

Splunk

Enhancing security

Sven Vande Cappelle

Presales consultant

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, Splunk> and Turn Data Into Doing 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. © 2023 Splunk Inc. All rights reserved.



Sven Vande Cappelle

Presales consultant

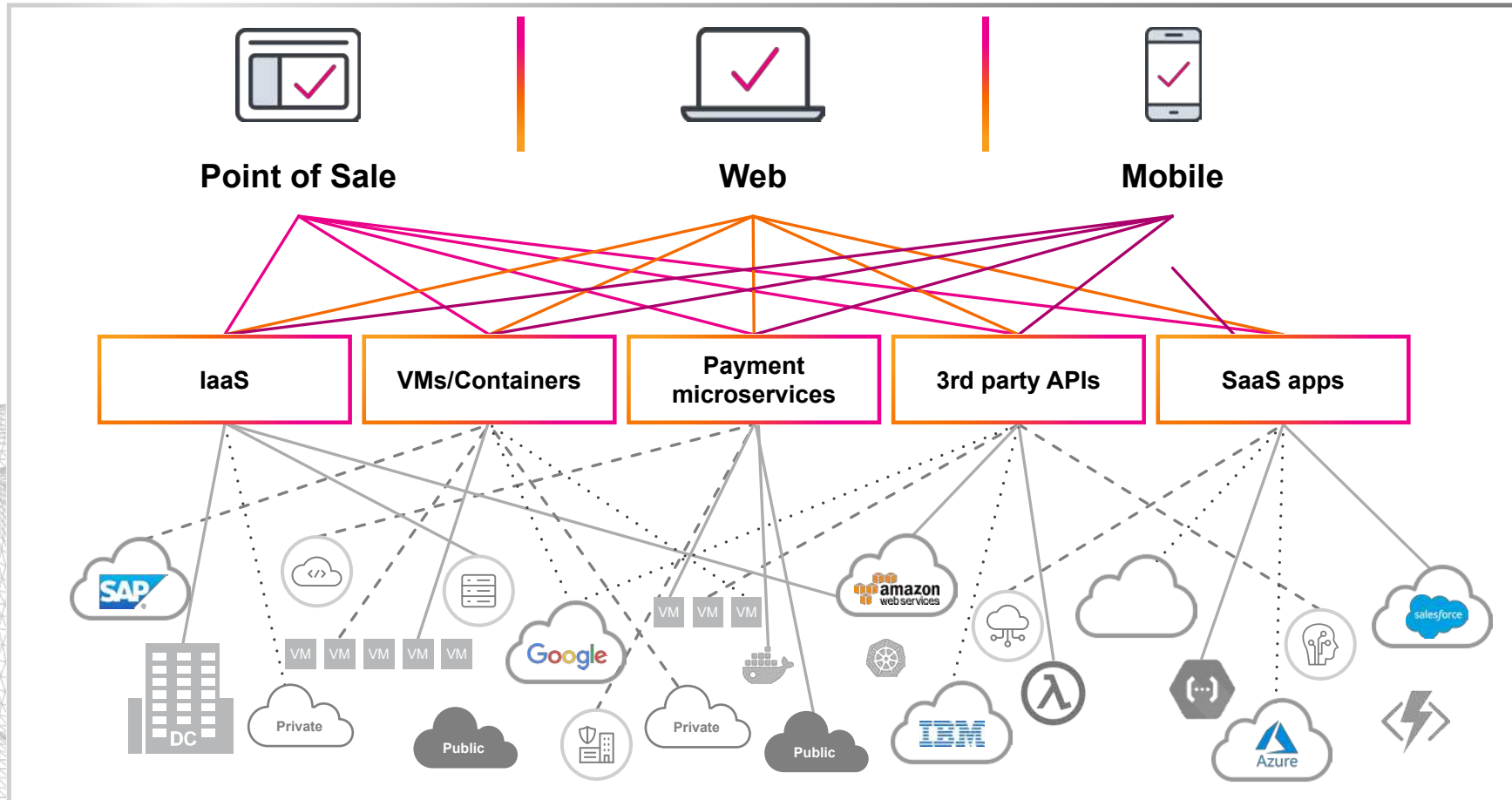


How can we rethink our
approach to keeping systems secure,
reliable and performing?

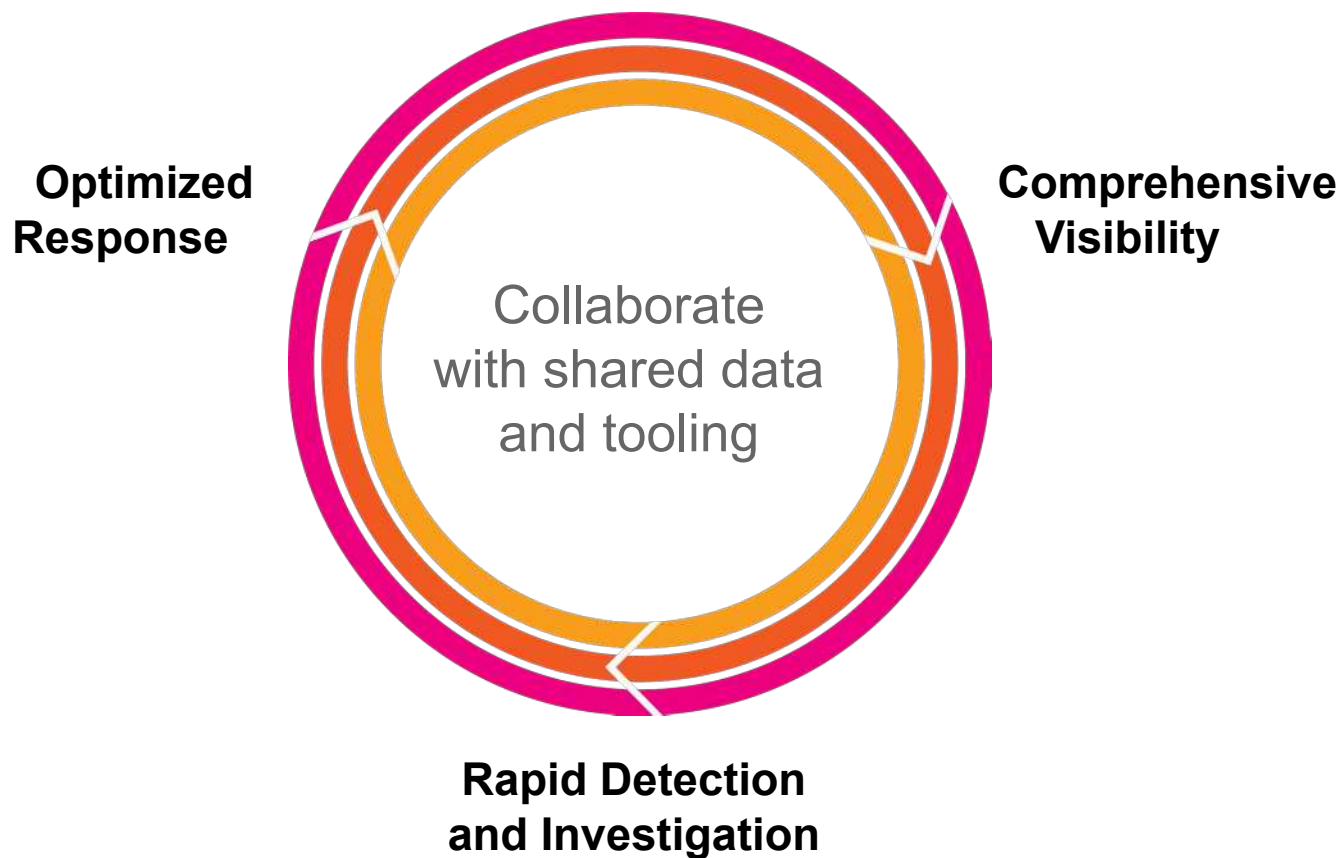


Build a foundation of
RESILIENCE

Hybrid and Multi Cloud Systems Create Complexity



Splunk enables faster detection, investigation and response

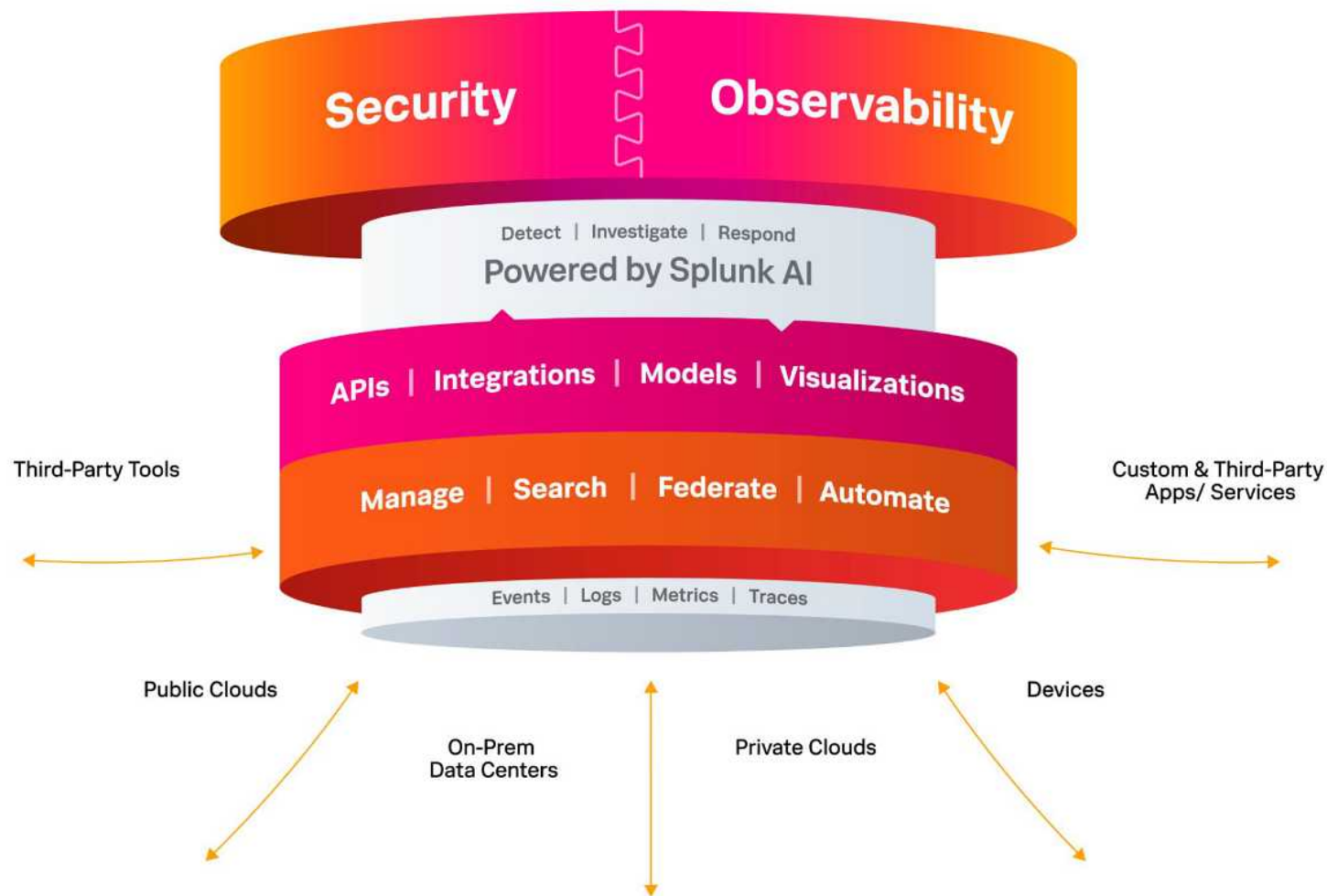


✓ Hybrid

✓ Scalable

✓ Interoperable

The Unified Security and Observability Platform



PLATFORM

Enable Unified Security and Observability

Monitor, investigate and respond rapidly at scale with comprehensive visibility and shared tooling.

Streaming

Machine learning

Scalable index

Search and visualization

Collaboration and orchestration



8B

monthly searches

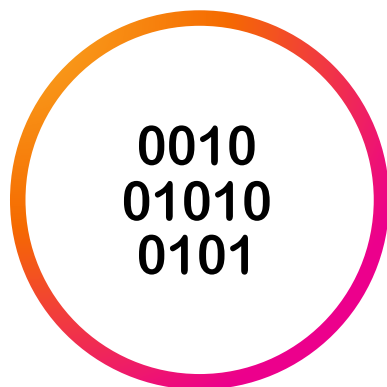
2.8K+

apps &
add-ons on
Splunkbase

~1K

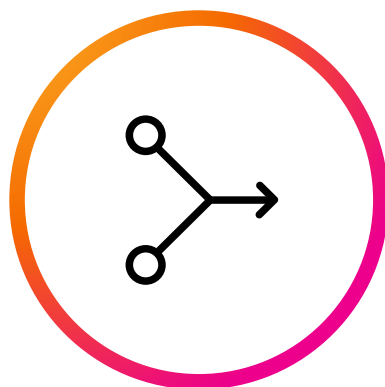
purpose built
data source
integrations

Scalable Index



What: Any and All Data

- Index Any and All streaming, machine, and historical data



How: Point it at a Source

- Point Splunk at a data source—tell it a bit about the source—that source becomes a data input



Then: Turn Source into Stream of Events

- Splunk indexes the data stream and transforms it into a series of events—you can view and search those events right away

Search and Visualization

Use Search Process Language (SPL) to search and investigate your data across cloud or on prem deployments to find the needle in your haystack



Search Any Data Source

With Schema on the Fly you can search any data source regardless of structure and across cloud or on prem deployments



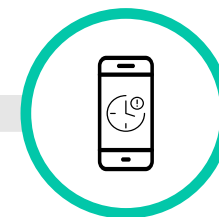
Spot Outliers

Visualize relationships within your data to easily spot outliers



Visualize and Save Dashboards

Add visualizations and save as dashboards



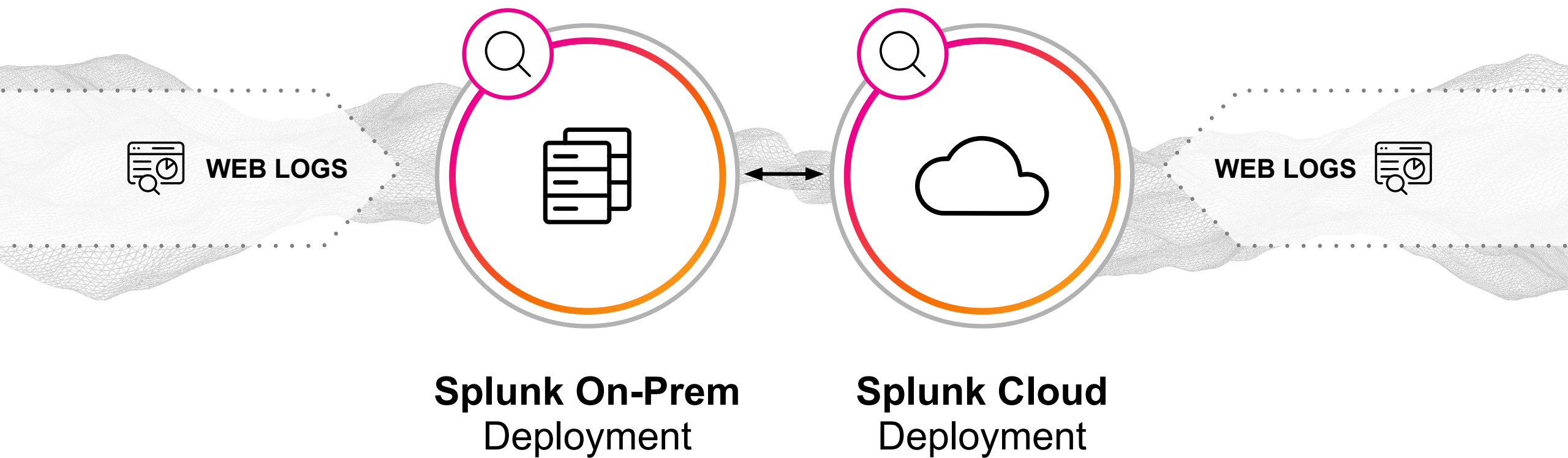
Create Ad Hoc Alerts

Create ad hoc alerts when you discover new issues or threats

Ubiquitous Machine Learning

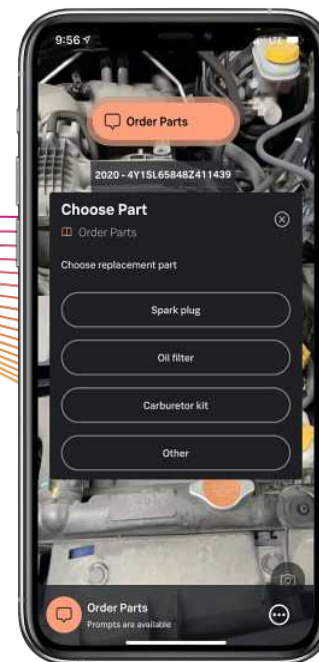
| | Turnkey | ▶ Configurable | ▶ Extensible |
|------------------|---|---|--|
| Theme | ML-powered Solutions: IT, Security, Observability | Extending use cases through streamlined ML application | New frontier of use cases through DS development |
| Splunk Solutions | <ul style="list-style-type: none"> • Enterprise Security • User Behavioral Analytics • Observability • IT Service Intelligence (ITSI) | <ul style="list-style-type: none"> • Machine Learning Toolkit (MLTK) • Splunk app for Data Science and Deep Learning | <ul style="list-style-type: none"> • Machine Learning Toolkit (MLTK) • Splunk App for Data Science and Deep Learning |
| Examples | <ul style="list-style-type: none"> • Anomaly Detection • Adaptive Thresholding • Predictive Insights • Pipeline Drift Detection | <ul style="list-style-type: none"> • Outlier detection • Forecast time series • Predict fields • Protect sensitive data | <ul style="list-style-type: none"> • Fraud detection • Predictive Maintenance • Domain generated algorithms (DGA) |
| Target Users | <ul style="list-style-type: none"> • Practitioners using embedded, low-touch ML | <ul style="list-style-type: none"> • Domain experts driving extended use cases | <ul style="list-style-type: none"> • Advanced data scientists building expansive custom use cases |

Search Across Environments with Federated Search



Splunk Makes Data Accessible and Actionable From Anywhere

Extend Splunk beyond the desktop

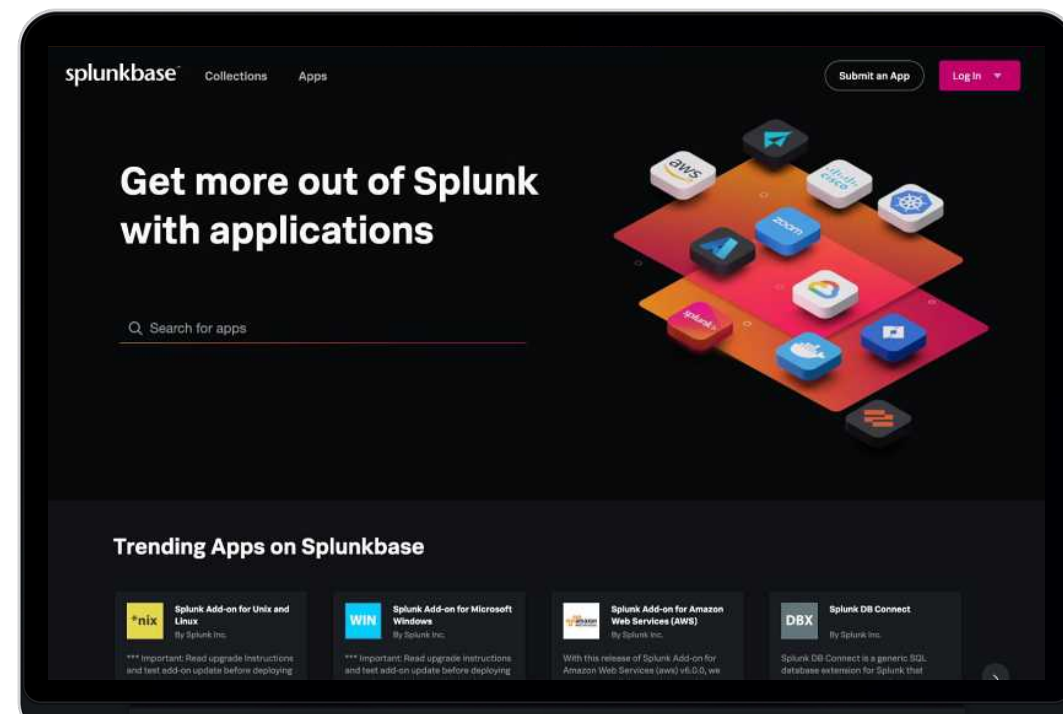


Splunk Mobile

Splunk Augmented Reality (AR)

Access free apps, or build your own

- Build an essential security foundation and accelerate IT troubleshooting with **free, high quality apps** and add-ons to extend the power of your Splunk investment - and developer tooling to build your own!
- Access to the **2800+ solutions** from Splunk, partners, and the community
- Discover new tools for your use case with:
 - Collections - Curated sets of top-rated apps for a variety of use cases and interests
 - App Directory - Complete list of apps filterable by your specific needs



2800+
applications available
on Splunkbase

~1K
Add-ons for data
source integrations

2400+
Community partners

Unified Security and Observability Platform

2M⁺

Security threats blocked in 6 months



99%

Of threats are handled by automation



100%

Uptime despite 300% increase in traffic during Black Friday



1.5M⁺

COVID-19 tests administered and tracked with Splunk Cloud



96%

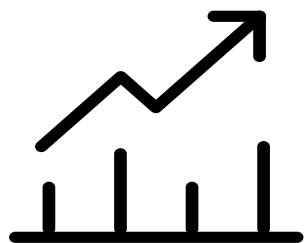
Faster application development powered by full-fidelity visibility



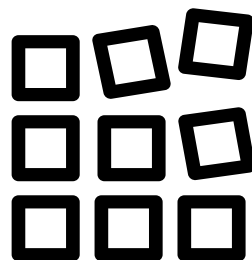


Data

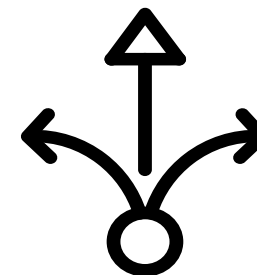
The World Of Data Is Changing



Data is growing exponentially

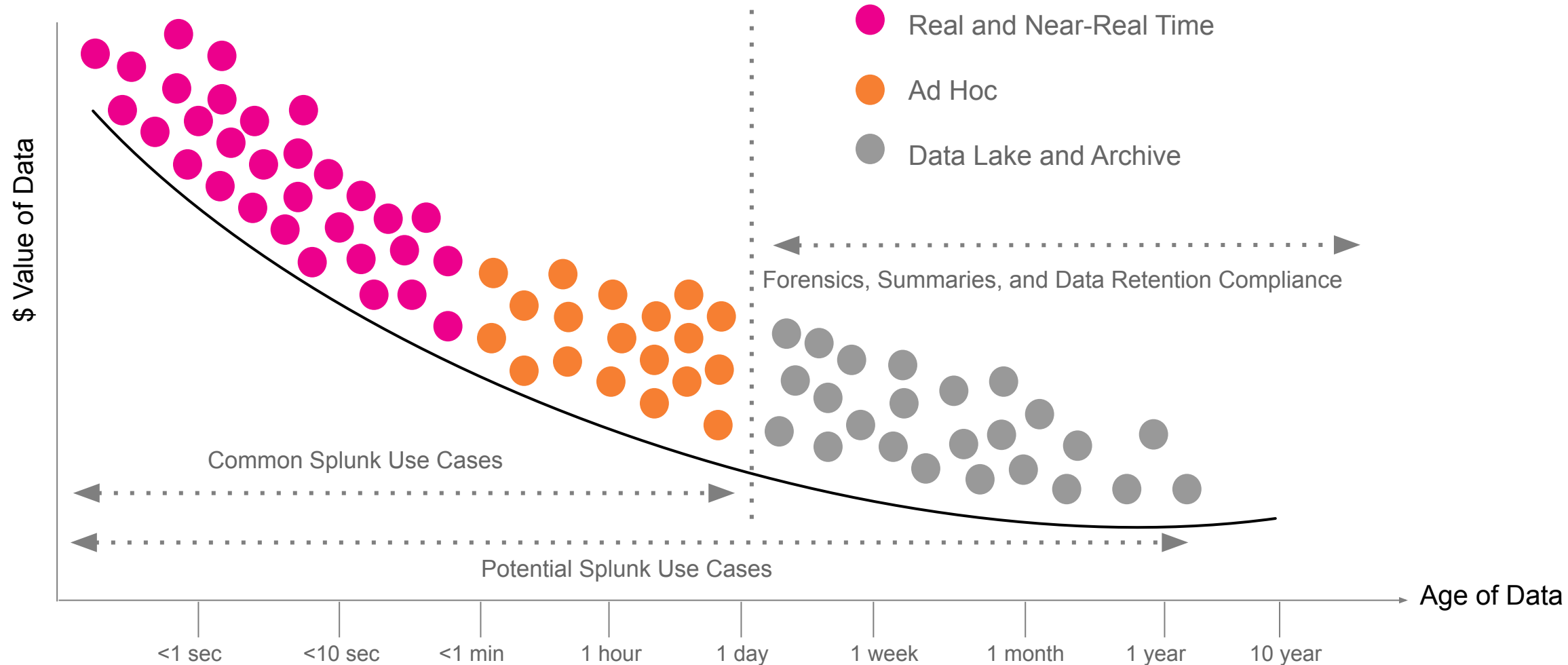


All data is not created equal

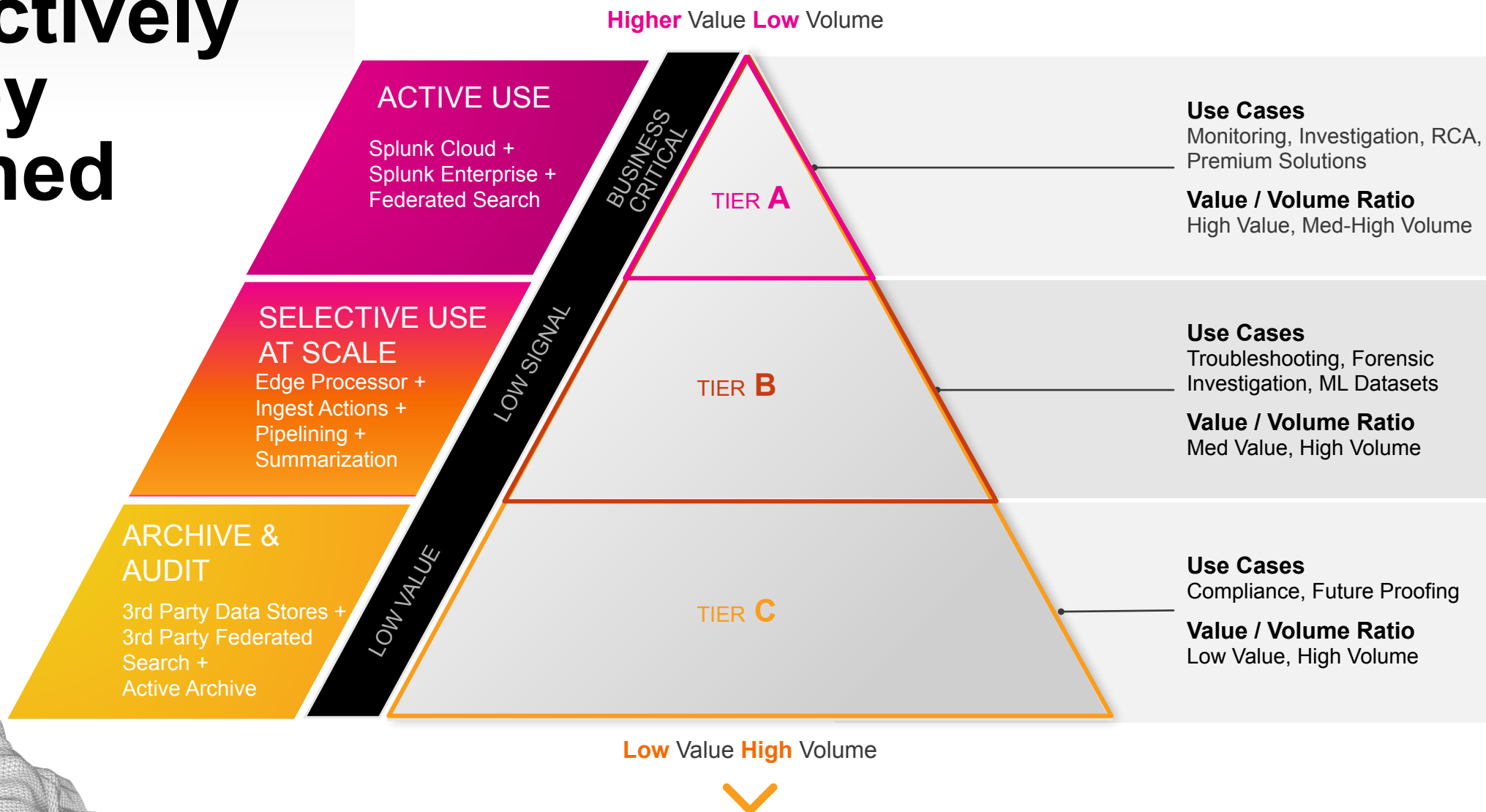


Data may not be able to be moved within a time frame or at all

Data Value Changes With Age



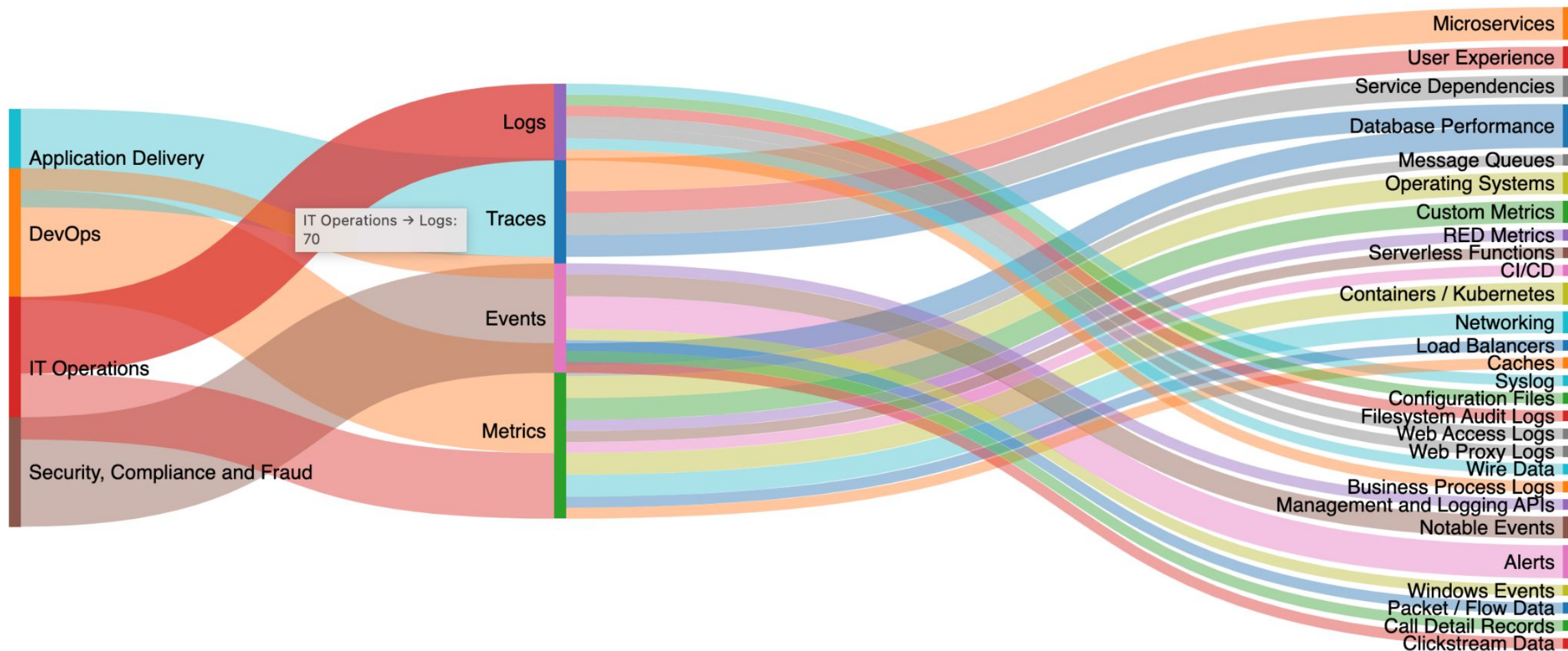
Proactively tier by planned use



0010
01010
0101

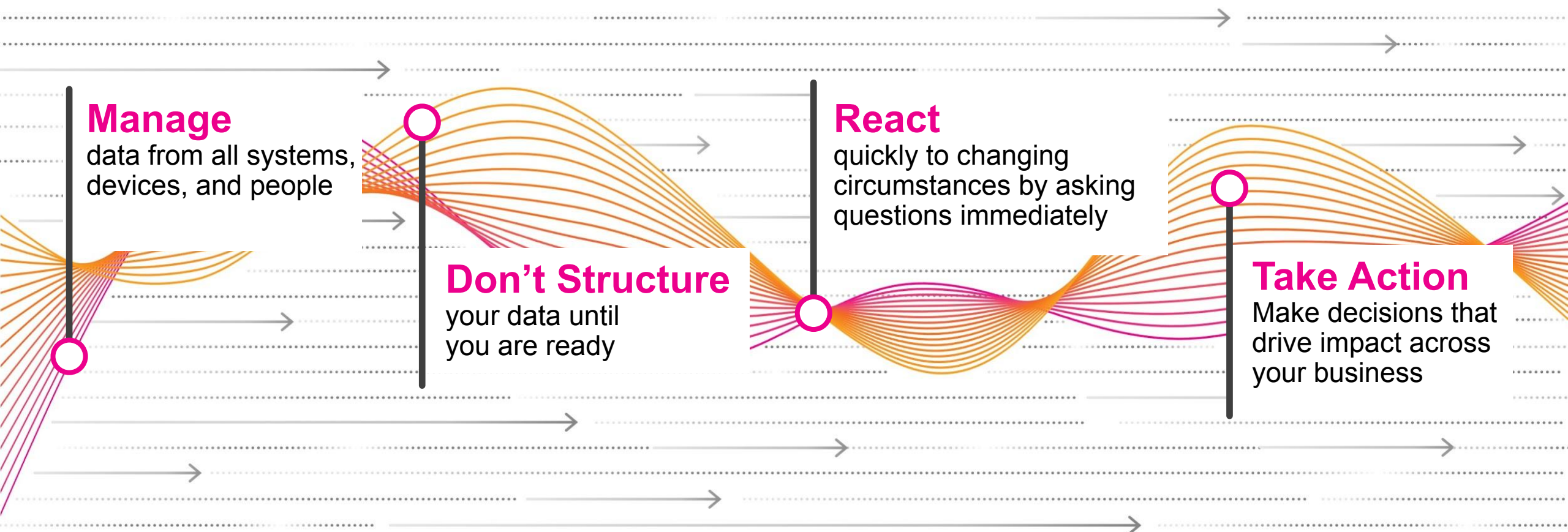
Multiple Use Cases On Common Data

Drives system security and observability



Dynamic and Complex Data Remain the Biggest Challenge & Opportunity

We solved one of the biggest challenges in data with our investigative approach

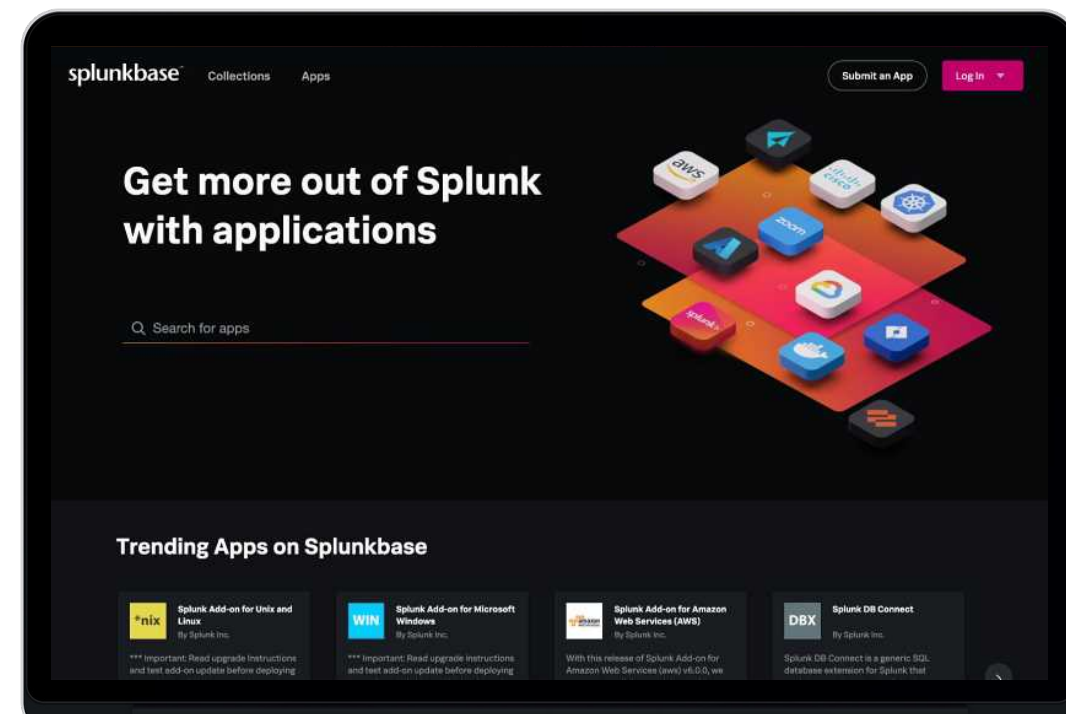


Getting Data In (GDI)

- Universal Forwarder (UF)
- Splunk Stream
- DB Connect
- Data Manager
- HTTP Event Collector (HEC)
- OpenTelemetry Collector
- Splunk Connect for Syslog (SC4S)
- Splunk Connect for SNMP (SC4SNMP)
- Splunk OpenTelemetry Connect for Kubernetes
- Edge Processor
- Edge Hub
- eBPF
- Common Information Model / OCSF
- ...

Access free apps, or build your own

- Build an essential security foundation and accelerate IT troubleshooting with **free, high quality apps** and add-ons to extend the power of your Splunk investment - and developer tooling to build your own!
- Access to the **2800+ solutions** from Splunk, partners, and the community
- Discover new tools for your use case with:
 - Collections - Curated sets of top-rated apps for a variety of use cases and interests
 - App Directory - Complete list of apps filterable by your specific needs



2800+
applications available
on Splunkbase

~1K
Add-ons for data
source integrations

2400+
Community partners

Splunk & Security

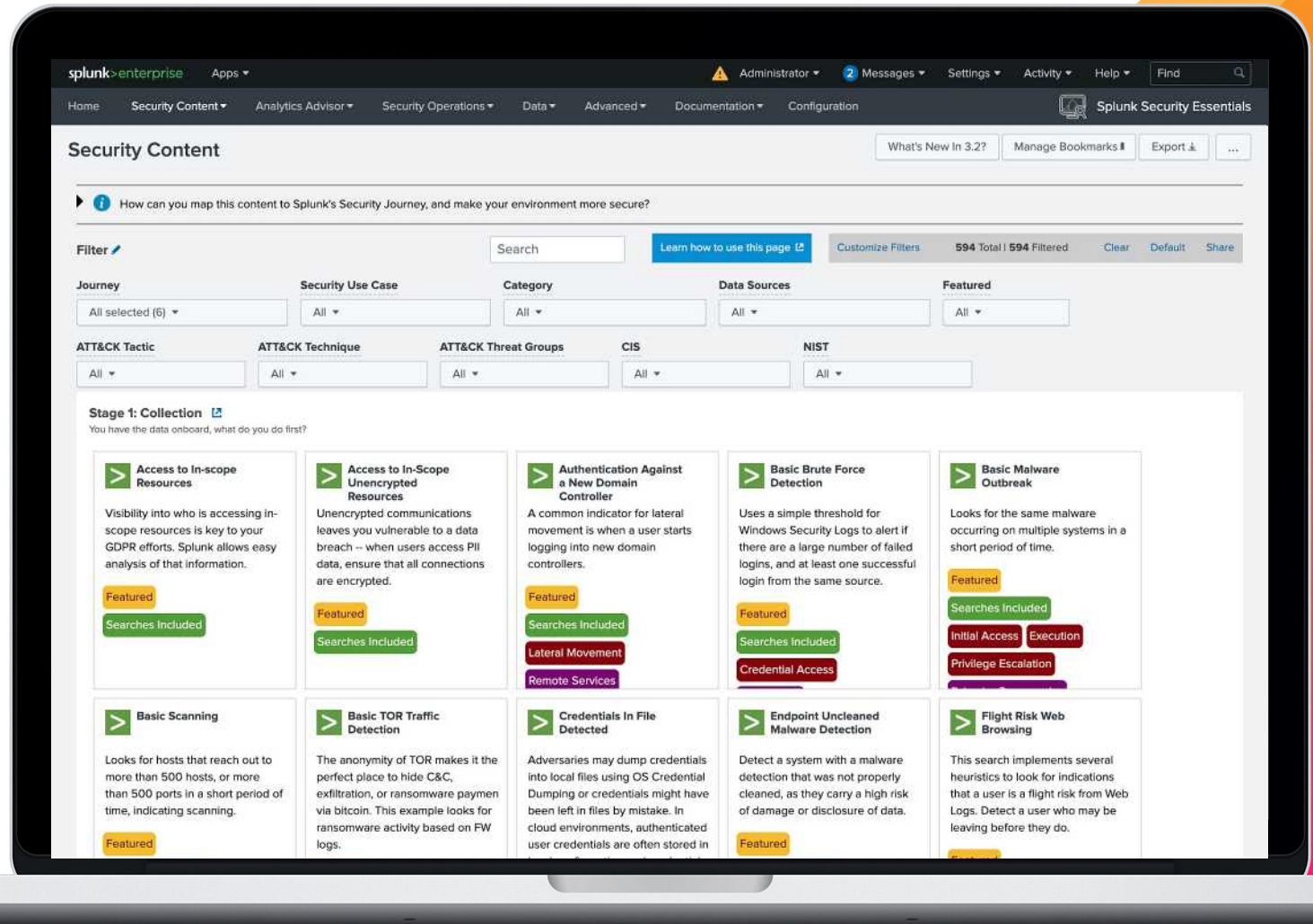
splunk>



Security Content Library

Browse, bookmark, and deploy 800+ security detections and analytic stories

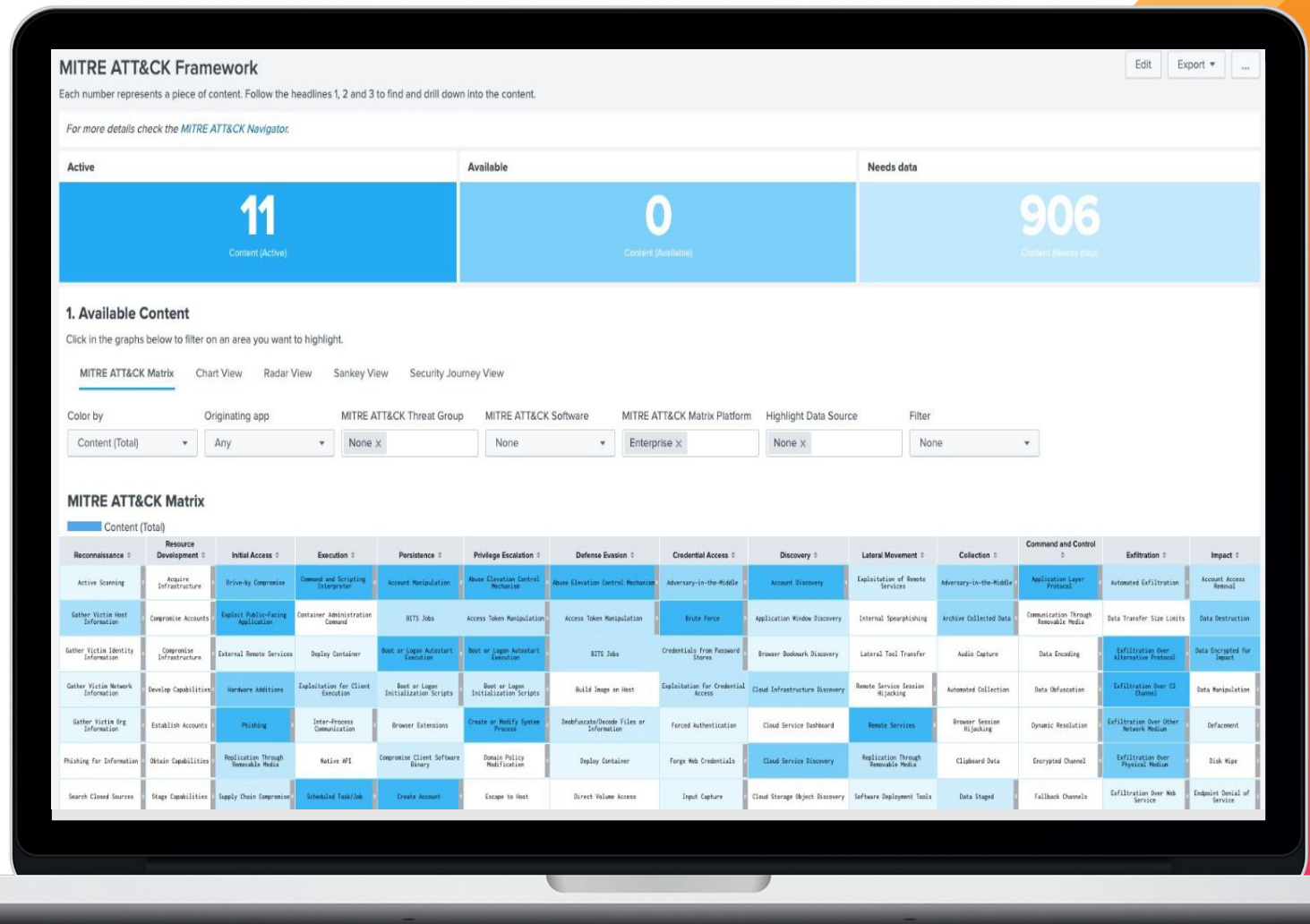
- Repository of Security Content for Splunk Cloud, Enterprise Security, UEBA, and SOAR
- Deploy security content within clicks
- Enrich notable events and run analytics with context from content library
- Stay up to date on ransomware + emerging threats



Operationalize Security Frameworks

Identify gaps, improve threat detection, and reduce risks

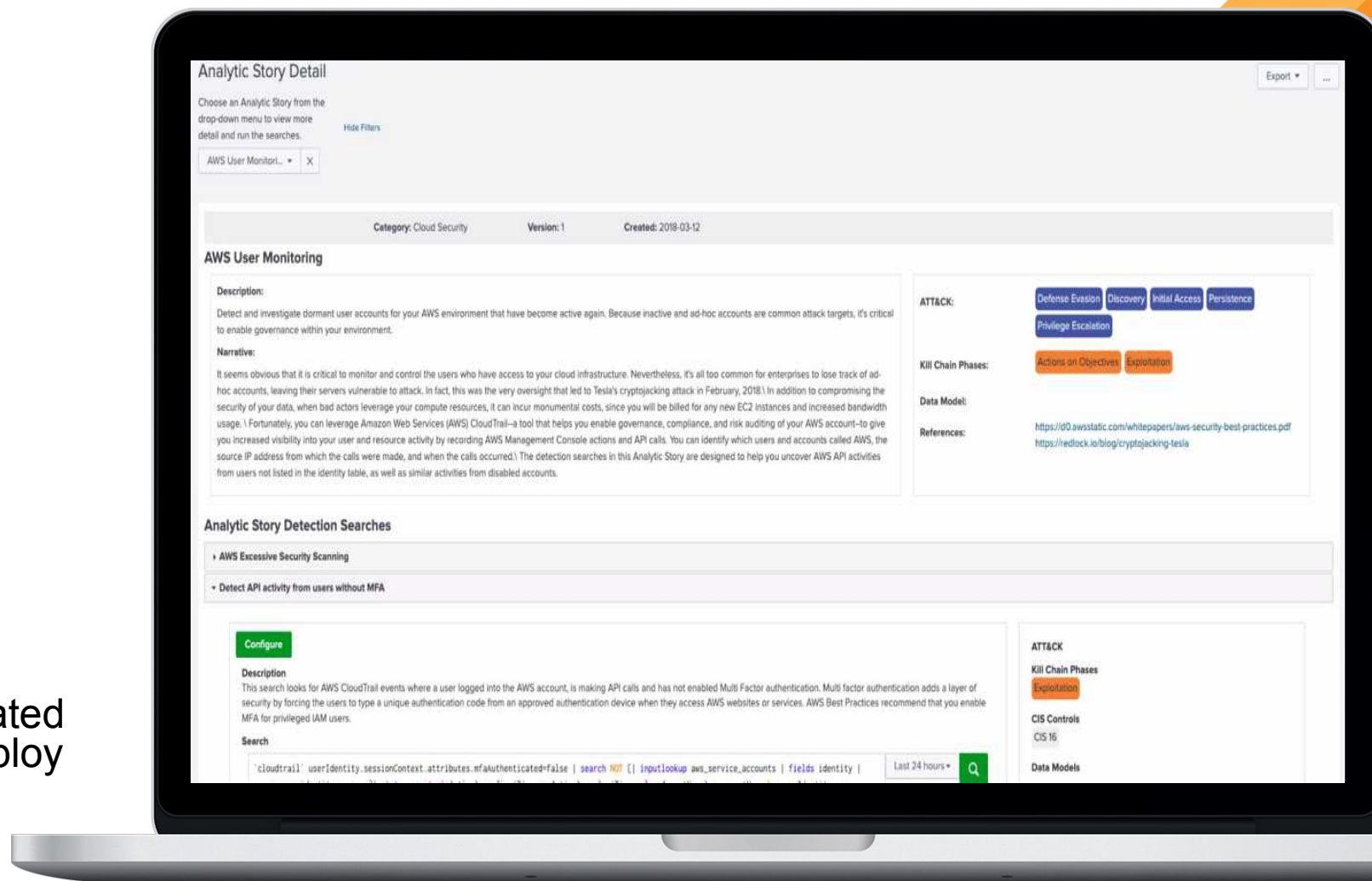
- Develop an understanding of your security posture against MITRE ATT&CK® and Cyber Kill Chain® frameworks
- Ability to import 3rd party content and filter using the originating app
- Drilldown on known Tactics and Techniques and Kill Chain Phases to get a holistic view of all your security content



Data and Content Introspection

Track data and saved searches to gain visibility

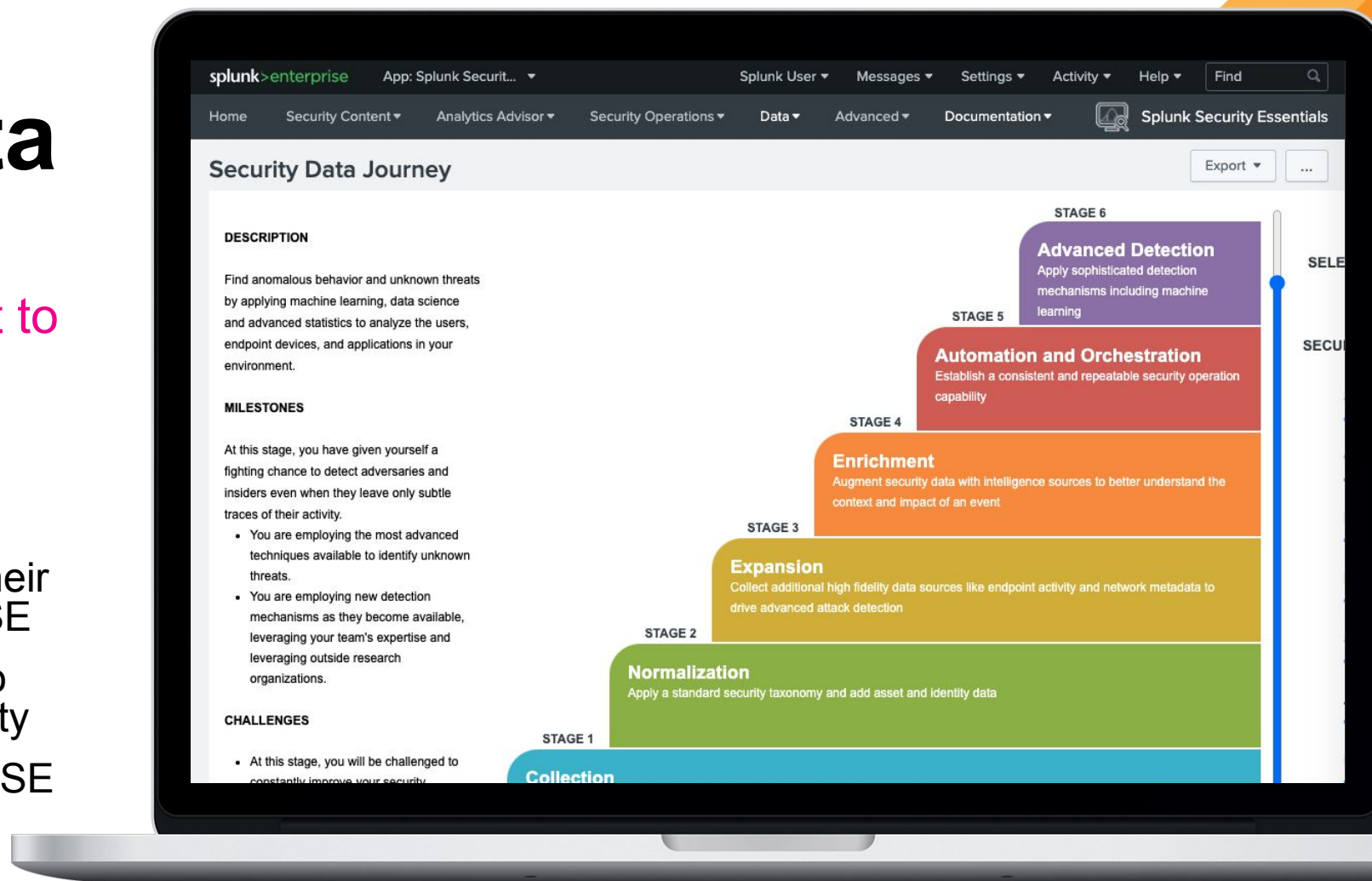
- Enrich saved searches with tags and metadata
- Automatic categorization by security products
- Visibility on ransomware related content and the ability to deploy directly from SSE



Security Data Journey

Use data to bring context to security

- Identify data and security milestones and challenges
- View analytics stories and their related contents easily in SSE
- Curate security detections to level up your security maturity
- Easily export content from SSE into Splunk ES



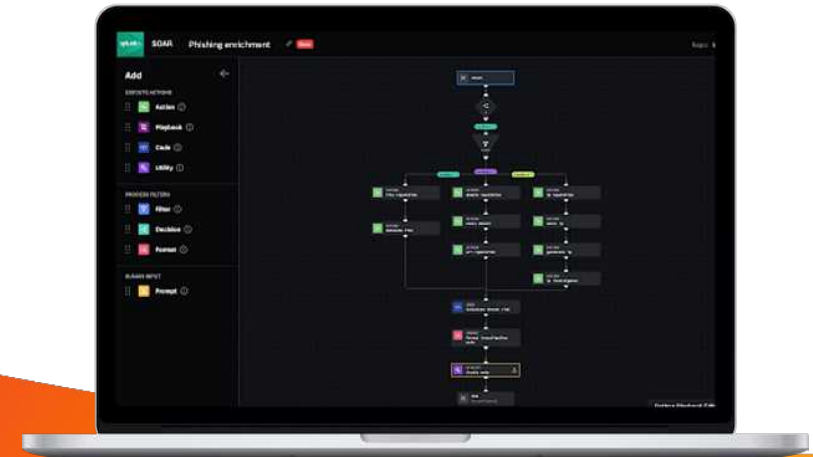
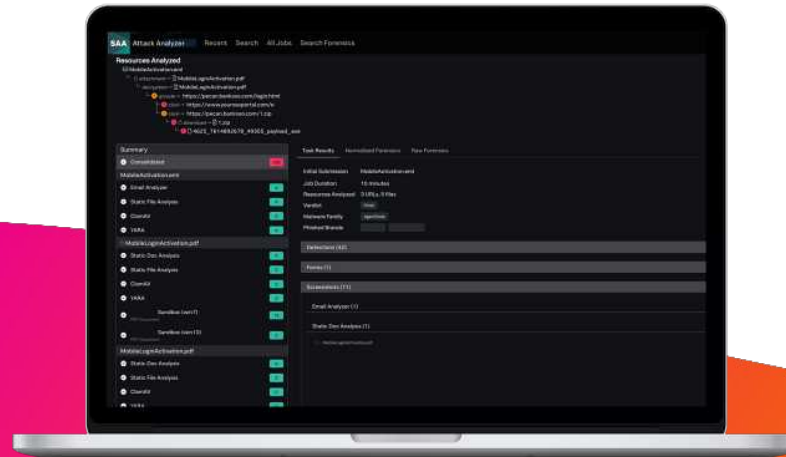
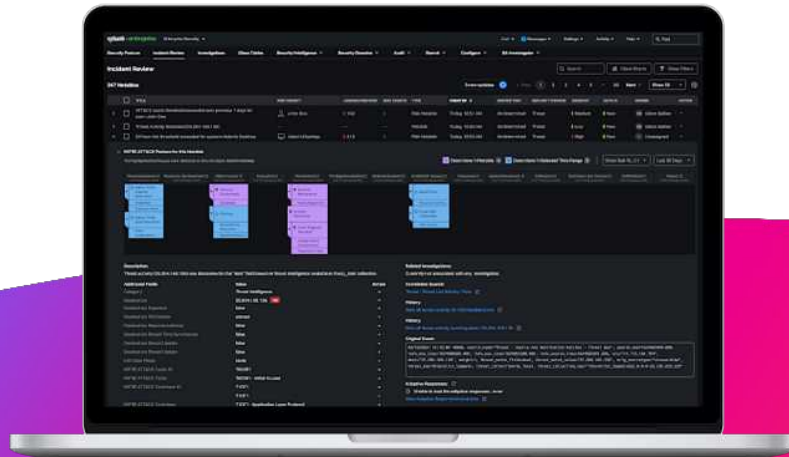
The Industry-Defining TDIR Solution

SPLUNK MISSION CONTROL

Splunk Enterprise Security

Splunk Attack Analyzer

Splunk SOAR

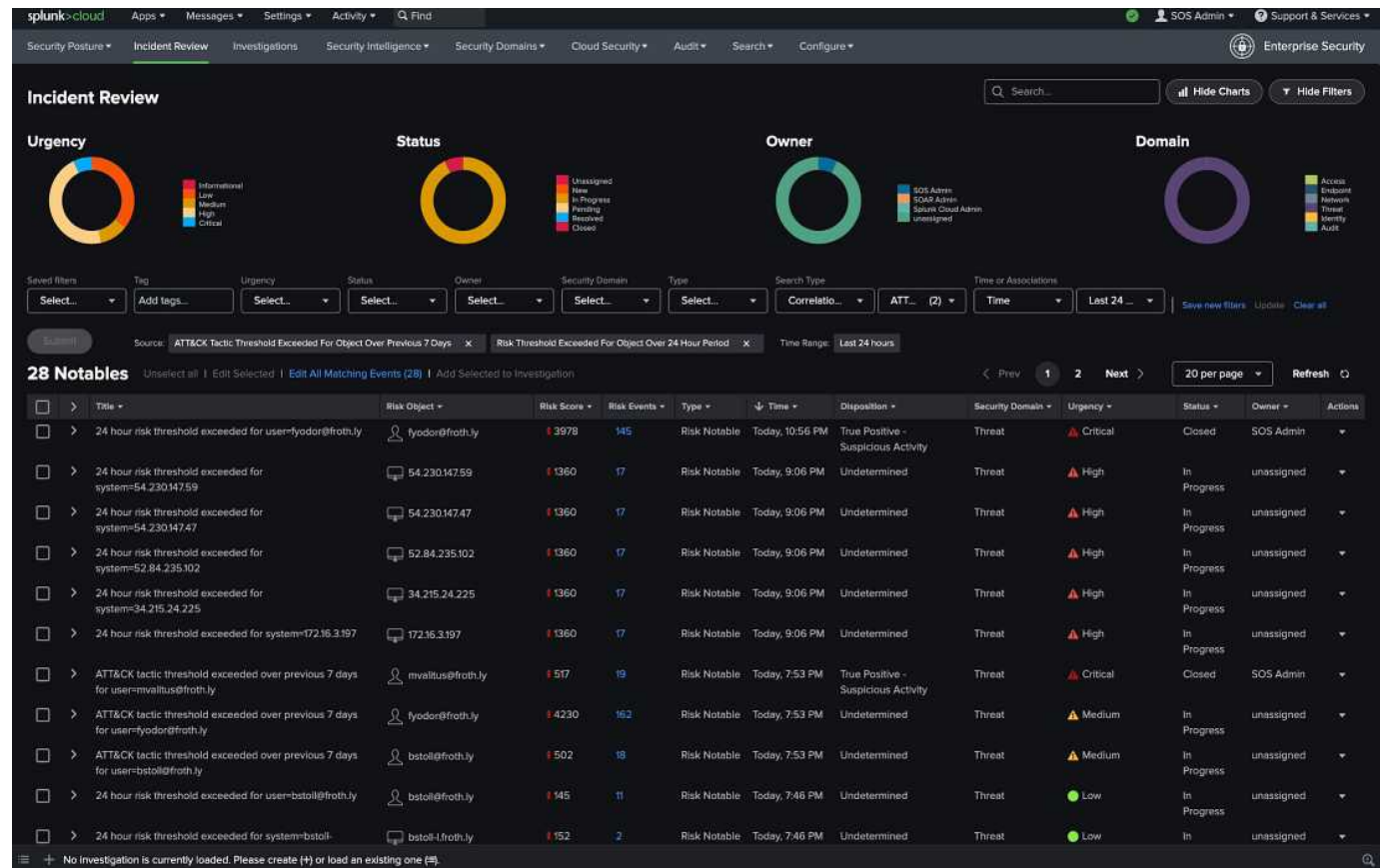


Detect | Investigate | Respond

Splunk Enterprise Security

A data-centric, modern SIEM

- Gain insight into your security posture and investigate with speed and flexibility
- Reduce false positives by up to 80%, detect more sophisticated threats, and align security operations to industry frameworks
- Use pre-built detection and investigation content to more easily secure your AWS, Azure, and Google Cloud Platform data
- Scale to search and monitor terabytes of data per day

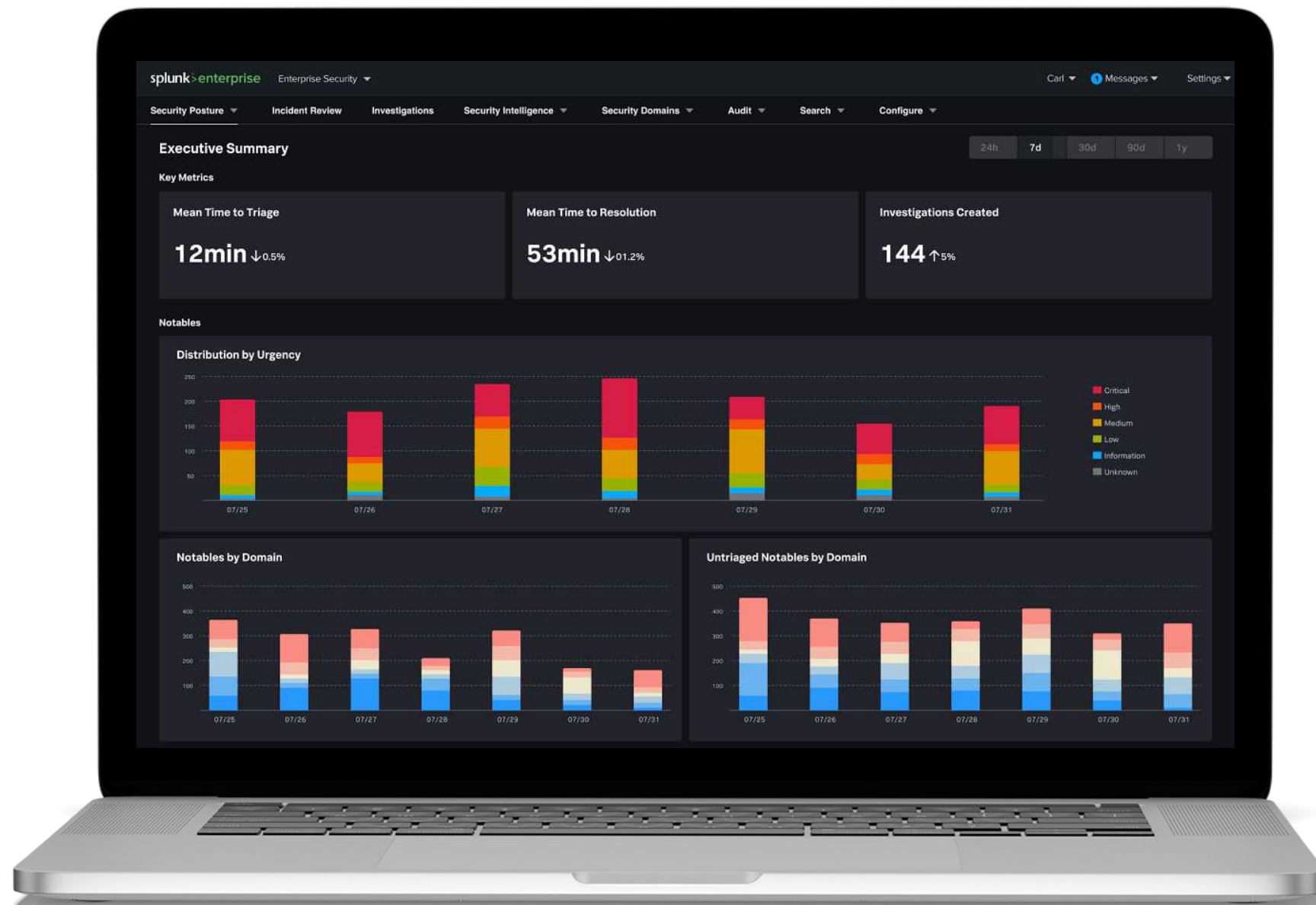




Data-Driven Insights

Full-breadth visibility

- Unlock the ability to ingest, normalize, and gain insights on any data from any source
- Schema-on-read and distributed indexing capabilities ensure fast, flexible investigations
- Perform continuous monitoring with pre-built and customizable dashboards, detections, content, reports, and frameworks
- Search and correlate across cloud, on-premises, or hybrid data sources and deployments

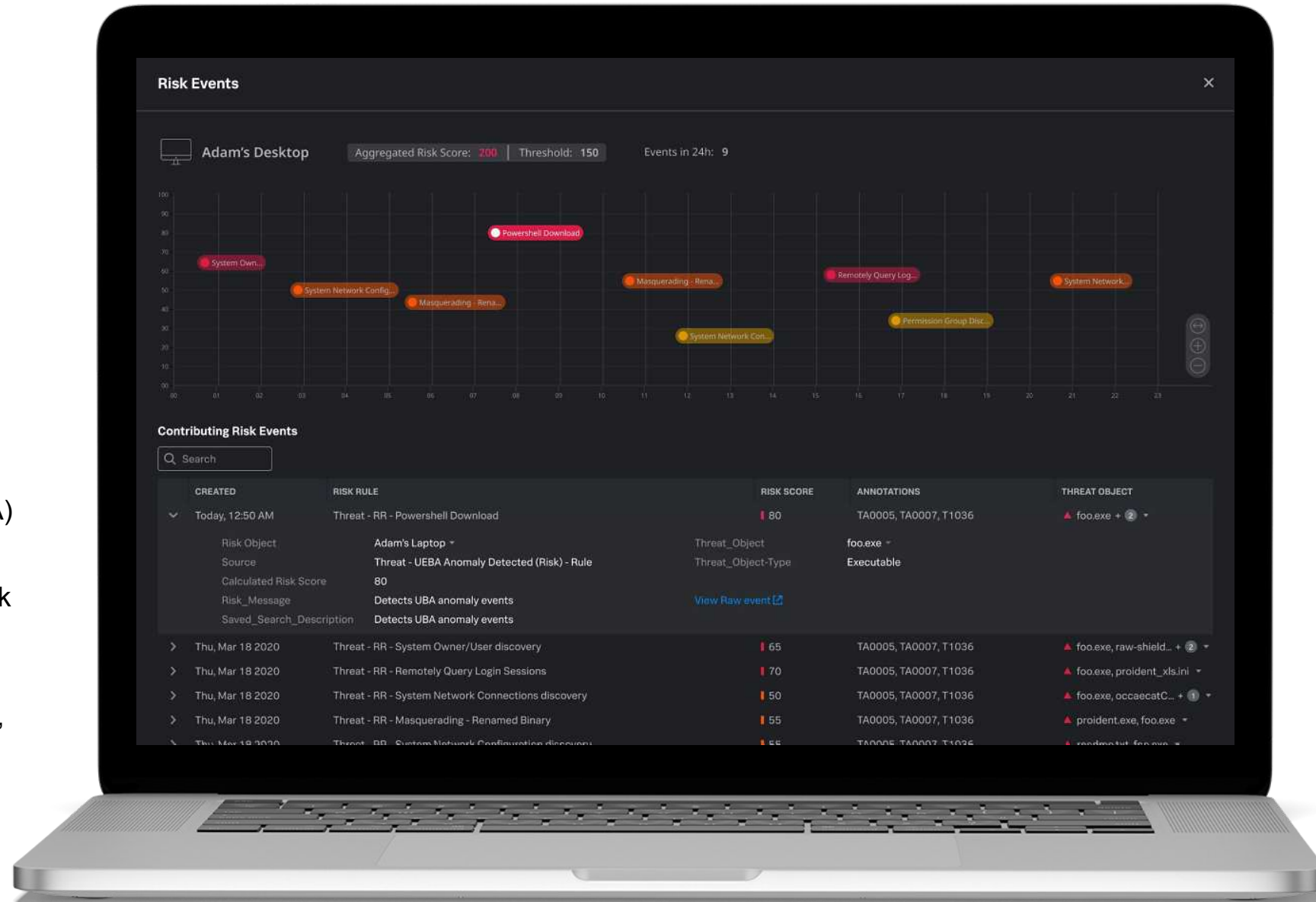




Advanced Analytics

Boost productivity

- 1400+ detections with 100+ cloud-based detections
- 30% increase in true-positive alert rates with Risk-Based Alerting (RBA)
- Enrich and prioritize alerts with integrated threat intelligence (Splunk Intelligence Management)
- Align security operations to industry frameworks (MITRE ATT&CK, NIST, CIS 20, and Kill Chain)
- Dive deep with intuitive search and investigation capabilities

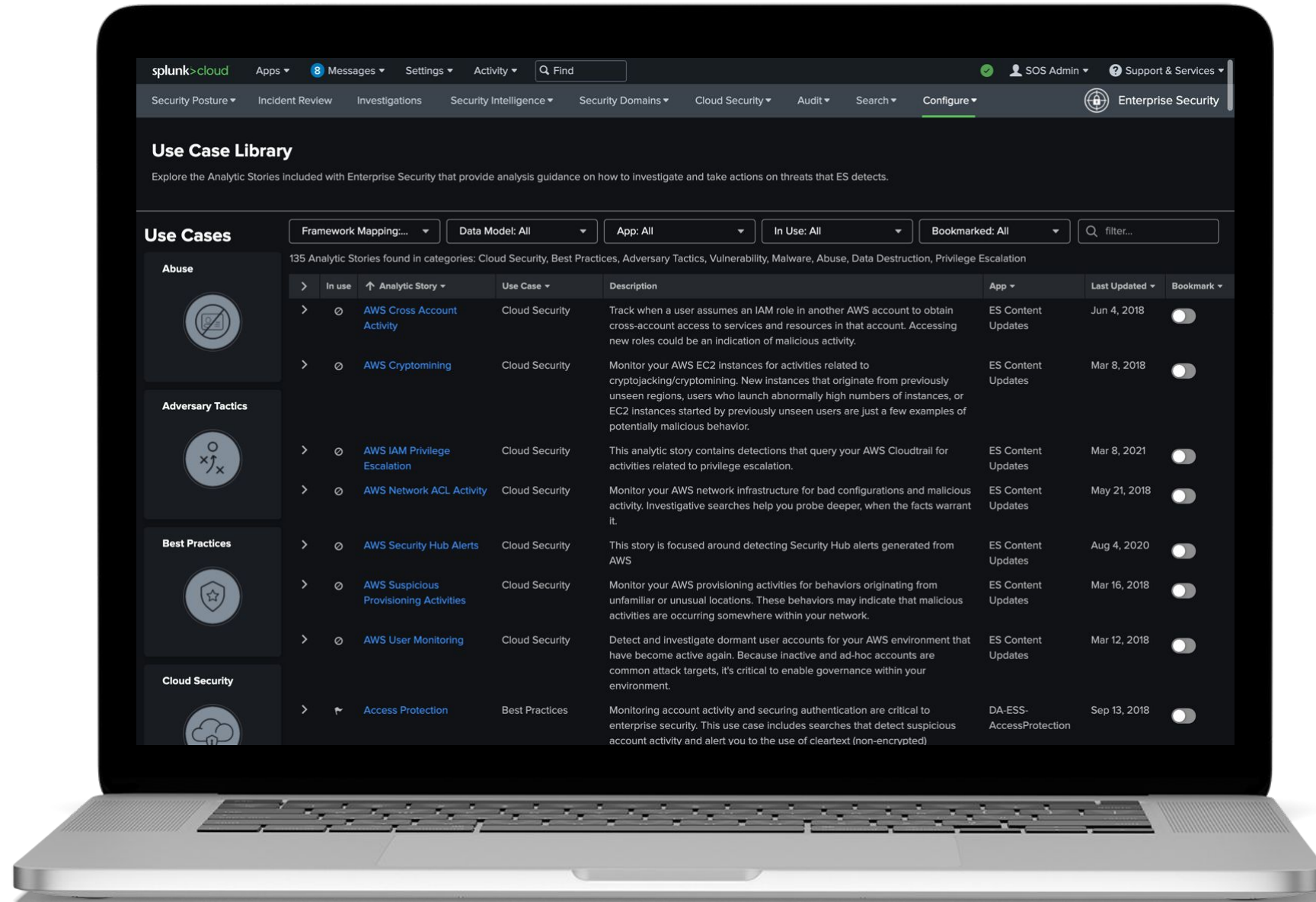




Scale and Flexibility

Open and extensible

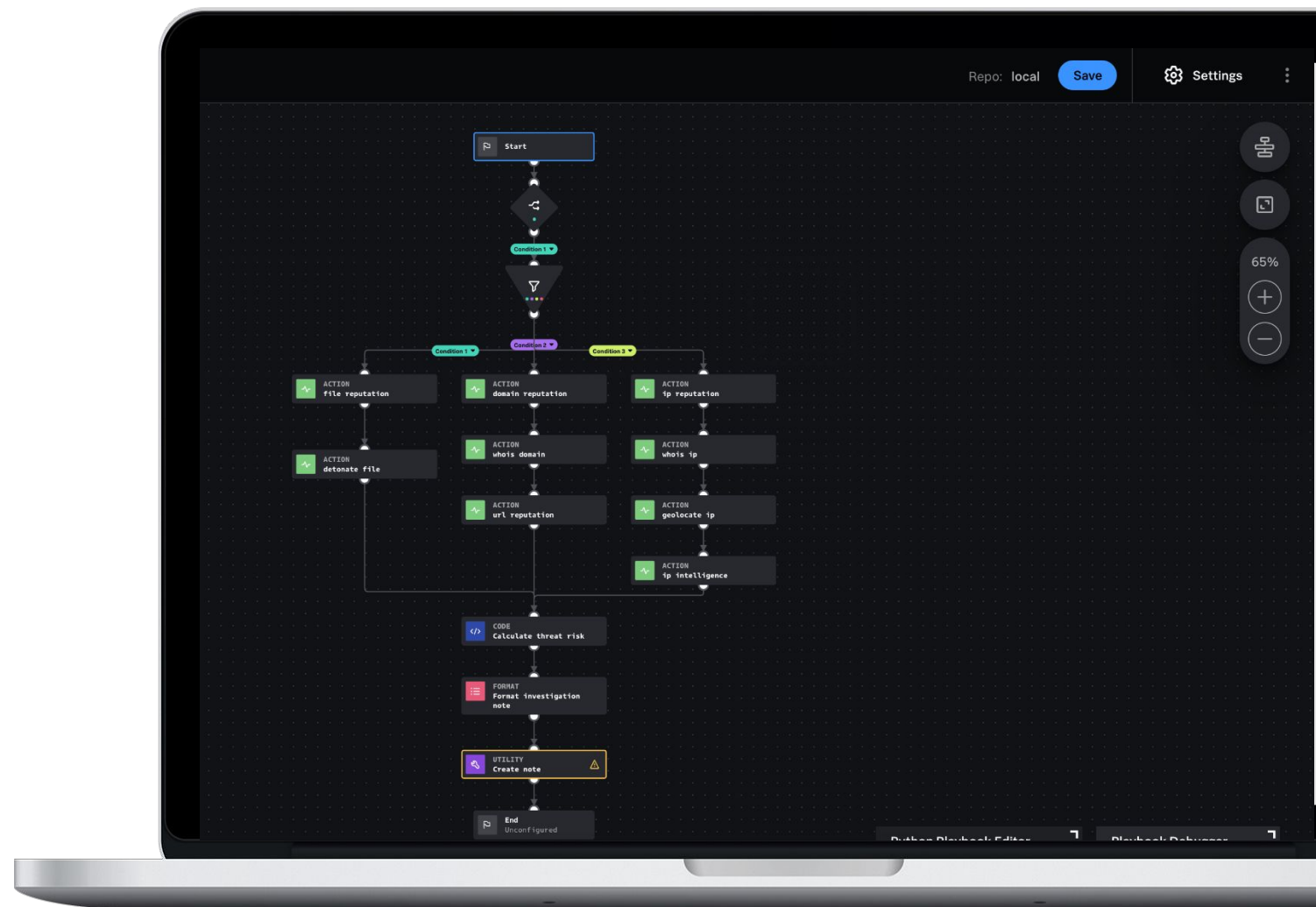
- Scale to search and monitor terabytes of data per day
- Gather context across your multi-vendor security and IT stack with technology integrations from Splunkbase
- Stay on top of new and emerging threats with automated content delivery from the Splunk Threat Research Team
- Customize and tune pre-built detections, content, frameworks to address what's critical





Automation

- Automate repetitive tasks to force multiply team efforts.
- Execute automated actions in seconds versus hours.
- Become proactive and focus on mission-critical objectives to protect your business.



Splunk Attack Analyzer

Automatic analysis of active threats.
Full-scope insights and rapid resolution.

The newest member of the
Splunk Security Family

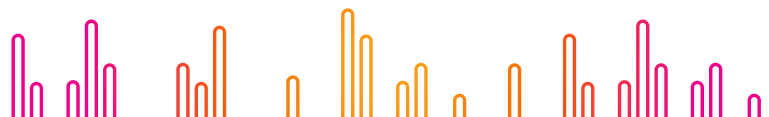
Acquisition of TwinWave announced on November 8th, 2022

Take the manual work out of threat analysis

See through the eyes of the threat actor

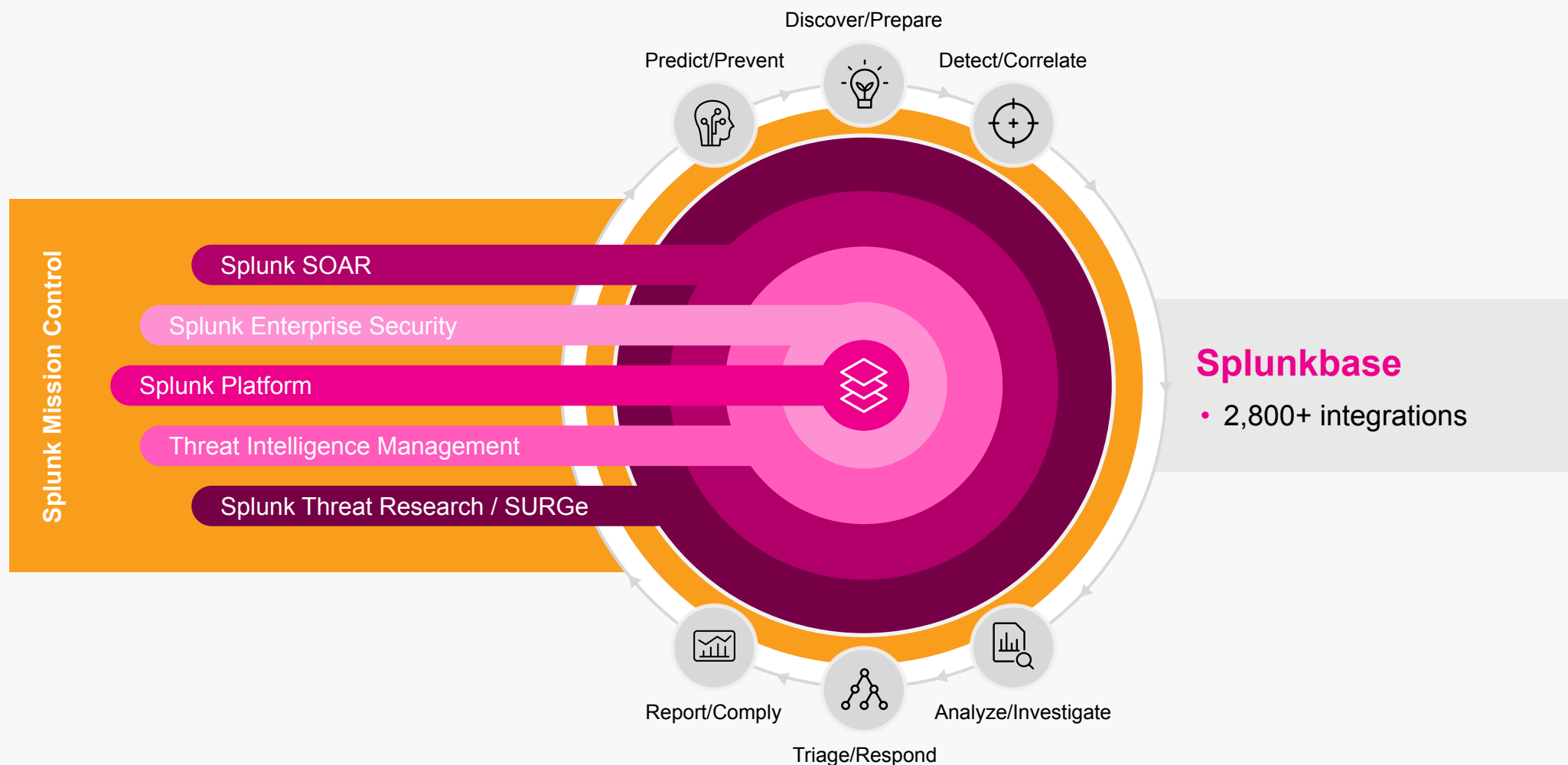
Interact with malicious content in a dedicated, unattributable environment

Fully automate end-to-end threat analysis and response workflow

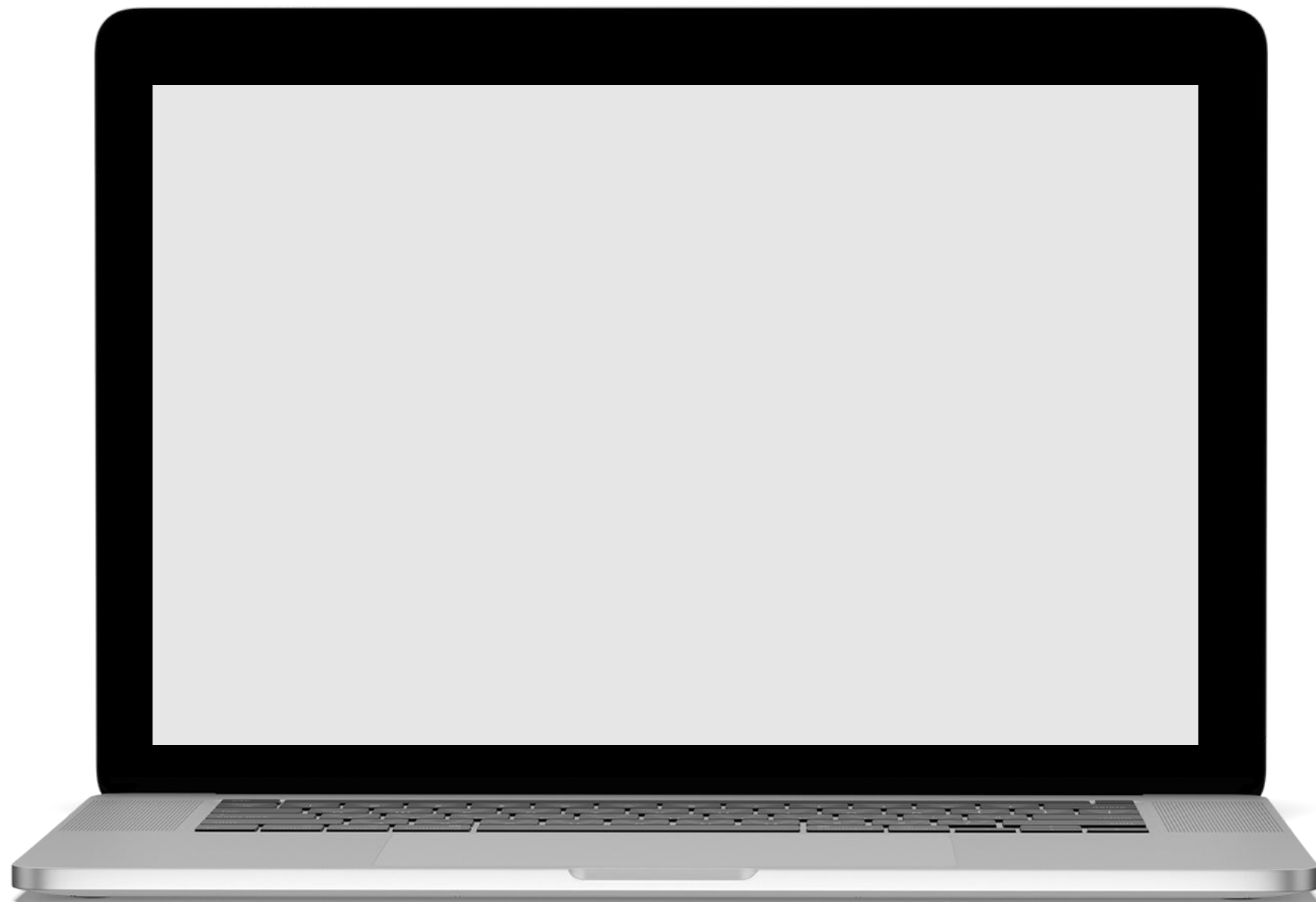


Splunk Security for Threat Detection, Investigation and Response

The tools you need to build a modern, data-centric SOC



Demo



The path to greater resilience



Splunk Leads the Way



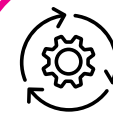
9 years

8 consecutive years as a
Leader in the SIEM MQ
by Gartner 2021



#1

Market share in
ITOM and SIEM by
Gartner 2021



Outperformer

Only “Outperformer”
for Cloud Observability,
Gigaom Radar 2021

In One Platform Accessible to all Your Business' Consumers

Shared tooling to drive resilience across critical consumer groups



Security Operations

- Security Monitoring
- Incident Management
- Advanced Threat Detection
- Insider Threats
- Incident Investigation and Forensics
- SOC Automation & Orchestration
- Compliance
- ICS Security



IT Operations

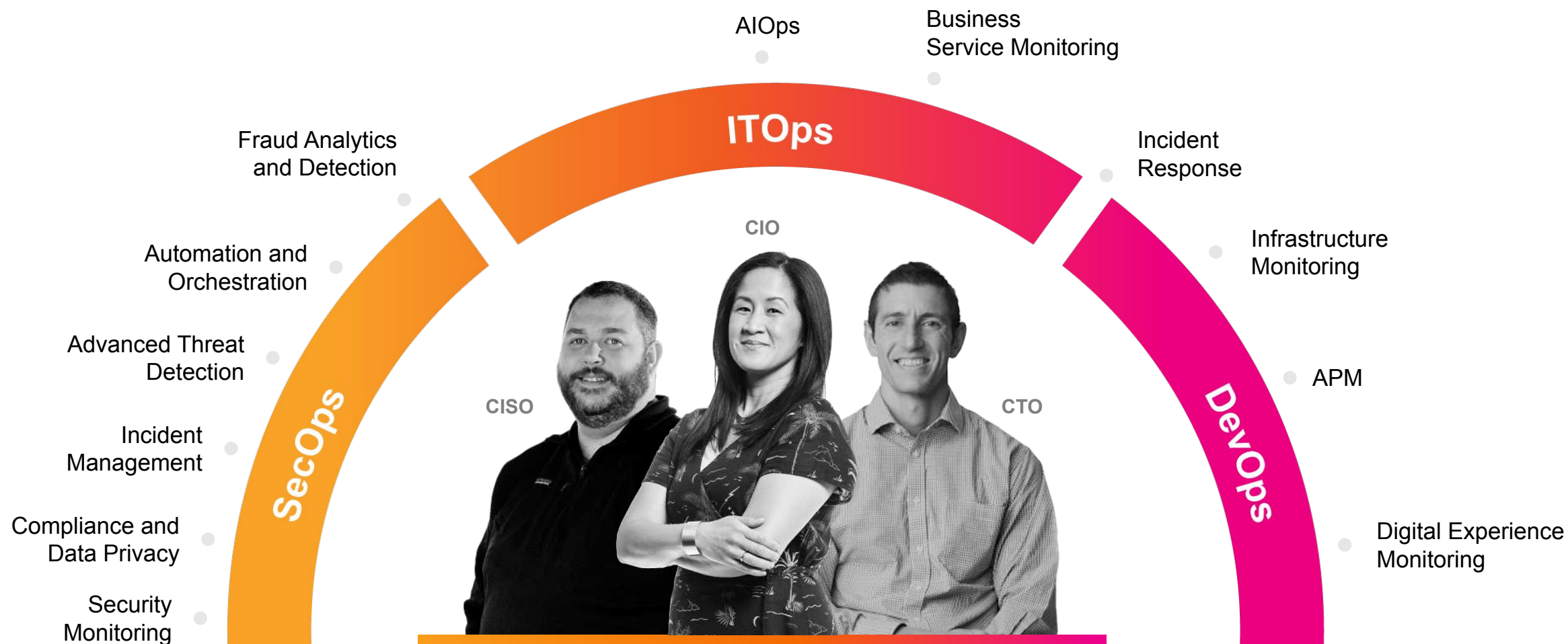
- Analytics for IT Troubleshooting
- Predictive Analytics
- SDKs for GO, Python, JavaScript
- Developer APIs
- Customer Experience Optimization
- Container Monitoring
- Infrastructure Monitoring
- High Volume, Low Cost Storage



DevOps

- Real-Time Observability with Monitoring and Diagnostics
- Infrastructure Monitoring
- Application Performance Monitoring
- Synthetics Monitoring
- Real User Monitoring
- Container Monitoring
- Distributed Tracing

We Bring Your Digital Teams Together



The Unified Security and Observability Platform

Thank You

