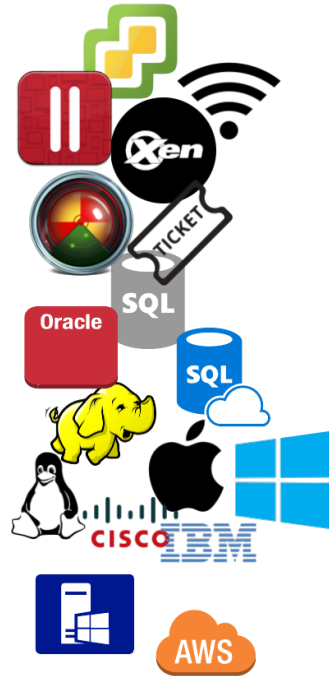
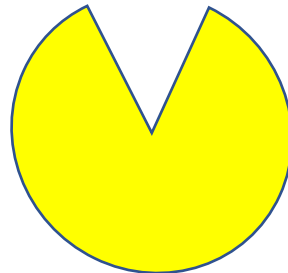


How Splunk Consumes Data >

- Virtual Machines
- Physical Machines
- Servers
- IoT
- Communications



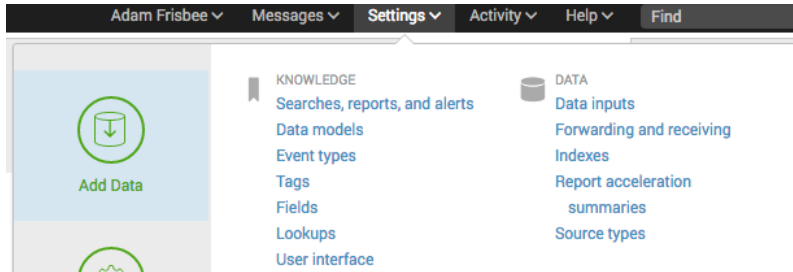
- Logs
- Configurations
- Scripts
- Tickets
- Alerts



How Splunk Consumes Data >

- Upload files
- Monitor files and directories
 - Local and remote
- SYSLOG
 - UDP or TCP
 - Local and remote
- SNMP (port udp:162)
- Scripted inputs from APIs

How Splunk Consumes Data >



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 indexer

Files - WMI - TCP/UDP - Scripts
Modular inputs for external data sources



forward

data from Splunk forwarder

Files - TCP/UDP - Scripts

How Splunk Consumes Data >

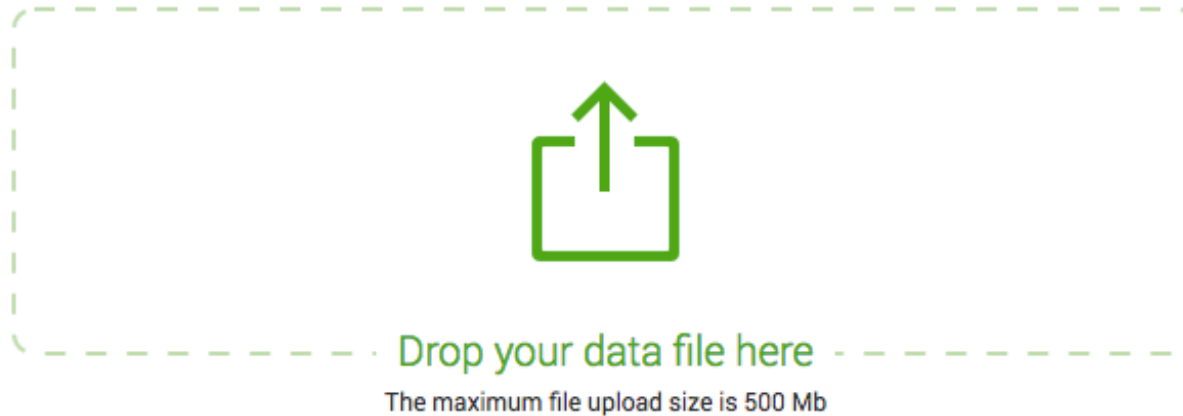


Select Source

Choose a file to upload to Splunk, either by browsing your computer or by dropping a file into the target box below. [Learn More](#)

Selected File: **No file selected**

Select File



How Splunk Consumes Data >



Add Data —●—

Select Source Input Settings Review

Local Event Logs
Collect event logs from this machine.

Remote Event Logs
Collect event logs from remote hosts. Note: this uses WMI and requires a domain account.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure Splunk to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Remote Performance Monitoring
Collect performance and event information from remote hosts. Requires domain credentials.

Registry monitoring
Have Splunk index the local Windows Registry, and monitor it for changes.

Active Directory monitoring
Index and monitor Active Directory.

Local Windows host monitoring
Collect up-to-date hardware and software (Computer, Operating System, Processor, Service, Disk, Network Adapter and Application) information about this machine.

Local Windows network monitoring
This is an input for Splunk Network Monitor.

- To monitor files and directories, Splunk needs to know what type of data to expect
- Apps and add-ons expand the list with more specific data types (Active Directory, VMware, etc.)

How Splunk Consumes Data >




forward

data from Splunk forwarder

Files - TCP/UDP - Scripts

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#) 

Select Server Class

New

Existing

Available host(s)

[add all »](#)

Selected host(s)

[« remove all](#)

New Server Class Name

Metadata >

That's *so* meta!

- Splunk automatically assigns metadata to the entire source unless you specify what the metadata should be.
- The default metadata assignments are as follows

| Metadata | Default |
|------------|---|
| source | The path of the input file |
| host | Splunk hostname of the instance (forwarder) |
| sourcetype | Splunk attempts to automatically determine |
| index | Defaults to main |



Demo: Getting Data In

How Splunk Consumes Data >

Review

- Splunk can consume and process all kinds of data
- The three primary ways to get data into Splunk are
 - Upload a file
 - Monitor a file or directory
 - Forward from another source with a heavy or universal forwarder

Thanks, Splunkers!

