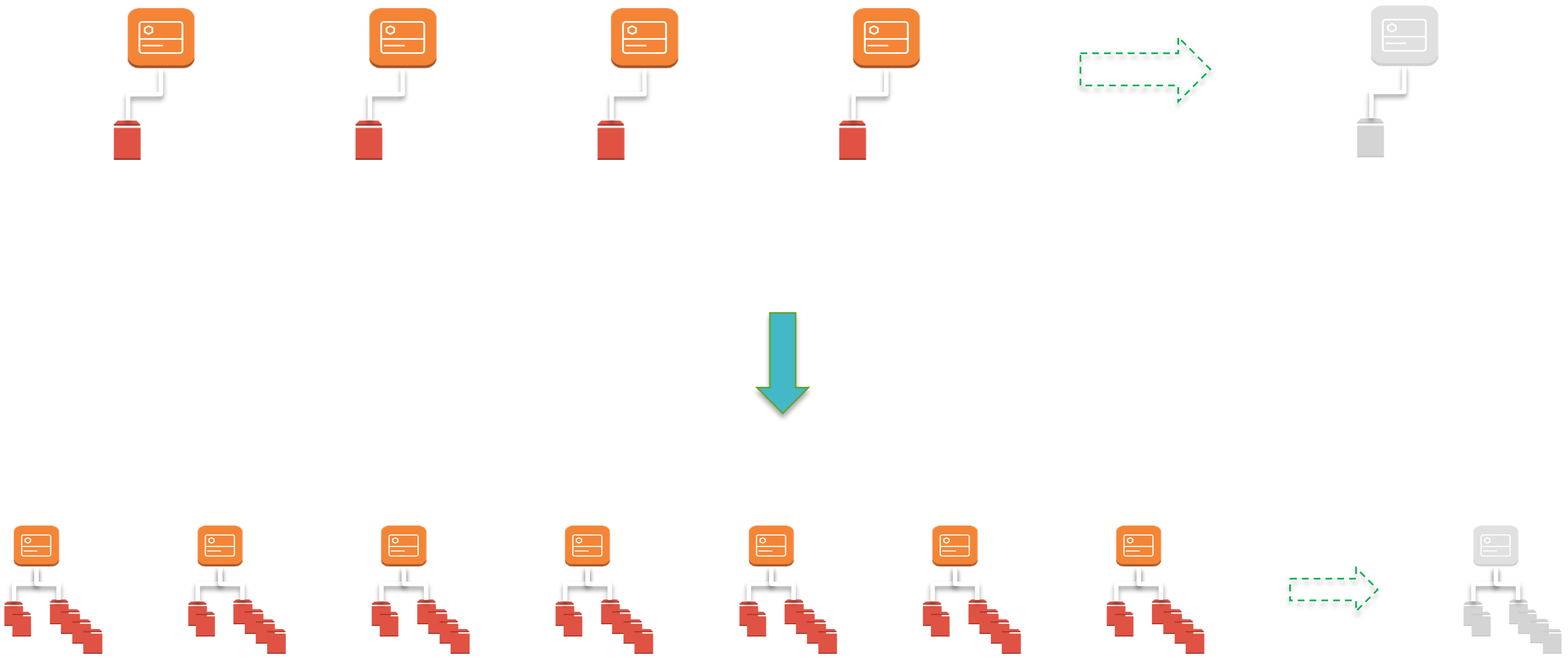
Architecting for incremental scalability

Ability to scale the platform depending on business growth

- Standard Auto-Scaling patterns inappropriate for Splunk distributed architecture
- Indexers and Search Head Cluster members managed in unique methods
- Indexer storage scaling requires additional design and operational considerations

# Scaling the Clusters

Architecting for incremental scalability



# Scaling the Clusters

Architecture and Automation Considerations

- Naming conventions and taxonomy
- Source of truth
- Stateless compute
  - EBS, ENI
- Infrastructure and baseline configuration
  - Roll forward and net-new systems
  - Paralleled outcomes

- Cluster membership management
  - Retaining IDs
  - Operations
- Configuration deltas within cluster members
- Distributed Management Console
- Master maintenance mode

# The Requirements

A set of non-negotiable core requirements were provided to our team to deliver

No outage during maintenance and patching periods

Reducing platform cost to allow for higher data ingestion rate

Ability to scale the platform depending on business growth

24x7 support to ensure highest possible platform availability

# Supporting Critical Systems

Meeting the needs of global operations

24x7 support to ensure highest possible platform availability

- Active operations 24/7
- Daily decisions leveraging insights
- Security and Incident response relying on service
- Logs received from sources around the globe

# Follow-the-Sun Support

- Leveraging Sourced’s global presence to deliver quality customer-centric support capability
- Service management best practices
- Hotline for emergency access to support engineers
- Regular operational governance meetings allowing client visibility and input

sourced | ENGINEERING

splunk>

Be an IT superhero. Go home early.

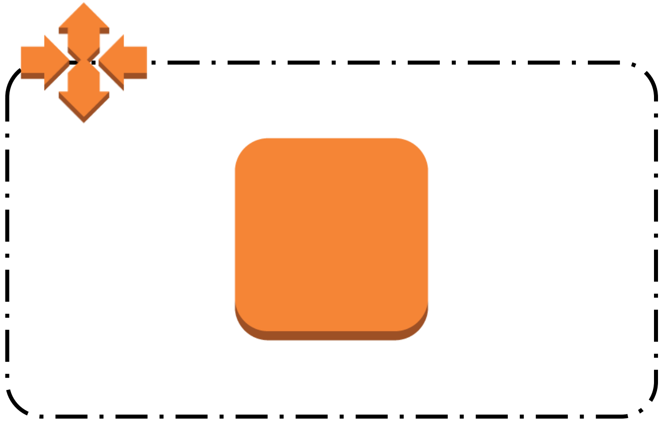
**Us too!**

sourced | ENGINEERING

# Self-Healing Capability

Reduce operational response requirements

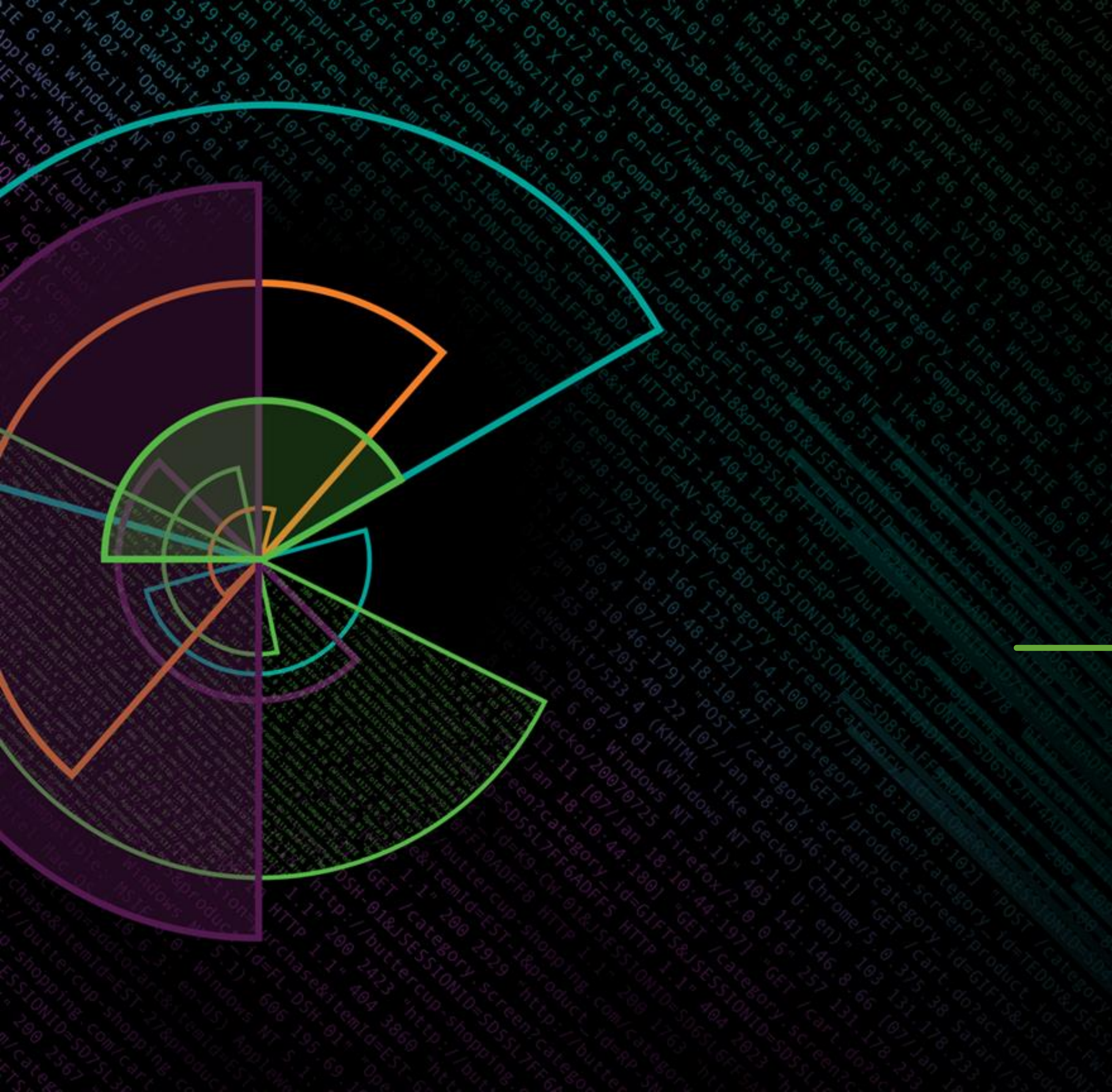
- Leverages automation built for scaling to restore nodes to a known good state
- Core focus on proactive over reactive operational responses
- Individual node failures no longer treated as pageable incidents
- Application or infrastructure failure reduced to a short predictable outage
- Failure of Self-Healing treated as incident



# Self-Service Portal

- Common tasks can be executed via RESTful APIs
- Application Management
- Portal backed by “API first” platform
- Integration to existing SAML presence
- Interactive roadmap based on customer requirements

BEAST



# BEAST Demo

splunk> .conf18

# The Outcomes

# Technical Impact

- 90+ unique apps in-use across user-base on GP Search Head Cluster
- ES and PCI installed on independent Search Head Cluster
- 320+ indexes cataloging data
- 2TB/day data ingestion rate and growing
- Indexing tier now 720 cores and 2.8 TB of RAM
- Regular patching and upgrades
- Zero downtime

# Business Impact

- Reduced storage cost of platform by 59%
- Increased confidence for expansion of Splunk integration and utilization with wider business
- Capacity for monitoring of hyper-scale critical systems including those used for the discovery of newly profitable routes (grid-compute)
- Enhanced security response capability with Splunk Enterprise Security Application

www.sourcedgroup.com

enquiries@sourcedgroup.com

# Thank You

**Don't forget to rate this session in the .conf18 mobile app**

.conf18

splunk>