© 2020 SPLUNK INC.

Splunk Observability Cloud

IT, 클라우드, 플랫폼, SRE, DevOps 팀을 위한 솔루션

Splunk Korea
이미정 매니저

splunk> turn data into doing™

© 2020 SPLUNK INC.

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. The forward-looking statements made in the this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, it may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements made herein.

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. Splunk undertakes no obligation either to develop the features or functionalities described or to include any such feature or functionality in a future release.

Splunk, Splunk>, Turn Data Into Doing, The Engine for Machine Data, Splunk Cloud, Splunk Light and SPL 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. © 2020 Splunk Inc. All rights reserved.

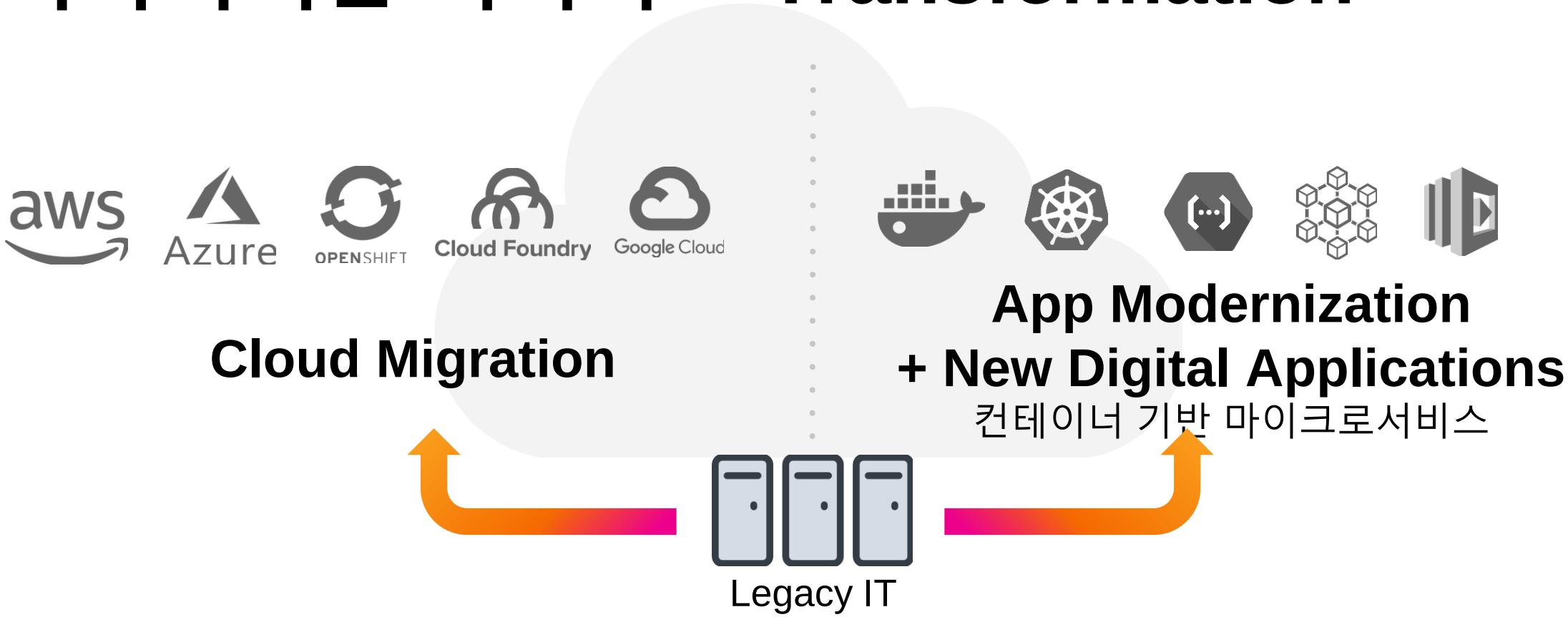
© 2020 SPLUNK INC.

What's Changed

splunk> turn data into doing™

© 2020 SPLUNK INC.

가속화되는 비지니스 Transformation



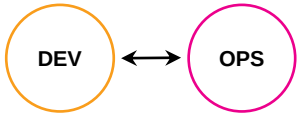
"2022년까지 전세계 조직의 75% 이상이 컨테이너화된 어플리케이션을 클라우드 환경에서의 운영에 적용할 것이다. 이는 지난해 30% 미만에서 크게 증가한 수치다." – Gartner, June 25, 2020

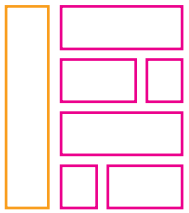
© 2020 SPLUNK INC.

Cloud Native 로의 전환 단계

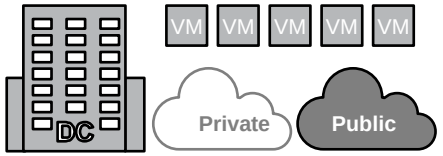
Organizations strive to increase velocity, agility and responsiveness

Lift & Shift

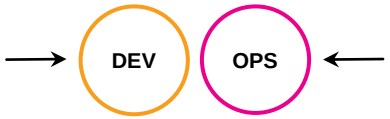




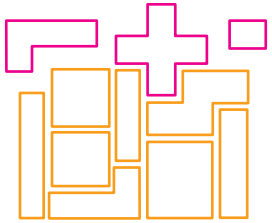
Primarily using
Cloud IaaS



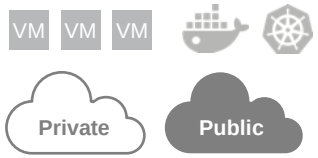
Re-Factor



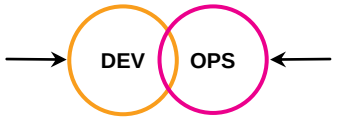
Cloud Managed e.g. RDS,
DynamoDB, SaaS



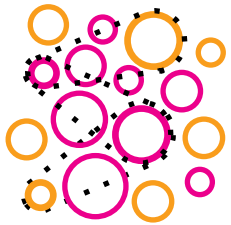
More Modular, but
Dependent App Components



Re-Architect / Cloud-Native



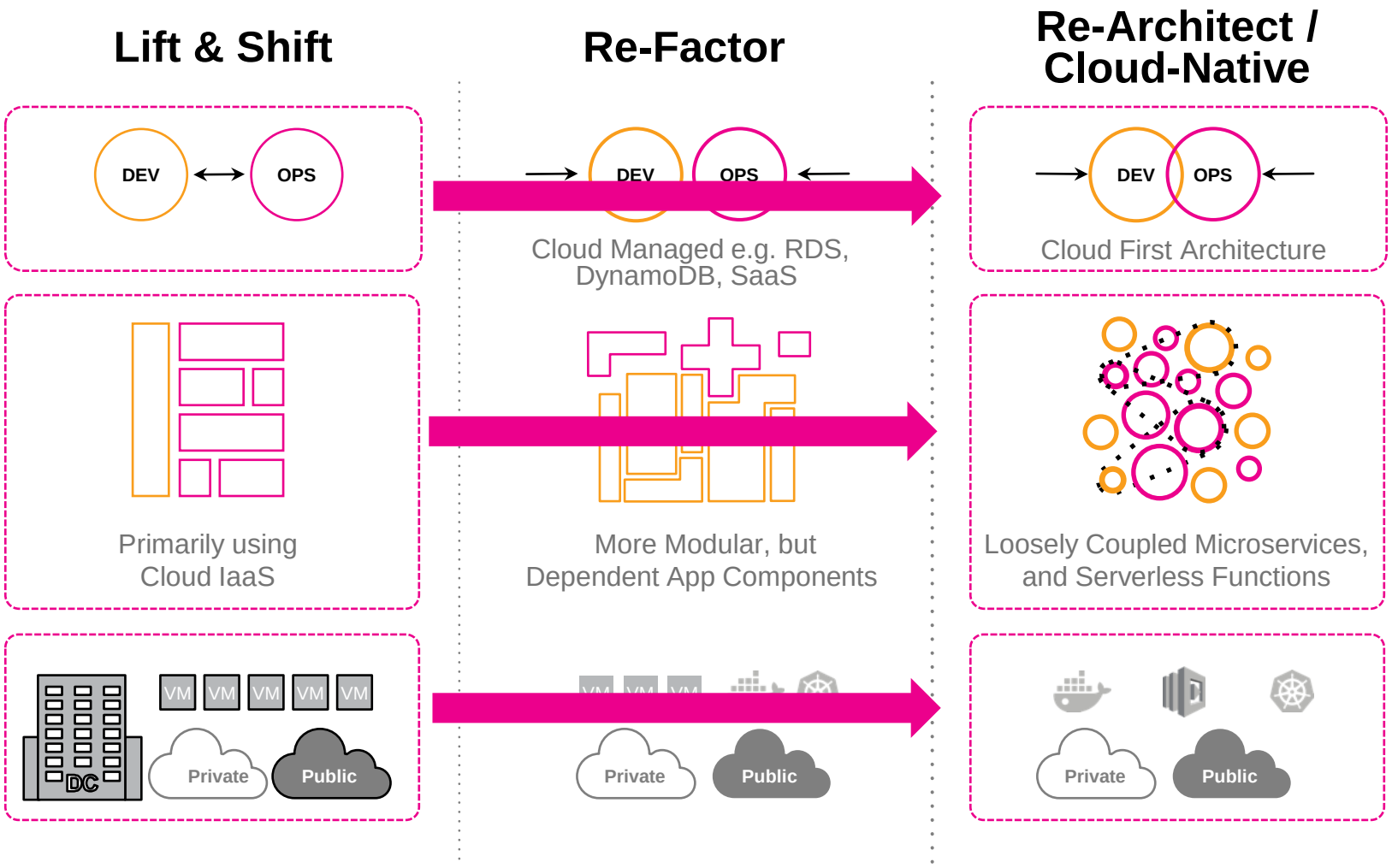
Cloud First Architecture



Loosely Coupled Microservices,
and Serverless Functions

© 2020 SPLUNK INC.

Cloud Native 와 모니터링 도전



DevOps

빈번한 코드 변경에 따른 더 많은 위험부담

Dev → Ops 까지 모니터링 영역 확장

Complex Dependencies

서비스 디펜던시가 높고 각자 다른 언어 기반

한 서비스가 미치는 영향 반경이 넓어짐

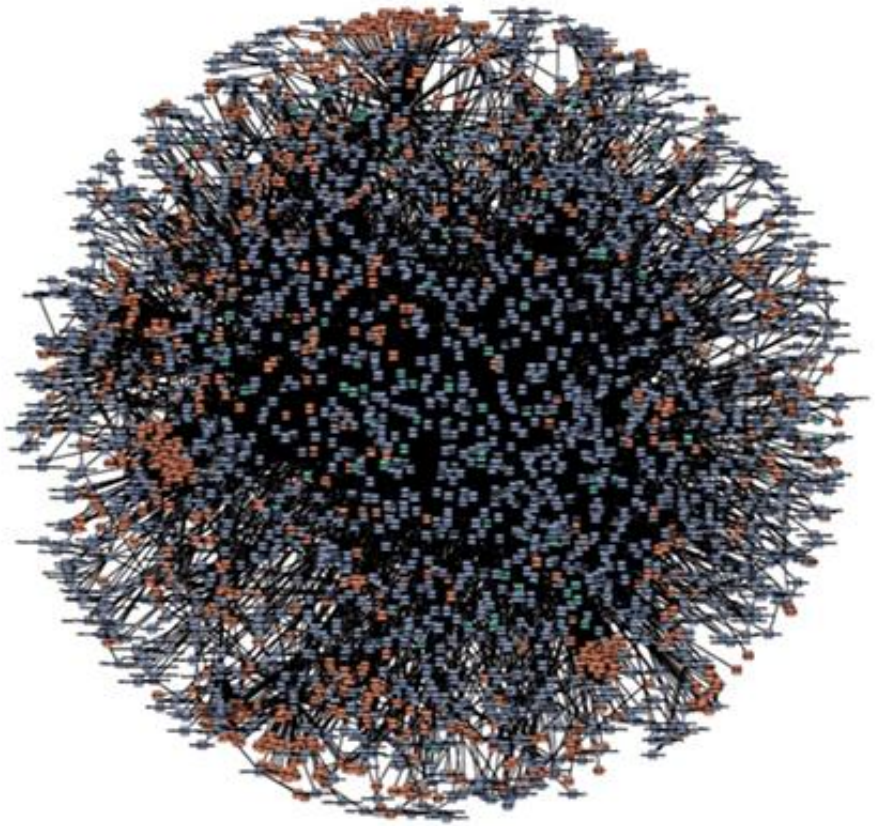
Elastic, Short-lived Infrastructure

추상화된 인프라, 동적인 멀티클라우드

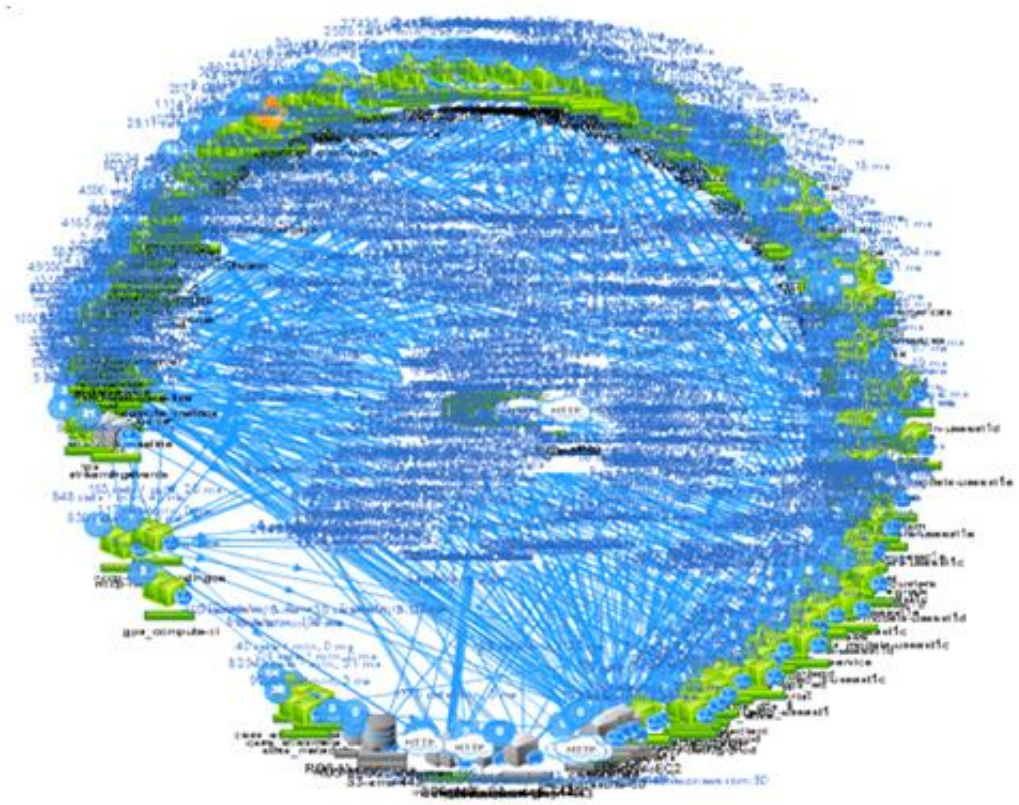
모니터링 항목과 대상 급증

© 2020 SPLUNK INC.

Cloud Native 에서의 복잡성 증가



amazon



NETFLIX

https://divante.com/blog/10-companies-that-implemented-the-microservice-architecture-and-paved-the-way-for-others/

© 2020 SPLUNK INC.

ttps://www.reportsanddata.com/report-
etail/cloud-monitoring-market

83% 의 운영조직은 클라우드의 복잡성 때문에 새로운 모니터링 방법을 찾고 있음

오직 11% 만이 현재 사용하는 모니터링 툴에 만족

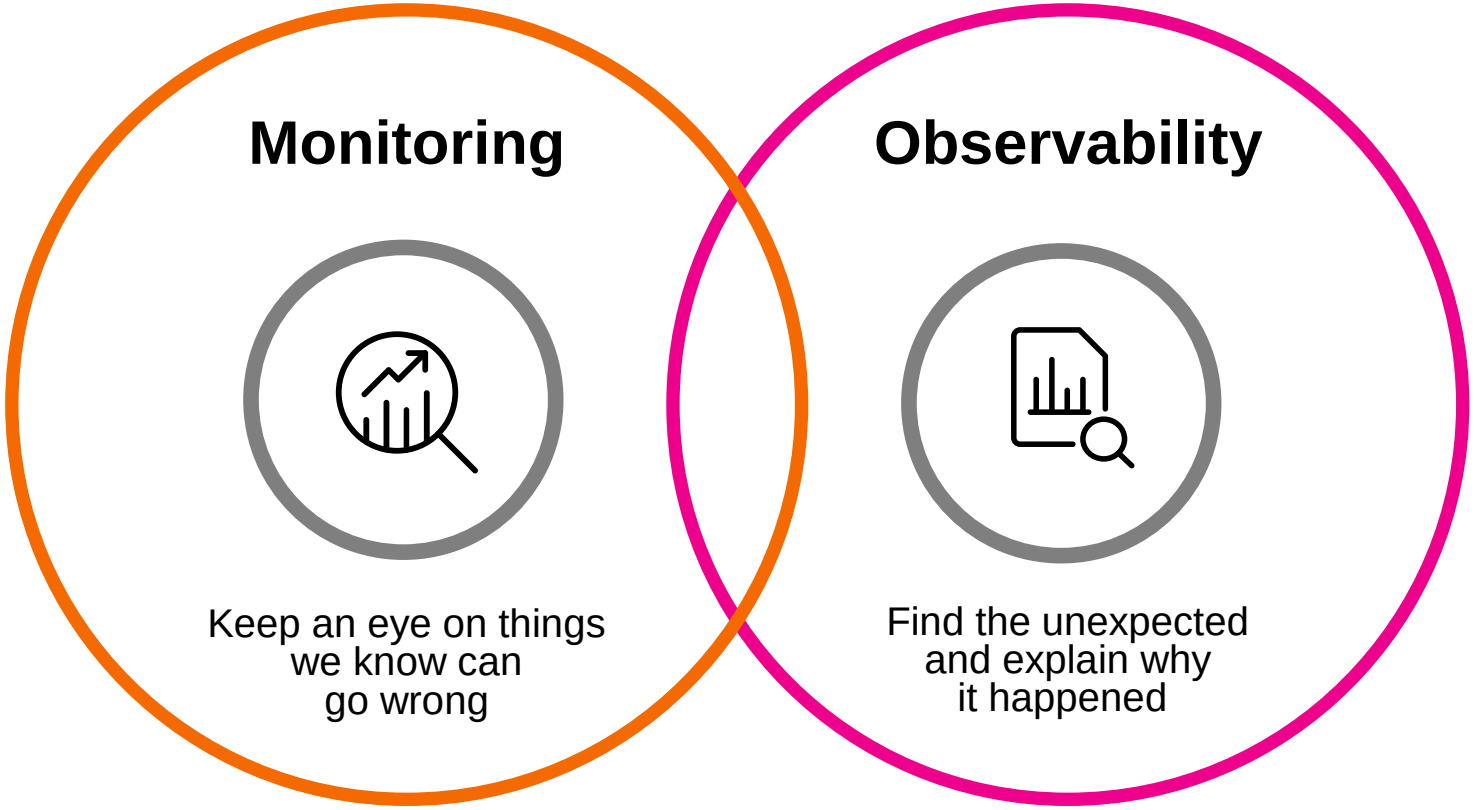
451 Research: IT Monitoring Meltdown, August 2020

splunk> turn data into doing™

© 2019 SPLUNK INC.

모니터링은 관측(Observability)으로 진화해야 합니다.

Observability 으로 unknown unknowns 을 빠르게 탐지, 조사, 해결!

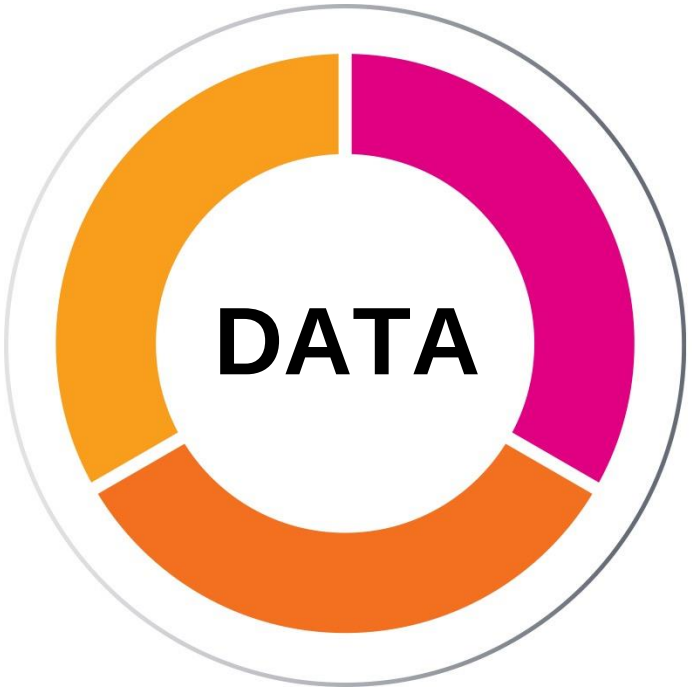


© 2020 SPLUNK INC.

Observability

뉴 노멀 새로운 모니터링 - 무엇이 필요한가?

- 모든 데이터 통합 저장
- 실시간 & 확장성
- 분석 & 머신러닝



- 고객 경험
- 제품 품질 및 출시 속도
- 개발자 효율
- 비지니스 도입

© 2020 SPLUNK INC.

How Splunk Can Help You

splunk> turn data into doing™

© 2020 SPLUNK INC.

Splunk Observability Cloud

문제를 해결하는 열쇠입니다.

시스템을 더 잘 관측할 수록 발생하는 문제에 더 빠르게 대처하고 더 빠르게 해결할 수 있습니다.

Full-Stack Visibility & Context-Rich Insights

splunk>

Metrics	Traces	Logs
문제가 있나?	어디가 문제인가?	왜 문제가 발생했나?
탐지	**트러블슈팅**	**근본원인**

splunk> turn data into doing™

© 2020 SPLUNK INC.

Splunk Observability Cloud

클라우드 네이티브 환경의 관측을 위한 통합 SaaS 서비스

Splunk APM

Splunk RUM

Splunk Infrastructure Monitoring

Splunk Log Observer

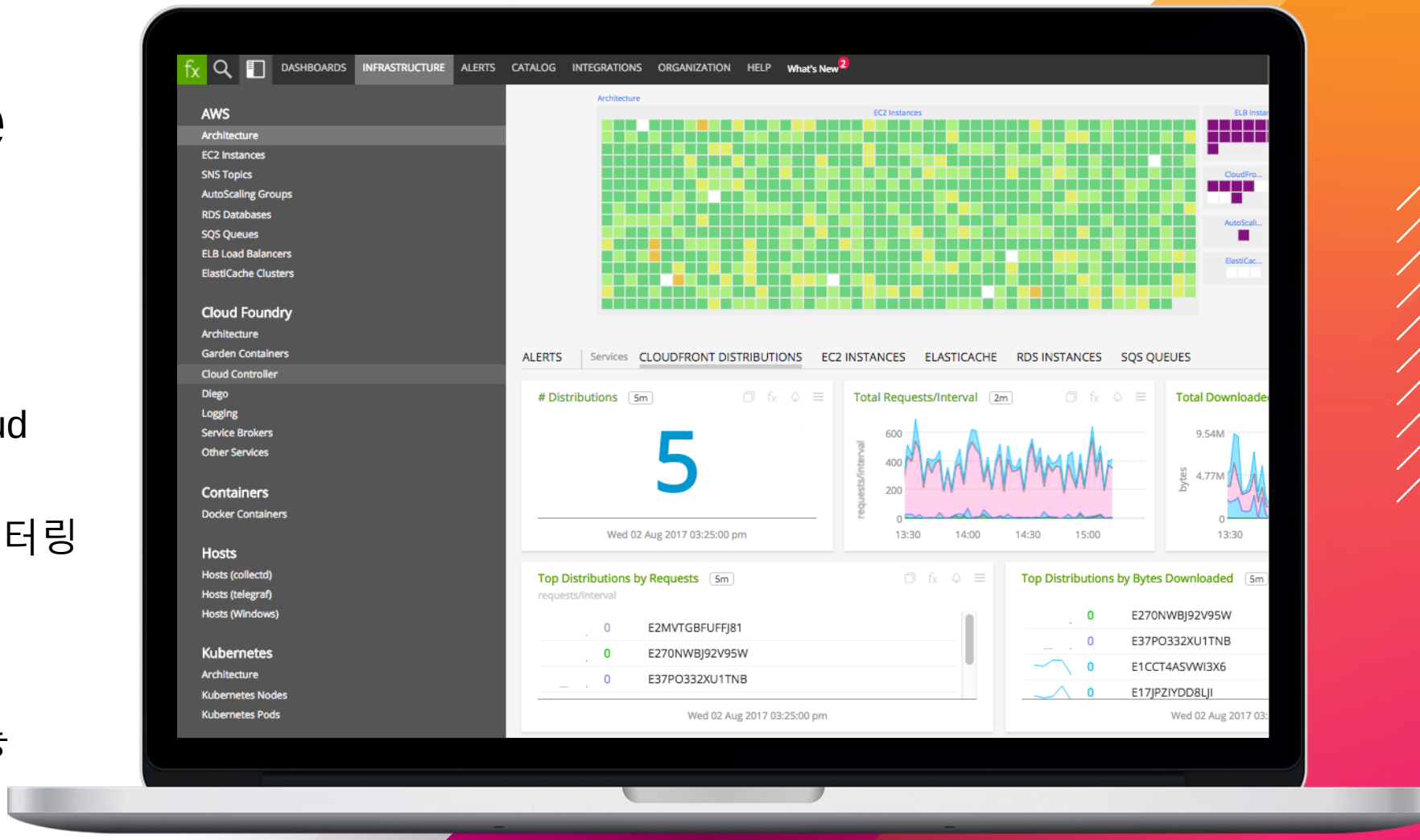
Splunk On-Call

splunk> turn data into doing™

Splunk Infrastructure Monitoring

실시간 스트리밍 메트릭

- On-prem & hybrid-/multi-cloud 모니터링
- Kubernetes & 컨테이너 모니터링
- Serverless 모티너링
- 200여개 빌트인 대시보드
- 서비스 자동 디스커버리 기능
- 간편한 스마트 경보 생성
- 1초 단위 커스텀 & 고해상도 메트릭 수집 분석



splunk > turn data into doing

© 2020 SPLUNK INC.

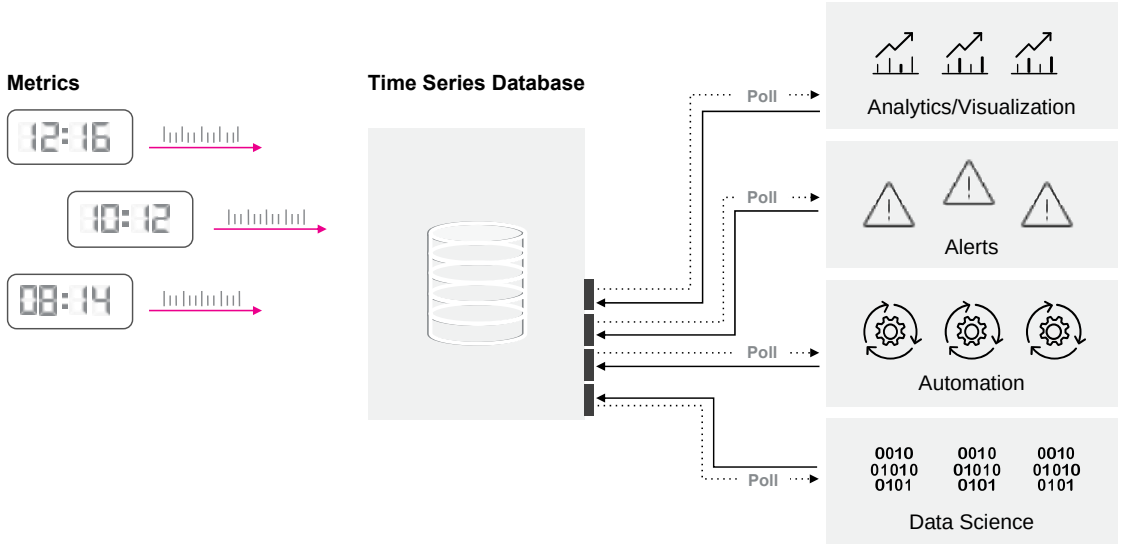
© 2020 SPLUNK INC.

수초내 인사이트를 가져오는 스트리밍 아키텍처

배치 메트릭 아키텍처가 갖는 낮은 확장성과 성능, 사일로 문제를 해결!

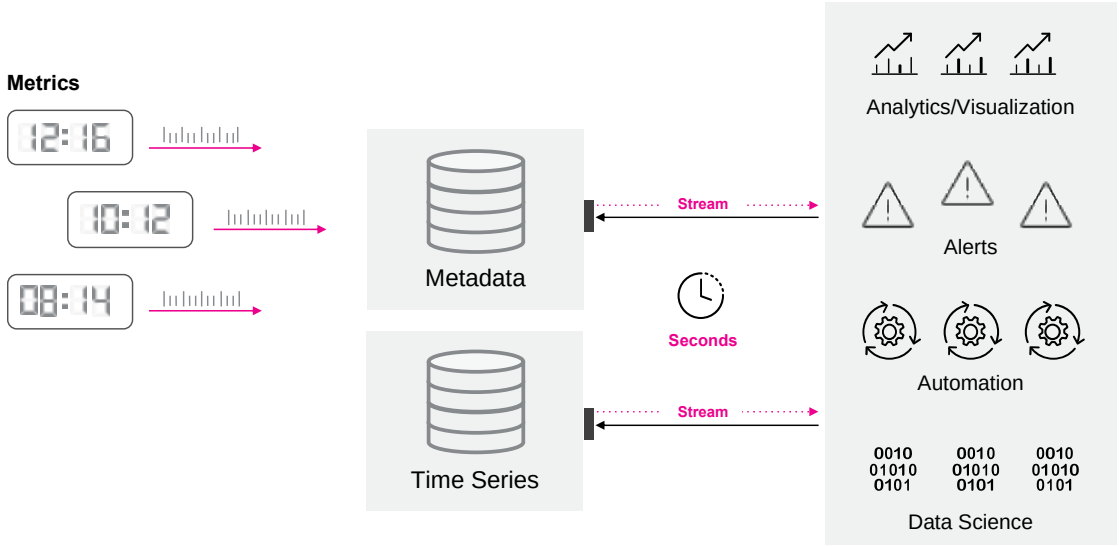
전통적 배치 아키텍처

→ 느린 대시보드, 알람



실시간 아키텍처

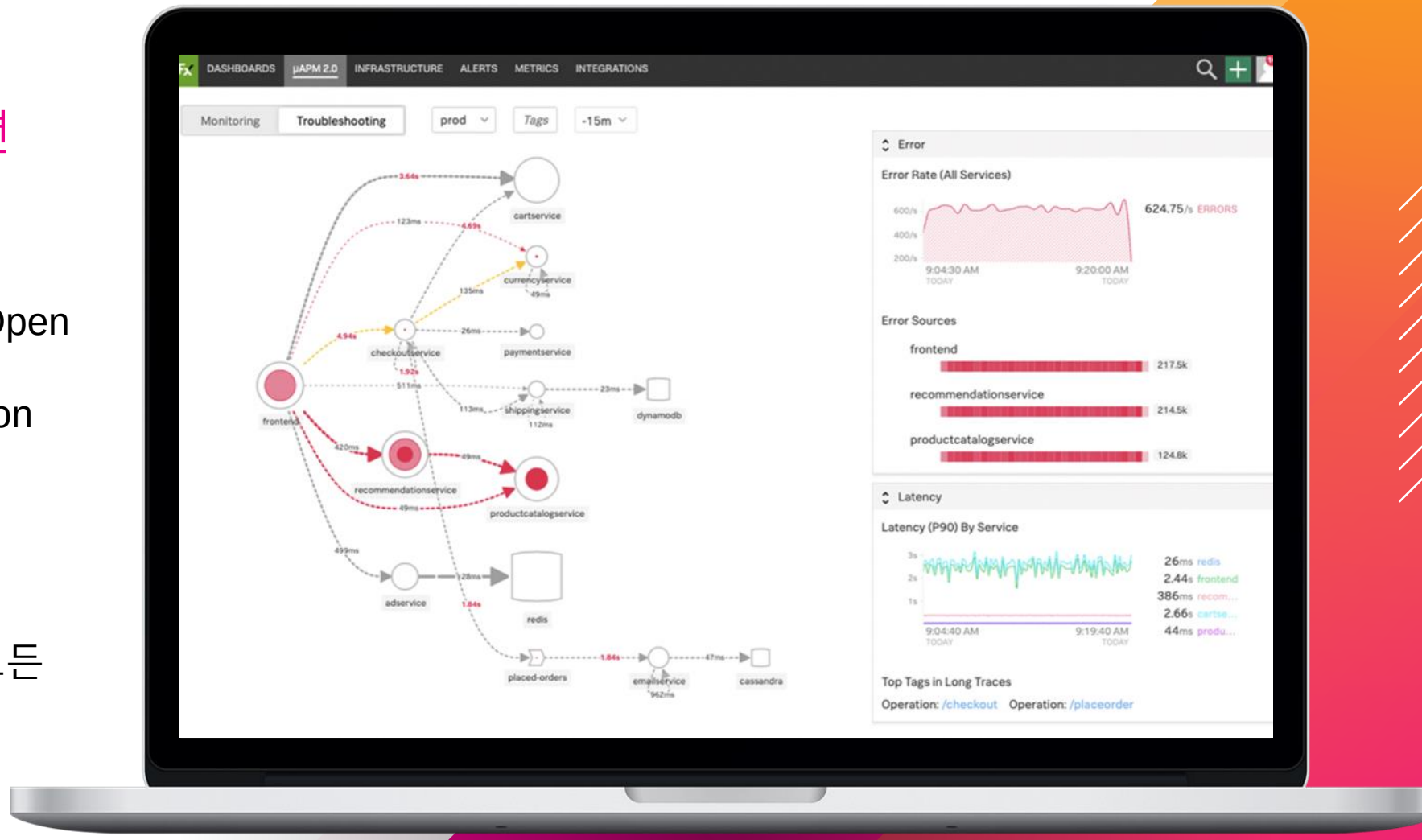
→ 빠른 대시보드, 알람 확인!



Splunk APM

End-to-End 어플리케이션 모니터링 및 트러블슈팅

- CNCF 분산 트레이싱 표준 Open Telemetry 를 통한 벤더 중립적인 경량 instrumentation
- Full-stack 상관분석
- NoSample™ full-fidelity 트레이싱
- 무제한 카디널러티 분석 – 모든 Tag/Dimension 분석 (UserName, TransactionID, Geography, etc.)
- 직관적 UI 를 통한 빠른 문제 파악



© 2020 SPLUNK INC.

splunk> turn data into doing

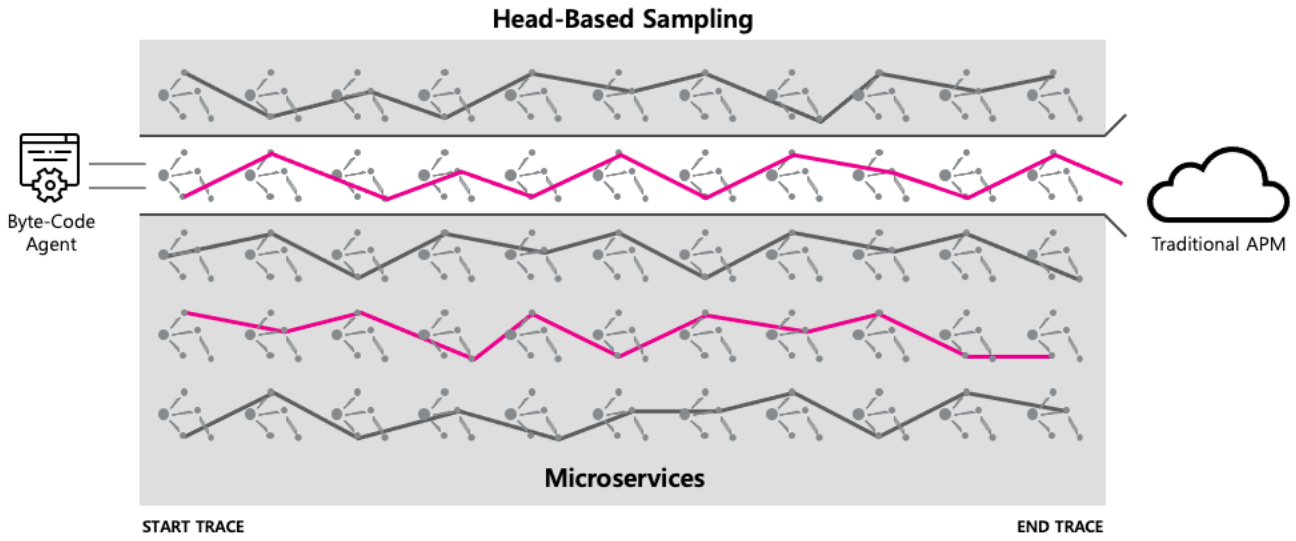
© 2020 SPLUNK INC.

NoSample™ full-fidelity 분산 트레이싱

배치 메트릭 아키텍처가 갖는 낮은 확장성과 성능, 사일로 문제를 해결!

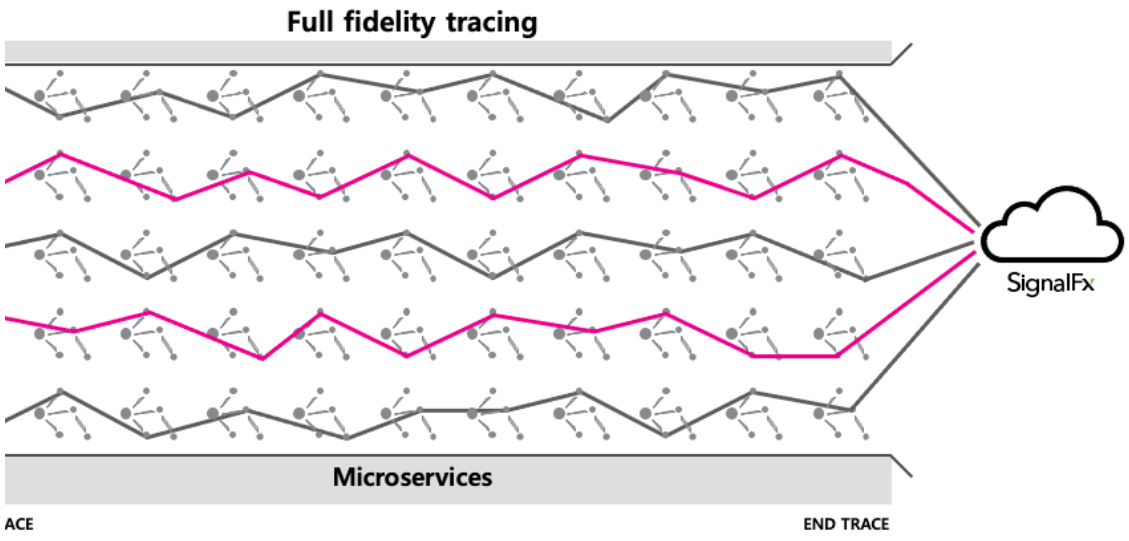
기존 APM 트레이스 방식

→ 문제가 있는 트레이스 누락



Splunk APM 트리이스 방식

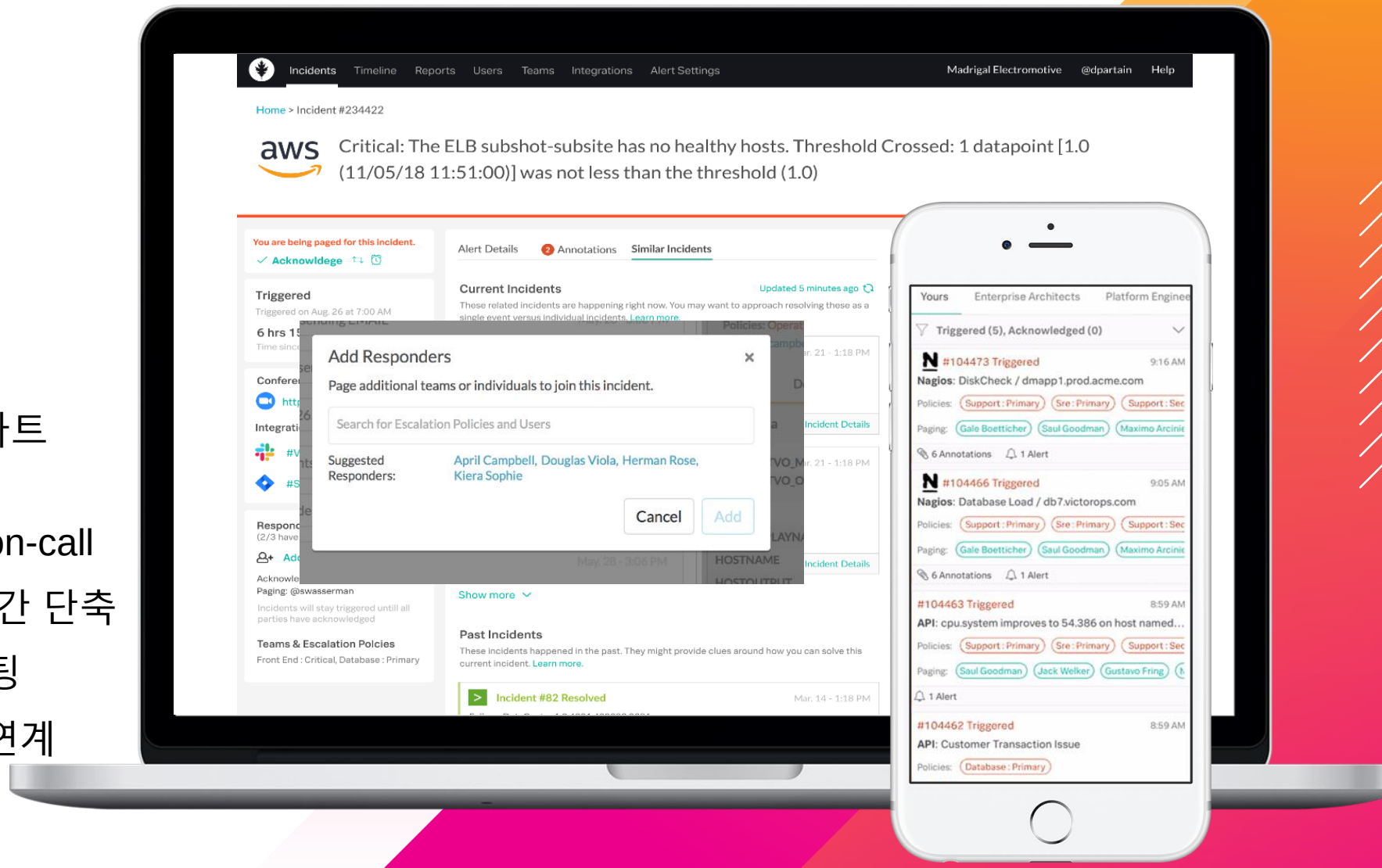
→ 모든 트레이스 수집!



Splunk On-Call

신속한 인시던트 응대와 효율적인 협업

- 인시던트를 담당자에게 스마트 라우팅
- 이해관계자에게 Intelligent on-call
- 알람 노이즈 제거 및 응대시간 단축
- 인시던트 사후 분석과 리포팅
- Okta, JIRA, MS Teams 등 연계
- 강화된 Mobile 지원



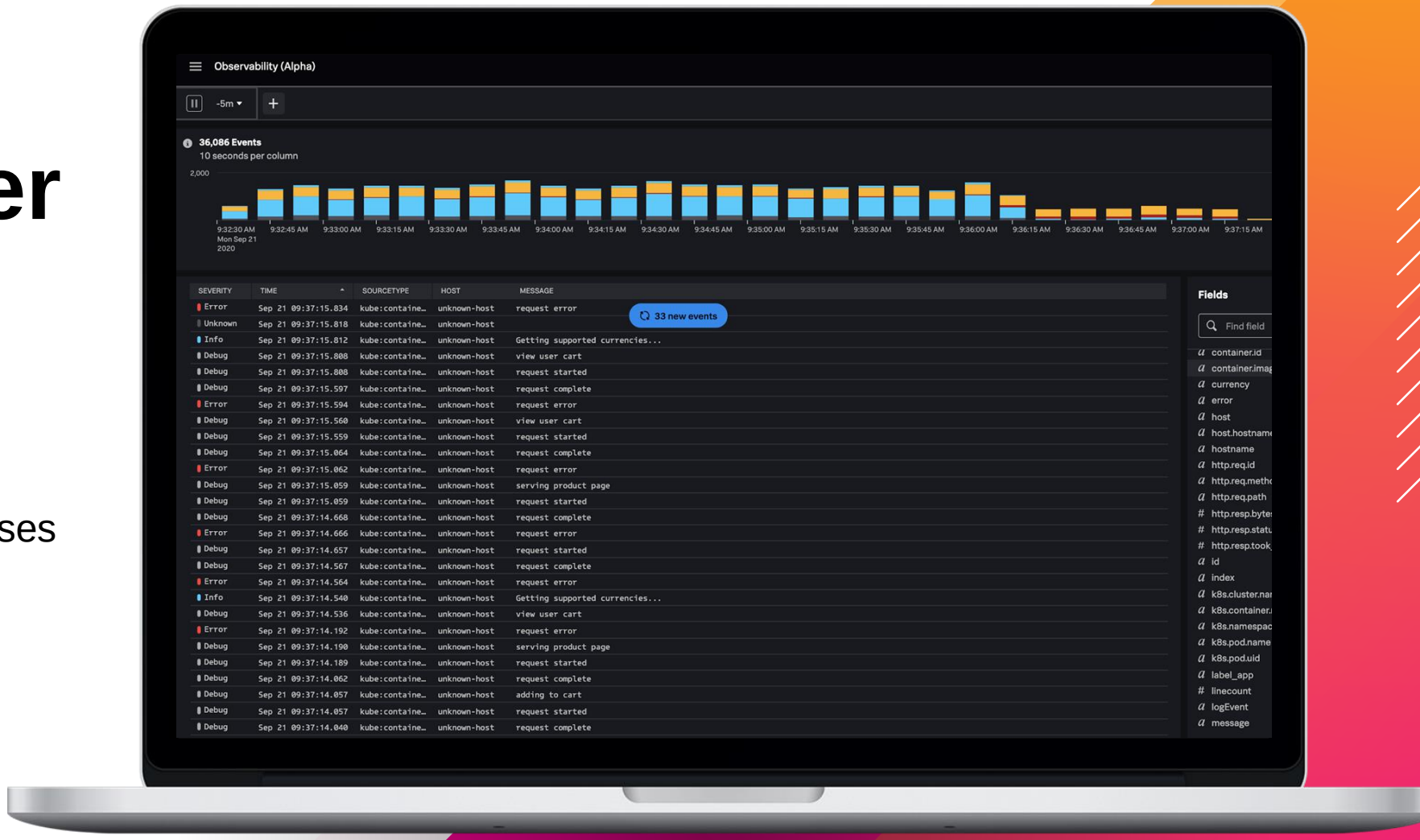
splunk> turn data into doing

© 2020 SPLUNK INC.

Splunk Log Observer

DevOps 를 위한 간편한 로그 탐색 UI

- 빠른 시작, 빠른 트러블슈팅
- Designed for DevOps use cases
- Live Tail
- Powered by Splunk



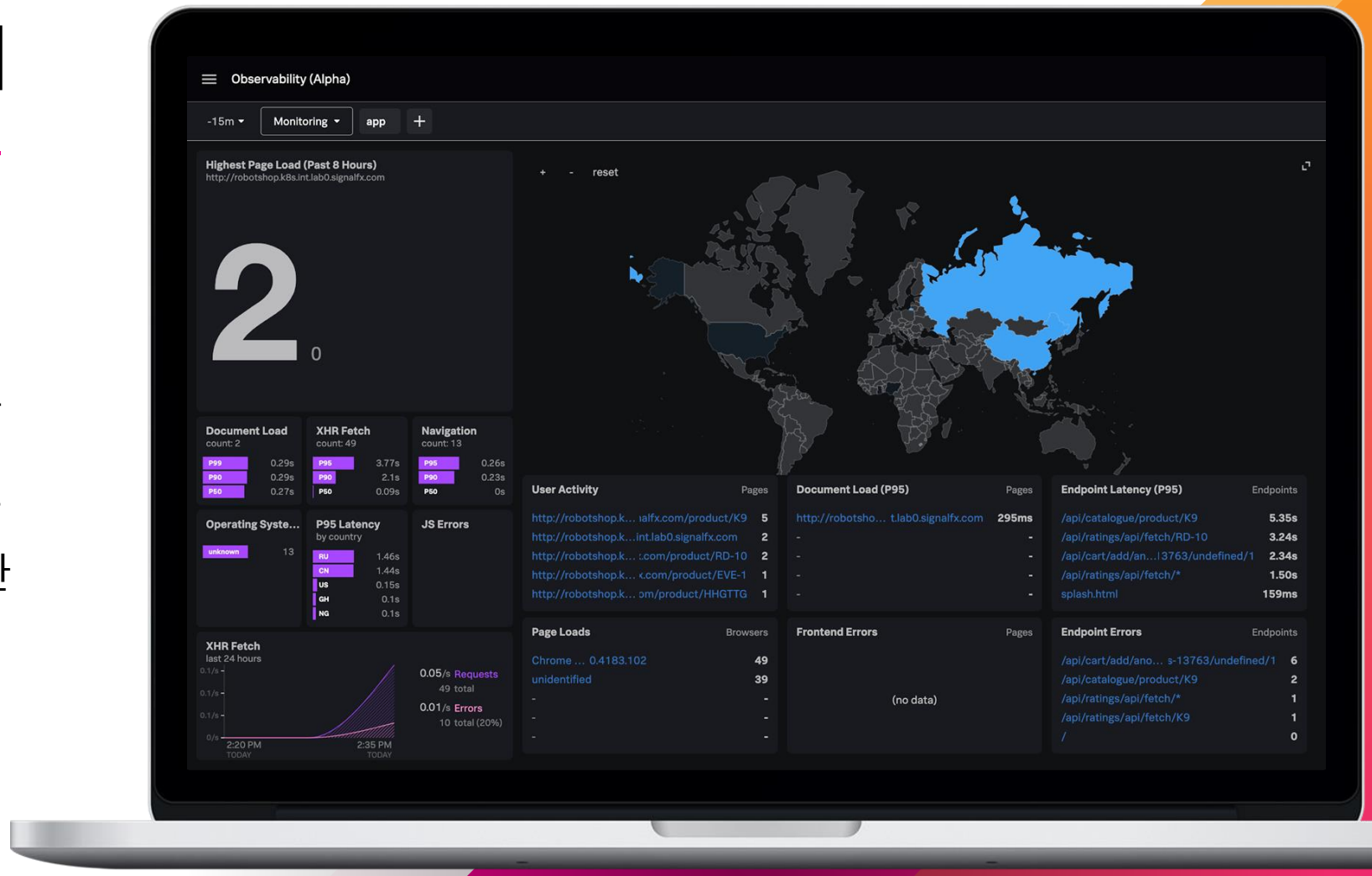
© 2020 SPLUNK INC.

splunk> turn data into doing

Splunk RUM

고객 경험에 대한 End-to-End, Full-Fidelity 가시성 확보

- Front-end 성능을 지속적으로 추적 모니터링
- 실시간으로 사용자 경험 평가
- 빠른 문제 해결을 위한 간편한 트러블슈팅
- 표준 방식으로 사용자 데이터 수집 및 활용



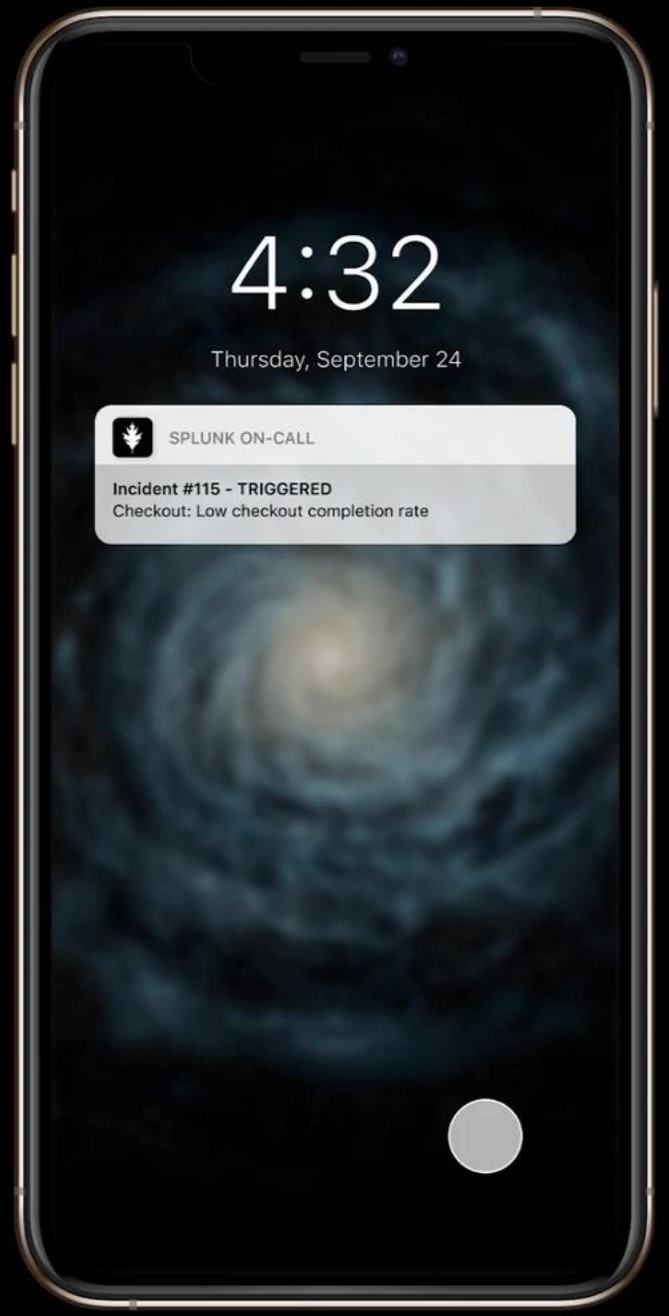
splunk > turn data into doing

© 2020 SPLUNK INC.

© 2020 SPLUNK INC.

Demo

splunk> turn data into doing™


4:32
Thursday, September 24
SPLUNK ON-CALL
Incident #115 - TRIGGERED
Checkout: Low checkout completion rate

Observability

-15m | Monitoring | app | +

Highest Page Load Last 8 Hours (P90)
http://demo.o11y.k8s.int.lab0.signalfx.com/cart

804ms ↓ -804ms

User Behavior

Page Loads	558	↑ +558

Front End Application

P95 Page Load	1.62s	↑ +1.62s
Console Errors	3	↑ +3

Backend Endpoints

P95 Latency	44.63s	↑ +44.63s
Errors	0	

+ - reset

Alerts

2 ↑ 2

P95 Latency
by country

BR	53.53s
US	905ms
JP	814ms
CA	553ms

User Activity — Pages

http://demo.o11y.k8... .lab0.signalfx.com/cart	3
http://demo.o11y.... int.lab0.signalfx.com	2
http://demo.o11y.k8s.int.l...signalfx.com/cart/checkout	2
http://demo.o11y.k8s.int.l...om/product/66VCHSJNUP	2
http://demo.o11y.k8s.int.l...m/product/1YMWWN1N4O	1

Document Load (P95) — Pages

http://demo.o11y.k8s.i... gnalfx.com/cart/checkout	1.72s
http://demo.o11y.k8s.i... m/product/66VCHSJNUP	1.03s
http://demo.o11y.k8... .lab0.signalfx.com/cart	870ms
http://demo.o11y.... int.lab0.signalfx.com	727ms
http://demo.o11y.k8s.i...product/1YMWWN1N4O	635ms

Endpoint Latency (P95) — Endpoints

/cart/checkout	53.53s
/	1.39s
/cart	510ms
-	-
-	-

Page Loads — Browsers

unidentified	554
Chrome ... 0.4183.102	4
-	-
-	-
-	-

Frontend Errors — Pages

http://demo.o11y.k8... .lab0.signalfx.com/cart	3
-	-
-	-
-	-
-	-

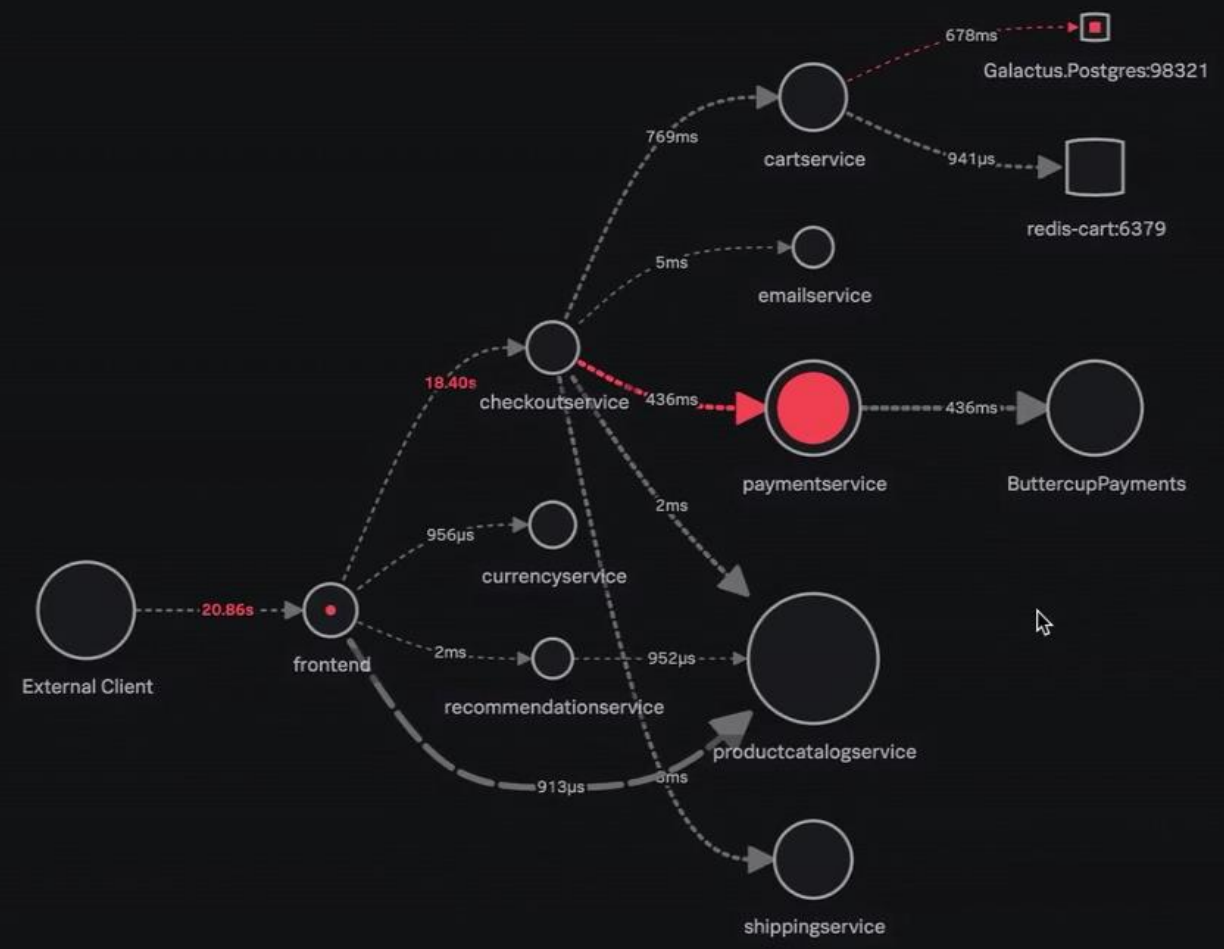
Endpoint Errors — Endpoints

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

Observability

-15m | All | frontend:/cart/che... | Services | Tags | Clear All

Monitoring | Troubleshooting



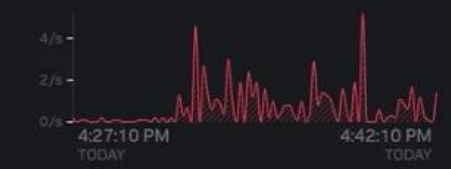
Show Traces | Show Legend

Business Workflow

frontend:/cart/checkout

Error

Error Rate (All Services)



0.67/s Errors

Error Sources

paymentservice 537

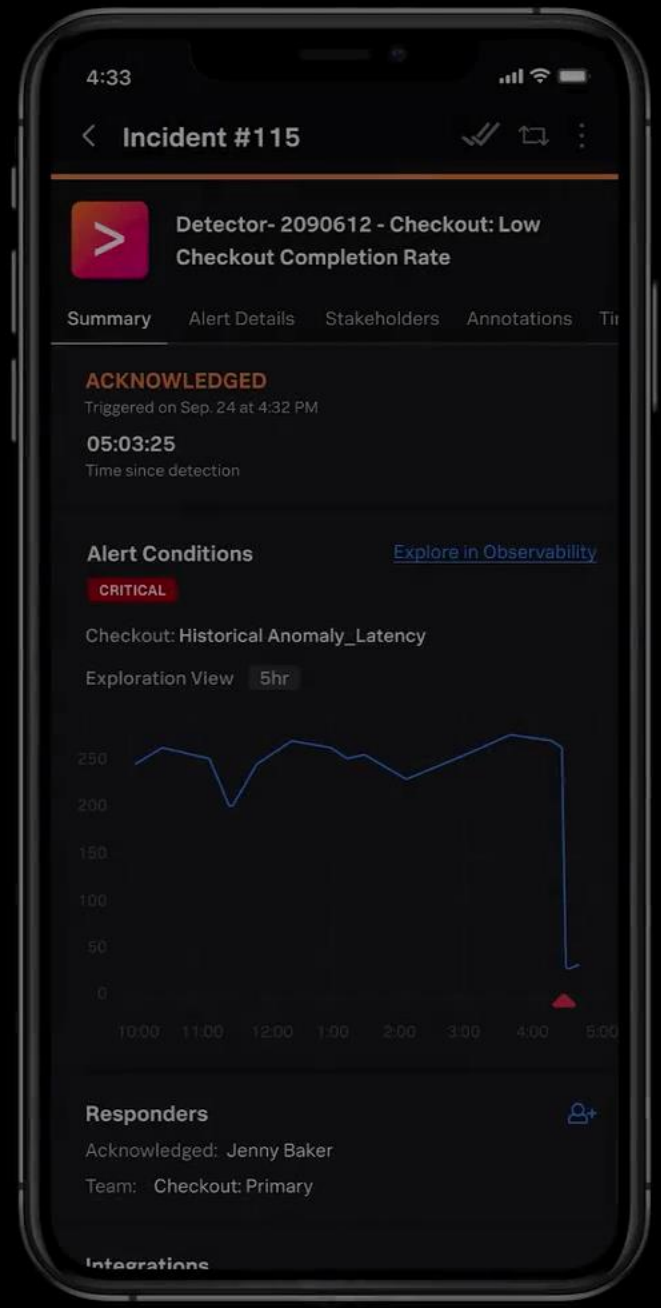
Latency

Latency (P90) By Service

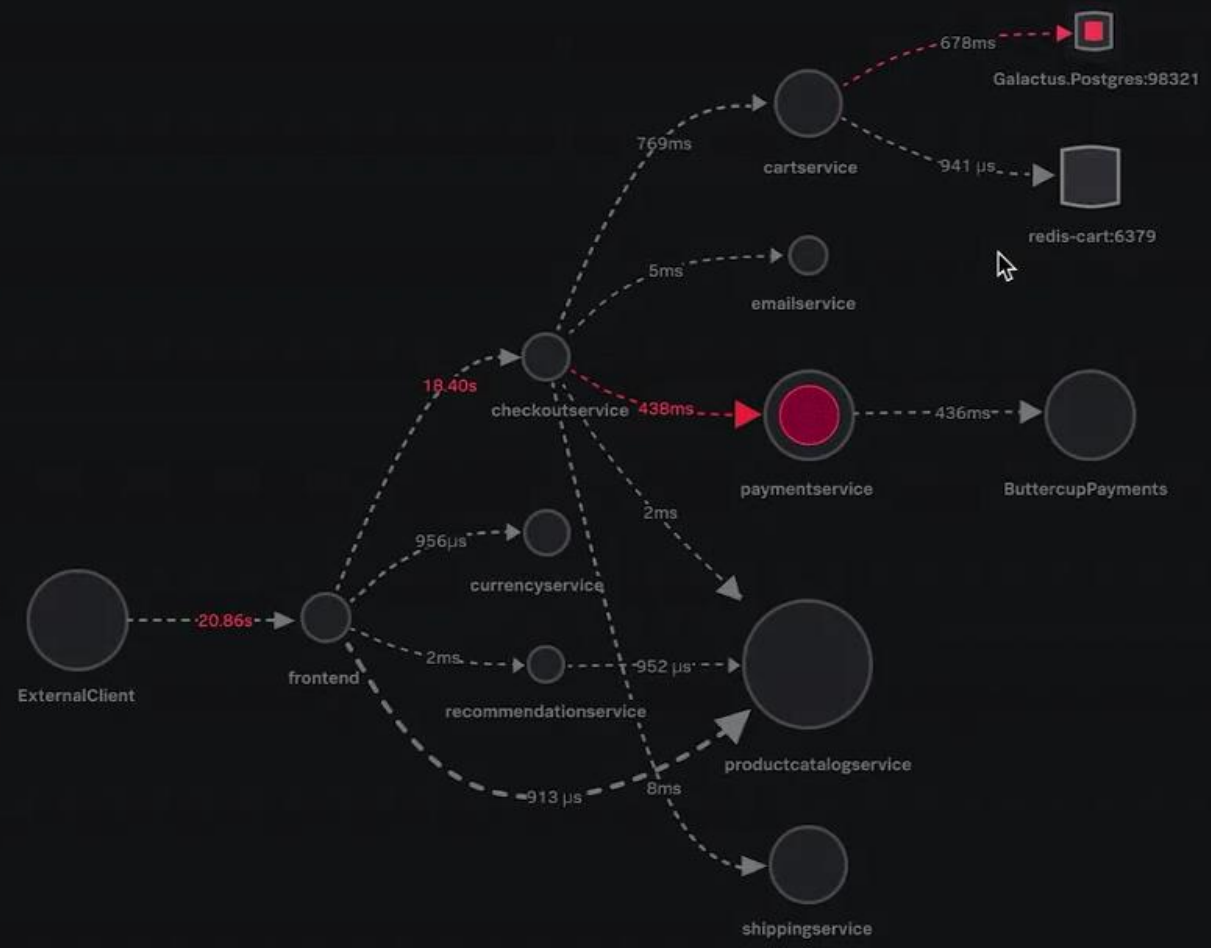
345µs productcat...
436ms Buttercup...
437ms paymentse...
661µs shippingse...
934µs cartservice

Top High-Latency Tags | Tag Spotlight

HTTP Method: POST Environment: production


4:33
Incident #115
Detector- 2090612 - Checkout: Low Checkout Completion Rate
Summary
Alert Details
Stakeholders
Annotations
ACKNOWLEDGED
Triggered on Sep. 24 at 4:32 PM
05:03:25
Time since detection
Alert Conditions
Explore in Observability
CRITICAL
Checkout: Historical Anomaly_Latency
Exploration View
5hr
250
200
150
100
50
0
10:00
11:00
12:00
1:00
2:00
3:00
4:00
5:00
Responders
Acknowledged: Jenny Baker
Team: Checkout: Primary

Monitoring | Troubleshooting



Business Workflow

frontend:/cart/checkout

Error

Error Rate (All Services)

0.67/s Errors

Error Sources

paymentservice 5

Latency

Latency (P90) By Service

345µs productcat...
436ms shippingse...
437ms Buttercup...
661µs Paymentse...
934µs cartservice

Top High-Latency Tags — Tag Spotlight

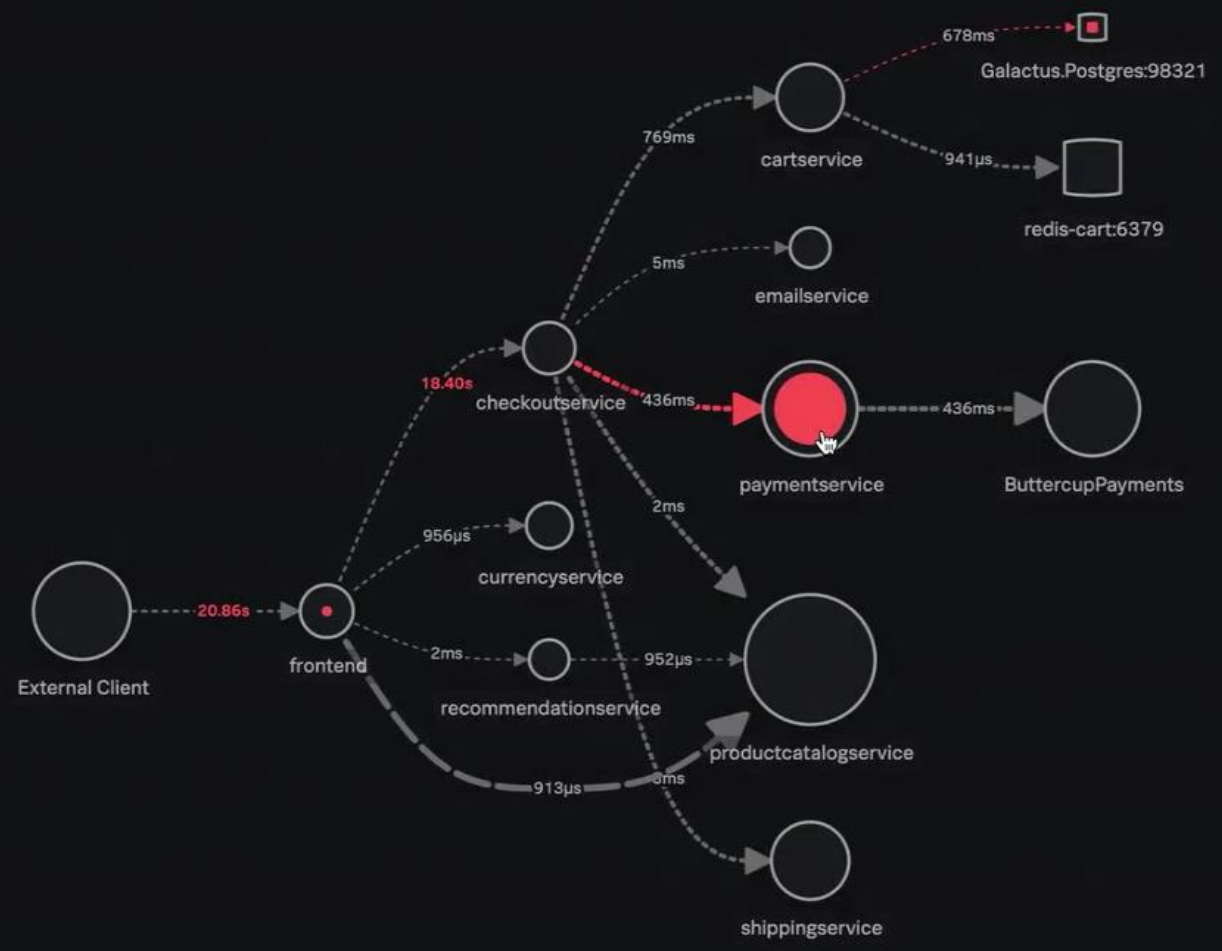
HTTP Method: POST Environment: production

Show Traces Show Legend

Observability

-15m | All | frontend:/cart/che... | Services | Tags | Clear All

Monitoring | Troubleshooting



Show Traces | Show Legend

Business Workflow

frontend:/cart/checkout

Error

Error Rate (All Services)

0.67/s Errors

Error Sources

paymentservice 537

Latency

Latency (P90) By Service

345µs productcat...
436ms Buttercup...
437ms paymentse...
661µs shippingse...
934µs cartservice

Top High-Latency Tags | Tag Spotlight

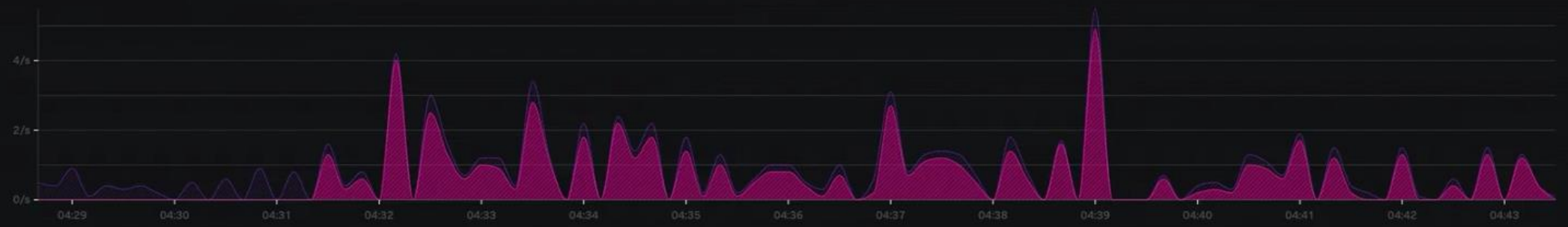
HTTP Method: POST Environment: production

Observability

-15m | All | frontend:/cart/che... | Services | Tags | Clear All

Monitoring | Troubleshooting

Tag Spotlight | Service: paymentservice | Requests/Errors | Latency



Requests 753
Errors (Root) 570 (570)

Endpoint

	Req	Err	Root
grpc.hipstershop.PaymentService/Charge	753	570	570

Environment

	Req	Err	Root
production	632	570	570
development	61	0	0
staging	60	0	0

HTTP Method

No Matched Values

Kind

	Req	Err	Root
SERVER	753	570	570

Operation

	Req	Err	Root
grpc.hipstershop.PaymentService/Charge	753	570	570

tenant.level

	Req	Err	Root
silver	282	215	215
bronze	241	181	181
gold	230	174	174

version

	Req	Err	Root
v350.10	570	570	570
v350.9	183	0	0

Workflow

	Req	Err	Root
frontend:/cart/checkout	753	570	570

Observability

-15m

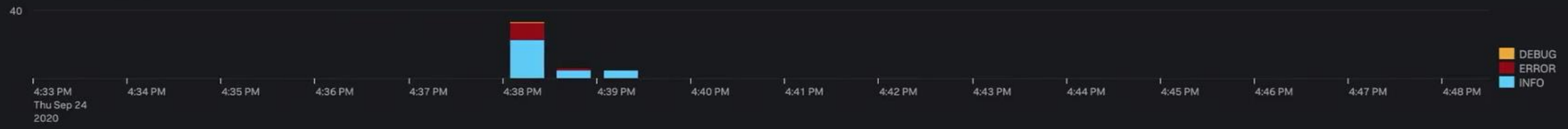
trace_id = 24685589db624f25

Clear All

45 Events

30 seconds per column

Visual Analysis



SEVERITY	TIME	SOURCETYPE	HOST	MESSAGE
Info	Sep 24 16:39:03.238	kube:containe…	ip-10-4-100-1…	order placed
Info	Sep 24 16:39:03.190	kube:containe…	ip-10-4-100-1…	[ShipOrder] completed request
Info	Sep 24 16:39:03.190	kube:containe…	ip-10-4-100-1…	[ShipOrder] received request
Info	Sep 24 16:39:03.168	kube:containe…	ip-10-4-100-1…	Transaction processed
Info	Sep 24 16:39:02.244	kube:containe…	ip-10-4-100-1…	PaymentService#Charge invoked with request {"amount":{"currency_code":"CAD","units":"3356","nanos":127731090},"credit_c…
Info	Sep 24 16:38:56.717	kube:containe…	ip-10-4-100-1…	payment went through (transaction_id: 36ea4de1-e712-48ba-b221-f5cdb329a6b0)
Info	Sep 24 16:38:56.624	kube:containe…	ip-10-4-100-1…	Charging through ButtercupPayments
Info	Sep 24 16:38:56.072	kube:containe…	ip-10-4-100-1…	order confirmation email sent to "someone@example.com"
Info	Sep 24 16:38:39.164	kube:containe…	ip-10-4-100-1…	Charging through ButtercupPayments
Info	Sep 24 16:38:39.164	kube:containe…	ip-10-4-100-1…	PaymentService#Charge invoked with request {"amount":{"currency_code":"CAD","units":"3356","nanos":127731090},"credit_c…
Error	Sep 24 16:38:31.232	kube:containe…	ip-10-4-100-1…	Failed payment processing through ButtercupPayments: Invalid API Token (test-20e26e90-356b-432e-a2c6-956fc03f5609)
Info	Sep 24 16:38:24.506	kube:containe…	ip-10-4-100-1…	Charging through ButtercupPayments
Info	Sep 24 16:38:18.527	kube:containe…	ip-10-4-100-1…	Charging through ButtercupPayments
Info	Sep 24 16:38:18.527	kube:containe…	ip-10-4-100-1…	PaymentService#Charge invoked with request {"amount":{"currency_code":"CAD","units":"3356","nanos":127731090},"credit_c…
Error	Sep 24 16:38:18.115	kube:containe…	ip-10-4-100-1…	Failed payment processing through ButtercupPayments: Invalid API Token (test-20e26e90-356b-432e-a2c6-956fc03f5609)
Info	Sep 24 16:38:17.750	kube:containe…	ip-10-4-100-1…	PaymentService#Charge invoked with request {"amount":{"currency_code":"CAD","units":"3356","nanos":127731090},"credit_c…
Error	Sep 24 16:38:14.493	kube:containe…	ip-10-4-100-1…	Failed payment processing through ButtercupPayments: Invalid API Token (test-20e26e90-356b-432e-a2c6-956fc03f5609)
Error	Sep 24 16:38:12.840	kube:containe…	ip-10-4-100-1…	Failed payment processing through ButtercupPayments: Invalid API Token (test-20e26e90-356b-432e-a2c6-956fc03f5609)
Error	Sep 24 16:38:12.749	kube:containe…	ip-10-4-100-1…	Failed payment processing through ButtercupPayments: Invalid API Token (test-20e26e90-356b-432e-a2c6-956fc03f5609)
Info	Sep 24 16:38:11.762	kube:containe…	ip-10-4-100-1…	Charging through ButtercupPayments
Info	Sep 24 16:38:11.761	kube:containe…	ip-10-4-100-1…	PaymentService#Charge invoked with request {"amount":{"currency_code":"CAD","units":"3356","nanos":127731090},"credit_c…
Info	Sep 24 16:38:10.850	kube:containe…	ip-10-4-100-1…	Charging through ButtercupPayments
Info	Sep 24 16:38:10.850	kube:containe…	ip-10-4-100-1…	PaymentService#Charge invoked with request {"amount":{"currency_code":"CAD","units":"3356","nanos":127731090},"credit_c…
Info	Sep 24 16:38:09.039	kube:containe…	ip-10-4-100-1…	Charging through ButtercupPayments

Fields

Find field

amount.currency_code	1
amount.nanos	1
amount.units	1
cardNumberEnding	1
cardType	1
container.id	45
container.image.name	45
host	45
host.hostname	45
hostname	36
http.req.id	2
http.req.method	2
http.req.path	2
index	45
k8s.cluster.name	45
k8s.container.name	45
k8s.namespace.name	45
k8s.pod.name	45
k8s.pod.uid	45
label_app	45

© 2020 SPLUNK INC.

업계 최고의 통합 Observability Cloud

모니터링, 트러블슈팅, 조사, 해결을 위한 원활한 워크플로우

Infrastructure Monitoring	Application Performance Monitoring	Real User Monitoring
Log Observer	On-call	

NoSample™ Full-Fidelity	Real-Time Streaming	Massively Scalable	AI/ML-Driven Analytics

OpenTelemetry

Logs | Metrics | Traces

© 2020 SPLUNK INC.

Use Case Examples

splunk> turn data into doing™

© 2020 SPLUNK INC.

여러 산업 분야의 다양한 고객

FINANCIAL SERVICES	HIGH TECH	CONSUMER MEDIA / ENTERTAINMENT	TRAVEL / TRANSPORTATION	ONLINE SERVICES	HEALTHCARE / LIFE SCIENCES	RETAIL / eCOMMERCE
EllieMae	ATLASSIAN	EPIC GAMES	lyft	Drift	athenahealth	NIKE
Square	Carbon Black.	PLUTO TV	CLEAR	yelp	Care.com	THE WAREHOUSE GROUP
Plus500	CLOUDREACH	verizon	KAYAK	freecharge	thinkresearch	SCENTBIRD
vaultbank	Acquia	FLOSPORTS	Rappi	OLX GROUP	align	lululemon
Nasdaq	HubSpot	Spotify	AMTRAK	BIDMOTION	patientslikeme	maxeda
Avalara	Segment	NBCUniversal	nauto	movebubble	Benchling	Shutterfly
snap! finance	Mist	Rakuten VIKI	REVINATE	coffee meets bagel	SYNTHEGO	
Nav	Qubole	hudl		meet me		
	MARK43	Harvard Business Publishing		UrbanClap		
	Menlo Security	MOONACTIVE				
	(x) matters					
	Tapjoy					

© 2020 SPLUNK INC.

확장성이 뛰어난 Infrastructure Monitoring 과 APM 을 통한 빠른 성장

고객 딜리버리 스피드를 최적으로 유지하기 위한 실시간 가시성

- 콜럼비아에 HQ 를 둔 온디맨드 딜리버리 스타트업으로, 라틴아메리카에 약 6K 의 호스트를 운영중
- 커스텀 메트릭 모니터링과 Traefik 환경에 대한 가시성 확보를 위해 Splunk IM 을 도입. 이후 Splunk APM 을 통해 메트릭과 트레이스에 대한 실시간 통합 뷰 확보
  - Real-time monitoring significantly reduced the MTTR on production from five minutes to seconds
  - More complex data analytics + better metrics correlation
- Splunk o11y 를 통해 ECS, K8s, Lambda 등 마이크로서비스 기반 아키텍처로의 성공적인 전환 (현재 100개 이상의 서비스 운영 중)

APM

- Real-time monitoring of service health & performance
- Full-fidelity NoSample visibility
- Infinite cardinality exploration
- AI-driven directed troubleshooting for shortest MTTR

© 2020 SPLUNK INC.

Splunk Observability Suite 의 효과

개발자는 더 생상적으로, 고객은 더 만족스럽게!

배포 품질 & 속도

8X

새로운 출시 및 업데이트 시 더 높은 품질과 더 빠른 코드 릴리즈

고객 경험

100X

더 적은 missed anomalies 와 사용자에 미치는 인시던트 감소, 사용자 경험을 효과적으로 증대

시스템 가용성

80%

신속한 문제 상황 탐지, 확인, 해결

개발자 효율성

70%

더 적은 장애, 더 짧은 트러블슈팅으로 인해 개발자 생산성 향상

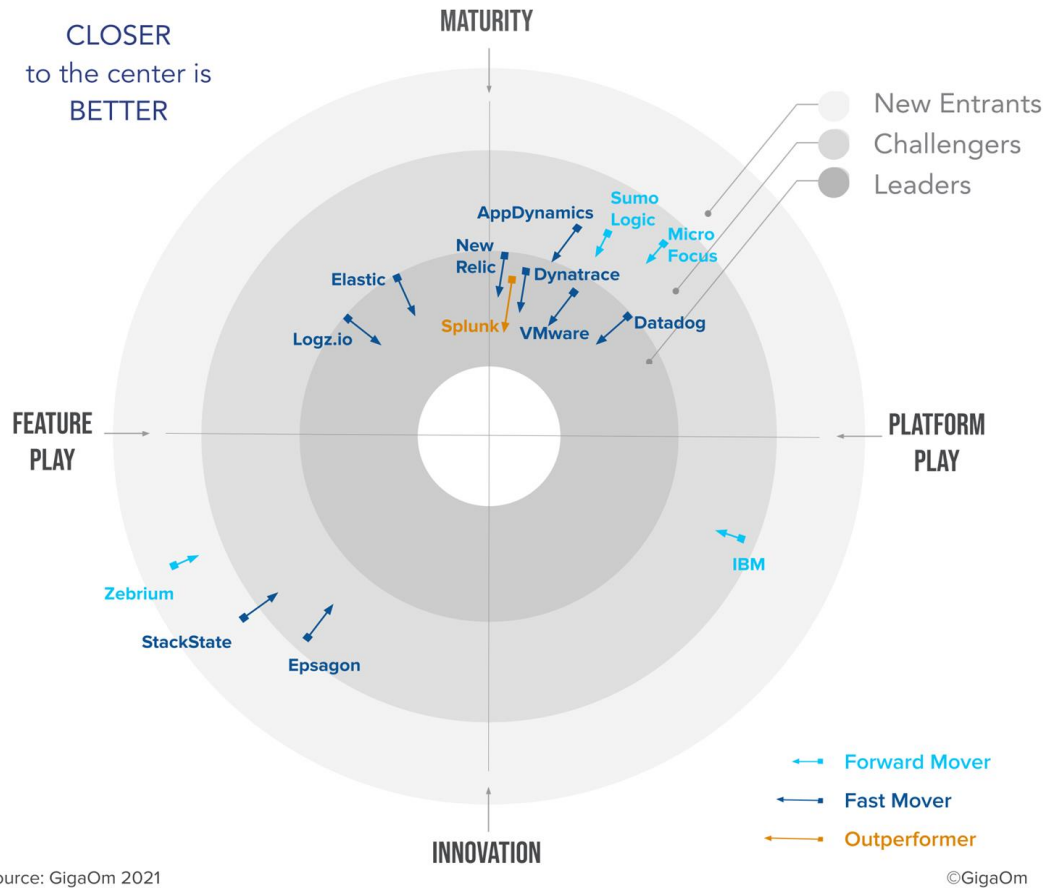
https://medium.com/nikeengineering/how-nikes-digital-transformation-is-monitored-3c0799b3e443

© 2020 SPLUNK INC.

Splunk, Observability 분야에서 Market Leader 로 선정

GIGAOM

Top-ranked vendor and only Outperformer in GigaOm Radar for Cloud Observability



- Splunk는 Datadog, New Relic & Dynatrace 등 모든 벤더를 제치고 최상위 랭킹
- GigaOm 은 Splunk Observability 의 "**대규모 확장성, 정교한 스트리밍 분석 방식, 네이티브 OpenTelemetry 지원**" 을 높게 평가
- "Observability 스택 강화를 위해 여러 회사를 인수한 Splunk 는 이 분야의 최강자다."

— Andy Thurai, Senior Analyst, GigaOm

https://www.splunk.com/en_us/form/2021-gigaom-radar-for-cloud-observability.html

splunk> turn data into doing™

© 2020 SPLUNK INC.

14일 무료 체험

http://observability.splunk.com

splunk> HOME INFRASTRUCTURE MONITORING APM LOG INVESTIGATION INCIDENT RESPONSE RESOURCES

SPLUNK OBSERVABILITY

End-to-End Observability

Get insights into your applications and infrastructure in real-time with the help of the monitoring, analytics and response tools of the Splunk Observability suite

Try Splunk Infrastructure Monitoring Free for 14 days

Select Region

Choose where you'd like your account hosted

Next

splunk> turn data into doing™

© 2020 SPLUNK INC.

Thank You

splunk> turn data into doing™