Observability Overview

splunk>

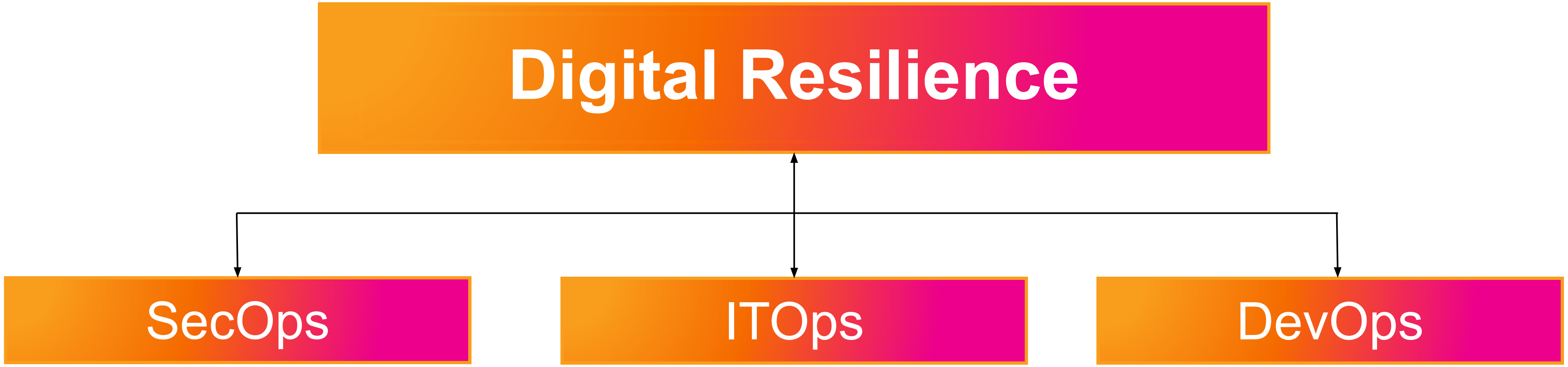
Will Cappelli

Observability Strategist, Splunk

Rachel Palmer

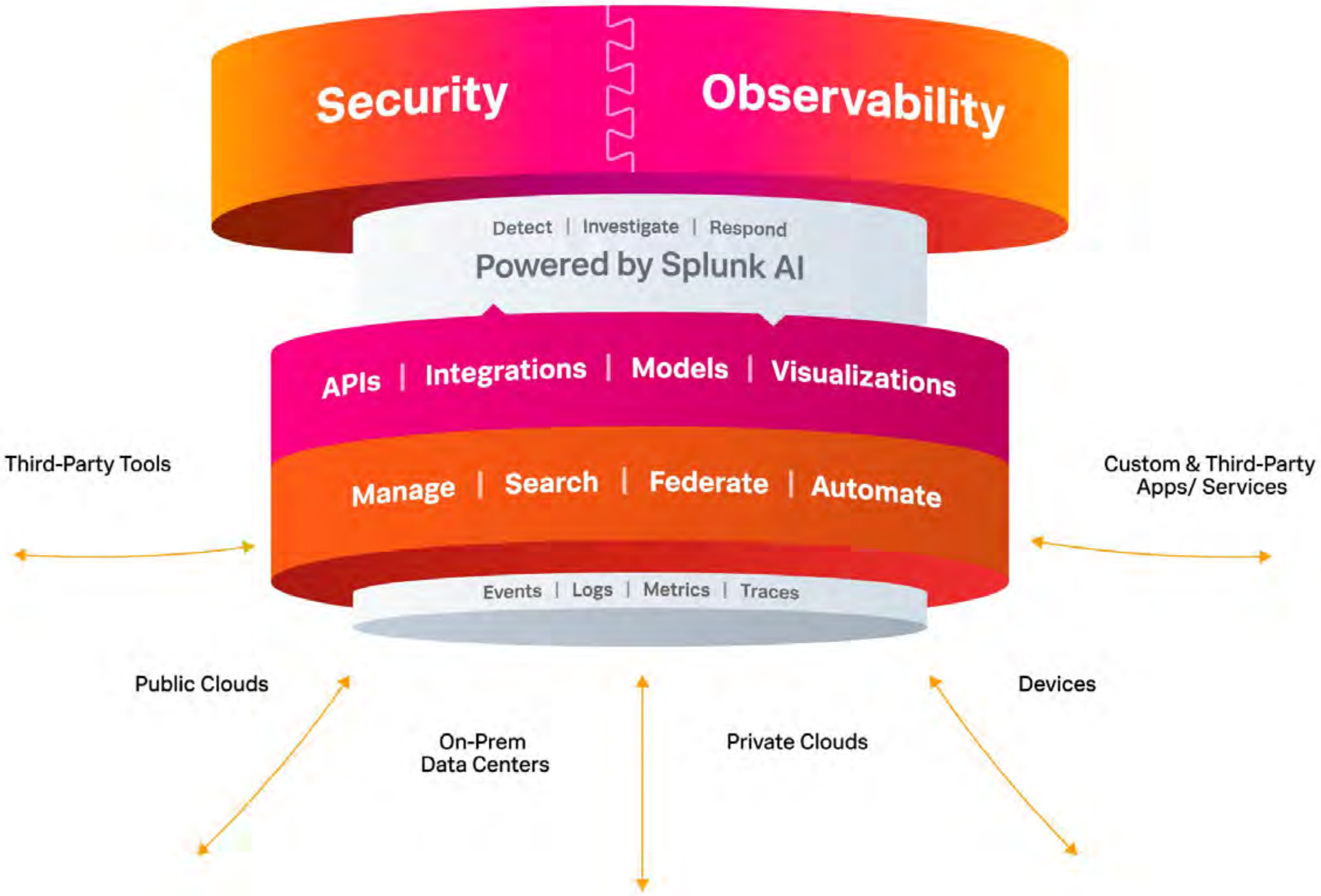
Observability Advisor, Splunk

Observability (O11y) is part of Resilience



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
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

A Leader

Gartner® Magic Quadrant™ for SIEM

A Leader

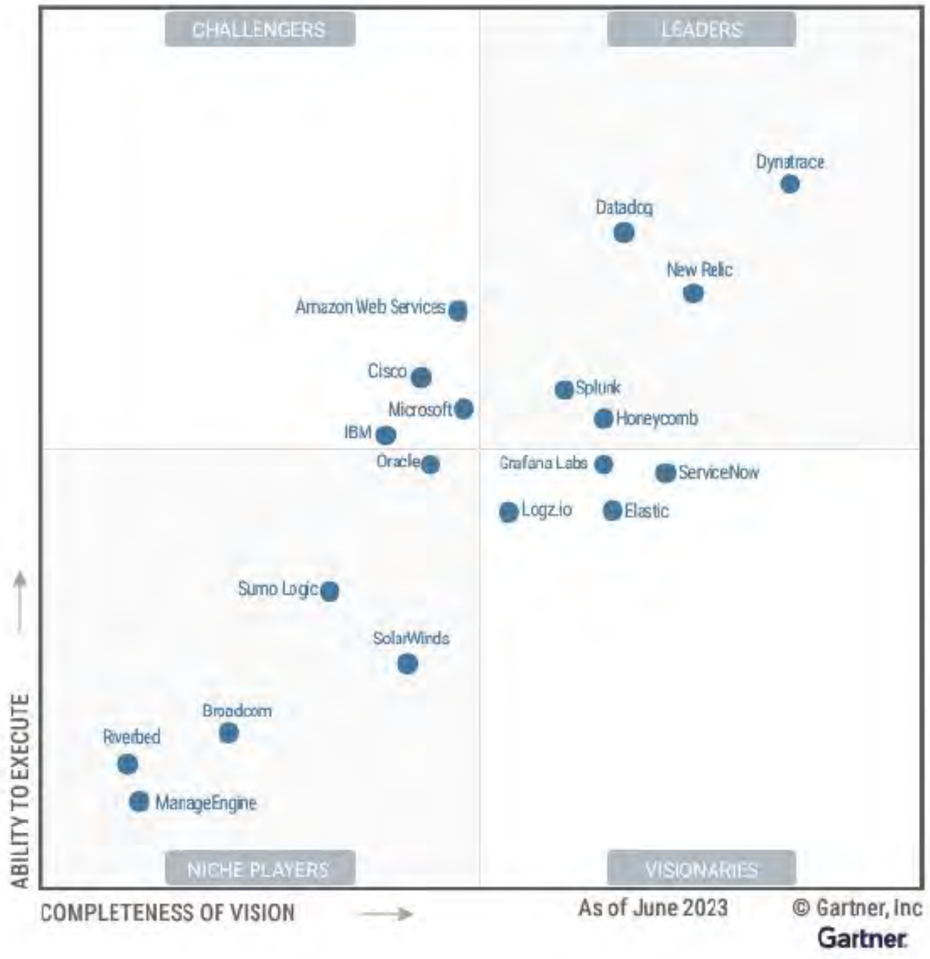
Gartner® Magic Quadrant™ for APM and Observability

2022 Gartner Magic Quadrant for Security Information and Event Management | 2023 Magic Quadrant for Application Performance Monitoring and Observability | 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.

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

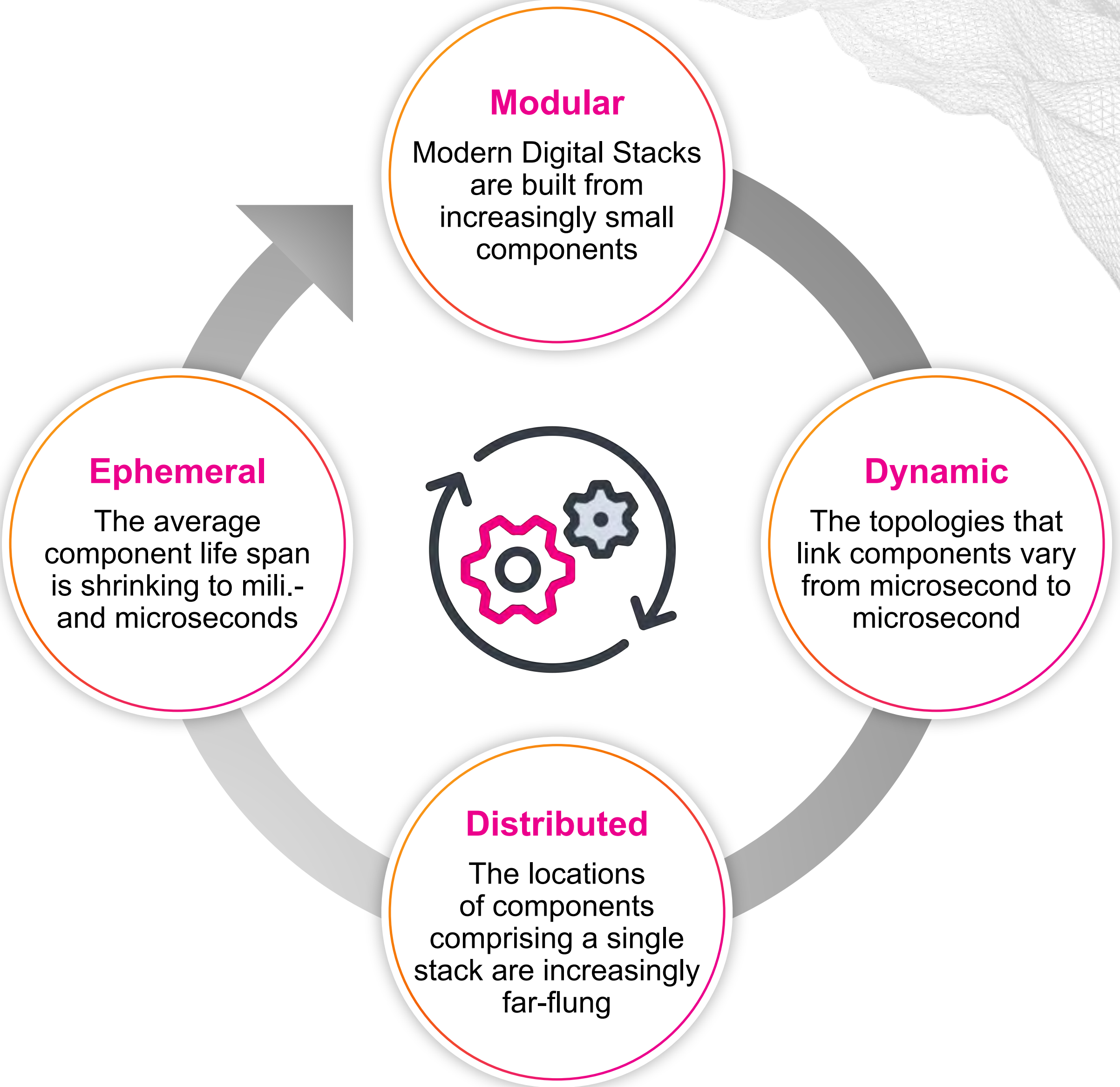
Splunk O11y is a Gartner MQ Leader

Finally! It’s taken 3 years hard work…



- 2023 Gartner MQ for APM + Observability Leader
- Splunk is the only new entrant in the leadership quadrant
- Strengths include:
  - OpenTelemetry support
  - Expanding coverage
  - Scalability

System
Complexity



Modular

Modern Digital Stacks are built from increasingly small components

Dynamic

The topologies that link components vary from microsecond to microsecond

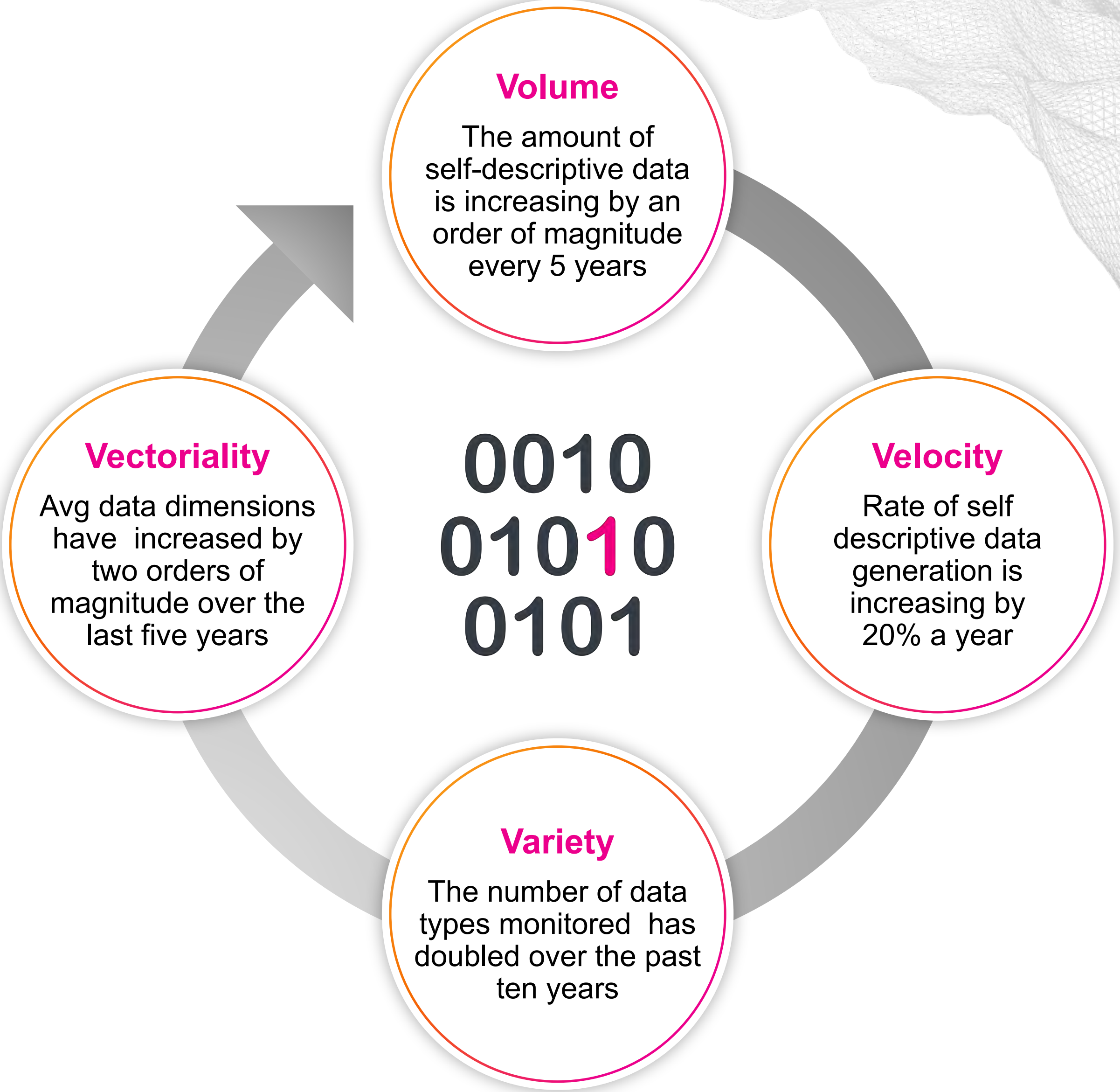
Distributed

The locations of components comprising a single stack are increasingly far-flung

Ephemeral

The average component life span is shrinking to mili.- and microseconds

Data
Complexity



Volume

The amount of self-descriptive data is increasing by an order of magnitude every 5 years

Velocity

Rate of self descriptive data generation is increasing by 20% a year

Variety

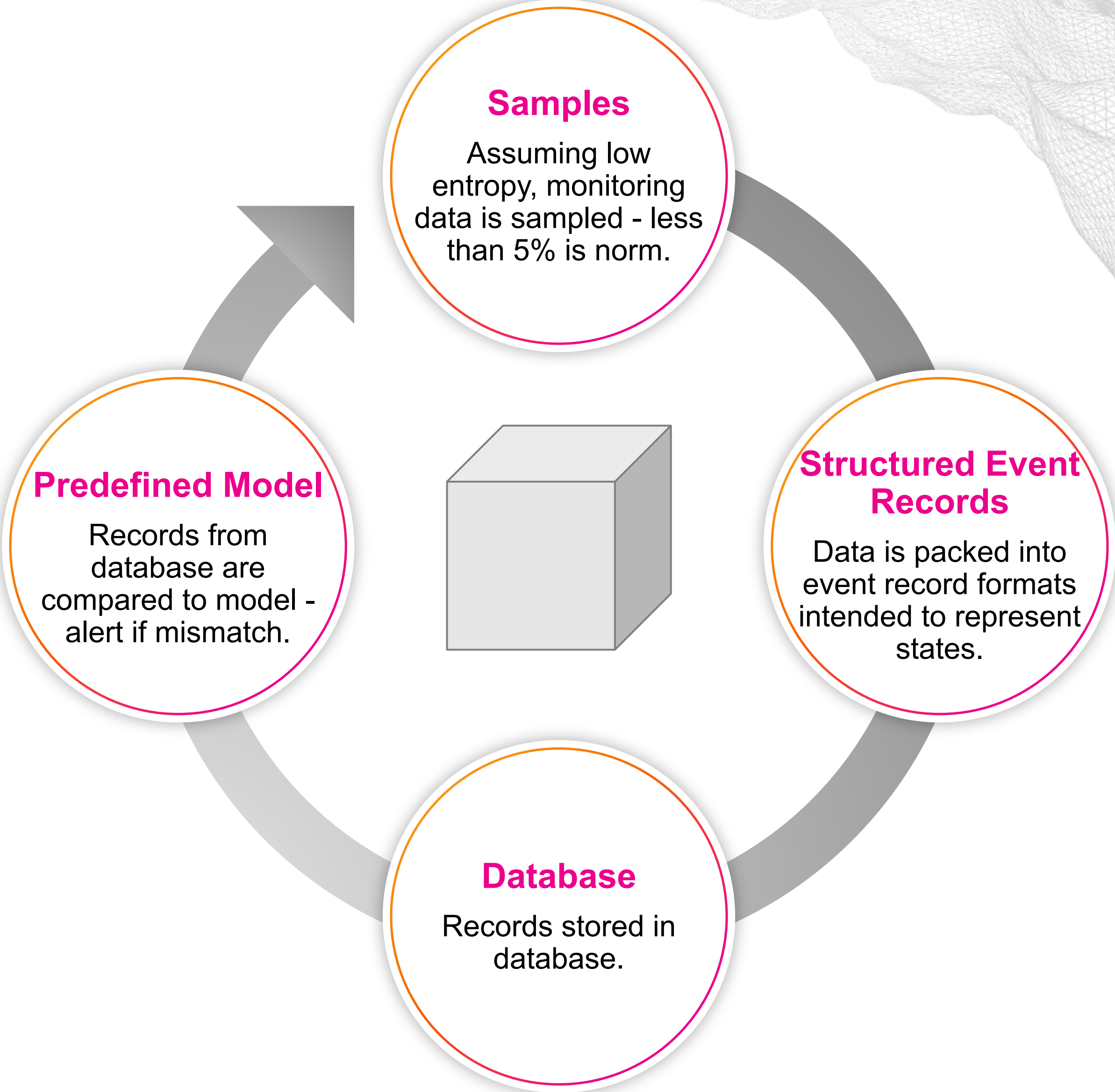
The number of data types monitored has doubled over the past ten years

Vectoriality

Avg data dimensions have increased by two orders of magnitude over the last five years

The Monitoring Design Plan

1975 - 2022



Samples

Assuming low entropy, monitoring data is sampled - less than 5% is norm.

Structured Event Records

Data is packed into event record formats intended to represent states.

Database

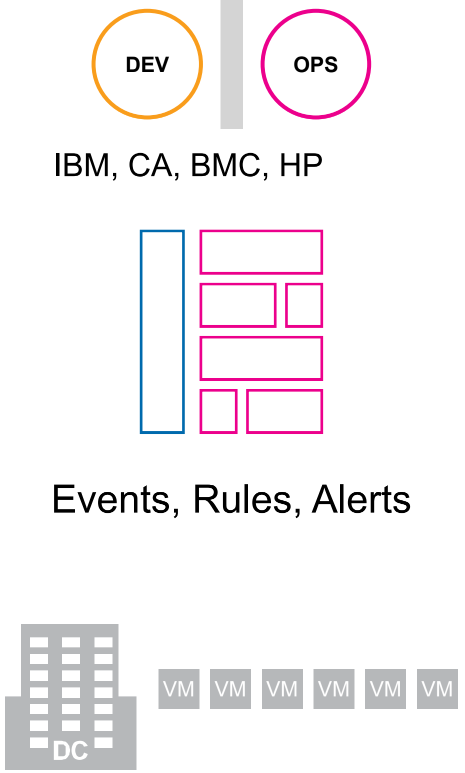
Records stored in database.

Predefined Model

Records from database are compared to model - alert if mismatch.

But, it doesn’t work anymore!

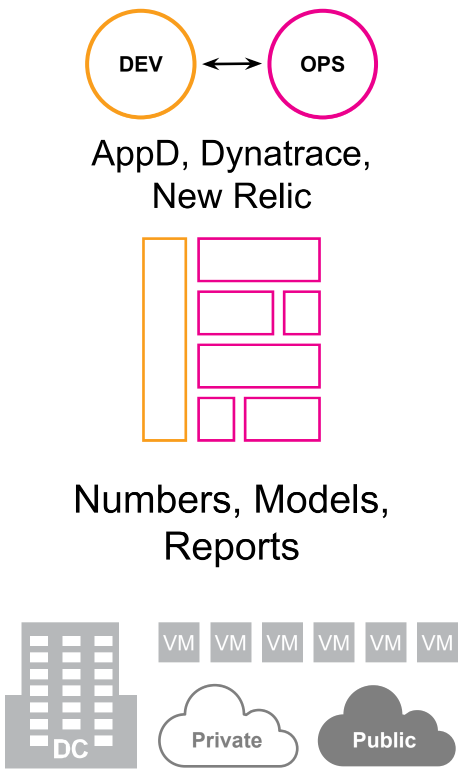
Monolithic Apps
(2007 -2011)



IBM, CA, BMC, HP

Events, Rules, Alerts

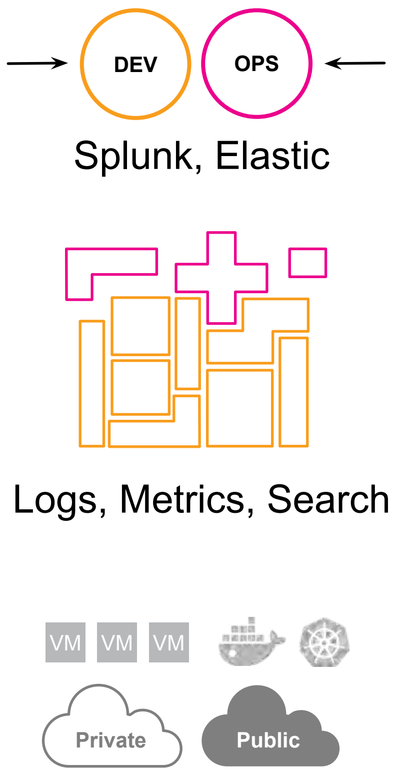
Multi-Tier Apps
(2011 - 2015)



AppD, Dynatrace, New Relic

Numbers, Models, Reports

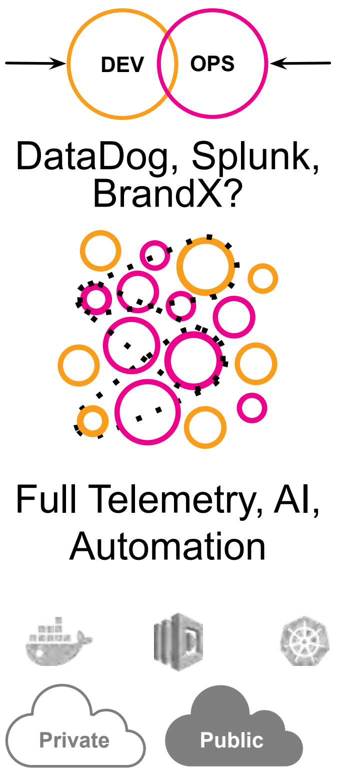
Modular Apps
(2015 -2020)



Splunk, Elastic

Logs, Metrics, Search

Ephemeral Apps
(2020 - ?)



DataDog, Splunk, BrandX?

Full Telemetry, AI, Automation

Observability

The Three Pillars

WHAT'S HAPPENING?

METRICS
Detect

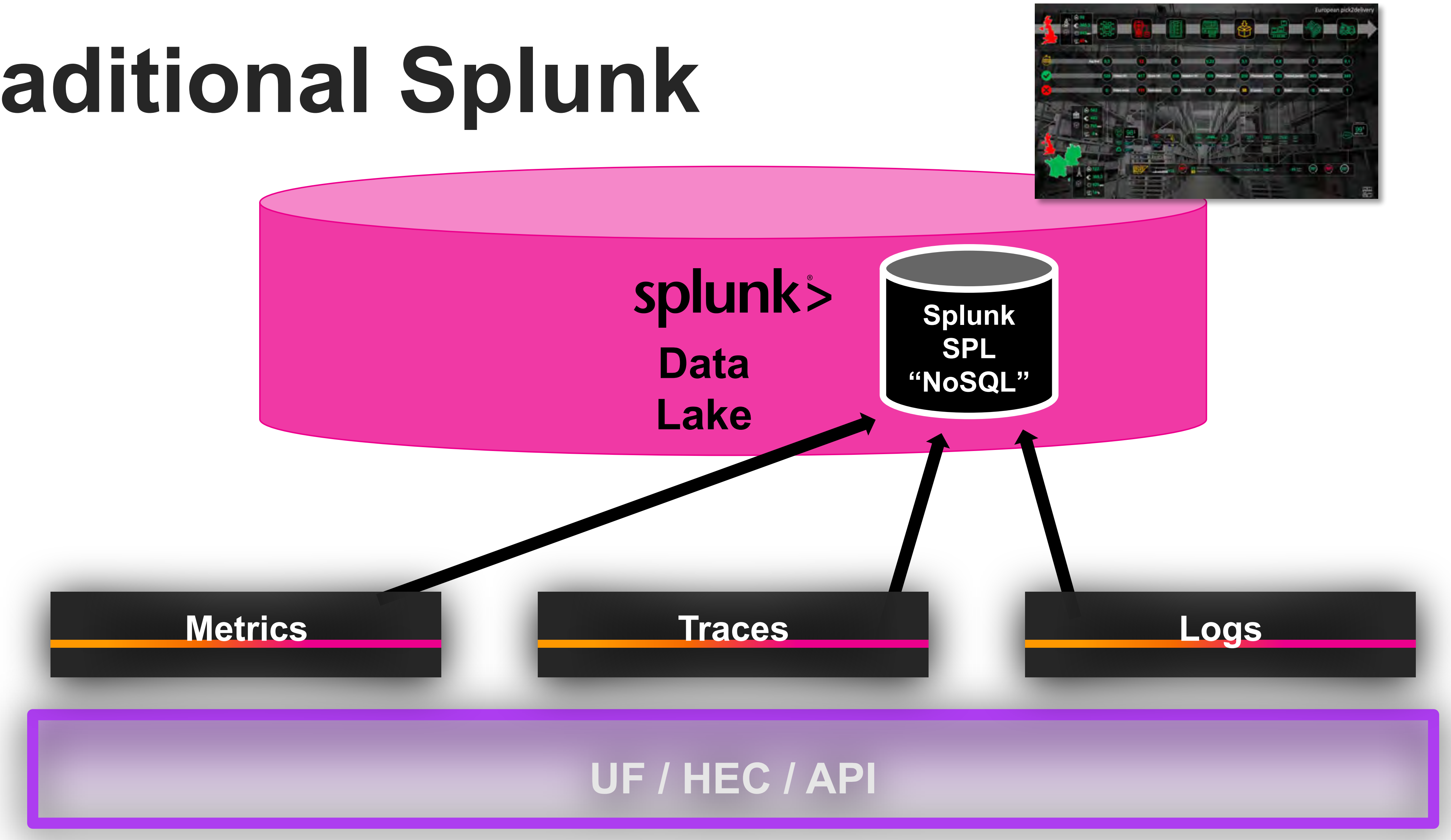
WHERE IS IT HAPPENING?

TRACES
Troubleshoot

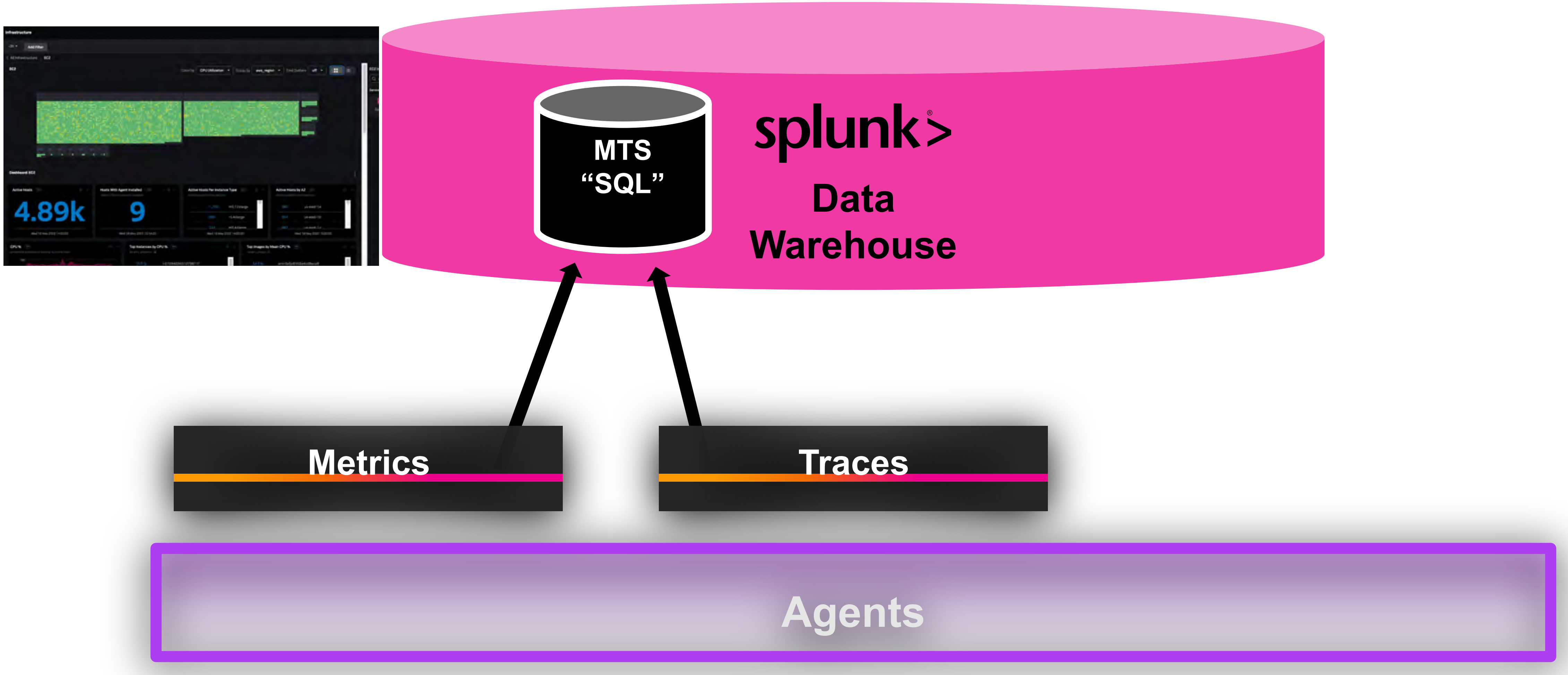
WHY IS IT HAPPENING?

EVENTS / LOGS
Pinpoint

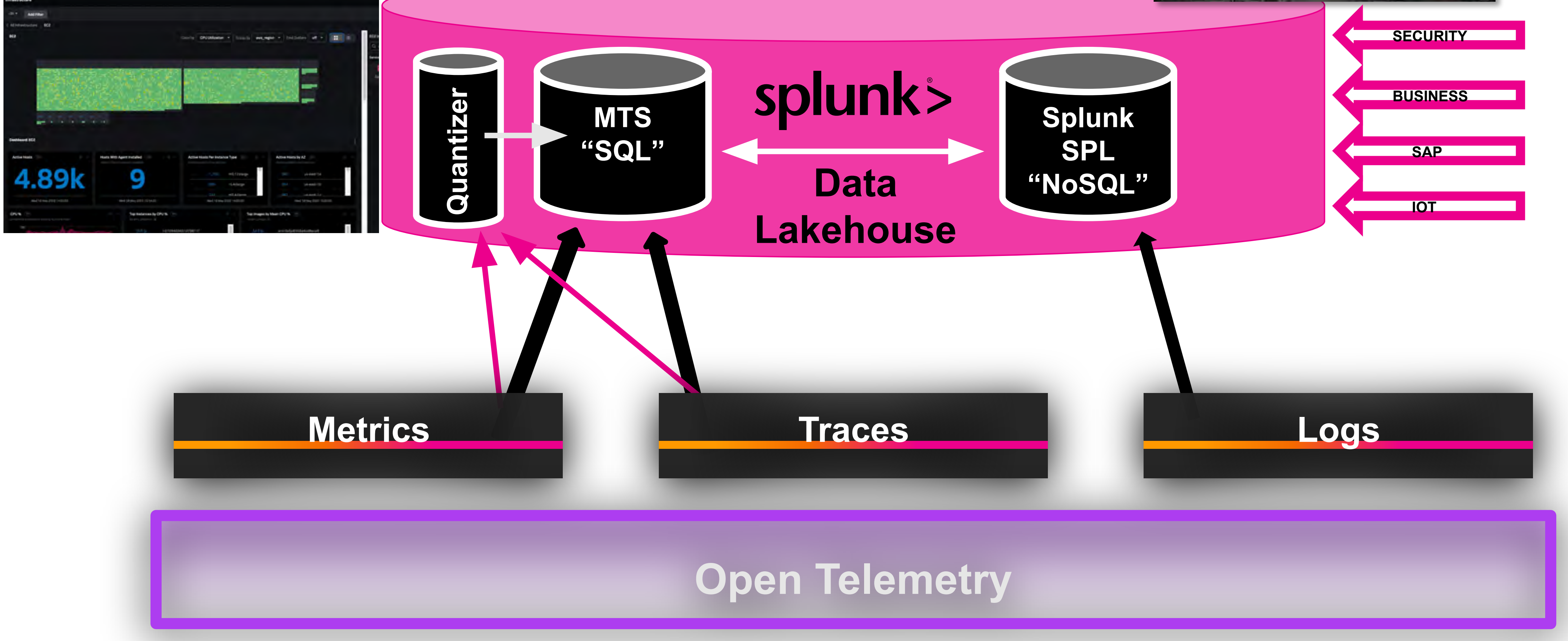
Traditional Splunk



Traditional IM / APM

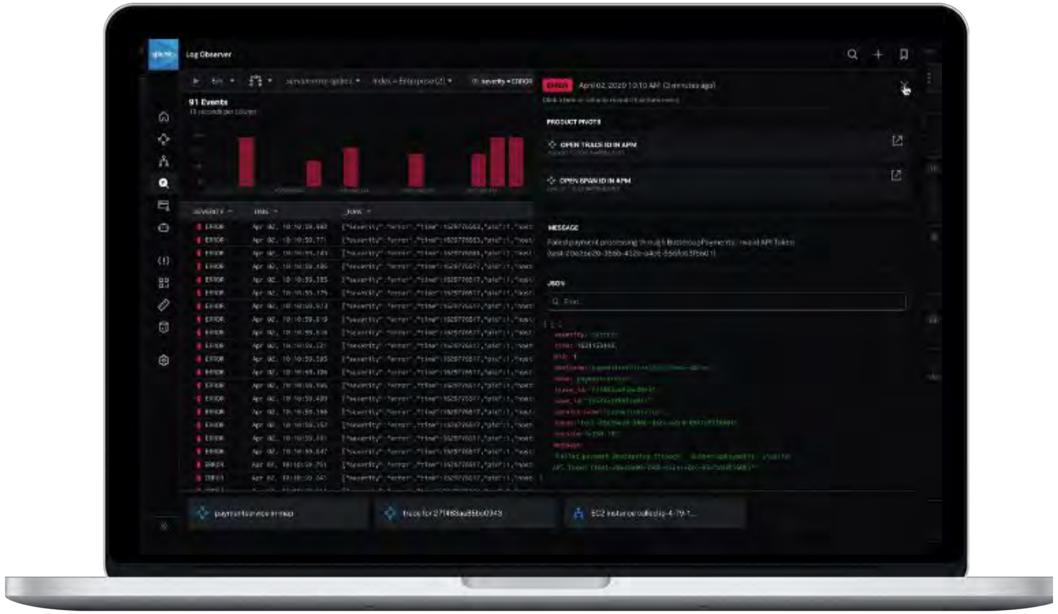


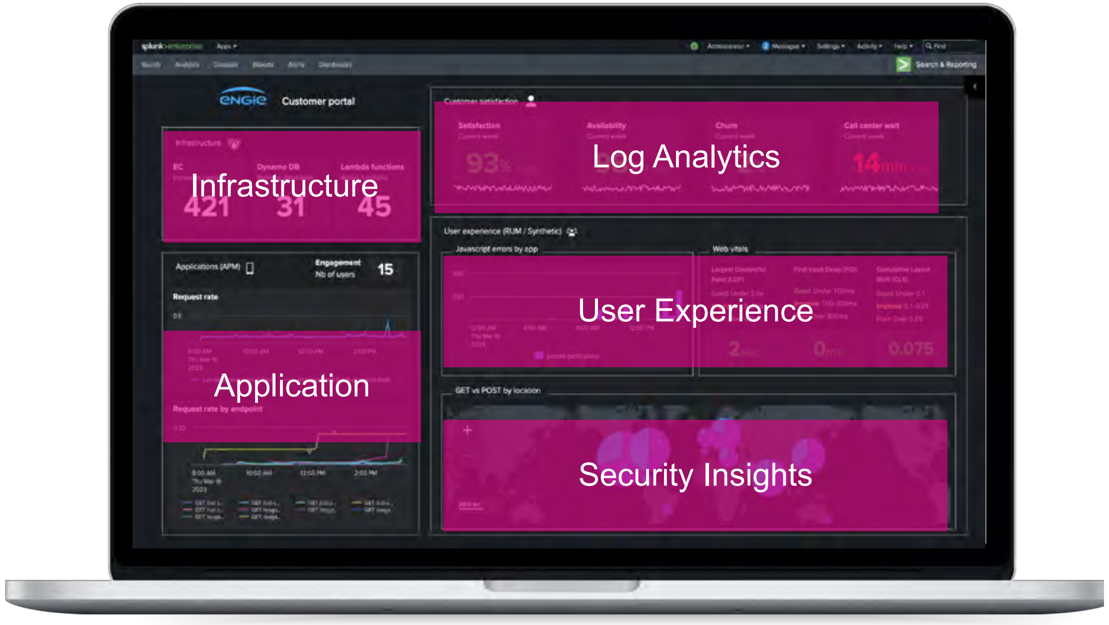
Splunk with O11Y



Who are you?

How do you want to consume your information?





Log Analytics

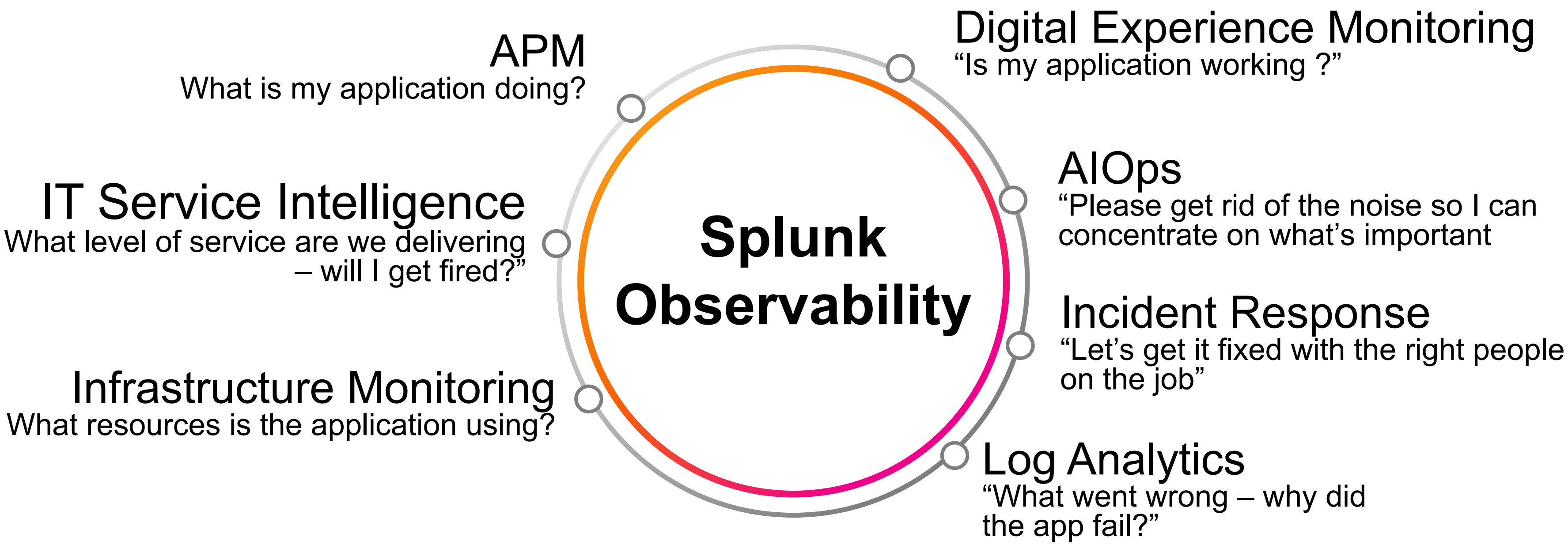
“The Engineer”

- Real Time
- What went wrong?
- How do I fix it?

“The Service Owner”

- Full Visibility
- How is the Service Running?
- Is there any action we need to take?

Splunk Observability Components



Splunk Observability

APM
What is my application doing?

IT Service Intelligence
What level of service are we delivering – will I get fired?"

Infrastructure Monitoring
What resources is the application using?

Digital Experience Monitoring
"Is my application working ?"

AIOps
"Please get rid of the noise so I can concentrate on what's important

Incident Response
"Let's get it fixed with the right people on the job"

Log Analytics
"What went wrong – why did the app fail?"

Full-Stack | Real-Time | Analytics-Powered | Enterprise-Grade | OpenTelemetry-Native

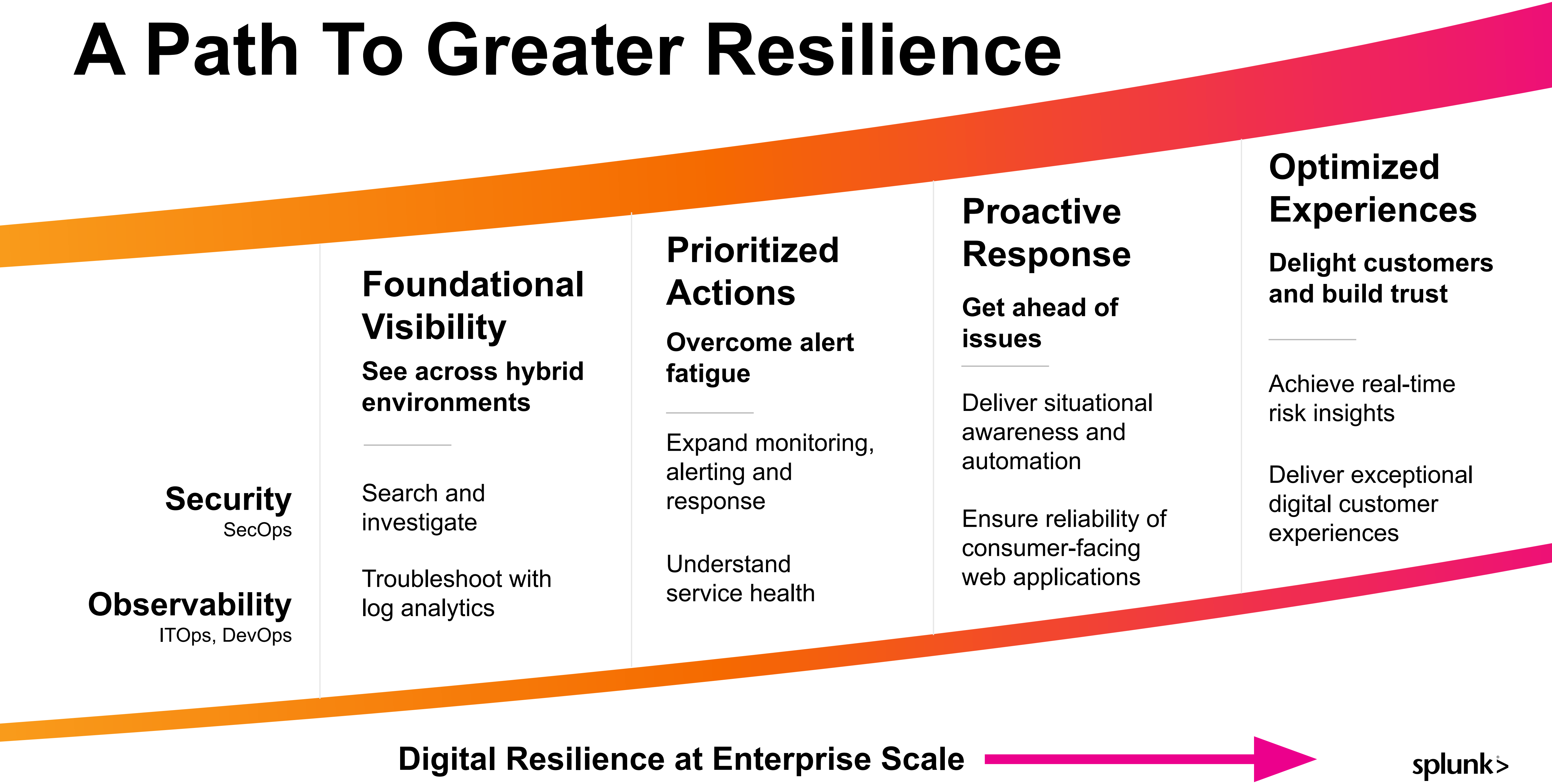
On-Prem | Hybrid Cloud | Multi-Cloud | Cloud-Native

Why Splunk for Observability?

Visibility and control across your all your business services, apps and infrastructure

Full-Stack	Full fidelity data collection and correlation across metrics, traces, logs, events and services.
Real-Time Streaming	Streaming analytics enable alerting in seconds
Analytics-Powered	Built-in AI/ML to deliver predictive analytics, more accurate alerts and “no dead-end” investigations
Enterprise-Grade	One platform and integrated suite to support many teams and all your environments
OpenTelemetry and Robust Ecosystem	Leader in OpenTelemetry. Extensive community of thousands Splunk developers, apps and add-ons

A Path To Greater Resilience



Security
SecOps

Observability
ITOps, DevOps

Foundational Visibility

See across hybrid environments

Search and investigate

Troubleshoot with log analytics

Prioritized Actions

Overcome alert fatigue

Expand monitoring, alerting and response

Understand service health

Proactive Response

Get ahead of issues

Deliver situational awareness and automation

Ensure reliability of consumer-facing web applications

Optimized Experiences

Delight customers and build trust

Achieve real-time risk insights

Deliver exceptional digital customer experiences

Digital Resilience at Enterprise Scale →

splunk>

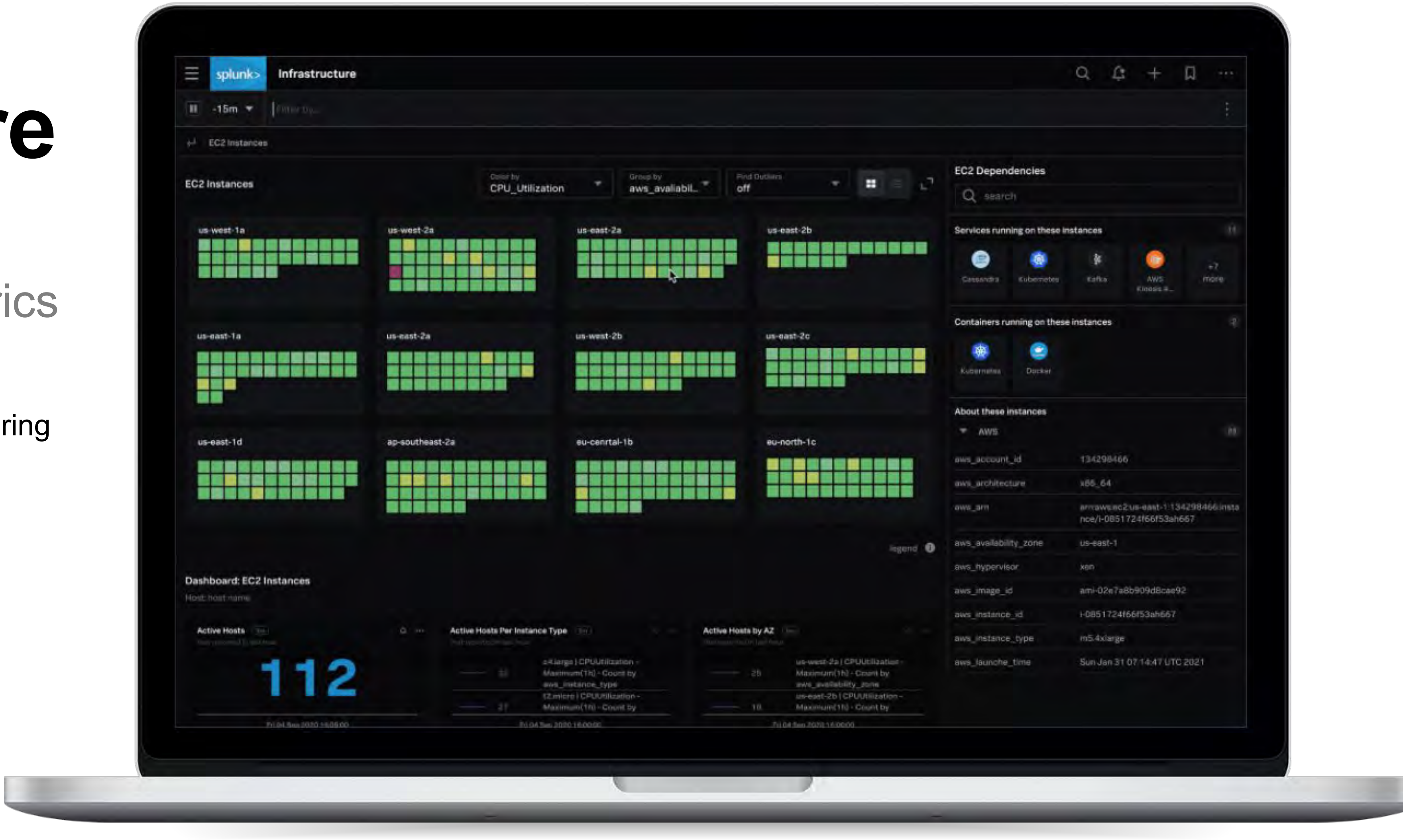
Thank You

splunk>

Splunk Infrastructure Monitoring

Real-time streaming metrics

- On-prem & hybrid-/multi-cloud monitoring
- Kubernetes & container monitoring
- Serverless monitoring
- Pre-built dashboards & hundreds of integrations
- Automatic service discovery
- Instant, analytics-driven alerting
- Seamless slice-and-dice
- Custom & high resolution metrics



Color by: CPU_Utilization
Group by: aws_availabil...
Find Outliers: off

Dashboard: EC2 Instances

Host: host name

22	c4.large | CPUUtilization - Maximum(1h) - Count by aws_instance_type
21	t2.micro | CPUUtilization - Maximum(1h) - Count by

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

Fri 04 Sep 2020 16:00:00

About these instances

AWS

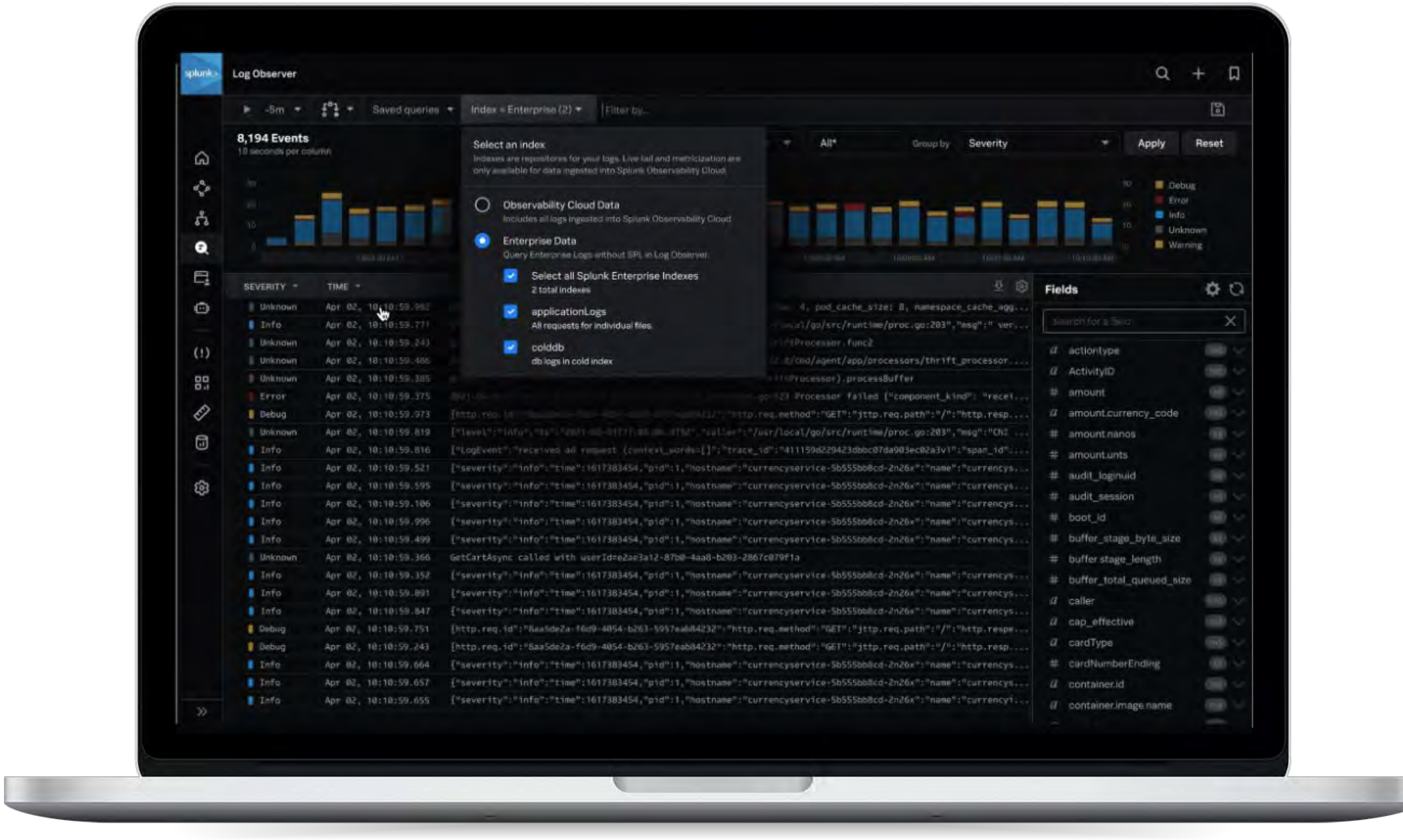
aws_account_id	134298466
aws_architecture	x86_64
aws_arn	arn:aws:ec2:us-east-1:134298466:instance/i-0851724f66f53ah667
aws_availability_zone	us-east-1
aws_hypervisor	xen
aws_image_id	ami-02e7a8b909d8cae92
aws_instance_id	i-0851724f66f53ah667
aws_instance_type	m5.4xlarge
aws_launche_time	Sun Jan 31 07:14:47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

splunk>

Log Observer Connect

Advanced observability capabilities with Splunk Enterprise and Splunk Cloud data

- **Centralize your data.** Leverage the power of Splunk Enterprise and Splunk Cloud data in-context with metrics and traces
- **Get started quickly.** Start using Log Observer Connect in less than 10 minutes
- Access to no-code Log Observer experience and related content links for **faster troubleshooting and root-cause analysis**
- **Extend the value of your Splunk investment** at no additional cost



Select an index

Indexes are repositories for your logs. Live tail and metricization are only available for data ingested into Splunk Observability Cloud

○ Observability Cloud Data
Includes all logs ingested into Splunk Observability Cloud

● Enterprise Data
Query Enterprise Logs without SPL in Log Observer

☑ Select all Splunk Enterprise Indexes
2 total indexes

☑ applicationLogs
All requests for individual files.

☑ colddb
db logs in cold index

```
SEVERITY   TIME
Unknown    Apr 02, 10:10:59.982    4, pod_cache_size: 8, namespace_cache_agg...
Info       Apr 02, 10:10:59.771    l/go/src/runtime/proc.go:203","msg":" ver...
Unknown    Apr 02, 10:10:59.243    Processor.func2
Unknown    Apr 02, 10:10:59.486    /cmd/agent/app/processors/thrift_processor....
Unknown    Apr 02, 10:10:59.385    Processor).processBuffer
Error      Apr 02, 10:10:59.375    Processor failed {"component_kind": "recei...
Debug      Apr 02, 10:10:59.973    {http.req.id "http.req.method":"GET":"jttp.req.path":"/":"http.resp....
Unknown    Apr 02, 10:10:59.819    {"level":"info", "caller":"/usr/local/go/src/runtime/proc.go:203","msg":"CNI ...
Info       Apr 02, 10:10:59.816    {"LogEvent":"received ad request (context_words=[]":"trace_id":"411159d229423dbbc07da903ec02a3v1":"span_id":...
Info       Apr 02, 10:10:59.521    {"severity":"info":"time":1617383454,"pid":1,"hostname":"currencyservice-5b555bb8cd-2n26x":"name":"currencys...
Info       Apr 02, 10:10:59.595    {"severity":"info":"time":1617383454,"pid":1,"hostname":"currencyservice-5b555bb8cd-2n26x":"name":"currencys...
Info       Apr 02, 10:10:59.106    {"severity":"info":"time":1617383454,"pid":1,"hostname":"currencyservice-5b555bb8cd-2n26x":"name":"currencys...
Info       Apr 02, 10:10:59.996    {"severity":"info":"time":1617383454,"pid":1,"hostname":"currencyservice-5b555bb8cd-2n26x":"name":"currencys...
Info       Apr 02, 10:10:59.499    {"severity":"info":"time":1617383454,"pid":1,"hostname":"currencyservice-5b555bb8cd-2n26x":"name":"currencys...
Unknown    Apr 02, 10:10:59.366    GetCartAsync called with userId=e2ae3a12-87b0-4aa8-b203-2867c079f1a
Info       Apr 02, 10:10:59.352    {"severity":"info":"time":1617383454,"pid":1,"hostname":"currencyservice-5b555bb8cd-2n26x":"name":"currencys...
Info       Apr 02, 10:10:59.891    {"severity":"info":"time":1617383454,"pid":1,"hostname":"currencyservice-5b555bb8cd-2n26x":"name":"currencys...
Info       Apr 02, 10:10:59.847    {"severity":"info":"time":1617383454,"pid":1,"hostname":"currencyservice-5b555bb8cd-2n26x":"name":"currencys...
Debug      Apr 02, 10:10:59.751    {http.req.id":"8aa5de2a-f6d9-4054-b263-5957eab84232":"http.req.method":"GET":"jttp.req.path":"/":"http.respe...
Debug      Apr 02, 10:10:59.243    {http.req.id":"8aa5de2a-f6d9-4054-b263-5957eab84232":"http.req.method":"GET":"jttp.req.path":"/":"http.resp....
Info       Apr 02, 10:10:59.664    {"severity":"info":"time":1617383454,"pid":1,"hostname":"currencyservice-5b555bb8cd-2n26x":"name":"currencys...
Info       Apr 02, 10:10:59.657    {"severity":"info":"time":1617383454,"pid":1,"hostname":"currencyservice-5b555bb8cd-2n26x":"name":"currencys...
Info       Apr 02, 10:10:59.655    {"severity":"info":"time":1617383454,"pid":1,"hostname":"currencyservice-5b555bb8cd-2n26x":"name":"currencyi...
```

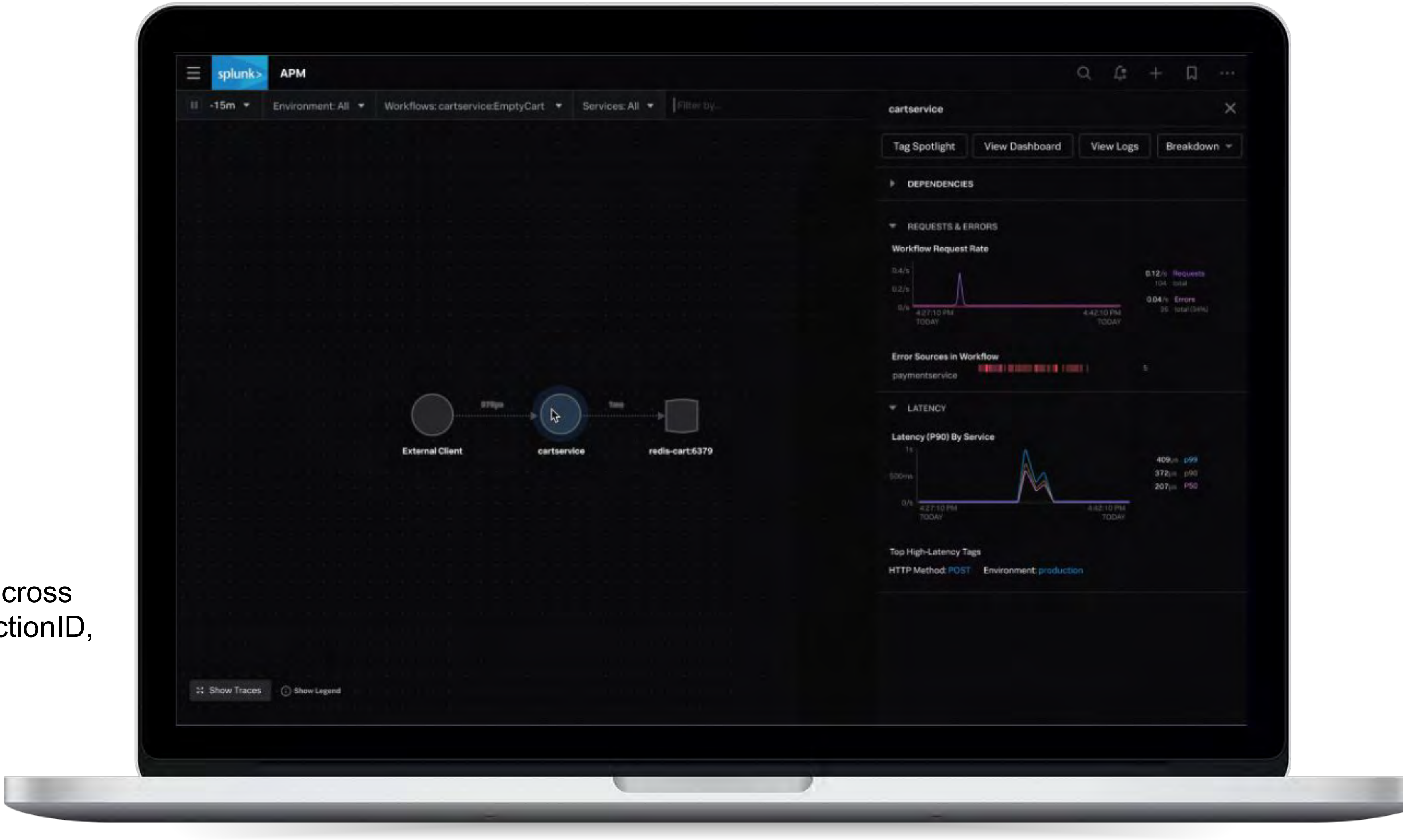
Fields

- actiontype
- ActivityID
- amount
- amount.currency_code
- amount.nanos
- amount.unts
- audit_loginuid
- audit_session
- boot_id
- buffer_stage_byte_size
- buffer stage_length
- buffer_total_queued_size
- caller
- cap_effective
- cardType
- cardNumberEnding
- container.id
- container.image.name

Splunk APM

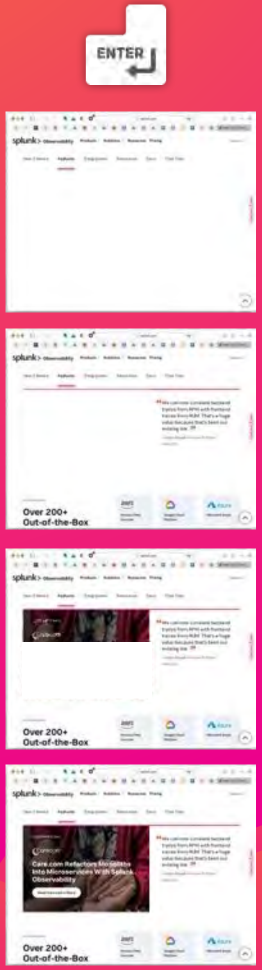
Application Monitoring and Troubleshooting

- Lightweight, open instrumentation
- Rich, dynamic service map
- Full-stack correlation
- NoSample™ full-fidelity ingestion
- Unlimited cardinality exploration- search across any tag or dimension (UserName, TransactionID, Geography, etc.)
- Speedy UI, analytics & drilldowns
- AI-driven alerting and directed troubleshooting

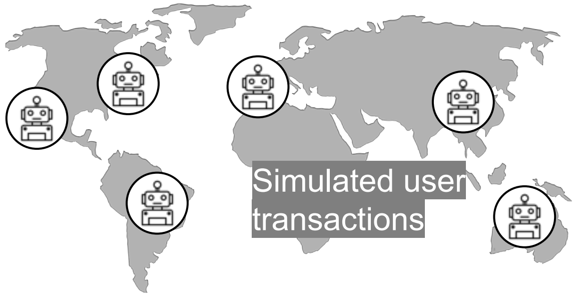


Digital Experience Monitoring

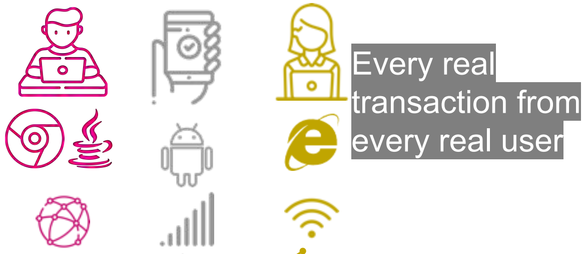
What the USER sees

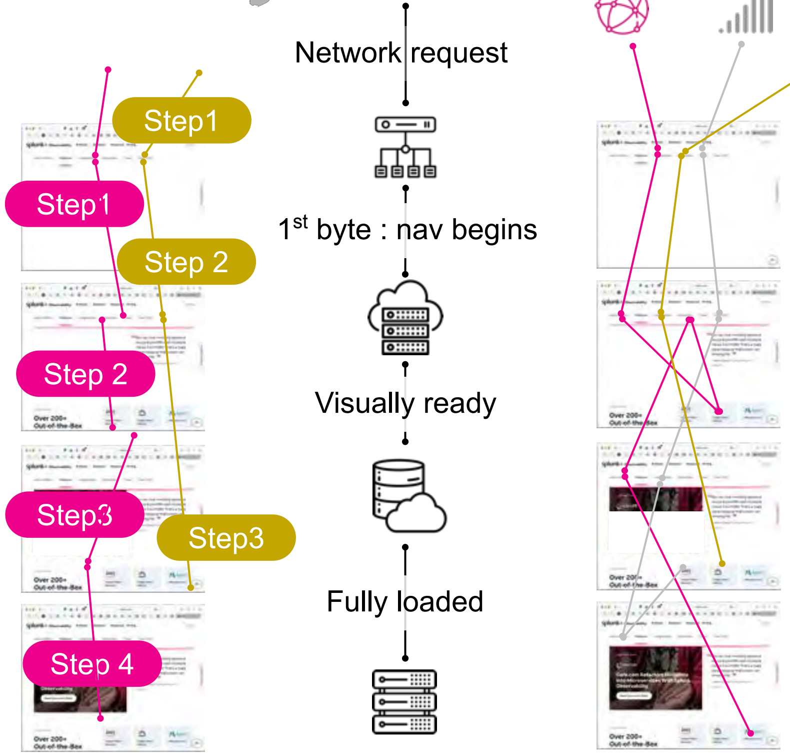


What SYNTHETIC does



What RUM does





Transaction monitoring

Availability monitoring

Competition benchmarking

Customer journey tracking

Overall web performance

User Context

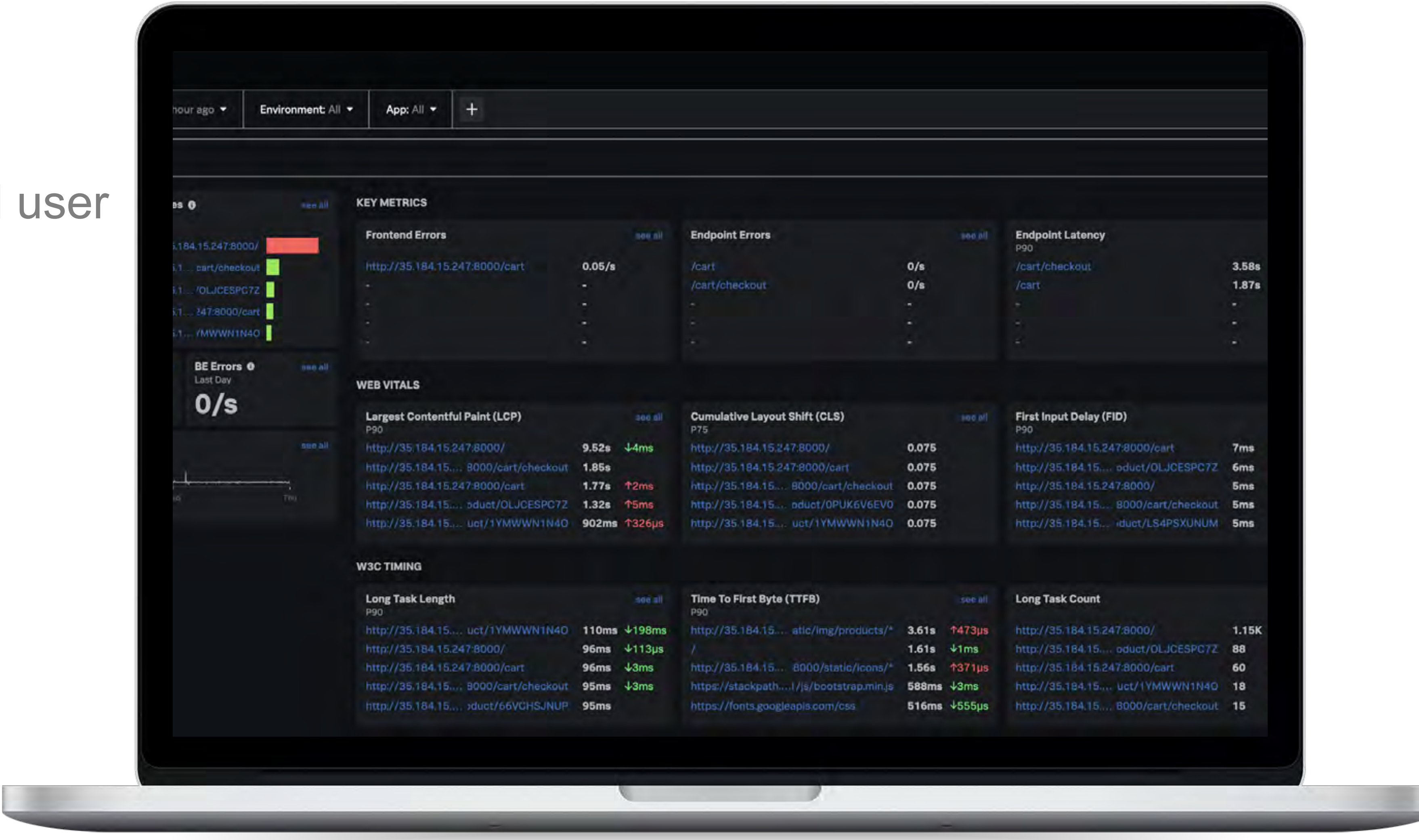
Web performance / 3rd party tag monitoring

splunk> turn data into doing

Splunk RUM

Industry’s only end-to-end, full-fidelity visibility into end user experiences

- Track and monitor continuously for performance
- Elevate quality end-user experiences in real time
- Simplify troubleshooting for faster resolution
- Unlock user data through open standards
- Built for Observability, with flexibility and choice
- Supports JavaScript (browsers), and iOS and Android native apps



KEY METRICS

Frontend Errors see all

http://35.184.15.247:8000/cart	0.05/s
-	-
-	-
-	-
-	-

Endpoint Errors see all

/cart	0/s
/cart/checkout	0/s
-	-
-	-
-	-

Endpoint Latency
P90

/cart/checkout	3.58s
/cart	1.87s
-	-
-	-
-	-

WEB VITALS

Largest Contentful Paint (LCP) see all
P90

http://35.184.15.247:8000/	9.52s	↓4ms
http://35.184.15.… 8000/cart/checkout	1.85s	
http://35.184.15.247:8000/cart	1.77s	↑2ms
http://35.184.15.… oduct/OLJCESPC7Z	1.32s	↑5ms
http://35.184.15.… uct/1YMWWN1N4O	902ms	↑326µs

Cumulative Layout Shift (CLS) see all
P75

http://35.184.15.247:8000/	0.075
http://35.184.15.247:8000/cart	0.075
http://35.184.15.… 8000/cart/checkout	0.075
http://35.184.15.… oduct/0PUK6V6EV0	0.075
http://35.184.15.… uct/1YMWWN1N4O	0.075

First Input Delay (FID)
P90

http://35.184.15.247:8000/cart	7ms
http://35.184.15.… oduct/OLJCESPC7Z	6ms
http://35.184.15.247:8000/	5ms
http://35.184.15.… 8000/cart/checkout	5ms
http://35.184.15.… iduct/LS4PSXUNUM	5ms

W3C TIMING

Long Task Length see all
P90

http://35.184.15.… uct/1YMWWN1N4O	110ms	↓198ms
http://35.184.15.247:8000/	96ms	↓113µs
http://35.184.15.247:8000/cart	96ms	↓3ms
http://35.184.15.… 8000/cart/checkout	95ms	↓3ms
http://35.184.15.… oduct/66VCHSJNUP	95ms	

Time To First Byte (TTFB) see all
P90

http://35.184.15.… atic/img/products/*	3.61s	↑473µs
/	1.61s	↓1ms
http://35.184.15.… 8000/static/icons/*	1.56s	↑371µs
https://stackpath.…l/js/bootstrap.min.js	588ms	↓3ms
https://fonts.googleapis.com/css	516ms	↓555µs

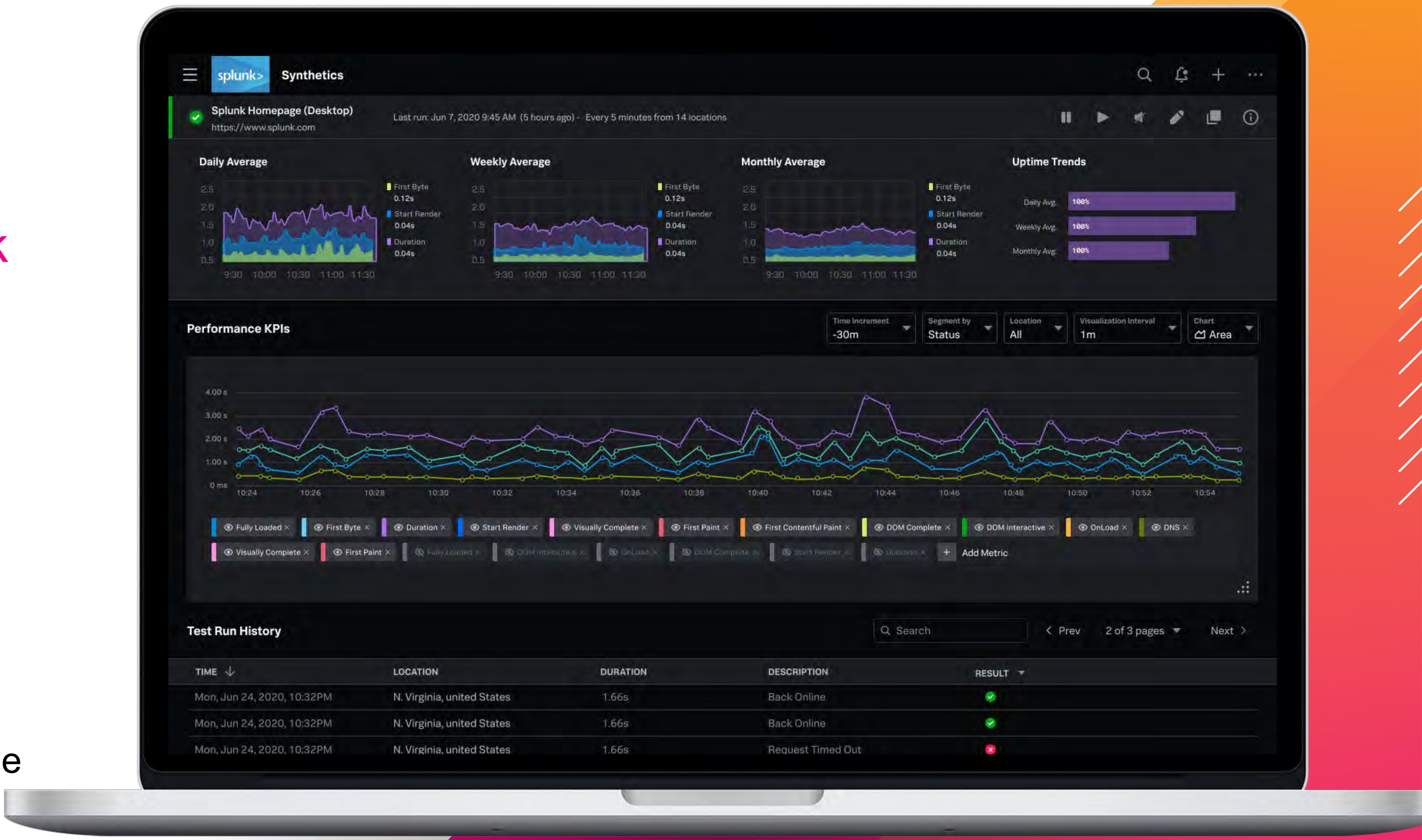
Long Task Count

http://35.184.15.247:8000/	1.15K
http://35.184.15.… oduct/OLJCESPC7Z	88
http://35.184.15.247:8000/cart	60
http://35.184.15.… uct/1YMWWN1N4O	18
http://35.184.15.… 8000/cart/checkout	15

Splunk Synthetics

Synthetic Monitoring Integrated into the Splunk Observability Platform

- Proactively detect issues in API and page performance, across entire user journeys
- Troubleshoot frontend and backend performance issues faster in a single UI
- Visualize the impact of new code on customer experience



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	✗

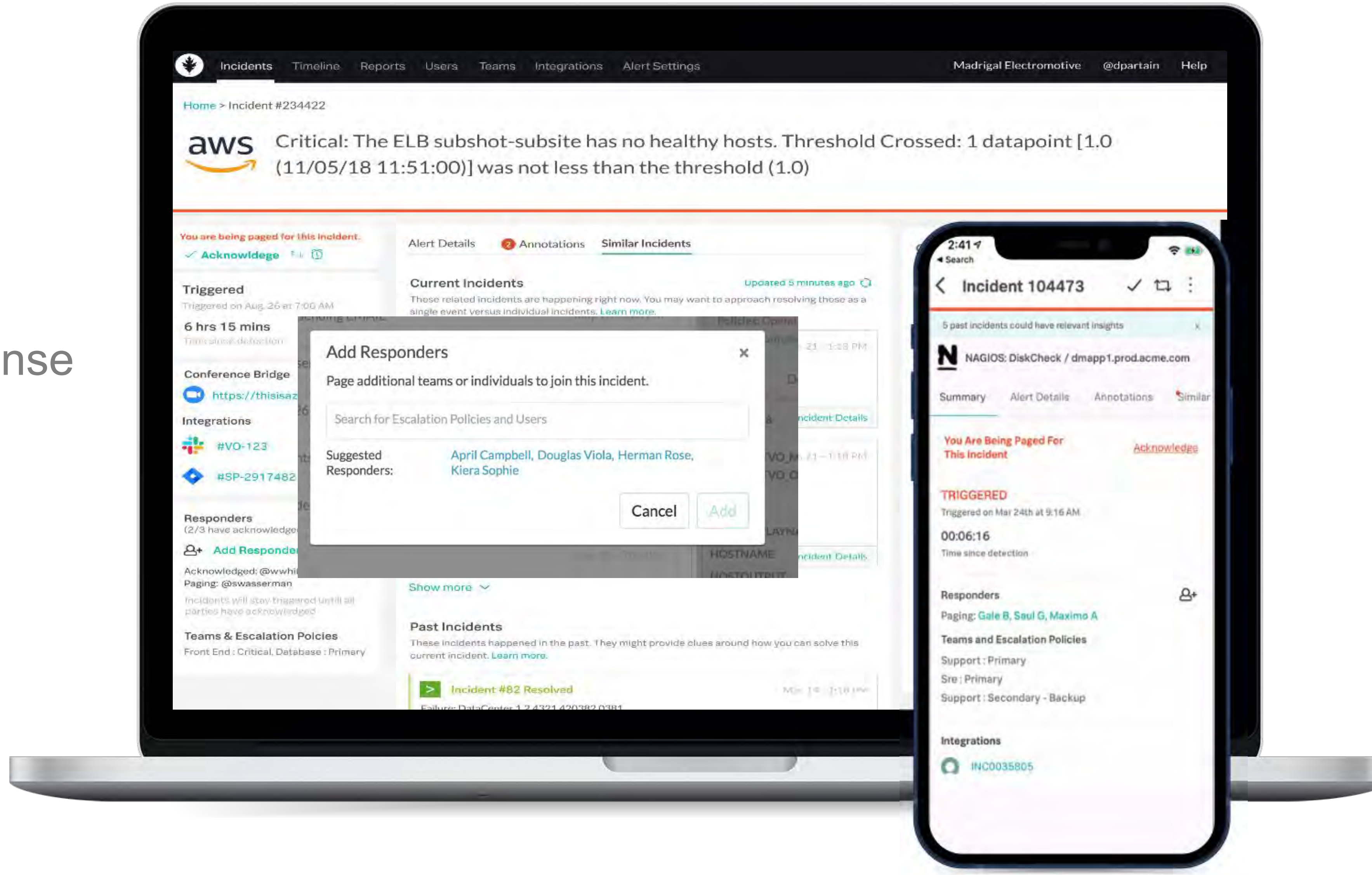
splunk> turn data into doing

Information on this page is provided to the <INSERT CUSTOMER NAME HERE> under the Trade Secrets Act (18 USC 1905) and other federal law and regulations and is proprietary to Splunk.

Splunk On-Call

Collaborative Incident Response

- Intelligent on-call
- Post-incident analysis and reporting
- Mobile-first



Home > Incident #234422

Critical: The ELB subshot-subsite has no healthy hosts. Threshold Crossed: 1 datapoint [1.0 (11/05/18 11:51:00)] was not less than the threshold (1.0)

You are being paged for this incident.
✓ Acknowldege

Triggered
Triggered on Aug. 26 at 7:00 AM

6 hrs 15 mins
Time since detection

Conference Bridge
https://thisisaz

Integrations
#VO-123
#SP-2917482

Responders
(2/3 have acknowledge
Add Responde
Acknowledged: @wwhi
Paging: @swasserman
Incidents will stay triggered until all parties have acknowledged

Teams & Escalation Policies
Front End : Critical, Database : Primary

Current Incidents
Updated 5 minutes ago
These related incidents are happening right now. You may want to approach resolving those as a single event versus individual incidents. Learn more.

Add Responders ×
Page additional teams or individuals to join this incident.
Search for Escalation Policies and Users
Suggested Responders: April Campbell, Douglas Viola, Herman Rose, Kiera Sophie
Cancel Add

Past Incidents
These incidents happened in the past. They might provide clues around how you can solve this current incident. Learn more.

Incident #82 Resolved

Incident 104473

5 past incidents could have relevant insights

NAGIOS: DiskCheck / dmapp1.prod.acme.com

You Are Being Paged For This Incident
Acknowledge

TRIGGERED
Triggered on Mar 24th at 9:16 AM

00:06:16
Time since detection

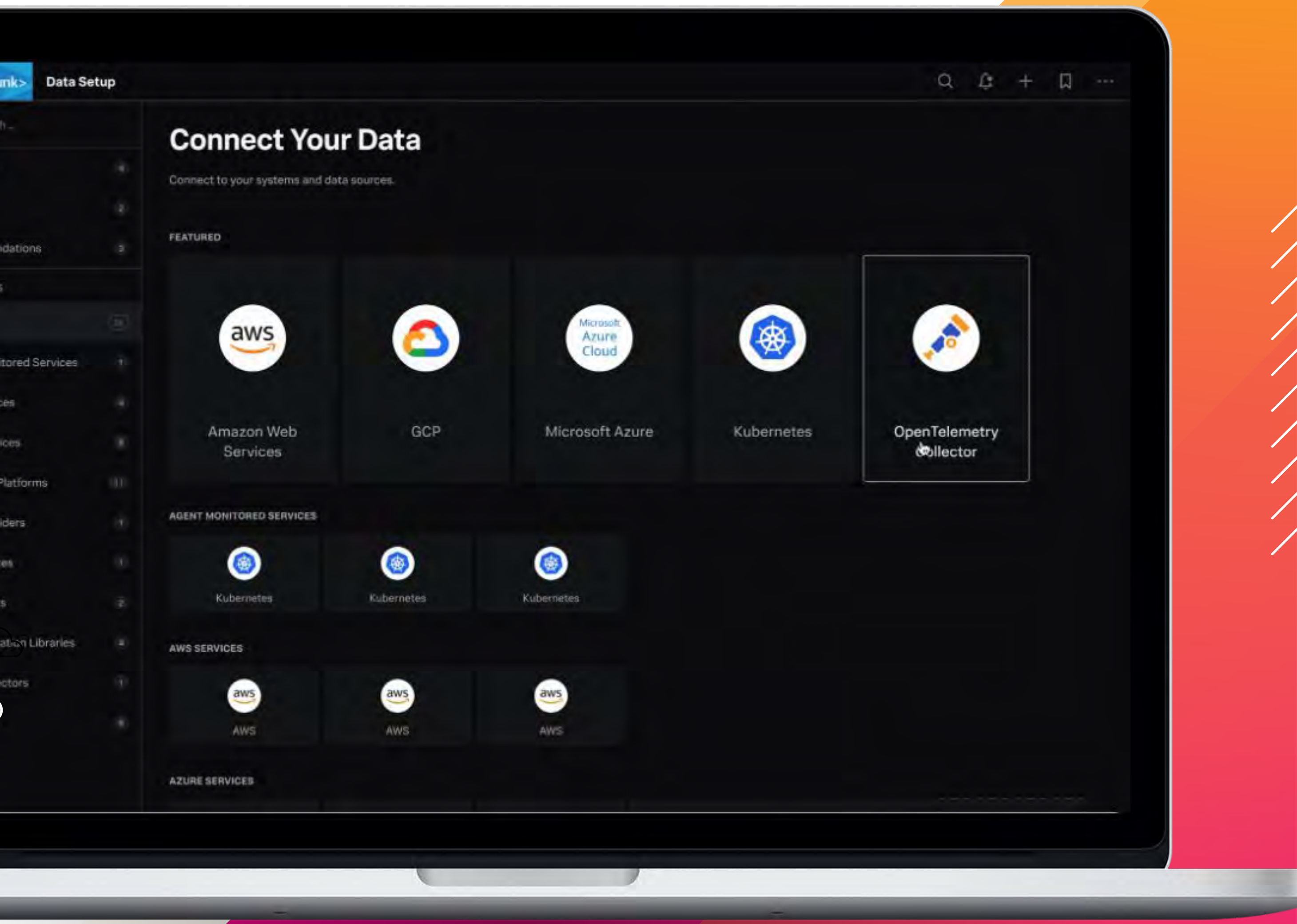
Responders
Paging: Gale B, Saul G, Maximo A

Teams and Escalation Policies
Support : Primary
Sre : Primary
Support : Secondary - Backup

Integrations
INC0035805

Open Telemetry-Native

Single, open standards-based agent for metrics, traces, logs and more for more control and greater ROI



Data Setup

- Deployed
- Drafts
- Recommendations

CATEGORIES

- All
- Agent Monitored Services
- AWS Services
- Azure Services
- Container Platforms
- Cloud Providers
- GCP Services
- Host Agents
- Instrumentation Libraries
- Other Collectors
- Serverless

Connect Your Data

Connect to your systems and data sources.

FEATURED

- Amazon Web Services
- GCP
- Microsoft Azure
- Kubernetes
- OpenTelemetry Collector

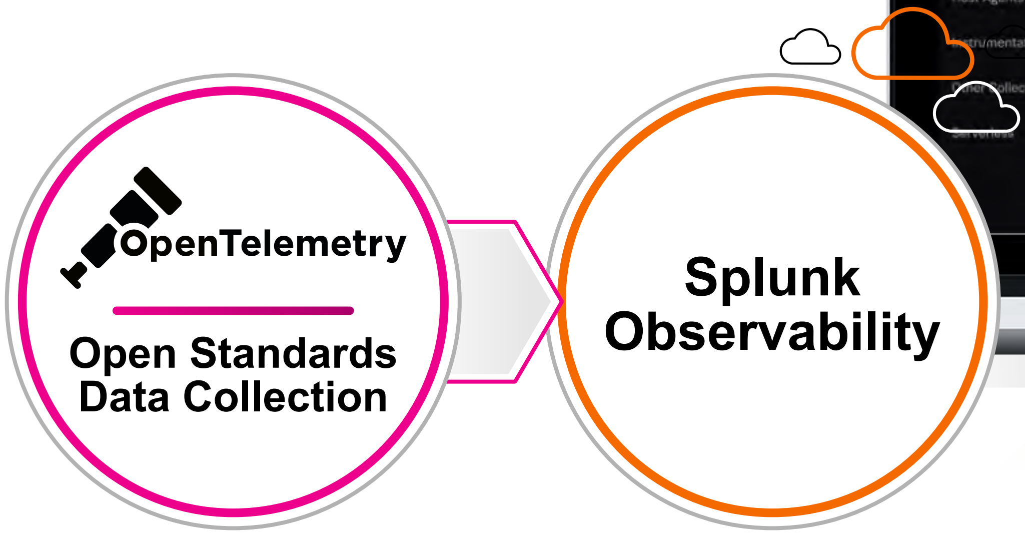
AGENT MONITORED SERVICES

- Kubernetes
- Kubernetes
- Kubernetes

AWS SERVICES

- AWS
- AWS
- AWS

AZURE SERVICES



OpenTelemetry

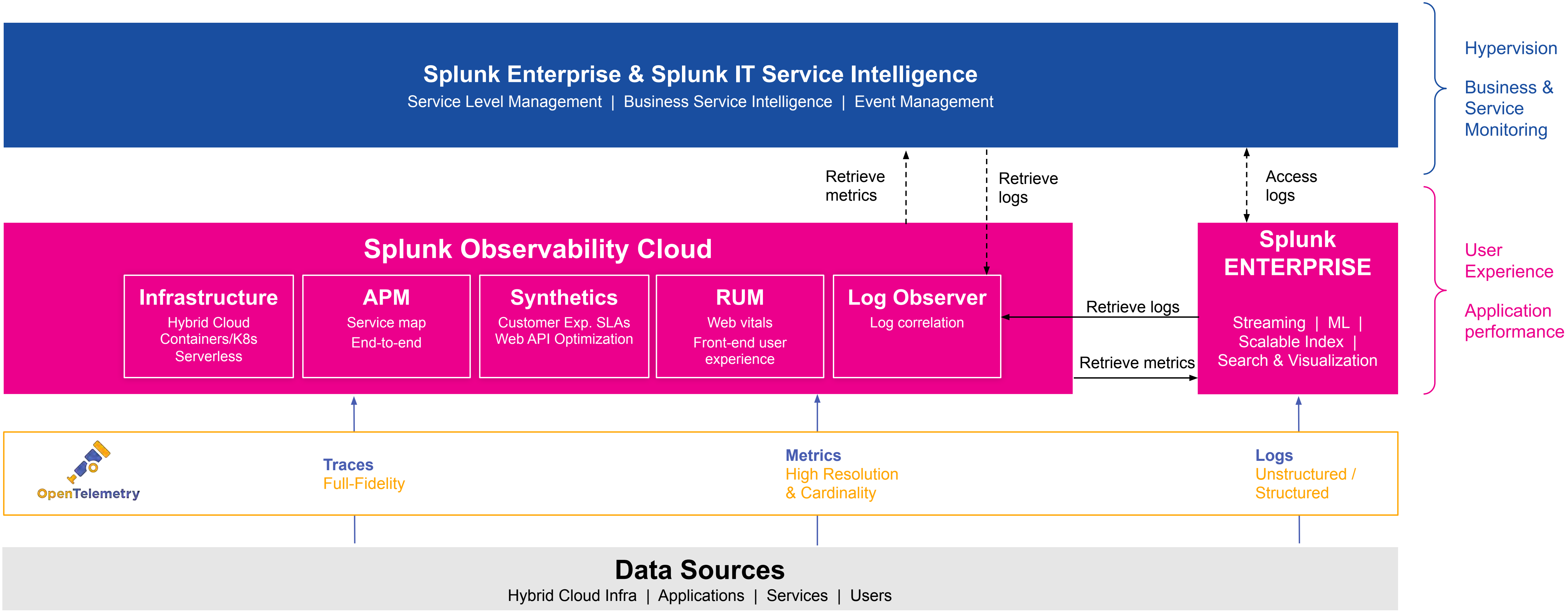
Open Standards Data Collection

Splunk Observability

Observability Cloud - An easier way to consume ….

	Infrastructure Per Host	Applications & Infra Per Host	End-to-End Per Host
Products and Entitlements Included	• **Splunk Infrastructure Monitoring Enterprise Edition** • 20 Containers or Serverless Functions • 200 Custom Metrics • Data Retention (1min Roll-Ups / 1sec Native): 13 months / 3 months • **Splunk Synthetic Monitoring - Uptime Tests, Enterprise Edition** • 10k Uptime Test Runs per Month • **Splunk Incident Intelligence** • 1 monthly active user per 10 hosts • **Log Observer Connect**	**Everything in Infrastructure PLUS:** • **Splunk Application Performance Monitoring, Enterprise Edition** • 20 Containers or Serverless Functions • 5 Profiled Containers • 40 Monitoring MetricSet • 400 Troubleshooting MetricSet • 20.48 MB TraceVolume ingested per min • 10.24 MB Profiling TraceVolume ingested per min • **Splunk Synthetic Monitoring - API Tests, Enterprise Edition** • 10k Synthetics API Test Runs per Month	**Everything in App & Infra PLUS:** • **Splunk Real User Monitoring, Enterprise Edition** • 10k Sessions/Month • **Splunk Synthetic Monitoring - Browser Tests, Enterprise Edition** 1000 Browser Test Runs per Month (Browser or Mobile)
Customer Success Plans (Support, EDU, PS)	All tiers include the Standard Customer Success Plan. Premium Customer Success Plans are available at additional cost per host.		

Splunk Observability



Splunk Enterprise & Splunk IT Service Intelligence
Service Level Management | Business Service Intelligence | Event Management
Retrieve metrics
Retrieve logs
Access logs
Splunk Observability Cloud
Infrastructure
Hybrid Cloud
Containers/K8s
Serverless
APM
Service map
End-to-end
Synthetics
Customer Exp. SLAs
Web API Optimization
RUM
Web vitals
Front-end user experience
Log Observer
Log correlation
Retrieve logs
Retrieve metrics
Splunk ENTERPRISE
Streaming | ML | Scalable Index | Search & Visualization
Hypervision
Business & Service Monitoring
User Experience
Application performance
OpenTelemetry
Traces
Full-Fidelity
Metrics
High Resolution & Cardinality
Logs
Unstructured / Structured
Data Sources
Hybrid Cloud Infra | Applications | Services | Users

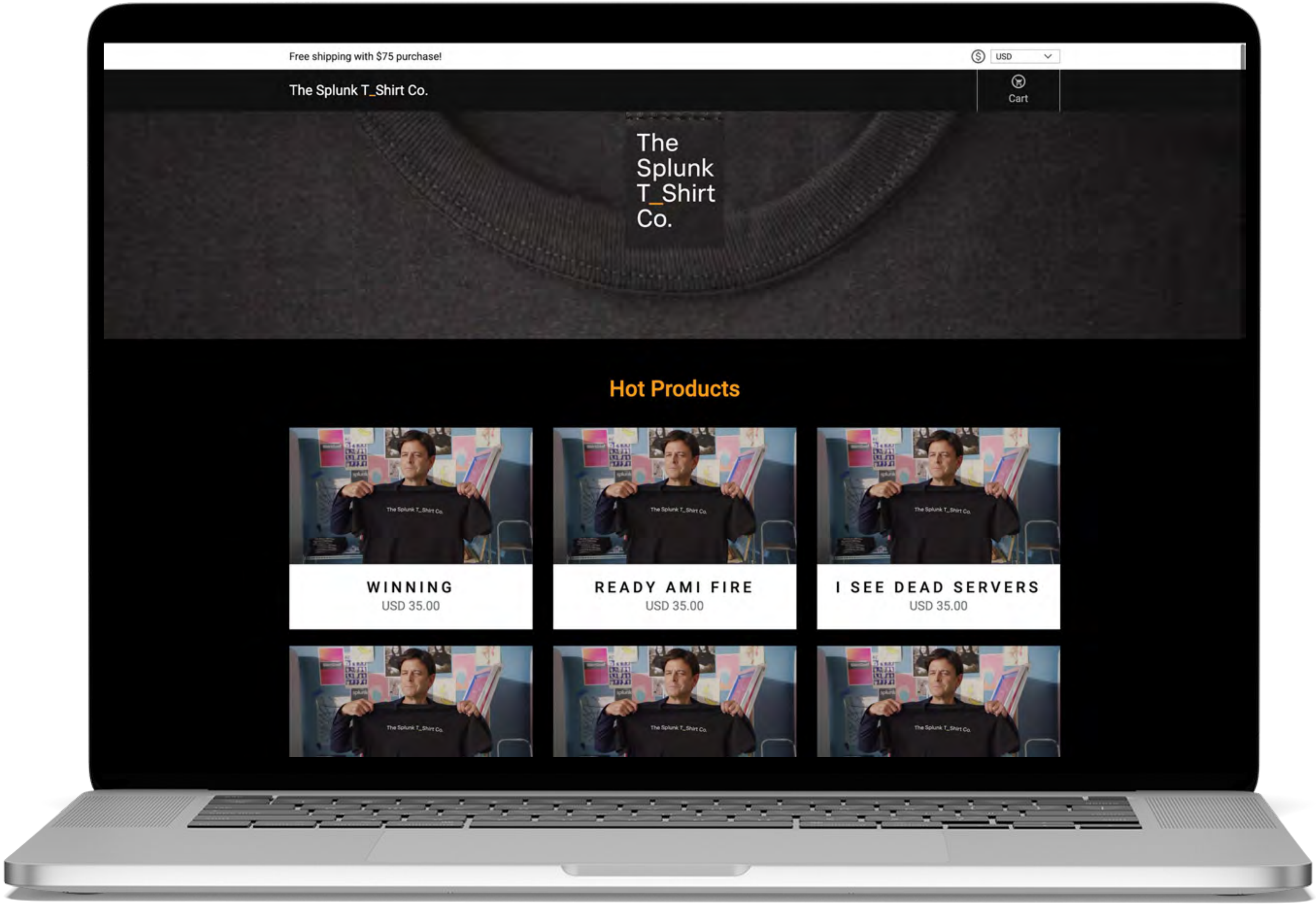
The Splunk T-Shirt Co.

How this comes together …..

The Splunk T-Shirt Co.

Online Store

- Niche Clothing brand
- Born in the Cloud
- Online Only



Free shipping with $75 purchase!

Hot Products

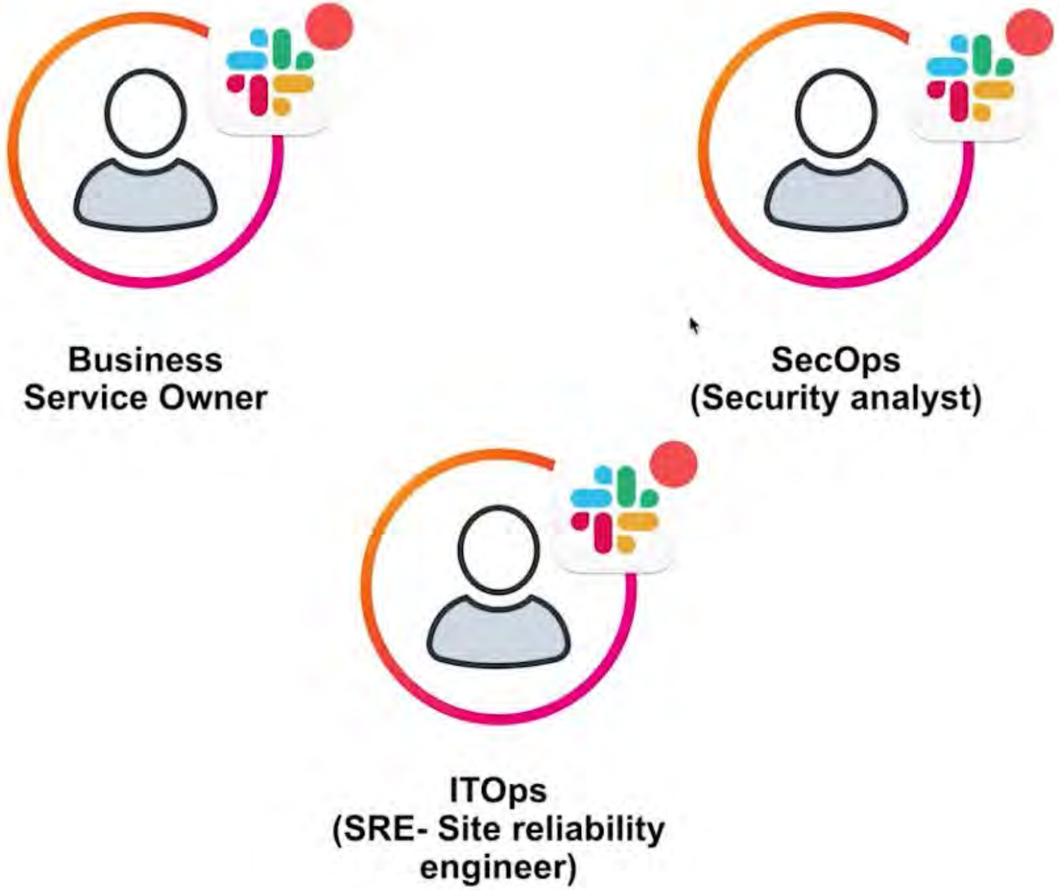
WINNING
USD 35.00

READY AMI FIRE
USD 35.00

I SEE DEAD SERVERS
USD 35.00

Unexpected traffic spike impacting website performance

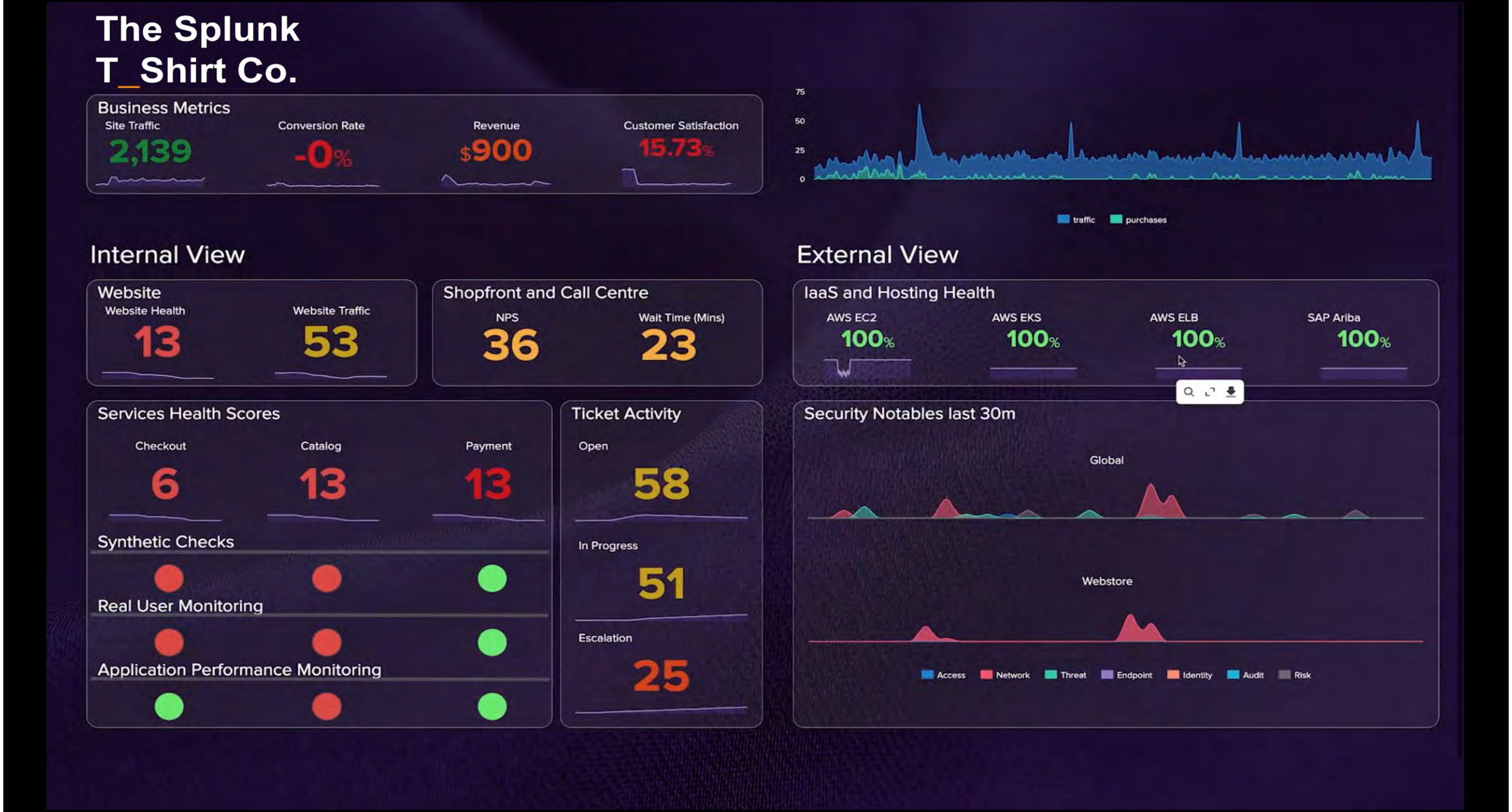
- Potential security and performance incidents
- Splunk intelligent alerting alerts business owner, SecOps and ITOp



Business Service Owner

SecOps (Security analyst)

ITOps (SRE- Site reliability engineer)



The Splunk T_Shirt Co.

Business Metrics

Site Traffic 2,139

Conversion Rate -0%

Revenue $900

Customer Satisfaction 15.73%

Internal View

Website

Website Health 13

Website Traffic 53

Shopfront and Call Centre

NPS 36

Wait Time (Mins) 23

Services Health Scores

Checkout 6

Catalog 13

Payment 13

Synthetic Checks

🔴 🔴 🟢

Real User Monitoring

🔴 🔴 🟢

Application Performance Monitoring

🟢 🔴 🟢

Ticket Activity

Open 58

In Progress 51

Escalation 25

External View

IaaS and Hosting Health

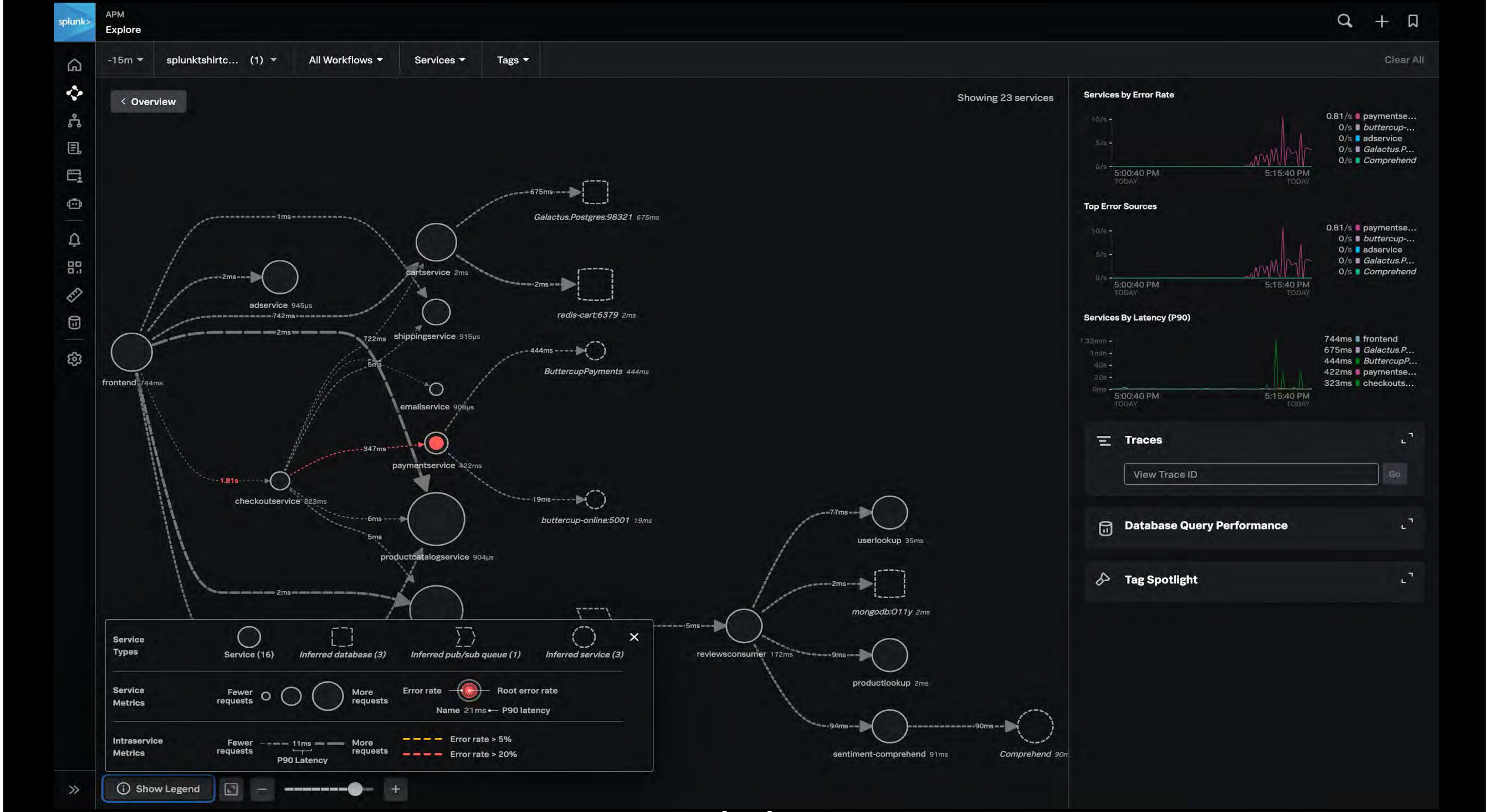
AWS EC2 100%

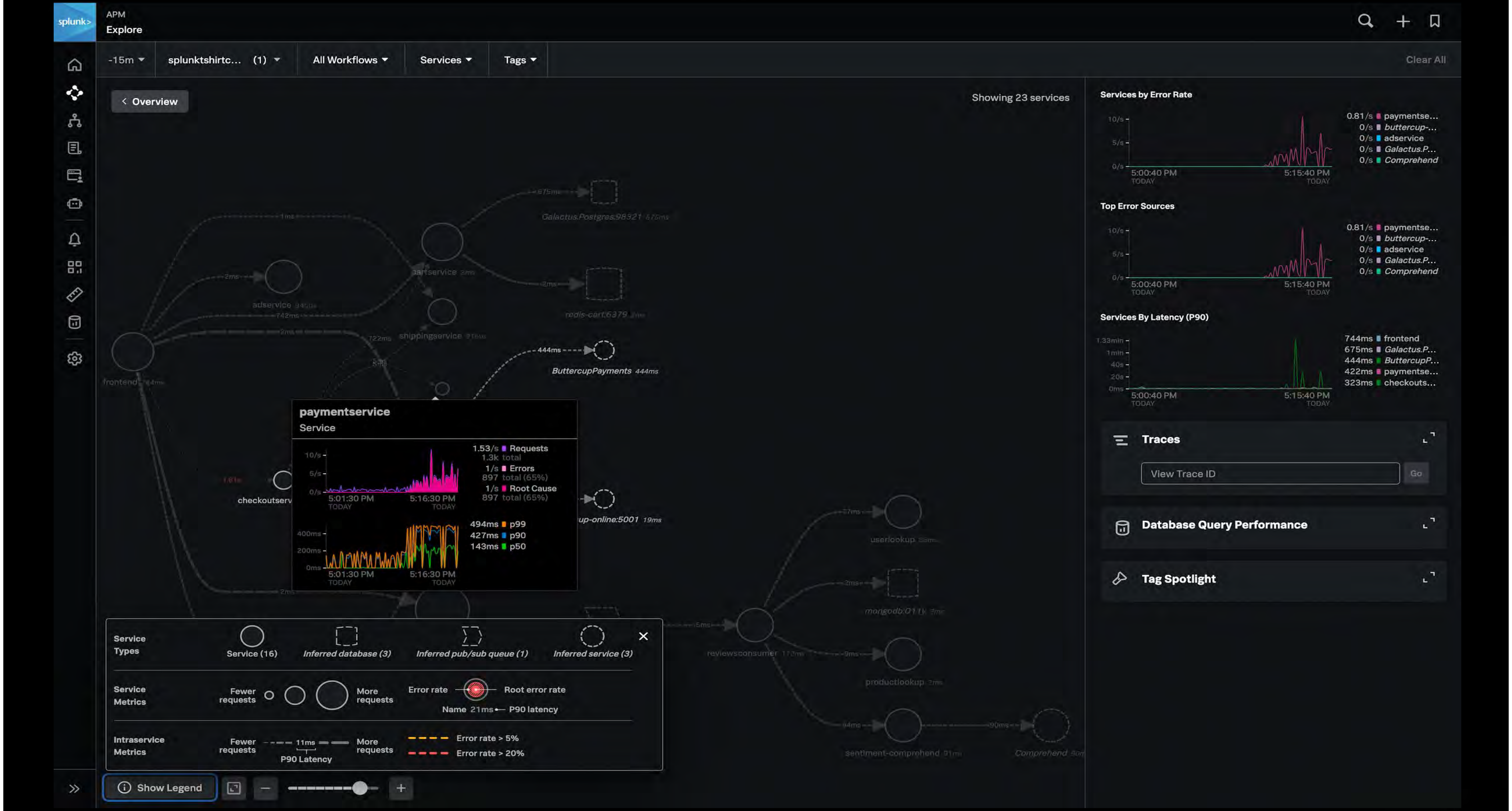
AWS EKS 100%

AWS ELB 100%

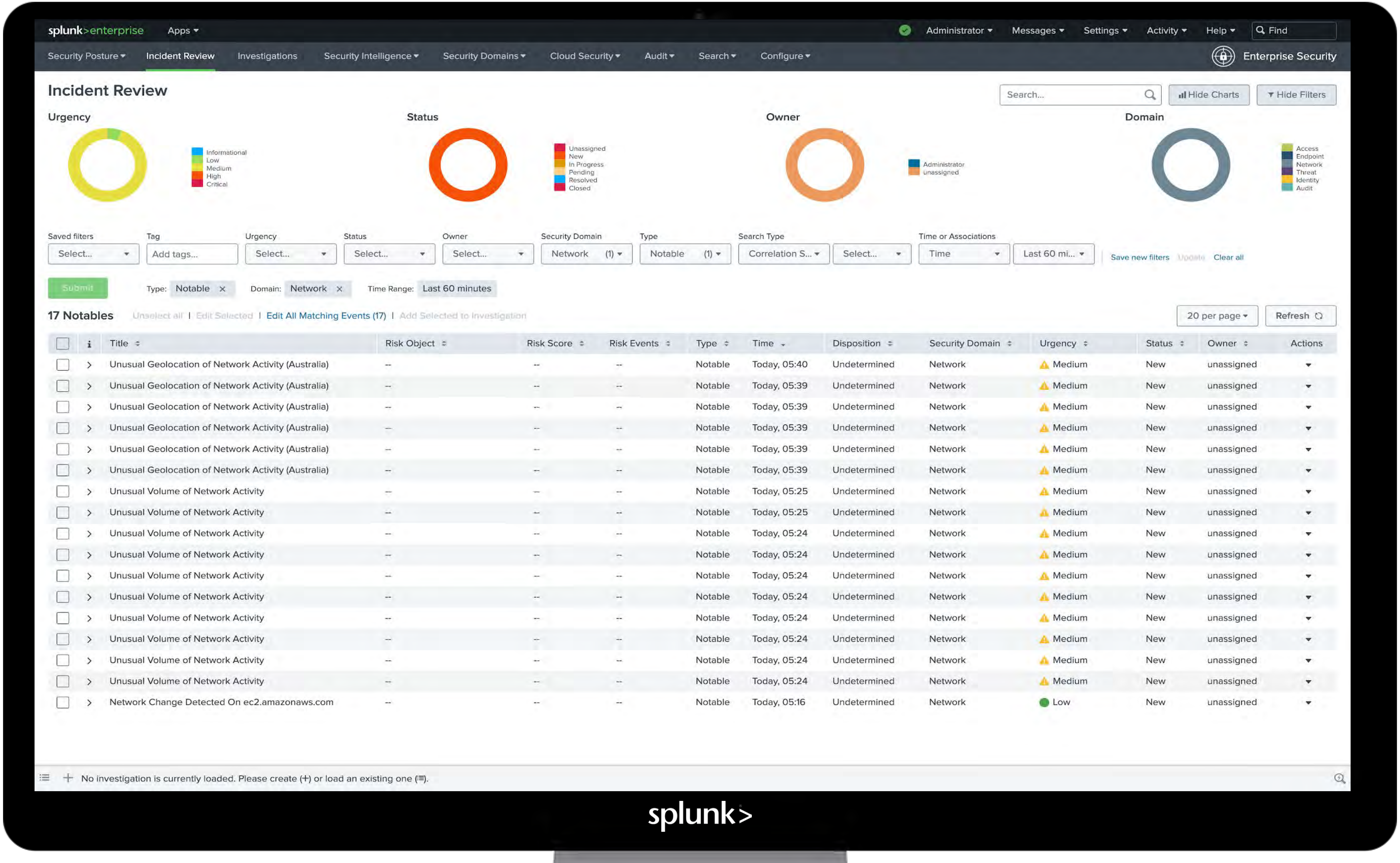
SAP Ariba 100%

Security Notables last 30m


splunk>
APM
Explore
-15m
splunkshirtc... (1)
All Workflows
Services
Tags
Clear All
Overview
Showing 23 services
frontend 744ms
adservice 945µs
cartservice 2ms
shippingservice 915µs
emailservice 908µs
paymentservice 422ms
checkoutservice 323ms
productcatalogservice 904µs
Galactus.Postgres:98321 675ms
redis-cart:6379 2ms
ButtercupPayments 444ms
buttercup-online:5001 19ms
reviewsconsumer 172ms
userlookup 35ms
mongodb:O11y 2ms
productlookup 2ms
sentiment-comprehend 91ms
Comprehend 90m
1ms
2ms
742ms
722ms
5ms
675ms
444ms
347ms
1.81s
19ms
6ms
77ms
9ms
94ms
90ms
Service Types
Service (16)
Inferred database (3)
Inferred pub/sub queue (1)
Inferred service (3)
Service Metrics
Fewer requests
More requests
Error rate
Root error rate
Name 21ms P90 latency
Intraservice Metrics
11ms
P90 Latency
Error rate > 5%
Error rate > 20%
Show Legend
Services by Error Rate
10/s
5/s
0/s
5:00:40 PM TODAY
5:15:40 PM TODAY
0.81/s paymentse...
0/s buttercup-...
0/s adservice
0/s Galactus.P...
0/s Comprehend
Top Error Sources
0.81/s paymentse...
0/s buttercup-...
0/s adservice
0/s Galactus.P...
0/s Comprehend
Services By Latency (P90)
1.33min
1min
40s
20s
0ms
744ms frontend
675ms Galactus.P...
444ms ButtercupP...
422ms paymentse...
323ms checkouts...
Traces
View Trace ID
Go
Database Query Performance
Tag Spotlight


splunk>
APM
Explore
-15m
splunktshirtc... (1)
All Workflows
Services
Tags
Clear All
Overview
Showing 23 services
1ms
675ms
Galactus.Postgres:98321 675ms
2ms
adservice 945µs
cartservice 2ms
redis-cart:6379 2ms
742ms
2ms
722ms
shippingservice 916µs
5ms
444ms
ButtercupPayments 444ms
frontend 744ms
1.61s
checkoutserv
up-online:5001 19ms
paymentservice
Service
10/s
5/s
0/s
5:01:30 PM TODAY
5:16:30 PM TODAY
1.53/s Requests
1.3k total
1/s Errors
897 total (65%)
1/s Root Cause
897 total (65%)
400ms
200ms
0ms
494ms p99
427ms p90
143ms p50
2ms
37ms
userlookup 35ms
2ms
mongodb:011k 2ms
5ms
reviewsconsumer 172ms
9ms
productlookup 2ms
94ms
sentiment-comprehend 91ms
90ms
Comprehend 90ms
Service Types
Service (16)
Inferred database (3)
Inferred pub/sub queue (1)
Inferred service (3)
Service Metrics
Fewer requests
More requests
Error rate
Root error rate
Name 21ms P90 latency
Intraservice Metrics
Fewer requests
11ms
More requests
P90 Latency
Error rate > 5%
Error rate > 20%
Show Legend
Services by Error Rate
10/s
5/s
0/s
5:00:40 PM TODAY
5:15:40 PM TODAY
0.81/s paymentse...
0/s buttercup-...
0/s adservice
0/s Galactus.P...
0/s Comprehend
Top Error Sources
10/s
5/s
0/s
5:00:40 PM TODAY
5:15:40 PM TODAY
0.81/s paymentse...
0/s buttercup-...
0/s adservice
0/s Galactus.P...
0/s Comprehend
Services By Latency (P90)
1.33min
1min
40s
20s
0ms
5:00:40 PM TODAY
5:15:40 PM TODAY
744ms frontend
675ms Galactus.P...
444ms ButtercupP...
422ms paymentse...
323ms checkouts...
Traces
View Trace ID
Go
Database Query Performance
Tag Spotlight

splunk>



Incident Review

Saved filters: Select... ▾
Tag: Add tags...
Urgency: Select... ▾
Status: Select... ▾
Owner: Select... ▾
Security Domain: Network (1) ▾
Type: Notable (1) ▾
Search Type: Correlation S... ▾ Select... ▾
Time or Associations: Time ▾ Last 60 mi... ▾

Save new filters | Update | Clear all

Submit

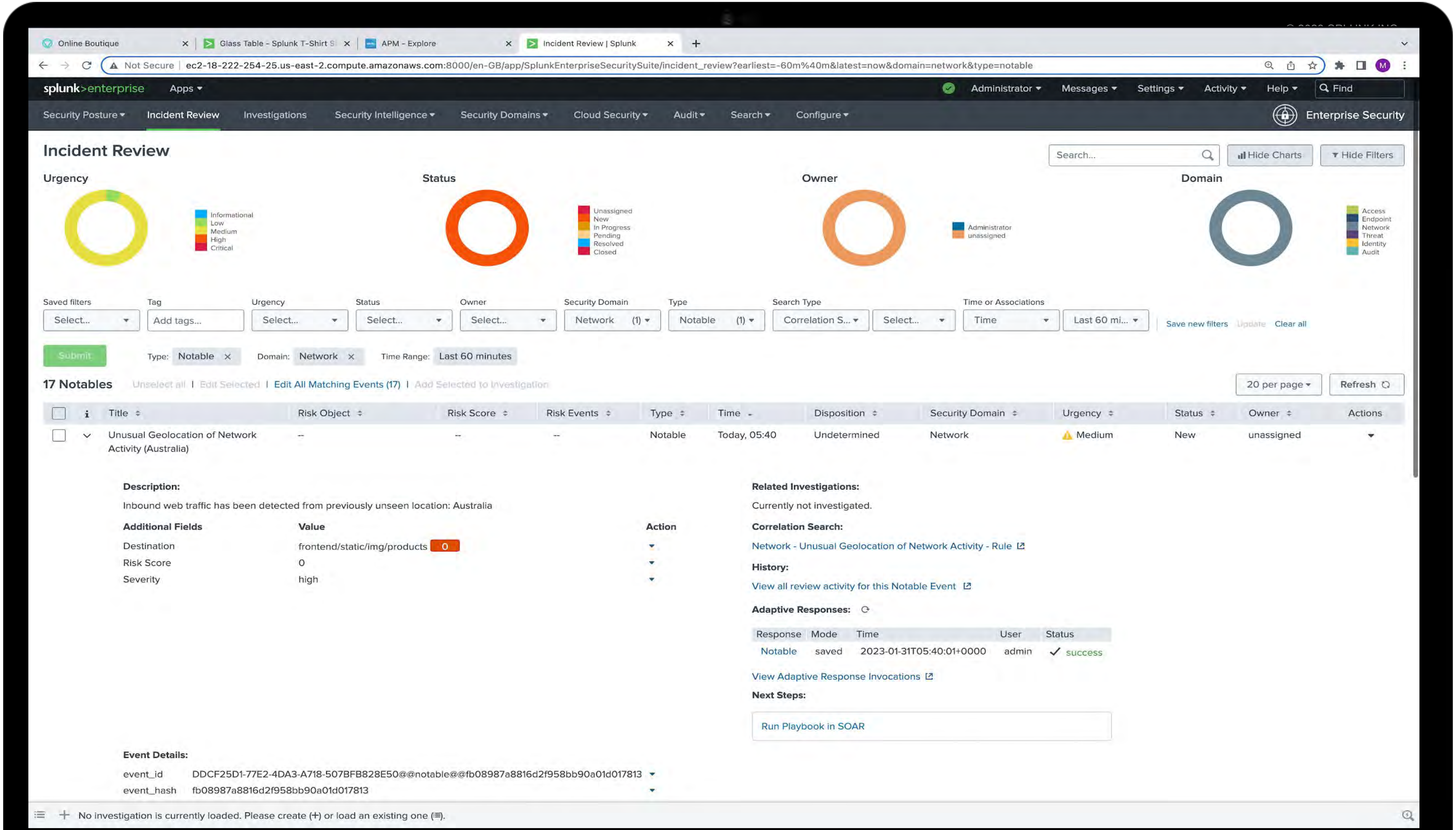
Type: Notable ×   Domain: Network ×   Time Range: Last 60 minutes

17 Notables   Unselect all | Edit Selected | Edit All Matching Events (17) | Add Selected to Investigation

20 per page ▾   Refresh

□	i	Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
□	›	Unusual Geolocation of Network Activity (Australia)	--	--	--	Notable	Today, 05:40	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Geolocation of Network Activity (Australia)	--	--	--	Notable	Today, 05:39	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Geolocation of Network Activity (Australia)	--	--	--	Notable	Today, 05:39	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Geolocation of Network Activity (Australia)	--	--	--	Notable	Today, 05:39	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Geolocation of Network Activity (Australia)	--	--	--	Notable	Today, 05:39	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Geolocation of Network Activity (Australia)	--	--	--	Notable	Today, 05:39	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Volume of Network Activity	--	--	--	Notable	Today, 05:25	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Volume of Network Activity	--	--	--	Notable	Today, 05:25	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Volume of Network Activity	--	--	--	Notable	Today, 05:24	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Volume of Network Activity	--	--	--	Notable	Today, 05:24	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Volume of Network Activity	--	--	--	Notable	Today, 05:24	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Volume of Network Activity	--	--	--	Notable	Today, 05:24	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Volume of Network Activity	--	--	--	Notable	Today, 05:24	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Volume of Network Activity	--	--	--	Notable	Today, 05:24	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Volume of Network Activity	--	--	--	Notable	Today, 05:24	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Unusual Volume of Network Activity	--	--	--	Notable	Today, 05:24	Undetermined	Network	⚠ Medium	New	unassigned	▾
□	›	Network Change Detected On ec2.amazonaws.com	--	--	--	Notable	Today, 05:16	Undetermined	Network	● Low	New	unassigned	▾

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



Incident Review

Saved filters	Tag	Urgency	Status	Owner	Security Domain	Type	Search Type		Time or Associations	
Select... ▾	Add tags...	Select... ▾	Select... ▾	Select... ▾	Network (1) ▾	Notable (1) ▾	Correlation S... ▾	Select... ▾	Time ▾	Last 60 mi... ▾

Save new filters Update Clear all

Submit Type: Notable × Domain: Network × Time Range: Last 60 minutes

17 Notables Unselect all | Edit Selected | Edit All Matching Events (17) | Add Selected to Investigation

20 per page ▾ Refresh

□	i	Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
□	⌄	Unusual Geolocation of Network Activity (Australia)	--	--	--	Notable	Today, 05:40	Undetermined	Network	⚠ Medium	New	unassigned	▾

Description:

Inbound web traffic has been detected from previously unseen location: Australia

Additional Fields	Value	Action
Destination	frontend/static/img/products 0	▾
Risk Score	0	▾
Severity	high	▾

Related Investigations:

Currently not investigated.

Correlation Search:

Network - Unusual Geolocation of Network Activity - Rule

History:

View all review activity for this Notable Event

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2023-01-31T05:40:01+0000	admin	✓ success

View Adaptive Response Invocations

Next Steps:

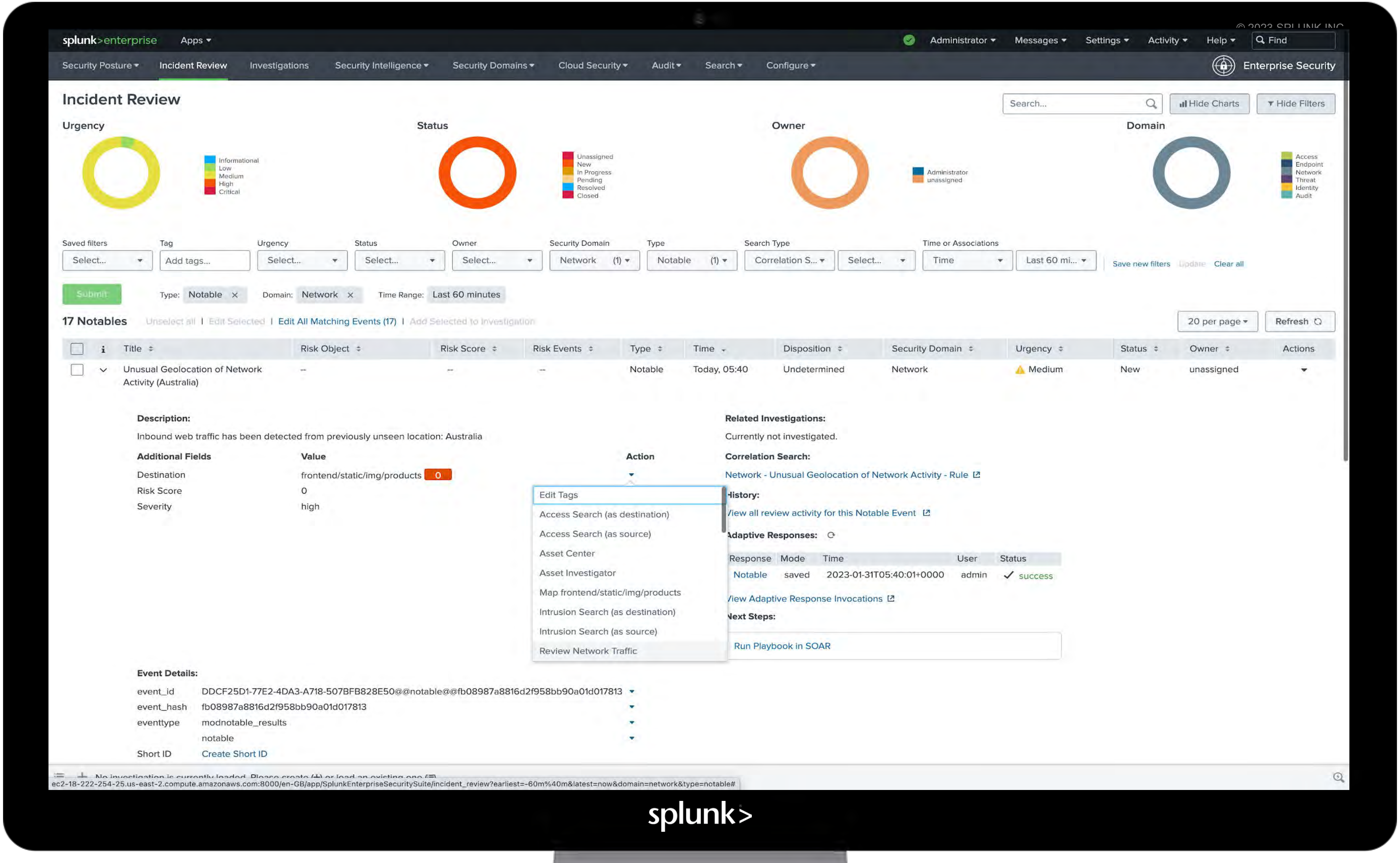
Run Playbook in SOAR

Event Details:

event_id	DDCF25D1-77E2-4DA3-A718-507BFB828E50@@notable@@fb08987a8816d2f958bb90a01d017813
event_hash	fb08987a8816d2f958bb90a01d017813

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

splunk>



Incident Review

Saved filters	Tag	Urgency	Status	Owner	Security Domain	Type	Search Type		Time or Associations	
Select...	Add tags...	Select...	Select...	Select...	Network (1)	Notable (1)	Correlation S...	Select...	Time	Last 60 mi...

Type: Notable × Domain: Network × Time Range: Last 60 minutes

17 Notables

□	i	Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
□	∨	Unusual Geolocation of Network Activity (Australia)	--	--	--	Notable	Today, 05:40	Undetermined	Network	⚠ Medium	New	unassigned	▾

Description:

Inbound web traffic has been detected from previously unseen location: Australia

Additional Fields	Value	Action
Destination	frontend/static/img/products 0	▾
Risk Score	0	
Severity	high	

Related Investigations:

Currently not investigated.

Correlation Search:

Network - Unusual Geolocation of Network Activity - Rule

History:

View all review activity for this Notable Event

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2023-01-31T05:40:01+0000	admin	✓ success

View Adaptive Response Invocations

Next Steps:

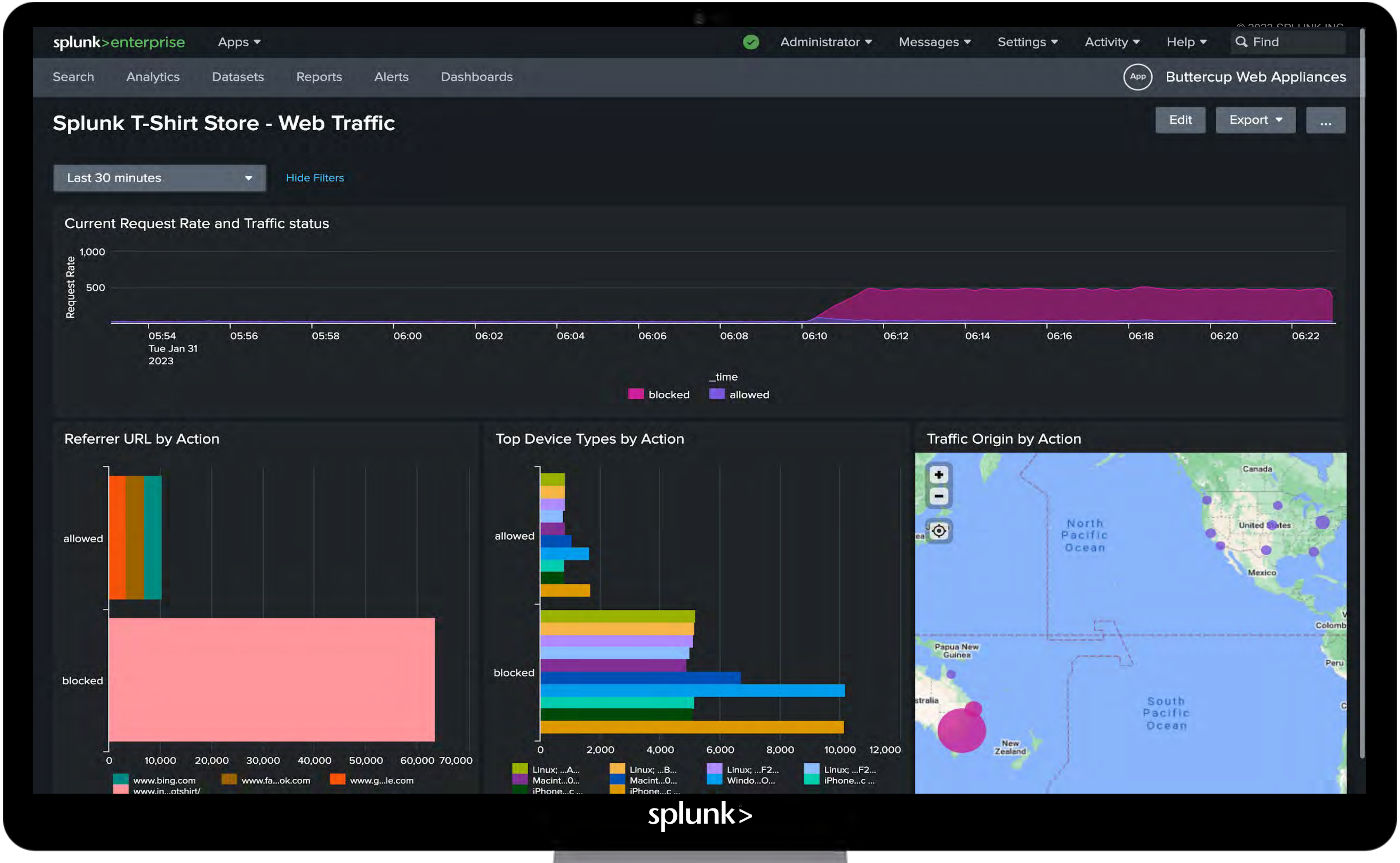
Run Playbook in SOAR

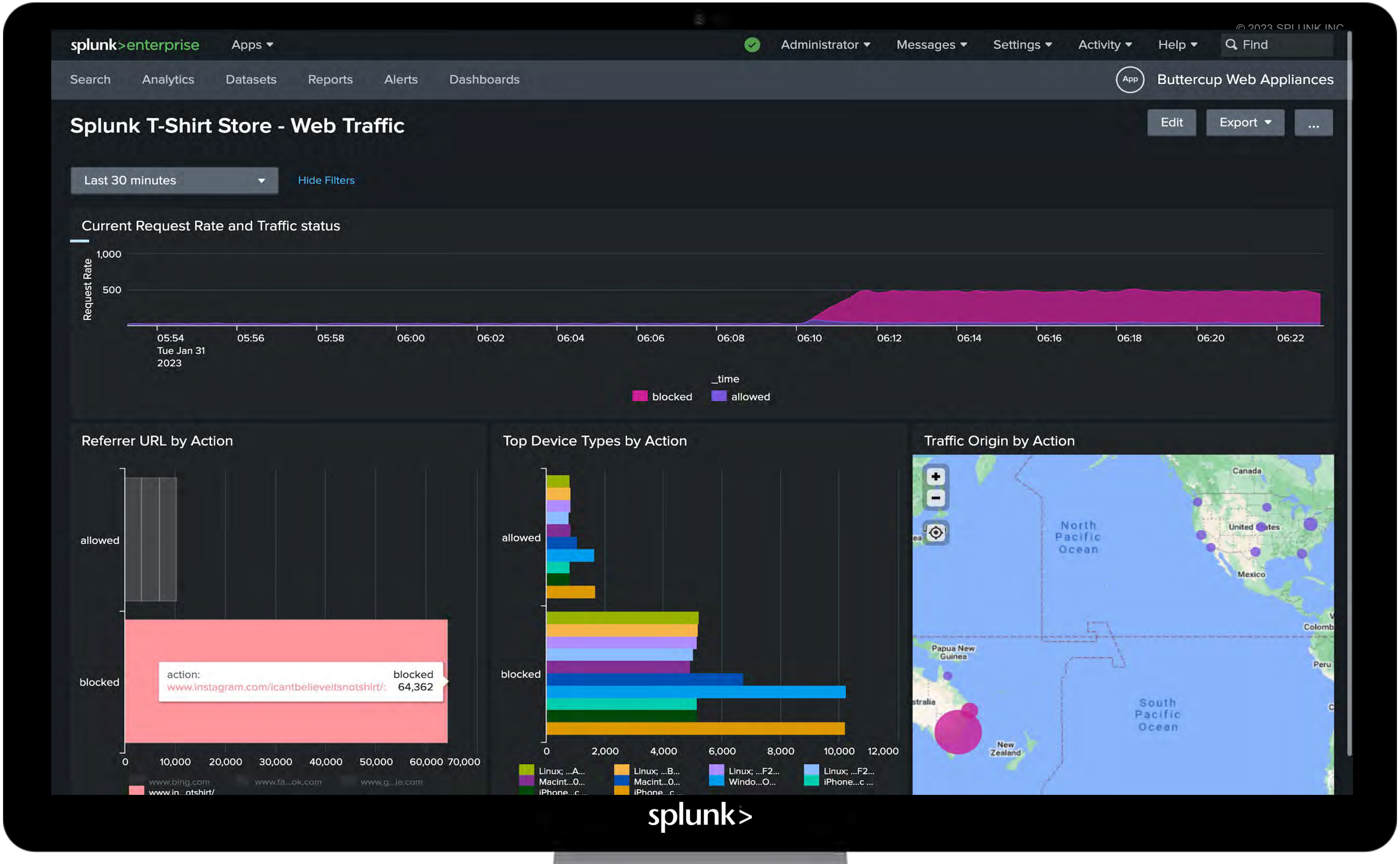
Event Details:

event_id	DDCF25D1-77E2-4DA3-A718-507BFB828E50@@notable@@fb08987a8816d2f958bb90a01d017813
event_hash	fb08987a8816d2f958bb90a01d017813
eventtype	modnotable_results
	notable
Short ID	Create Short ID

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

ec2-18-222-254-25.us-east-2.compute.amazonaws.com:8000/en-GB/app/SplunkEnterpriseSecuritySuite/incident_review?earliest=-60m%40m&latest=now&domain=network&type=notable#


© 2023 SPLUNK INC.
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
App
Buttercup Web Appliances
Splunk T-Shirt Store - Web Traffic
Edit
Export
...
Last 30 minutes
Hide Filters
Current Request Rate and Traffic status
Request Rate
1,000
500
05:54
Tue Jan 31
2023
05:56
05:58
06:00
06:02
06:04
06:06
06:08
06:10
06:12
06:14
06:16
06:18
06:20
06:22
_time
blocked
allowed
Referrer URL by Action
allowed
blocked
0
10,000
20,000
30,000
40,000
50,000
60,000
70,000
www.bing.com
www.fa...ok.com
www.g...le.com
www.in...otshirt/
Top Device Types by Action
allowed
blocked
0
2,000
4,000
6,000
8,000
10,000
12,000
Linux; ...A...
Linux; ...B...
Linux; ...F2...
Linux; ...F2...
Macint...O...
Macint...O...
Windo...O...
iPhone...c ...
iPhone...c ...
iPhone...c ...
Traffic Origin by Action
Canada
United States
Mexico
North Pacific Ocean
Papua New Guinea
stralia
New Zealand
South Pacific Ocean
Colomb
Peru
splunk>



Splunk T-Shirt Store - Web Traffic

Last 30 minutes

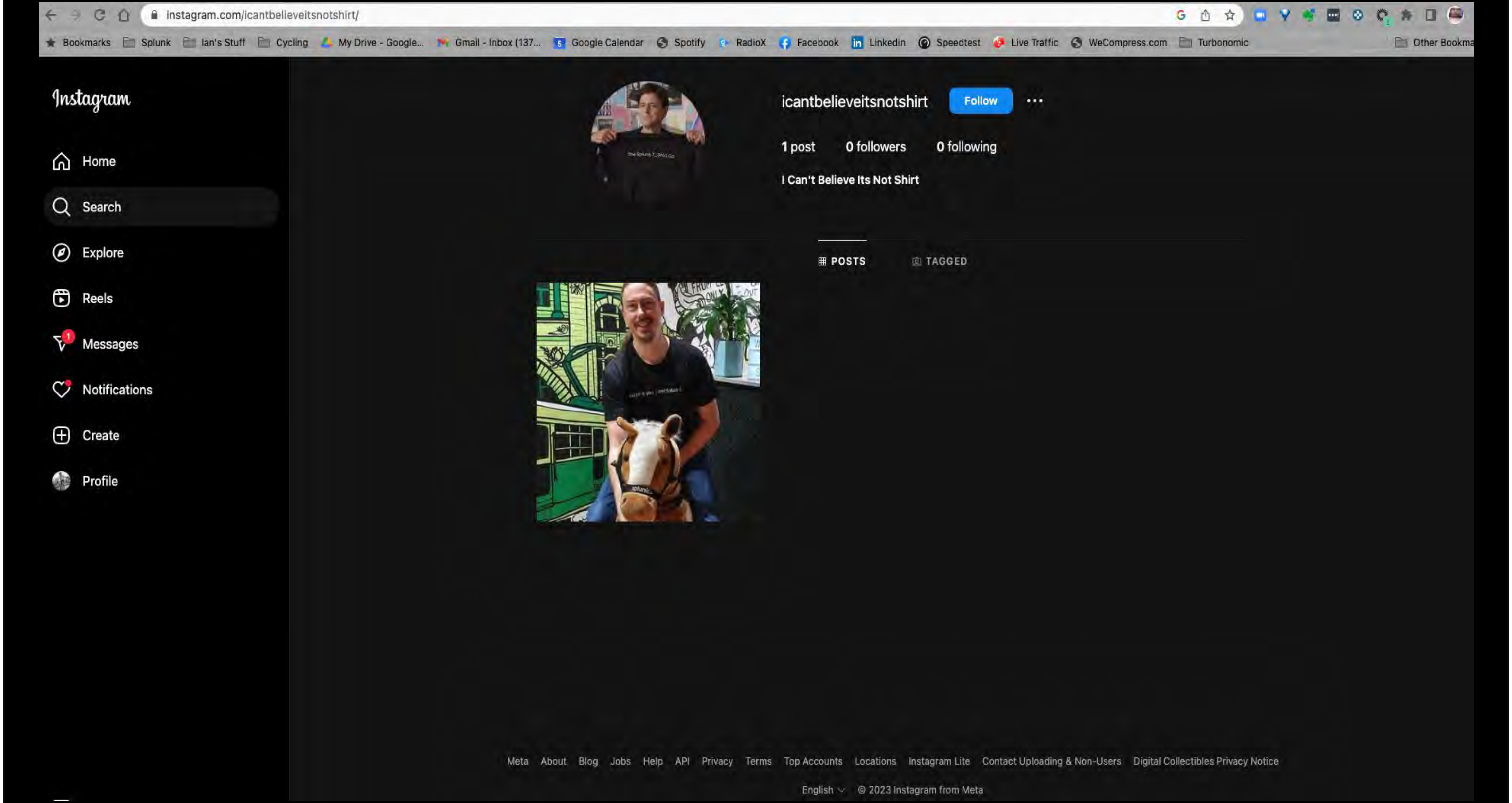
Current Request Rate and Traffic status

Referrer URL by Action

action: www.instagram.com/icantbelieveitsnotshirt/: blocked 64,362

Top Device Types by Action

Traffic Origin by Action



instagram.com/icantbelieveitsnotshirt/

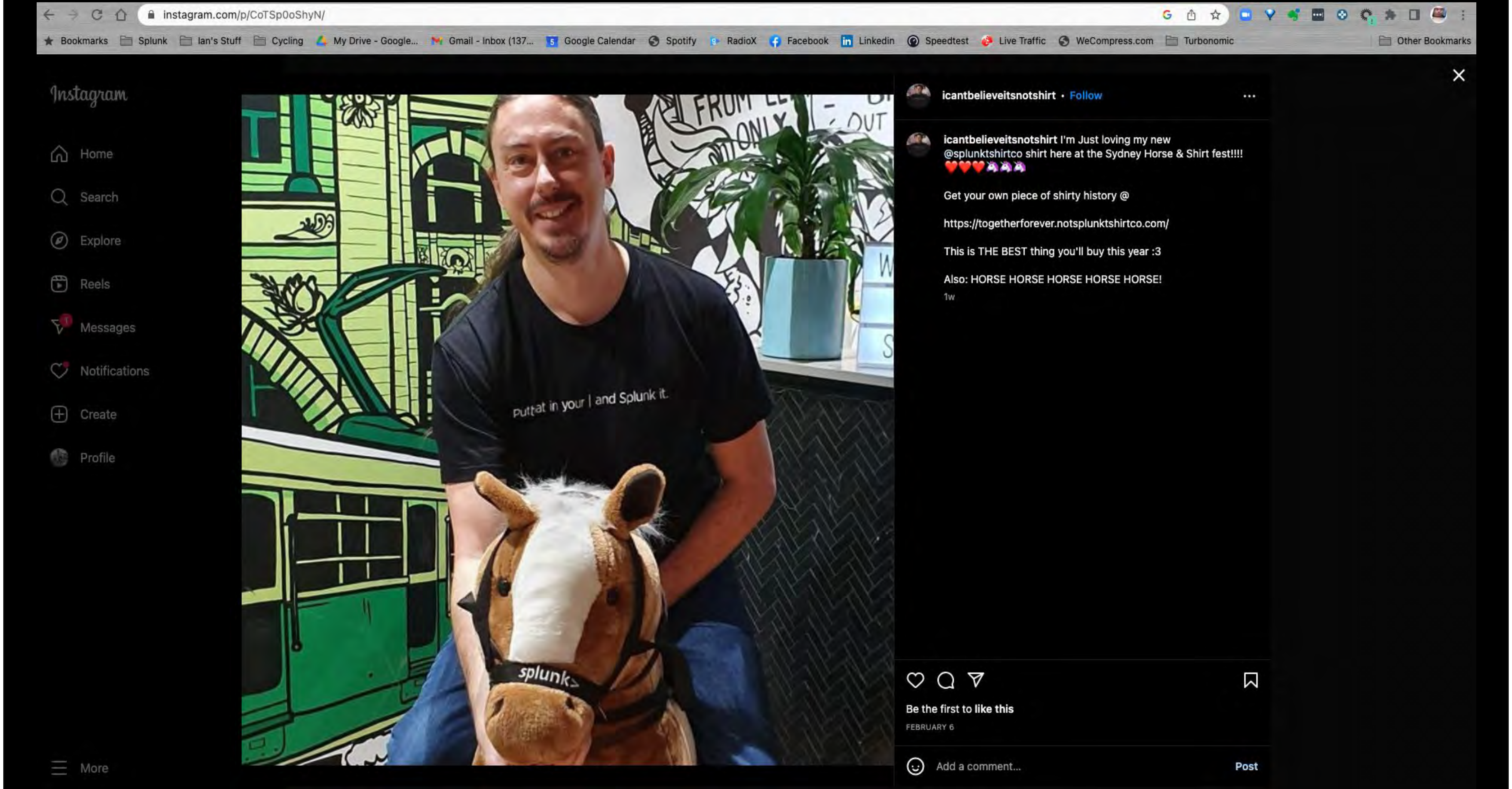
icantbelieveitsnotshirt

1 post 0 followers 0 following

I Can't Believe Its Not Shirt

© 2023 Instagram from Meta

splunk>



icantbelieveitsnotshirt I'm Just loving my new @splunktshirtco shirt here at the Sydney Horse & Shirt fest!!!! ❤️❤️❤️🦄🦄🦄

Get your own piece of shirty history @

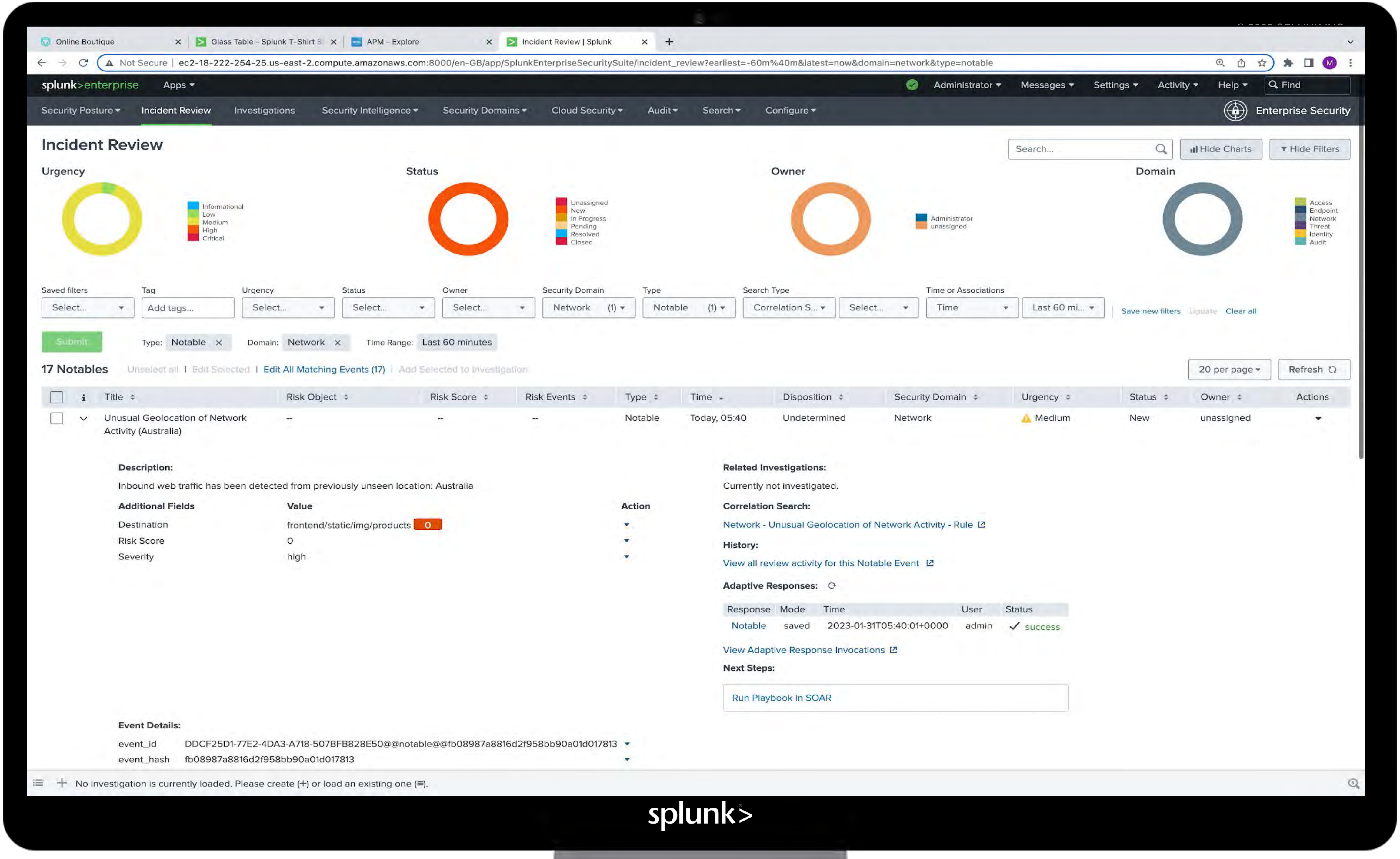
https://togetherforever.notsplunktshirtco.com/

This is THE BEST thing you'll buy this year :3

Also: HORSE HORSE HORSE HORSE HORSE!

1w

splunk>



Incident Review

Saved filters	Tag	Urgency	Status	Owner	Security Domain	Type	Search Type		Time or Associations	
Select...	Add tags...	Select...	Select...	Select...	Network (1)	Notable (1)	Correlation S...	Select...	Time	Last 60 mi...

Type: Notable × Domain: Network × Time Range: Last 60 minutes

17 Notables Unselect all | Edit Selected | Edit All Matching Events (17) | Add Selected to Investigation

□	i	Title	Risk Object	Risk Score	Risk Events	Type	Time	Disposition	Security Domain	Urgency	Status	Owner	Actions
□	⌄	Unusual Geolocation of Network Activity (Australia)	--	--	--	Notable	Today, 05:40	Undetermined	Network	⚠ Medium	New	unassigned	▾

Description:

Inbound web traffic has been detected from previously unseen location: Australia

Additional Fields	Value	Action
Destination	frontend/static/img/products 0	▾
Risk Score	0	▾
Severity	high	▾

Related Investigations:

Currently not investigated.

Correlation Search:

Network - Unusual Geolocation of Network Activity - Rule

History:

View all review activity for this Notable Event

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2023-01-31T05:40:01+0000	admin	✓ success

View Adaptive Response Invocations

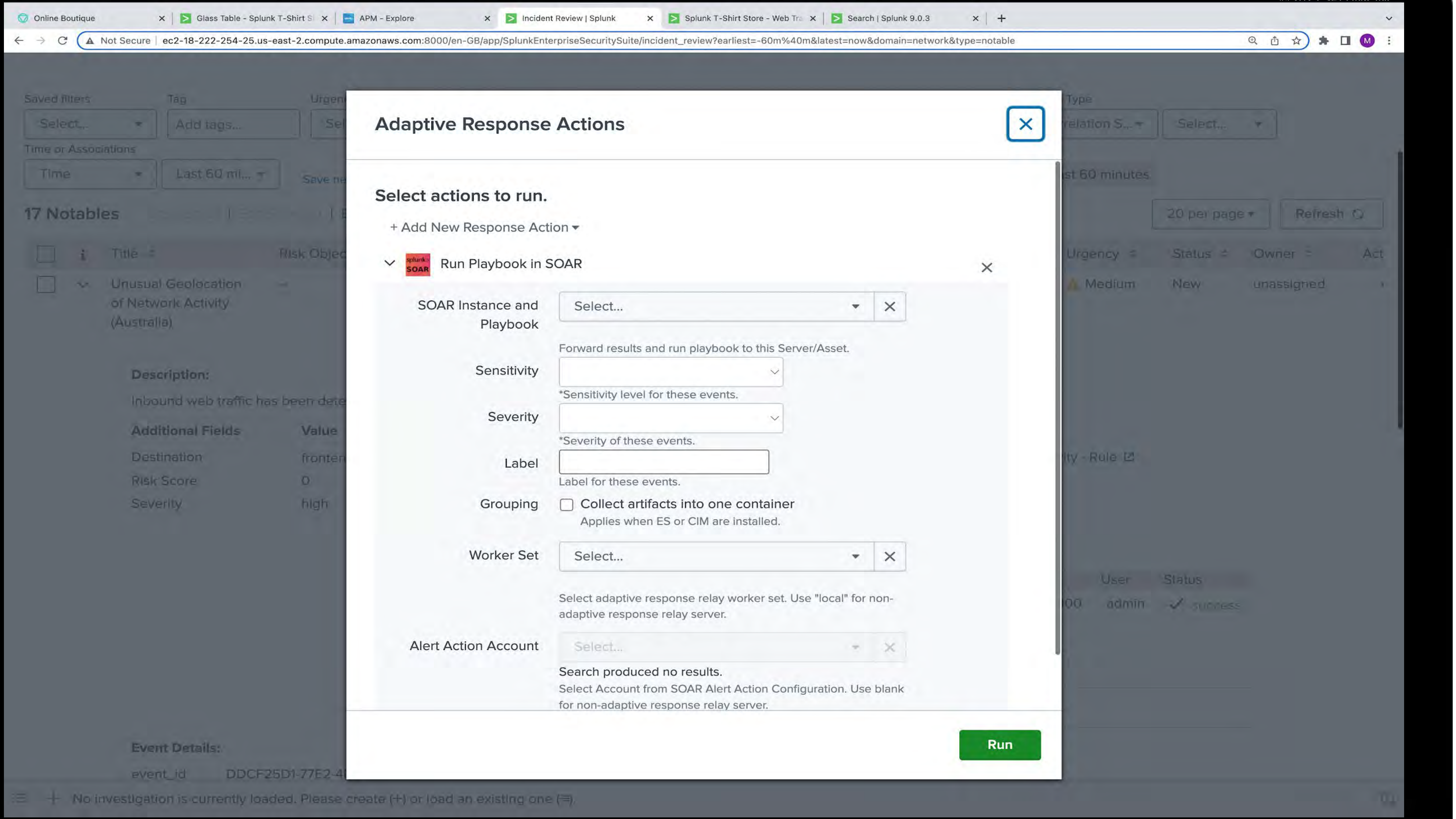
Next Steps:

Run Playbook in SOAR

Event Details:

event_id	DDCF25D1-77E2-4DA3-A718-507BFB828E50@@notable@@fb08987a8816d2f958bb90a01d017813
event_hash	fb08987a8816d2f958bb90a01d017813

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



Online Boutique
Glass Table - Splunk T-Shirt St
APM - Explore
Incident Review | Splunk
Splunk T-Shirt Store - Web Tra
Search | Splunk 9.0.3
Not Secure | ec2-18-222-254-25.us-east-2.compute.amazonaws.com:8000/en-GB/app/SplunkEnterpriseSecuritySuite/incident_review?earliest=-60m%40m&latest=now&domain=network&type=notable
17 Notables
Unusual Geolocation of Network Activity (Australia)
Medium
New
unassigned
No investigation is currently loaded. Please create (+) or load an existing one (≡).

Adaptive Response Actions

Select actions to run.

+ Add New Response Action ▾

Run Playbook in SOAR

SOAR Instance and Playbook: Select...

Forward results and run playbook to this Server/Asset.

Sensitivity:

*Sensitivity level for these events.

Severity:

*Severity of these events.

Label:

Label for these events.

Grouping: □ Collect artifacts into one container

Applies when ES or CIM are installed.

Worker Set: Select...

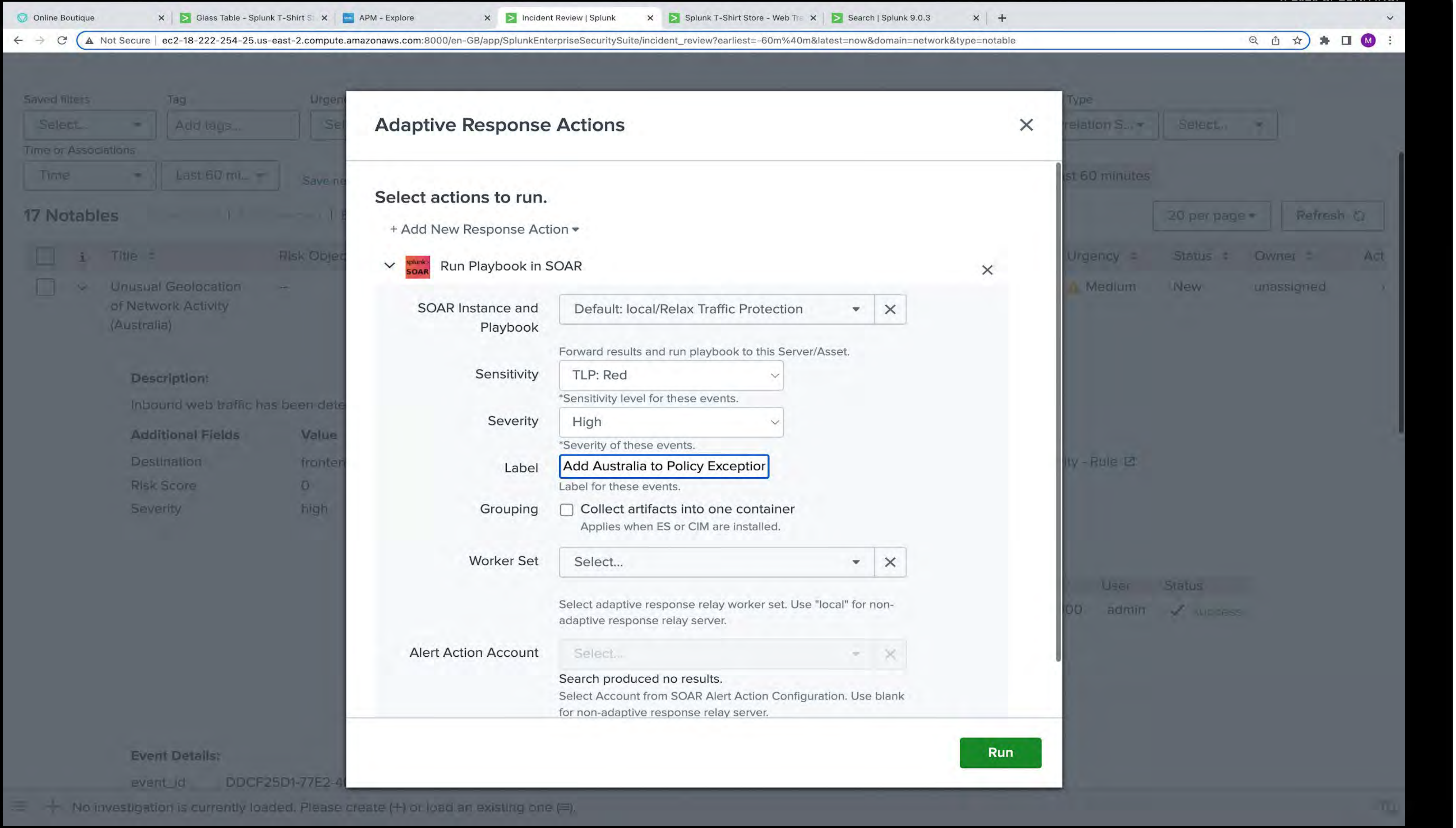
Select adaptive response relay worker set. Use "local" for non-adaptive response relay server.

Alert Action Account: Select...

Search produced no results.

Select Account from SOAR Alert Action Configuration. Use blank for non-adaptive response relay server.

splunk>



Online Boutique
Glass Table - Splunk T-Shirt S
APM - Explore
Incident Review | Splunk
Splunk T-Shirt Store - Web Tr
Search | Splunk 9.0.3
Not Secure
ec2-18-222-254-25.us-east-2.compute.amazonaws.com:8000/en-GB/app/SplunkEnterpriseSecuritySuite/incident_review?earliest=-60m%40m&latest=now&domain=network&type=notable

Adaptive Response Actions

Select actions to run.

+ Add New Response Action ▾

Run Playbook in SOAR

SOAR Instance and Playbook: Default: local/Relax Traffic Protection

Forward results and run playbook to this Server/Asset.

Sensitivity: TLP: Red

*Sensitivity level for these events.

Severity: High

*Severity of these events.

Label: Add Australia to Policy Exceptior

Label for these events.

Grouping: □ Collect artifacts into one container

Applies when ES or CIM are installed.

Worker Set: Select...

Select adaptive response relay worker set. Use "local" for non-adaptive response relay server.

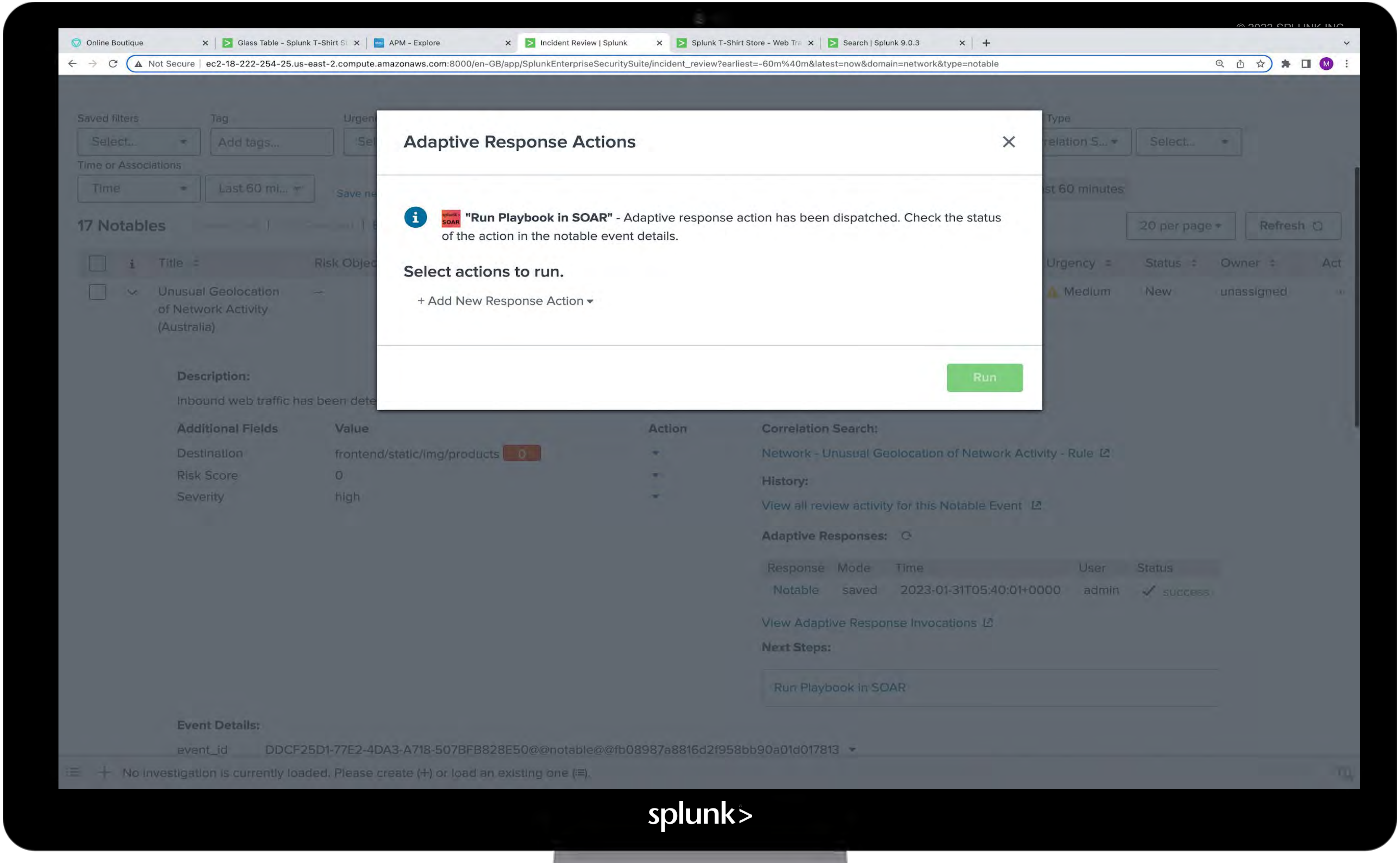
Alert Action Account: Select...

Search produced no results.

Select Account from SOAR Alert Action Configuration. Use blank for non-adaptive response relay server.

Run
17 Notables
Unusual Geolocation of Network Activity (Australia)
Description:
Inbound web traffic has been dete
Additional Fields
Value
Destination
fronten
Risk Score
0
Severity
high
Medium
New
unassigned
No investigation is currently loaded. Please create (+) or load an existing one (☰).

splunk>



Online Boutique
Glass Table - Splunk T-Shirt S
APM - Explore
Incident Review | Splunk
Splunk T-Shirt Store - Web Tra
Search | Splunk 9.0.3
Not Secure | ec2-18-222-254-25.us-east-2.compute.amazonaws.com:8000/en-GB/app/SplunkEnterpriseSecuritySuite/incident_review?earliest=-60m%40m&latest=now&domain=network&type=notable

Adaptive Response Actions

"Run Playbook in SOAR" - Adaptive response action has been dispatched. Check the status of the action in the notable event details.

Select actions to run.

+ Add New Response Action ▾
Run
Saved filters
Select...
Tag
Add tags...
Type
Select...
Time or Associations
Time
Last 60 mi...
17 Notables
20 per page
Refresh

Title	Risk Object	Urgency	Status	Owner
Unusual Geolocation of Network Activity (Australia)	–	Medium	New	unassigned

Description:

Inbound web traffic has been dete

Additional Fields	Value	Action
Destination	frontend/static/img/products 0	▾
Risk Score	0	▾
Severity	high	▾

Correlation Search:

Network - Unusual Geolocation of Network Activity - Rule

History:

View all review activity for this Notable Event

Adaptive Responses:

Response	Mode	Time	User	Status
Notable	saved	2023-01-31T05:40:01+0000	admin	✓ success

View Adaptive Response Invocations

Next Steps:

Run Playbook in SOAR

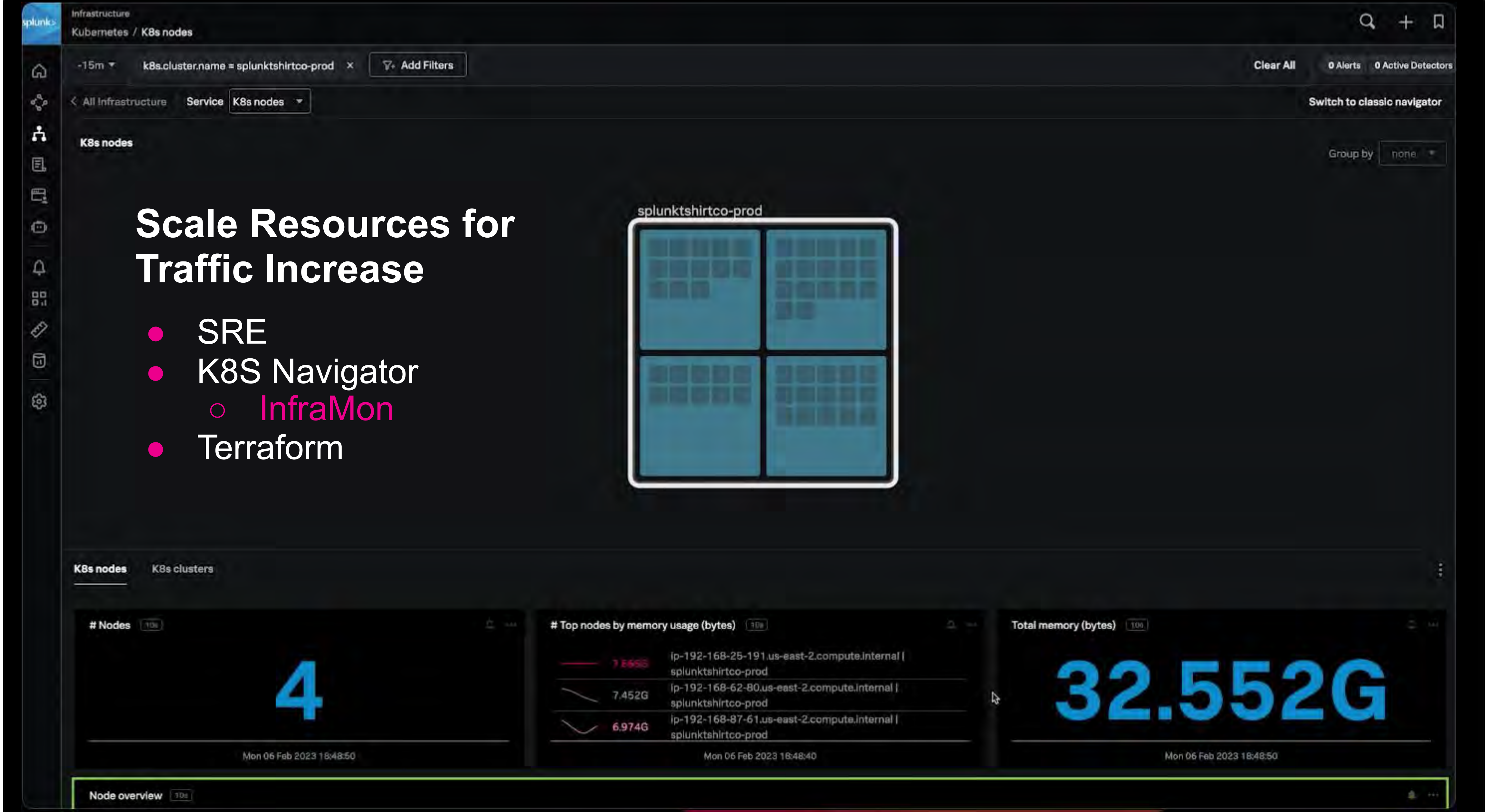
Event Details:

event_id DDCF25D1-77E2-4DA3-A718-507BFB828E50@@notable@@fb08987a8816d2f958bb90a01d017813

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

Scale Resources for Traffic Increase

- SRE
- K8S Navigator
  - InfraMon
- Terraform



Infrastructure

Kubernetes / K8s nodes

-15m ▾ k8s.cluster.name = splunktshirtco-prod × Add Filters

Clear All 0 Alerts 0 Active Detectors

‹ All Infrastructure Service K8s nodes ▾

Switch to classic navigator

K8s nodes

Group by none ▾

K8s nodes K8s clusters

Nodes 10s

4

Mon 06 Feb 2023 18:48:50

Top nodes by memory usage (bytes) 10s

7.656G	ip-192-168-25-191.us-east-2.compute.internal | splunktshirtco-prod
7.452G	ip-192-168-62-80.us-east-2.compute.internal | splunktshirtco-prod
6.974G	ip-192-168-87-61.us-east-2.compute.internal | splunktshirtco-prod

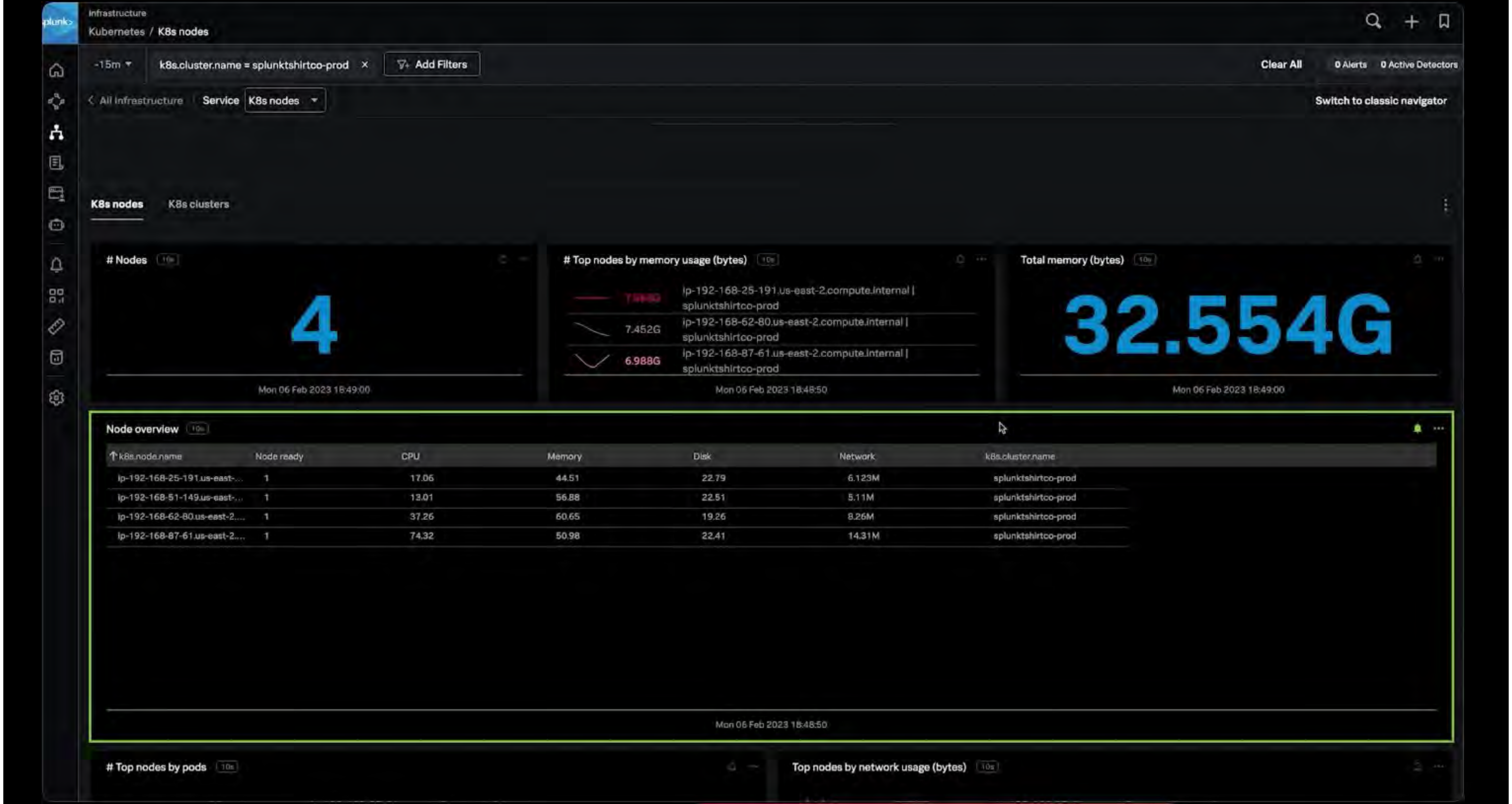
Mon 06 Feb 2023 18:48:40

Total memory (bytes) 10s

32.552G

Mon 06 Feb 2023 18:48:50

Node overview 10s



Nodes 10s

4

Mon 06 Feb 2023 18:49:00

Top nodes by memory usage (bytes) 10s

[illegible]	ip-192-168-25-191.us-east-2.compute.internal | splunktshirtco-prod
7.452G	ip-192-168-62-80.us-east-2.compute.internal | splunktshirtco-prod
6.988G	ip-192-168-87-61.us-east-2.compute.internal | splunktshirtco-prod

Mon 06 Feb 2023 18:48:50

Total memory (bytes) 10s

32.554G

Mon 06 Feb 2023 18:49:00

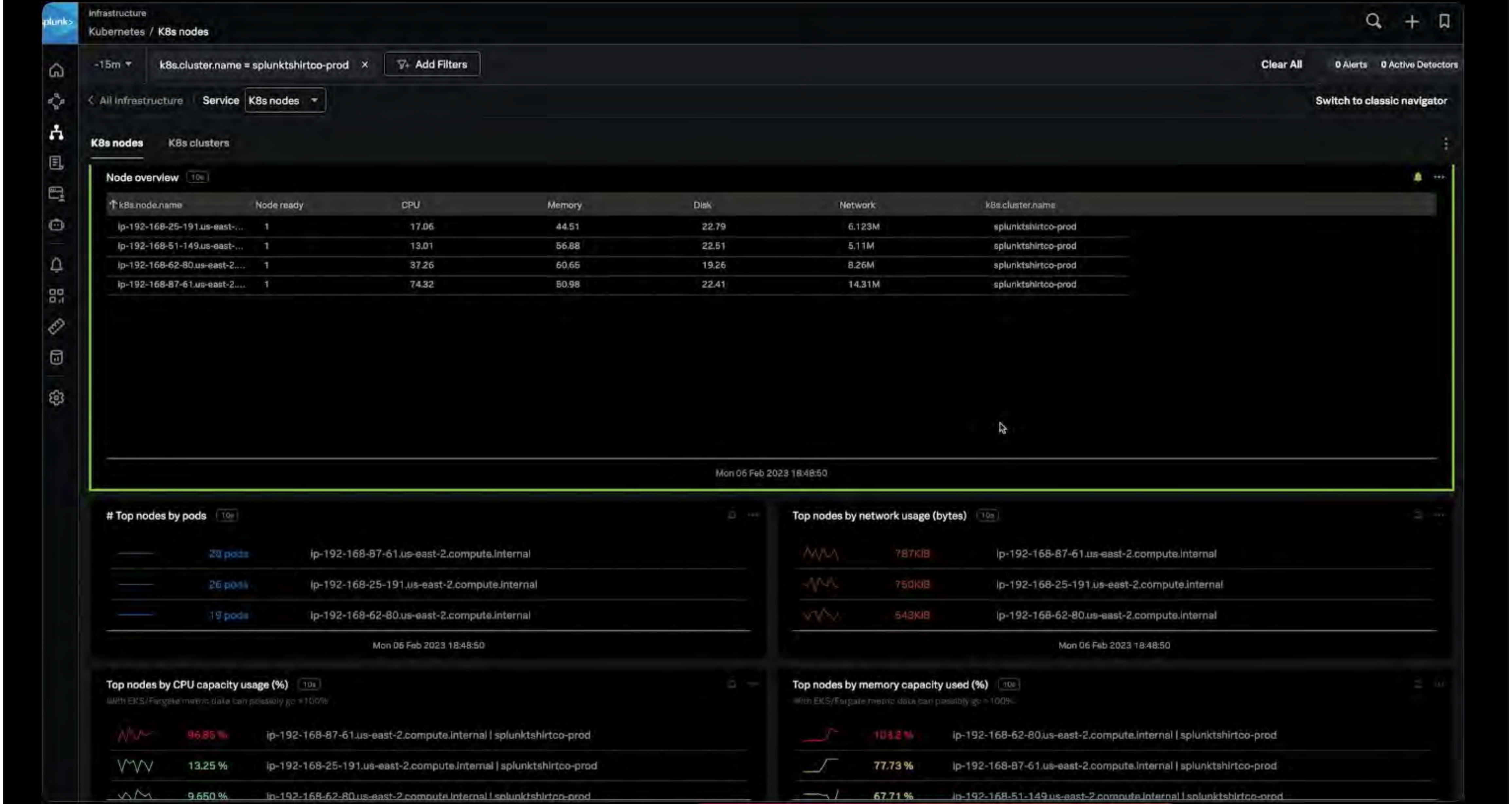
Node overview 10s

↑ k8s.node.name	Node ready	CPU	Memory	Disk	Network	k8s.cluster.name
ip-192-168-25-191.us-east-...	1	17.06	44.51	22.79	6.123M	splunktshirtco-prod
ip-192-168-51-149.us-east-...	1	13.01	56.88	22.51	5.11M	splunktshirtco-prod
ip-192-168-62-80.us-east-2....	1	37.26	60.65	19.26	8.26M	splunktshirtco-prod
ip-192-168-87-61.us-east-2....	1	74.32	50.98	22.41	14.31M	splunktshirtco-prod

Mon 06 Feb 2023 18:48:50

Top nodes by pods 10s

Top nodes by network usage (bytes) 10s



k8s.cluster.name = splunktshirtco-prod

Service: K8s nodes

Node overview

k8s.node.name	Node ready	CPU	Memory	Disk	Network	k8s.cluster.name
ip-192-168-25-191.us-east-...	1	17.06	44.51	22.79	6.123M	splunktshirtco-prod
ip-192-168-51-149.us-east-...	1	13.01	56.88	22.51	5.11M	splunktshirtco-prod
ip-192-168-62-80.us-east-2....	1	37.26	60.65	19.26	8.26M	splunktshirtco-prod
ip-192-168-87-61.us-east-2....	1	74.32	50.98	22.41	14.31M	splunktshirtco-prod

Mon 06 Feb 2023 18:48:50

# Top nodes by pods

28 pods	ip-192-168-87-61.us-east-2.compute.internal
26 pods	ip-192-168-25-191.us-east-2.compute.internal
19 pods	ip-192-168-62-80.us-east-2.compute.internal

Mon 06 Feb 2023 18:48:50

Top nodes by network usage (bytes)

787KiB	ip-192-168-87-61.us-east-2.compute.internal
750KiB	ip-192-168-25-191.us-east-2.compute.internal
543KiB	ip-192-168-62-80.us-east-2.compute.internal

Mon 06 Feb 2023 18:48:50

Top nodes by CPU capacity usage (%)

With EKS/Fargate metric data can possibly go >100%

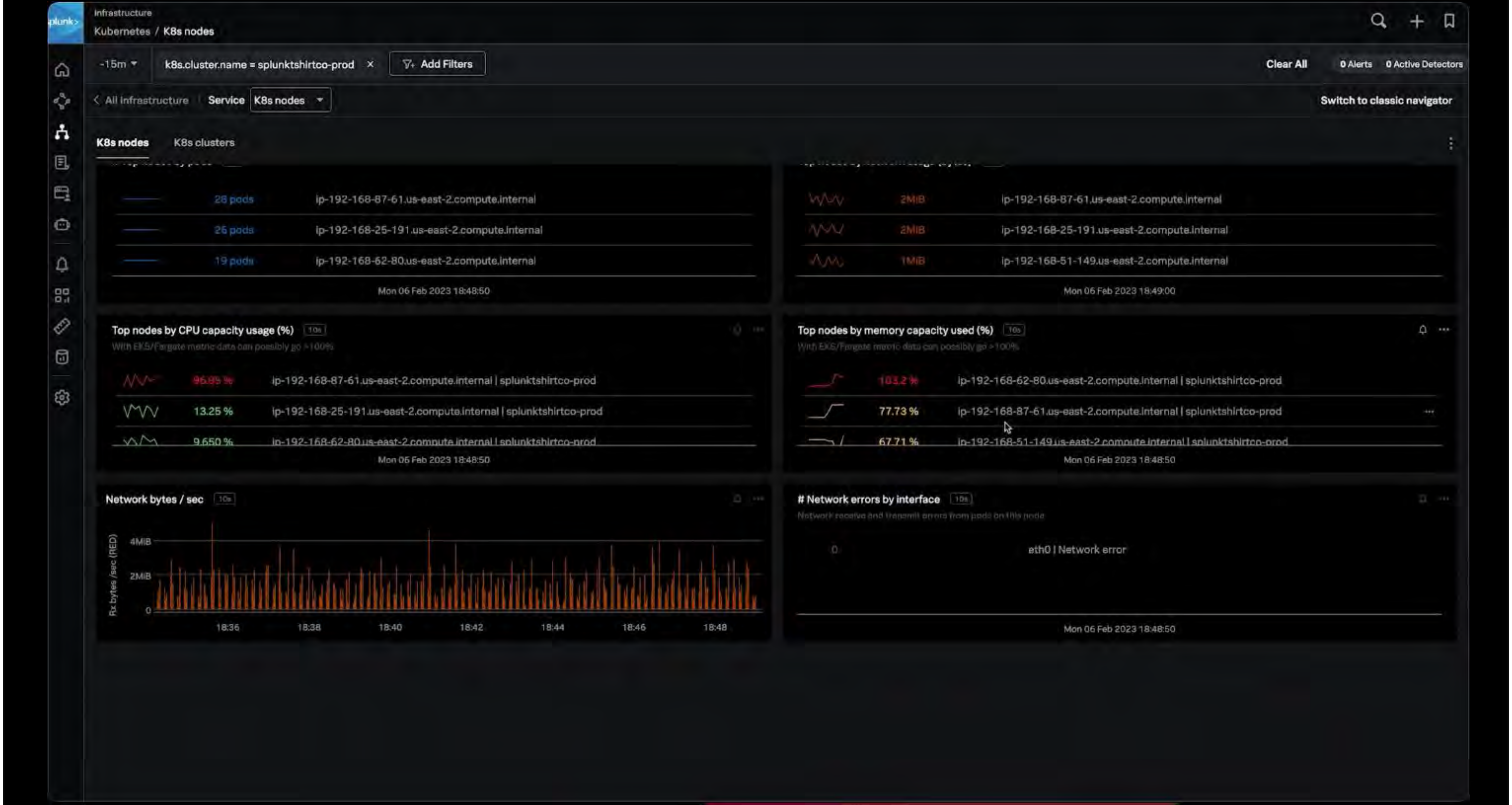
96.85 %	ip-192-168-87-61.us-east-2.compute.internal | splunktshirtco-prod
13.25 %	ip-192-168-25-191.us-east-2.compute.internal | splunktshirtco-prod
9.650 %	ip-192-168-62-80.us-east-2.compute.internal | splunktshirtco-prod

Top nodes by memory capacity used (%)

With EKS/Fargate metric data can possibly go > 100%

103.2 %	ip-192-168-62-80.us-east-2.compute.internal | splunktshirtco-prod
77.73 %	ip-192-168-87-61.us-east-2.compute.internal | splunktshirtco-prod
67.71 %	ip-192-168-51-149.us-east-2.compute.internal | splunktshirtco-prod

splunk>



k8s.cluster.name = splunktshirtco-prod

Service: K8s nodes

28 pods	ip-192-168-87-61.us-east-2.compute.internal
26 pods	ip-192-168-25-191.us-east-2.compute.internal
19 pods	ip-192-168-62-80.us-east-2.compute.internal

Mon 06 Feb 2023 18:48:50

2MIB	ip-192-168-87-61.us-east-2.compute.internal
2MIB	ip-192-168-25-191.us-east-2.compute.internal
1MIB	ip-192-168-51-149.us-east-2.compute.internal

Mon 06 Feb 2023 18:49:00

Top nodes by CPU capacity usage (%) 10s

With EKS/Fargate metric data can possibly go >100%

96.95 %	ip-192-168-87-61.us-east-2.compute.internal | splunktshirtco-prod
13.25 %	ip-192-168-25-191.us-east-2.compute.internal | splunktshirtco-prod
9.650 %	ip-192-168-62-80.us-east-2.compute.internal | splunktshirtco-prod

Mon 06 Feb 2023 18:48:50

Top nodes by memory capacity used (%) 10s

With EKS/Fargate metric data can possibly go >100%

103.2 %	ip-192-168-62-80.us-east-2.compute.internal | splunktshirtco-prod
77.73 %	ip-192-168-87-61.us-east-2.compute.internal | splunktshirtco-prod
67.71 %	ip-192-168-51-149.us-east-2.compute.internal | splunktshirtco-prod

Mon 06 Feb 2023 18:48:50

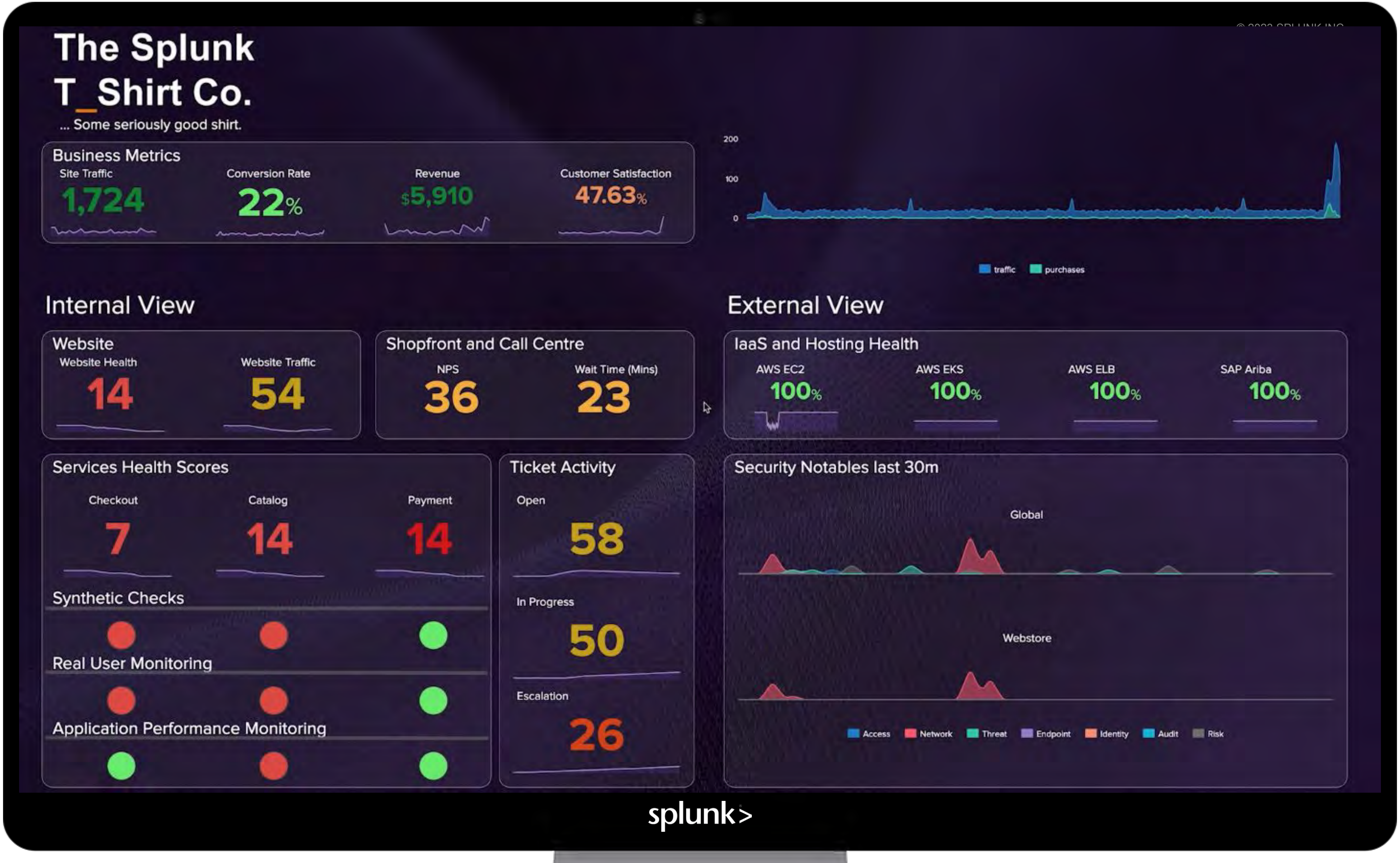
Network bytes / sec 10s

Network errors by interface 10s

Network receive and transmit errors from pods on this node

0	eth0 | Network error

Mon 06 Feb 2023 18:48:50



The Splunk T_Shirt Co.

... Some seriously good shirt.

Business Metrics

Site Traffic 1,724

Conversion Rate 22%

Revenue $5,910

Customer Satisfaction 47.63%

Internal View

Website

Website Health 14

Website Traffic 54

Shopfront and Call Centre

NPS 36

Wait Time (Mins) 23

Services Health Scores

Checkout 7

Catalog 14

Payment 14

Synthetic Checks

🔴 🔴 🟢

Real User Monitoring

🔴 🔴 🟢

Application Performance Monitoring

🟢 🔴 🟢

Ticket Activity

Open 58

In Progress 50

Escalation 26

External View

IaaS and Hosting Health

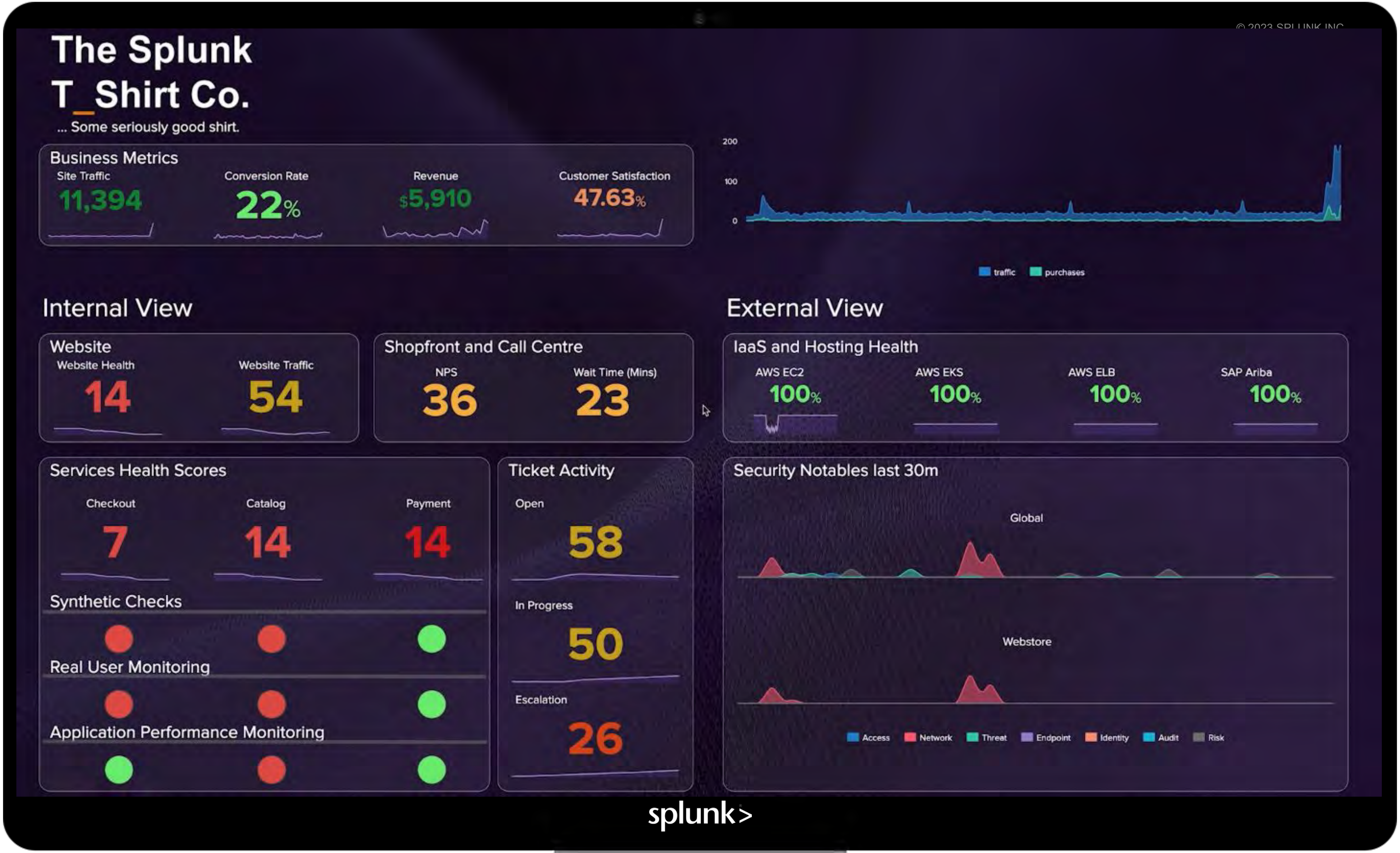
AWS EC2 100%

AWS EKS 100%

AWS ELB 100%

SAP Ariba 100%

Security Notables last 30m



The Splunk T_Shirt Co.

... Some seriously good shirt.

Business Metrics

Site Traffic	Conversion Rate	Revenue	Customer Satisfaction
11,394	22%	$5,910	47.63%

Internal View

Website

Website Health	Website Traffic
14	54

Shopfront and Call Centre

NPS	Wait Time (Mins)
36	23

Services Health Scores

Checkout	Catalog	Payment
7	14	14

Synthetic Checks

🔴 🔴 🟢

Real User Monitoring

🔴 🔴 🟢

Application Performance Monitoring

🟢 🔴 🟢

Ticket Activity

Open 58

In Progress 50

Escalation 26

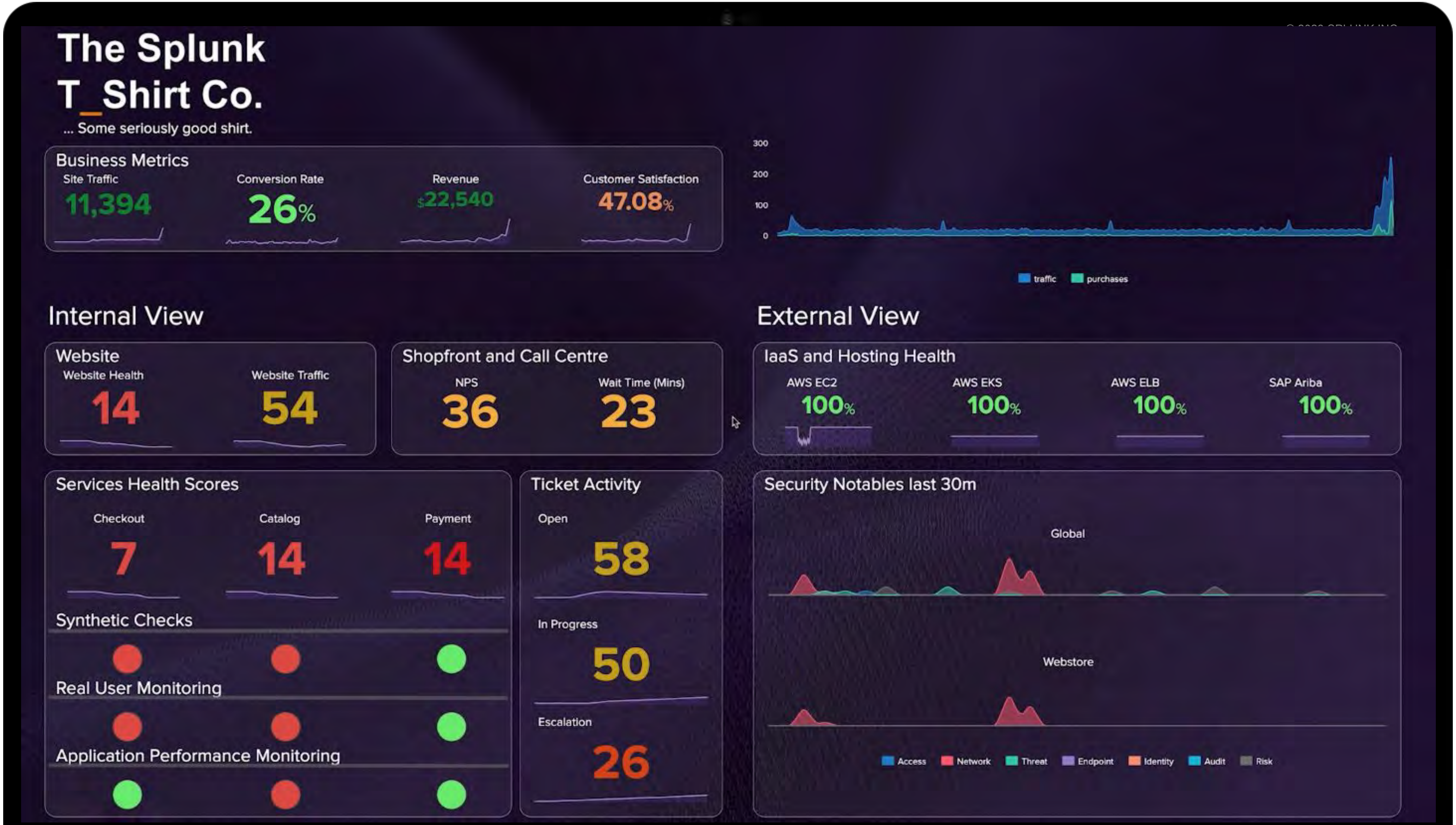
External View

IaaS and Hosting Health

AWS EC2	AWS EKS	AWS ELB	SAP Ariba
100%	100%	100%	100%

Security Notables last 30m

splunk>



The Splunk T_Shirt Co.

... Some seriously good shirt.

Business Metrics

Site Traffic 11,394

Conversion Rate 26%

Revenue $22,540

Customer Satisfaction 47.08%

Internal View

Website

Website Health 14

Website Traffic 54

Shopfront and Call Centre

NPS 36

Wait Time (Mins) 23

Services Health Scores

Checkout 7

Catalog 14

Payment 14

Synthetic Checks

● ● ●

Real User Monitoring

● ● ●

Application Performance Monitoring

● ● ●

Ticket Activity

Open 58

In Progress 50

Escalation 26

External View

IaaS and Hosting Health

AWS EC2 100%

AWS EKS 100%

AWS ELB 100%

SAP Ariba 100%

Security Notables last 30m

splunk>