.conf18

splunk>

Taming GDI: The Wild World of "Getting Data Into" Splunk

Peter Chen, Principal Software Engineer
Blaine Wastell, Director Product Management

October 2018 | Version 1.0

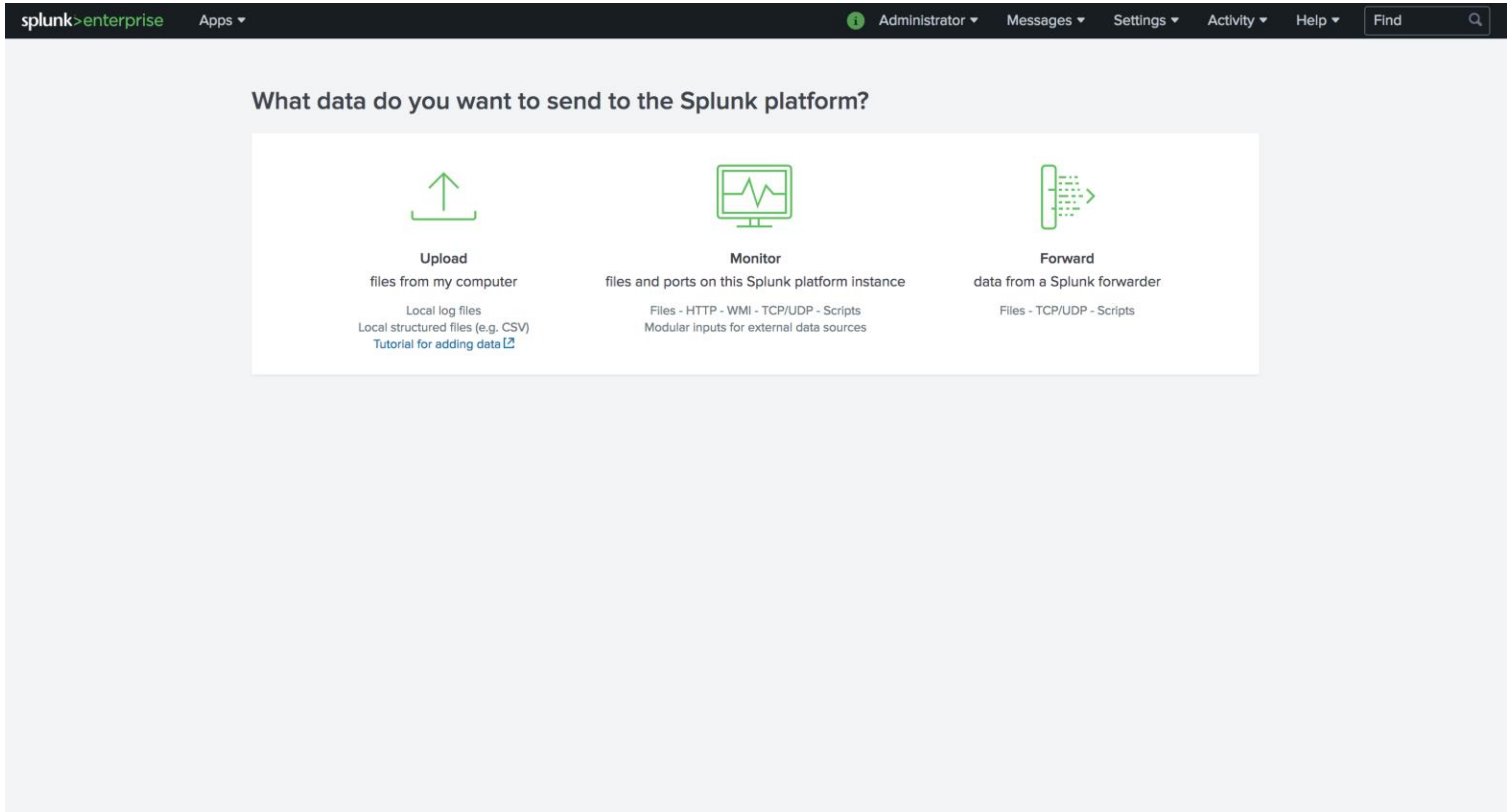
Forward-Looking Statements

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.

Current Add Data Screen

- How do I Ingest
- Windows Events or Linux Logs
- AWS CloudWatch Logs
- AWS CloudWatch Events
- Firewall Syslogs?



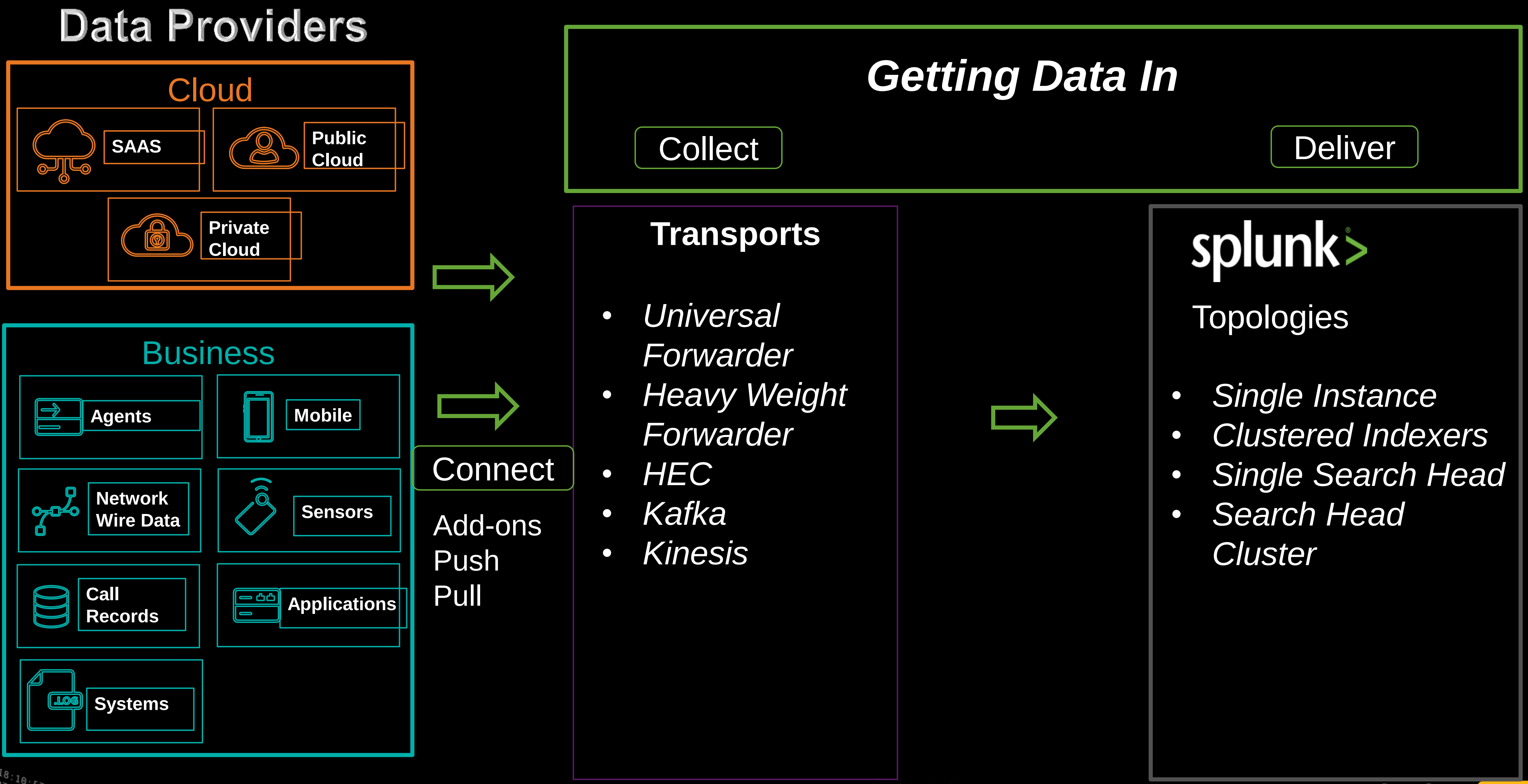
What data do you want to send to the Splunk platform?

Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

Forward
data from a Splunk forwarder
Files - TCP/UDP - Scripts

Data Collection Options



Data Providers

Cloud

- SAAS
- Public Cloud
- Private Cloud

Business

- Agents
- Mobile
- Network Wire Data
- Sensors
- Call Records
- Applications
- Systems

Getting Data In

Collect

Deliver

Connect

Add-ons
Push
Pull

Transports

- *Universal Forwarder*
- *Heavy Weight Forwarder*
- *HEC*
- *Kafka*
- *Kinesis*

splunk>

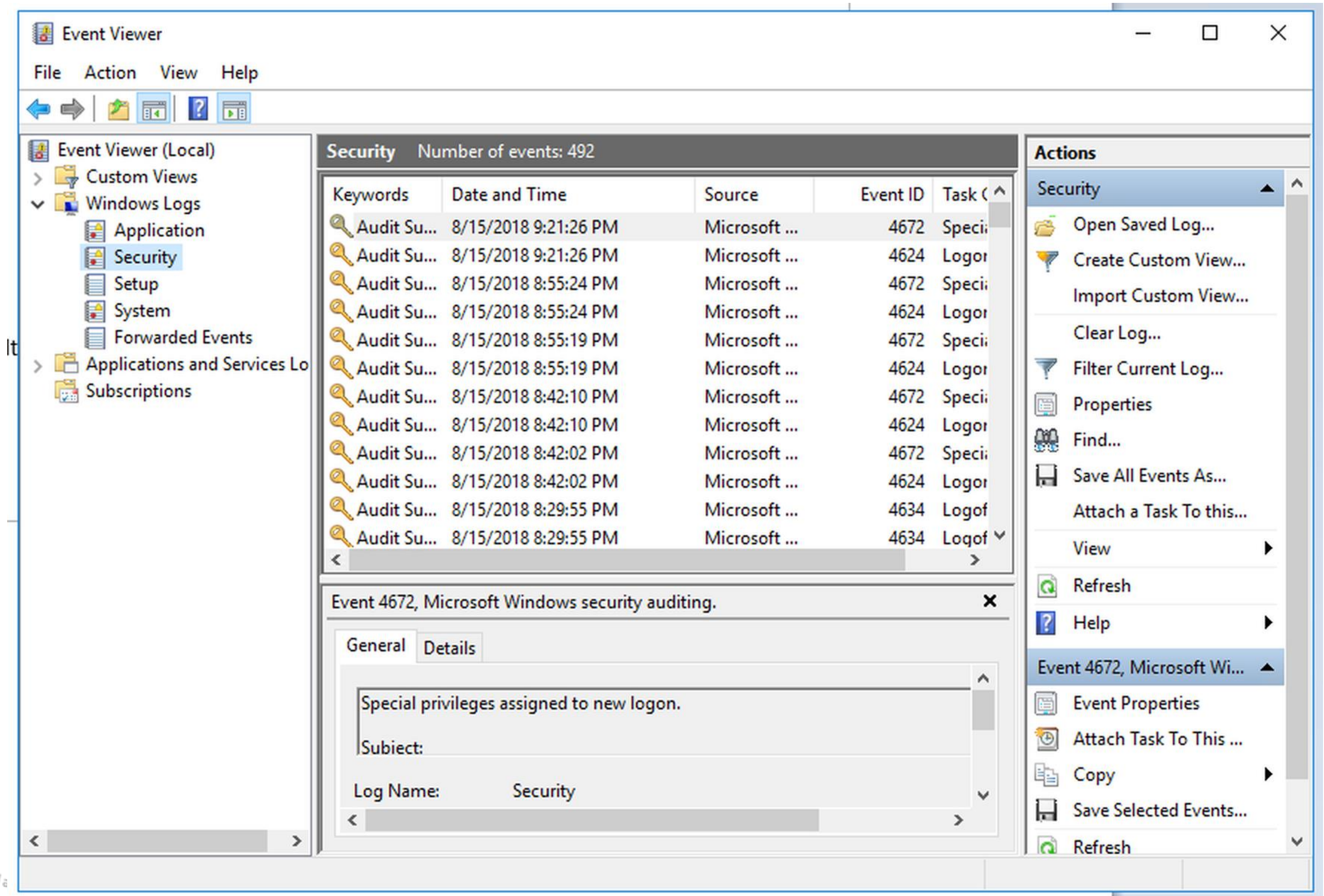
Topologies

- *Single Instance*
- *Clustered Indexers*
- *Single Search Head*
- *Search Head Cluster*

Collect Windows Events or Linux Logs

Windows Logs

- Universal Forward



Security Number of events: 492

Keywords	Date and Time	Source	Event ID	Task (
Audit Su...	8/15/2018 9:21:26 PM	Microsoft ...	4672	Speci
Audit Su...	8/15/2018 9:21:26 PM	Microsoft ...	4624	Logor
Audit Su...	8/15/2018 8:55:24 PM	Microsoft ...	4672	Speci
Audit Su...	8/15/2018 8:55:24 PM	Microsoft ...	4624	Logor
Audit Su...	8/15/2018 8:55:19 PM	Microsoft ...	4672	Speci
Audit Su...	8/15/2018 8:55:19 PM	Microsoft ...	4624	Logor
Audit Su...	8/15/2018 8:42:10 PM	Microsoft ...	4672	Speci
Audit Su...	8/15/2018 8:42:10 PM	Microsoft ...	4624	Logor
Audit Su...	8/15/2018 8:42:02 PM	Microsoft ...	4672	Speci
Audit Su...	8/15/2018 8:42:02 PM	Microsoft ...	4624	Logor
Audit Su...	8/15/2018 8:29:55 PM	Microsoft ...	4634	Logof
Audit Su...	8/15/2018 8:29:55 PM	Microsoft ...	4634	Logof

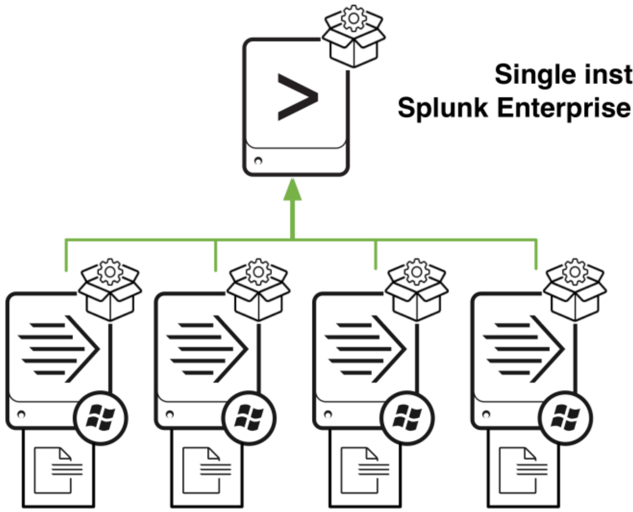
Event 4672, Microsoft Windows security auditing.

General Details

Special privileges assigned to new logon.

Subject:

Log Name: Security

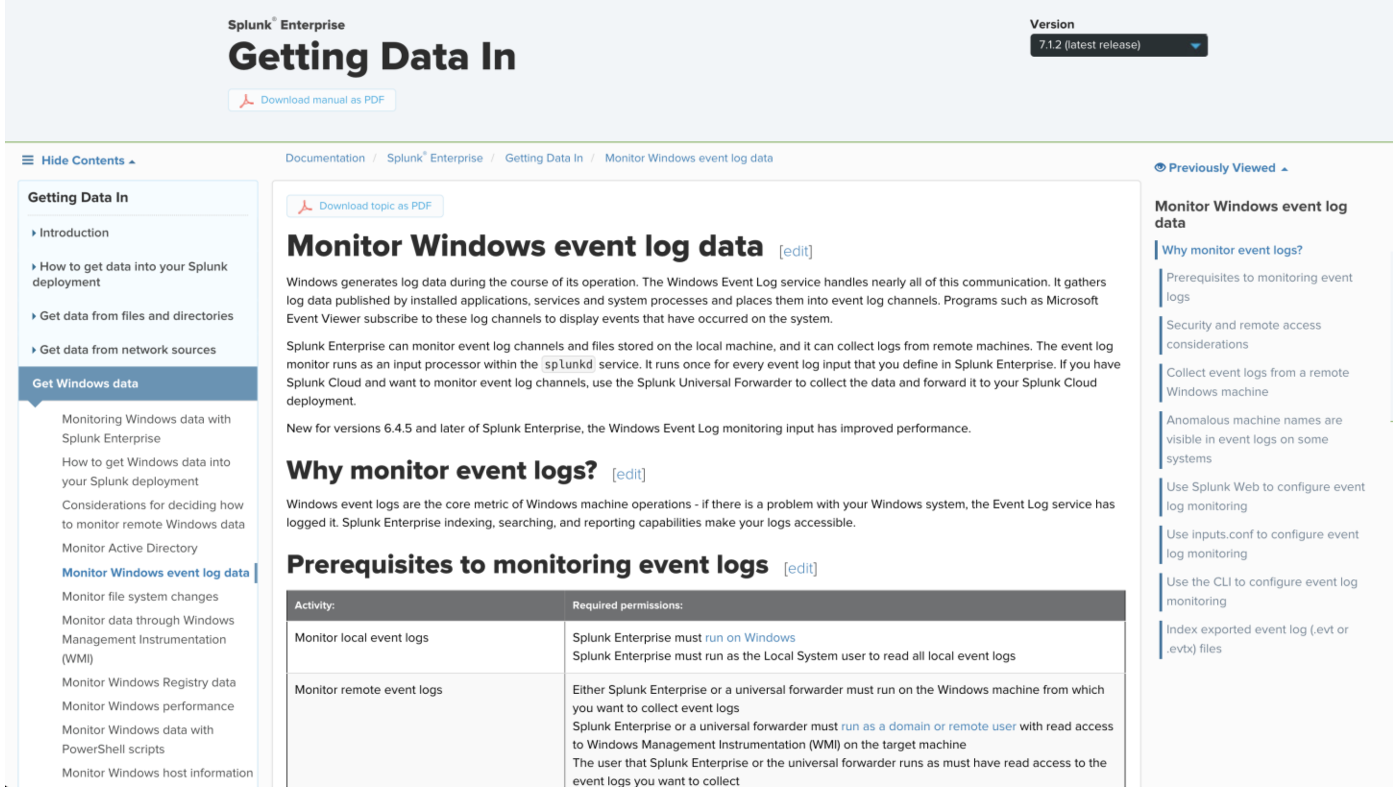


Single instance Splunk Enterprise deployment

Splunk Universal Forwarders on Microsoft Windows servers

Windows Logs

- Universal Forward



Splunk® Enterprise

Getting Data In

Download manual as PDF

Version 7.1.2 (latest release)

Hide Contents ▴

Documentation / Splunk® Enterprise / Getting Data In / Monitor Windows event log data

Getting Data In

- Introduction
- How to get data into your Splunk deployment
- Get data from files and directories
- Get data from network sources
- **Get Windows data**
  - Monitoring Windows data with Splunk Enterprise
  - How to get Windows data into your Splunk deployment
  - Considerations for deciding how to monitor remote Windows data
  - Monitor Active Directory
  - **Monitor Windows event log data**
  - Monitor file system changes
  - Monitor data through Windows Management Instrumentation (WMI)
  - Monitor Windows Registry data
  - Monitor Windows performance
  - Monitor Windows data with PowerShell scripts
  - Monitor Windows host information

Download topic as PDF

Monitor Windows event log data [edit]

Windows generates log data during the course of its operation. The Windows Event Log service handles nearly all of this communication. It gathers log data published by installed applications, services and system processes and places them into event log channels. Programs such as Microsoft Event Viewer subscribe to these log channels to display events that have occurred on the system.

Splunk Enterprise can monitor event log channels and files stored on the local machine, and it can collect logs from remote machines. The event log monitor runs as an input processor within the `splunkd` service. It runs once for every event log input that you define in Splunk Enterprise. If you have Splunk Cloud and want to monitor event log channels, use the Splunk Universal Forwarder to collect the data and forward it to your Splunk Cloud deployment.

New for versions 6.4.5 and later of Splunk Enterprise, the Windows Event Log monitoring input has improved performance.

Why monitor event logs? [edit]

Windows event logs are the core metric of Windows machine operations - if there is a problem with your Windows system, the Event Log service has logged it. Splunk Enterprise indexing, searching, and reporting capabilities make your logs accessible.

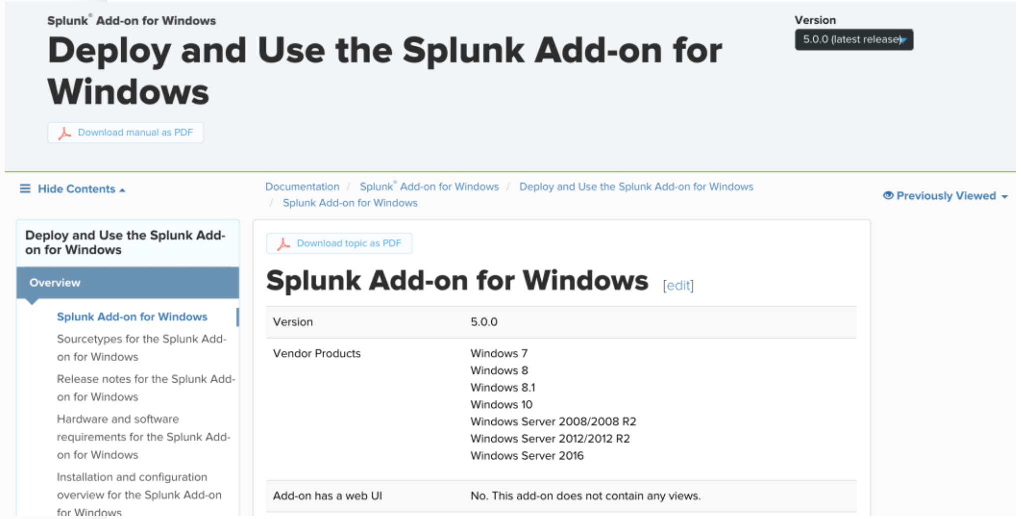
Prerequisites to monitoring event logs [edit]

Activity:	Required permissions:
Monitor local event logs	Splunk Enterprise must run on Windows Splunk Enterprise must run as the Local System user to read all local event logs
Monitor remote event logs	Either Splunk Enterprise or a universal forwarder must run on the Windows machine from which you want to collect event logs Splunk Enterprise or a universal forwarder must run as a domain or remote user with read access to Windows Management Instrumentation (WMI) on the target machine The user that Splunk Enterprise or the universal forwarder runs as must have read access to the event logs you want to collect

Previously Viewed ▴

Monitor Windows event log data

- Why monitor event logs?
- Prerequisites to monitoring event logs
- Security and remote access considerations
- Collect event logs from a remote Windows machine
- Anomalous machine names are visible in event logs on some systems
- Use Splunk Web to configure event log monitoring
- Use inputs.conf to configure event log monitoring
- Use the CLI to configure event log monitoring
- Index exported event log (.evt or .evtx) files



Splunk® Add-on for Windows

Deploy and Use the Splunk Add-on for Windows

Download manual as PDF

Version 5.0.0 (latest release)

Hide Contents ▴

Documentation / Splunk® Add-on for Windows / Deploy and Use the Splunk Add-on for Windows / Splunk Add-on for Windows

Previously Viewed ▾

Deploy and Use the Splunk Add-on for Windows

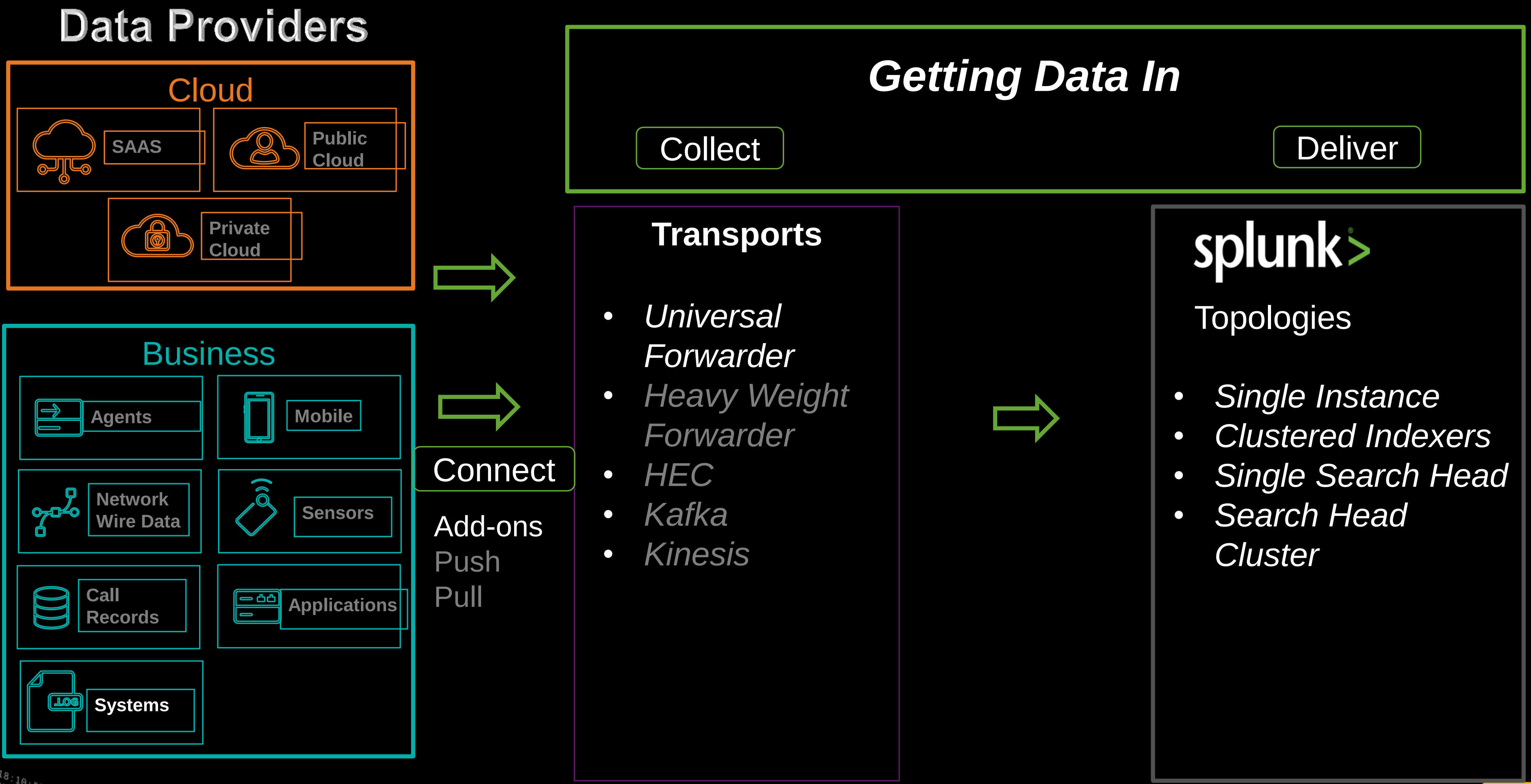
- **Overview**
  - Splunk Add-on for Windows
  - Sourcetypes for the Splunk Add-on for Windows
  - Release notes for the Splunk Add-on for Windows
  - Hardware and software requirements for the Splunk Add-on for Windows
  - Installation and configuration overview for the Splunk Add-on for Windows

Download topic as PDF

Splunk Add-on for Windows [edit]

Version	5.0.0
Vendor Products	Windows 7 Windows 8 Windows 8.1 Windows 10 Windows Server 2008/2008 R2 Windows Server 2012/2012 R2 Windows Server 2016
Add-on has a web UI	No. This add-on does not contain any views.

Collect Linux Logs & Windows Events



Data Providers

Cloud

- SAAS
- Public Cloud
- Private Cloud

Business

- Agents
- Mobile
- Network Wire Data
- Sensors
- Call Records
- Applications
- Systems

Connect

Add-ons
Push
Pull

Getting Data In

Collect

Deliver

Transports

- *Universal Forwarder*
- *Heavy Weight Forwarder*
- *HEC*
- *Kafka*
- *Kinesis*

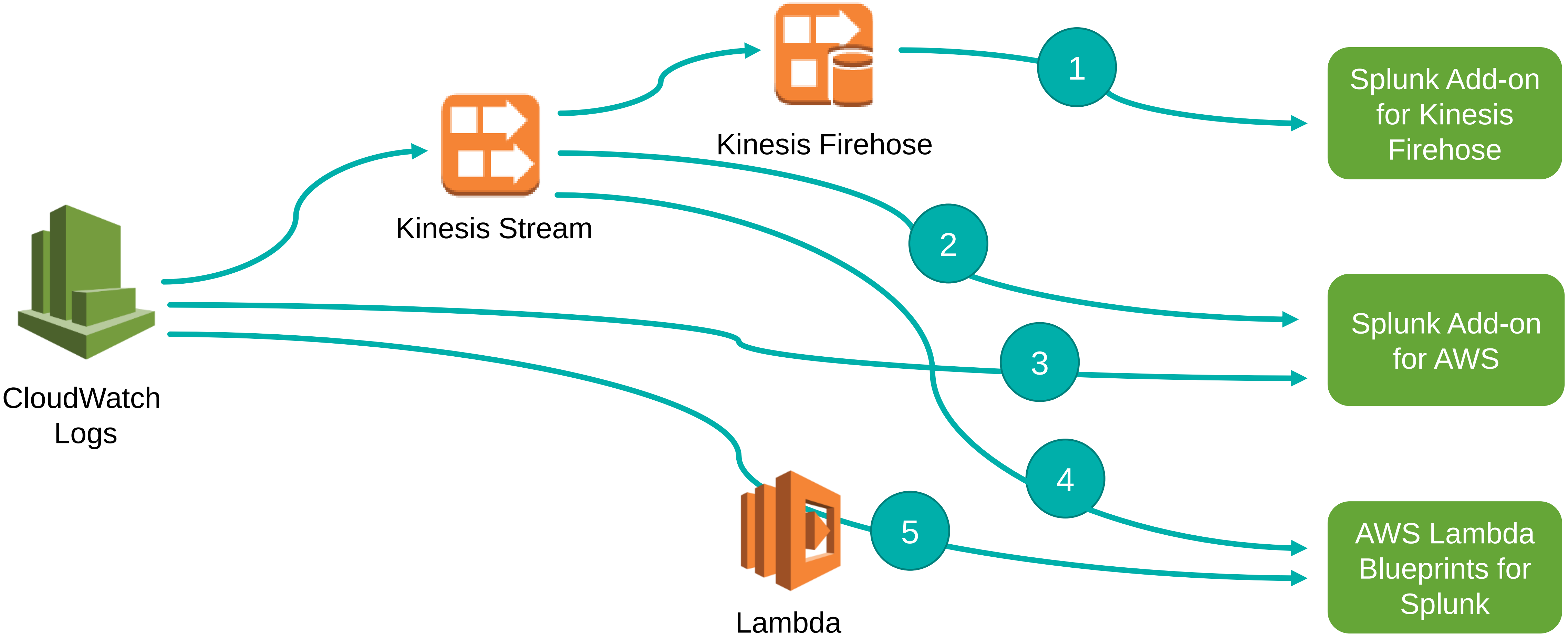
splunk>

Topologies

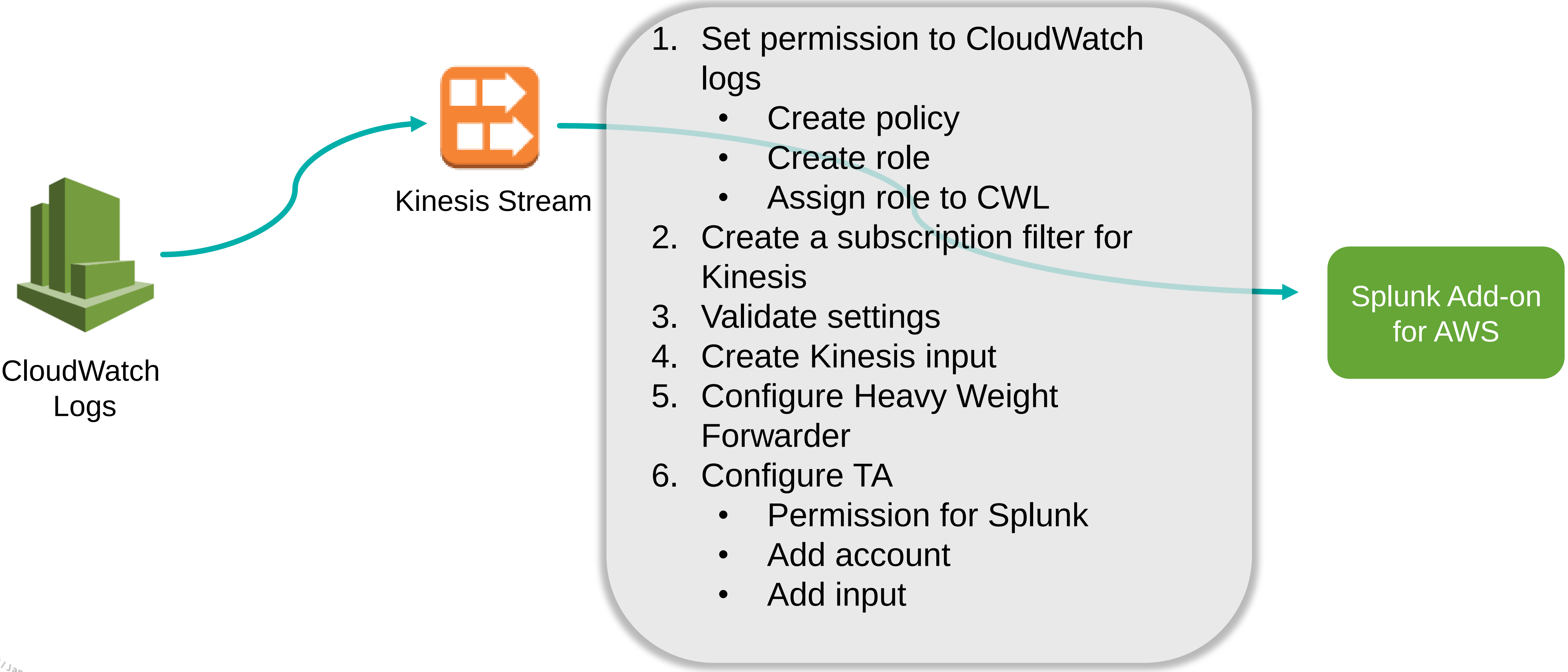
- *Single Instance*
- *Clustered Indexers*
- *Single Search Head*
- *Search Head Cluster*

Collect AWS Cloud Watch Logs

AWS CloudWatch Logs

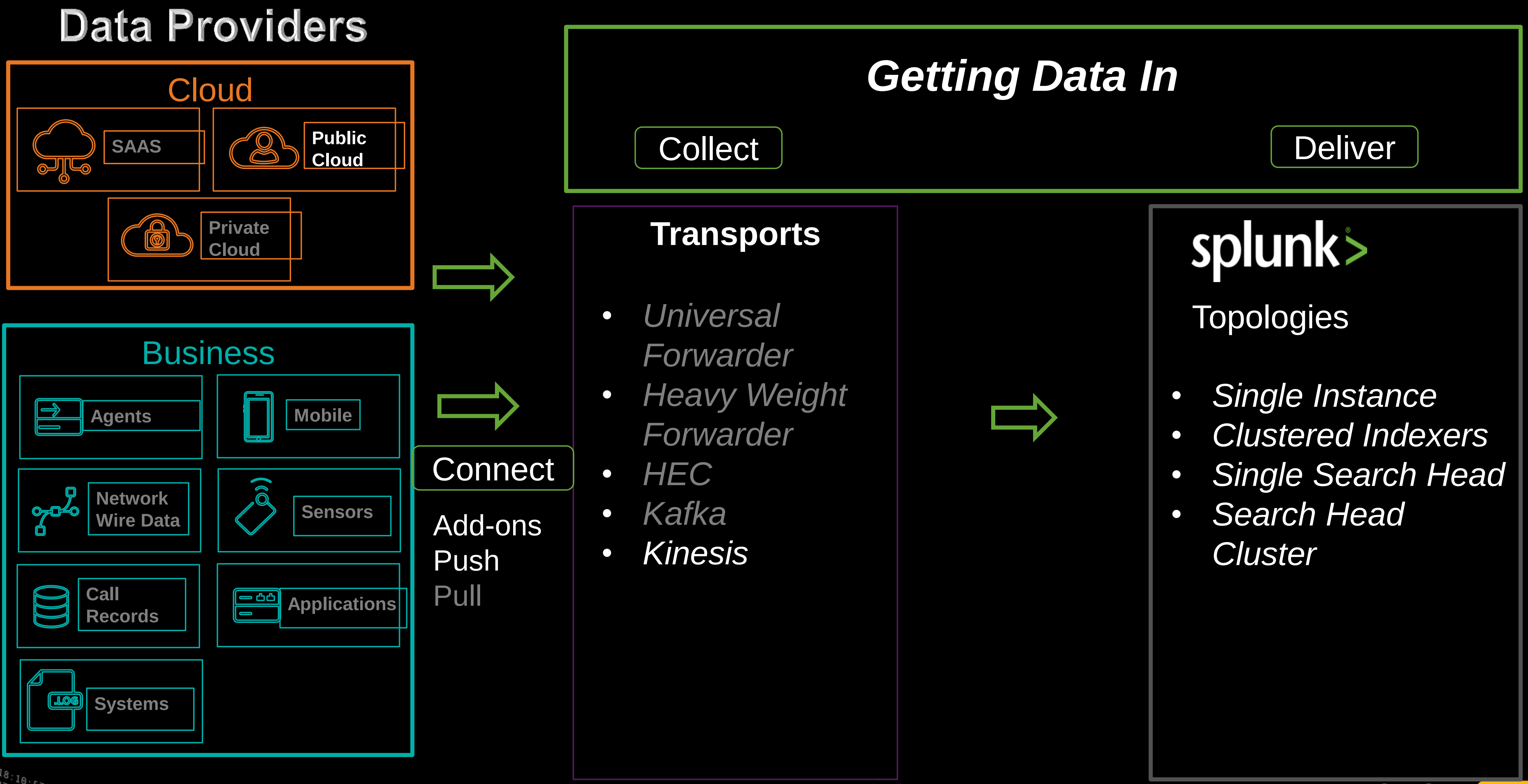


AWS CloudWatch Logs



1. Set permission to CloudWatch logs
   - Create policy
   - Create role
   - Assign role to CWL
2. Create a subscription filter for Kinesis
3. Validate settings
4. Create Kinesis input
5. Configure Heavy Weight Forwarder
6. Configure TA
   - Permission for Splunk
   - Add account
   - Add input

Collect AWS CloudWatch Logs



Data Providers

Cloud
- SAAS
- Public Cloud
- Private Cloud

Business
- Agents
- Mobile
- Network Wire Data
- Sensors
- Call Records
- Applications
- Systems

Connect

Add-ons
Push
Pull

Getting Data In

Collect

Deliver

Transports

- *Universal Forwarder*
- *Heavy Weight Forwarder*
- *HEC*
- *Kafka*
- *Kinesis*

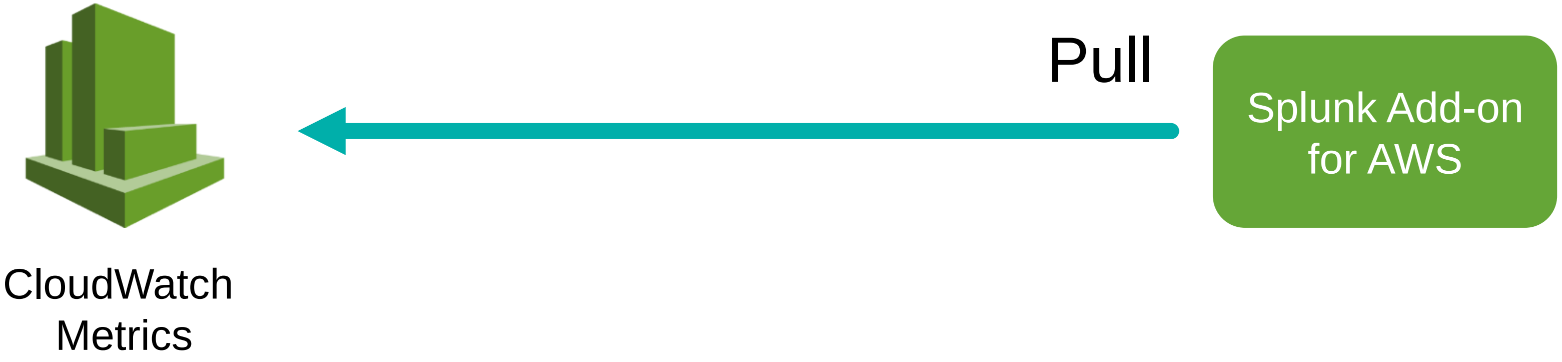
splunk>

Topologies

- *Single Instance*
- *Clustered Indexers*
- *Single Search Head*
- *Search Head Cluster*

Collect CloudWatch Metrics or Azure Events

AWS CloudWatch Metrics

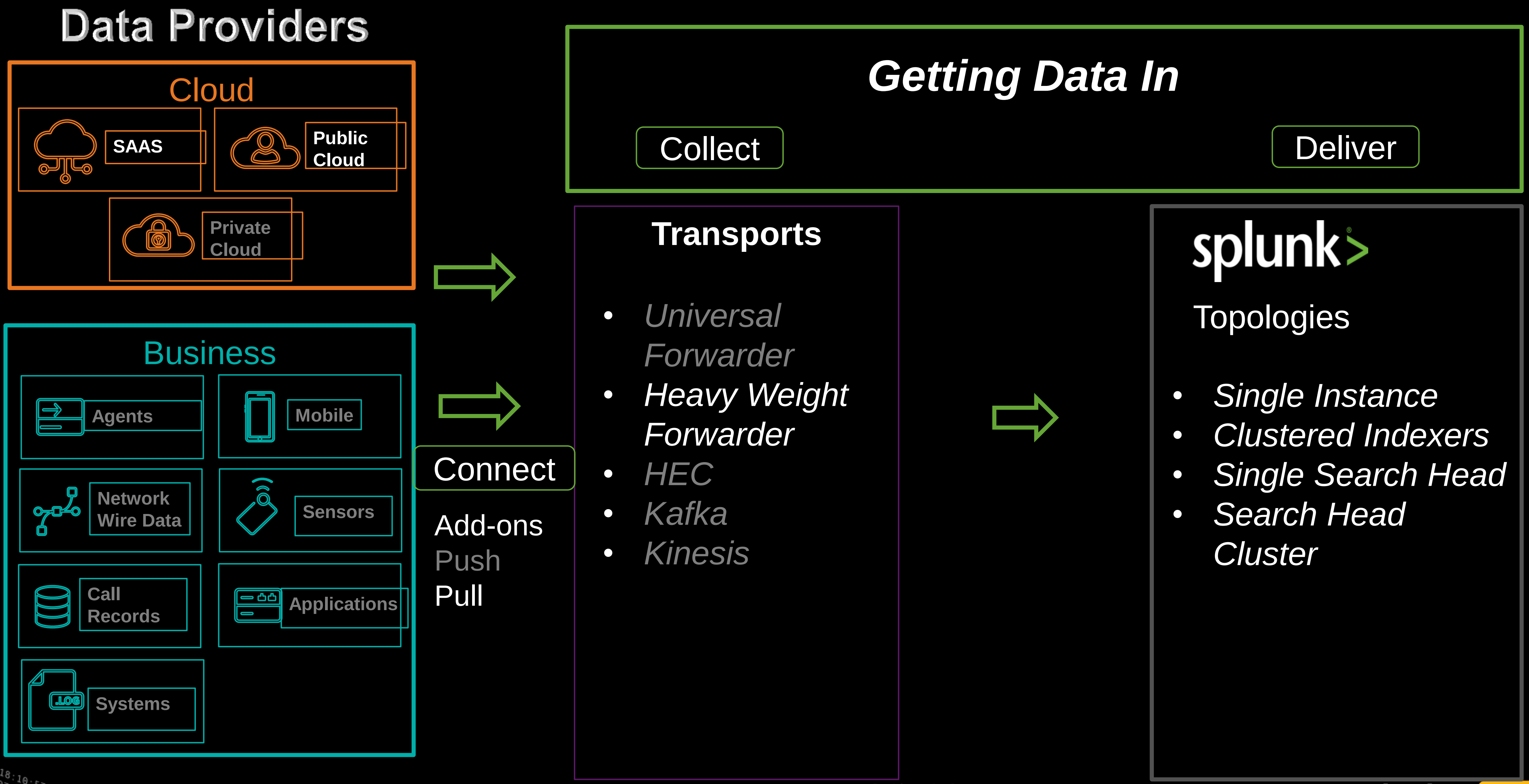


Pull

Splunk Add-on for AWS

CloudWatch Metrics

Collect AWS CloudWatch Metrics / Azure Logs / Service Now



Data Providers

Cloud
- SAAS
- Public Cloud
- Private Cloud

Business
- Agents
- Mobile
- Network Wire Data
- Sensors
- Call Records
- Applications
- Systems

Getting Data In

Collect

Deliver

Connect

Add-ons

Push

Pull

Transports

- *Universal Forwarder*
- *Heavy Weight Forwarder*
- *HEC*
- *Kafka*
- *Kinesis*

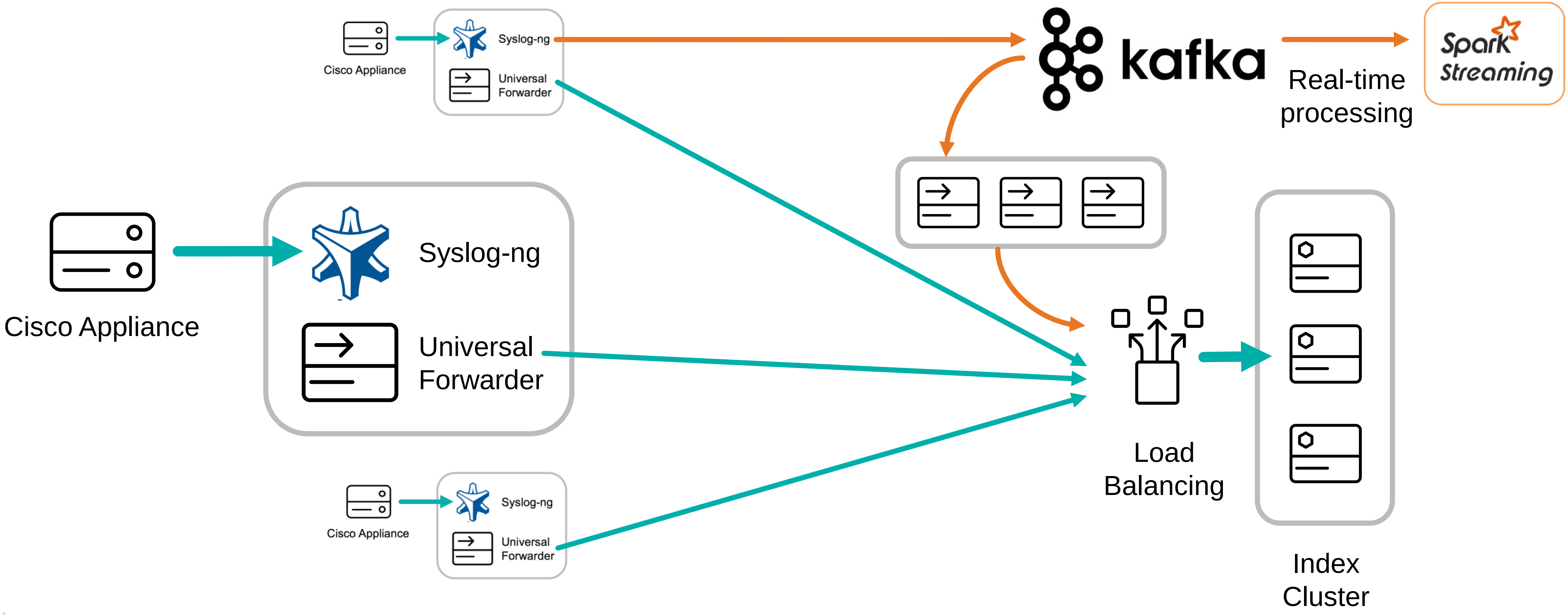
splunk>

Topologies

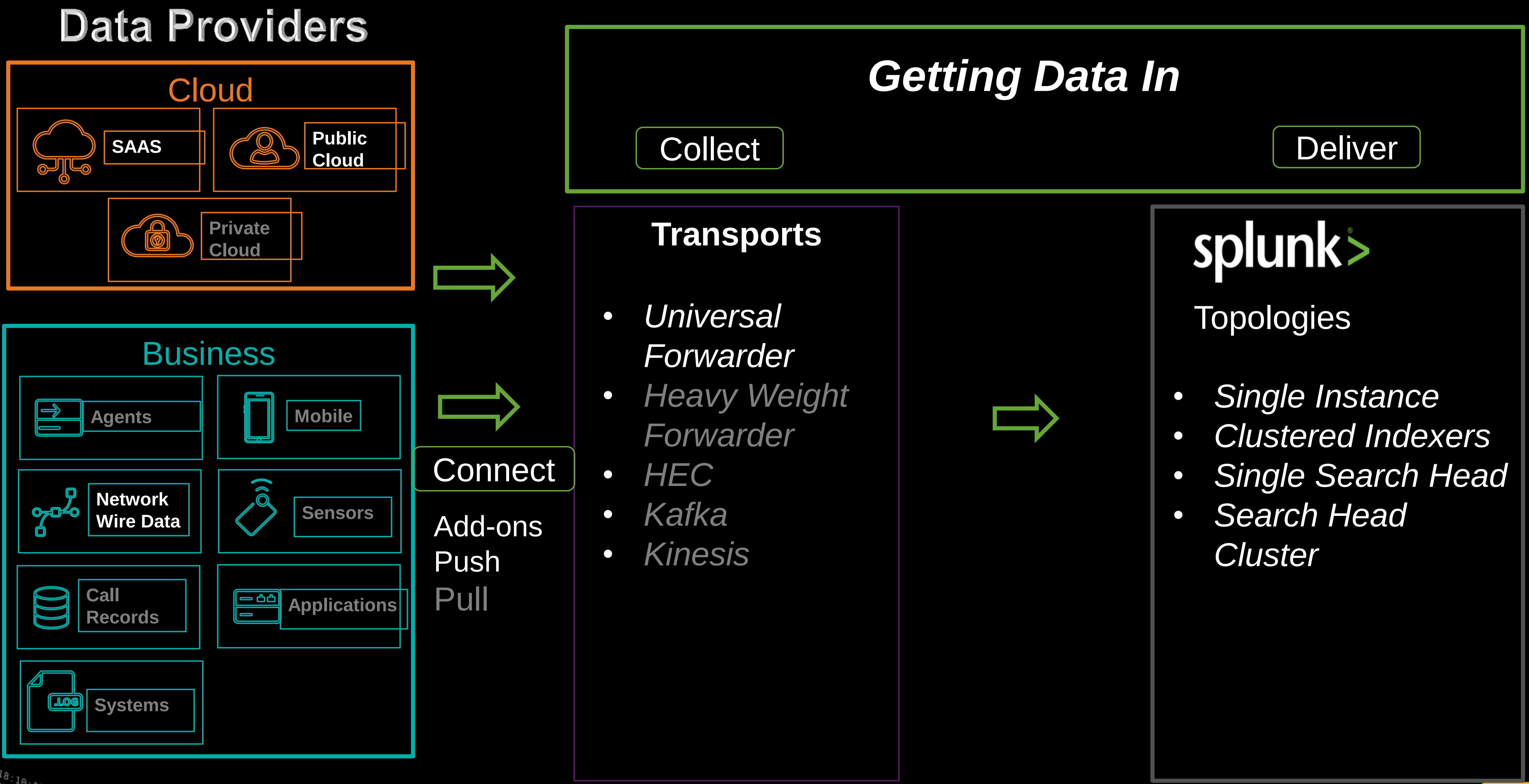
- *Single Instance*
- *Clustered Indexers*
- *Single Search Head*
- *Search Head Cluster*

Collect Firewall Syslog

Cisco Firewall Syslog Data



Collect Cisco ASA Syslogs



Data Providers

Cloud

- SAAS
- Public Cloud
- Private Cloud

Business

- Agents
- Mobile
- Network Wire Data
- Sensors
- Call Records
- Applications
- Systems

Getting Data In

Collect

Deliver

Connect

Add-ons
Push
Pull

Transports

- *Universal Forwarder*
- *Heavy Weight Forwarder*
- *HEC*
- *Kafka*
- *Kinesis*

splunk>

Topologies

- *Single Instance*
- *Clustered Indexers*
- *Single Search Head*
- *Search Head Cluster*

Top Customer Challenges for Data Collection

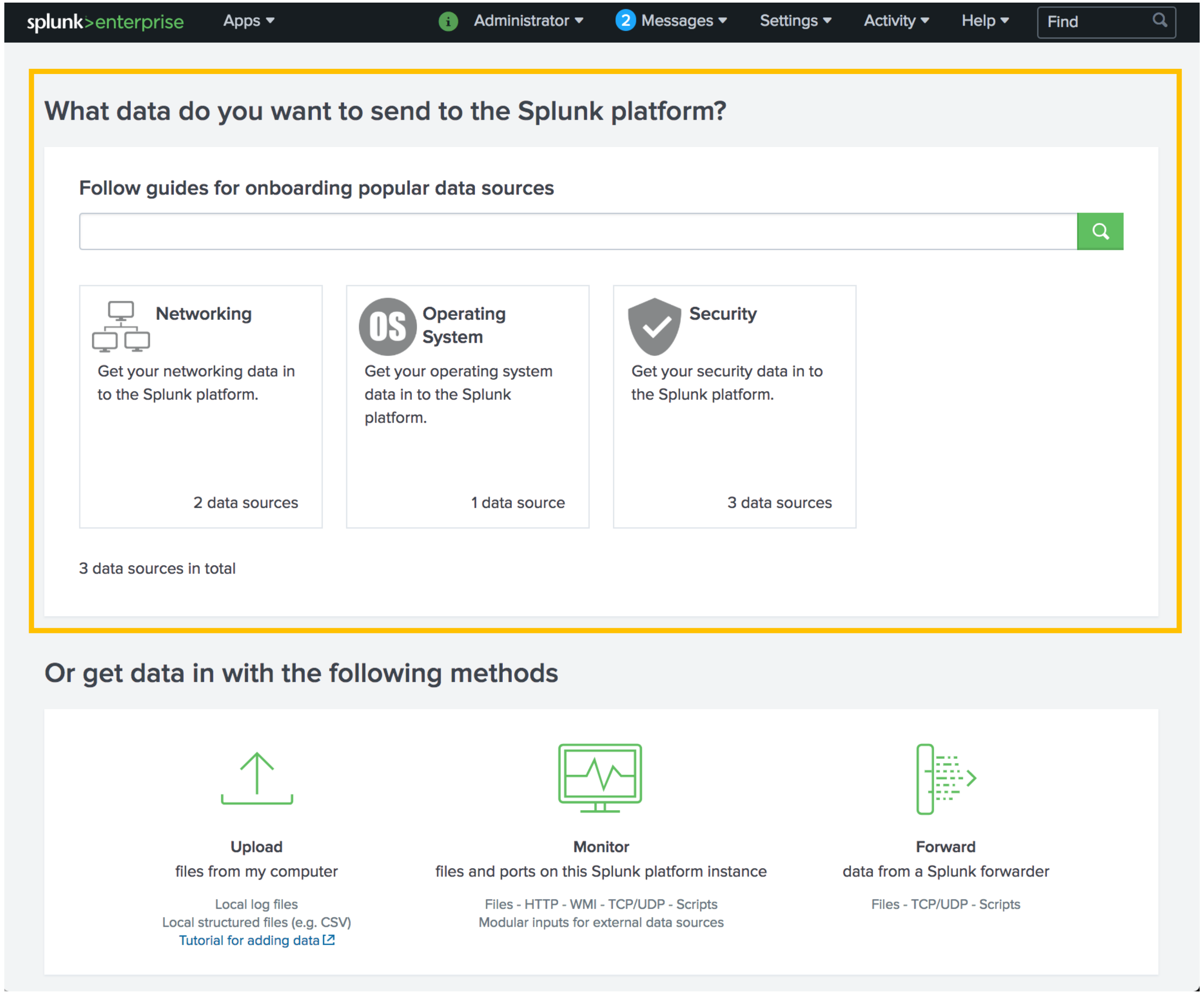
Survey from .conf 2017

1. Ability to monitor health of the data transfer lifecycle
2. Managing components on the edge is challenging
3. Would like to Iterate on the data flow and see what’s happening each step of the way
4. Data quality challenges creating inconsistent experiences for users
5. Keeping up with and responding to data drift which impacts #4
6. **Knowing which data to get and how to get that data in is challenging**

Announcing Guided Data Onboarding

New Add Data Screen

How do I Ingest Windows Logs, AWS Cloud Metrics, AWS CloudWatch Events, Firewall Logs?



What data do you want to send to the Splunk platform?

Follow guides for onboarding popular data sources

Networking
Get your networking data in to the Splunk platform.
2 data sources

Operating System
Get your operating system data in to the Splunk platform.
1 data source

Security
Get your security data in to the Splunk platform.
3 data sources

3 data sources in total

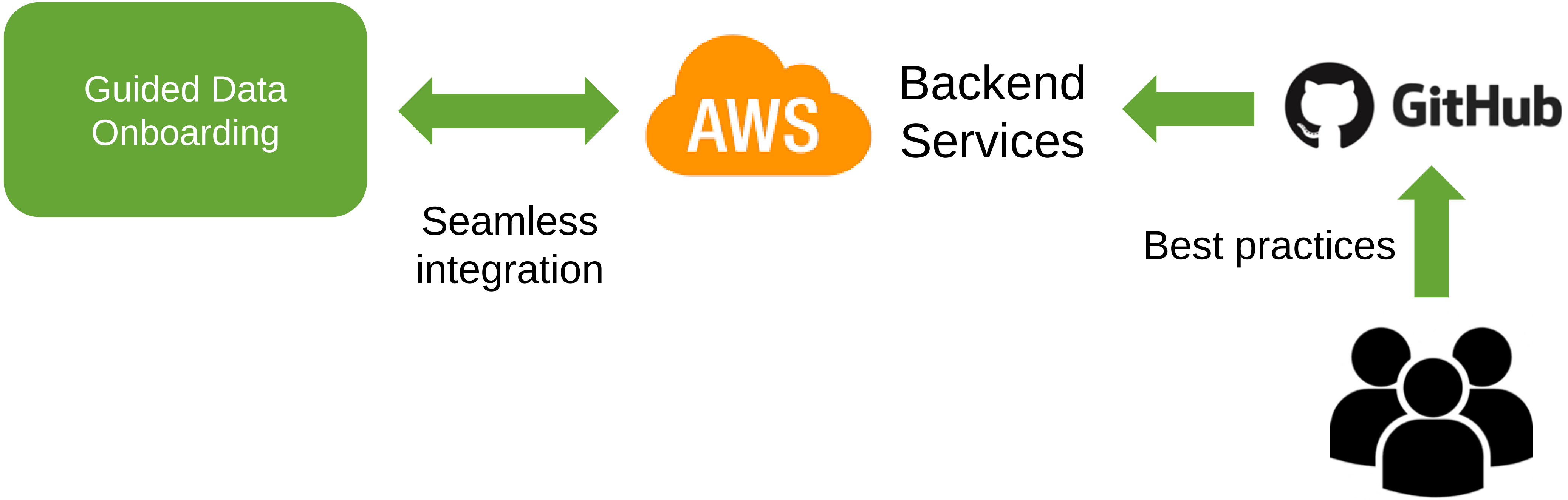
Or get data in with the following methods

Upload
files from my computer
Local log files
Local structured files (e.g. CSV)
Tutorial for adding data

Monitor
files and ports on this Splunk platform instance
Files - HTTP - WMI - TCP/UDP - Scripts
Modular inputs for external data sources

Forward
data from a Splunk forwarder
Files - TCP/UDP - Scripts

Demo of Guided Data Onboarding



Guided Data Onboarding

Seamless integration

Backend Services

Best practices

Doc writer, Professional Services,
3rd party contributor

Guided Data Onboarding Demo

Presented by Peter Chen

splunk> .conf18

Key Takeaways

- New Guided Data Onboarding: setup and configuration guidance for ingesting data into Splunk
- More data sources to come

Data Ingestion Sessions

Tuesday	2:15 – 3:00	FN1913 - Old Meets New: Syslog and Splunk Connect for Kafka	**Scott Haskell**, Principal SE Architect, Splunk **Mark Bonsack** Staff Sales Engineer, Splunk
	2:15 – 3:00	FN1313 – Taming GDI: The Wild World of “Getting Data Into” Splunk	**Peter Chen**, Principal Software Engineer, Splunk **Blaine Wastell**, Product Management Director, Splunk
Wednesday	3:15 – 4:00	FN1185 - Unleashing Data Ingestion From Apache Kafka	**Scott Haskell**, Principal SE Architect, Splunk **Donald Tregonning,** Senior Software Engineer, Splunk **Sharon Xie**, Software Engineer, Splunk
	3:15 – 4:00	IT1647 - A Container Adventure: Scaling and Monitoring Kubernetes Logging Infrastructure	**Matthew Modestino**, ITOA Practitioner, Splunk **David Baldwin**, Principal Product Manager, Splunk **Gimi Liang,** Senior Software Engineer, Splunk
	4:30 – 5:15	FN1211 - Don't Miss the Bus — Splunking Kafka at Scale	**Scott Haskell**, Principal SE Architect, Splunk **Ken Chen**, Principal Software Engineer, Splunk **Donald Tregonning,** Senior Software Engineer, Splunk
	4:30 – 5:15	FN1919 - Gain Control of Your Data Flow Using Stream Processing	**Thor Taylor**, Director of Product Management, Splunk **Joey Echeverria**, Senior Principal Software Engineer, Splunk
	4:30 – 5:15	IT1402 - Using Splunk to Increase Developer Confidence in the Pivotal Cloud Foundry Platform	**Kirk Hanson,** Sales Engineer, Splunk **Ram Gogineni,** Senior Manager – Cloud Operations, Charles Schwab **Shubham Jain,** Software Engineer, Splunk
Thursday	12:15 – 1:00	FN1729 - Splunk DB Connect Deep Dive: Beyond the Basics	**Denis Vergnes**, Principal Software Engineer, Splunk **Tyler Muth**, Analytics Architect, Splunk

Q&A

Peter Chen

Blaine Wastell

Making machine data accessible, usable and valuable to everyone.

Thank You

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

.conf18 splunk>