



YOU KNOW, FOR SEARCH (AND  
VISIBILITY)

CARLY RICHMOND





# History

**2000**

Creation of Compass, the first iteration, and later Elasticsearch based on Apache Lucene

**2012**

Founding of Elasticsearch Inc. with ELK

**2015**

Welcoming Beats into the Elastic family

**2018**

Opening of the commercial X-Pack features

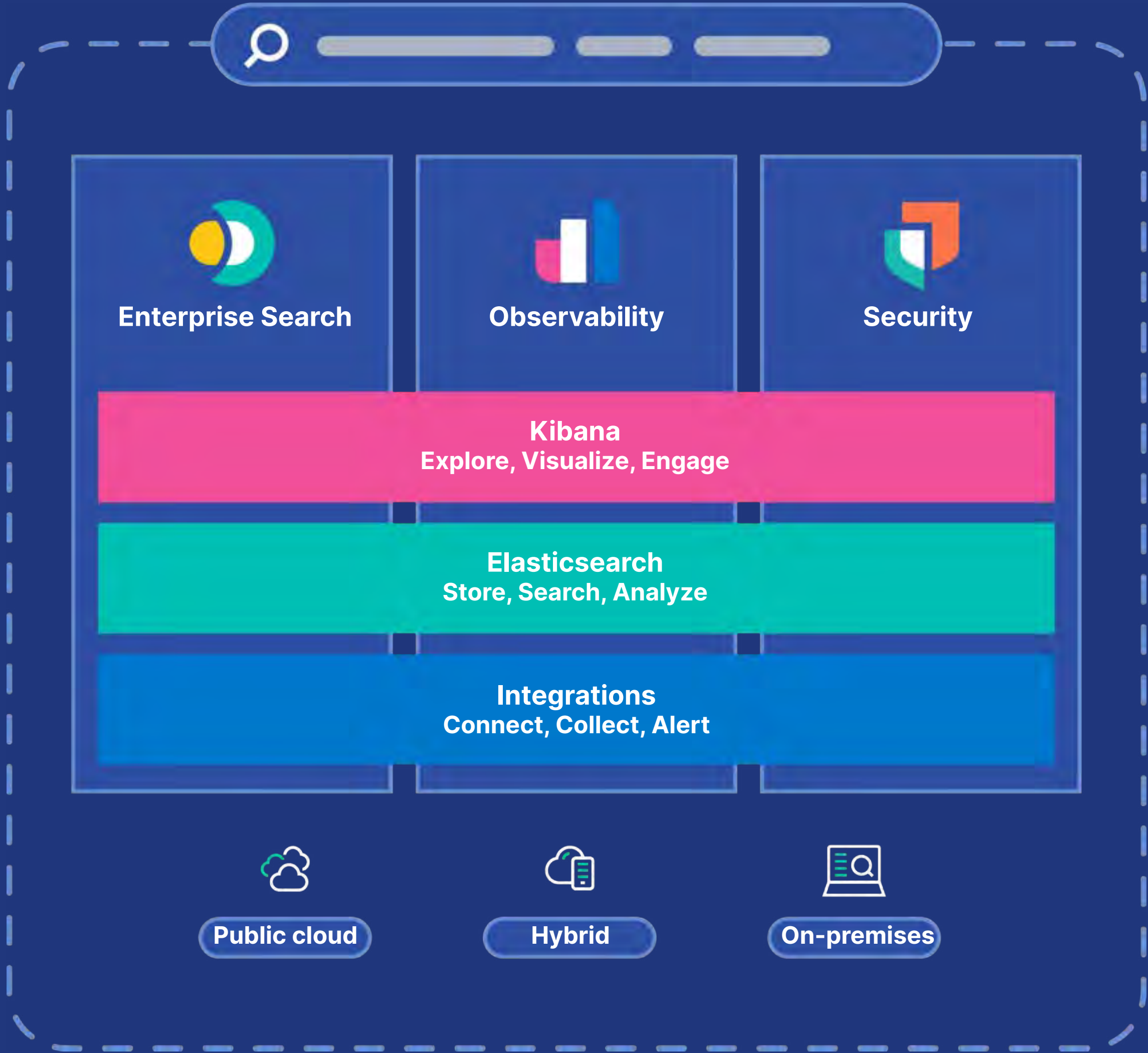
**2019**

Launch of Elastic SIEM and acquisition of Endgame

**2021**

1st annual Elastic Community Conference

# The Elastic Search Platform



Developers like me



“All programmers are optimists. Perhaps this modern sorcery especially attracts those who believe in happy endings and fairy godmothers.”

–FREDERICK P. BROOKS JR, THE MYTHICAL MAN-MONTH



DONE

DOING

To Do



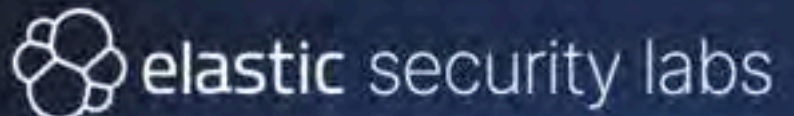




**DARKNET**  
  
**DIARIES**



Security Labs | Elastic  
elastic.co/security-labs/



# 2023 Elastic Global Threat Report - Spring




## Elastic publishes 2023 Global Threat Report Spring Edition

This week, we're publishing a new version of this report that's online and interactive, which includes additional data covering the remainder of 2022, written using Elastic technologies.

By **Devon Kerr**  
24 April 2023

### Featured

- Elastic Security Labs discovers the LOBSHOT malware**  
By **Daniel Stepanic**  
25 April 2023
- Elastic Global Threat Report Multipart Series Overview**  
By **Devon Kerr**  
17 April 2023
- Attack chain leads to XWORM and AGENTTESLA**  
By **Salim Bitam**  
07 April 2023



Learn more about HackerOne

Log In



# Elastic

<https://www.elastic.co/> · @elastic

Submit report

Bug Bounty Program  
Launched on Aug 2021

- Managed by HackerOne
- Includes retesting ?
- Bounty splitting enabled ?

Reports resolved	Assets in scope	Average bounty
245	19	\$245-\$250

- Policy
- Scope
- New!
- Hacktivity
- Thanks
- Updates (0)
- Collaborators

## Rewards

- Low
- Medium
- High
- Critical

### Elastic Synthetics Monitoring

\$300 - \$1,400	\$1,400 - \$3,000	\$3,000 - \$6,000	\$6,000 - \$14,000
-----------------	-------------------	-------------------	--------------------

### other

\$100 - \$200	\$200 - \$300	\$300 - \$800	\$800 - \$2,000
---------------	---------------	---------------	-----------------

### All Elastic Products

## Response Efficiency

- 9 hrs  
Average time to first response
- about 1 day  
Average time to triage
- 10 days  
Average time to bounty
- about 1 month  
Average time to resolution
- 94% of reports  
Meet [response standards](#)

**COME  
TOGE  
THER**

“**Traceability** allows you to track configuration items across the development cycle to where requirements are implemented in the code. This can play a crucial part in your organization’s control framework as it helps achieve compliance, reduce bugs, ensure secure code in application development, and help code maintainability.”

–IBM, WHAT IS DEVSECOPS?

“**Traceability** allows you to track configuration items across the development cycle to where requirements are implemented in the code. This can play a crucial part in your organization’s control framework as it helps achieve compliance, **reduce bugs, ensure secure code in application development**, and help code maintainability.”

–IBM, WHAT IS DEVSECOPS?

# UNDER THE HOOD

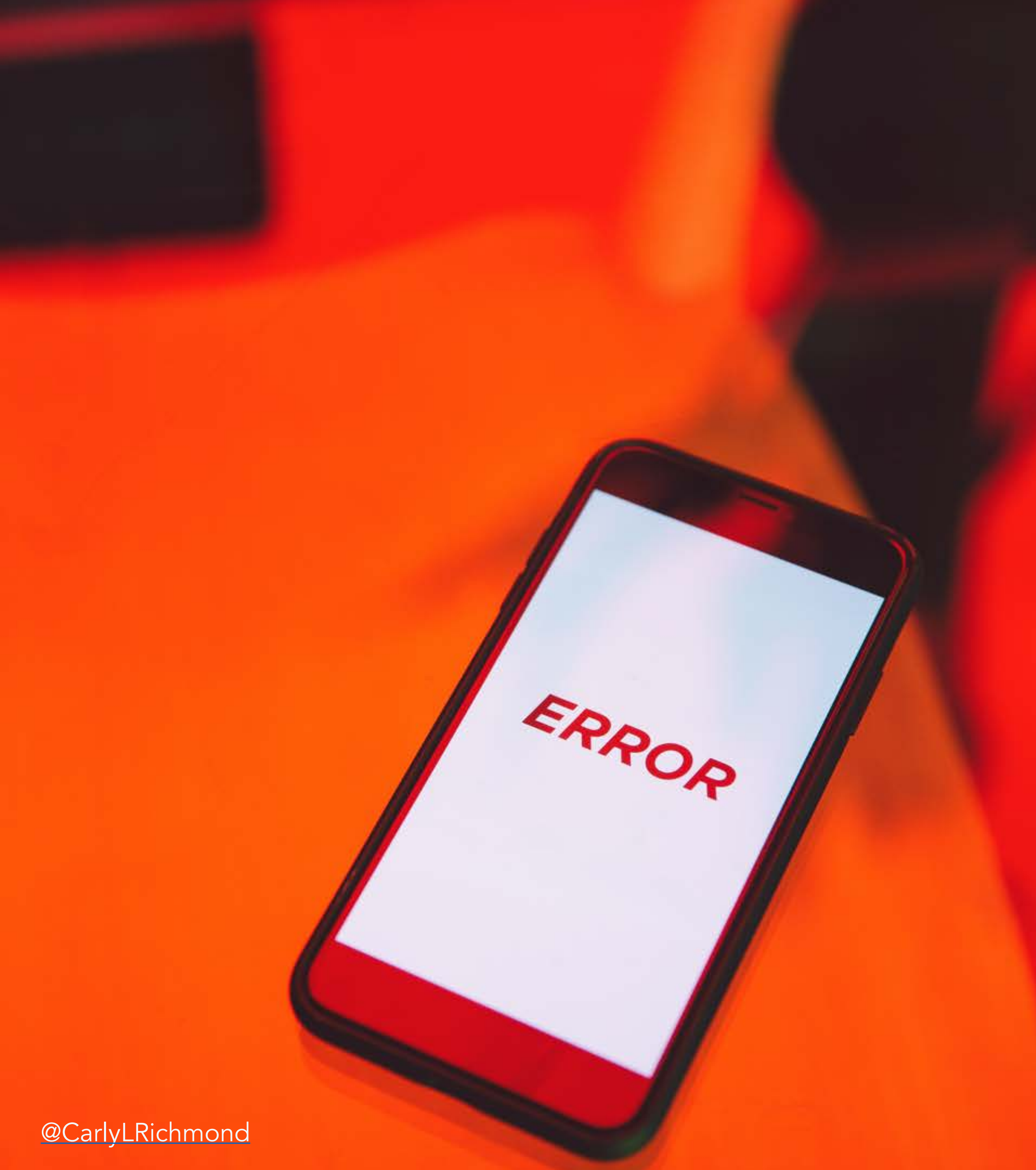


# ELASTICSEARCH BASIC SECURITY

- Automatic as of v8.x, with manual guides available
- Enable password protection
- RBAC out of the box
- mTLS communication between Elasticsearch and Kibana
- TLS certificates and keys generated for transport and HTTP layers







“Security Misconfigurations Caused 35% of All Time Cyber Incidents”

-SOCRADAR, FEBRUARY 23 2023

UPDATED 20:05 EDT / OCTOBER 27 2022



# Thomson Reuters exposes 3TB+ of sensitive data on unsecured ElasticSearch database

BY DUNCAN RILEY



Media conglomerate Thomson Reuters Corp. has been found to have exposed more than 3 terabytes of sensitive customer and corporate data, the latest company to fail in applying basic security to its

### CUBE EVENT COVERAGE



Breaking Analysis: RSA 2023 Security Identity Crisis Part 2

VIEW FULL VIDEO

### LATEST FROM THECUBE

- Pepperdata and AWS join forces to tackle big data cost challenges
- nOps leverages AI to optimize cloud costs in pay-for-savings-only model

# BOOTSTRAP CHECKS

- Java checks
- All permission check
- System call filter check
- Early-access check
- SSL/TLS check
- ... and others



# PLUGINS

- Isolate Elasticsearch plugins
- Seccomp



# PAINLESS

- Java Security Manager usage
- Sandboxing
- Per-method allow list
- Self-reference detection



# DIVE FURTHER INTO THE RABBIT HOLE



SCAN ME



“**Traceability** allows you to **track configuration items across the development cycle** to where requirements are implemented in the code. This can play a crucial part in your organization’s control framework as it helps achieve compliance, reduce bugs, ensure secure code in application development, and help code maintainability.”

–IBM, WHAT IS DEVSECOPS?



# SYNTHETIC MONITORS AS E2E TESTS



CLICK ME!



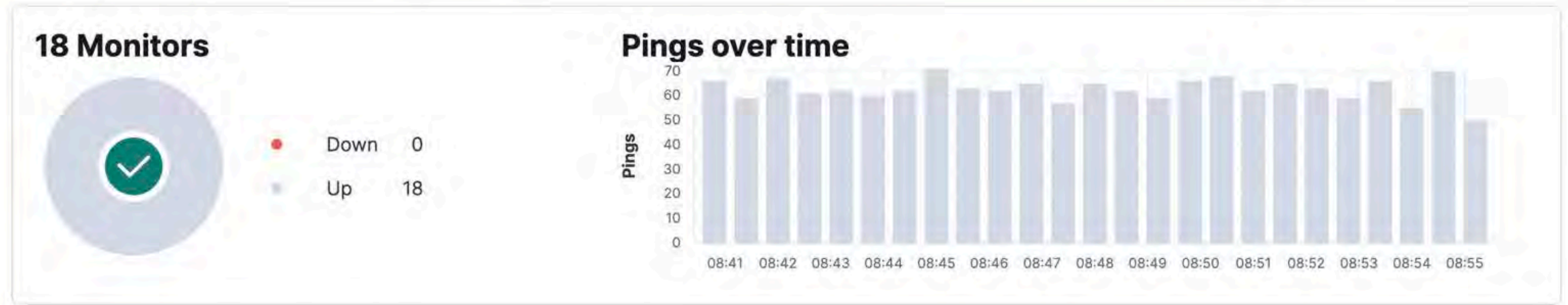
- Observability
- Overview
- Alerts
- Cases
- Logs
- Stream
- Anomalies
- Categories
- Infrastructure
- Inventory
- Metrics Explorer
- Hosts
- APM
- Services
- Traces
- Dependencies
- Uptime
- Uptime Monitors
- TLS Certificates

# Monitors

Last 15 minutes 1 m Refresh

Search by monitor ID, name, URL, port or tags

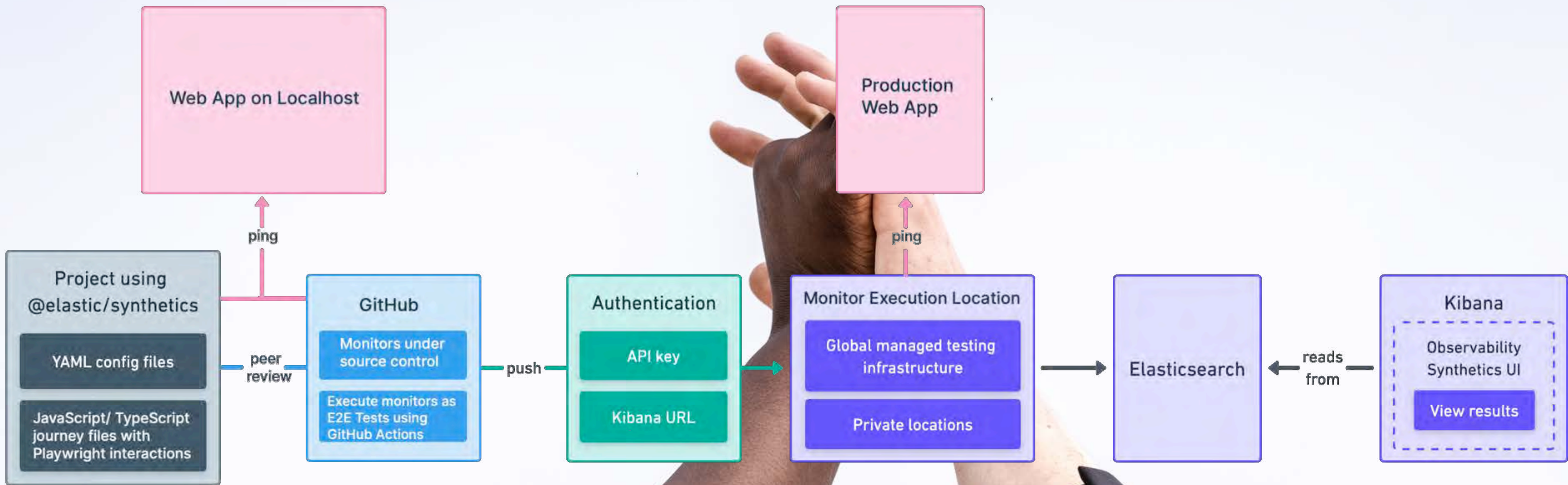
Location 8 Port 12 Scheme 2 Tag 0



### Monitors

All Up Down

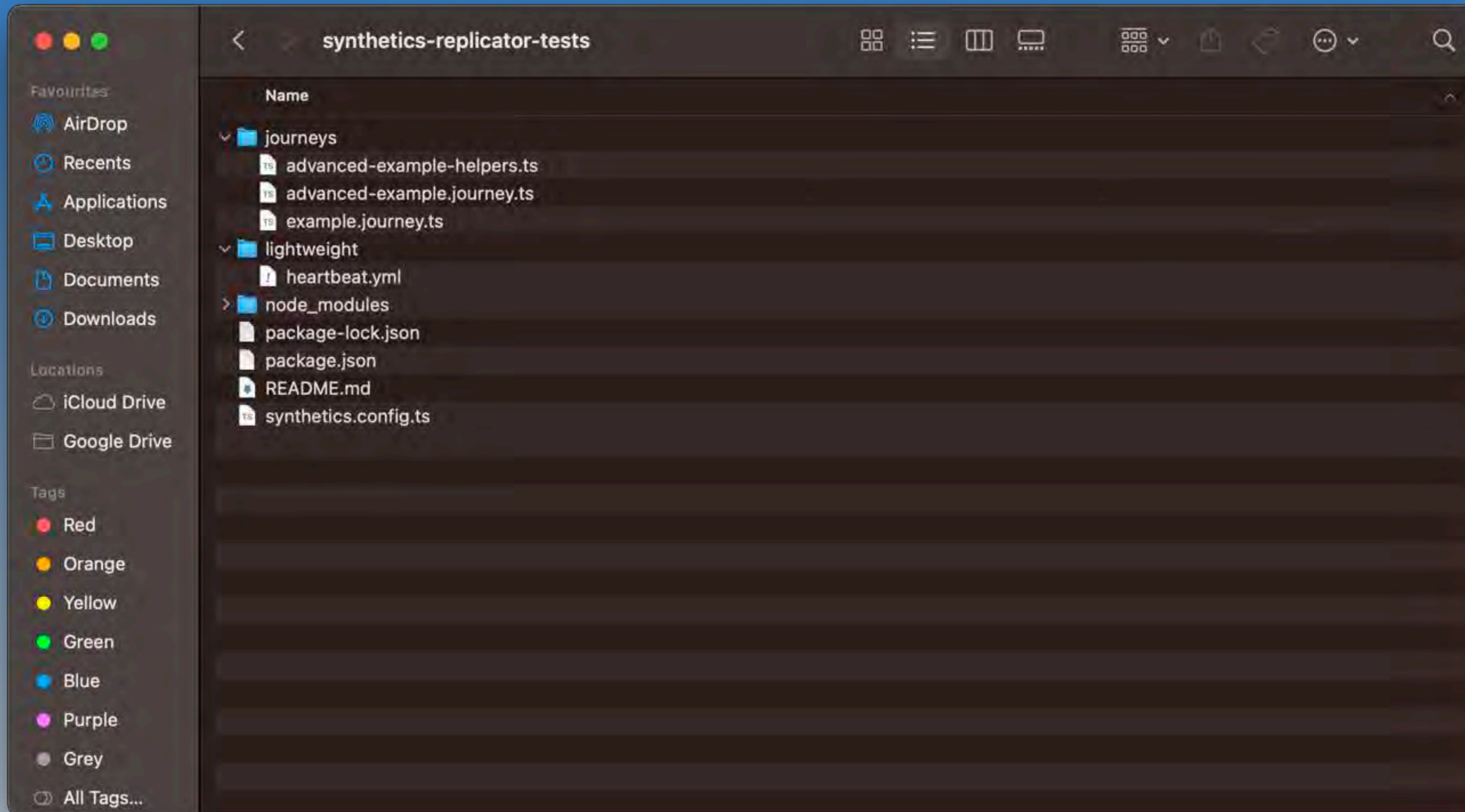
Status	Name	Url	Tags	TLS Certificate	Downtime history	Status alert	Test now
Up in 3/3 locations, Checked 8:51:09 AM	https://elastic.co Browser	https://elastic.co/		--	--	<input type="checkbox"/>	<input type="button" value="▶"/>
Up in 1/1 location, Checked 8:55:37 AM	cartservice-green TCP Ping	tcp://10.72.0.114:11000		--	--	<input type="checkbox"/>	<input type="button" value="▶"/>



# SYNTHETIC MONITORING



CLICK ME!



heartbeat.yml

```
1 heartbeat.monitors:  
2 - type: http  
3   name: Replicator HTTP ping  
4   id: synthetics-replicator-monitor-http  
5   enabled: true  
6   urls: "https://synthetics-replicator.netlify.app/"  
7   schedule: '@every 3m'  
8   timeout: 16s
```



```

orders.journey.ts

1 import { journey, step, monitor, expect, before } from '@elastic/synthetics';
2
3 journey('Replicator Order Journey', ({ page, params }) => {
4   // Only relevant for the push command to create
5   // monitors in Kibana
6   monitor.use({
7     id: 'synthetics-replicator-monitor',
8     schedule: 10,
9   });
10
11  before(async () => {
12    await page.goto(params.url);
13  });
14
15  step('assert home page loads', async () => {
16    const header = await page.locator('h1');
17    expect(await header.textContent()).toBe('Replicatr');
18  });
19
20  step('assert move to order page', async () => {
21    const orderButton = await page.getByTestId('order-button');
22    await orderButton.click();
23
24    const url = page.url();
25    expect(url).toContain('/order');
26
27    const menuTiles = await page.getByTestId('menu-item-card');
28    expect(await menuTiles.count()).toBeGreaterThan(2);
29  });
30
31  step('assert adding to order', async () => {
32    const addItemButtons = await page.getByTestId('add-item-button');
33    expect(await addItemButtons.count()).toBeGreaterThan(10);
34
35    const cartCount = await page.getByTestId('cart-count-label');
36    expect(await cartCount.innerText()).toBe('0');
37
38    await addItemButtons.first().click();
39    expect(await cartCount.innerText()).toBe('1');
40
41    await addItemButtons.nth(4).click();
42    await addItemButtons.last().click();
43    expect(await cartCount.innerText()).toBe('3');
44  });
45 });

```



```
synthetics-replicator — -zsh — 99x27
carly.richmond@Carlys-MBP synthetics-replicator % npm run test

> synthetics-replicator@0.0.0 test
> cd apps/synthetics-replicator-tests && npm run test

> synthetics-replicator-tests@1.0.0 test
> npx @elastic/synthetics journeys

Journey: Replicator Order Journey
  ✓ Step: 'launch application' succeeded (2030 ms)
  ✓ Step: 'assert home page loads' succeeded (48 ms)
  ✓ Step: 'assert move to order page' succeeded (132 ms)
  ✓ Step: 'assert adding to order' succeeded (150 ms)

Journey: Recorded Order journey
  ✓ Step: 'Go to order items page' succeeded (1752 ms)
  ✓ Step: 'Add item to cart successfully' succeeded (99 ms)
  ✓ Step: 'Add 2nd item to cart successfully' succeeded (66 ms)
  ✓ Step: 'Add 3rd item to cart successfully' succeeded (67 ms)

8 passed (5388 ms)

carly.richmond@Carlys-MBP synthetics-replicator %
```





**“Visibility**... means the organization has a solid monitoring system in place to measure the heartbeat of the operation, send alerts, increase awareness of changes and cyberattacks as they occur, and provide accountability during the whole project lifecycle.”

-IBM, WHAT IS DEVSECOPS?

“**Visibility**... means the organization has a **solid monitoring system in place to measure the heartbeat of the operation**, send alerts, increase awareness of changes and cyberattacks as they occur, and provide accountability during the whole project lifecycle.”

–IBM, WHAT IS DEVSECOPS?



# OBSERVABILITY

**Logs**

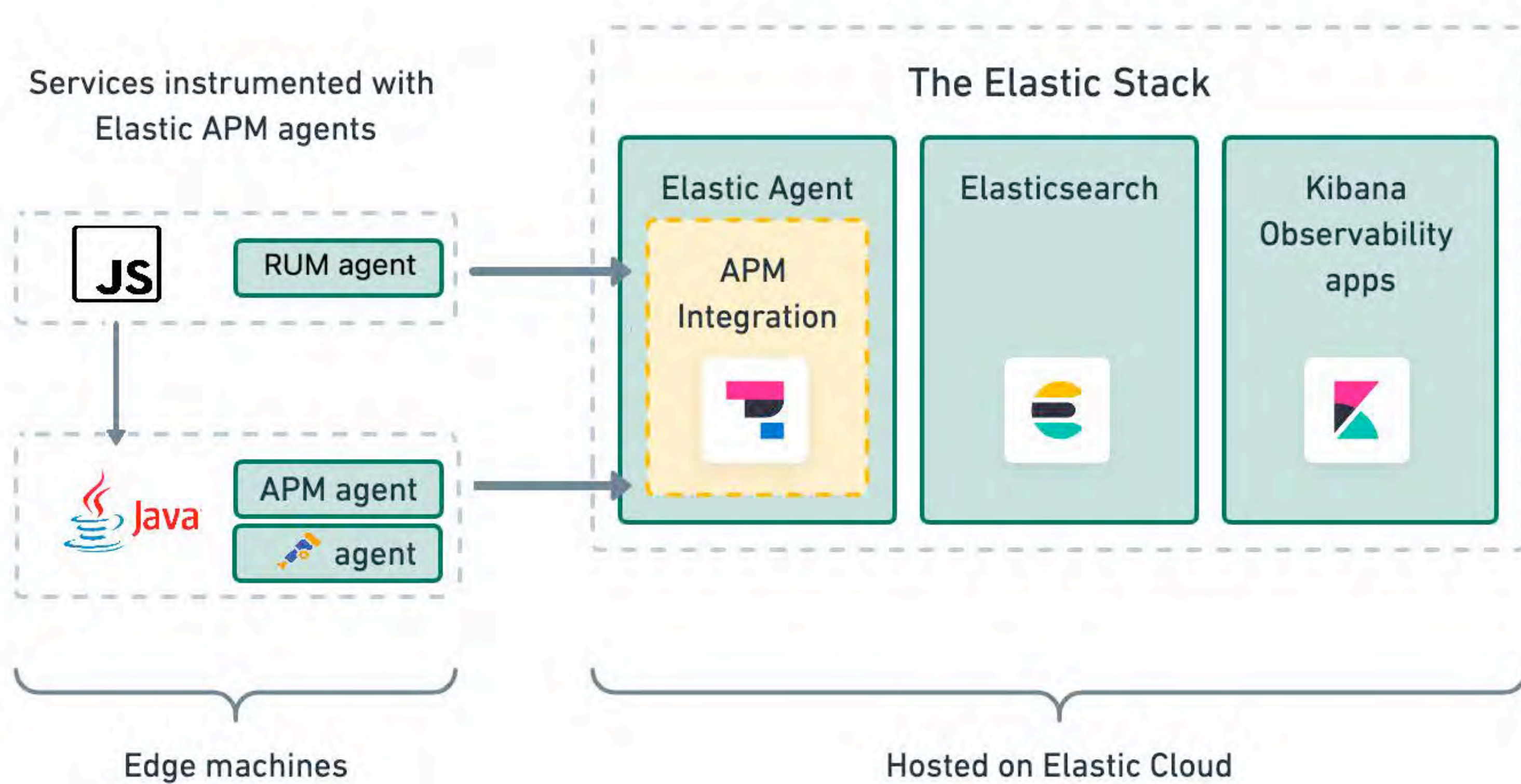
**Metrics**

**Traces  
(APM)**

# APM & RUM



# APM & RUM





app.js

```
1 import { init as initApm } from '@elastic/apm-rum';  
2  
3 const apm = initApm({  
4   serviceName: 'rum-records-react-ui',  
5   distributedTracingOrigins: ['http://localhost:8080'],  
6   serverUrl: 'https://my-elastic-deployment:122',  
7   serviceVersion: '1',  
8   environment: 'dev'  
9 });
```

## run-my-java-app.sh

```
1 export OTEL_RESOURCE_ATTRIBUTES=  
2     service.name=rum-records-server,  
3     service.version=1,  
4     deployment.environment=dev  
5 export OTEL_EXPORTER_OTLP_ENDPOINT=https://my-elastic-deployment:122  
6 export OTEL_EXPORTER_OTLP_HEADERS=Authorization=Bearer ssss$$$hhhhhhhhhhh  
7 export OTEL_METRICS_EXPORTER=otlp  
8 export OTEL_LOGS_EXPORTER=otlp  
9 export OTEL_TRACES_EXPORTER=otlp  
10  
11 java -javaagent:/path/to/opentelemetry-javaagent.jar  
12     com.rum.records.store.server.RumRecordsServerApplication
```

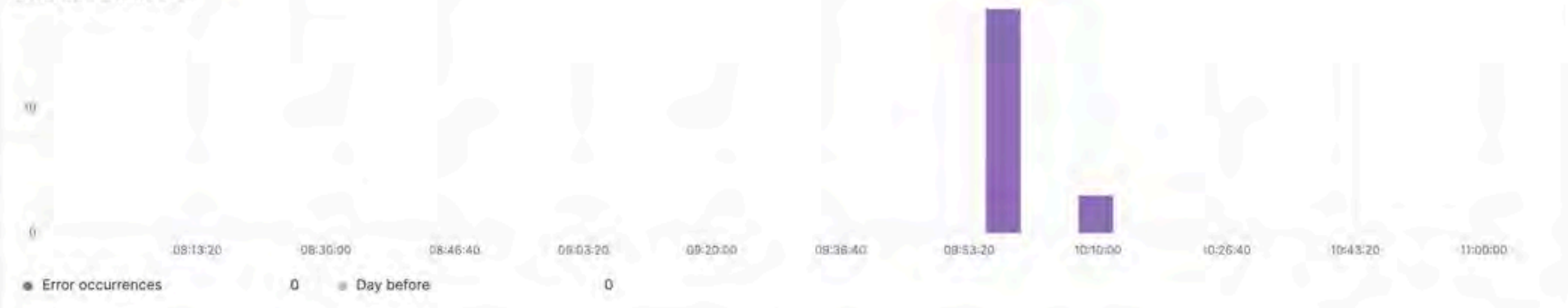


RED ALERT!

# Error group 3b5dc 21 occ

- Observability
- Overview
- Alerts
- Cases
- Logs
- Stream
- Anomalies
- Categories
- Infrastructure
- Inventory
- Metrics Explorer
- Hosts
- APM
- Services
- Traces
- Dependencies
- Uptime
- Uptime Monitors
- TLS Certificates
- Synthetics BETA
- User Experience
- Dashboard

## Error occurrences



## Top 5 affected transactions

Transaction name	Error
No errors found associated with transactions	

## Error sample

2 years ago | /hipstershop.AdService/getAds | prod | 1.8.0 [View 21 occurrences](#)

### Exception message

```
1,000 milliseconds timeout on connection http-outgoing-8 [ACTIVE]
```

### Culprit

```
hipstershop.AdService.getAdsFromES(AdService.java:304)
```

### Exception stack trace Metadata

#### java.net.SocketTimeoutException: 1,000 milliseconds timeout on connection http-outgoing-8 [ACTIVE]

```
> 7 library frames
at hipstershop.AdService.getAdsFromES(AdService.java:304)
at hipstershop.AdService.getAdsByCategory(AdService.java:262)
at hipstershop.AdService.access$400(AdService.java:49)
at hipstershop.AdService$AdServiceImpl.getAds(AdService.java:173)
at hipstershop.AdServiceGrpc$MethodHandlers.invoke(AdServiceGrpc.java:209)
> 12 library frames
```

### CAUSED BY

#### 1,000 milliseconds timeout on connection http-outgoing-8 [ACTIVE]

```
at org.apache.http.nio.protocol.HttpAsyncRequestExecutor.timeout(HttpAsyncRequestExecutor.java:387)
at org.apache.http.impl.nio.client.InternalIODispatch.onTimeout(InternalIODispatch.java:92)
at org.apache.http.impl.nio.client.InternalIODispatch.onTimeout(InternalIODispatch.java:39)
at org.apache.http.impl.nio.reactor.AbstractIODispatch.timeout(AbstractIODispatch.java:175)
at org.apache.http.impl.nio.reactor.BaseIOReactor.sessionTimedOut(BaseIOReactor.java:261)
```

- Observability**
- Overview
- Alerts
- Cases
- Logs**
- Stream**
- Anomalies
- Categories
- Infrastructure**
- Inventory
- Metrics Explorer
- Hosts
- APM**
- Services
- Traces
- Dependencies
- Uptime**
- [@CarlyLRichmond](#)
- Uptime Monitors

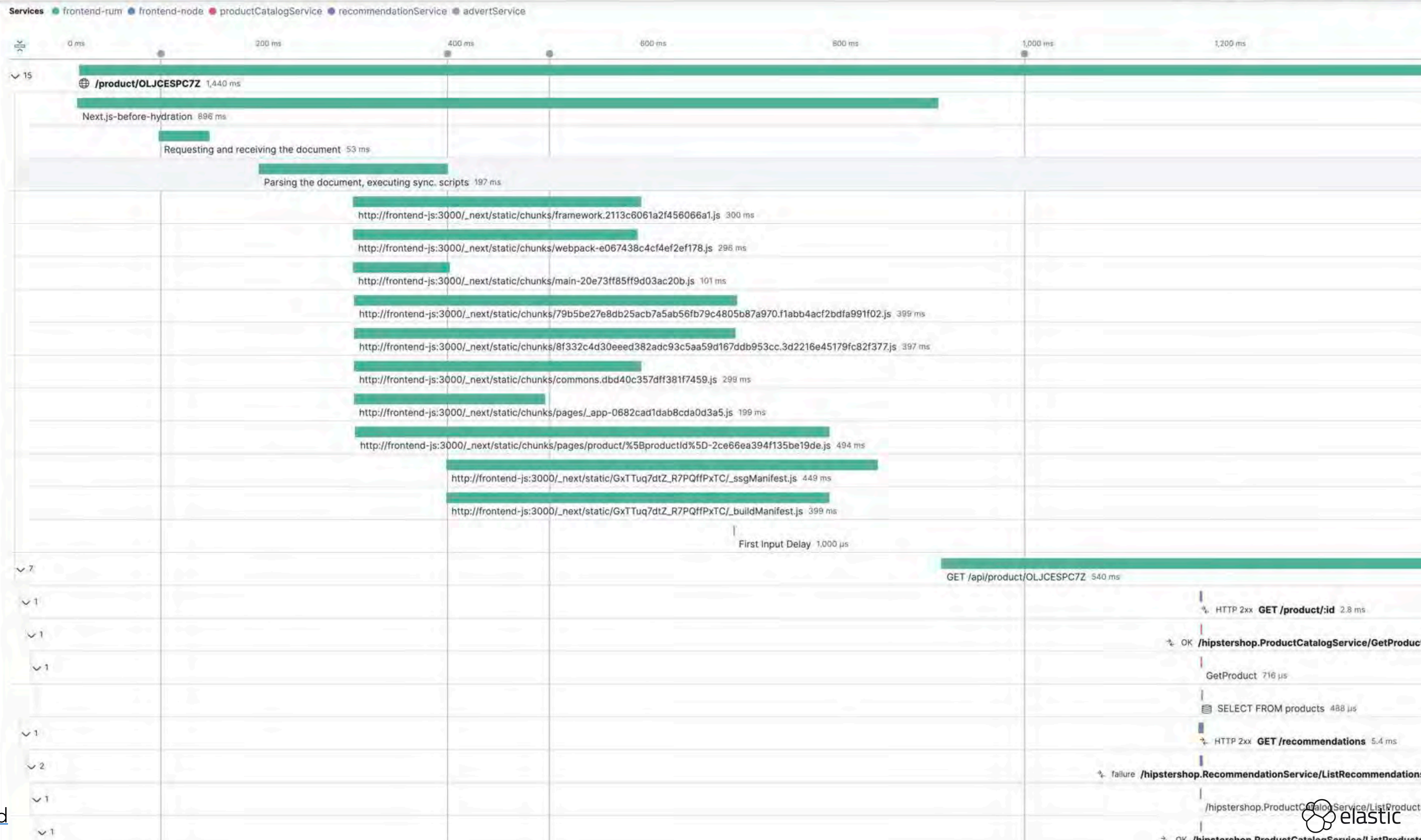
# Stream

Feb 3, 2021 @ 08:00:00.000 → Feb 3, 2021 @ 11:00:00.000

Customize Highlights

Feb 3, 2021	event.dataset	Message	
10:59:42.453	frontend-node.log	[frontend-node.log][info] /recommendations - fetching recommendations	
10:59:42.458	advertService.log	[advertService.log][INFO] received ad request (context_words=[Gardenin g])	08:15
10:59:42.868	advertService.log	[advertService.log][INFO] Returning 2 ads	
10:59:42.872	frontend-node.log	[frontend-node.log][info] /ads - fetching ads	08:30
10:59:42.878	productCatalogService.log	[productCatalogService.log][info] 2384.285000152886-1612349979241	
10:59:42.878	productCatalogService.log	[productCatalogService.log][info] Getting product with ID 0PUK6V6EV0	
10:59:42.878	productCatalogService.log	[productCatalogService.log][info] 2384.285000152886-1612349979241	08:45
10:59:42.878	productCatalogService.log	[productCatalogService.log][info] Getting product with ID LS4PSXUNUM	
10:59:42.878	productCatalogService.log	[productCatalogService.log][info] 2384.285000152886-1612349979241	
10:59:42.878	productCatalogService.log	[productCatalogService.log][info] Getting product with ID L9ECAV7KIM	
10:59:42.878	productCatalogService.log	[productCatalogService.log][info] 2384.285000152886-1612349979241	09 AM
10:59:42.878	productCatalogService.log	[productCatalogService.log][info] Getting product with ID 0LJCESPC7Z	
10:59:42.878	productCatalogService.log	[productCatalogService.log][info] Found product with ID LS4PSXUNUM	
10:59:42.878	productCatalogService.log	[productCatalogService.log][info] Found product with ID 0PUK6V6EV0	09:15
10:59:42.879	frontend-node.log	[frontend-node.log][info] /product/:id - fetching product by ID	

- Observability
- Overview
- Alerts
- Cases
- Logs
- Stream
- Anomalies
- Categories
- Infrastructure
- Inventory
- Metrics Explorer
- Hosts
- APM
- Services
- Traces
- Dependencies
- Uptime
- Uptime Monitors
- TLS Certificates
- Synthetics
- User Experience
- Dashboard



- Observability
- Overview
- Alerts
- Cases
- Logs
- Stream
- Anomalies
- Categories
- Infrastructure
- Inventory
- Metrics Explorer
- Hosts
- APM
- Services
- Traces
- Dependencies
- Uptime
- Uptime Monitors
- TLS Certificates
- Synthetics
- User Experience
- Dashboard

# Hosts TECHNICAL PREVIEW

Search hosts (E.g. cloud.provider:gcp AND system.load.1 > 0.5)

Feb 3, 2021 @ 08:00:00.000 → Feb 3, 2021 @ 11:00:00.000

Operating System Any Cloud Provider Any

Hosts  
**5**

CPU usage  
Average  
**28.6%**

Memory usage  
Average  
**18%**

Network inbound (RX)  
Average  
**0 bit/s**

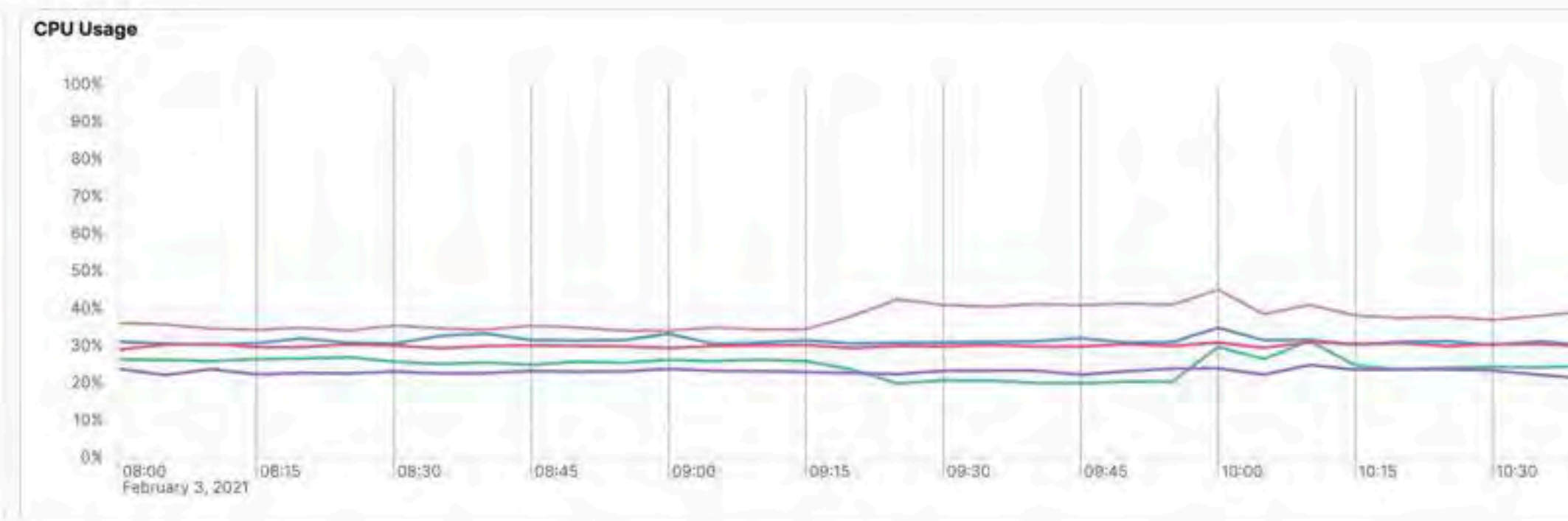
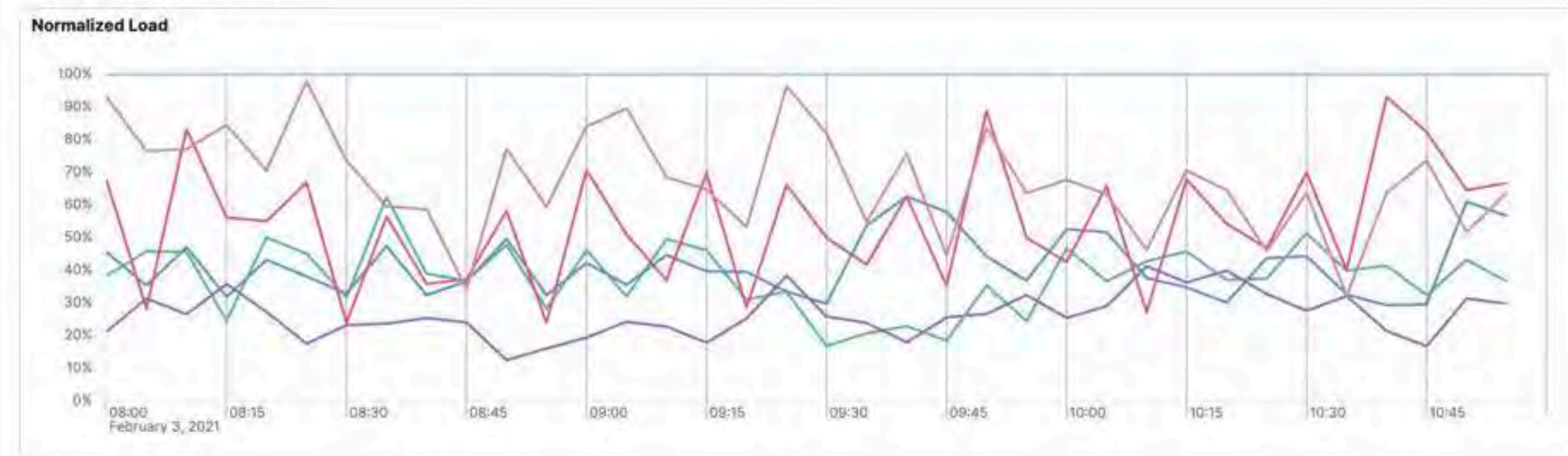
Network outbound (TX)  
Average  
**0 bit/s**

Name	Operating System	# of CPUs	Disk Latency (avg.)	RX (avg.)	TX (avg.)	Memory total (avg.)
gke-eden-3-staging-ssd-3-bc76...	CentOS Linux	16	0 ms	0 bit/s	0 bit/s	63.3 GB
gke-eden-3-staging-ssd-3-bc76...	CentOS Linux	16	0 ms	0 bit/s	0 bit/s	63.3 GB
gke-eden-3-staging-ssd-3-bc76...	CentOS Linux	16	0 ms	0 bit/s	0 bit/s	63.3 GB
gke-eden-3-staging-ssd-3-bc76...	CentOS Linux	16	0 ms	0 bit/s	0 bit/s	63.3 GB
gke-eden-3-staging-ssd-3-bc76...	CentOS Linux	16	0 ms	0 bit/s	0 bit/s	63.3 GB

Rows per page: 10

## Metrics

Showing for Top 20 hosts by name



- Observability
- Overview
- Alerts
- Cases
- Logs
- Stream
- Anomalies
- Categories
- Infrastructure
- Inventory
- Metrics Explorer
- Hosts
- APM
- Services
- Traces
- Dependencies
- Uptime
- Uptime Monitors
- TLS Certificates
- Synthetics BETA
- User Experience
- Dashboard

# Dashboard

Web application frontend-rum Percentile 50th (Median) Environment All

Filter by URL Location 50 Device 26 OS 12 Browser 17

### Page load (median)

Total	Backend	Frontend	Total page views
<b>983 ms</b>	<b>8 ms</b>	<b>975 ms</b>	<b>13 k</b>

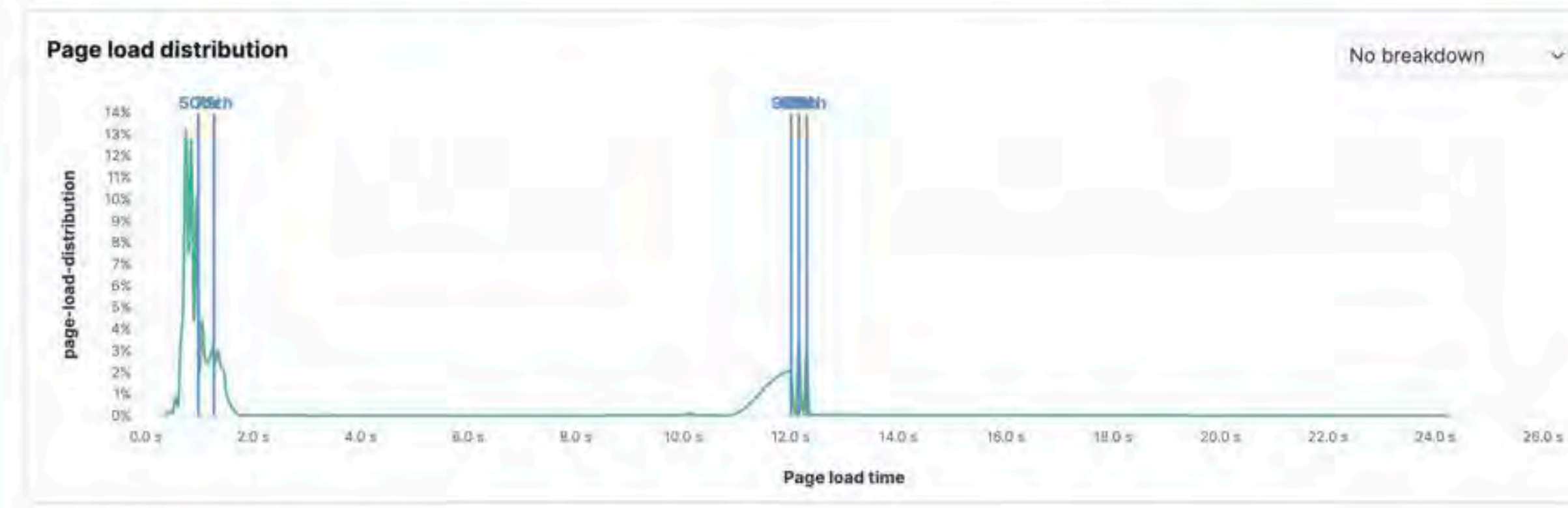
### Metrics (median)

First contentful paint	Total blocking time	No. of long tasks	Longest long task duration	Total long tasks duration
<b>299 ms</b>	<b>49 ms</b>	<b>1</b>	<b>102 ms</b>	<b>105 ms</b>

### Core web vitals

Largest contentful paint	First input delay	Cumulative layout shift
<b>305 ms</b>	<b>2 ms</b>	<b>0.000</b>

Good (100%) Needs improvement (0%) Poor (0%)
 Good (99%) Needs improvement (1%) Poor (0%)
Good (100%) Needs improvement (0%) Poor (0%)



# SYNTHETIC MONITORING



- Observability
- Overview
- Alerts
- Cases
- Logs
- Stream
- Anomalies
- Categories
- Infrastructure
- Inventory
- Metrics Explorer
- Hosts
- APM
- Services
- Traces
- Dependencies
- Uptime
- Uptime Monitors
- TLS Certificates

# Monitors BETA

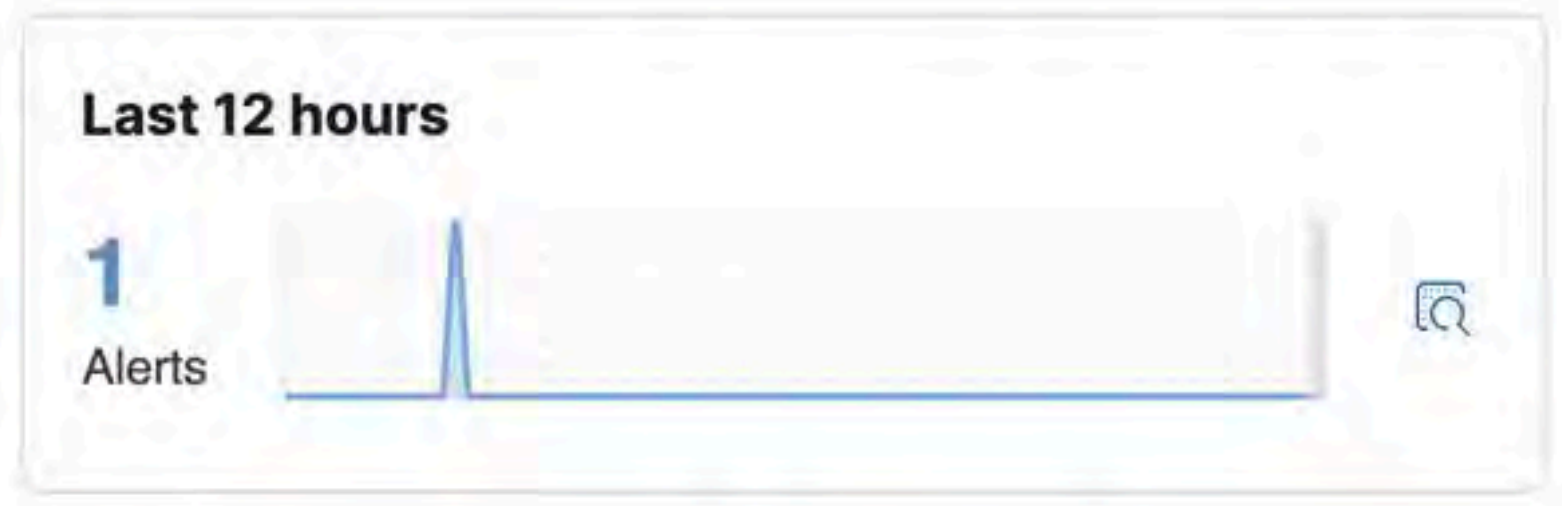
[+ Create Monitor](#) [Refresh](#)

[Overview](#) [Management](#)

Up Down Disabled Type 2 Location 1 Tags 0 Frequency 2 Project 1

### Current status

**3** Up   **0** Down   **0** Disabled



Showing 3 Monitors

Sort by Status Group by None



Showing all monitors



- Observability
- Overview
- Alerts
- Cases
- Logs
- Stream
- Anomalies
- Categories
- Infrastructure
- Inventory
- Metrics Explorer
- Hosts
- APM
- Services
- Traces
- Dependencies
- Uptime
- Uptime Monitors
- TLS Certificates

< Recorded Order journey

# Test run details

Location  
Europe - Unit

**Error running test**  
 error executing step: expect(received).toMatch(expected) Expected substring: "2" Received string: "3"

**Step 4 of 4** < Previous 4 / 4 Next >



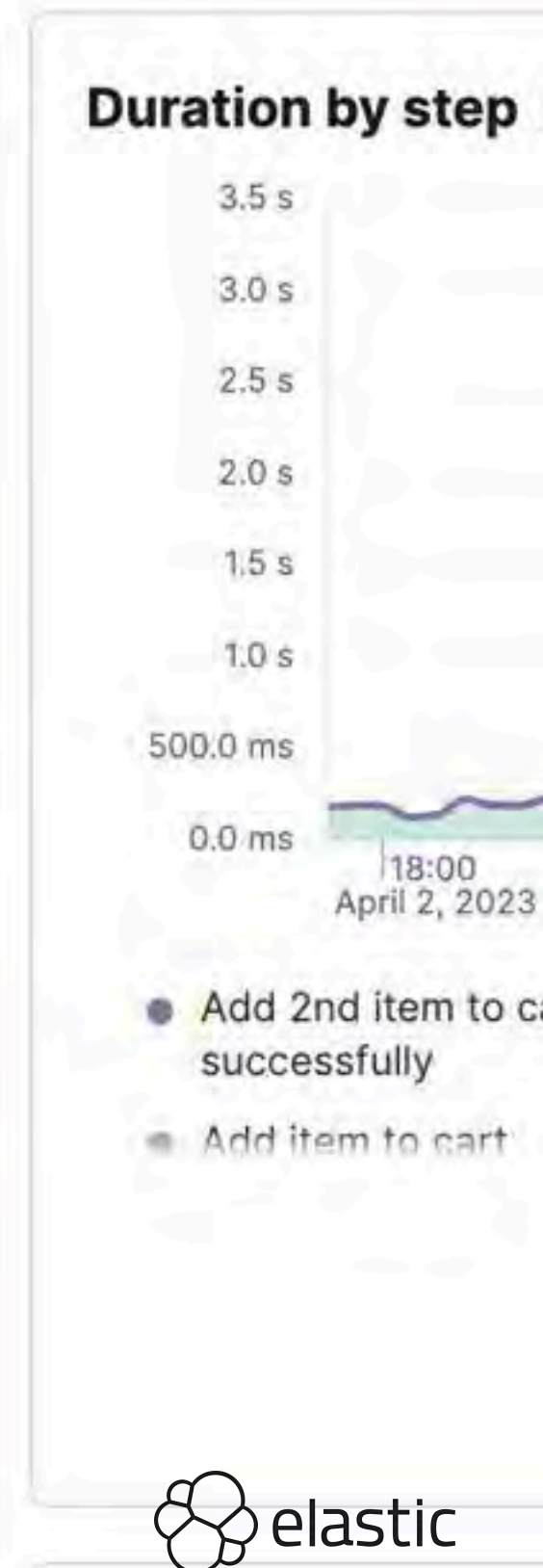
**Step name**  
 Add 3rd item to cart successfully  
**Failed** After 267 ms  
[View error details](#) [View performance breakdown](#)

**Stacktrace** **Code executed** **Console**

```

Error: expect(received).toMatch(expected)

Expected substring: "2"
Received string:    "3"
    at Step.callback (/tmp/elastic-synthetics-unzip-384981578/journeys/journeys/orders-generated.journey.ts:33:72)
    at Runner.runStep (/usr/share/heartbeat/.node/node/lib/node_modules/@elastic/synthetics/src/core/runner.ts:211:7)
    at Runner.runSteps (/usr/share/heartbeat/.node/node/lib/node_modules/@elastic/synthetics/src/core/runner.ts:261:16)
    at Runner.runJourney (/usr/share/heartbeat/.node/node/lib/node_modules/@elastic/synthetics/src/core/runner.ts:351:27)
    at Runner.run (/usr/share/heartbeat/.node/node/lib/node_modules/@elastic/synthetics/src/core/runner.ts:445:11)
    at Command.<anonymous> (/usr/share/heartbeat/.node/node/lib/node_modules/@elastic/synthetics/src/cli.ts:133:23)
  
```



### Observability

- Overview
- Alerts**
- Cases
- Logs
- Stream
- Anomalies
- Categories
- Infrastructure
- Inventory
- Metrics Explorer
- APM
- Services
- Traces
- Dependencies
- Service Map
- Uptime
- Monitors
- TLS Certificates
- User Experience
- Dashboard

# Rules

● Active: 0 ● Error: 0 ● Warning: 0 ● Ok: 2 ● Pending: 0 ● Unknown: 0

5 columns hidden 2 rules

<input type="checkbox"/>	Name ↑	Last run ⓘ	Notify ⓘ
<input type="checkbox"/>	<a href="#">monitors-alive-check</a> Uptime monitor status	Jan 25, 2023 17:07:00pm a few seconds ago	
<input type="checkbox"/>	<a href="#">Replicator Order Journey(Simple status alert)</a> Uptime monitor status	Jan 25, 2023 17:06:12pm a minute ago	

Rows per page: 10

## Edit rule

Name:

Tags (optional):

Check every ⓘ:

Notify ⓘ:

### Uptime monitor status

Alert when a monitor is down or an availability threshold is breached. [Learn more](#)

ⓘ This alert will apply to approximately 2 monitors.

+ Add filter

Status check

ANY MONITOR IS DOWN > 5 times

WITHIN last 15 minutes

Availability

ANY MONITOR IS UP IN < 99% of checks

WITHIN THE LAST 30 days

### Actions

> Elastic-Cloud-SMTP (preconfigured) Uptime Down Monitor

“**Visibility**... means the organization has a solid monitoring system in place to measure the heartbeat of the operation, **send alerts**, increase awareness of changes and cyberattacks as they occur, and provide accountability during the whole project lifecycle.”

–IBM, WHAT IS DEVSECOPS?

“**Visibility**... means the organization has a solid monitoring system in place to measure the heartbeat of the operation, send alerts, **increase awareness of changes and cyberattacks as they occur**, and provide accountability during the whole project lifecycle.”

–IBM, WHAT IS DEVSECOPS?

SIEM



Data sources ▾

### Recent cases



No cases have been created yet. Put your detective hat on and [start a new case!](#)

[View all cases](#)

### Recent timelines



You haven't favorited any timelines yet. Get out there and start threat hunting!

[View all timelines](#)

### Security news

#### Bringing home the beacon (from Cobalt Strike)



2022-01-25

Elastic Security engineers have documented a less tedious way to find network beaconing from Cobalt Strike.

#### Operation Bleeding Bear



2022-01-21

Elastic Security verifies new destructive malware targeting Ukraine; Operation Bleeding Bear.

#### Elastic Security uncovers BLISTER malware campaign



2021-12-22

Elastic Security has uncovered and provided preventions for a stealthy malware campaign that leverages valid code signing certificates to evade detection.

## Detection alert trend

Stack by `signal.rule.name` ▾

[View alerts](#)



## External alert trend

Stack by `event.module` ▾

[View alerts](#)

Showing: 1 external alert

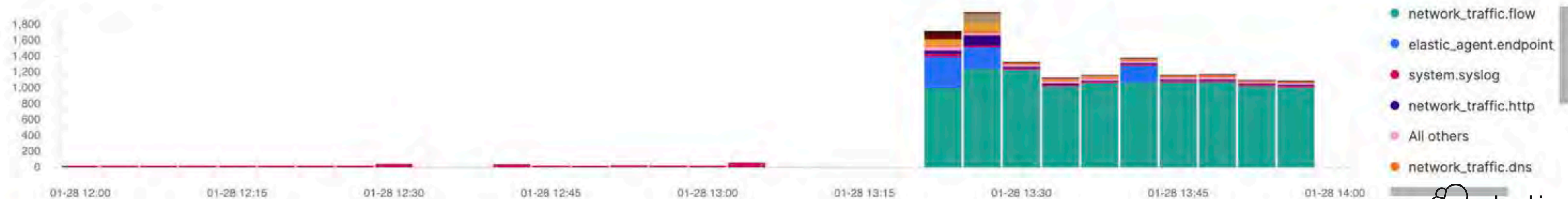


## Events

Stack by `event.dataset` ▾

[View events](#)

Showing: 13,693 events



DANKE!

THANK YOU!

MERCI!

GRAZIE!

GRACIAS!

DANK JE WEL!





**Infosecurity Europe**

20 - 22 June 2023, ExCeL London

# We're attending InfoSec Europe!

**20-22 June**  
**ExCel London**  
**Stand W55**



