

Introducing Splunk Mission Control

splunk> .conf19

.conf19

splunk>





Chris Simmons

Product Marketing Director | Splunk

Rob Truesdell

Sr. Director, Product Management | Splunk

© 2019 SPLUNK INC.

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.

Splunk, Splunk>, Listen to Your Data, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2019 Splunk Inc. All rights reserved.

© 2019 SPLUNK INC.

State of Security Operations



.conf19

splunk>

© 2019 SPLUNK INC.

State of Security Operations



Tools



Alerts



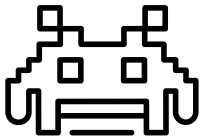
Hiring



Cost



Education



Adversaries



Techniques



Users & Devices

© 2019 SPLUNK INC.

Problems & Challenges

We've talked to a lot of people…

Operations



Tier 1
Security Analyst



Tier 2
Threat Response



Tier 3
Threat Response

Management



SOC Director



Chief Information
Security Officer

© 2019 SPLUNK INC.

Problems & Challenges

These were the common threads

- Lack of process
- Baby steps towards automation
- Too many tools
- Escalating to ticketing systems is arduous
- Increasing volume of events
- Speed of response time
- Human resource challenges
- Events lack context
- Difficulty tracking event lifecycle
- No common information model
- Content development is increasingly critical
- Products
- Static controls
- Costs

© 2019 SPLUNK INC.

Desired Outcomes

Ingest Any Data from Anywhere
Full data visibility

Predictive Analytics
Better detection

Machine Learning & Guidance
Faster response

Proactive Threat Hunting
Threat prevention

Testing Capabilities
Improved troubleshooting

Heavily Automated
Lower MTTR

Communication & ChatOps
Higher collaboration

Integrated Case Management
Full lifecycle visibility and tracking

Performance & Scalability
Faster response

Community Sharing
Improved Intel and process

Single Pane of Glass
Consolidated toolset

Process Workflows
Consistency and compliance

Immediate Situational Awareness
Full context

Robust Dashboards & Reporting
Tailored visibility

Immediate Proof of Value
Measurable success

© 2019 SPLUNK INC.

Atom Coffman

Manager of Cybersecurity Operations, Starbucks



.conf19

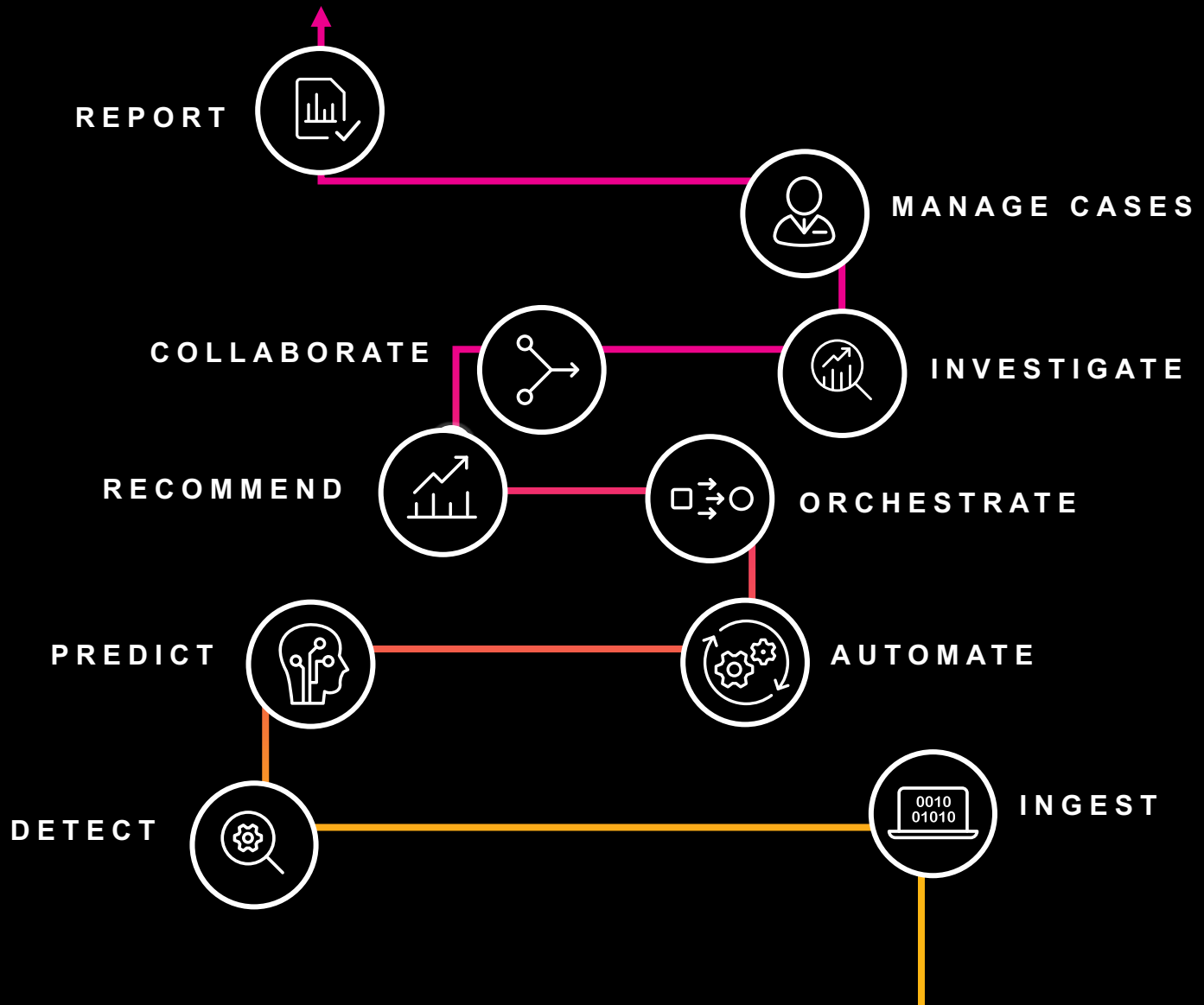
splunk>

© 2019 SPLUNK INC.

How Should We Do This?

© 2019 SPLUNK INC.

The Security Event Lifecycle



splunk> .conf19

© 2019 SPLUNK INC.

What is our Objective?



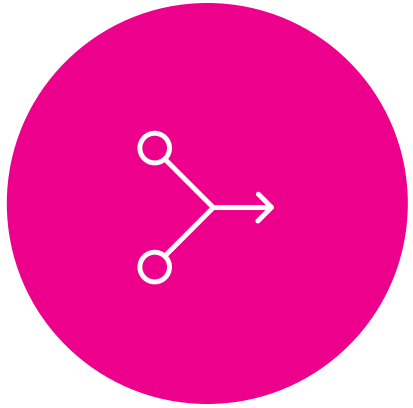
Change the way SecOps are managed



Prioritize the analyst experience first



Optimize for hybrid environments



Unify and simplify



Improve security effectiveness

Splunk Mission Control

A Modern, Cloud-Based, and Unified Security Operations Experience

- A new user experience for managing the entire **security operations event lifecycle** from a common work surface
- Detect, manage, investigate, hunt, contain, and remediate threats and other high-priority security issues



© 2019 SPLUNK INC.

Future Splunk Security Solution Architecture

Customer Delivery

Solutions

Applications

Platform

Data Sources

© 2019 SPLUNK INC.

Future Splunk Security Solution Architecture

Customer Delivery



Splunk Mission Control

User Control & Entry Point to SOC in Future

Solutions

Applications

Platform

Data Sources

© 2019 SPLUNK INC.

Future Splunk Security Solution Architecture

Customer Delivery

Solutions

Splunk Mission Control
User Control & Entry Point to SOC in Future

Applications

Splunk Enterprise Security™ + Splunk User Behavior Analytics™

Platform

Data Sources

© 2019 SPLUNK INC.

Future Splunk Security Solution Architecture

Customer Delivery

Solutions

Applications

Platform

Data Sources



© 2019 SPLUNK INC.

Future Splunk Security Solution Architecture

Customer Delivery

Solutions

Splunk Mission Control
User Control & Entry Point to SOC in Future

Applications

Splunk Enterprise Security™ + Splunk User Behavior Analytics™

splunk> phantom

Future Splunk Solutions

Platform

Data Sources

© 2019 SPLUNK INC.

Future Splunk Security Solution Architecture

Customer Delivery

Solutions

Applications

Platform

Data Sources



© 2019 SPLUNK INC.

Future Splunk Security Solution Architecture

Customer Delivery

Solutions

Splunk Mission Control
User Control & Entry Point to SOC in Future

Applications

Splunk Enterprise Security™ + Splunk User Behavior Analytics™

splunk> phantom

Future Splunk Solutions

3rd Party Plug-ins

Platform

splunk> Platform for Machine Data

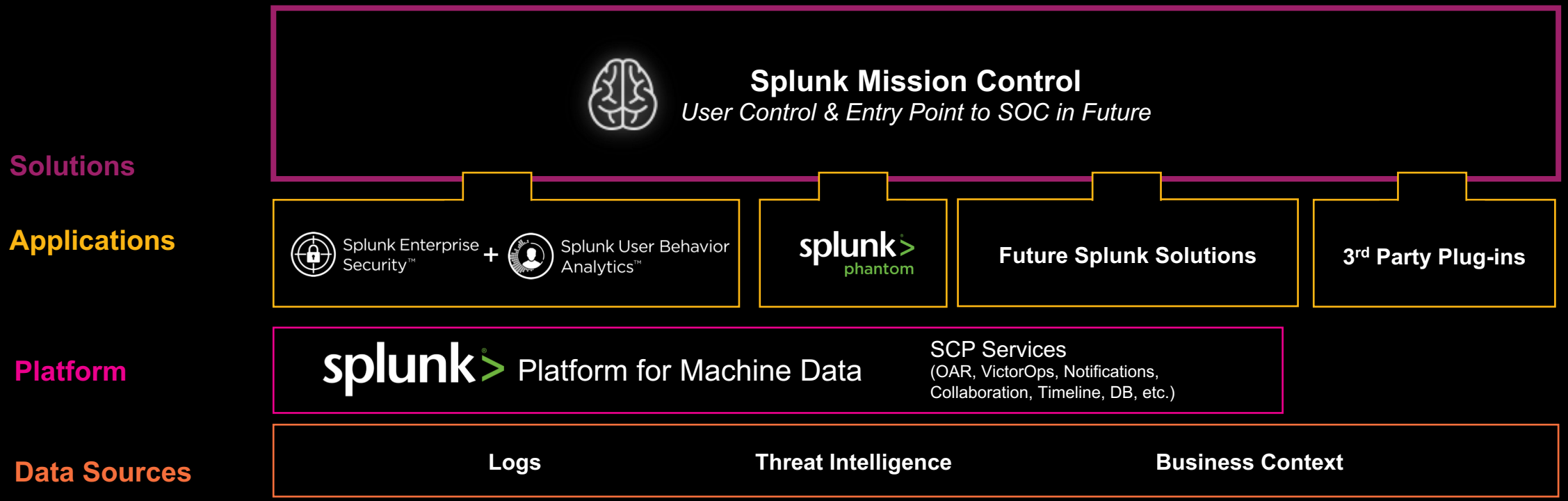
SCP Services
(OAR, VictorOps, Notifications, Collaboration, Timeline, DB, etc.)

Data Sources

© 2019 SPLUNK INC.

Future Splunk Security Solution Architecture

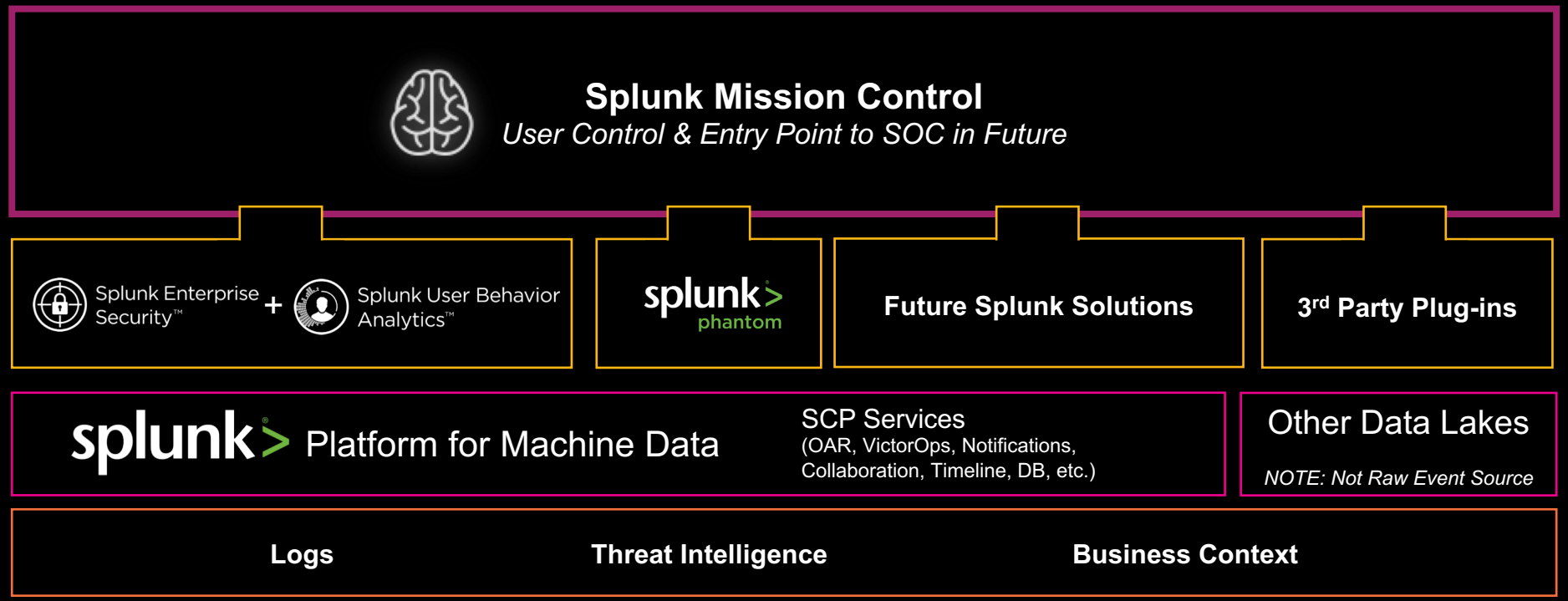
Customer Delivery



© 2019 SPLUNK INC.

Future Splunk Security Solution Architecture

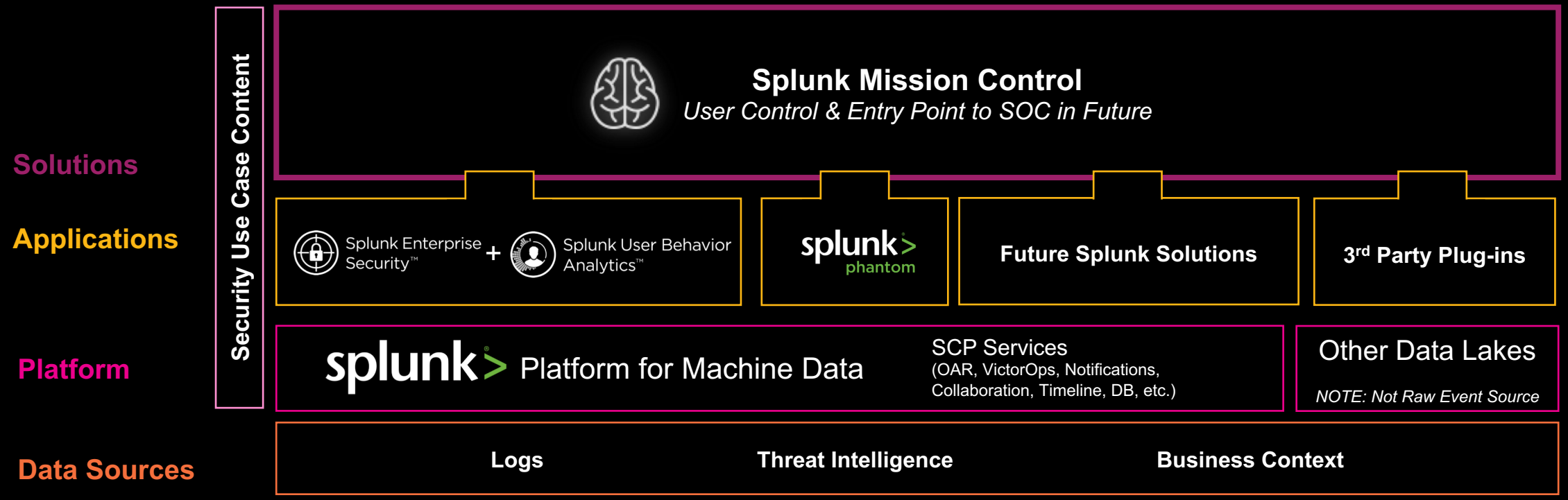
Customer Delivery



© 2019 SPLUNK INC.

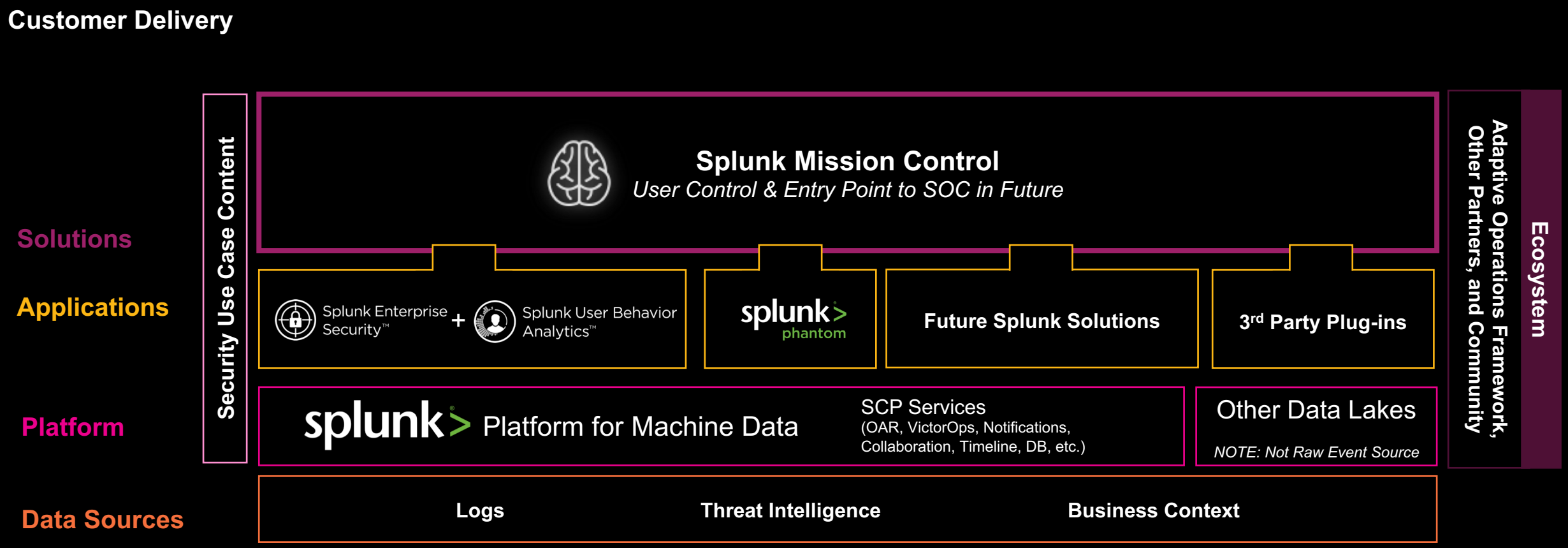
Future Splunk Security Solution Architecture

Customer Delivery



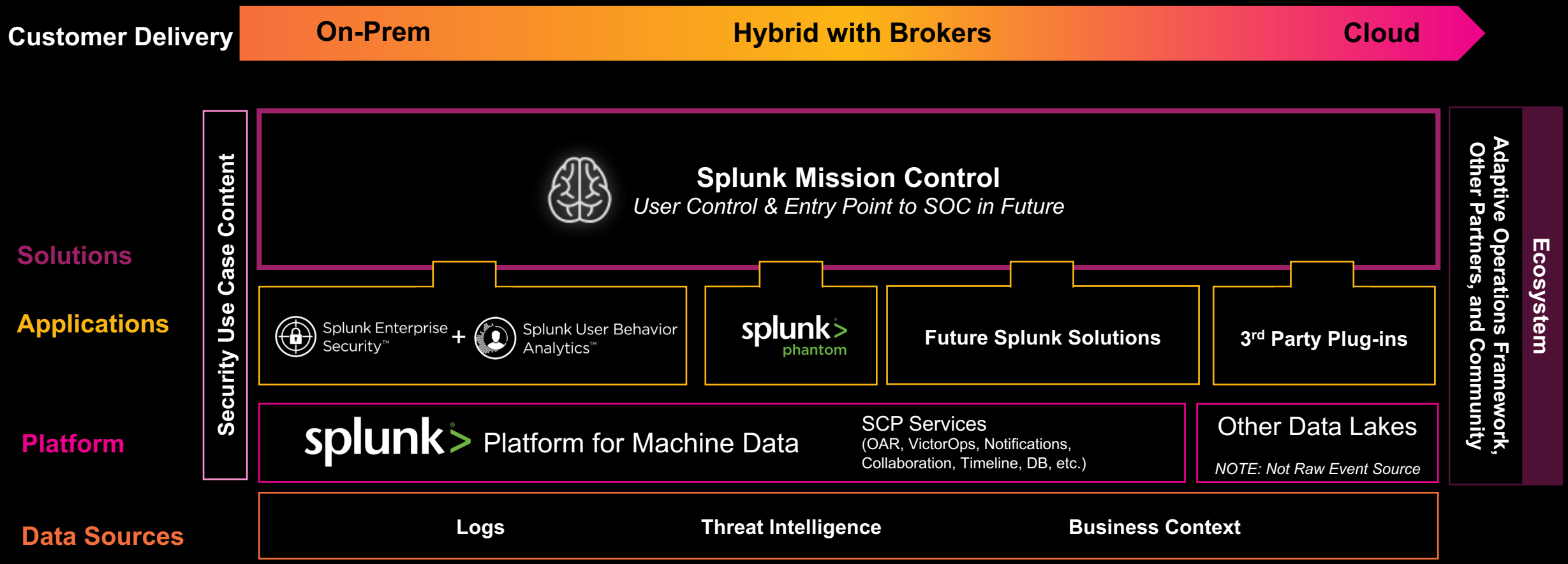
© 2019 SPLUNK INC.

Future Splunk Security Solution Architecture



© 2019 SPLUNK INC.

Future Splunk Security Solution Architecture



© 2019 SPLUNK INC.

Why Should You Care?

© 2019 SPLUNK INC.

Stand Up

© 2019 SPLUNK INC.

If You Are a CISO…

- **You're concerned about:**
  - Improving security posture through integration
  - Career success of your team
  - Reclamation of your personal time
  - Accelerating time-to-value

- **Splunk Mission Control enables you to:**
  - Monitor and manage Security Operations
  - Mature your team and its processes
  - Show ROI such as dwell time, cost savings, and MTTR

Please have a seat

© 2019 SPLUNK INC.

If You Are a SOC Manager or Director…

- **You're concerned about:**
  - Improving security posture through integration
  - Career success of your team
  - Reclamation of your personal time
  - Accelerating time-to-value

  PLUS
  - Driving efficiency and productivity
  - Retaining knowledge across your team
  - Augmenting knowledge of your junior staff

- **Splunk Mission Control enables you to:**
  - Monitor and manage Security Operations
  - Mature your team and its processes
  - Show ROI such as dwell time, cost savings, and MTTR

Please have a seat

© 2019 SPLUNK INC.

If You Are a Tier 1, 2, 3 Analyst…

- **You're concerned about:**
  - Efficiently triaging events / cases
  - "Swivel chair syndrome"
  - Situational awareness
  - Better collaboration

- **Splunk Mission Control enables you to:**
  - Focus by providing a single interface
  - Utilize better prescriptive guidance using playbooks
  - Focus on more challenging events and incidents
  - Collaborate with other SOC team members for better remediation

Please have a seat

© 2019 SPLUNK INC.

If You Are Anyone Else…

You should still care because…

Your data is likely being protected by the people that were standing before you!

© 2019 SPLUNK INC.

Benefits of Splunk Mission Control

Recover time spent performing repetitive actions manually

Integrated automation and orchestration allow you to recover time spent performing repetitive actions and execute playbooks at machine speed.

Improve precision, accuracy, and auditability of your response

Workbooks model an organization's security response plans and are essential to achieve complete, repeatable, and auditable security operations at scale.

Modernize and optimize your security operations

Detect, manage, investigate, hunt, contain, and remediate threats and other high-priority security issues across the entire event lifecycle—all from one common work surface.

© 2019 SPLUNK INC.

Mission Control Base

Foundational Capabilities to Manage Your SOC

- Notable event investigation (any data source)
- Notable management and triage
- Notable event investigation
- Search against Splunk Enterprise
- Artifact Actions
- CIM data mappings
- Dashboarding
- Reporting
- Collaboration
- Response Templates
- SLAs
- Application settings
- UI Extension framework

© 2019 SPLUNK INC.

Mission Control with Analytics

Advanced Detection and Visualization

- Notable event investigation (any data source)
- Notable management and triage
- Notable event investigation
- Search against Splunk Enterprise
- Artifact Actions
- CIM data mappings
- Dashboarding
- Reporting
- Collaboration
- Response Templates
- SLAs
- Application settings
- UI Extension framework

- Security Posture
- Artifact Info Service
- Entities Explorer (Assets & Identities)
- Threat Intel Framework
- ES Content Dashboards

Mission Control Analytics connects to an existing Splunk Enterprise Security Instance (on-prem or cloud)

© 2019 SPLUNK INC.

Mission Control with Automation

Streamline Execution of SOC Processes

- Notable event investigation (any data source)
- Notable management and triage
- Notable event investigation
- Search against Splunk Enterprise
- Artifact Actions
- CIM data mappings
- Dashboarding
- Reporting
- Collaboration
- Response Templates
- SLAs
- Application settings
- UI Extension framework

- Visual Playbook Editor
- Connector Configuration
- Manual & Automated Playbook Execution
- Automation Result Viewer

Mission Control with Automation brings key Phantom capabilities to cloud

© 2019 SPLUNK INC.

Mission Control + Analytics + Automation

Leverage the Full, Unified Security Operations Experience

- Notable event investigation (any data source)
- Notable management and triage
- Notable event investigation
- Search against Splunk Enterprise
- Artifact Actions
- CIM data mappings
- Dashboarding
- Reporting
- Collaboration
- Response Templates
- SLAs
- Application settings
- UI Extension framework

- Security Posture
- Artifact Info Service
- Entities Explorer (Assets & Identities)
- Threat Intel Framework
- ES Content Dashboards

- Visual Playbook Editor
- Connector Configuration
- Manual & Automated Playbook Execution
- Automation Result Viewer

Mission Control Analytics connects to an existing Splunk Enterprise Security Instance (on-prem or cloud)

Mission Control with Automation brings key Phantom capabilities to cloud

© 2019 SPLUNK INC.

Mission Control Base

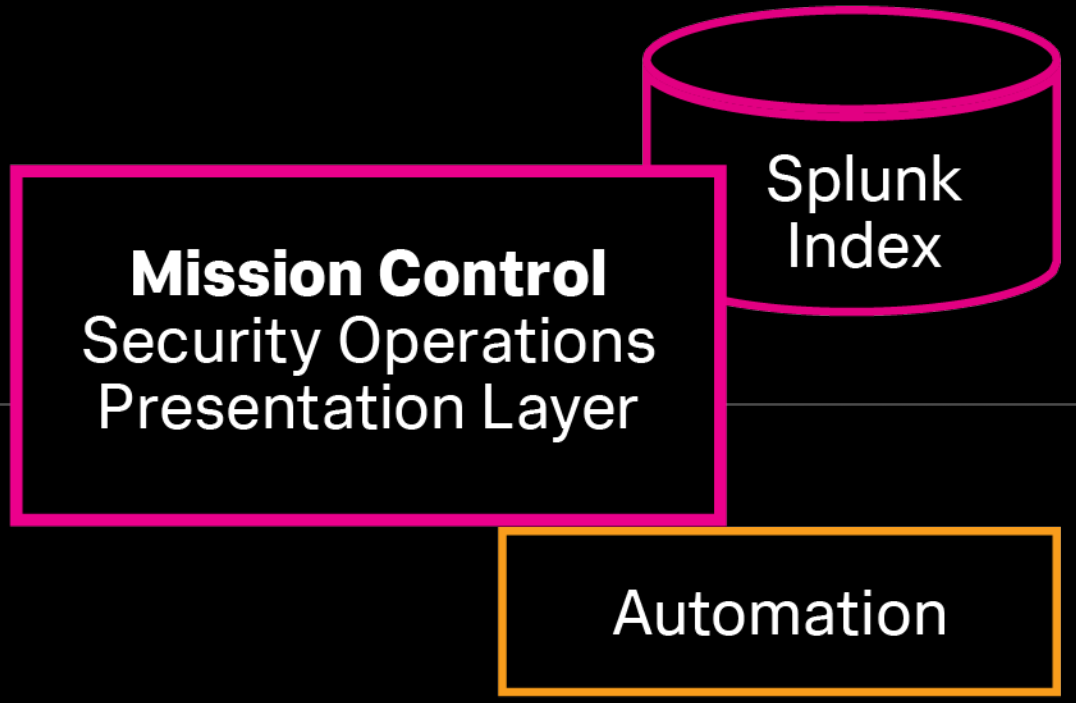
Foundational Capabilities to Manage Your SOC

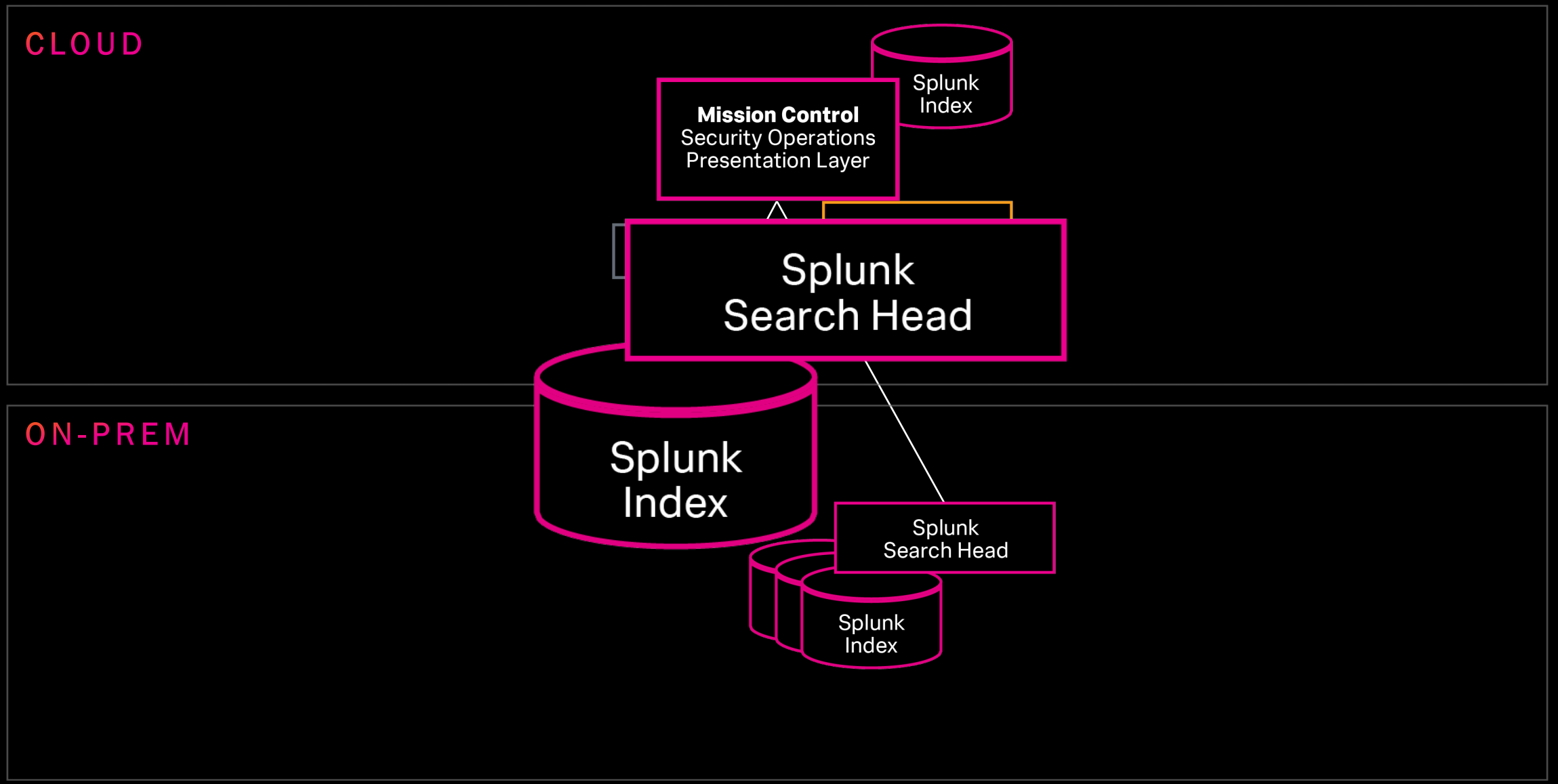
- Notable event investigation (any data source)
- Notable management and triage
- Notable event investigation
- Search against Splunk Enterprise
- Artifact Actions
- CIM data mappings
- Dashboarding
- Reporting
- Collaboration
- Response Templates
- SLAs
- Application settings
- UI Extension framework

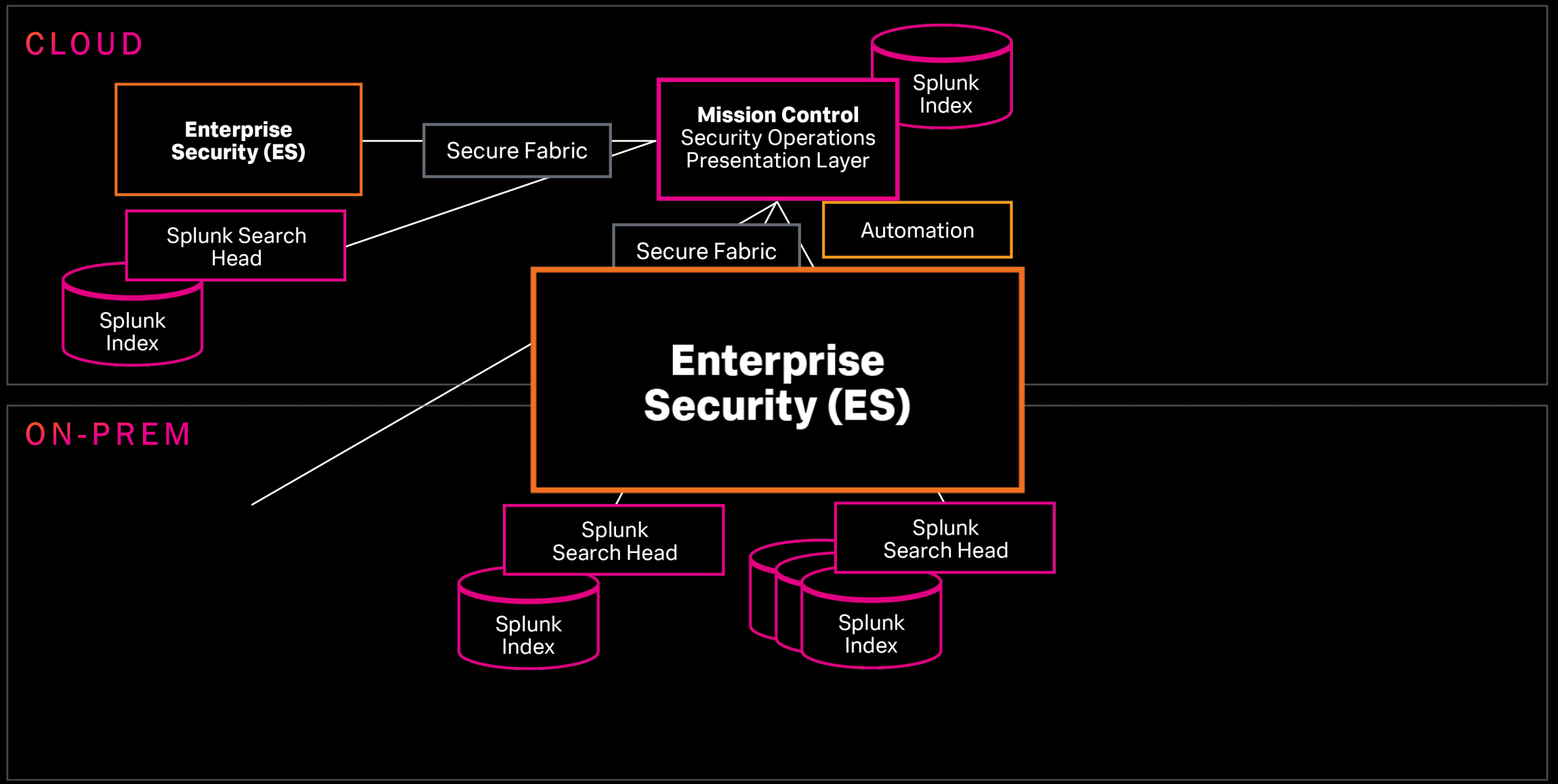
© 2019 SPLUNK INC.

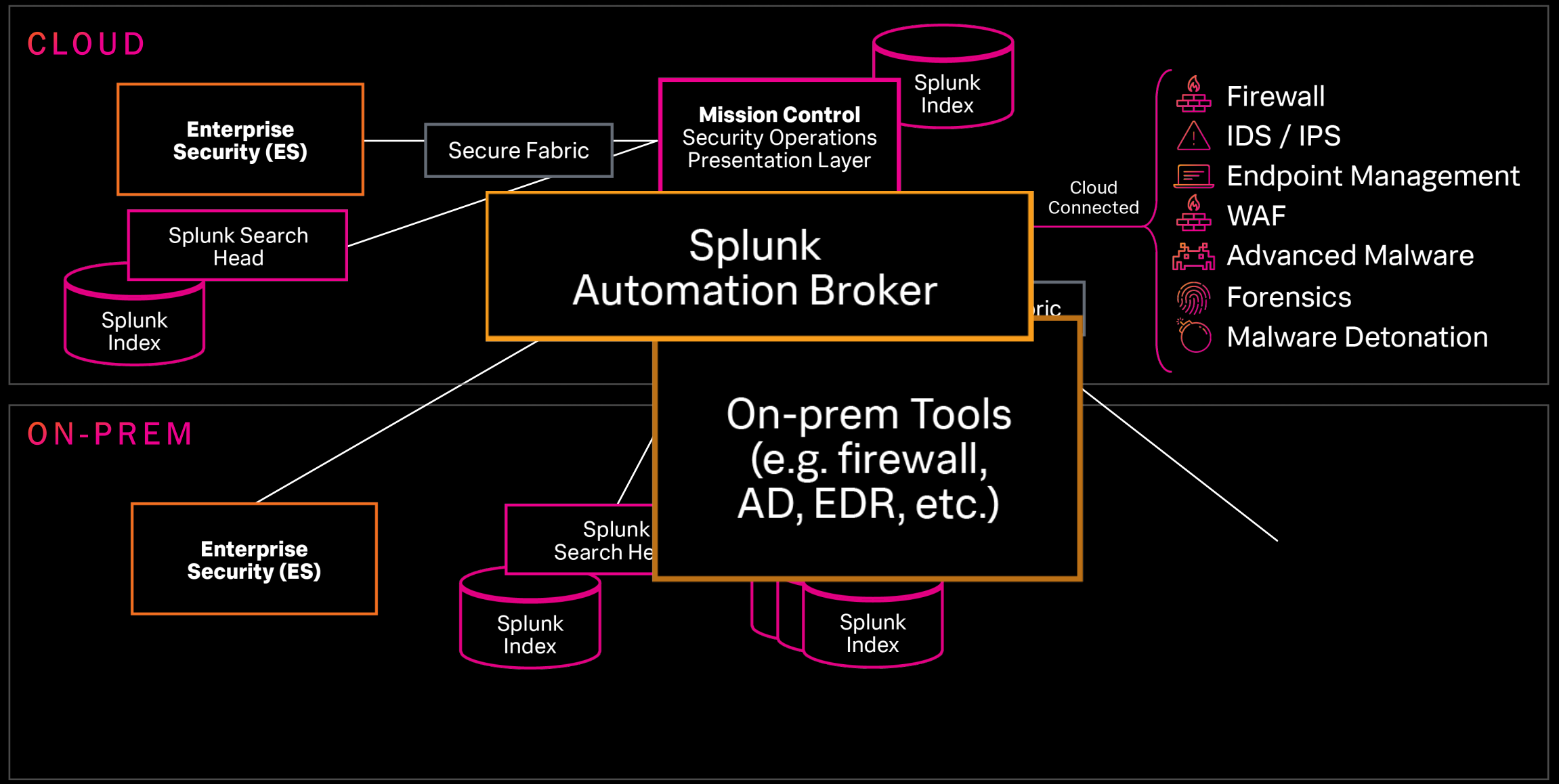
Architecture

CLOUD


Splunk
Index
Mission Control
Security Operations
Presentation Layer
Automation


CLOUD
Splunk Index
Mission Control
Security Operations
Presentation Layer
Splunk
Search Head
ON-PREM
Splunk
Index
Splunk
Search Head
Splunk
Index


CLOUD
Enterprise Security (ES)
Secure Fabric
Mission Control
Security Operations
Presentation Layer
Splunk Index
Splunk Search Head
Splunk Index
Secure Fabric
Automation
Enterprise Security (ES)
ON-PREM
Splunk Search Head
Splunk Index
Splunk Search Head
Splunk Index


CLOUD
Enterprise Security (ES)
Secure Fabric
Mission Control
Security Operations
Presentation Layer
Splunk Index
Splunk Search Head
Splunk Index
Splunk Automation Broker
Cloud Connected
Firewall
IDS / IPS
Endpoint Management
WAF
Advanced Malware
Forensics
Malware Detonation
ON-PREM
On-prem Tools (e.g. firewall, AD, EDR, etc.)
Enterprise Security (ES)
Splunk Search He
Splunk Index
Splunk Index

© 2019 SPLUNK INC.

What can you do?

Operations Use Cases



Tier 1
Security Analyst

Phishing Investigation

Threat Intelligence

Event Triage



Tier 2
Threat Response

Threat Hunting

Malware Investigation

Insider Threat



Tier 3
Threat Response

Management Use Cases



SOC Director

Team Performance

Process & Operations

Metrics & Reporting



Chief Information
Security Officer

© 2019 SPLUNK INC.

Key Takeaways

1. We're currently in Beta with Early Access Users
2. General Availability in the near future
3. For updates, sign-up here: splunk.com/mission-control

© 2019 SPLUNK INC.



splunk>

Thank You!

Go to the .conf19 mobile app to

RATE THIS SESSION