Cisco webinar Splunk

28. květen 2024

Petr Slačík
Sr. Sales Engineer - GSS

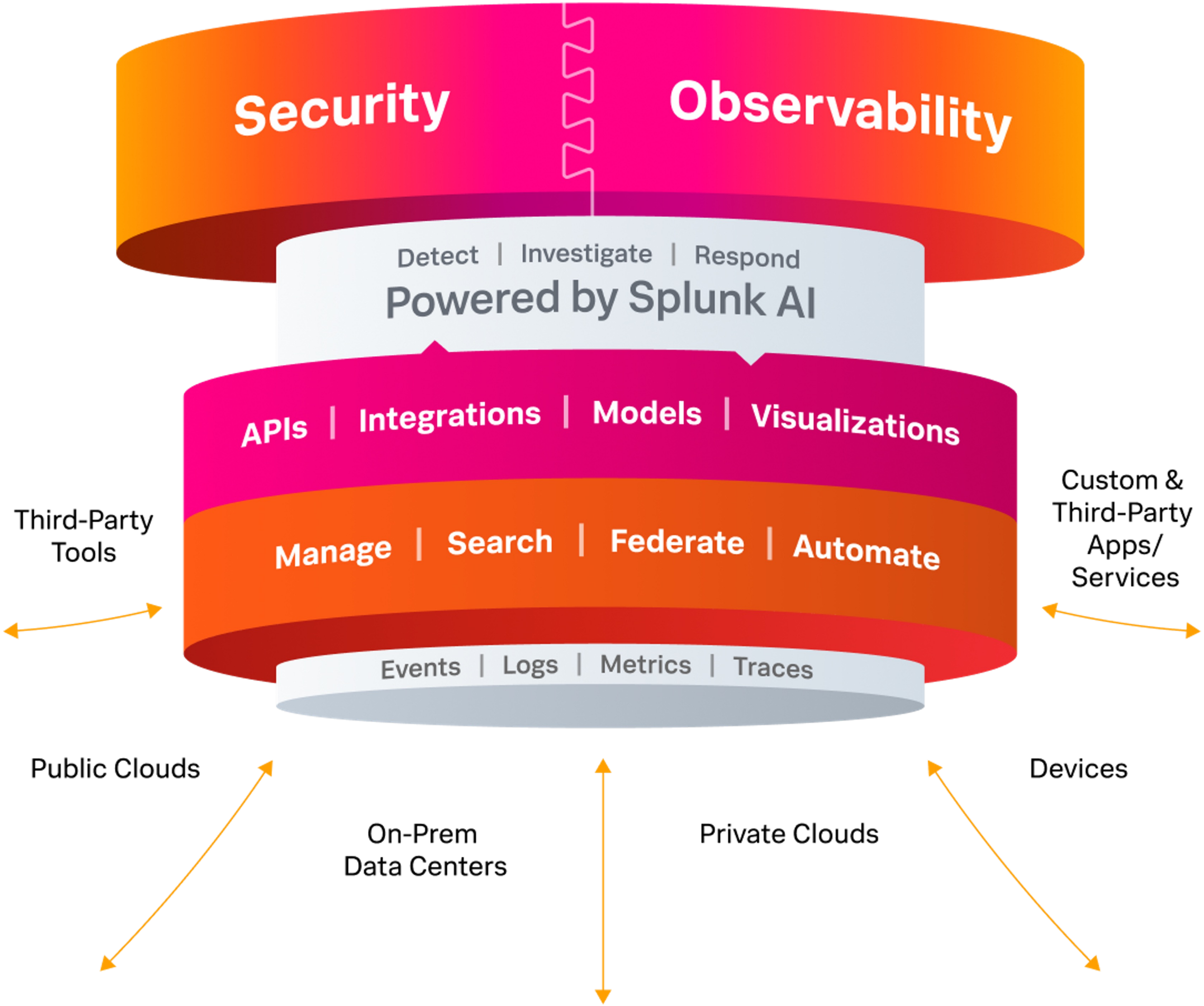
splunk>
a CISCO company

Agenda

- Intro
- Core - Splunk Enterprise
- Core - Splunk Cloud
- Splunk Apps
- Security
- Splunk O11y Cloud
- Splunk AI
- DEMO
- Q & A

Intro
Splunk

The Unified Security and Observability Platform


Security
Observability
Detect | Investigate | Respond
Powered by Splunk AI
APIs | Integrations | Models | Visualizations
Manage | Search | Federate | Automate
Events | Logs | Metrics | Traces
Third-Party Tools
Custom & Third-Party Apps/ Services
Public Clouds
On-Prem Data Centers
Private Clouds
Devices

Splunk is the only vendor recognized as a leader in the latest Magic Quadrant™ Reports for SIEM and APM and Observability.

Gartner

A Leader

Gartner® Magic Quadrant™ for Security Information and Event Management

A Leader

Gartner® Magic Quadrant™ for APM and Observability

Gartner, Magic Quadrant for Security Information and Event Management, October 2022

Gartner, Magic Quadrant for Application Performance Monitoring and Observability, July 2023

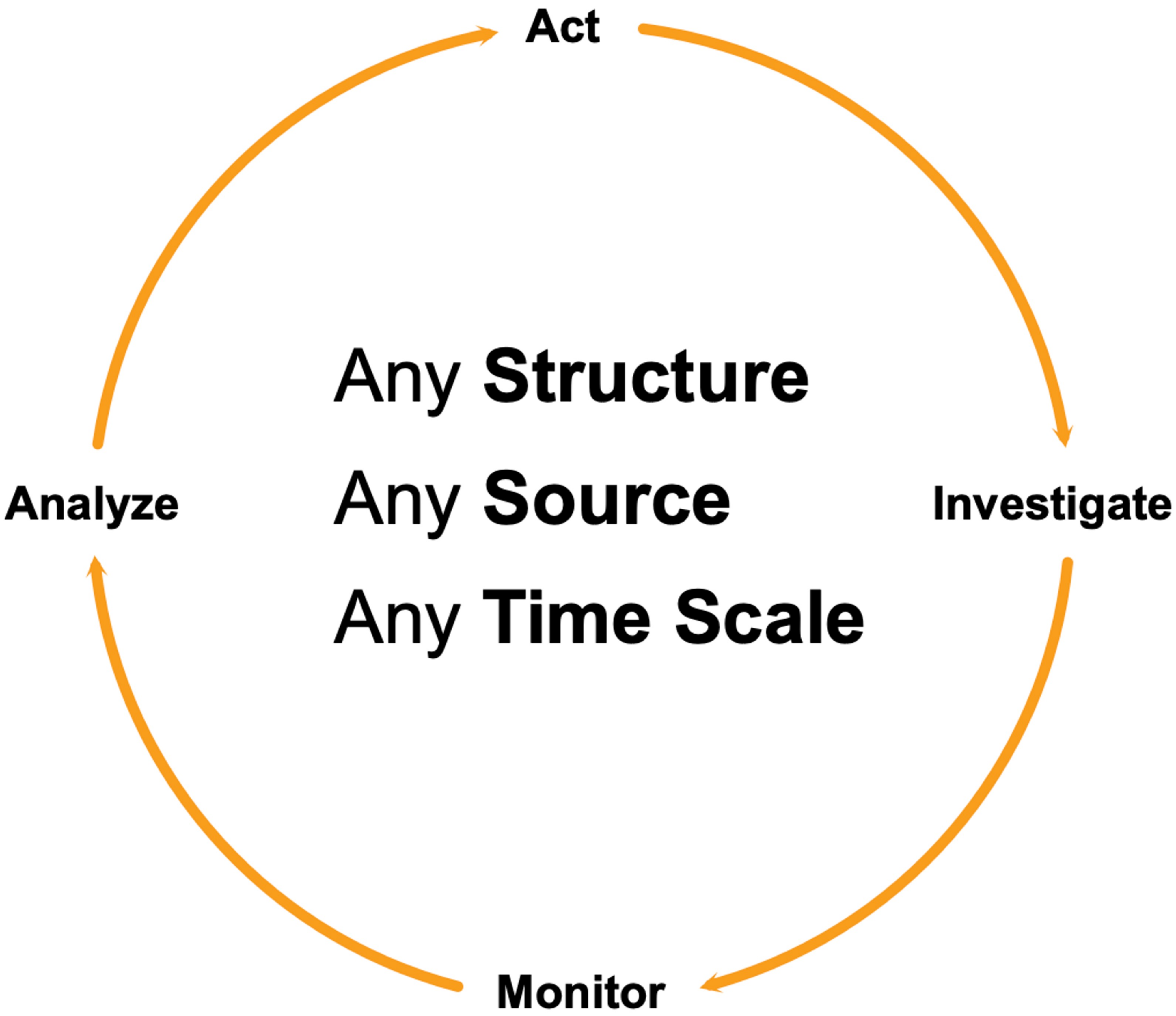
The Gartner documents are available upon request from Splunk. Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates and are used herein with permission.
All rights reserved.

Core
Splunk Enterprise

splunk>

The Data-to-Everything Platform



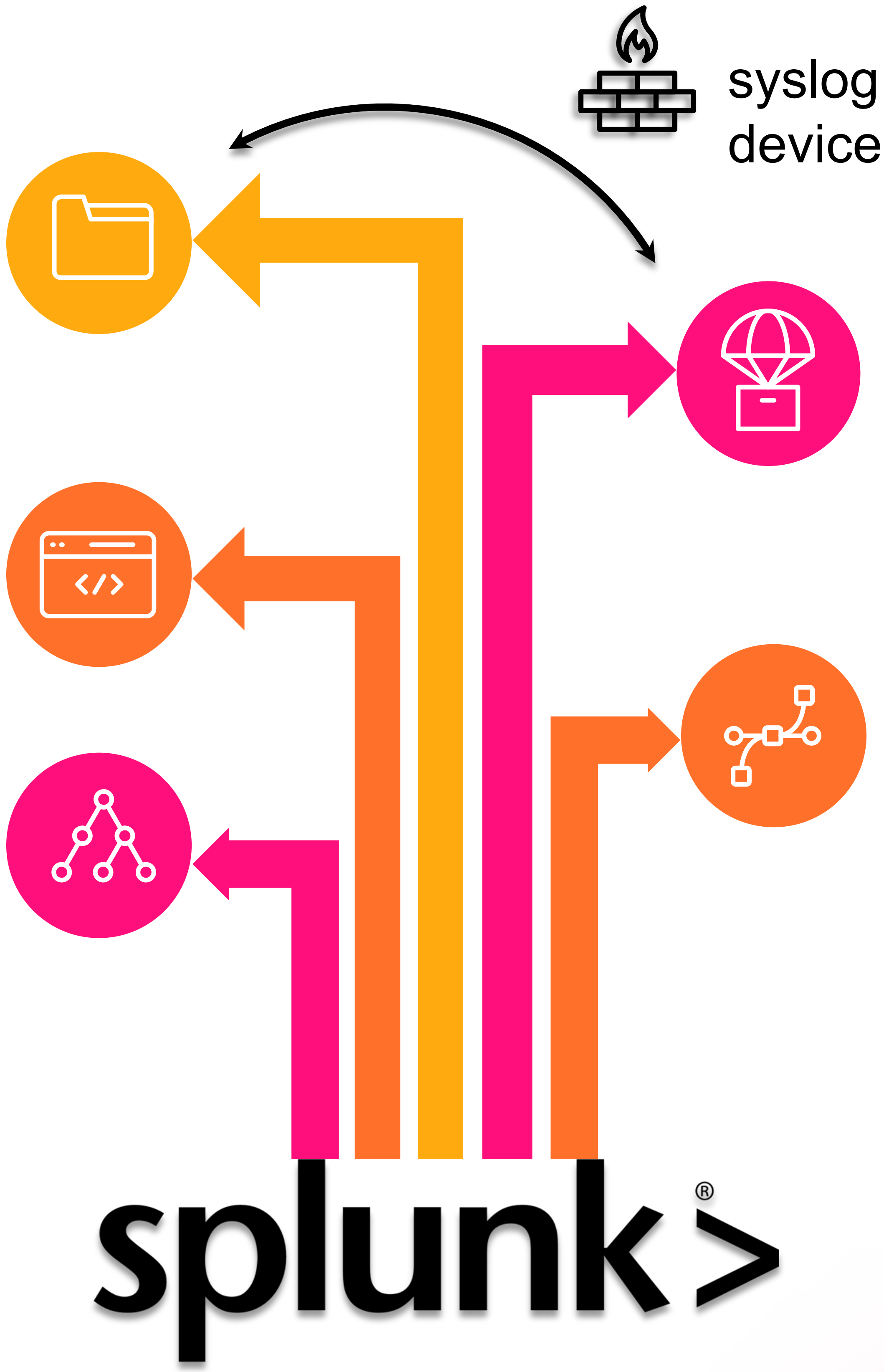
Any **Structure**

Any **Source**

Any **Time Scale**

splunk> turn data into doing™

What Can Splunk Ingest?



Local File Monitoring

- Universal Forwarder

Aggregated / API Sources

- Heavy Forwarder

Event Logs, Active Directory, OS Stats, Unix/Linux/ Windows Hosts

- Universal Forwarder

syslog hosts & network devices

DevOps, IoT, Containers

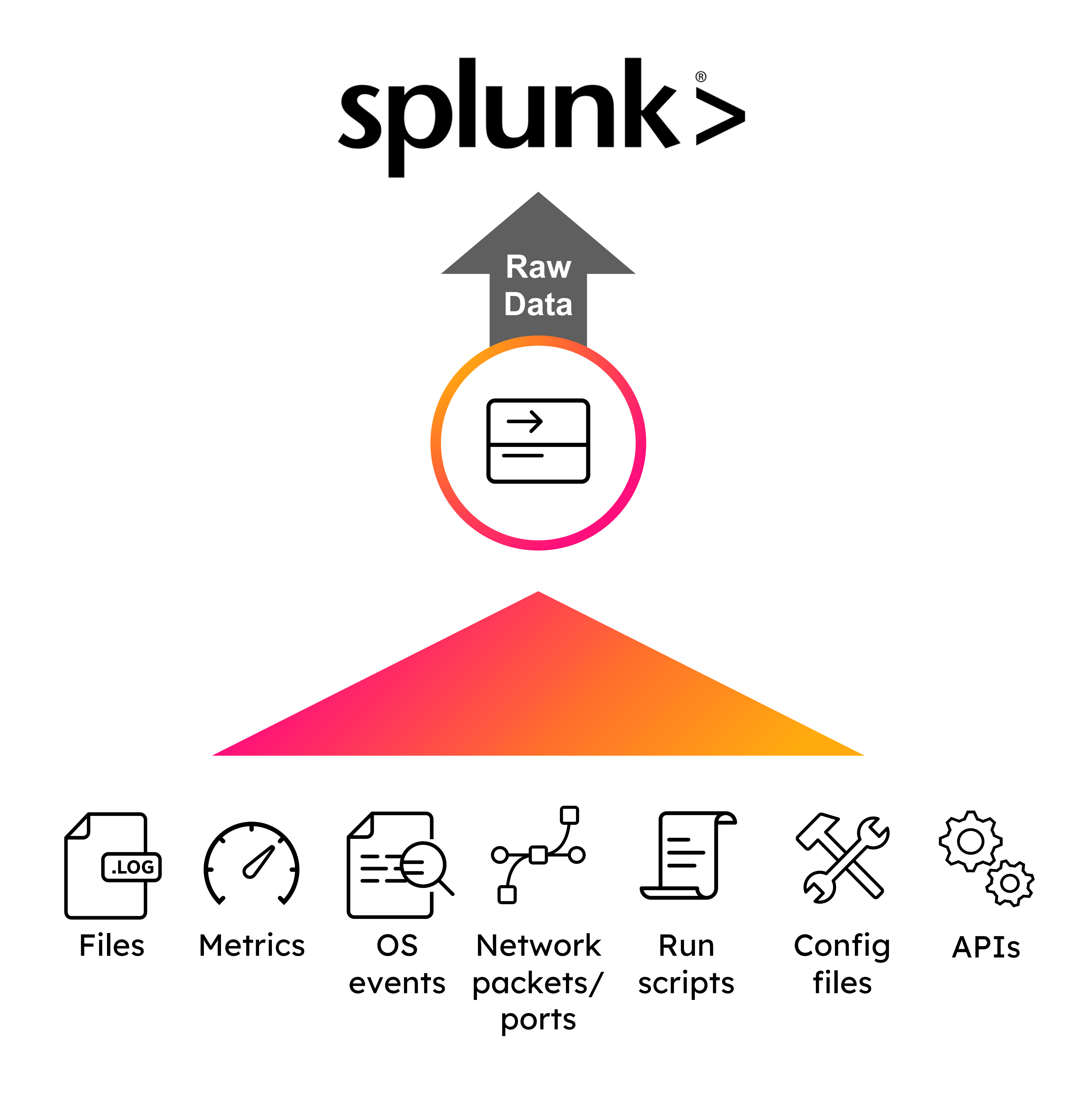
- HTTP Event Collector (HEC)
- Agentless

Wire Data

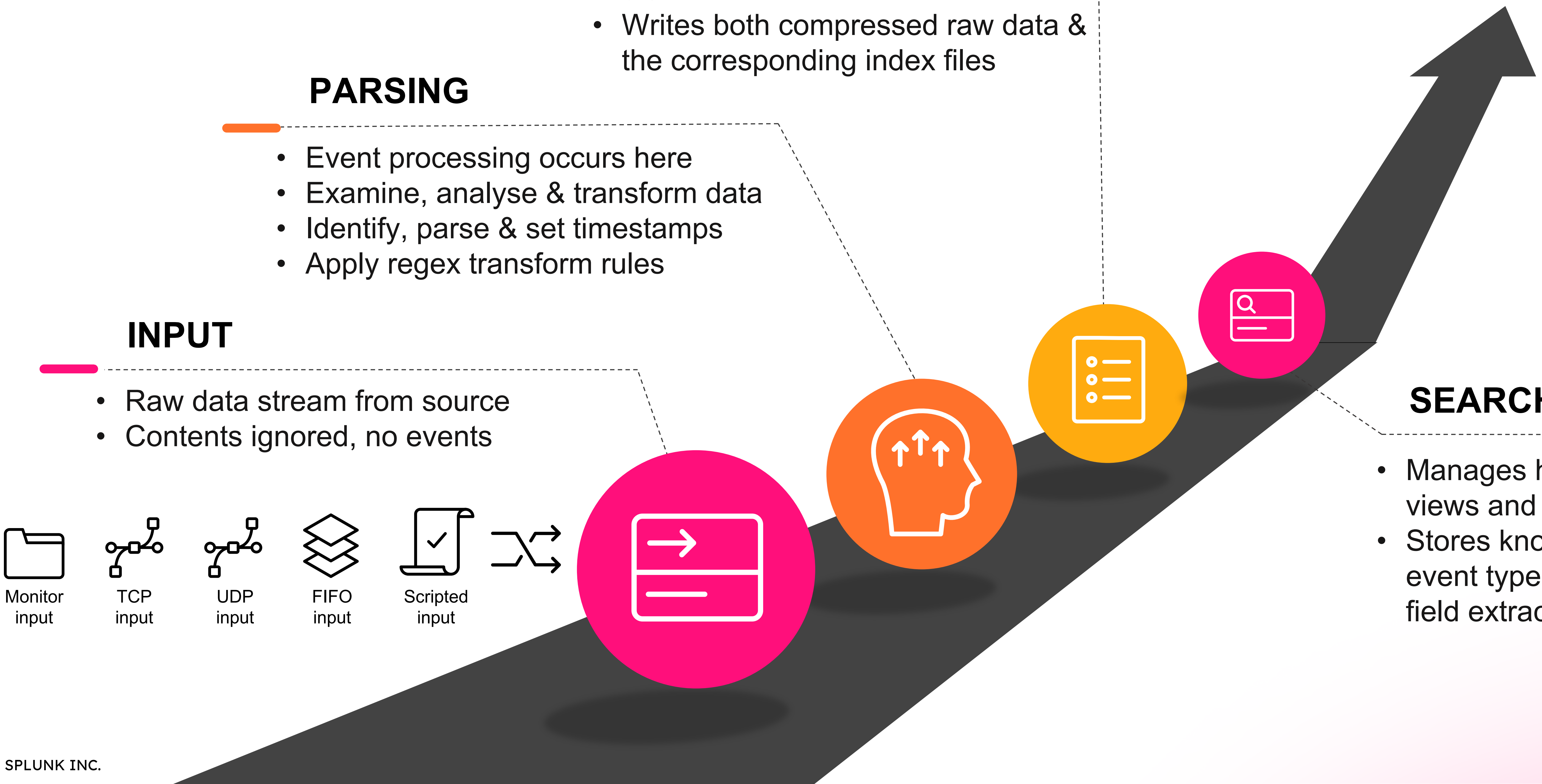
- via Splunk Stream
- HTTP Event Collector (HEC) or Universal Forwarder

What is a Splunk Universal Forwarder?

- **Reliable** collection of data from remote locations
- Includes **methods** for collecting from a variety of data sources
- **Lightweight** but powerful:
  - Buffering / guaranteed delivery
  - Encryption
  - Compression
  - Load balancing
  - And more!
- Very **small footprint**
- **Just forwards** data – no parsing beforehand!



How Data Moves Through Splunk



INPUT

- Raw data stream from source
- Contents ignored, no events

PARSING

- Event processing occurs here
- Examine, analyse & transform data
- Identify, parse & set timestamps
- Apply regex transform rules

INDEXING

- Parsed events written to index on disk
- Writes both compressed raw data & the corresponding index files

SEARCH

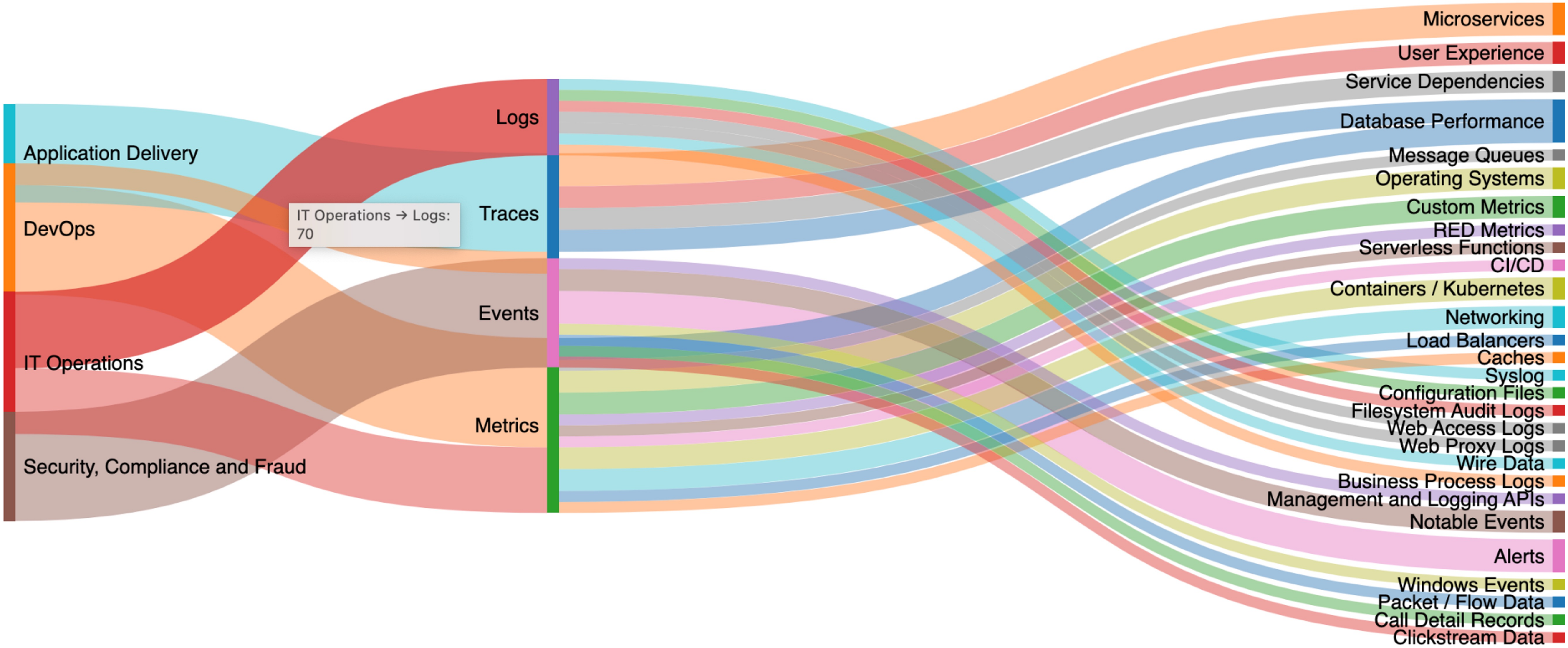
- Manages how the user accesses, views and searches the indexed data
- Stores knowledge objects: reports, event types, dashboards, alerts and field extractions

DATA RETENTION

- Buckets: **HOT**, **WARM**, **COLD**, **FROZEN** and **THAWED**
- Cloud: Smart Store, Active Archive

Multiple Use Cases On Common Data

Drives system security and observability



Core Splunk Cloud

Splunk as a Service

Fastest time to value | Minimum Infrastructure | Maximum Value

3 Simple Steps:

1. Onboard data
2. Onboard users
3. Get value from your data

splunk>cloud

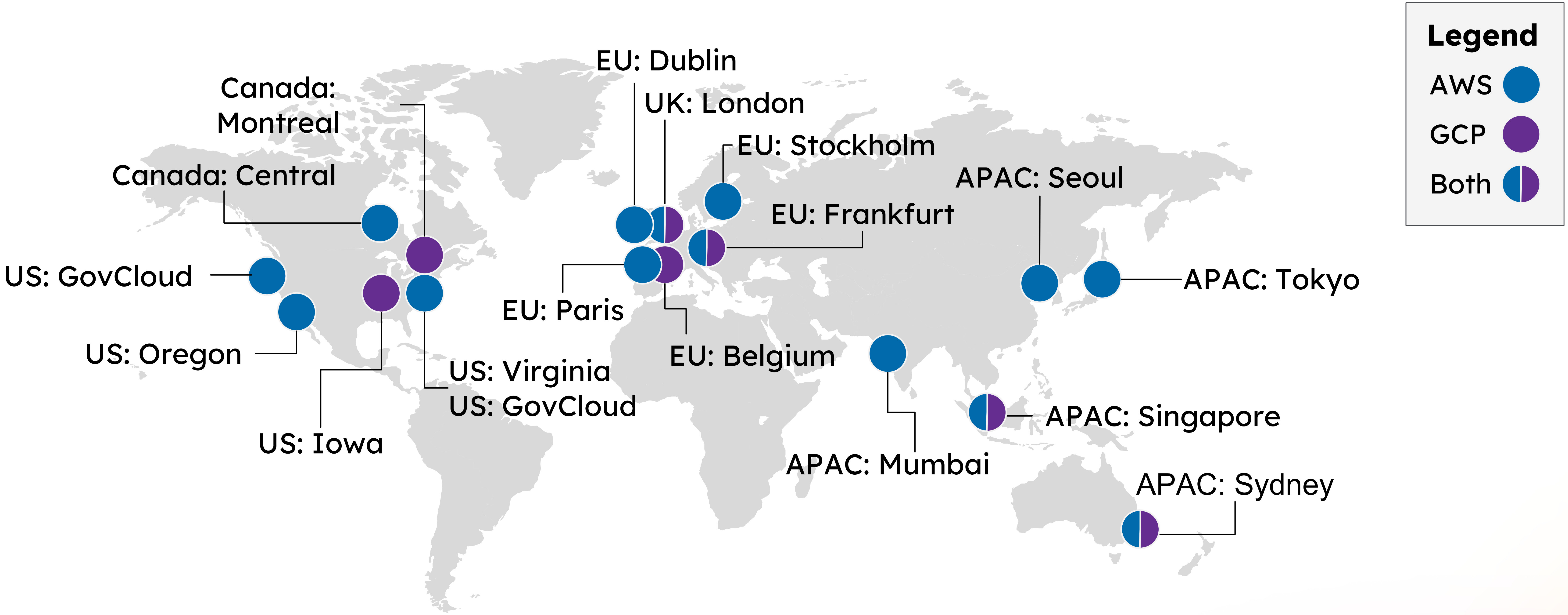
- **Fastest time to value**
- **Software as a service** - AWS or GCP
- **Secure** - ISO 27001, SOC 2 Type II, PCI DSS, HIPAA, FedRAMP Moderate, DoD IL5, IRAP
- **Encryption-in-transit** - plus optional encryption-at-rest
- **Resilient infrastructure**
- **100% uptime guarantee**
- **24/7 NOC/SOC support team**

Flexible options for data collection and forwarding

- Wire Data
- API
- SDKs
- HTTP
- TCP/UDP
- RDBMS
- Containers
- Apps
- Cloud Services
- OpenTelemetry
- Splunk Forwarders

Splunk Cloud Service Description: https://splk.it/SplunkCloudServDesc

Splunk Cloud Regions on AWS & GCP



Splunk Apps

Splunkbase

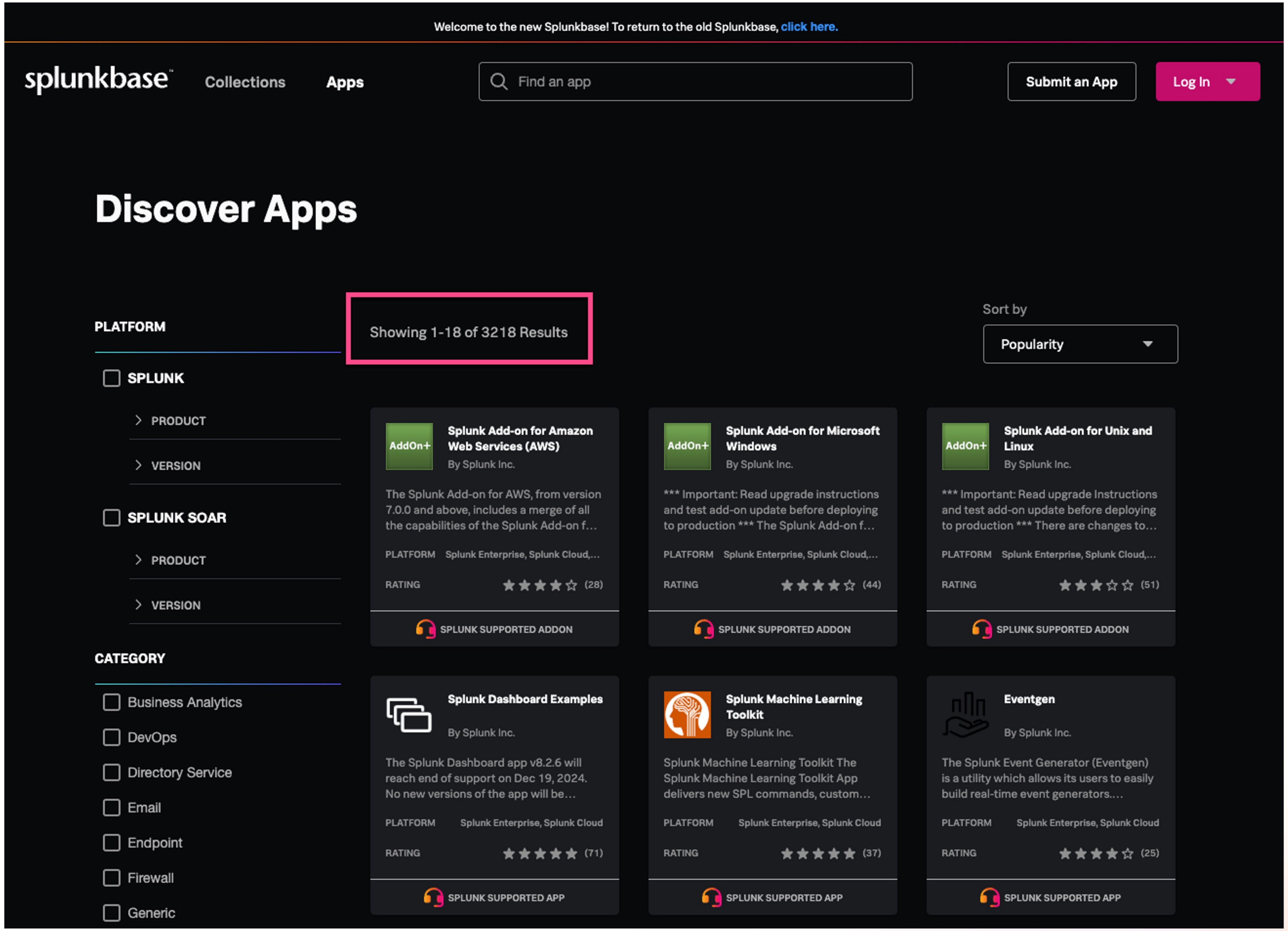
Splunk App Store Portal

Splunk Application

- Unified structure
- Extension to Splunk capabilities
- Vetted before submission!

App purpose

- Search-time parsing
- Index-time parsing
- Modular input
- Alert actions
- Custom visualizations
- Reports, Dashboards



Welcome to the new Splunkbase! To return to the old Splunkbase, click here.

Discover Apps

Showing 1-18 of 3218 Results

Sort by: Popularity

PLATFORM

- □ SPLUNK
  - PRODUCT
  - VERSION
- □ SPLUNK SOAR
  - PRODUCT
  - VERSION

CATEGORY

- □ Business Analytics
- □ DevOps
- □ Directory Service
- □ Email
- □ Endpoint
- □ Firewall
- □ Generic

Splunk Add-on for Amazon Web Services (AWS)
By Splunk Inc.
The Splunk Add-on for AWS, from version 7.0.0 and above, includes a merge of all the capabilities of the Splunk Add-on f…
PLATFORM Splunk Enterprise, Splunk Cloud,…
RATING ★★★★☆ (28)
SPLUNK SUPPORTED ADDON

Splunk Add-on for Microsoft Windows
By Splunk Inc.
*** Important: Read upgrade instructions and test add-on update before deploying to production *** The Splunk Add-on f…
PLATFORM Splunk Enterprise, Splunk Cloud,…
RATING ★★★★☆ (44)
SPLUNK SUPPORTED ADDON

Splunk Add-on for Unix and Linux
By Splunk Inc.
*** Important: Read upgrade Instructions and test add-on update before deploying to production *** There are changes to…
PLATFORM Splunk Enterprise, Splunk Cloud,…
RATING ★★★☆☆ (51)
SPLUNK SUPPORTED ADDON

Splunk Dashboard Examples
By Splunk Inc.
The Splunk Dashboard app v8.2.6 will reach end of support on Dec 19, 2024. No new versions of the app will be…
PLATFORM Splunk Enterprise, Splunk Cloud
RATING ★★★★★ (71)
SPLUNK SUPPORTED APP

Splunk Machine Learning Toolkit
By Splunk Inc.
Splunk Machine Learning Toolkit The Splunk Machine Learning Toolkit App delivers new SPL commands, custom…
PLATFORM Splunk Enterprise, Splunk Cloud
RATING ★★★★★ (37)
SPLUNK SUPPORTED APP

Eventgen
By Splunk Inc.
The Splunk Event Generator (Eventgen) is a utility which allows its users to easily build real-time event generators.…
PLATFORM Splunk Enterprise, Splunk Cloud
RATING ★★★★☆ (25)
SPLUNK SUPPORTED APP

https://apps.splunk.com

Splunk Apps

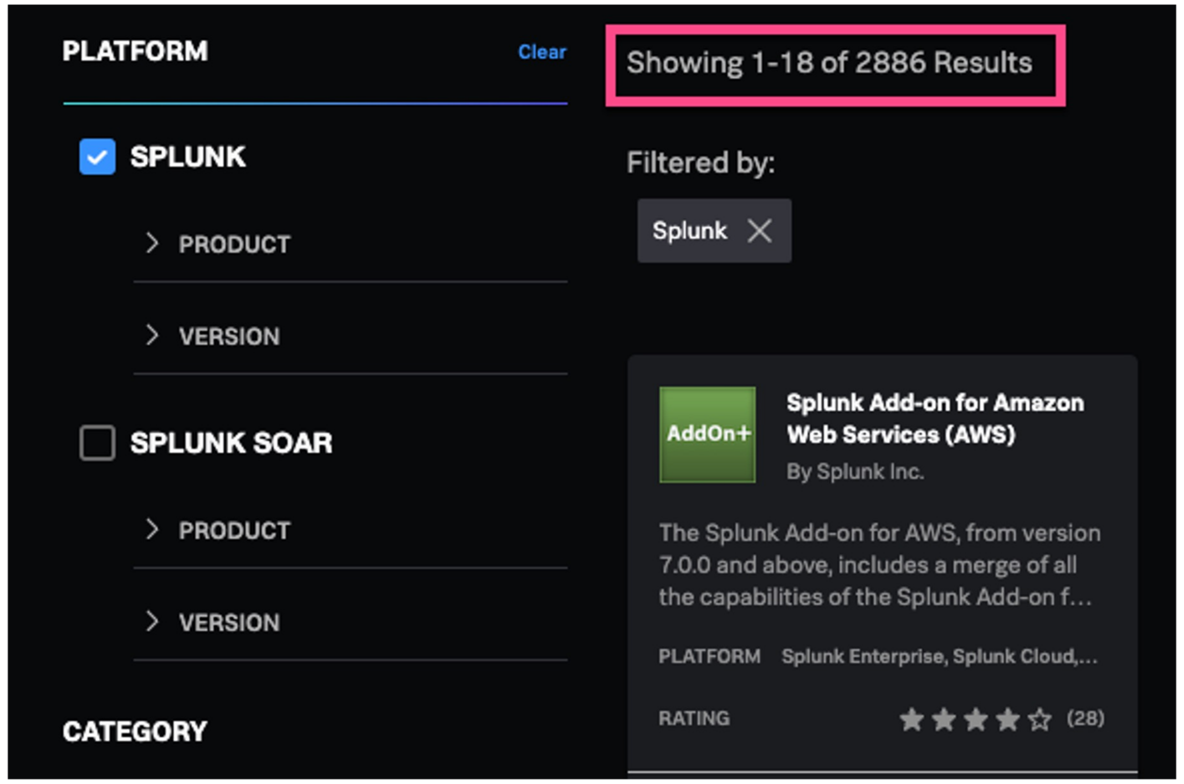
Apps support

- Splunk | Splunk Cloud
- Splunk SOAR

Where to install on Splunk?

- Any Splunk core node
- Splunk HF
- Splunk UF
- Splunk Cloud
  - private apps must be vetted!

Splunk Core (2886)



PLATFORM Clear

☑ SPLUNK

> PRODUCT

> VERSION

□ SPLUNK SOAR

> PRODUCT

> VERSION

CATEGORY

Showing 1-18 of 2886 Results

Filtered by:

Splunk ✕

AddOn+

Splunk Add-on for Amazon Web Services (AWS)

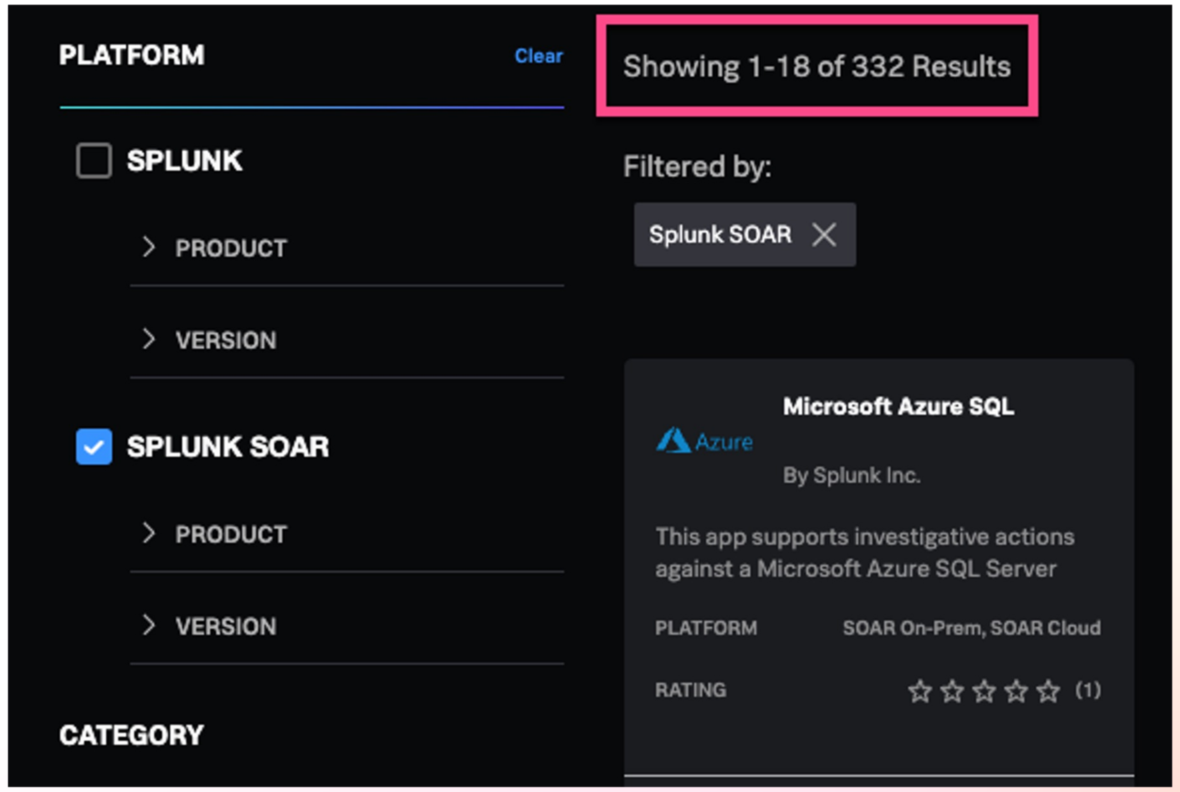
By Splunk Inc.

The Splunk Add-on for AWS, from version 7.0.0 and above, includes a merge of all the capabilities of the Splunk Add-on f...

PLATFORM Splunk Enterprise, Splunk Cloud,...

RATING ★★★★☆ (28)

Splunk SOAR (332)



PLATFORM Clear

□ SPLUNK

> PRODUCT

> VERSION

☑ SPLUNK SOAR

> PRODUCT

> VERSION

CATEGORY

Showing 1-18 of 332 Results

Filtered by:

Splunk SOAR ✕

Azure

Microsoft Azure SQL

By Splunk Inc.

This app supports investigative actions against a Microsoft Azure SQL Server

PLATFORM SOAR On-Prem, SOAR Cloud

RATING ☆☆☆☆☆ (1)

Splunk Security

Splunk Security Portfolio

DATA

splunk> cloud

splunk> enterprise

ANALYTICS

splunk>
Security Essentials

InfoSec App for Splunk

Splunk Enterprise Security™

ES CONTENT UPDATE

Splunk User Behavior Analytics™

Machine Learning Toolkit (MLTK)

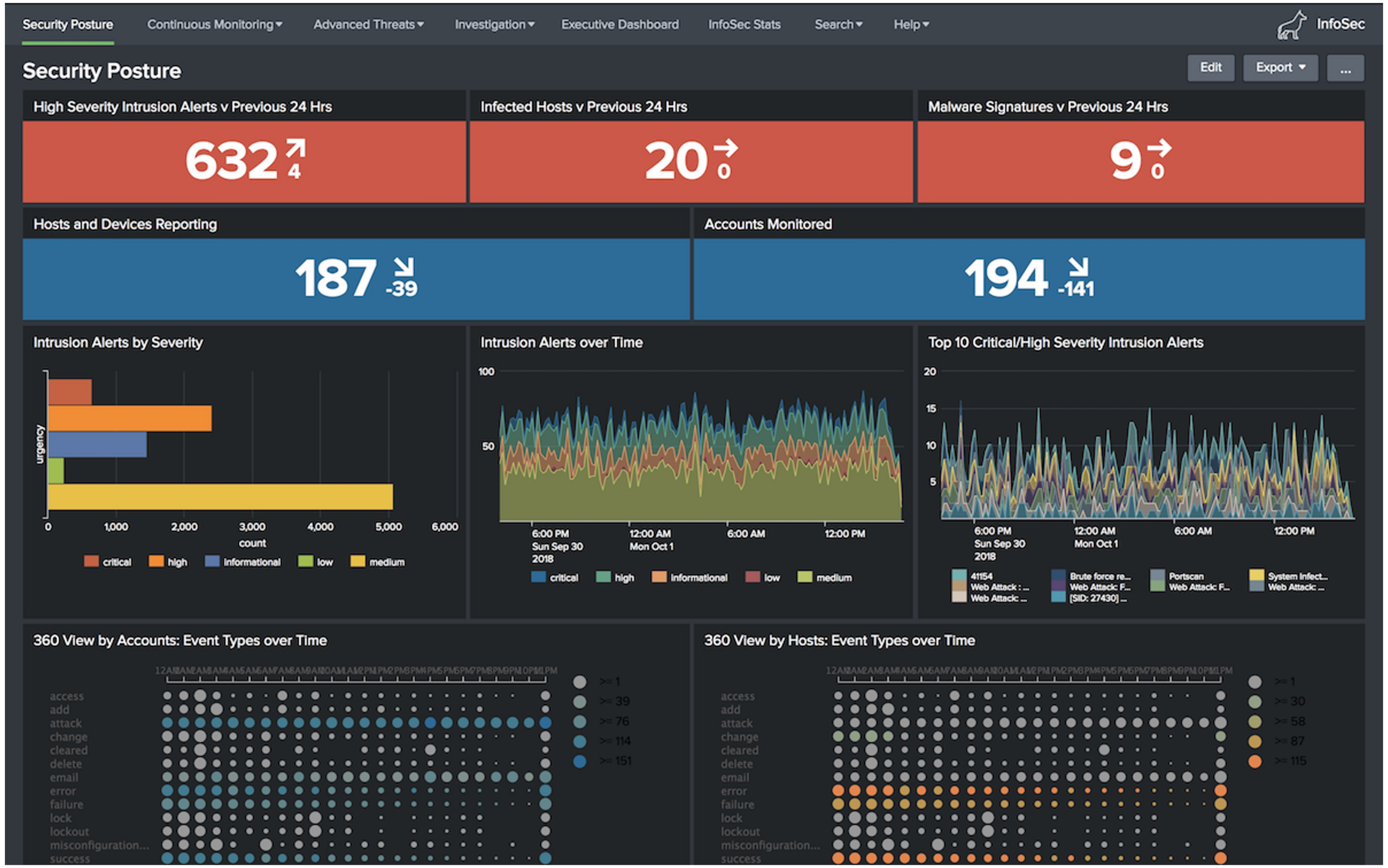
OPERATIONS

splunk>
SOAR

Splunk Enterprise Security™

ADAPTIVE RESPONSE

Splunk InfoSec App

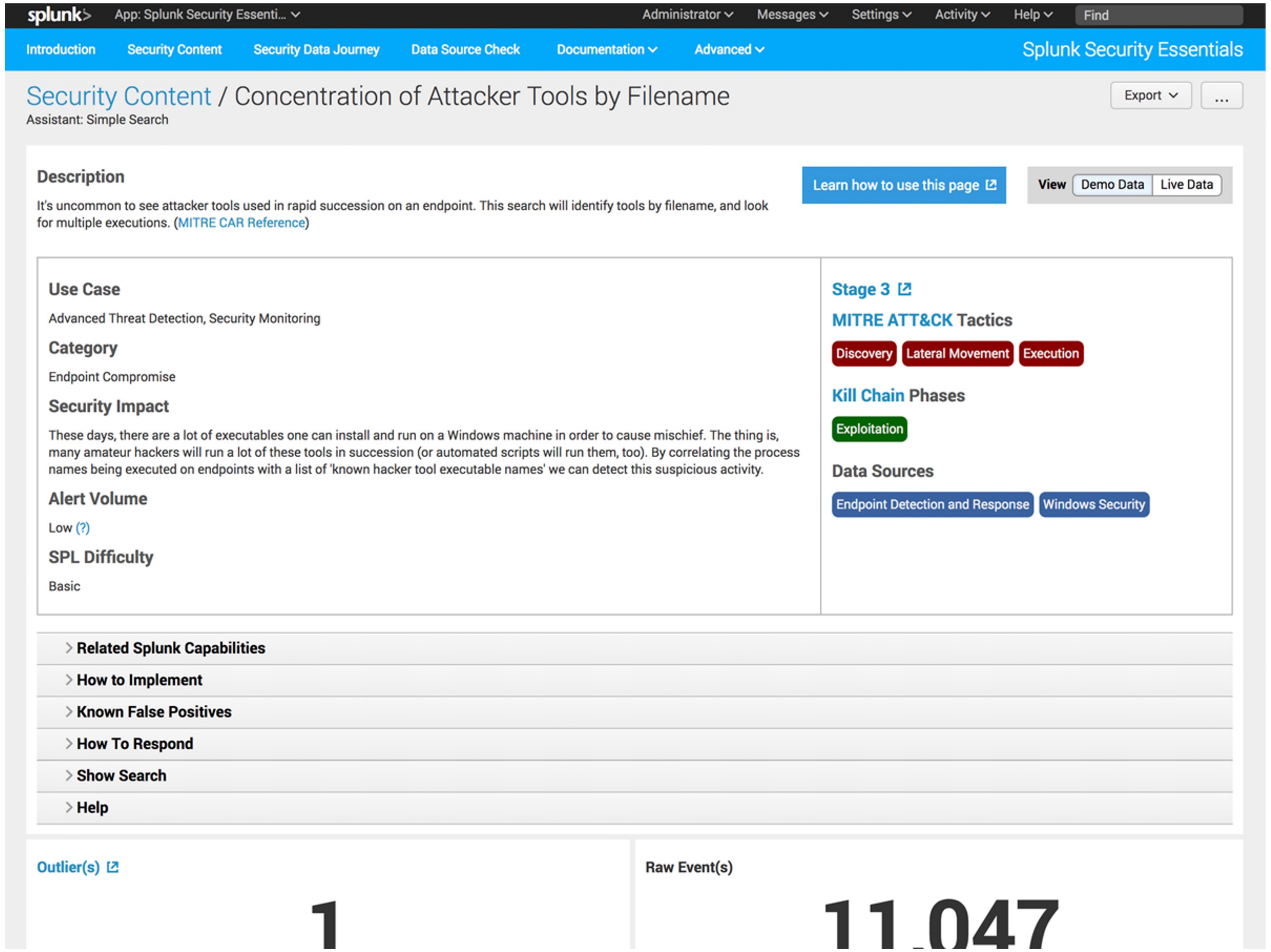


The app uses the most common security data sources to quickly get most value out of Splunk

- Firewall & Network
- Authentication (AD)
- Antivirus & Malware
- Endpoint data

https://splunk-infosec-documentation.readthedocs.io/en/latest/
https://splunkbase.splunk.com/app/4240/

Splunk Security Essentials (SSE)



Security Content / Concentration of Attacker Tools by Filename

Assistant: Simple Search

Description

It's uncommon to see attacker tools used in rapid succession on an endpoint. This search will identify tools by filename, and look for multiple executions. (MITRE CAR Reference)

Use Case

Advanced Threat Detection, Security Monitoring

Category

Endpoint Compromise

Security Impact

These days, there are a lot of executables one can install and run on a Windows machine in order to cause mischief. The thing is, many amateur hackers will run a lot of these tools in succession (or automated scripts will run them, too). By correlating the process names being executed on endpoints with a list of 'known hacker tool executable names' we can detect this suspicious activity.

Alert Volume

Low (?)

SPL Difficulty

Basic

Stage 3

MITRE ATT&CK Tactics

Discovery Lateral Movement Execution

Kill Chain Phases

Exploitation

Data Sources

Endpoint Detection and Response Windows Security

- Related Splunk Capabilities
- How to Implement
- Known False Positives
- How To Respond
- Show Search
- Help

Outlier(s)

1

Raw Event(s)

11,047

Provides recommendations to guide you through your security maturity journey

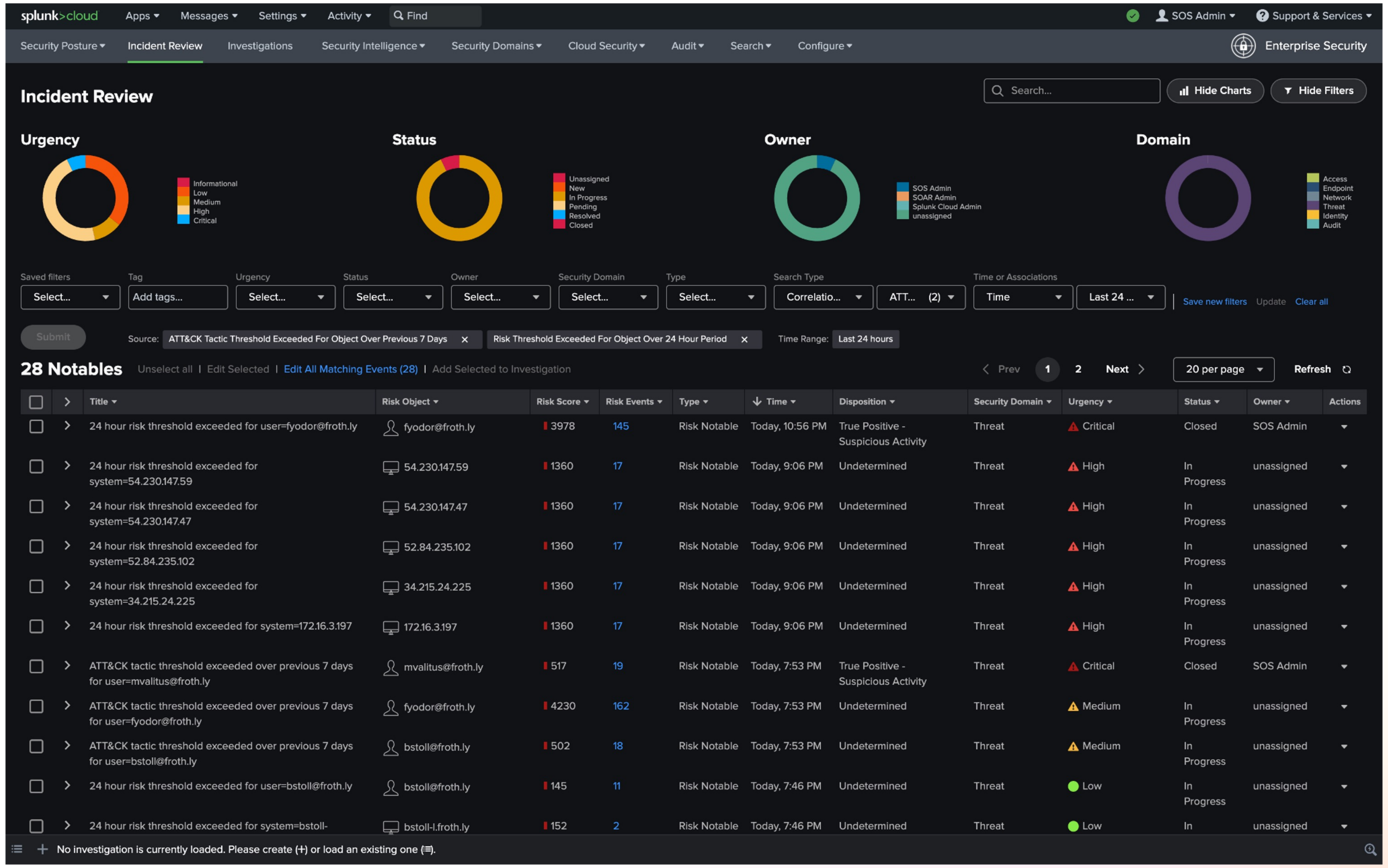
- 1300+ pre-built security detections and analytic stories
- mapping security data to MITRE ATT&CK and Cyber Kill Chain frameworks
- learn what use cases you can run with the data you are already collecting

https://docs.splunksecurityessentials.com/
https://splunkbase.splunk.com/app/3435/

Splunk Enterprise Security (ES)

Splunk ES provides the security practitioner with visibility into security-relevant threats:

- it is built on the Splunk core platform and uses the search and correlation capabilities
- users can capture, monitor, and report on data from security devices, systems, and applications
- security analysts can quickly investigate and resolve the security threats across the access, endpoint, and network protection domains.



Source: ATT&CK Tactic Threshold Exceeded For Object Over Previous 7 Days × | Risk Threshold Exceeded For Object Over 24 Hour Period × | Time Range: Last 24 hours

28 Notables Unselect all | Edit Selected | Edit All Matching Events (28) | Add Selected to Investigation

Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
24 hour risk threshold exceeded for user=fyodor@froth.ly	fyodor@froth.ly	3978	145	Risk Notable	Today, 10:56 PM	True Positive - Suspicious Activity	Threat	Critical	Closed	SOS Admin	▾
24 hour risk threshold exceeded for system=54.230.147.59	54.230.147.59	1360	17	Risk Notable	Today, 9:06 PM	Undetermined	Threat	High	In Progress	unassigned	▾
24 hour risk threshold exceeded for system=54.230.147.47	54.230.147.47	1360	17	Risk Notable	Today, 9:06 PM	Undetermined	Threat	High	In Progress	unassigned	▾
24 hour risk threshold exceeded for system=52.84.235.102	52.84.235.102	1360	17	Risk Notable	Today, 9:06 PM	Undetermined	Threat	High	In Progress	unassigned	▾
24 hour risk threshold exceeded for system=34.215.24.225	34.215.24.225	1360	17	Risk Notable	Today, 9:06 PM	Undetermined	Threat	High	In Progress	unassigned	▾
24 hour risk threshold exceeded for system=172.16.3.197	172.16.3.197	1360	17	Risk Notable	Today, 9:06 PM	Undetermined	Threat	High	In Progress	unassigned	▾
ATT&CK tactic threshold exceeded over previous 7 days for user=mvalitus@froth.ly	mvalitus@froth.ly	517	19	Risk Notable	Today, 7:53 PM	True Positive - Suspicious Activity	Threat	Critical	Closed	SOS Admin	▾
ATT&CK tactic threshold exceeded over previous 7 days for user=fyodor@froth.ly	fyodor@froth.ly	4230	162	Risk Notable	Today, 7:53 PM	Undetermined	Threat	Medium	In Progress	unassigned	▾
ATT&CK tactic threshold exceeded over previous 7 days for user=bstoll@froth.ly	bstoll@froth.ly	502	18	Risk Notable	Today, 7:53 PM	Undetermined	Threat	Medium	In Progress	unassigned	▾
24 hour risk threshold exceeded for user=bstoll@froth.ly	bstoll@froth.ly	145	11	Risk Notable	Today, 7:46 PM	Undetermined	Threat	Low	In Progress	unassigned	▾
24 hour risk threshold exceeded for system=bstoll-	bstoll-l.froth.ly	152	2	Risk Notable	Today, 7:46 PM	Undetermined	Threat	Low	In	unassigned	▾

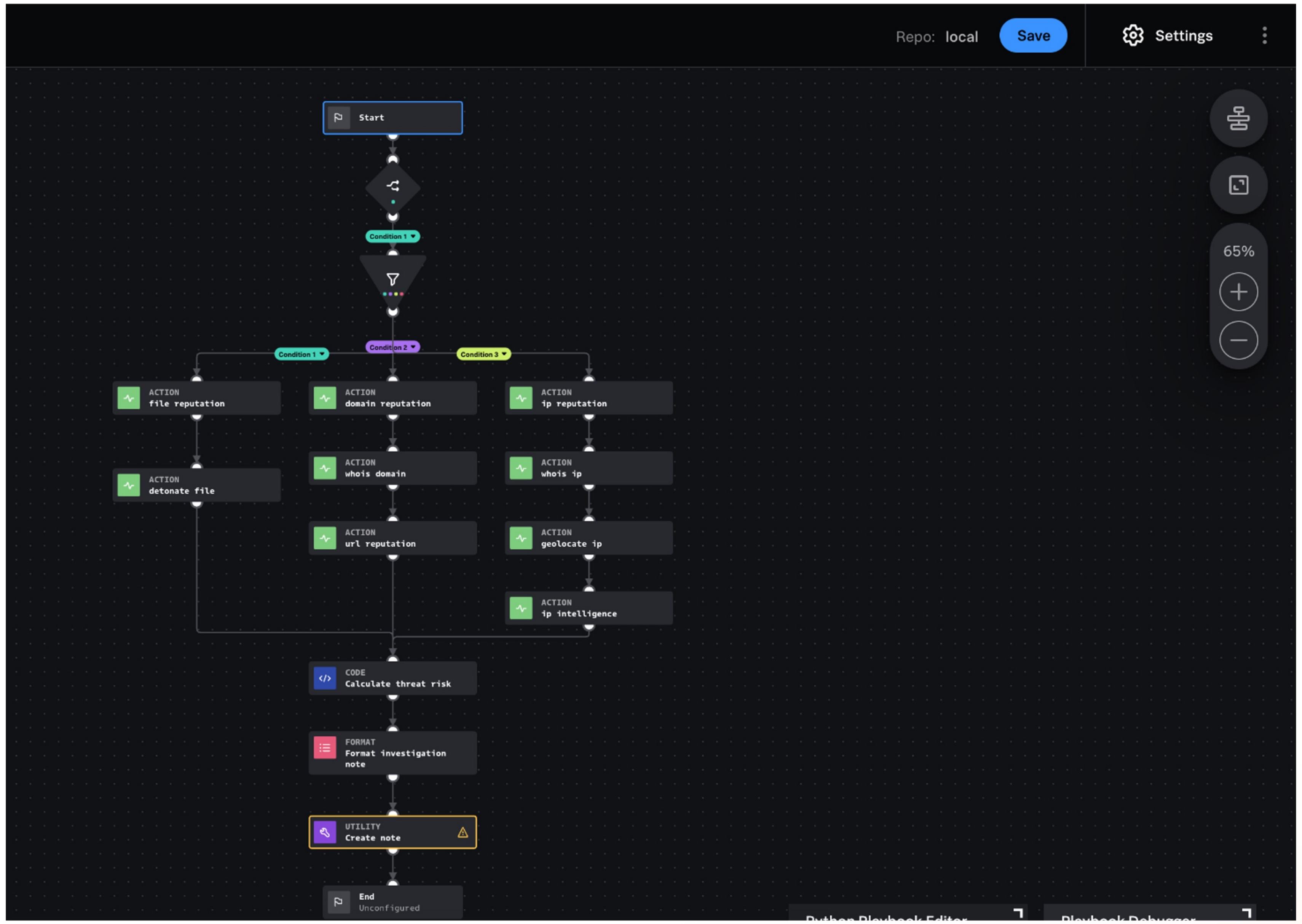
No investigation is currently loaded. Please create (+) or load an existing one (≡).

https://docs.splunk.com/Documentation/ES

Splunk SOAR

Splunk SOAR combines security infrastructure orchestration, playbook automation, and case management capabilities:

- help you orchestrate security workflows
- automate repetitive security tasks
- quickly respond to threats
- access and run actions that are provided by the third-party technologie

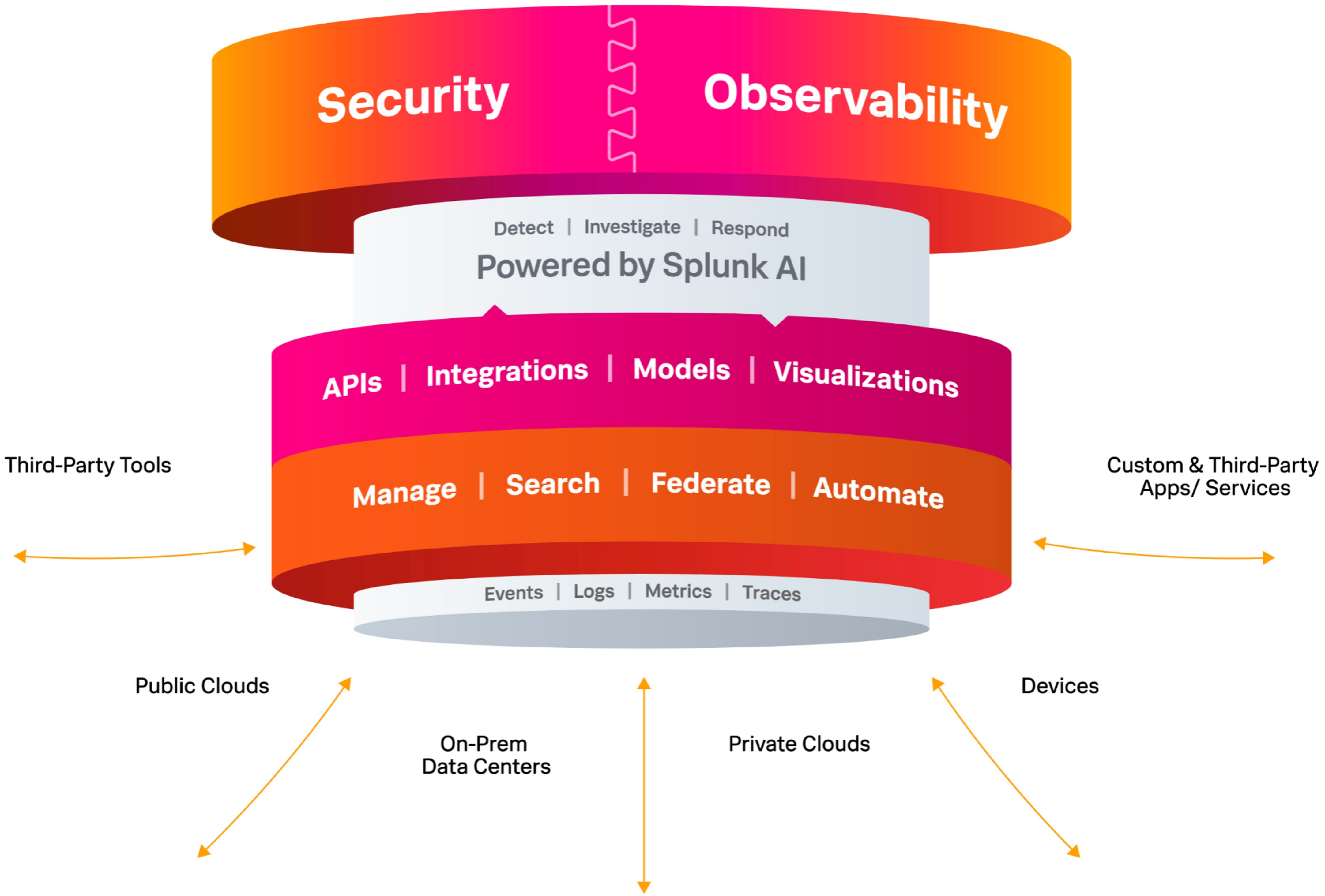


https://docs.splunk.com/Documentation/SOAR

Splunk Observability

The Unified Security and Observability Platform

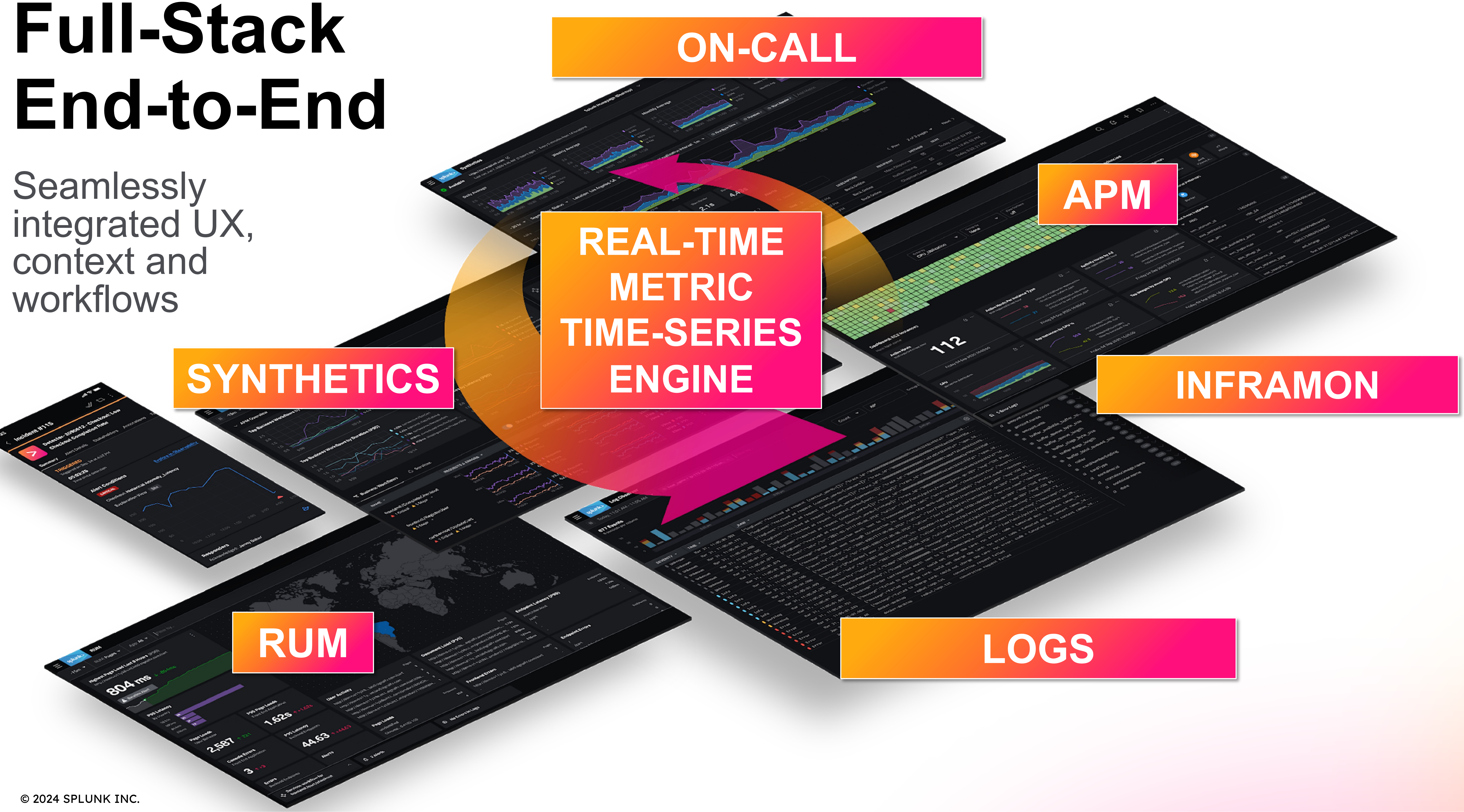
The foundation for Digital Resilience



Security
Observability
Detect | Investigate | Respond
Powered by Splunk AI
APIs | Integrations | Models | Visualizations
Manage | Search | Federate | Automate
Events | Logs | Metrics | Traces
Third-Party Tools
Custom & Third-Party Apps/ Services
Public Clouds
Devices
On-Prem Data Centers
Private Clouds

Full-Stack End-to-End

Seamlessly integrated UX, context and workflows



ON-CALL

APM

REAL-TIME METRIC TIME-SERIES ENGINE

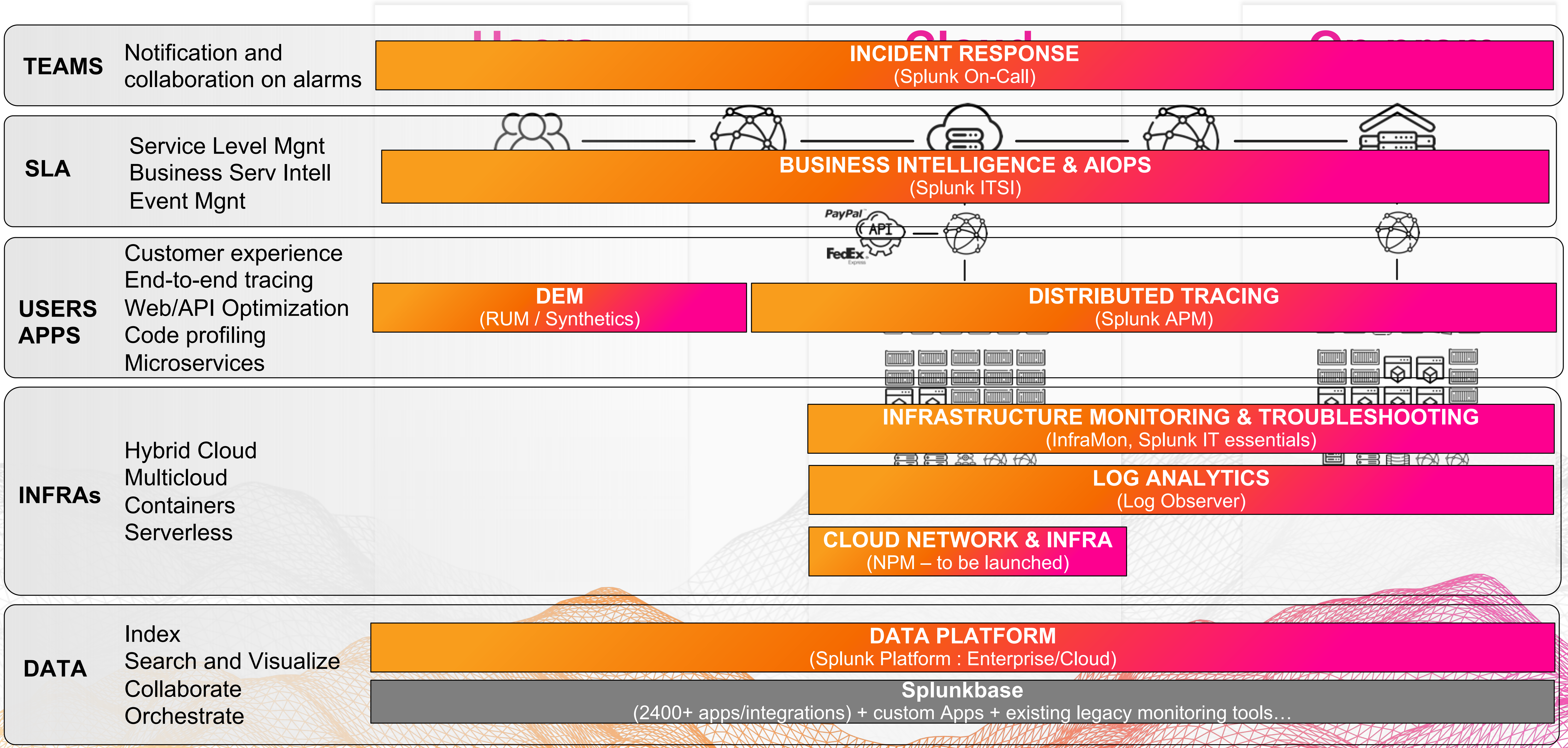
SYNTHETICS

INFRAMON

RUM

LOGS

Where can Splunk help?



TEAMS Notification and collaboration on alarms

INCIDENT RESPONSE
(Splunk On-Call)

SLA Service Level Mgnt
Business Serv Intell
Event Mgnt

BUSINESS INTELLIGENCE & AIOPS
(Splunk ITSI)

USERS APPS Customer experience
End-to-end tracing
Web/API Optimization
Code profiling
Microservices

DEM
(RUM / Synthetics)

DISTRIBUTED TRACING
(Splunk APM)

INFRAs Hybrid Cloud
Multicloud
Containers
Serverless

INFRASTRUCTURE MONITORING & TROUBLESHOOTING
(InfraMon, Splunk IT essentials)

LOG ANALYTICS
(Log Observer)

CLOUD NETWORK & INFRA
(NPM – to be launched)

DATA Index
Search and Visualize
Collaborate
Orchestrate

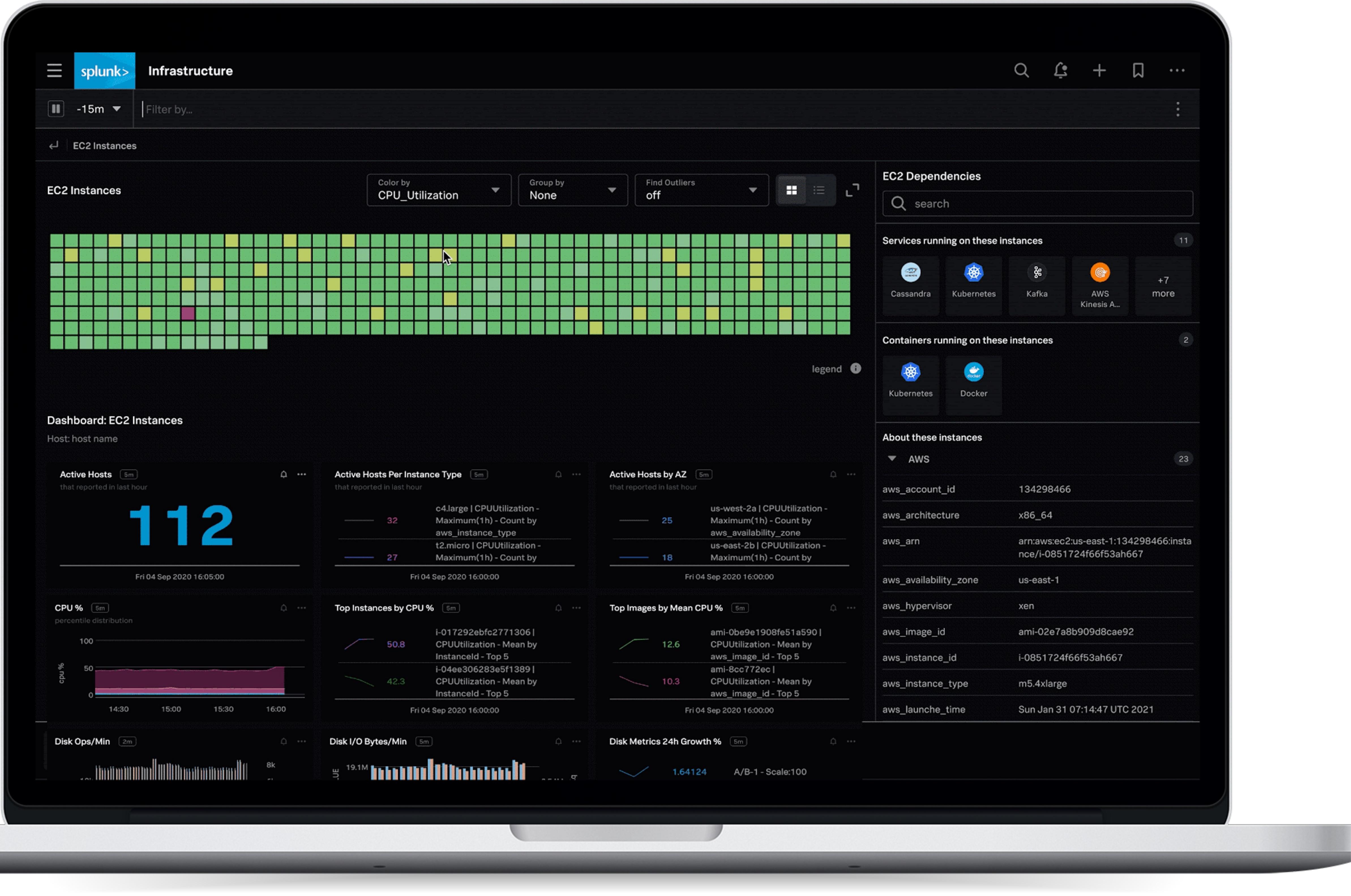
DATA PLATFORM
(Splunk Platform : Enterprise/Cloud)

Splunkbase
(2400+ apps/integrations) + custom Apps + existing legacy monitoring tools…

Splunk Infrastructure Monitoring

Built on a real-time streaming metrics platform

- On-prem to multi cloud monitoring
  - Linux, Windows, VMware
  - AWS, Google Cloud, Azure
  - Kubernetes & Serverless
- Automatic service discovery
- 200+ pre-built integrations
- Analytics-driven alerting



EC2 Instances

Color by: CPU_Utilization

Group by: None

Find Outliers: off

Active Hosts Per Instance Type:

32 c4.large | CPUUtilization - Maximum(1h) - Count by aws_instance_type

27 t2.micro | CPUUtilization - Maximum(1h) - Count by

Active Hosts by AZ:

25 us-west-2a | CPUUtilization - Maximum(1h) - Count by aws_availability_zone

18 us-east-2b | CPUUtilization - Maximum(1h) - Count by

Top Instances by CPU %:

50.8 i-017292ebfc2771306 | CPUUtilization - Mean by InstanceId - Top 5

42.3 i-04ee306283e5f1389 | CPUUtilization - Mean by InstanceId - Top 5

Top Images by Mean CPU %:

12.6 ami-0be9e1908fe51a590 | CPUUtilization - Mean by aws_image_id - Top 5

10.3 ami-8cc772ec | CPUUtilization - Mean by aws_image_id - Top 5

Disk Metrics 24h Growth %:

1.64124 A/B-1 - Scale:100

About these instances

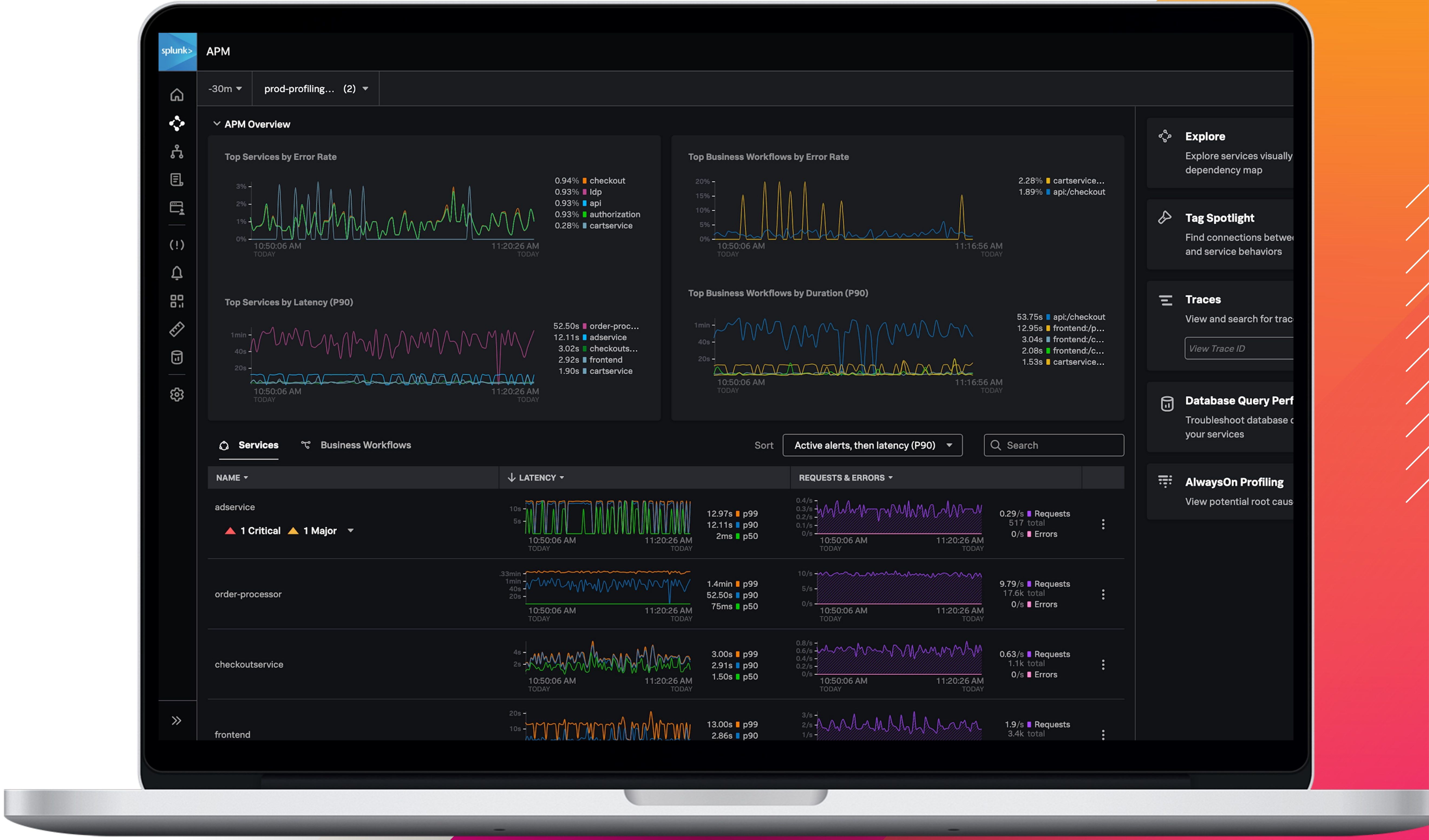
aws_account_id	134298466
aws_architecture	x86_64
aws_arn	arn:aws:ec2:us-east-1:134298466:instance/i-0851724f66f53ah667
aws_availability_zone	us-east-1
aws_hypervisor	xen
aws_image_id	ami-02e7a8b909d8cae92
aws_instance_id	i-0851724f66f53ah667
aws_instance_type	m5.4xlarge
aws_launche_time	Sun Jan 31 07:14:47 UTC 2021

splunk> turn data into doing™

Splunk APM

End to end visibility to isolate problems faster, from monoliths to microservices

- Analyze every transaction from web and mobile apps, to backend services and database queries, to troubleshoot faster
- Continuously measure how your code impacts CPU and memory allocation to identify slowness and bottlenecks in your services
- Quickly identify the sources of latency, errors, and anomalies with AI-directed troubleshooting and dynamic telemetry maps



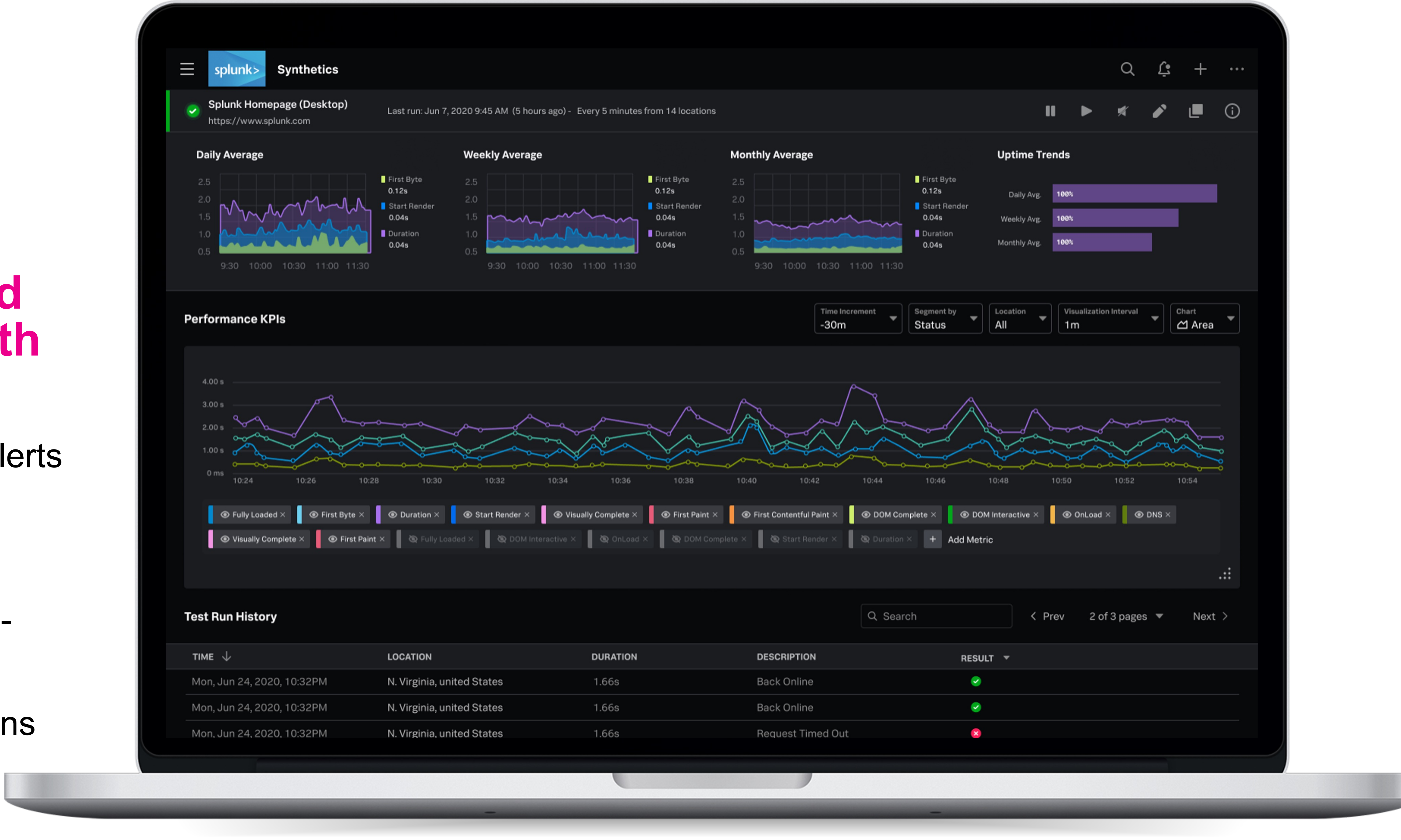
NAME	↓ LATENCY	REQUESTS & ERRORS
adservice 1 Critical 1 Major	12.97s p99 12.11s p90 2ms p50	0.29/s Requests 517 total 0/s Errors
order-processor	1.4min p99 52.50s p90 75ms p50	9.79/s Requests 17.6k total 0/s Errors
checkoutservice	3.00s p99 2.91s p90 1.50s p50	0.63/s Requests 1.1k total 0/s Errors
frontend	13.00s p99 2.86s p90	1.9/s Requests 3.4k total

splunk> turn data into doing

Splunk Synthetic Monitoring

Optimize performance and ensure exceptional CX with every deployment

- URL, API & service performance alerts
- 50+ public locations simulate performance of users globally
- Test within CI/CD pipelines to auto-pass/fail SLA-tier deployments
- 300+ performance recommendations prioritize issues & optimize critical web services



splunk> Synthetics

Splunk Homepage (Desktop)
https://www.splunk.com

Last run: Jun 7, 2020 9:45 AM (5 hours ago) - Every 5 minutes from 14 locations

Performance KPIs

Time Increment: -30m
Segment by: Status
Location: All
Visualization Interval: 1m
Chart: Area

Test Run History

Search ‹ Prev 2 of 3 pages Next ›

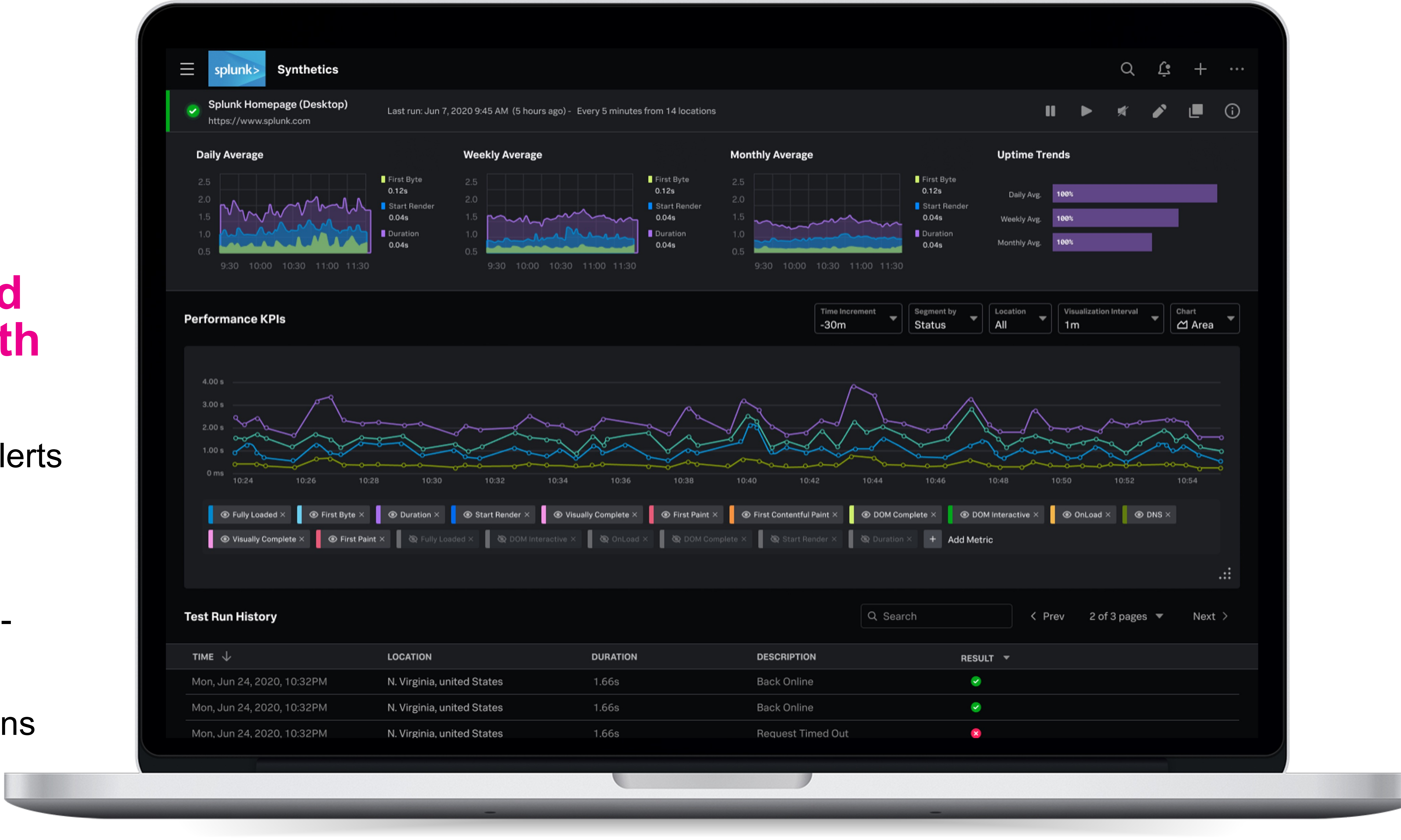
TIME	LOCATION	DURATION	DESCRIPTION	RESULT
Mon, Jun 24, 2020, 10:32PM	N. Virginia, united States	1.66s	Back Online	✓
Mon, Jun 24, 2020, 10:32PM	N. Virginia, united States	1.66s	Back Online	✓
Mon, Jun 24, 2020, 10:32PM	N. Virginia, united States	1.66s	Request Timed Out	✗

splunk> turn data into doing

Splunk Synthetic Monitoring

Optimize performance and ensure exceptional CX with every deployment

- URL, API & service performance alerts
- 50+ public locations simulate performance of users globally
- Test within CI/CD pipelines to auto-pass/fail SLA-tier deployments
- 300+ performance recommendations prioritize issues & optimize critical web services



Splunk Homepage (Desktop)
https://www.splunk.com

Last run: Jun 7, 2020 9:45 AM (5 hours ago) - Every 5 minutes from 14 locations

Time Increment: -30m
Segment by: Status
Location: All
Visualization Interval: 1m
Chart: Area

Test Run History

TIME	LOCATION	DURATION	DESCRIPTION	RESULT
Mon, Jun 24, 2020, 10:32PM	N. Virginia, united States	1.66s	Back Online	✓
Mon, Jun 24, 2020, 10:32PM	N. Virginia, united States	1.66s	Back Online	✓
Mon, Jun 24, 2020, 10:32PM	N. Virginia, united States	1.66s	Request Timed Out	✕

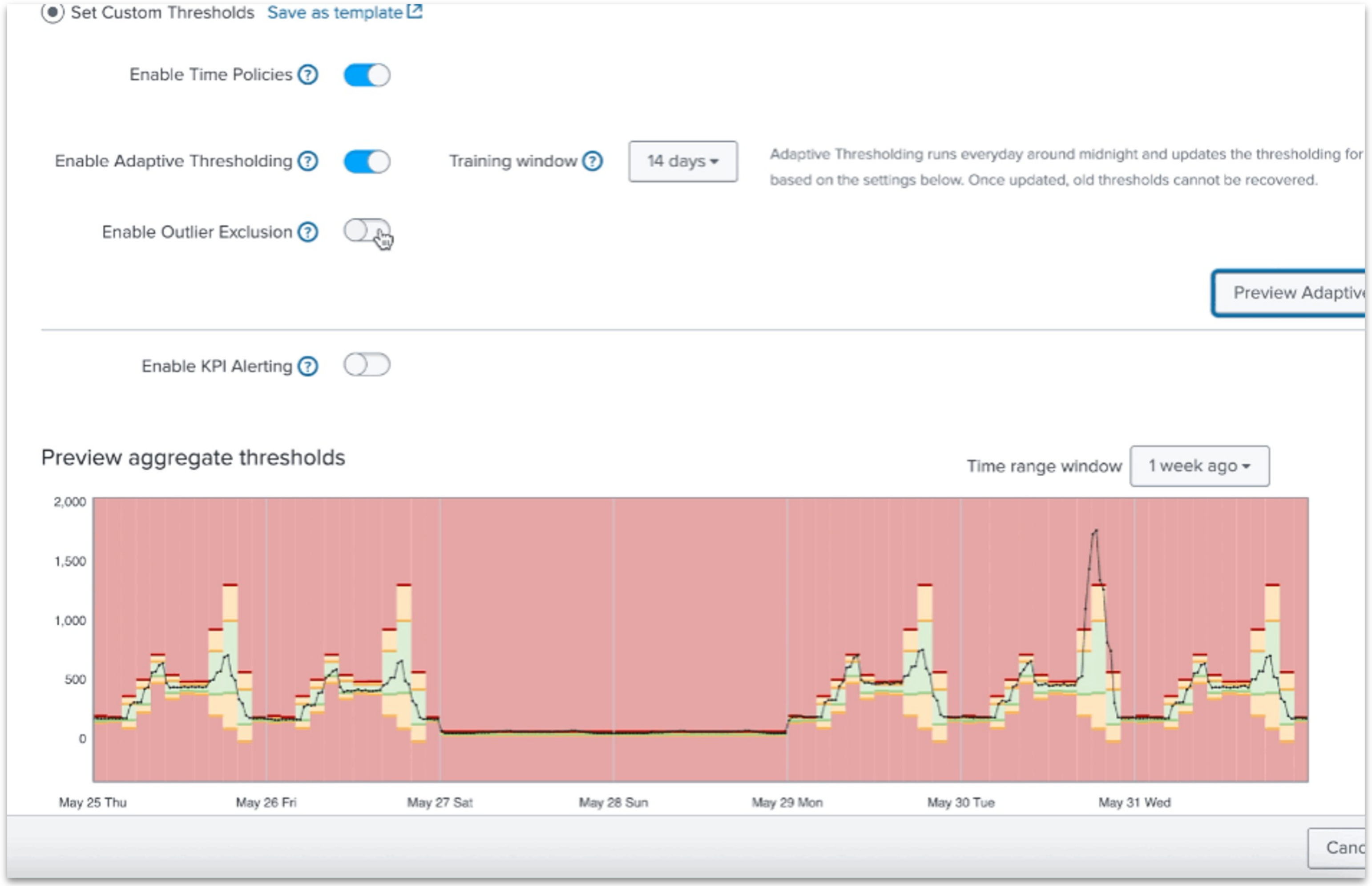
splunk> turn data into doing™

Splunk IT Service Intelligence (ITSI)

Splunk's **AIOps** Solution

Splunk ITSI applies machine learning to **proactively prevent outages** by correlating and reducing alerts, monitoring service health, and streamlining incident management.

- ❑ Clustering & aggregation to reduce alert noise
- ❑ Adaptive (dynamic) thresholds incorporate seasonality
- ❑ Anomaly and outlier detection
- ❑ Actionable additional context
- ❑ Assisted root cause investigation
- ❑ Predict service health to prevent outages



● Set Custom Thresholds

Enable Time Policies: on

Enable Adaptive Thresholding: on

Training window: 14 days

Adaptive Thresholding runs everyday around midnight and updates the thresholding for based on the settings below. Once updated, old thresholds cannot be recovered.

Enable Outlier Exclusion: off

Enable KPI Alerting: off

Preview aggregate thresholds

Time range window: 1 week ago

New updates! .conf23 ★

- ❑ Outlier Exclusion in Adaptive Thresholds
- ❑ ML-Assisted Thresholding *(Preview)*

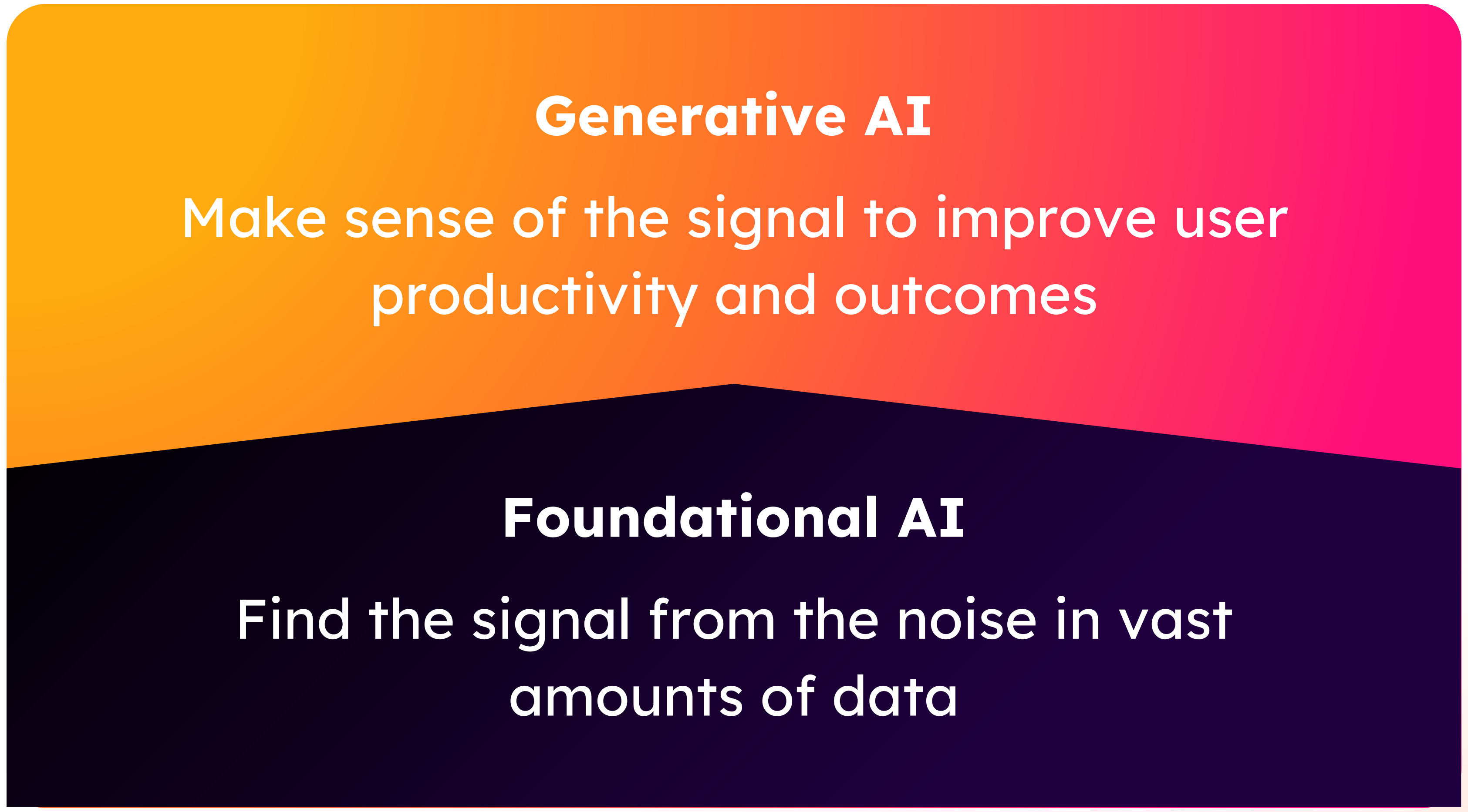
Splunk AI

AI and ML capabilities across our portfolio accelerate detection, investigation, and response.

Our approach

- Domain and Splunk specific
- Human-in-the-loop and trusted
- Open and extensible

What we offer



Generative AI

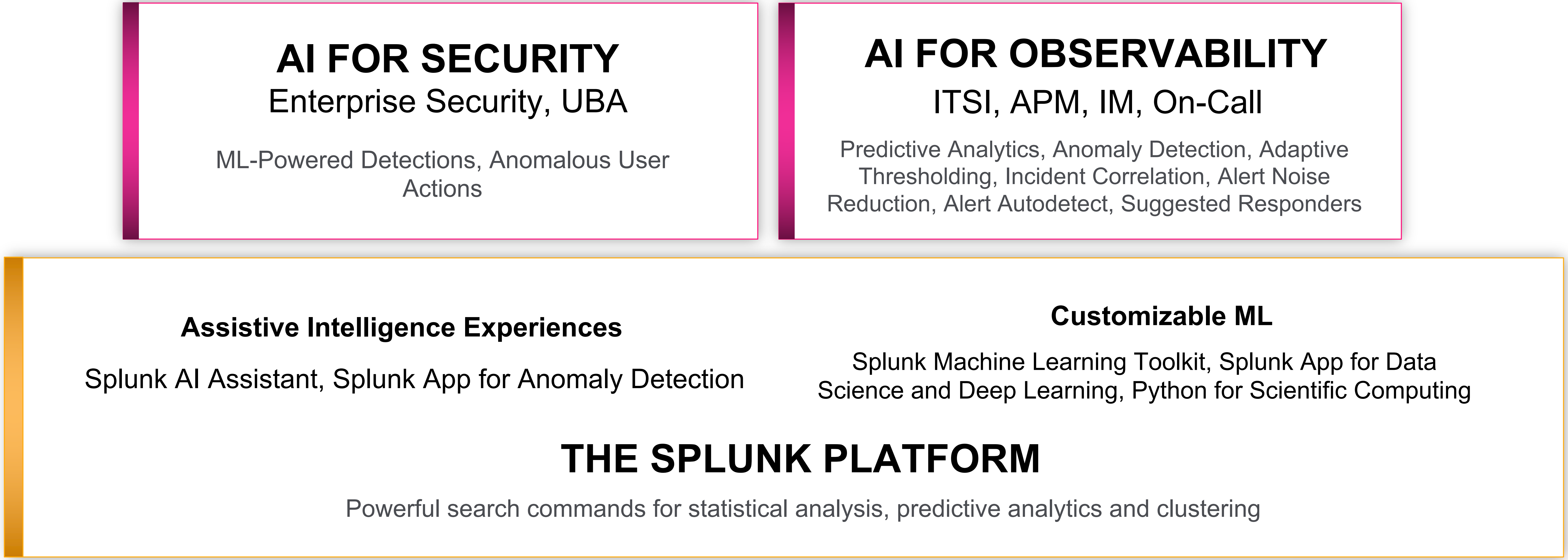
Make sense of the signal to improve user productivity and outcomes

Foundational AI

Find the signal from the noise in vast amounts of data

Splunk AI

Catalyze Resilience with Embedded AI and Machine Learning



AI FOR SECURITY

Enterprise Security, UBA

ML-Powered Detections, Anomalous User Actions

AI FOR OBSERVABILITY

ITSI, APM, IM, On-Call

Predictive Analytics, Anomaly Detection, Adaptive Thresholding, Incident Correlation, Alert Noise Reduction, Alert Autodetect, Suggested Responders

Assistive Intelligence Experiences

Splunk AI Assistant, Splunk App for Anomaly Detection

Customizable ML

Splunk Machine Learning Toolkit, Splunk App for Data Science and Deep Learning, Python for Scientific Computing

THE SPLUNK PLATFORM

Powerful search commands for statistical analysis, predictive analytics and clustering

DEMO

Splunk

Thank you

splunk>
a CISCO company