Transitioning to Splunk Enterprise 10.0: What You Need to Know

PLA2002

.conf25

splunk>

Forward-looking statements

This presentation may contain forward-looking statements regarding future events, plans or the expected financial performance of our company, including our expectations regarding our products, technology, strategy, customers, markets, acquisitions and investments. These statements reflect management's current expectations, estimates and assumptions based on the information currently available to us. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation.

For additional information about factors that could cause actual results to differ materially from those described in the forward-looking statements made in this presentation, please refer to our periodic reports and other filings with the SEC, including the risk factors identified in our most recent quarterly reports on Form 10-Q and annual reports on Form 10-K, copies of which may be obtained by visiting the Splunk Investor Relations website at www.investors.splunk.com or the SEC's website at www.sec.gov. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by us, on our website or otherwise, it may not contain current or accurate information. We disclaim any obligation to update or revise any forward-looking statement based on new information, future events or otherwise, except as required by applicable law.

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. We undertake no obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release.

splunk> .conf25

Transitioning to Splunk Enterprise 10.0: What You Need to Know

Hywel Matthews

Chief Technical Advisor, TS&I Platform, CSX
Splunk — a CISCO company

.conf25
splunk>

Powered By

Casey Pike

Splunk Ninja

Shane Newman

Splunk Sommelier

Agenda

Preparations and Health Checks

Splunk Enterprise 10 Intro

General Process to Upgrade Splunk Enterprise

Splunk 10 Breaking Changes

App Compatibility

KVStore amd Infrastructure

Splunk IT Service Intelligence (ITSI) Upgrade Info

Splunk Enterprise Security (ES) Upgrade Info

FIPS 140-3

Splunk 10 Intro

What’s new & breaking changes

Splunk Platform 10 New Features

Splunk Enterprise 10.0 and Splunk Cloud Platform 10.0

- IPv6
- Edge Processor for Splunk Enterprise
- Splunk Observability Related Content in Splunk Enterprise
- Upgrade Readiness App replaced by Splunk Health Assistant Add-On
- Agent Manager 1.0: Effective Configuration — Visibility & Insights into Agents Status, Health, Performance
- Edge Processor Validated Architecture
- Observability Metrics & Charts in Splunk Enterprise Dashboard Studio
- Publication of Dashboards for Splunk Enterprise

Splunk Platform 10 Breaking Changes

Splunk Enterprise 10.0 and Splunk Cloud Platform 10.0

NodeJSv20

OS & Hardware Support Matrix

FIPS-140-3

Docker EULA User Acceptance

Hadoop Data-Roll Disabled*

Depracated

Python 3.9

OpenSSL3.0

MongoDB v7.0*

IF upgrading from Splunk Ent 9.3 or lower

Preparations and Health Checks

In preparation of the breaking changes

References

- Splunk Health Assistant Add-On, enhancing the **Monitoring Console**
- Head to the #office-hours Community Slack channel to ask questions (request access here)

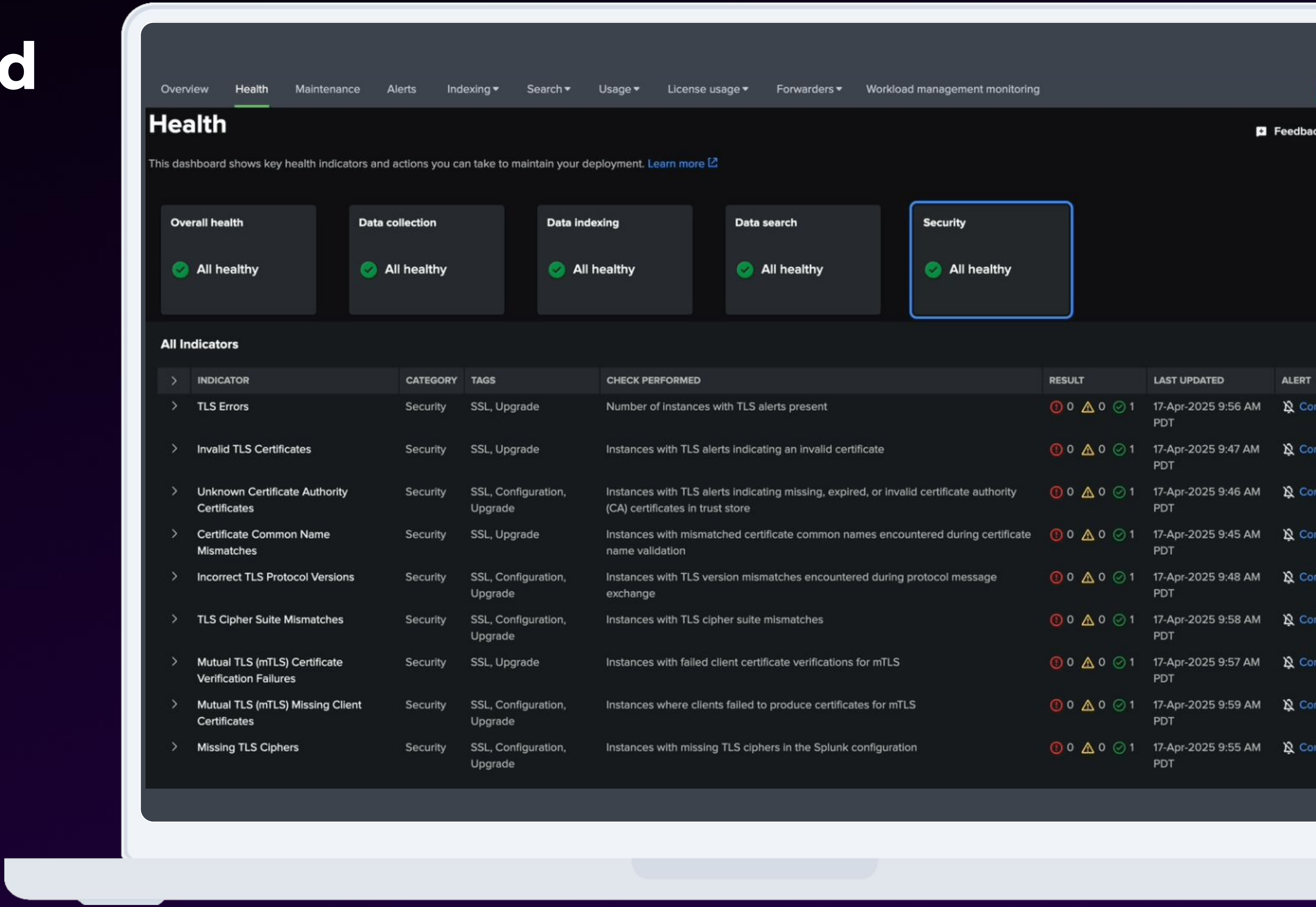
Preparations and Health Checks

Use when preparing to upgrade from 9.x to Splunk Enterprise and Cloud Platform 10.0.

This enables validation logic to be updated before a platform upgrade.

Each new validation offers remediation steps of any breaking changes, ensuring a smoother upgrade experience.

The Cloud Monitoring Console will have its own subset of validations relevant to Splunk Cloud Platform.



Health

This dashboard shows key health indicators and actions you can take to maintain your deployment. Learn more

Overall health	Data collection	Data indexing	Data search	Security
✓ All healthy	✓ All healthy	✓ All healthy	✓ All healthy	✓ All healthy

All Indicators

INDICATOR	CATEGORY	TAGS	CHECK PERFORMED	RESULT	LAST UPDATED	ALERT
TLS Errors	Security	SSL, Upgrade	Number of instances with TLS alerts present	! 0 ⚠ 0 ✓ 1	17-Apr-2025 9:56 AM PDT	Co
Invalid TLS Certificates	Security	SSL, Upgrade	Instances with TLS alerts indicating an invalid certificate	! 0 ⚠ 0 ✓ 1	17-Apr-2025 9:47 AM PDT	Co
Unknown Certificate Authority Certificates	Security	SSL, Configuration, Upgrade	Instances with TLS alerts indicating missing, expired, or invalid certificate authority (CA) certificates in trust store	! 0 ⚠ 0 ✓ 1	17-Apr-2025 9:46 AM PDT	Co
Certificate Common Name Mismatches	Security	SSL, Upgrade	Instances with mismatched certificate common names encountered during certificate name validation	! 0 ⚠ 0 ✓ 1	17-Apr-2025 9:45 AM PDT	Co
Incorrect TLS Protocol Versions	Security	SSL, Configuration, Upgrade	Instances with TLS version mismatches encountered during protocol message exchange	! 0 ⚠ 0 ✓ 1	17-Apr-2025 9:48 AM PDT	Co
TLS Cipher Suite Mismatches	Security	SSL, Configuration, Upgrade	Instances with TLS cipher suite mismatches	! 0 ⚠ 0 ✓ 1	17-Apr-2025 9:58 AM PDT	Co
Mutual TLS (mTLS) Certificate Verification Failures	Security	SSL, Upgrade	Instances with failed client certificate verifications for mTLS	! 0 ⚠ 0 ✓ 1	17-Apr-2025 9:57 AM PDT	Co
Mutual TLS (mTLS) Missing Client Certificates	Security	SSL, Configuration, Upgrade	Instances where clients failed to produce certificates for mTLS	! 0 ⚠ 0 ✓ 1	17-Apr-2025 9:59 AM PDT	Co
Missing TLS Ciphers	Security	SSL, Configuration, Upgrade	Instances with missing TLS ciphers in the Splunk configuration	! 0 ⚠ 0 ✓ 1	17-Apr-2025 9:55 AM PDT	Co

Image
https://lantern.splunk.com/Splunk_Platform/Product_Tips/Upgrades_and_Migration/Preparing_to_upgrade_from_9.x_to_Splunk_Enterprise_and_Cloud_Platform_10.0

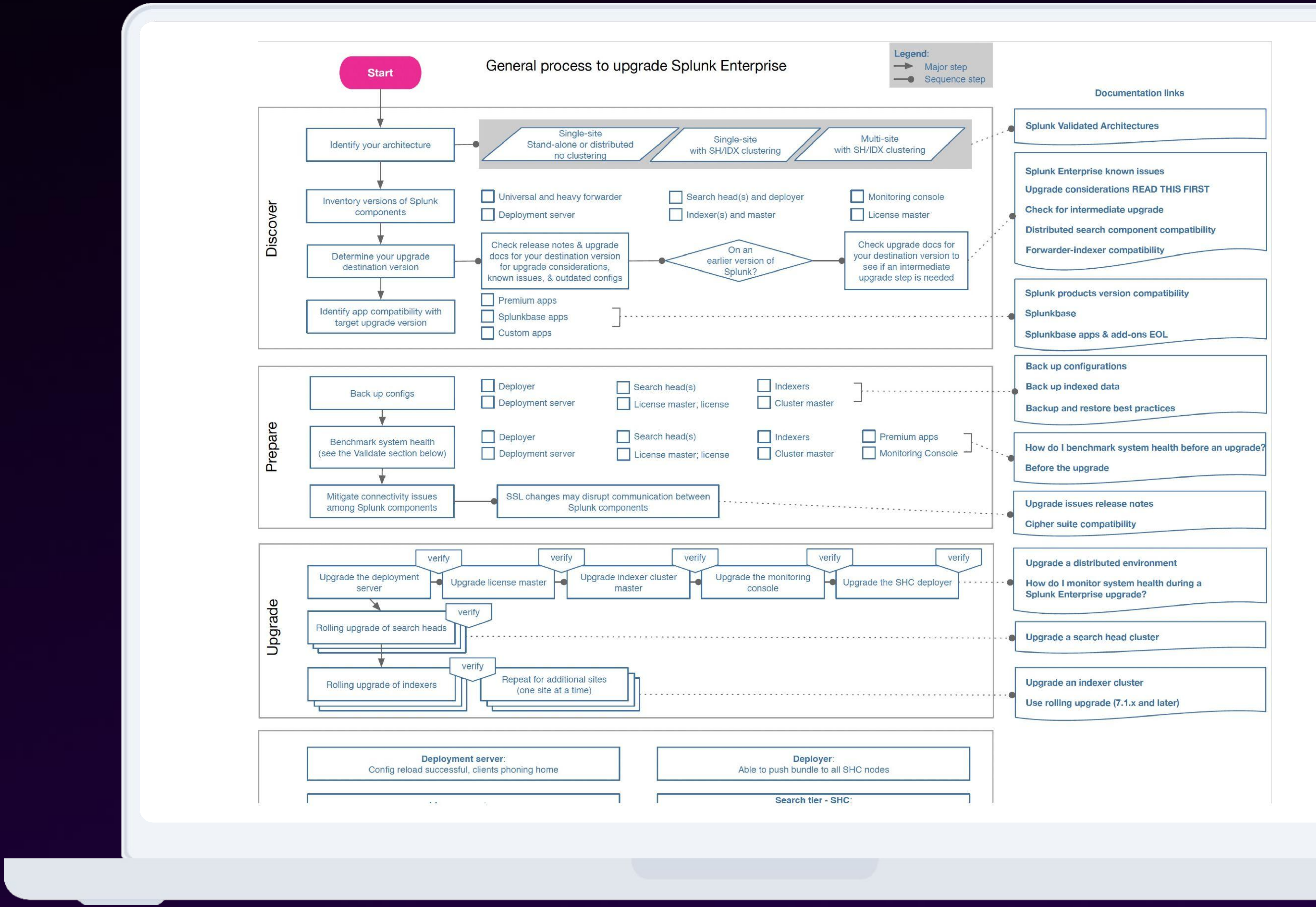
General Process to Upgrade Splunk Enterprise

… order… order …

Core Upgrade Order

Follow the path …

Search for “splunk upgrade order of operations pdf”



General process to upgrade Splunk Enterprise

Legend:
- Major step
- Sequence step

Start

Discover

- Identify your architecture → Single-site Stand-alone or distributed no clustering / Single-site with SH/IDX clustering / Multi-site with SH/IDX clustering
- Inventory versions of Splunk components → □ Universal and heavy forwarder □ Deployment server □ Search head(s) and deployer □ Indexer(s) and master □ Monitoring console □ License master
- Determine your upgrade destination version → Check release notes & upgrade docs for your destination version for upgrade considerations, known issues, & outdated configs → On an earlier version of Splunk? → Check upgrade docs for your destination version to see if an intermediate upgrade step is needed
- Identify app compatibility with target upgrade version → □ Premium apps □ Splunkbase apps □ Custom apps

Prepare

- Back up configs → □ Deployer □ Deployment server □ Search head(s) □ License master; license □ Indexers □ Cluster master
- Benchmark system health (see the Validate section below) → □ Deployer □ Deployment server □ Search head(s) □ License master; license □ Indexers □ Cluster master □ Premium apps □ Monitoring Console
- Mitigate connectivity issues among Splunk components → SSL changes may disrupt communication between Splunk components

Upgrade

- Upgrade the deployment server (verify) → Upgrade license master (verify) → Upgrade indexer cluster master (verify) → Upgrade the monitoring console (verify) → Upgrade the SHC deployer (verify)
- Rolling upgrade of search heads (verify)
- Rolling upgrade of indexers (verify) → Repeat for additional sites (one site at a time)

Deployment server: Config reload successful, clients phoning home

Deployer: Able to push bundle to all SHC nodes

Search tier - SHC:

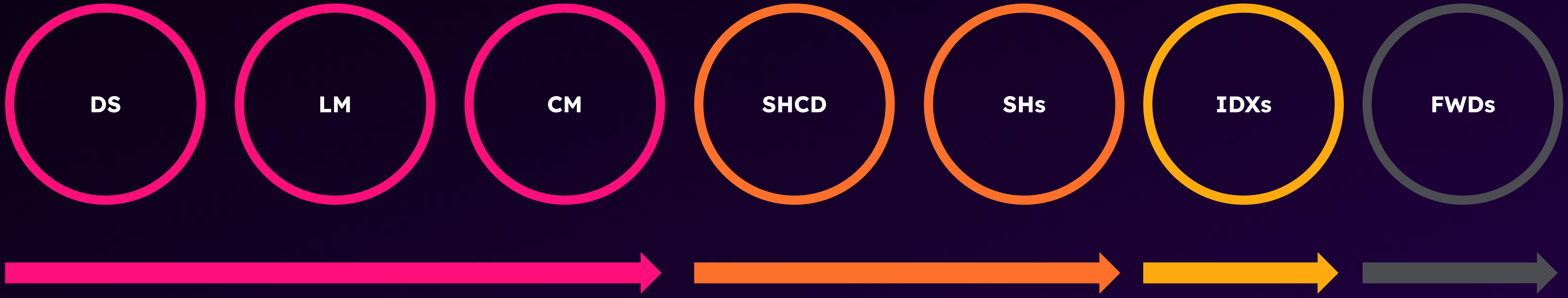
Documentation links

- Splunk Validated Architectures
- Splunk Enterprise known issues
- Upgrade considerations READ THIS FIRST
- Check for intermediate upgrade
- Distributed search component compatibility
- Forwarder-indexer compatibility
- Splunk products version compatibility
- Splunkbase
- Splunkbase apps & add-ons EOL
- Back up configurations
- Back up indexed data
- Backup and restore best practices
- How do I benchmark system health before an upgrade?
- Before the upgrade
- Upgrade issues release notes
- Cipher suite compatibility
- Upgrade a distributed environment
- How do I monitor system health during a Splunk Enterprise upgrade?
- Upgrade a search head cluster
- Upgrade an indexer cluster
- Use rolling upgrade (7.1.x and later)

Image
https://docs.splunk.com/images/d/d3/Splunk_upgrade_order_of_ops.pdf?_gl=1*w492xt*_gcl_au*NTMwOTc5NTU0LjE3NTEzMDA4NzE.*FPAU*NTMwOTc5NTU0LjE3NTEzMDA4NzE.*_ga*MTU5MjY5MjM5Mi4xNzE5NDg1MTg5*_ga_5EPM2P39FV*czE3NTI4Mjk1NzkkbzY4MSRnMSR0MTc1MjgzNDgwMSRqNjAkbDAkaDIwNDQ1MzIyMTQ.*_fplc*eFJTbVdJa296RWp6U1FUcDBraDJVY1pKRFA3bWV1TndXYTl3S2VmJTJGb2wzcDNMOGJjUjRIZFhleUtQJTJCWkclMkZ2Wk50dlhNZG1iWTdzRThrWnBldTZaTXM1bVBXRngzaGhTMGVqTHBFWnJGYUFET0t5JTJGSGptRURDNlR1NiUyRkpDdyUzRCUzRA..

Core Upgrade Order Recap

… For Splunk Enterprise



Verify instances functioning as expected

Move on to next layer

Breaking Changes

… The 7 Ps of planning …

References

- [Preparing to upgrade from 9.x to the upcoming release of Splunk Enterprise and Cloud Platform]

Breaking Changes May Impact Splunk 10?

What and who…

Category	Breaking Change	Splunk Role Affected?
Dependency Updates	OpenSSL library version update	Admin
	Python runtime environment version update and removal of support of older versions	Admin & App Developers
	Upgrade to Node.js JavaScript runtime environment version update	Admin & App Developers
Security	Certificate Authority (CA) certificate is required due to OpenSSL3	Admin
	TLS network security protocol version 1.2 or higher is required	Admin & App Developers
	Extended Master Secret requirement for FIPS 140-3	Admin
Deprecation and Removals	Hadoop Data-Roll turned off by default	Admin
	Changes to Supported CPU Instruction Sets	Admin
	Unsafe v1 search APIs turned off by default	Admin & App Developers
	Incompatible Apps	Admin & App Developers
Compliance Changes	MongoDB upgrade for OpenSSL support	Admin
	FIPS 140-3 enforces minimum OS version requirements	Admin & App Developers
Legal	Docker EULA User Acceptance	Admin

App Compatibility

… measure twice, cut once …

References

- Splunk 10.0 compatible Splunk Supported Apps
- 3rd Party / Private Apps
- Preparing to upgrade from 9.x to the upcoming release of Splunk Enterprise and Cloud Platform
- Preparing your Splunk Environment for OpenSSL3
- Deprecated and removed in version 9.0
- Splunk Docs Locate the source of your deprecated REST calls

App Compatibility

Do your homework…

Upgrade to Splunk 10 Compatible Versions From Splunkbase

- Splunk 10.0 compatible Splunk Supported Apps — Splunkbase Filter link
- 3rd Party / Private Apps — Splunkbase Filter link
  - Developers have been sent emails, lantern article and news community post
  - Splunk Lantern: Preparing to upgrade from 9.x to the upcoming release of Splunk Enterprise and Cloud Platform
  - Splunk Community: Preparing your Splunk Environment for OpenSSL3

Incompatible Apps and Customizations

- Compatibility with Python 3.9 + OpenSSL3 (can fallback to OpenSSL1 for non FIPS)
- Convert all v1 Search APIs to v2
- Compatibility with Node.js 20.18.2+

Python Consideration

- Splunk Enterprise 10.0 only ships with Python 3.9
- Python 2.7 and 3.7 **DO NOT** exist in Splunk Enterprise 10.0
- When you upgrade to Splunk Enterprise 10.0, if there are python issues, **THERE IS NO FALLBACK**

Test Your Apps!

Version 1 APIs

Version 1 APIs Deprecated

- V1 APIs were deprecated in Splunk Enterprise 9.0 — Deprecated Features Doc
- Splunk Enterprise 9.0 was initially released on June 14, **2022**
- Splunk Enterprise 9.0.1 reached its End-of-Life (EOL) on June 14, **2024**

Discover Deprecated REST Calls

- Check apps and users still using the V1 API, reference the Splunk doc for searches
  - Splunk Docs Locate the source of your deprecated REST calls
- There are 2 searches that can be used to validate V1 APIs are no longer used

Enable V1 API?

- Want to enable V1 API?
  - Use `restmap.conf`
    - `[global]`
      `v1APIBlockGETSearchLaunch=false`
- Is set to true by default in Splunk Enterprise 10.0
  - Set to false if there is a dependency on V1 APIs missed during validation

Test Your Apps! Part 2

Python 3.9

Splunk's Recommendation (Email / Blog Articles)

- Create Splunk Enterprise 10 Beta test instance
- Install applications referencing python (.py files in etc/apps/*)
- Configure apps to work on the Splunk Enterprise 10 Beta instance
- Test to confirm apps work
  - Check logs for error messages, assuming they are logged, and not silent
  - Inclide log level "INFO" and "WARN"

Using Splunk Enterprise 9.3 / 9.4

- Splunk Enterprise 9.3 & 9.4 have a feature flag to force python 3.9
  - Can be turned on and off for testing, switching between 3.7 and 3.9
  - Use `Server.conf`

    ```
    [general]
    python.version = force_python3
    ```
  - https://docs.splunk.com/Documentation/Splunk/9.4.2/Python3Migration/ChangesEnterprise
  - Test apps in production during a maintenance window in python 3.9. if issues switch back and resolve

Reminder

- Splunk Enterprise 10.0 only ships with Python 3.9
- Python 2.7 and 3.7 **DO NOT** exist in Splunk Enterprise 10.0
- When upgrading to Splunk Enterprise 10.0, if there are python issues, **THERE IS NO FALLBACK**

Test Your Apps! Part 3

OpenSSLv3

Splunk Enterprise 10.0

- Only option is to test on Splunk Enterprise 10.0 - is the first version of Splunk including OpenSSLv3
- There are only a few apps OpenSSLv3 has impacted, across all Splunk apps

Fallback to OpenSSLv1 … as a failsafe …

- The “fallback” mode runs python 3.9 + OpenSSLv1
  - Use for apps that depend on OpenSSLv1, but conflict if OpenSSLv3 is in use
- The “fallback” Mode is global
- Whenever splunkd launches python, OpenSSL 1.0 is used
- To enable use `server.conf`

```
[general]
python.not_compatible =
openssl3.0
```

Reminder

- Any python module that uses deprecated APIs needs to be updated to versions that work with OpenSSLv3 or later for FIPS 140-3 compliance
- Refer to the OpenSSL Migration Guide (docs.openssl.org) for detailed information

Test Your Apps! Part 4

NodeJSv20

NodeJSv20

- NodeJS was upgraded from v8 to v20
- NodeJS is deprecated as of Splunk Enterprise and Splunk Cloud 10.0
- **NodeJS will be removed in the next release after Splunk Enterprise 10.0 - apps that call NodeJS will break**
- App developers have received multiple emails and blog posts informing them of these changes in 2025

Developer Responsibility

- Review NodeJS's deprecation notes
  - Identify APIs that may have been removed between v8 and v20
- Check for script invocation errors relating to extension points in apps implemented in NodeJS
  - Custom Search Commands, Modular Alerts, and Modular Inputs support NodeJS natively (i.e. Splunk will look for .js files matching the files specified in .conf files even if the file extension isn't specified) making it tricky to identify NodeJS usage using SPL alone
  - Some extension points might also be implemented using a shell script as a shim for NodeJS code
- Consider converting extension points to python or another supported language

Customer / User Responsibility

- Use the Splunk Enterprise 10 Beta to determine if any key apps or workflows are impacted
- Always ensure that Splunk-built and 3rd party apps are updated to the latest version!

KVStore and Infrastructure

Important changes

- MongoDB (KV Store) Upgrade to v7.0
- Intel and AMD Processors

KVStore and Infrastructure

Important changes

MongoDB (KV Store): Upgrade to v7.0

- Upgrade to v7.0 (Requires AVX enabled, Required for FIPS 140-2 after March & FIPS 140-3)
- On upgrading to Splunk Enterprise 9.4.x or 10.0, upgrade will automatically be attempted twice, after splunkd is started
- **Warning: FIPS mode will result in a startup failure**

MongoDB v4.2 Unsupported in Splunk 10

- If the upgrade fails twice, MongoDB will revert to v4.2
  - Manual upgrade required
  - Contact Splunk Support for assistance
- KVstore will continue to operate with Splunk Enterprise 9.4 and 10.0
- MongoDB v4.2 **is NOT supported with Splunk Enterprise 10.0**
  - Splunk Enterprise 10.0 and premium apps will still function

Infrastructure Changes CPU Requirements:

- For Intel x86_64, a Sandy Bridge or higher Core processor is required, with the SSE4.2, AVX, and AES-NI instructions enabled
- For AMD x86_64, a Bulldozer or higher processor is required, with the AVX instructions enabled

IT Service Intelligence (ITSI & ITEW)

Recommendations

References

- Splunk Docs - Splunk products version compatibility matrix
- Splunk Docs - ITSI compatibility with related apps and add-ons

IT Service Intelligence (ITSI & ITEW)

Recommendations

- ITSI 4.21 - **Recommended** - Splunk 10 compatible ✅
  - **Availability** September 2nd, 2025
- ITSI 4.20.1 - **Not Recommended** - Requires v1 API flag ❌
  - **Availability** June 30th, 2025

- Dependencies:
  - MLTK 5.5.x (min for ITSI 4.20.x)
  - MLTK 5.6.0 (Required for FIPS 140-3)
- Check ITSI Compatibility Matrix!
  - Splunk Docs - Splunk products version compatibility matrix
  - Splunk Docs - ITSI compatibility with related apps and add-ons

Enterprise Security (ES)

Recommendations & advice

References

- Splunk Lantern - Upgrading to Enterprise Security 8.0.x - Walkthrough and validation
- Splunk Docs - Splunk products version compatibility matrix
- Splunk Docs - Upgrade Splunk Enterprise Security 8
- Splunk Lantern: Upgrading to Enterprise Security 8.0.x - Compatibility checks

Enterprise Security (ES)

Recommendations

- ES 8.1.1 - **Recommended** - API v2, MLTK 5.5+ - Splunk 10 compatible ✅
  - **Availability** July 17th, 2025
- ES 7.3.4 - **Recommended** - Patch expected for Splunk 10 compatible ✅
  - **Availability** July 30th, 2025
  - Customers with a Centralized SOC / RBAC / Multi-tenancy should remain on this version while reviewing security requirements

- ES 8.1.0 - **Not Recommended** - MLTK 5.4 - NOT Splunk 10 compatible ❌
  - **Availability** June 10th, 2025
- ES 8.0.40 - **Not Recommended** - MLTK 5.4 - NOT Splunk 10 compatible ❌
  - **Availability** April 30th, 2025
- ES 8.0.1 - **Not Recommended** - MLTK and v1 API only - NOT Splunk 10 compatible without feature flag ❌
  - **Availability** December 5th, 2024
- ES < 7.3.4 - **Not Recommended** - NOT Splunk 10 compatible ❌

Enterprise Security (ES)

Incompatible apps/configs — DO NOT upgrade to ES 8.0.x if using PCI, Mothership, SOAR

Splunk SOAR - configurations not supported in ES 8.0.x:

- Hybrid architecture (CMP & Cloud)
- Container labels to segregate roles/access to incidents and investigations
- SOAR clusters (CMP)

Splunk PCI

- No current version compatible with Splunk Enterprise Security 8.0.x
- Support for the PCI app is tentatively slated for Enterprise Security 8.1.x

Mothership

- Core functionality (sending SPL to remote environments) remains compatible with ES 8.0.x
- ES 8.0.x taxonomy changes:
  - Notable references (for example, multi_es_security_posture_view) require updates to align with the ES 8.0.x taxonomy
- Finding groups & roll-up findings:
  - In ES 8.0.x, AQ FBD findings can be grouped and expanded.
  - However, in Mothership, child findings do not appear when pulling in parent findings, which breaks the grouping relationship

FIPS

... Not pips ...

References

- Secure Splunk Enterprise with FIPS

FIPS

Splunk Enterprise 10 supports FIPS 140-3

- Splunk Enterprise 10.0 defaults to FIPS 140-2
- When ready, change to 140-3

Many Requirements

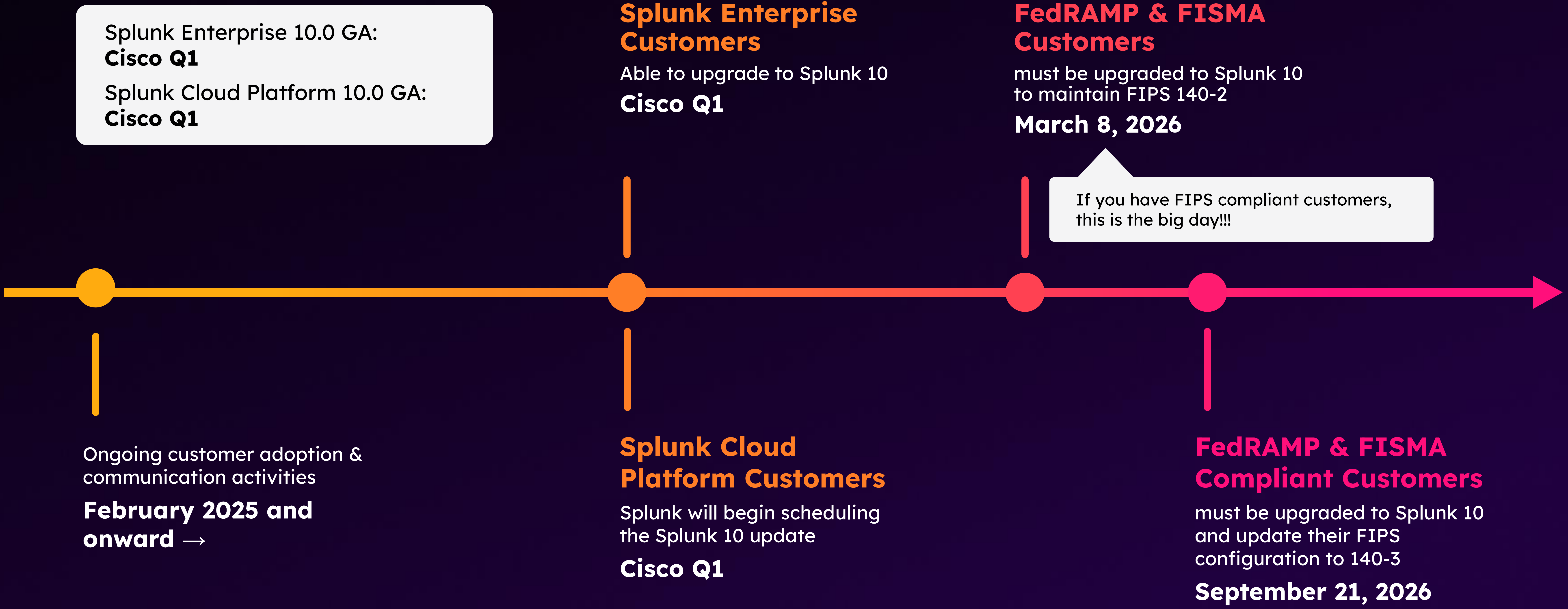
- Requires FIPS 140-3 Hardware
- Requires ITSI 4.21
- Requires MLTK 5.6.0
- SSL Certificates must be OpenSSL 3.0 / FIPS compliant (Use SHAA MC Checks)
- Mongo 7.0
- OpenSSLv3
- All instances on Ubuntu 22.04 or higher
- Python 3.9
- Splunk DB Connect 4.0 requires a fresh installation

Many Compatibility Requirements

- Between Splunk UF / Splunk Cloud / Splunk Enterprise
- Read and check the Splunk 10 Documentation
  - Secure Splunk Enterprise with FIPS

Splunk 10 and FIPS Compliance Timeline

When customers operating a FIPS compliance environment need to upgrade



Splunk Enterprise 10.0 GA:
Cisco Q1

Splunk Cloud Platform 10.0 GA:
Cisco Q1

Ongoing customer adoption & communication activities

February 2025 and onward →

Splunk Enterprise Customers

Able to upgrade to Splunk 10

Cisco Q1

Splunk Cloud Platform Customers

Splunk will begin scheduling the Splunk 10 update

Cisco Q1

FedRAMP & FISMA Customers

must be upgraded to Splunk 10 to maintain FIPS 140-2

March 8, 2026

If you have FIPS compliant customers, this is the big day!!!

FedRAMP & FISMA Compliant Customers

must be upgraded to Splunk 10 and update their FIPS configuration to 140-3

September 21, 2026

FIPS Compatibility

Before switching Splunk 10.0 to FIPS 140-3, ensure all Splunk 9.x (and prior) instances have first been upgraded to Splunk 10.0.

FIPS 140-2 is the default for Splunk 10.0.

Universal Forwarder			
Splunk Enterprise / Cloud	Splunk UF 9.x FIPS 140-2	Splunk UF 10 FIPS 140-2	Splunk UF 10 FIPS 140-3
Splunk 9.x FIPS 140-2	✅	✅	❌
Splunk 10 FIPS 140-2	✅	✅	✅
Splunk 10 FIPS 140-3	❌	✅	✅

Splunk Enterprise / Cloud			
Splunk Enterprise / Cloud	Splunk 9.x FIPS 140-2	Splunk 10 FIPS 140-2	Splunk 10 FIPS 140-3
Splunk 9.x FIPS 140-2	✅	✅	❌
Splunk 10 FIPS 140-2	✅	✅	✅
Splunk 10 FIPS 140-3	❌	✅	✅

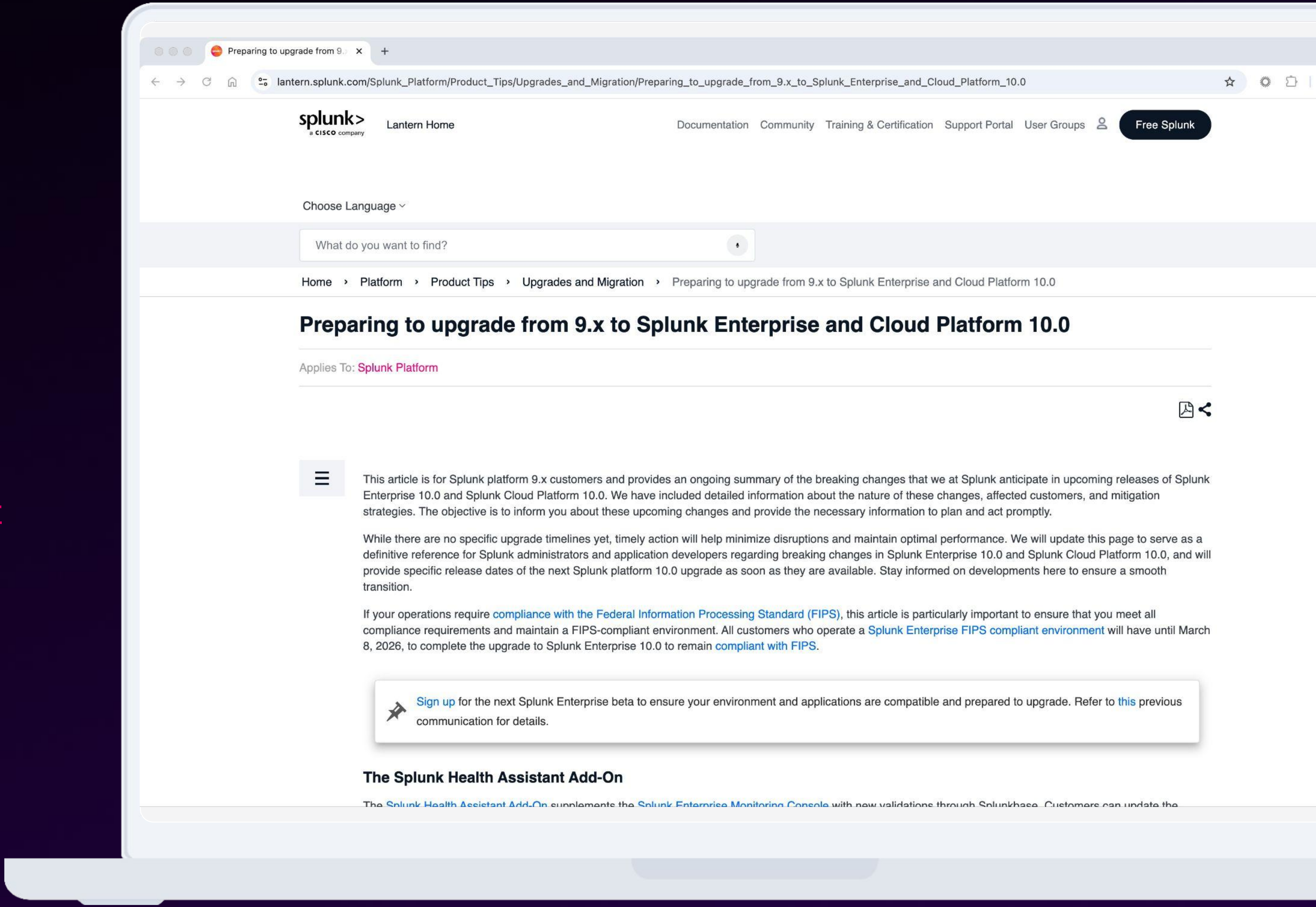
Call To Action!

To do list when you get home

Lantern

Preparing to upgrade from 9.x to Splunk Enterprise and Cloud Platform 10.0

https://lantern.splunk.com/Splunk_Platform/Product_Tips/Upgrades_and_Migration/Preparing_to_upgrade_from_9.x_to_Splunk_Enterprise_and_Cloud_Platform_10.0


Preparing to upgrade from 9.
lantern.splunk.com/Splunk_Platform/Product_Tips/Upgrades_and_Migration/Preparing_to_upgrade_from_9.x_to_Splunk_Enterprise_and_Cloud_Platform_10.0
splunk> a CISCO company
Lantern Home
Documentation
Community
Training & Certification
Support Portal
User Groups
Free Splunk
Choose Language
What do you want to find?
Home › Platform › Product Tips › Upgrades and Migration › Preparing to upgrade from 9.x to Splunk Enterprise and Cloud Platform 10.0

Preparing to upgrade from 9.x to Splunk Enterprise and Cloud Platform 10.0

Applies To: Splunk Platform

This article is for Splunk platform 9.x customers and provides an ongoing summary of the breaking changes that we at Splunk anticipate in upcoming releases of Splunk Enterprise 10.0 and Splunk Cloud Platform 10.0. We have included detailed information about the nature of these changes, affected customers, and mitigation strategies. The objective is to inform you about these upcoming changes and provide the necessary information to plan and act promptly.

While there are no specific upgrade timelines yet, timely action will help minimize disruptions and maintain optimal performance. We will update this page to serve as a definitive reference for Splunk administrators and application developers regarding breaking changes in Splunk Enterprise 10.0 and Splunk Cloud Platform 10.0, and will provide specific release dates of the next Splunk platform 10.0 upgrade as soon as they are available. Stay informed on developments here to ensure a smooth transition.

If your operations require compliance with the Federal Information Processing Standard (FIPS), this article is particularly important to ensure that you meet all compliance requirements and maintain a FIPS-compliant environment. All customers who operate a Splunk Enterprise FIPS compliant environment will have until March 8, 2026, to complete the upgrade to Splunk Enterprise 10.0 to remain compliant with FIPS.

Sign up for the next Splunk Enterprise beta to ensure your environment and applications are compatible and prepared to upgrade. Refer to this previous communication for details.

The Splunk Health Assistant Add-On

The Splunk Health Assistant Add-On supplements the Splunk Enterprise Monitoring Console with new validations through Splunkbase. Customers can update the

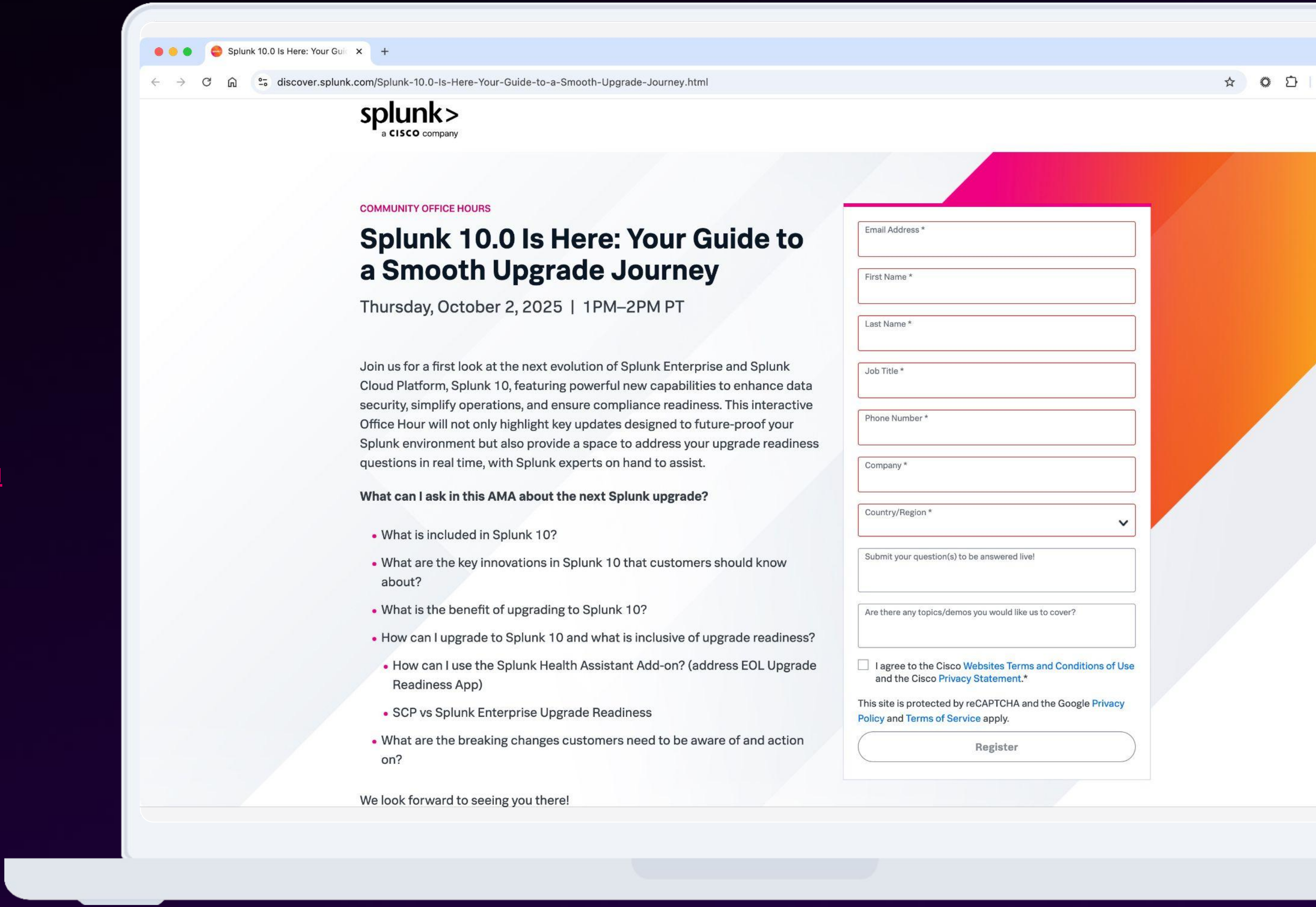
Image
https://lantern.splunk.com/Splunk_Platform/Product_Tips/Upgrades_and_Migration/Preparing_to_upgrade_from_9.x_to_Splunk_Enterprise_and_Cloud_Platform_10.0

Splunk 10.0 Is Here:

Your Guide to a Smooth Upgrade Journey

Thursday, October 2, 2025 | 1PM–2PM PT. Register here https://discover.splunk.com/Splunk-10.0-Is-Here-Your-Guide-to-a-Smooth-Upgrade-Journey.html

Head to the #office-hours Community Slack channel to ask questions (request access here)


Splunk 10.0 Is Here: Your Gui
discover.splunk.com/Splunk-10.0-Is-Here-Your-Guide-to-a-Smooth-Upgrade-Journey.html
splunk>
a CISCO company

COMMUNITY OFFICE HOURS

Splunk 10.0 Is Here: Your Guide to a Smooth Upgrade Journey

Thursday, October 2, 2025 | 1PM–2PM PT

Join us for a first look at the next evolution of Splunk Enterprise and Splunk Cloud Platform, Splunk 10, featuring powerful new capabilities to enhance data security, simplify operations, and ensure compliance readiness. This interactive Office Hour will not only highlight key updates designed to future-proof your Splunk environment but also provide a space to address your upgrade readiness questions in real time, with Splunk experts on hand to assist.

What can I ask in this AMA about the next Splunk upgrade?

- What is included in Splunk 10?
- What are the key innovations in Splunk 10 that customers should know about?
- What is the benefit of upgrading to Splunk 10?
- How can I upgrade to Splunk 10 and what is inclusive of upgrade readiness?
  - How can I use the Splunk Health Assistant Add-on? (address EOL Upgrade Readiness App)
  - SCP vs Splunk Enterprise Upgrade Readiness
- What are the breaking changes customers need to be aware of and action on?

We look forward to seeing you there!

Email Address *

First Name *

Last Name *

Job Title *

Phone Number *

Company *

Country/Region *

Submit your question(s) to be answered live!

Are there any topics/demos you would like us to cover?

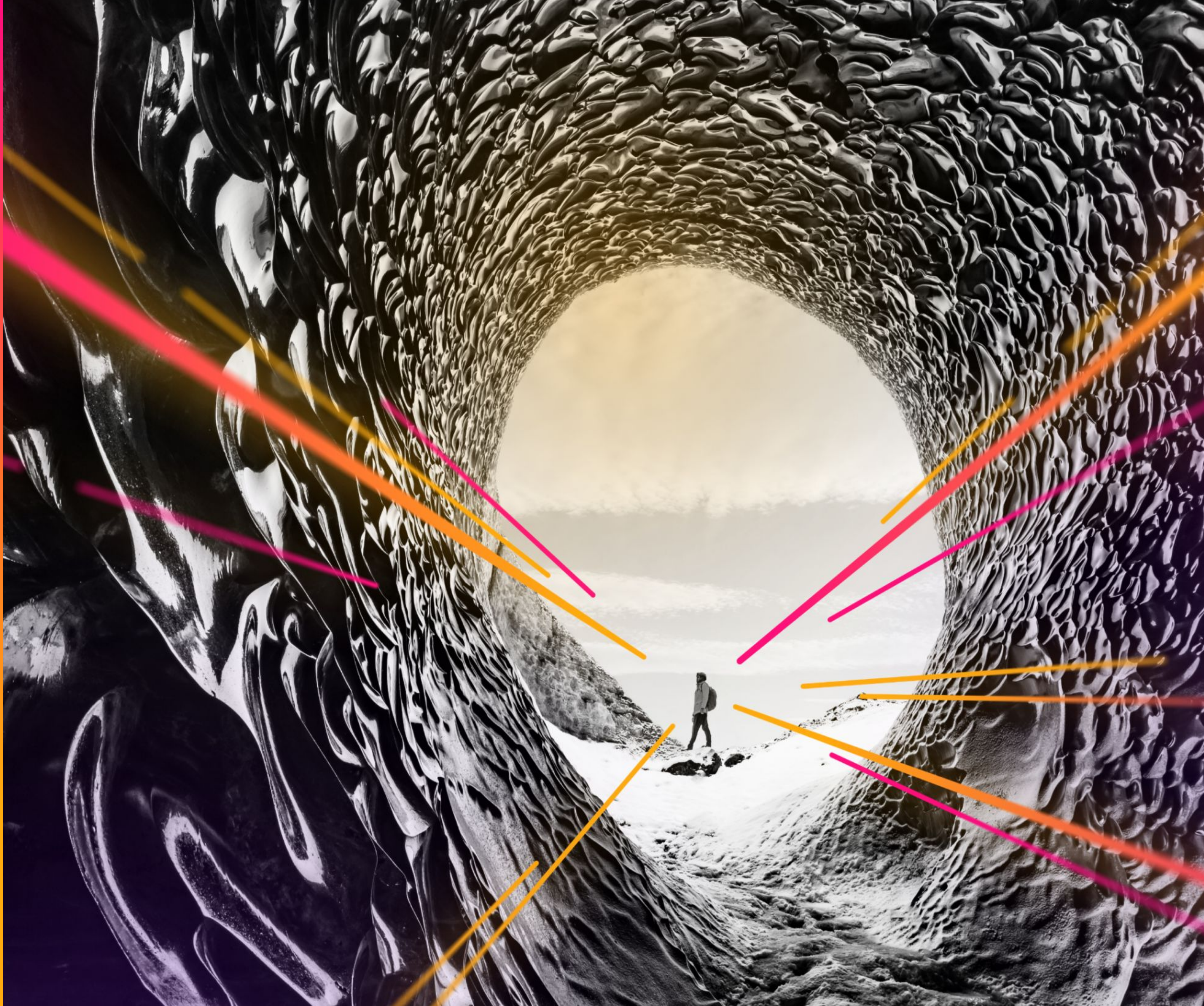
□ I agree to the Cisco Websites Terms and Conditions of Use and the Cisco Privacy Statement.*

This site is protected by reCAPTCHA and the Google Privacy Policy and Terms of Service apply.

Register

Image
https://discover.splunk.com/Splunk-10.0-Is-Here-Your-Guide-to-a-Smooth-Upgrade-Journey.html

Q&A



Thank you

.conf25
splunk>

Appendix

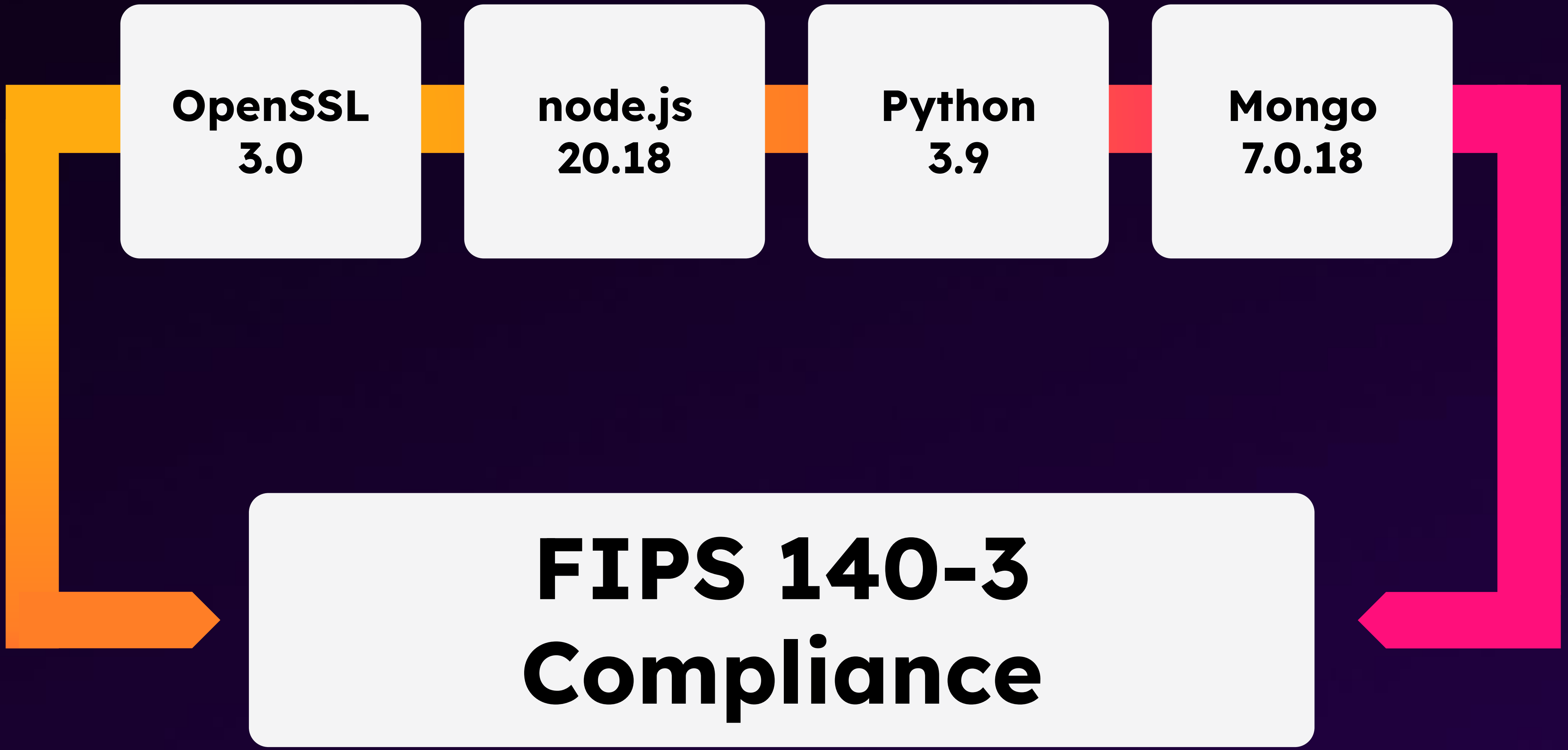
Value of Splunk 10

SPLUNK ENTERPRISE
& CLOUD PLATFORM

ANNOUNCING

Compliant-Ready Environment

A more **secure and compliant environment**, reducing the compliance and administrative overhead for Splunk admins and allowing them to focus more on strategic business priorities.



OpenSSL 3.0

node.js 20.18

Python 3.9

Mongo 7.0.18

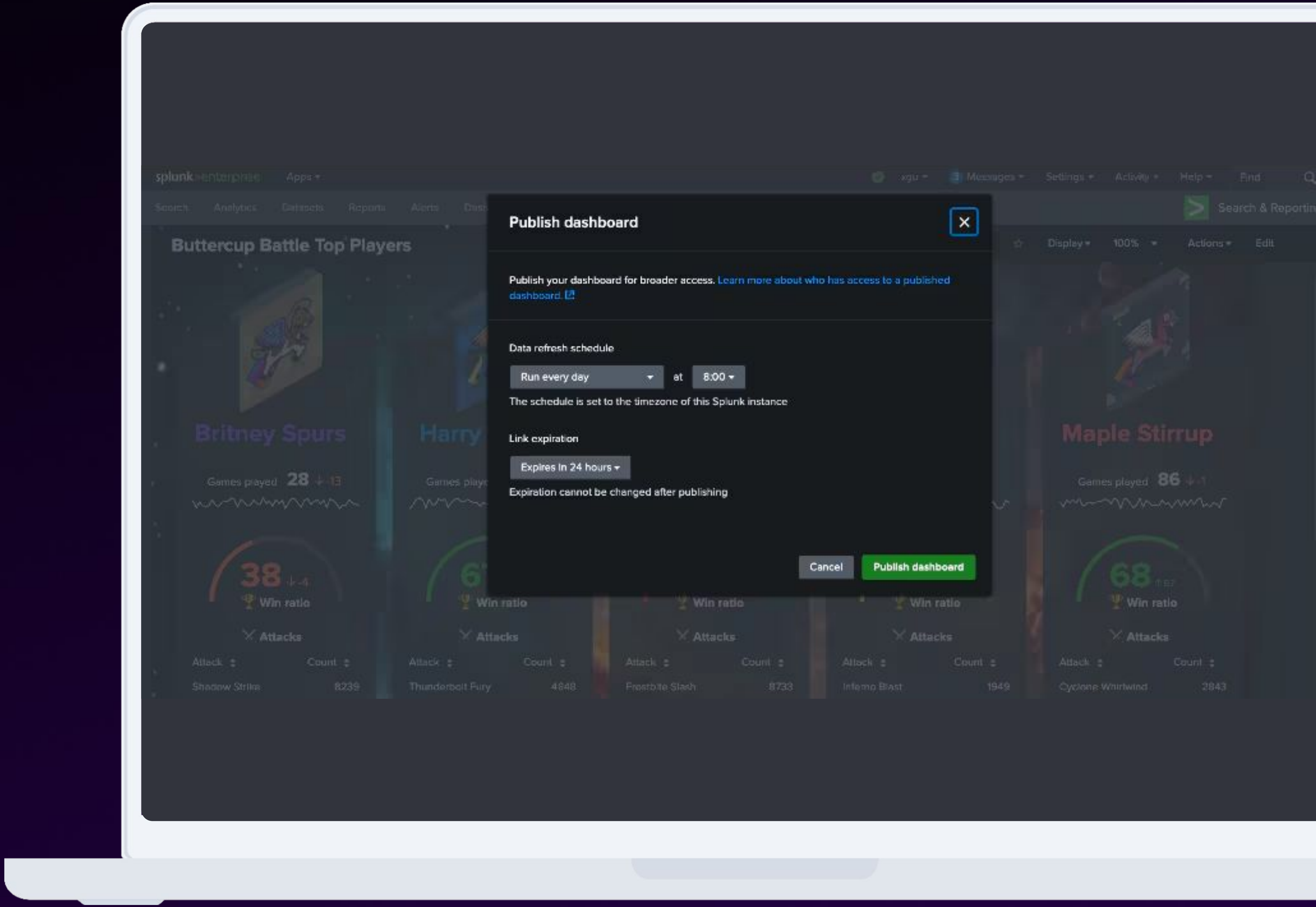
FIPS 140-3 Compliance

SPLUNK ENTERPRISE

ANNOUNCING

Dashboard Studio Updates

Sharing Splunk data without security risks: the publication of Dashboards!



Publish dashboard

Publish your dashboard for broader access. Learn more about who has access to a published dashboard.

Data refresh schedule

Run every day at 8:00

The schedule is set to the timezone of this Splunk instance

Link expiration

Expires in 24 hours

Expiration cannot be changed after publishing

SPLUNK ENTERPRISE

ANNOUNCING

Observability Cloud Related Content

Accelerate **root cause analysis** by bringing in application and infrastructure data to your logs for more context of your events.

SPLUNK ENTERPRISE

ANNOUNCING

Observability Cloud metrics and Service Map in Dashboard Studio

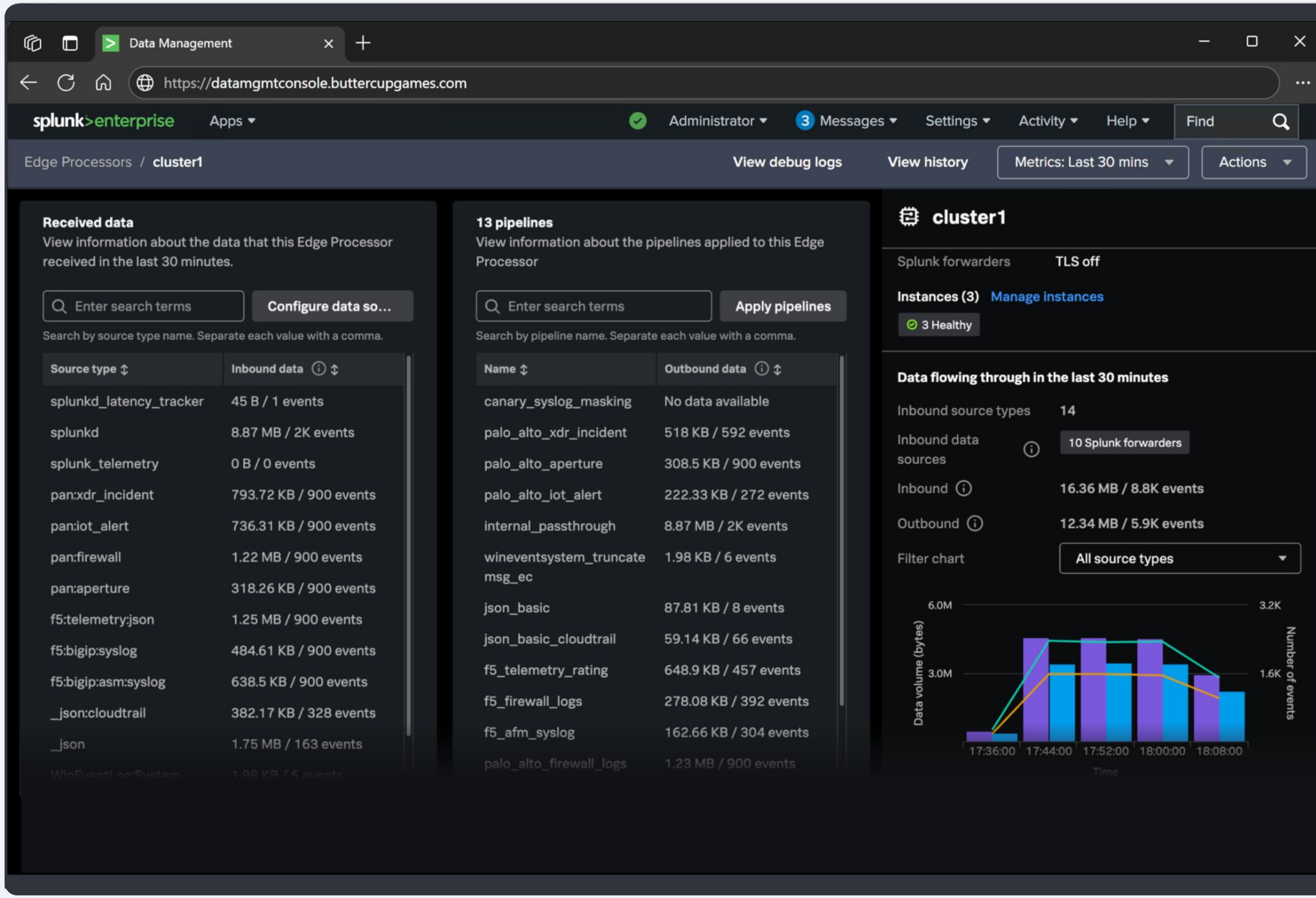
Leverage Splunk Observability Cloud's **powerful metric store** and Service Map views for your ITOps and security use cases by bringing real-time monitoring metrics into Splunk Dashboard Studio.

SPLUNK ENTERPRISE

ANNOUNCING

Edge Processor

Gain more control over data pipelines with flexible filtering, transformation, masking, encrypting and routing capabilities - powered by SPL2.



Edge Processors / cluster1

Received data
View information about the data that this Edge Processor received in the last 30 minutes.

Search by source type name. Separate each value with a comma.

Source type	Inbound data
splunkd_latency_tracker	45 B / 1 events
splunkd	8.87 MB / 2K events
splunk_telemetry	0 B / 0 events
pan:xdr_incident	793.72 KB / 900 events
pan:iot_alert	736.31 KB / 900 events
pan:firewall	1.22 MB / 900 events
pan:aperture	318.26 KB / 900 events
f5:telemetry:json	1.25 MB / 900 events
f5:bigip:syslog	484.61 KB / 900 events
f5:bigip:asm:syslog	638.5 KB / 900 events
_json:cloudtrail	382.17 KB / 328 events
_json	1.75 MB / 163 events
WinEventLog:System	1.98 KB / 6 events

13 pipelines
View information about the pipelines applied to this Edge Processor

Search by pipeline name. Separate each value with a comma.

Name	Outbound data
canary_syslog_masking	No data available
palo_alto_xdr_incident	518 KB / 592 events
palo_alto_aperture	308.5 KB / 900 events
palo_alto_iot_alert	222.33 KB / 272 events
internal_passthrough	8.87 MB / 2K events
wineventsystem_truncate msg_ec	1.98 KB / 6 events
json_basic	87.81 KB / 8 events
json_basic_cloudtrail	59.14 KB / 66 events
f5_telemetry_rating	648.9 KB / 457 events
f5_firewall_logs	278.08 KB / 392 events
f5_afm_syslog	162.66 KB / 304 events
palo_alto_firewall_logs	1.23 MB / 900 events

cluster1

Splunk forwarders TLS off

Instances (3) Manage instances

✓ 3 Healthy

Data flowing through in the last 30 minutes

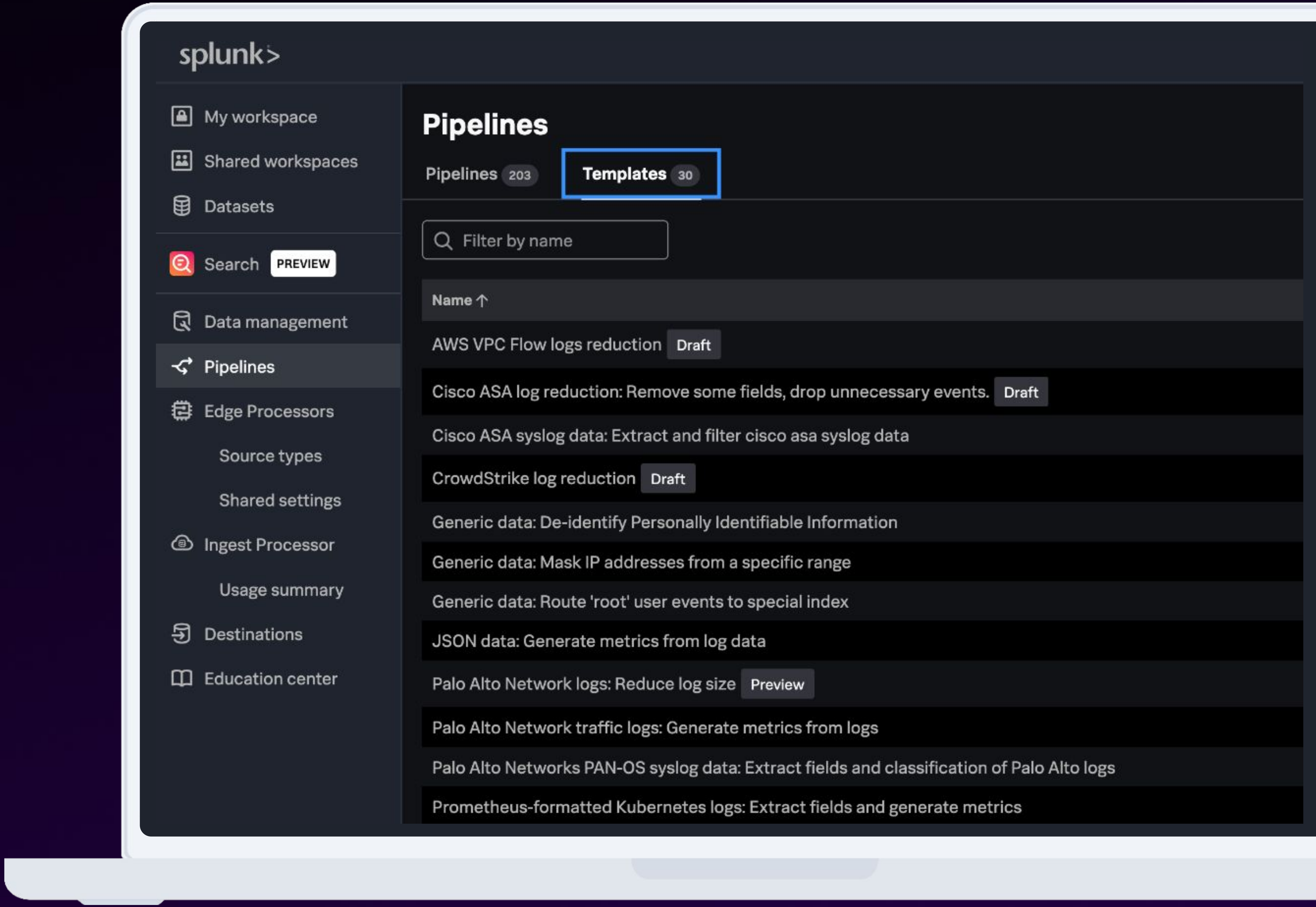
Inbound source types	14
Inbound data sources	10 Splunk forwarders
Inbound	16.36 MB / 8.8K events
Outbound	12.34 MB / 5.9K events
Filter chart	All source types

SPLUNK ENTERPRISE & CLOUD PLATFORM

ANNOUNCING

Pipeline templates

Production ready, SPL2-based code for Edge Processor and Ingest Processor.



Pipelines

Pipelines 203 | Templates 30

Filter by name

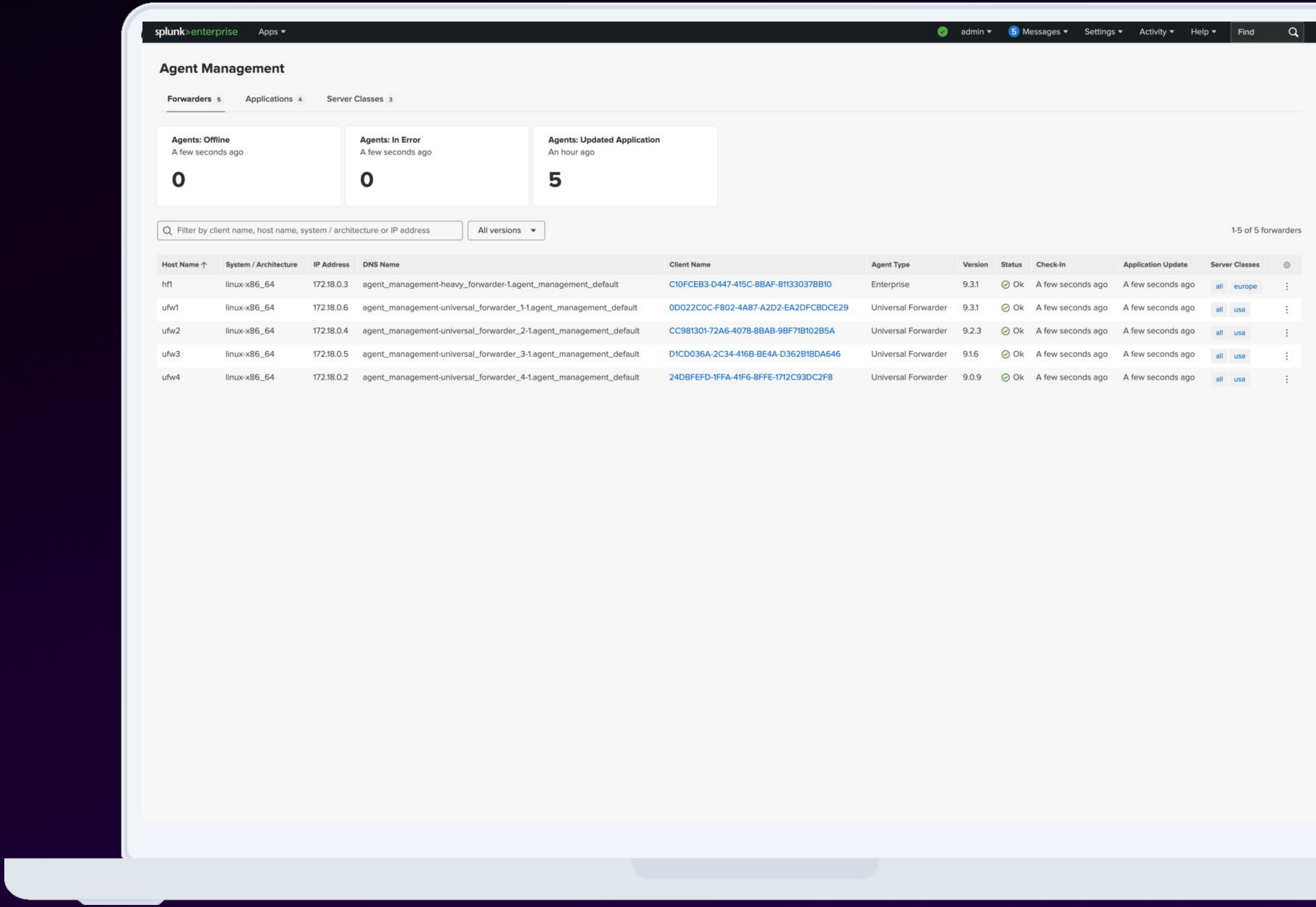
Name ↑
AWS VPC Flow logs reduction Draft
Cisco ASA log reduction: Remove some fields, drop unnecessary events. Draft
Cisco ASA syslog data: Extract and filter cisco asa syslog data
CrowdStrike log reduction Draft
Generic data: De-identify Personally Identifiable Information
Generic data: Mask IP addresses from a specific range
Generic data: Route 'root' user events to special index
JSON data: Generate metrics from log data
Palo Alto Network logs: Reduce log size Preview
Palo Alto Network traffic logs: Generate metrics from logs
Palo Alto Networks PAN-OS syslog data: Extract fields and classification of Palo Alto logs
Prometheus-formatted Kubernetes logs: Extract fields and generate metrics

SPLUNK ENTERPRISE

ANNOUNCING

Agent management

Accelerate data ingestion and reduce administrative overhead with centralized configuration, upgrades and troubleshooting of the agent fleet.



Agent Management

Agents: Offline
A few seconds ago
0

Agents: In Error
A few seconds ago
0

Agents: Updated Application
An hour ago
5

Filter by client name, host name, system / architecture or IP address
All versions

1-5 of 5 forwarders

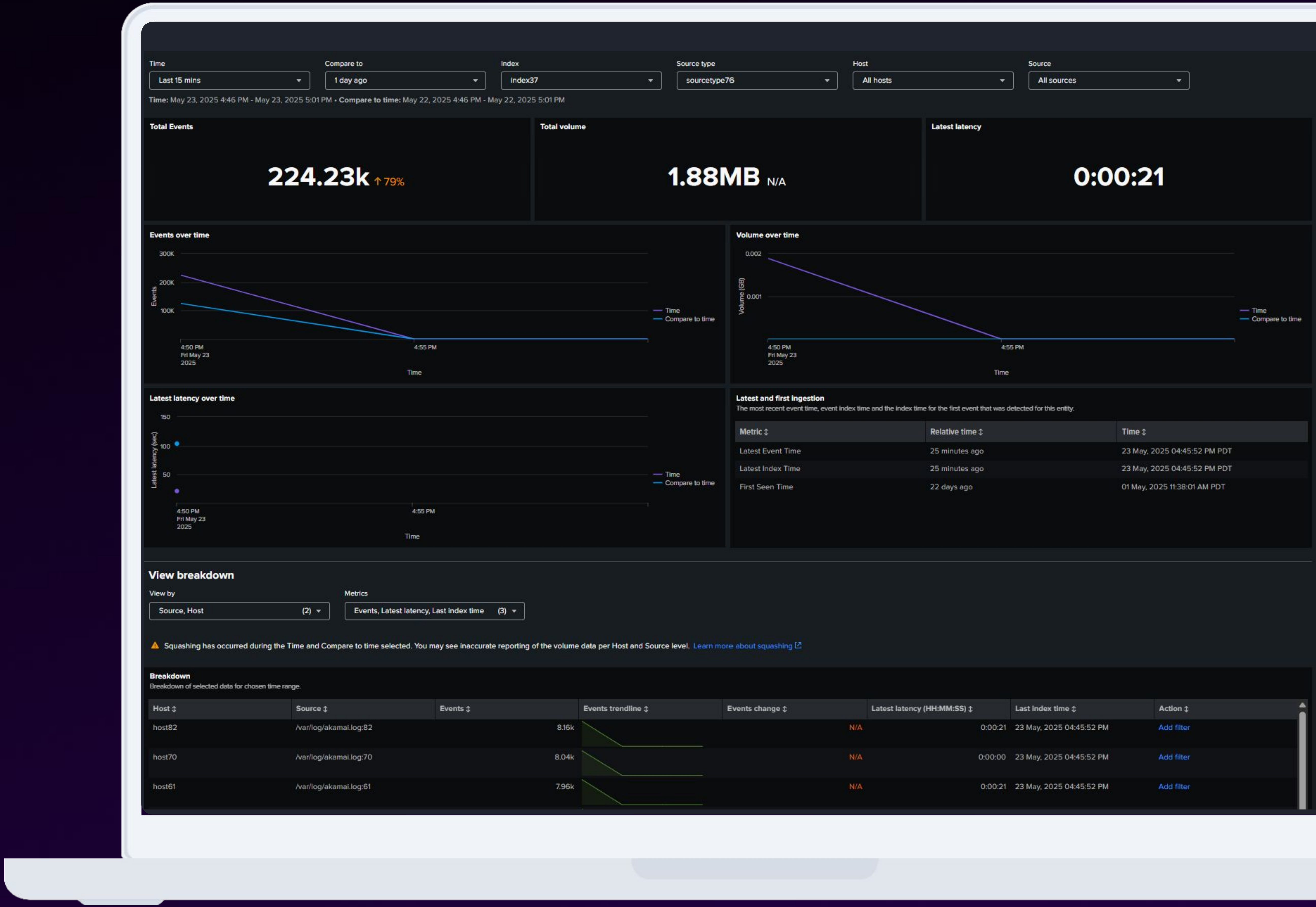
Host Name ↑	System / Architecture	IP Address	DNS Name	Client Name	Agent Type	Version	Status	Check-In	Application Update	Server Classes
hf1	linux-x86_64	172.18.0.3	agent_management-heavy_forwarder-1.agent_management_default	C10FCEB3-D447-415C-8BAF-81133037BB10	Enterprise	9.3.1	✓ Ok	A few seconds ago	A few seconds ago	all europe
ufw1	linux-x86_64	172.18.0.6	agent_management-universal_forwarder_1-1.agent_management_default	0D022C0C-F802-4A87-A2D2-EA2DFCBDCE29	Universal Forwarder	9.3.1	✓ Ok	A few seconds ago	A few seconds ago	all usa
ufw2	linux-x86_64	172.18.0.4	agent_management-universal_forwarder_2-1.agent_management_default	CC981301-72A6-4078-8BAB-9BF71B102B5A	Universal Forwarder	9.2.3	✓ Ok	A few seconds ago	A few seconds ago	all usa
ufw3	linux-x86_64	172.18.0.5	agent_management-universal_forwarder_3-1.agent_management_default	D1CD036A-2C34-416B-BE4A-D362B1BDA646	Universal Forwarder	9.1.6	✓ Ok	A few seconds ago	A few seconds ago	all usa
ufw4	linux-x86_64	172.18.0.2	agent_management-universal_forwarder_4-1.agent_management_default	24DBFEFD-1FFA-41F6-8FFE-1712C93DC2F8	Universal Forwarder	9.0.9	✓ Ok	A few seconds ago	A few seconds ago	all usa

SPLUNK CLOUD PLATFORM

ANNOUNCING

Ingest monitoring

Understand and monitor real-time data movement, including ingestion volumes and latency, to optimize and effectively manage data flows across diverse ingestion pathways.



Time: Last 15 mins
Compare to: 1 day ago
Index: index37
Source type: sourcetype76
Host: All hosts
Source: All sources

Time: May 23, 2025 4:46 PM - May 23, 2025 5:01 PM • **Compare to time:** May 22, 2025 4:46 PM - May 22, 2025 5:01 PM

Total Events: 224.23k ↑ 79%

Total volume: 1.88MB N/A

Latest latency: 0:00:21

Latest and first ingestion

The most recent event time, event index time and the index time for the first event that was detected for this entity.

Metric ↕	Relative time ↕	Time ↕
Latest Event Time	25 minutes ago	23 May, 2025 04:45:52 PM PDT
Latest Index Time	25 minutes ago	23 May, 2025 04:45:52 PM PDT
First Seen Time	22 days ago	01 May, 2025 11:38:01 AM PDT

View breakdown

View by: Source, Host (2)
Metrics: Events, Latest latency, Last index time (3)

⚠ Squashing has occurred during the Time and Compare to time selected. You may see inaccurate reporting of the volume data per Host and Source level. Learn more about squashing

Breakdown

Breakdown of selected data for chosen time range.

Host ↕	Source ↕	Events ↕	Events trendline ↕	Events change ↕	Latest latency (HH:MM:SS) ↕	Last index time ↕	Action ↕
host82	/var/log/akamai.log:82	8.16k		N/A	0:00:21	23 May, 2025 04:45:52 PM	Add filter
host70	/var/log/akamai.log:70	8.04k		N/A	0:00:00	23 May, 2025 04:45:52 PM	Add filter
host61	/var/log/akamai.log:61	7.96k		N/A	0:00:21	23 May, 2025 04:45:52 PM	Add filter