Splunk for ITOps + DevOps

이교선 / 최창배 매니저

December 11, 2019

splunk>Forum

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.

Agenda

1) Splunk's Vision for New IT

2) Splunk for IT Ops

3) SignalFX

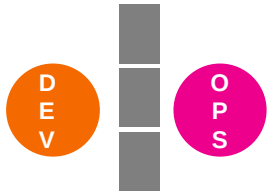
4) Splunk Investigate

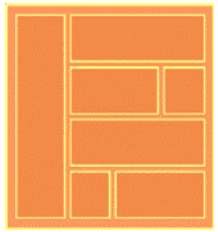
Splunk's Vision for New IT

splunk>Forum

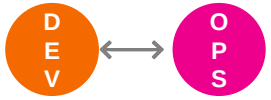
App 개발과 운영을 위한 환경은 변하고 있습니다

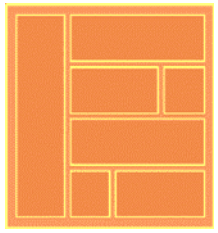
From classic on-prem IT orgs, to cloud native ones, and everything in between





Tightly Coupled Apps, Slow Deployment Cycles





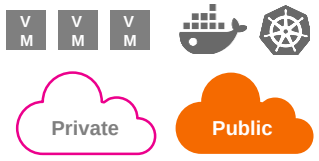
Primarily using Cloud IaaS

Cloud Managed e.g. RDS, DynamoDB, SaaS

More Modular, but Dependent App Components

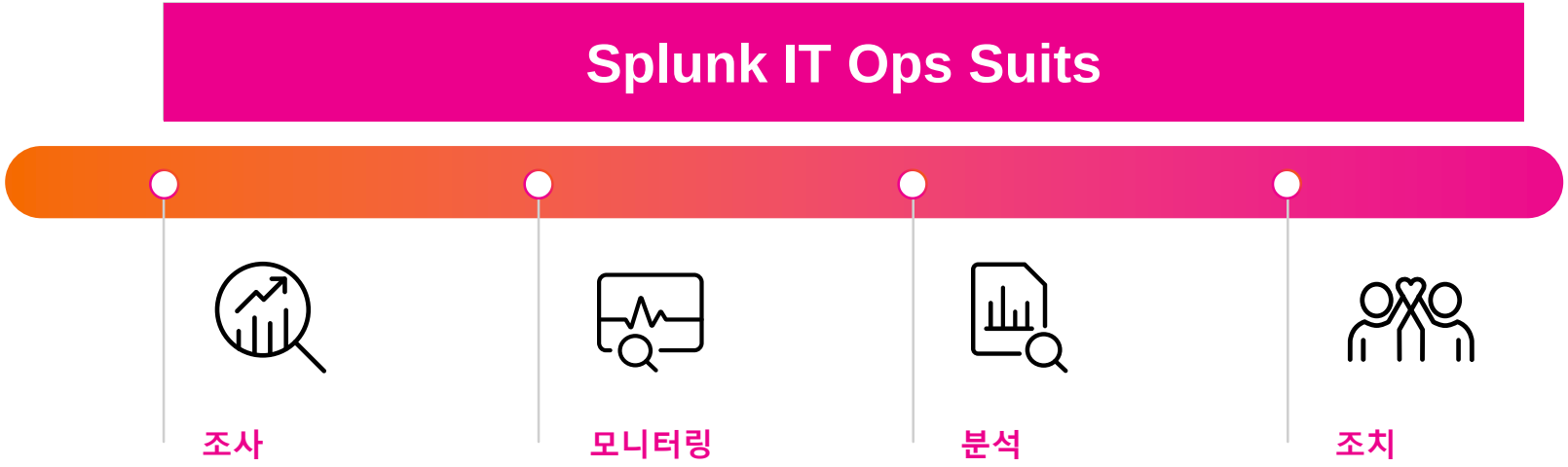
Cloud First Architecture

Loosely Coupled Microservices, and Serverless Functions



Data-to-Everything for IT Ops

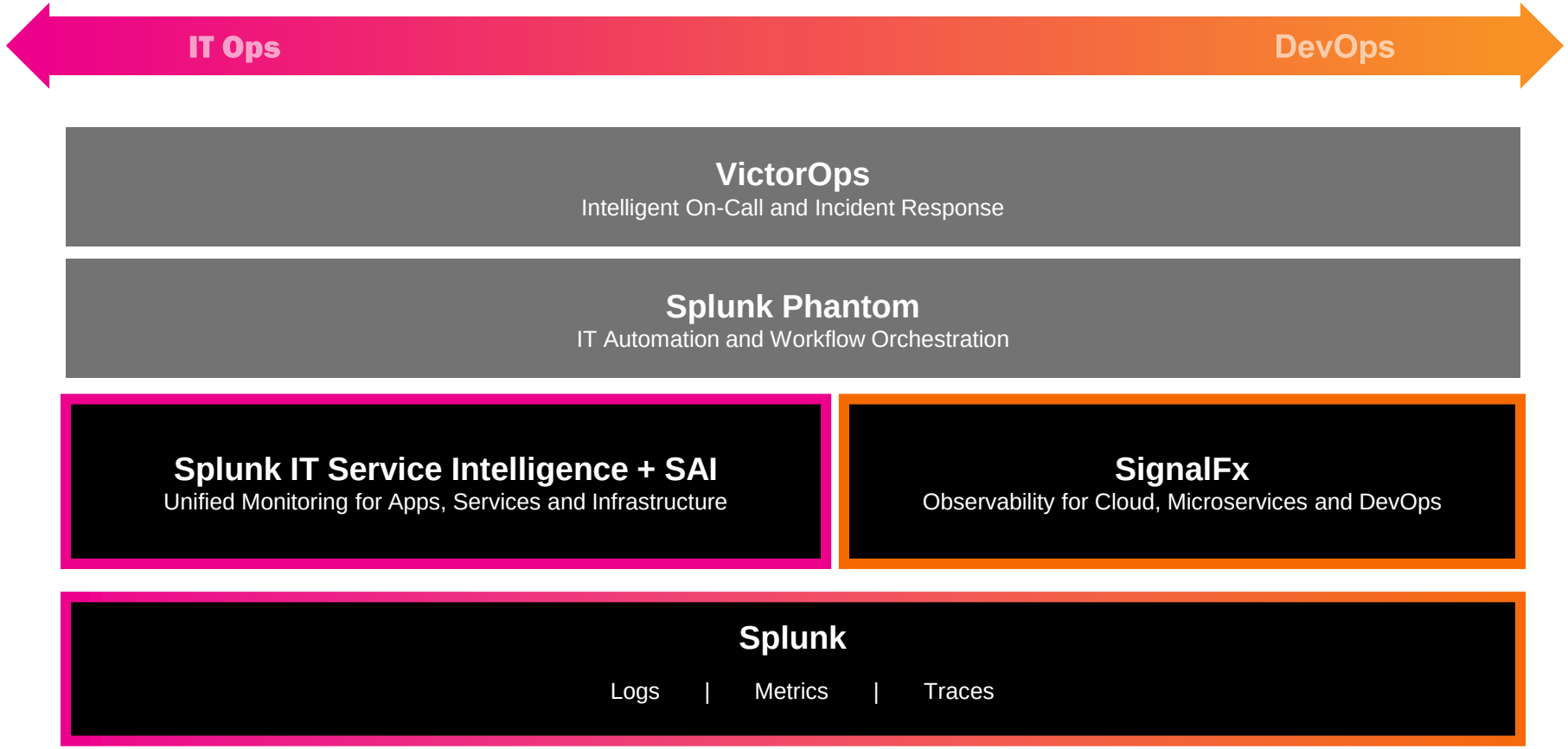
Faster time to business outcomes



IT Ops				
	Speed up investigations: Spot trends and pinpoint root causes leveraging metrics and logs	**Streamline monitoring:** Visibility to services, apps, physical, virtual, and cloud infrastructure	**Understand health of systems:** Service Insights & Event Analytics to focus on what's important, not just what's noisy	**Increase productivity:** Smart collaboration, orchestration and automation

NEW IT / DEV 환경을 위한 SPLUNK 포트폴리오

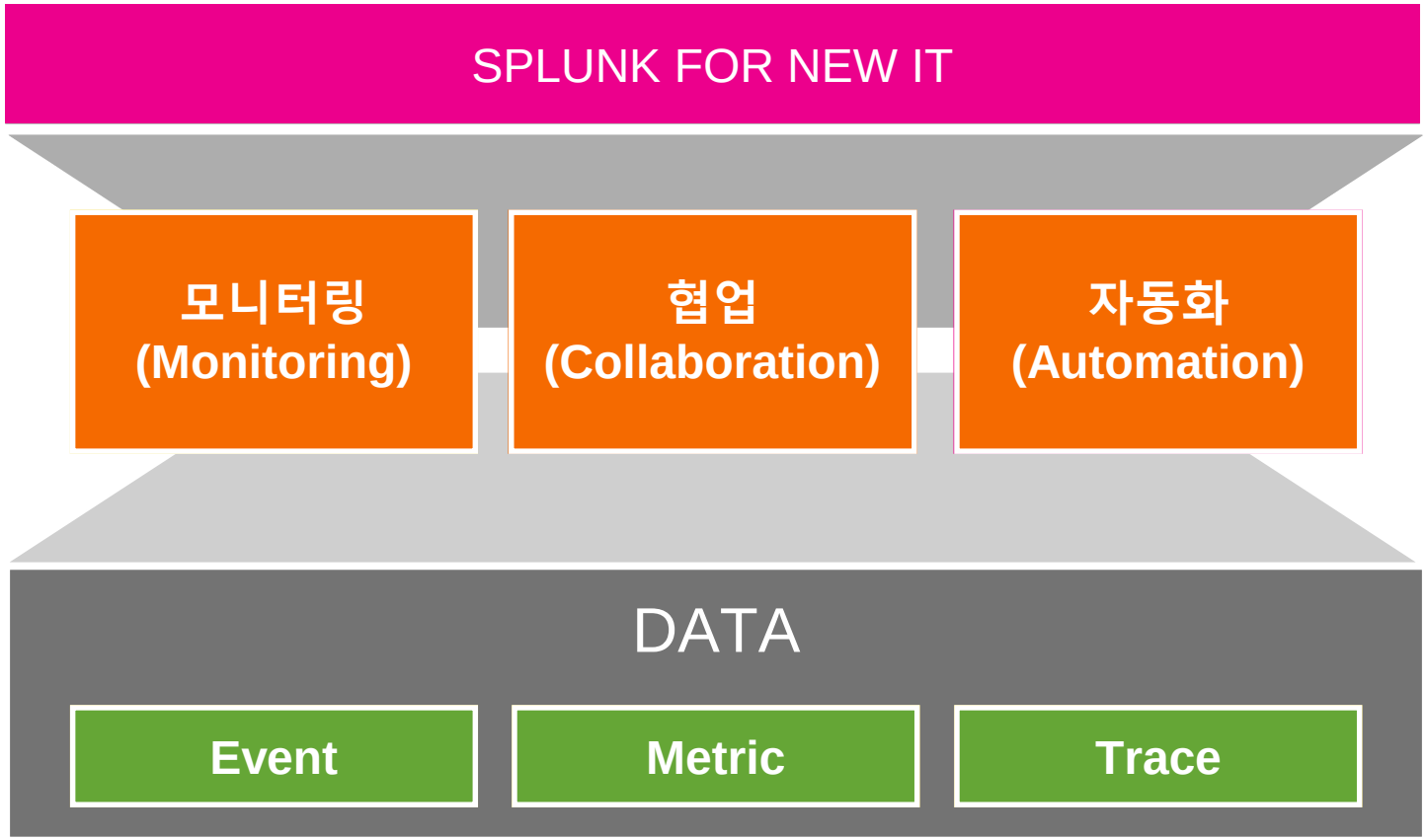
The only platform for monitoring, observability & AIOps - every app, every team



Splunk for IT Ops

splunk>Forum

New IT 환경을 위한 Splunk의 세가지 주요 기능



Splunk for ITOps

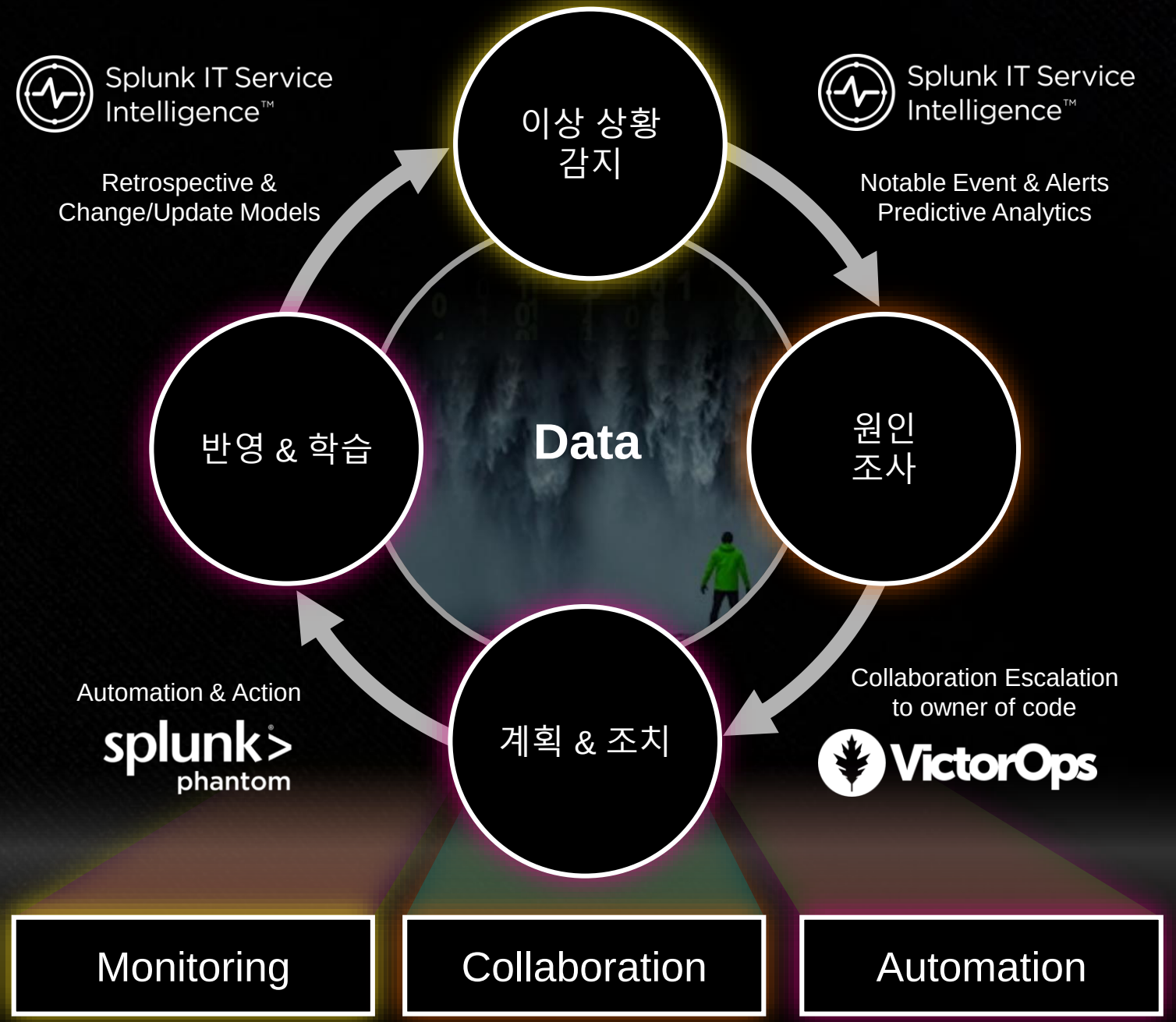
The Modern Suite of Solutions for the New IT Operations

splunk>

Splunk IT Service Intelligence™

VictorOps

splunk> phantom



Splunk IT Service Intelligence (ITSI)

Turn data into doing with predictive insights across apps, services & infrastructure

PREDICTIVE ANALYTICS & AIOPS | SERVICE INSIGHTS | EVENT MANAGEMENT | INFRASTRUCTURE MONITORING

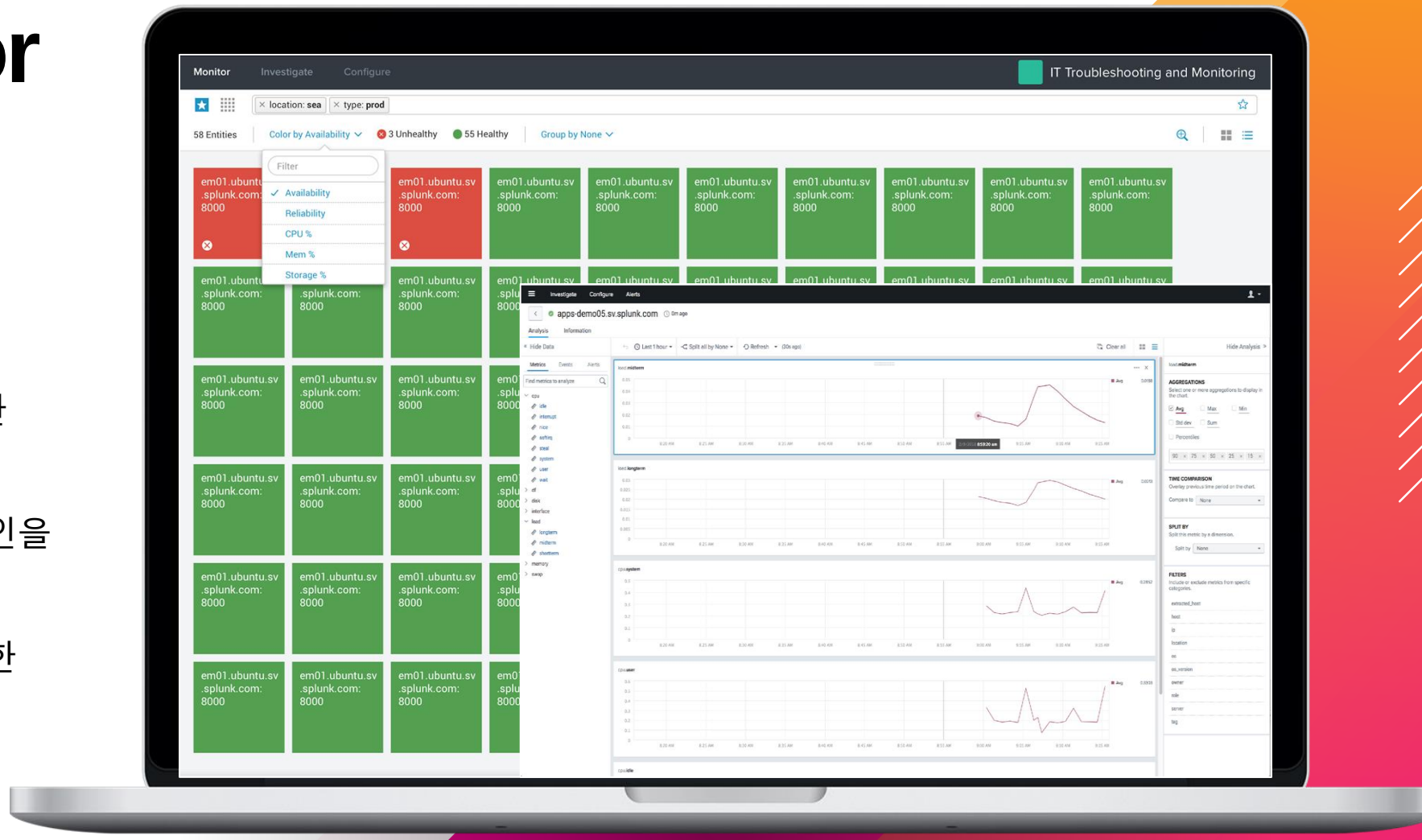
데이터 기반 IT운영 관제
Silo 형태로 관리되는 로그와 지표를 IT와 비즈니스 레벨에서 실시간 / 통합 형태로 사용 가능한 플랫폼

예측 및 예방
이벤트 노이즈 및 MTTR을 빠르게 줄이면서 통합 모니터링, 장애 조치 및 조사를 위한 기능 지원

AIOps On-Prem & Cloud Platform
확장 가능하고 최신 아키텍처를 지원하는 AIOps 플랫폼

Splunk App for Infrastructure

- **다양한 OS, VM, 클라우드, 컨테이너 모니터링을 위한 앱**
- 빠른 가치 실현 : 손쉬운 설정을 통한 데이터 수집
- 가이드 기반으로 트렌드와 장애 원인을 빠르게 조사할 수 있도록 지원
- 지표와 로그에 대한 유연하고 다양한 형태로 분석할 수 있는 기능 지원
- ITSI 통합 기능 제공
- Splunk Cloud 지원

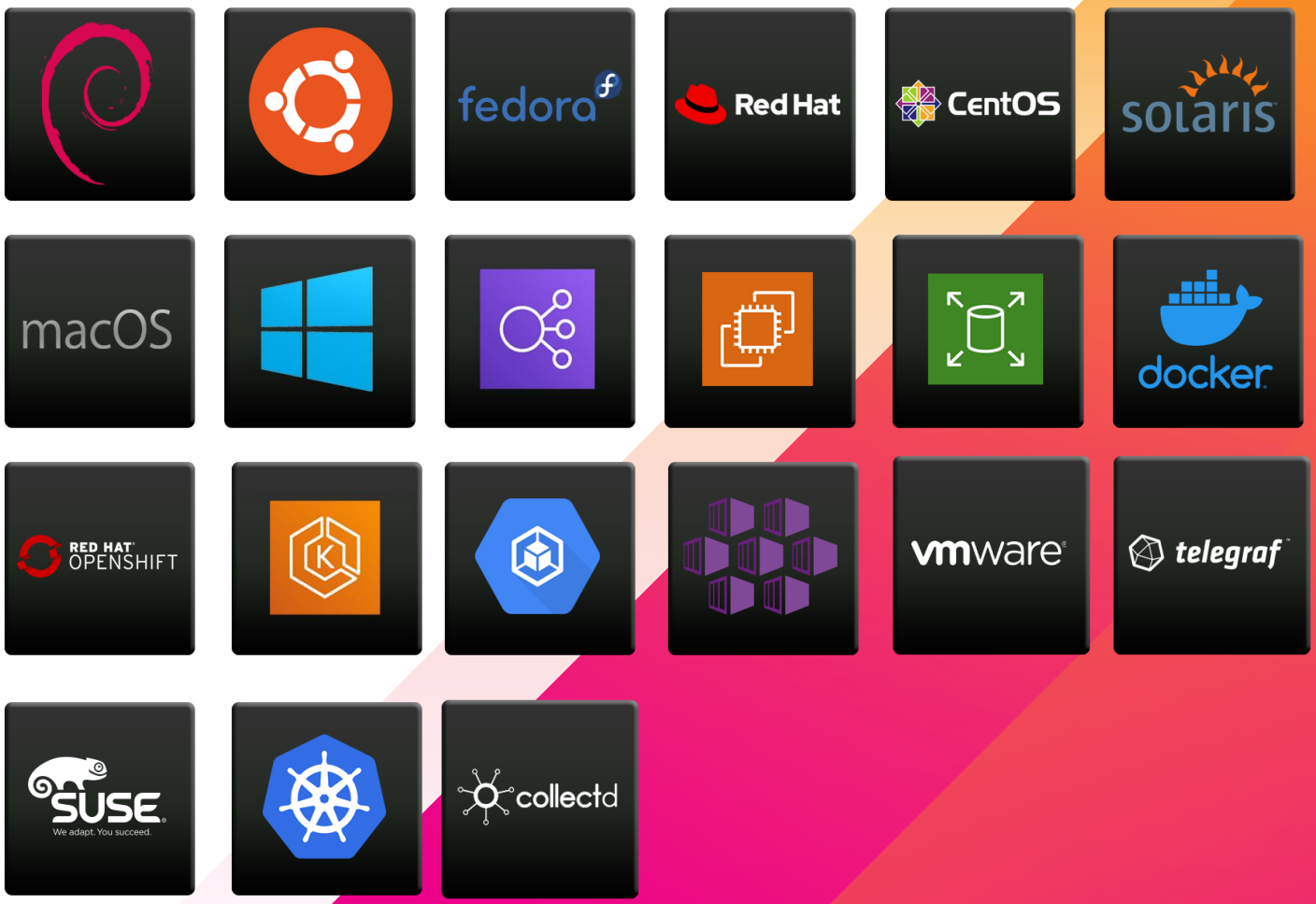


splunk> turn data into doing

Data Collection

Onboard thousands of servers in the time it takes to install other enterprise monitoring tools

- 가이드 기반의 데이터 수집 :
  - **Linux/Unix/OSx**
  - **Windows**
  - **Kubernetes**
  - **Docker**
  - **OpenShift**
  - **VMware vSphere**
  - **AWS**
  - **Azure**
- 수분 이내에 로그와 지표 데이터를 수집할 수 있도록 손쉬운 설치 지원
- 커스텀 메타 데이터와 데이터 수집 관리를 위한 UI 지원



VictorOps

Splunk 포함 다양한 모니터링 툴에서 발생한 경고를 Right Team / People 이 처리 가능토록 지원

Alarm

Infrastructure and application monitoring

splunk> Splunk ITSI System Monitoring
Splunk Insights for Infrastructure System Monitoring
amazon web services
Nagios
solarwinds The Power to Manage IT
APPDYNAMICS
New Relic.
DATADOG
RACKSPACE CLOUD MONITORING
boundary
uptime
catchpoint
PRTG NETWORK MONITOR
ruxit
DNSCheck
sumologic
bugsnag
pingdom
ZABBIX

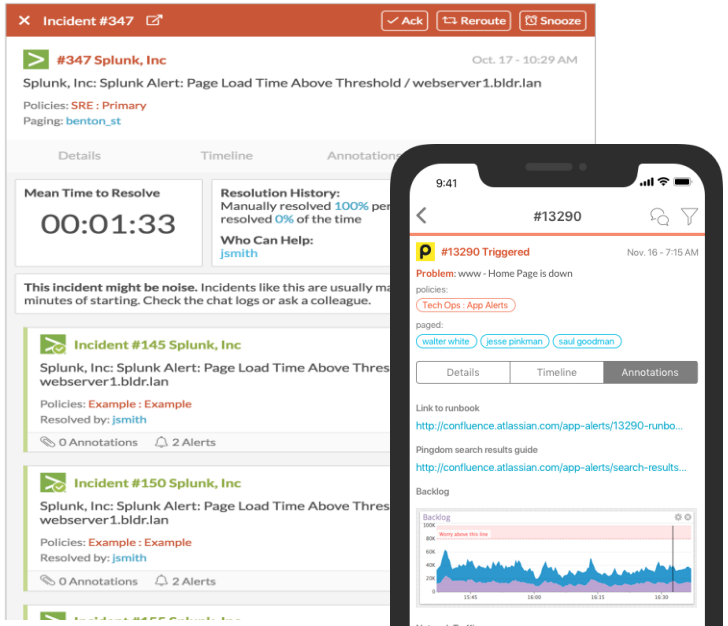
slack
Statuspage
salesforce.com
Google Voice

servicenow
Jira Software

GitHub
puppet
Jenkins

모니터링 툴에서 경고 발생 시
해당 정보를 VictorOps로 전달

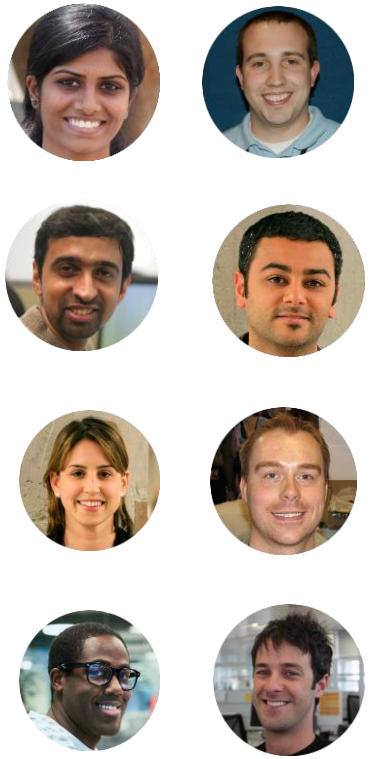
Routing / Collaboration



- Mobile Notification
- Live Phone Call
- Email
- WebHook

VictorOps는 해당 경고를 처리하기
위한 적합한 팀/사람을 할당

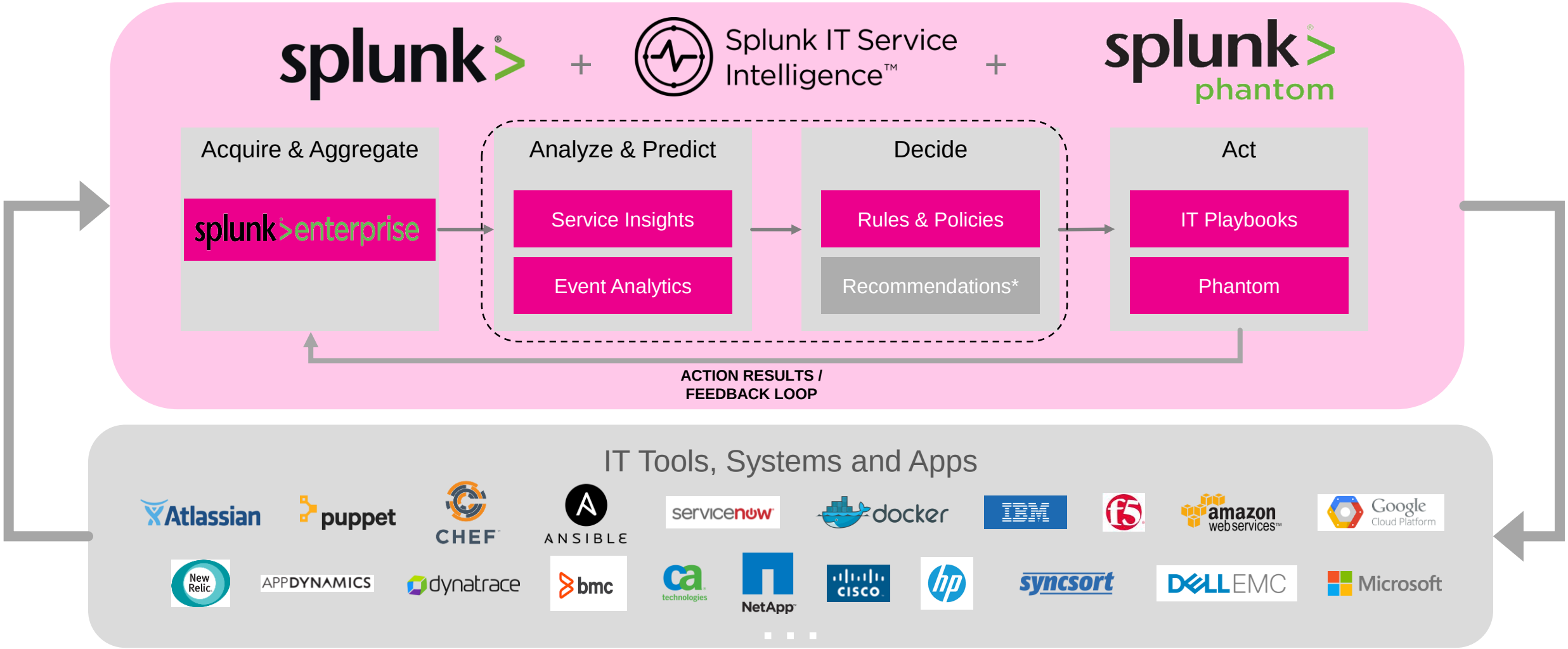
Action



팀/사람은 VictorOps 의 협업 기능을
통하여 장애 처리 수행

splunk> turn data into doing

Phantom – ITOps Automation



Phantom – Playbook for ITOps

Key IT Apps & Actions

Available in Phantom v4.3

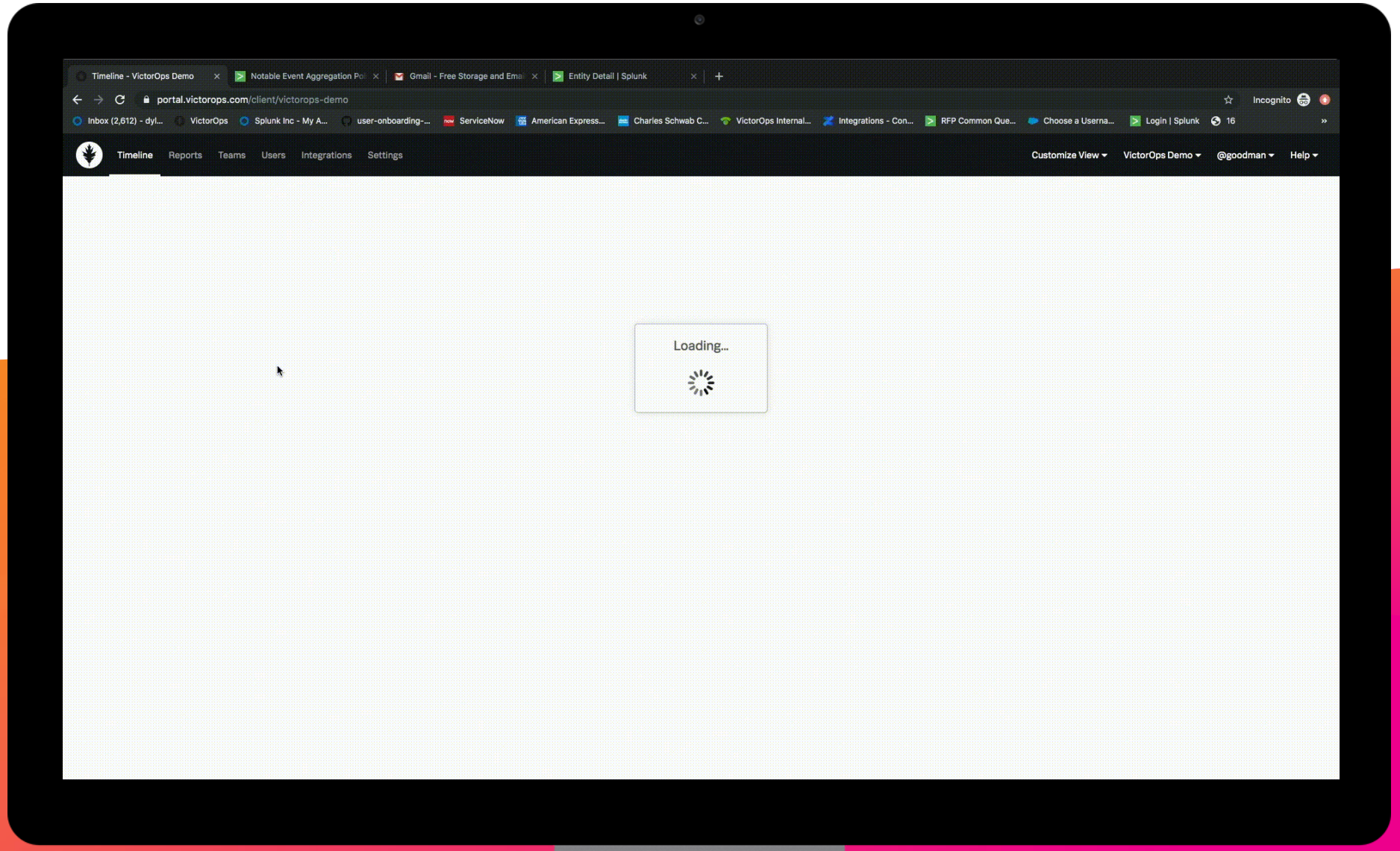
70+ Apps

500+ Actions

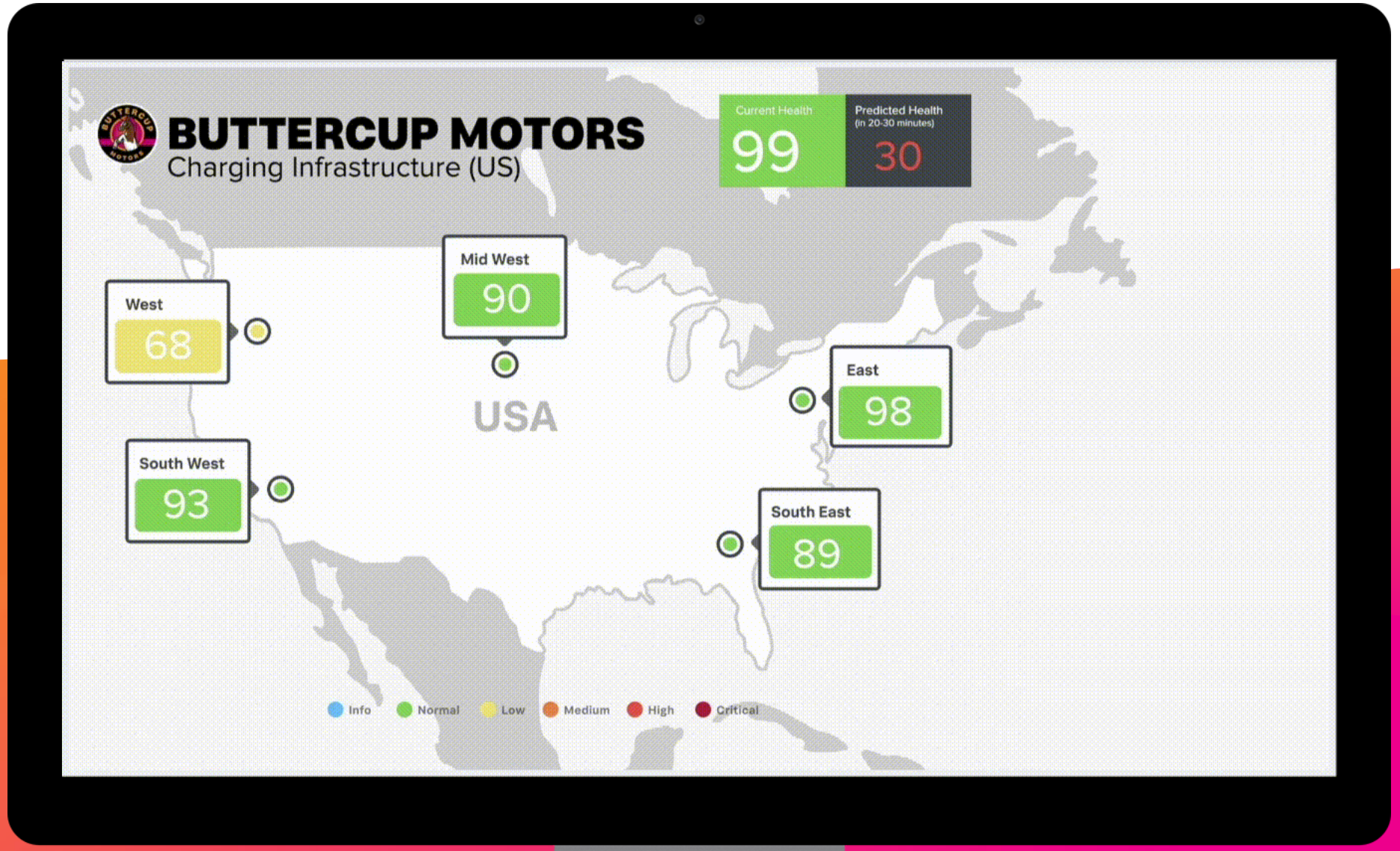
Key Categories	Products	Use cases
ITSM	SNOW, BMC, Cherwell, Zendesk, Jira, Microsoft SCCM	Create, Update, Delete, Search Tickets
Incident Management	VictorOps, PagerDuty, xMatters	Create, Update Incidents List Teams, Users, Routing
Authentication	LDAP, AWS IAM, Okta, Duo	Password reset; enable, disable users
Virtualization	vSphere, OpenStack, NSX	List, start, stop, suspend, snapshot VMs
Cloud	AWS, AWS S3, Azure	Create, start, stop, snapshot instance
Operating Systems	Windows, Linux, OS X	Run scripts, commands; list, terminate processes; shutdown, restart
Databases	MySQL, SQLite, Microsoft SQL, MongoDB, Postgres	Run query, list tables, columns,
Email	Exchange, Office, Gmail, SMTP, IMAP	Send Email; run query
Collaboration	Slack, HipChat, Cisco Spark	Send message, ask question, get response, upload file, list users, channels
Config Mgmt Tools	Ansible Tower	Run Ansible playbooks
API	REST, HTTP	Request and response actions

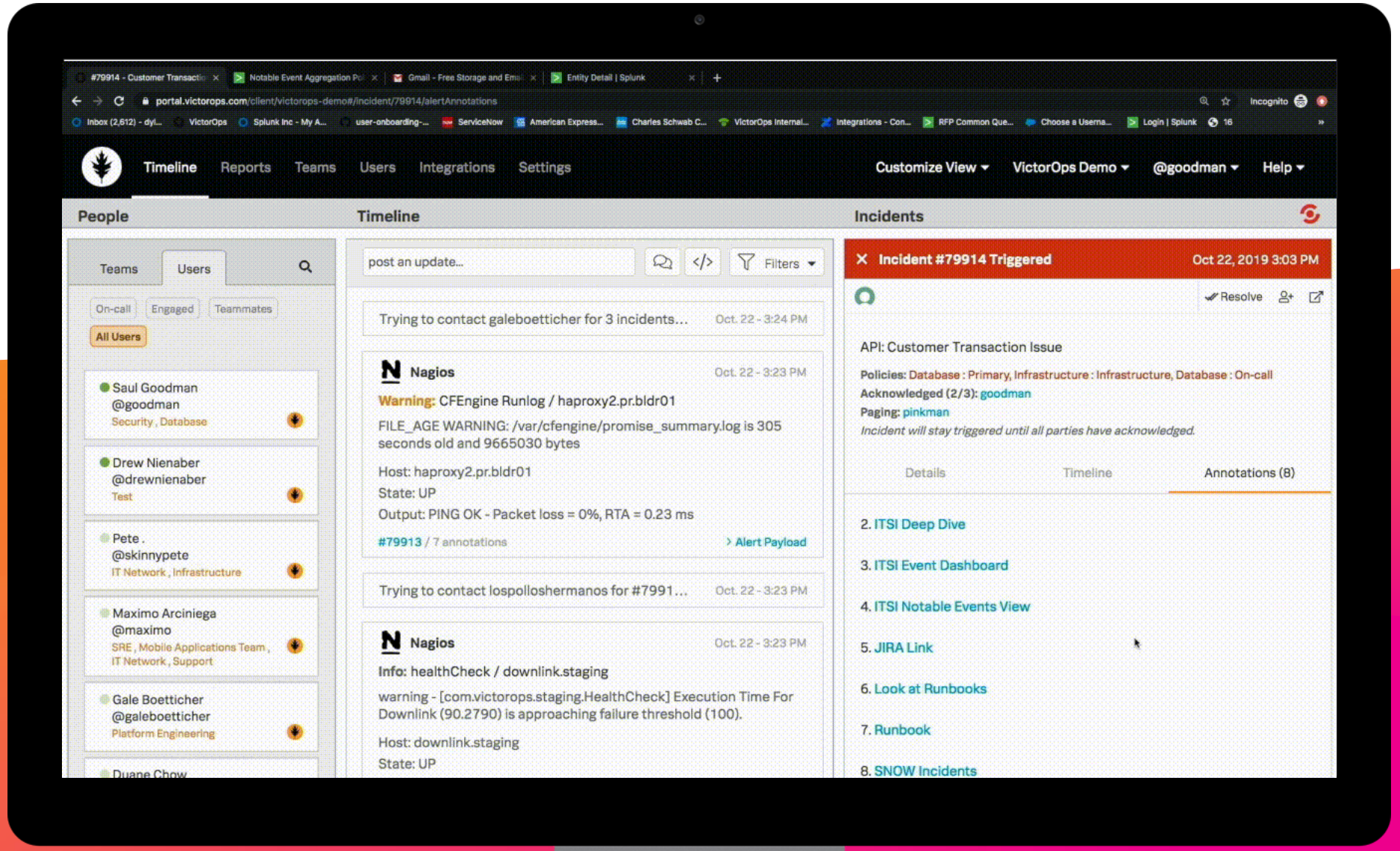

100%
19:31
Tuesday, October 15
VICTOROPS
now
Incident #78928 - Triggered
"Alert: Charging Service Health Score is predicted to drop below 50 within 30min": - "Alert: Charging Service Health Score
Press home to unlock


100%
19:31
Tuesday, October 15
VICTOROPS
now
Incident #78928 - Triggered
"Alert: Charging Service Health Score is predicted to drop below 50 within 30min": - "Alert: Charging Service Health Score
Press home to unlock



splunk> turn data into doing®





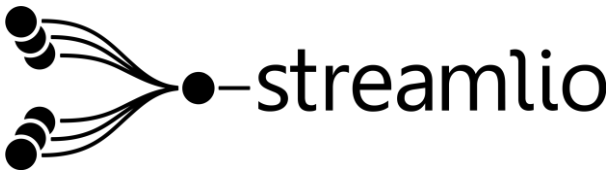
ITOps 강화를 위한 지속적인 투자

Incident Management

Automation

DevOps & Container Monitoring

Distributed Tracing

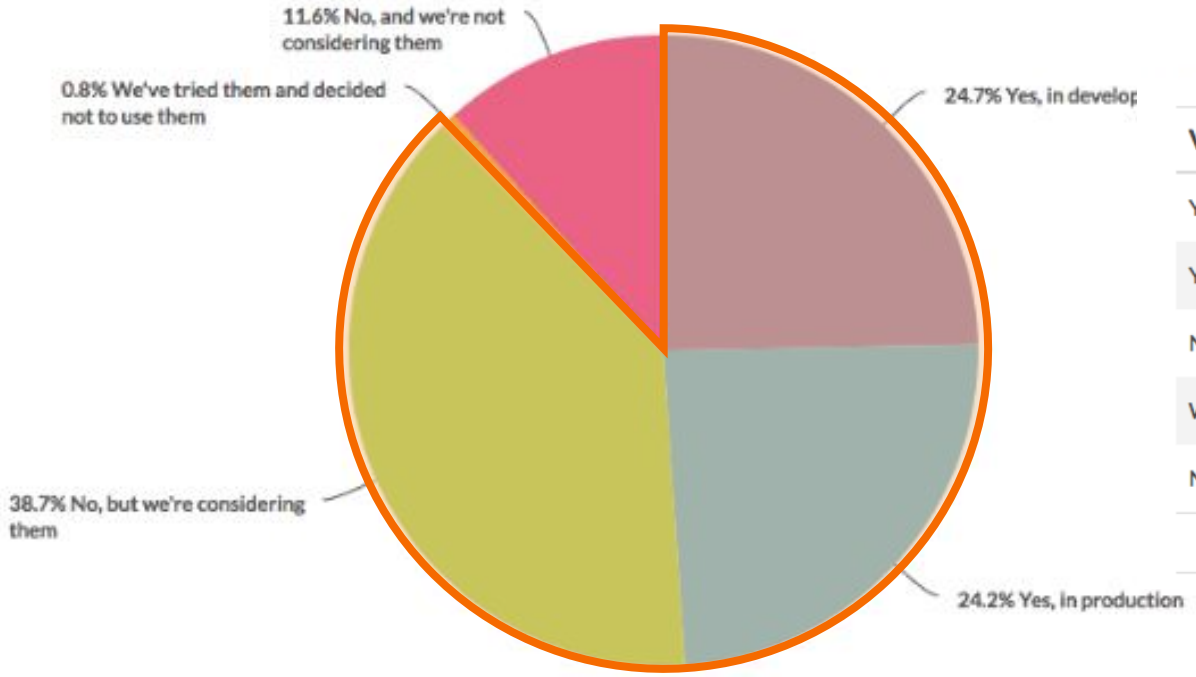


Real time stream processing

SignalFX

splunk>Forum

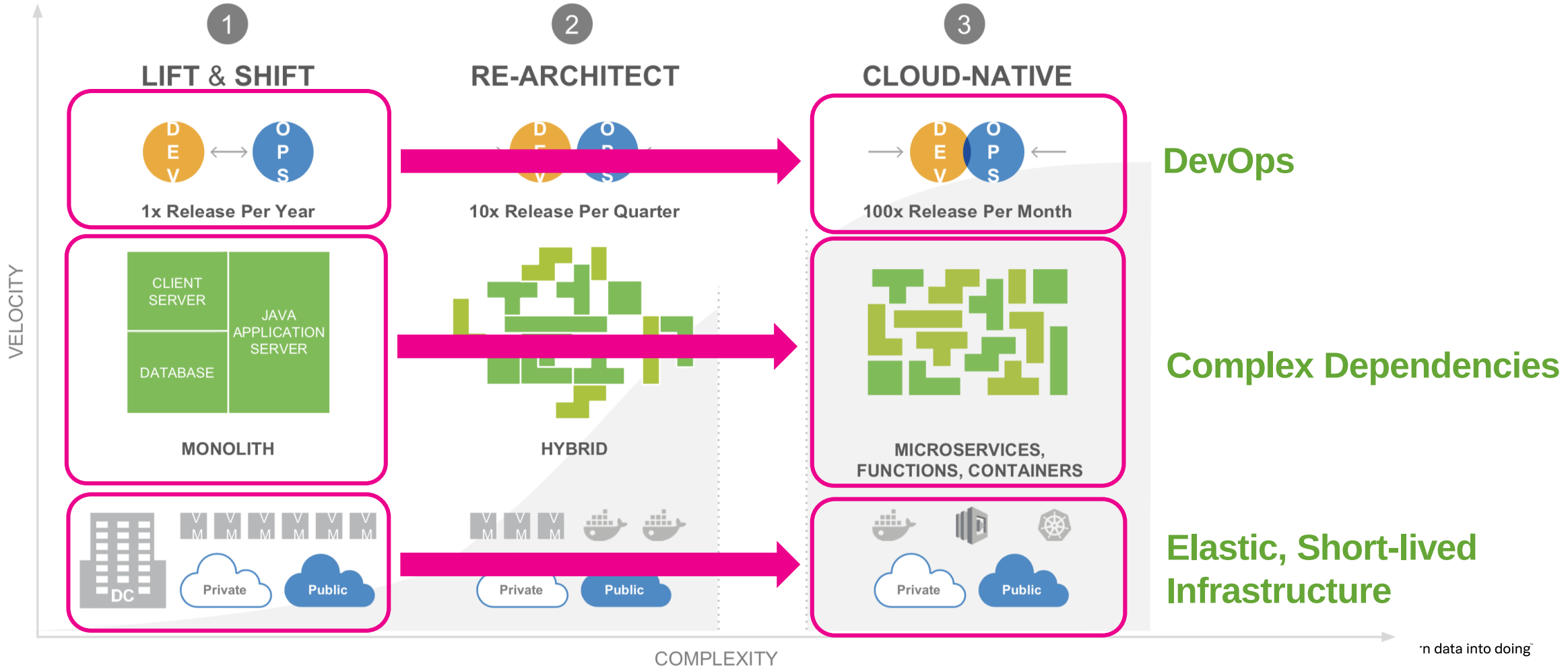
Micro Service 인기



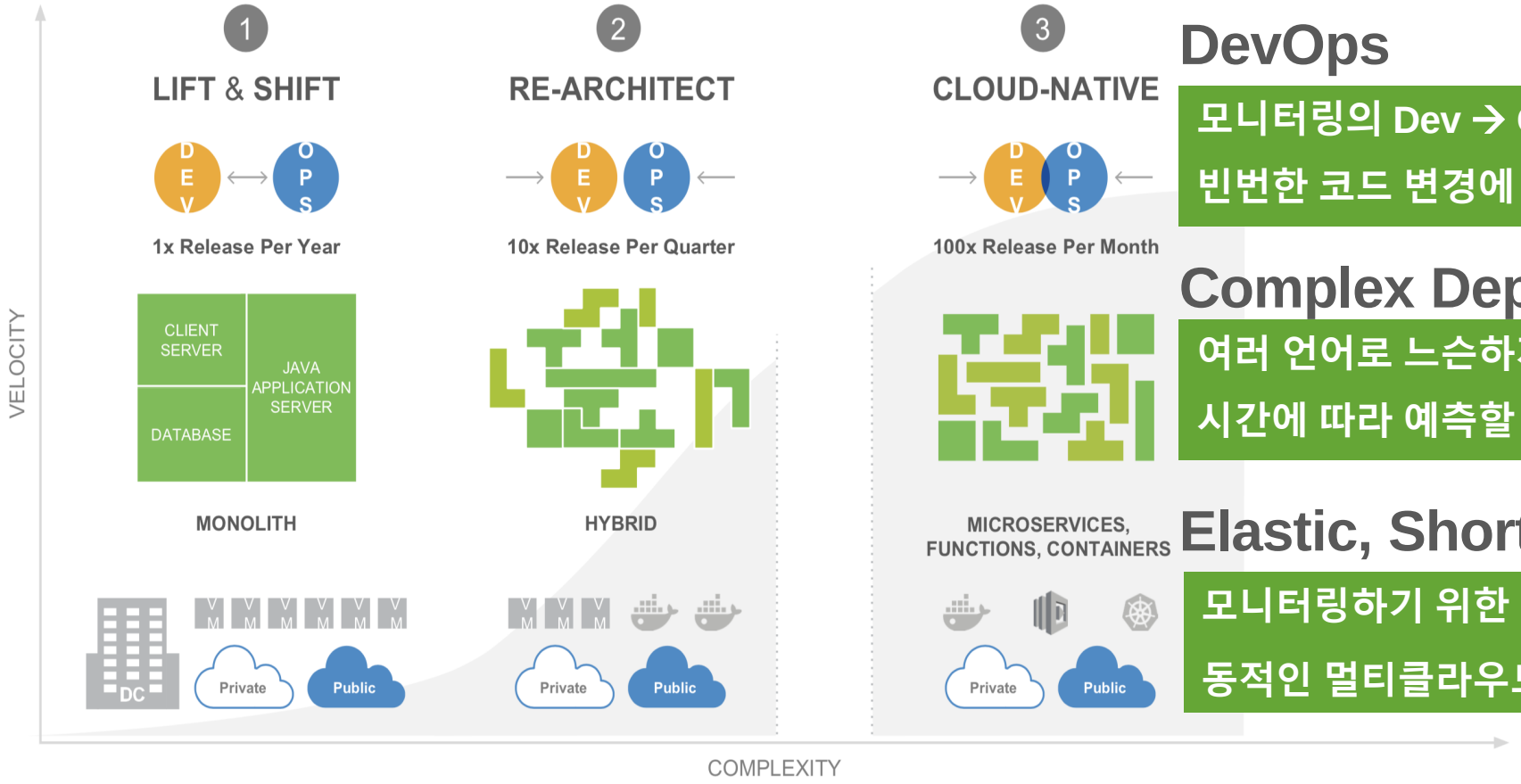
Value	Percent	Responses
Yes, in development	24.7%	181
Yes, in production	24.2%	177
No, but we're considering them	38.7%	283
We've tried them and decided not to use them	0.8%	6
No, and we're not considering them	11.6%	85
		Totals: 732

[출처: 2018 DZone Resarch]

Cloud-Native 로의 전환



Cloud-Native 와 모니터링 도전



DevOps

모니터링의 Dev → Ops 까지 확장

빈번한 코드 변경에 따른 더 많은 위험부담

Complex Dependencies

여러 언어로 느슨하게 서로 연결된 서비스

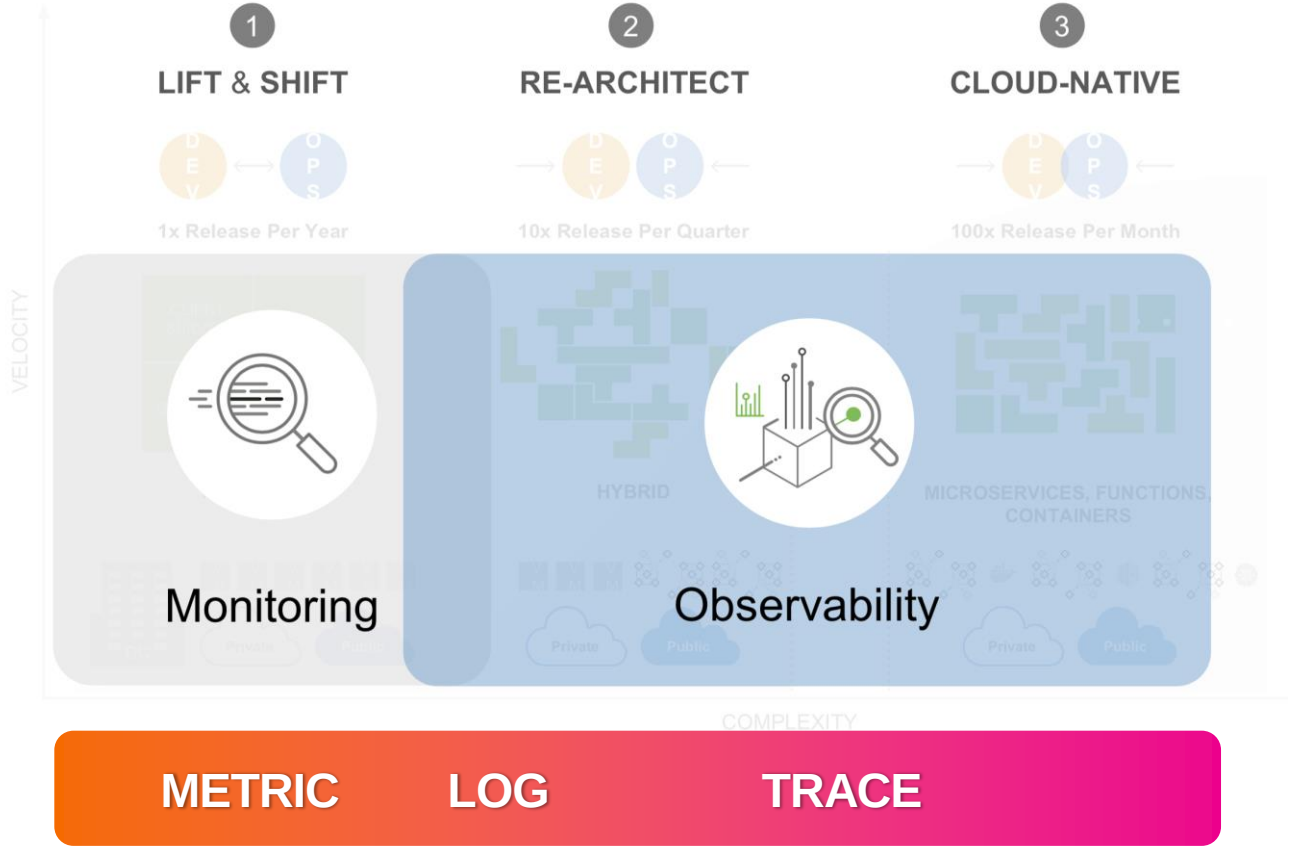
시간에 따라 예측할 수없이 변경되는 시스템

Elastic, Short-lived Infrastructure

모니터링하기 위한 급증

동적인 멀티클라우드, 추상화된 인프라

Monitoring 과 Observability

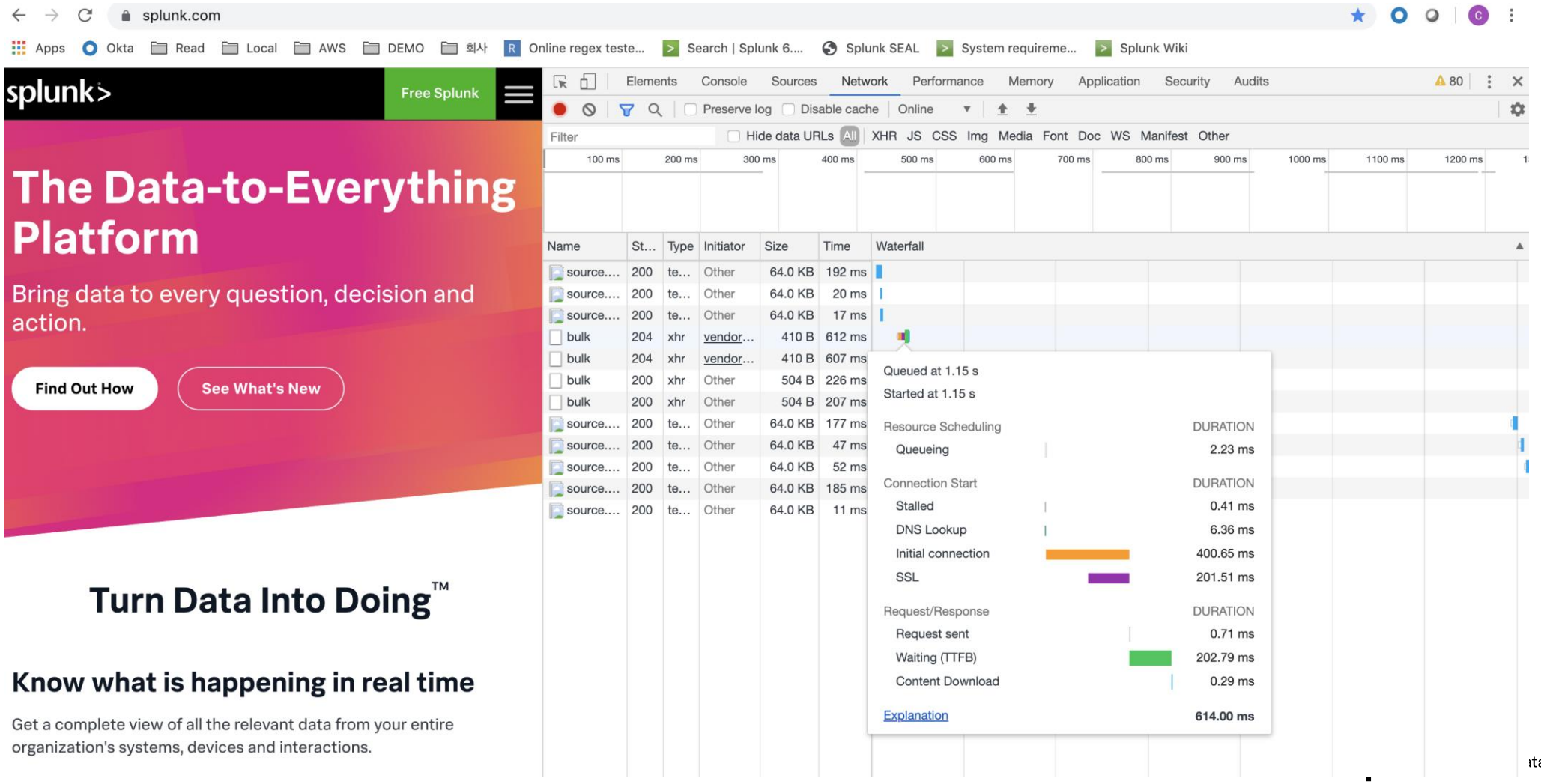


"Traditional monitoring systems capture and examine signals in relative isolation, with alerts tied to threshold or rate-of-change violations.

Observability tools enable a developer or an SRE — to **more effectively explain unexpected system behavior**."

– GARTNER

Trace?

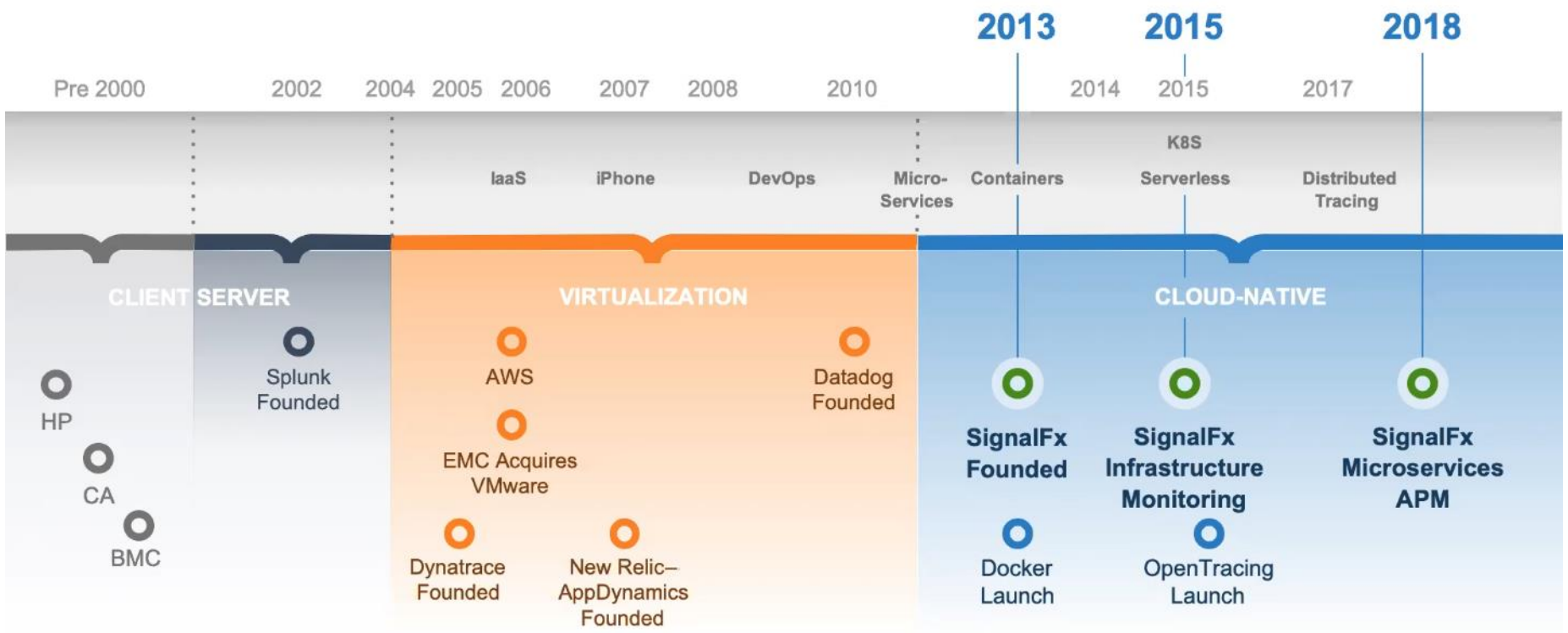


SignalFx

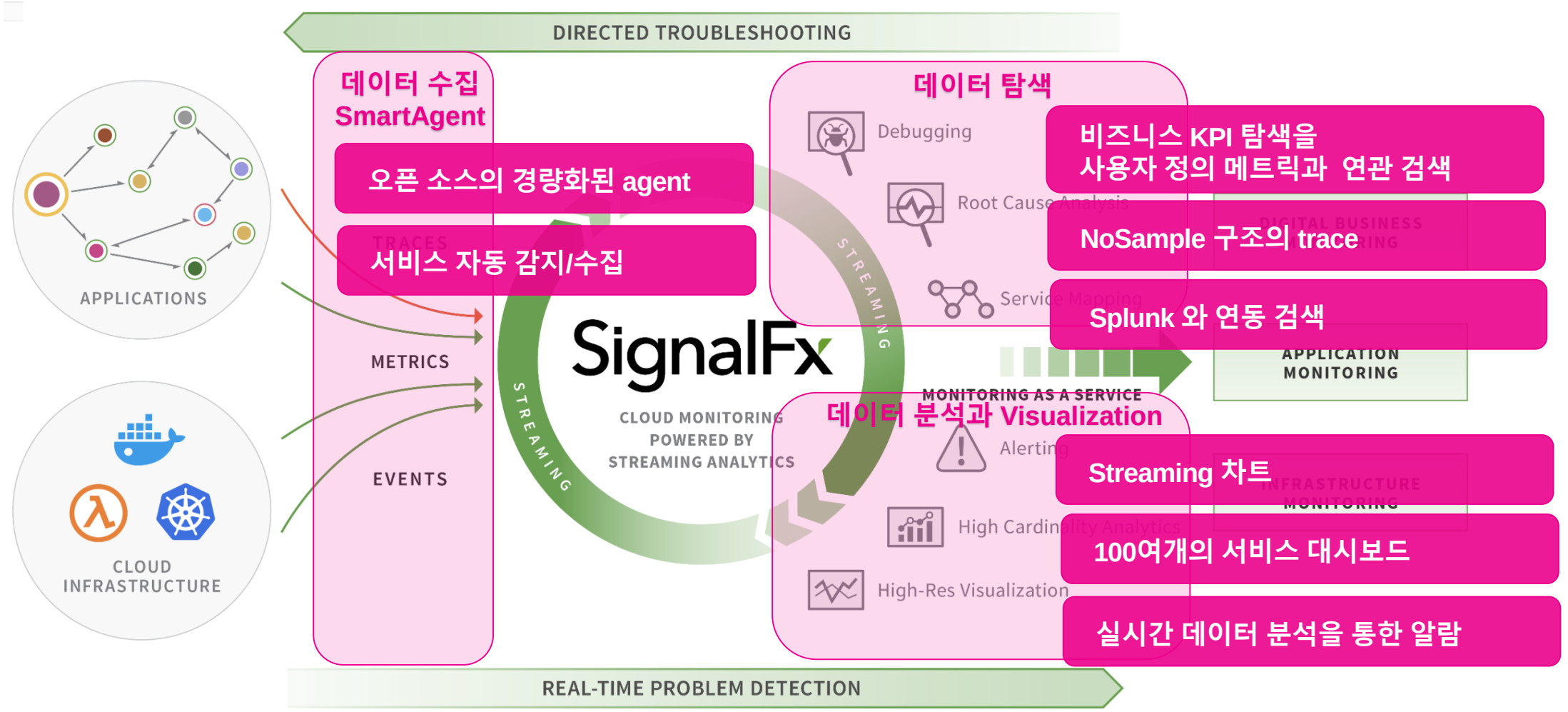
"Real-Time ***Cloud Monitoring and Observability*** *for Infrastructure, Microservice and Applications"*

splunk> turn data into doing

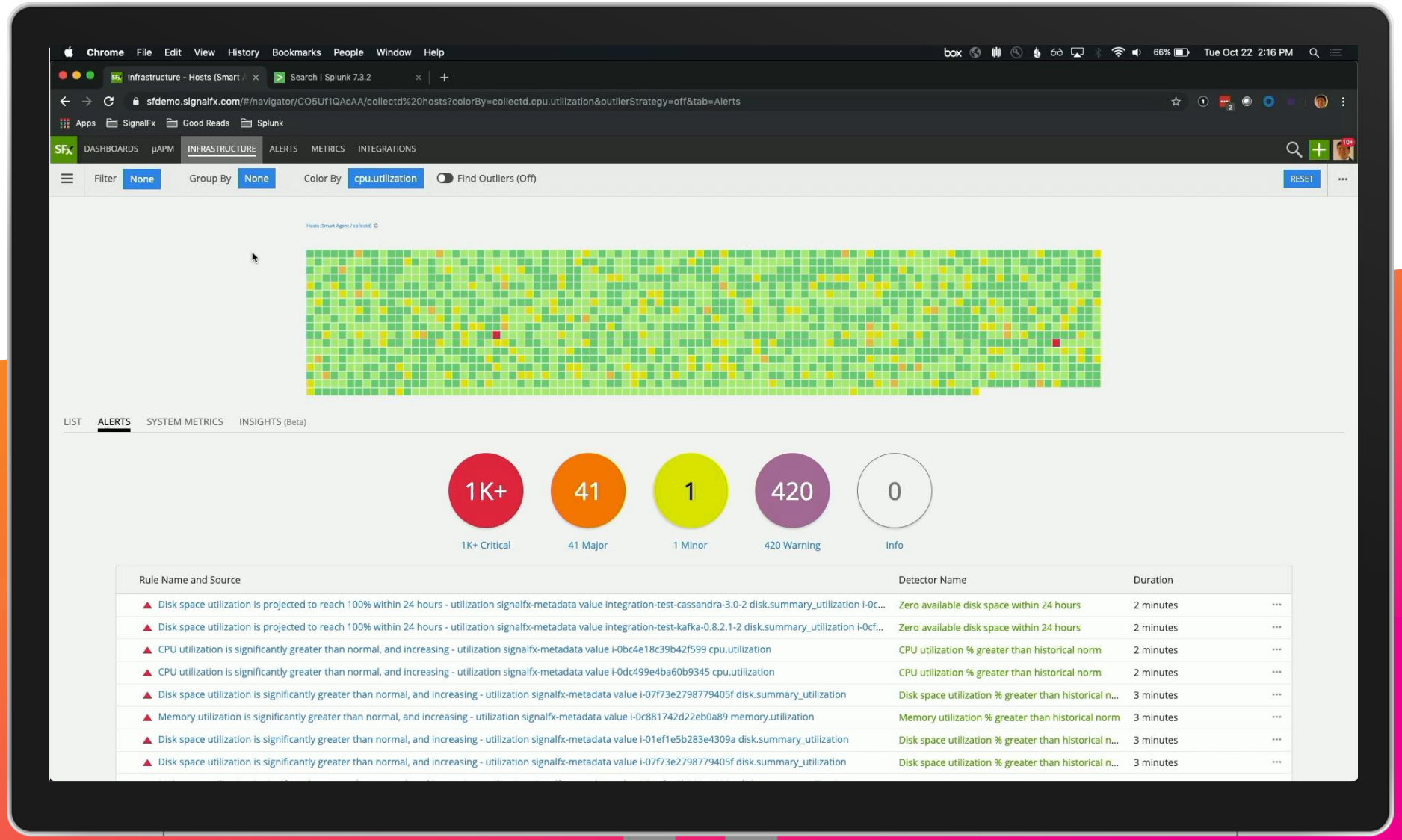
Cloud-Native 시대와 SignalFx



SignalFx 기능

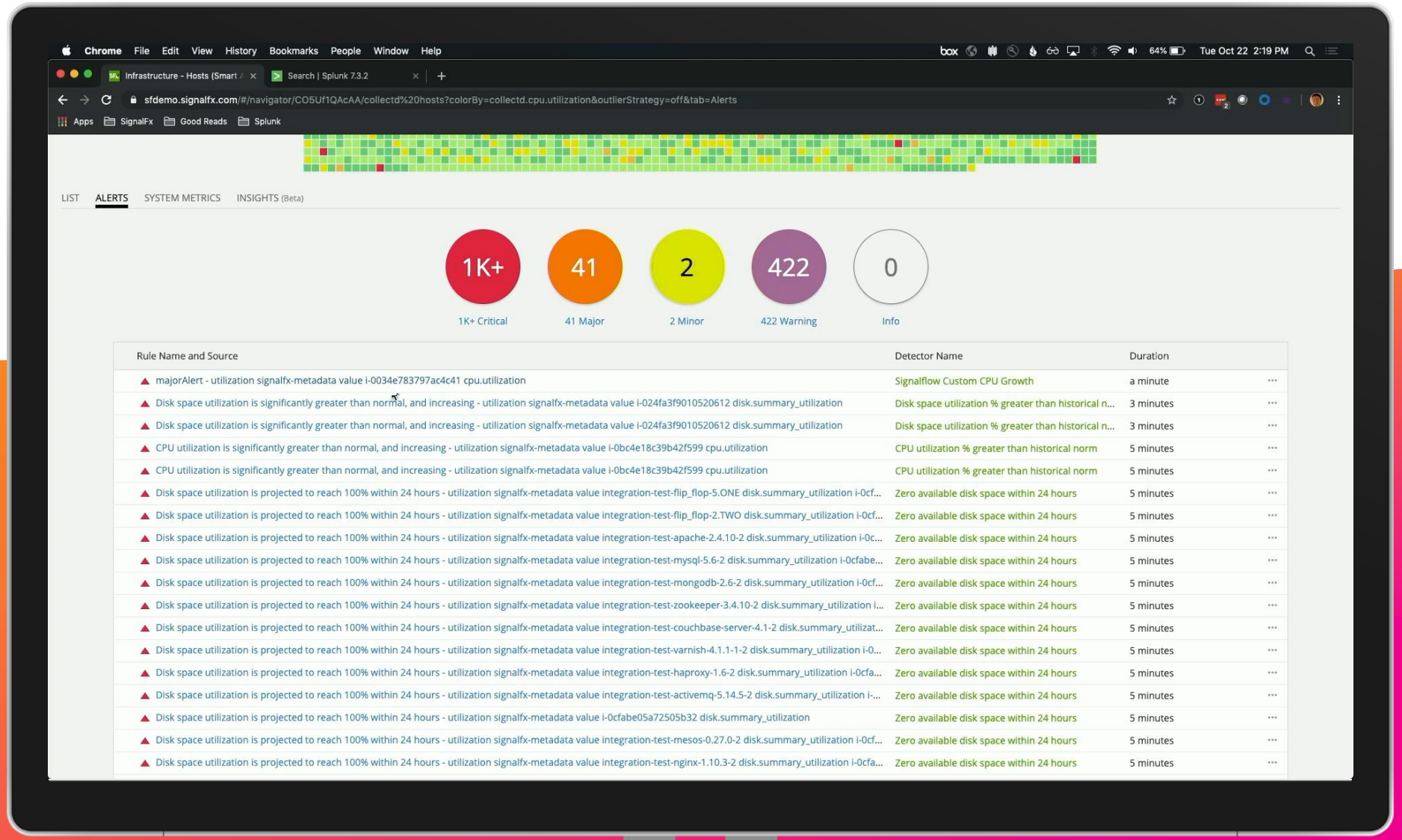


Infrastructure Monitoring

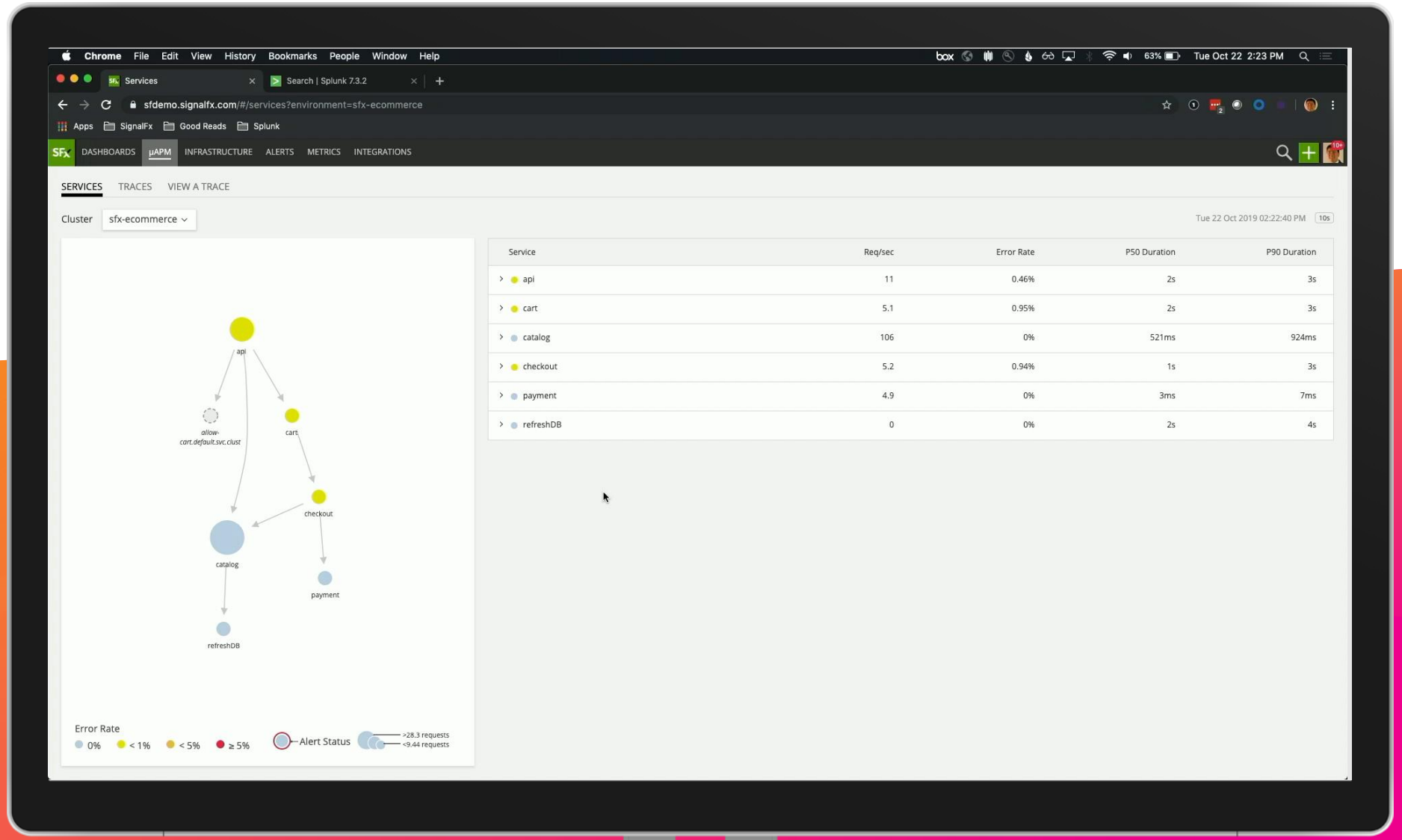


splunk> turn data into doing

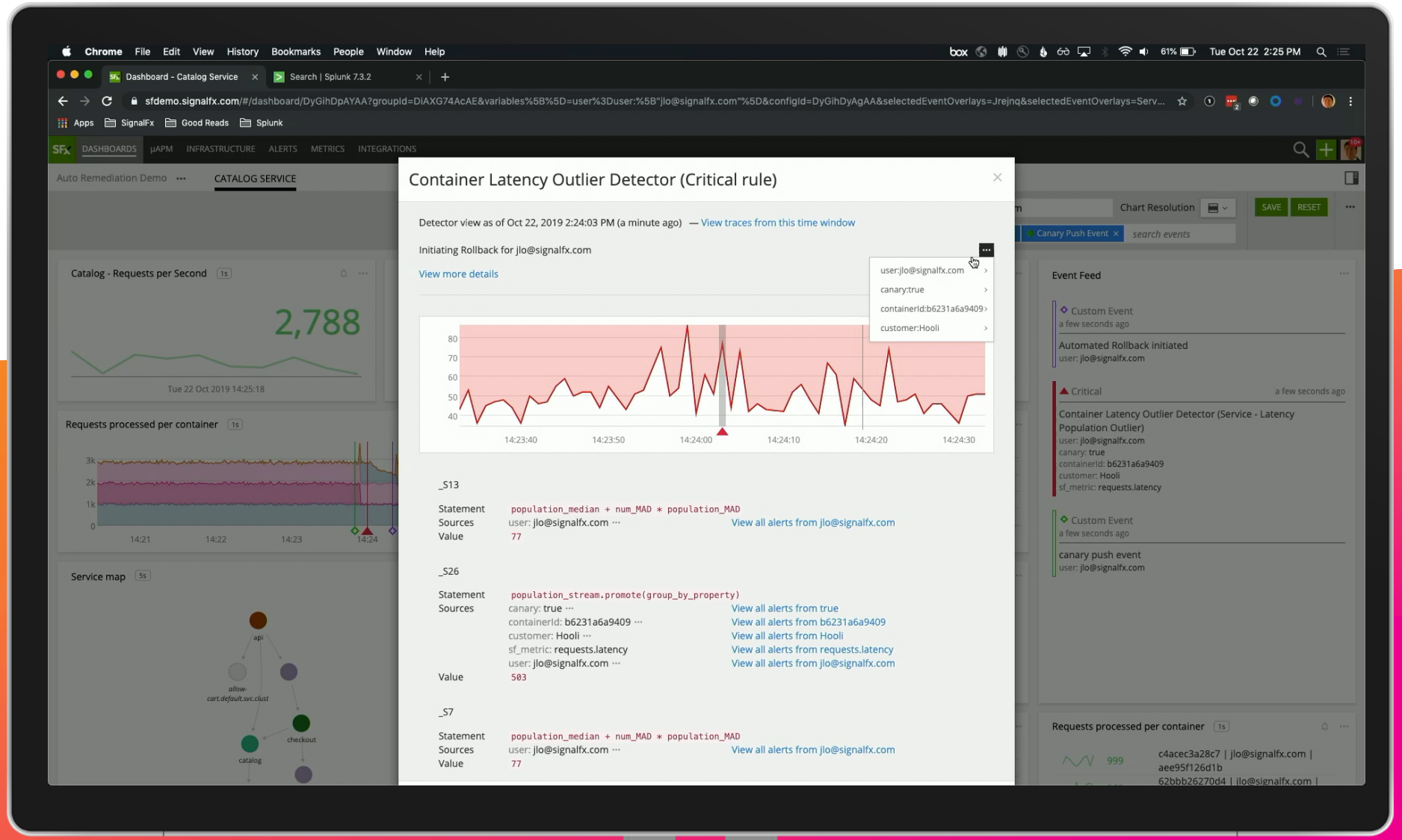
Alert



Micro APM

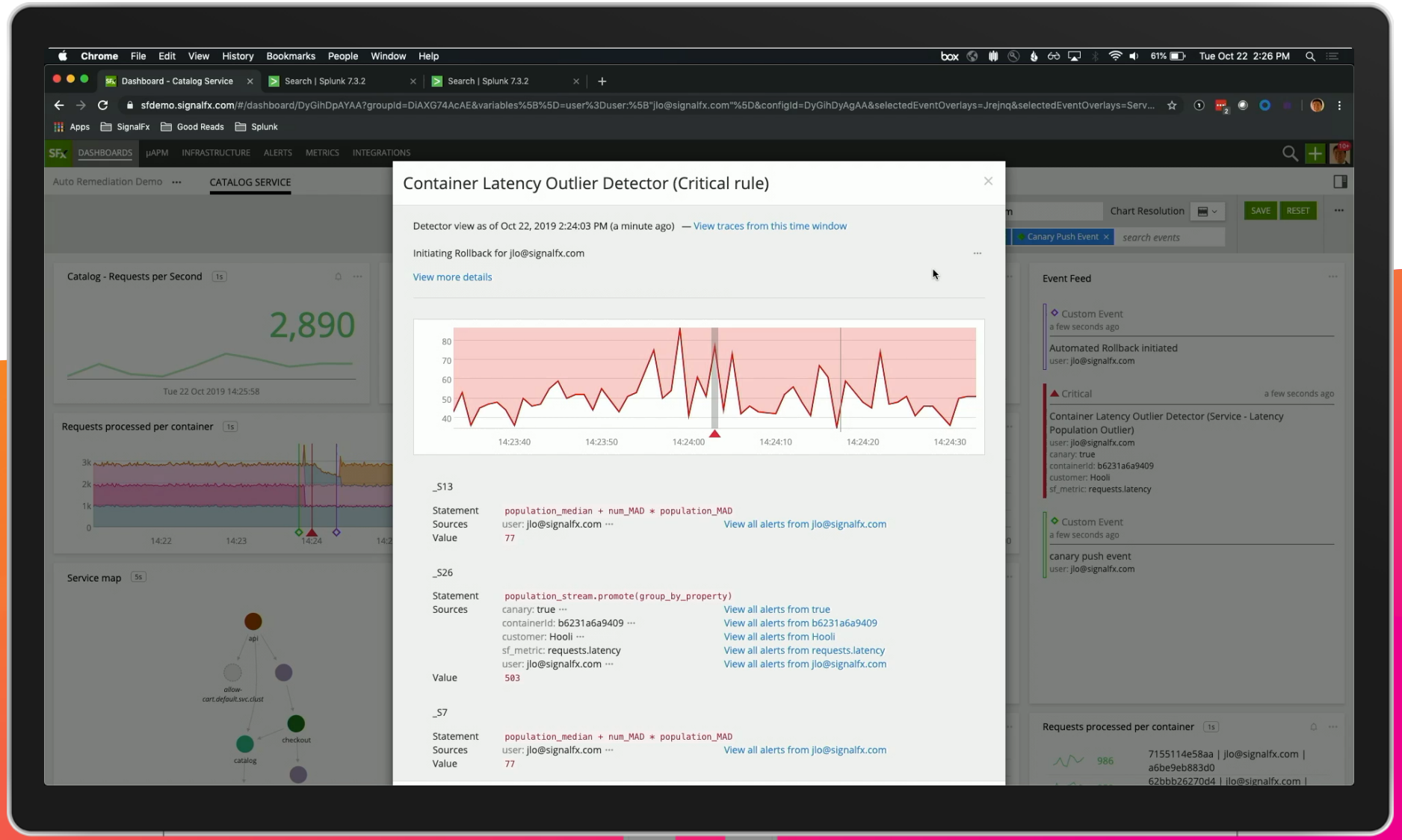


SPLUNK 와 연동



splunk> turn data into doing®

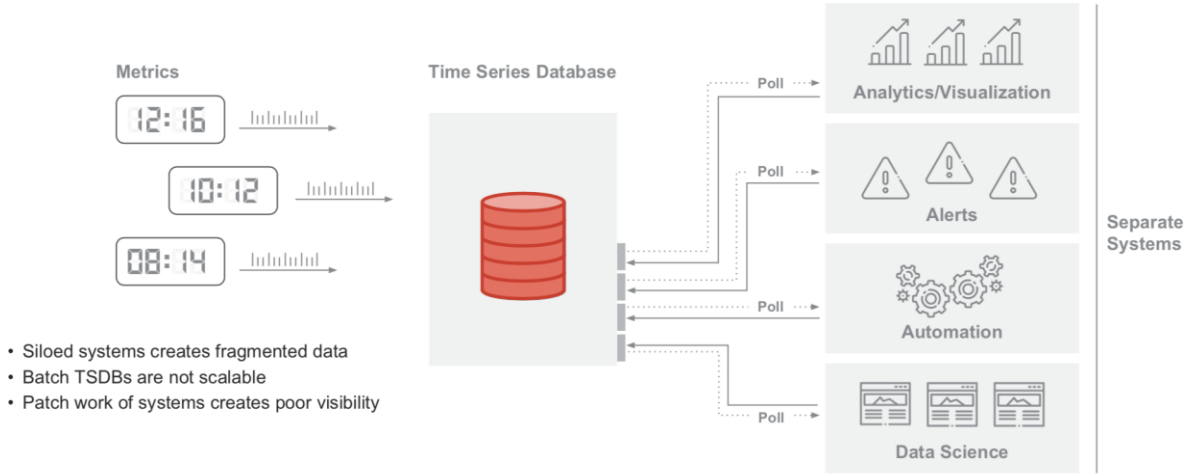
Observability & Stack Trace

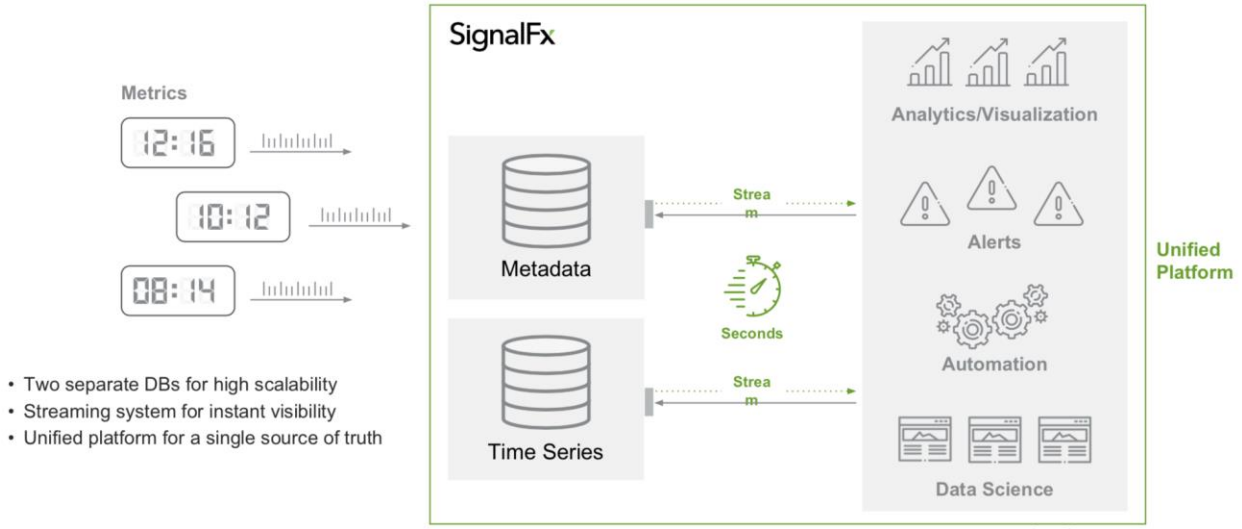


splunk> turn data into doing®

SingalFX 차별성 1/2

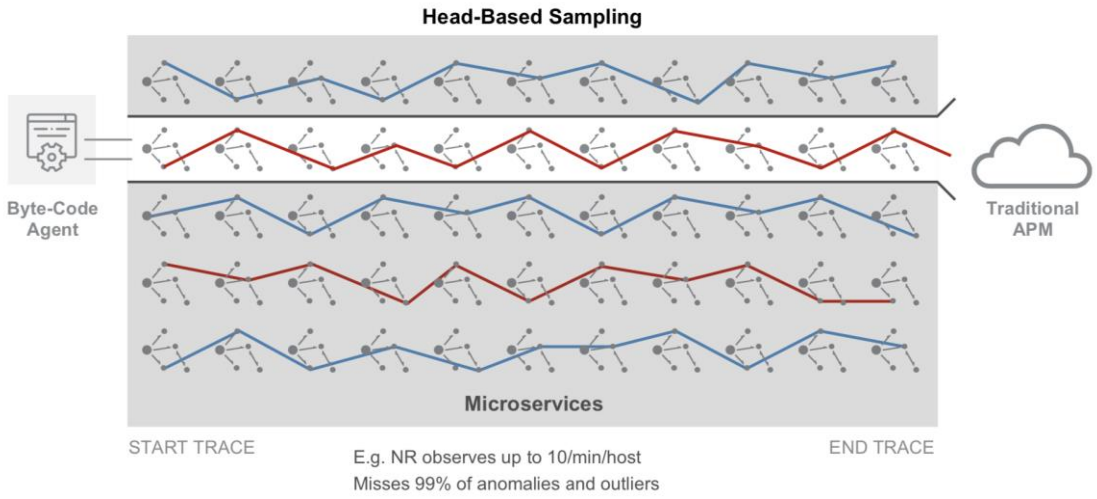
초 단위의 stream 모니터링

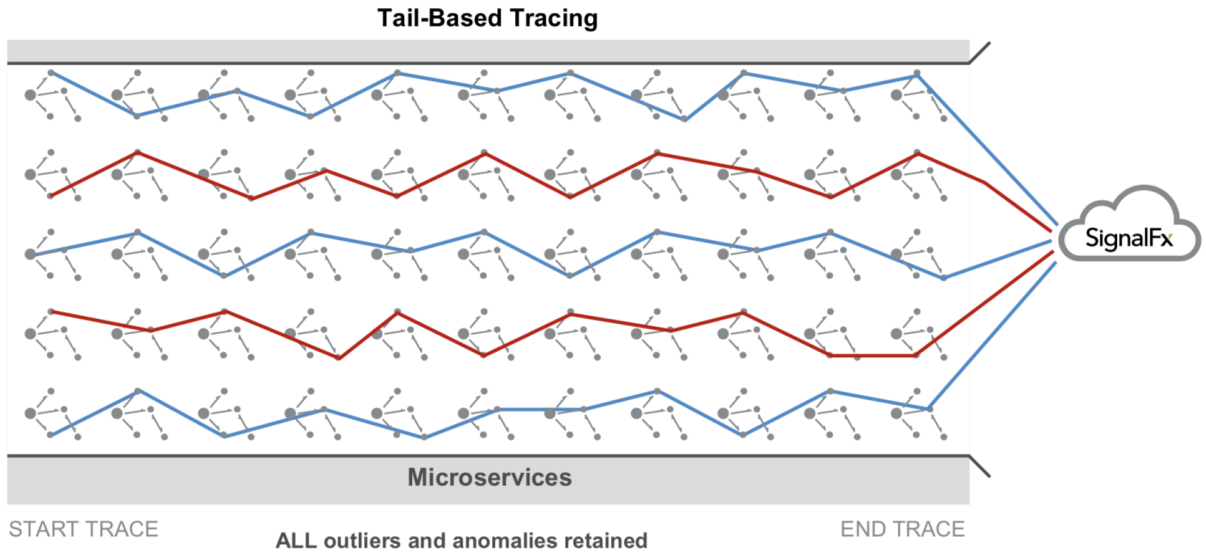




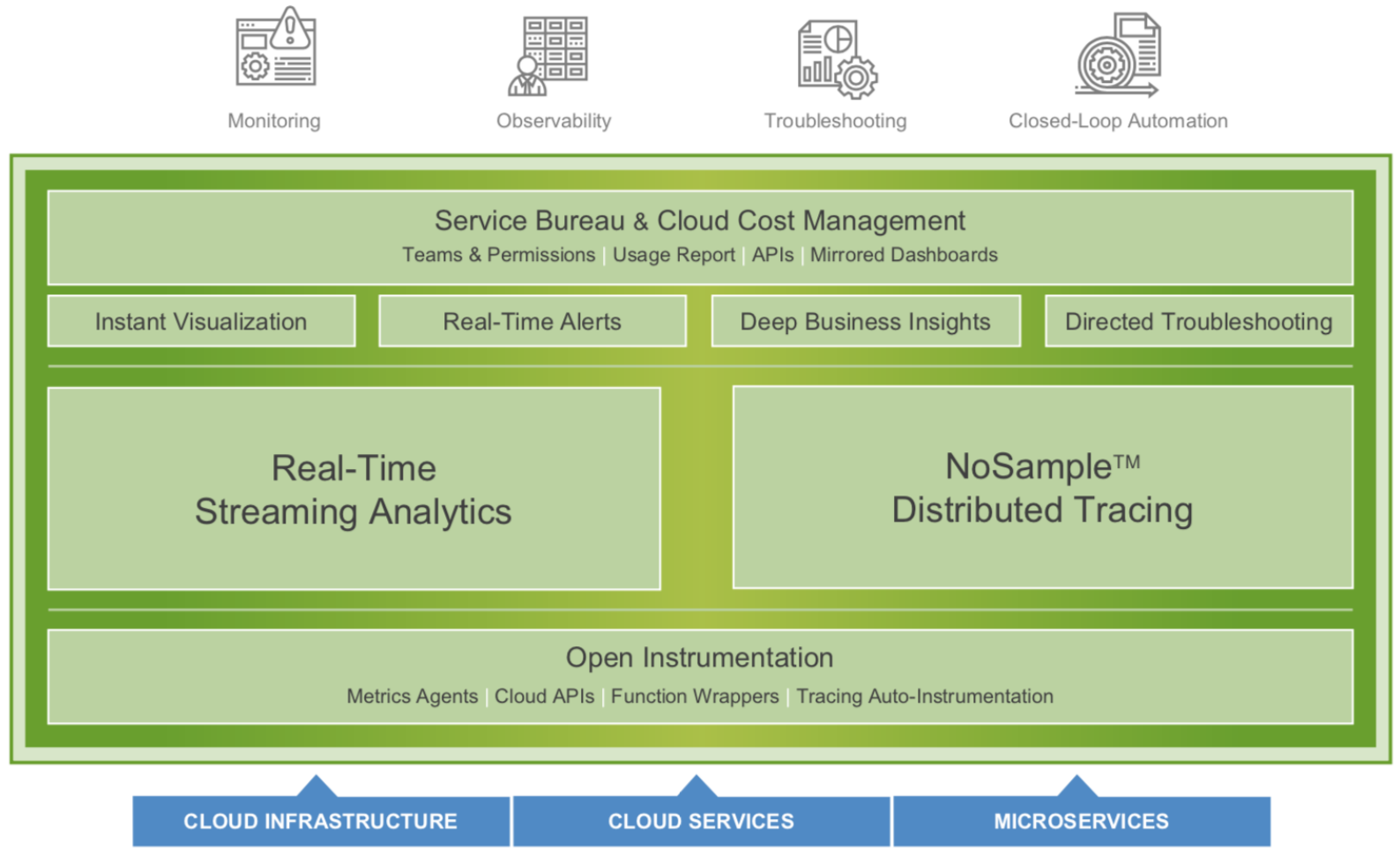
SingalFX 차별성 2/2

NoSample Tail-Based Tracing





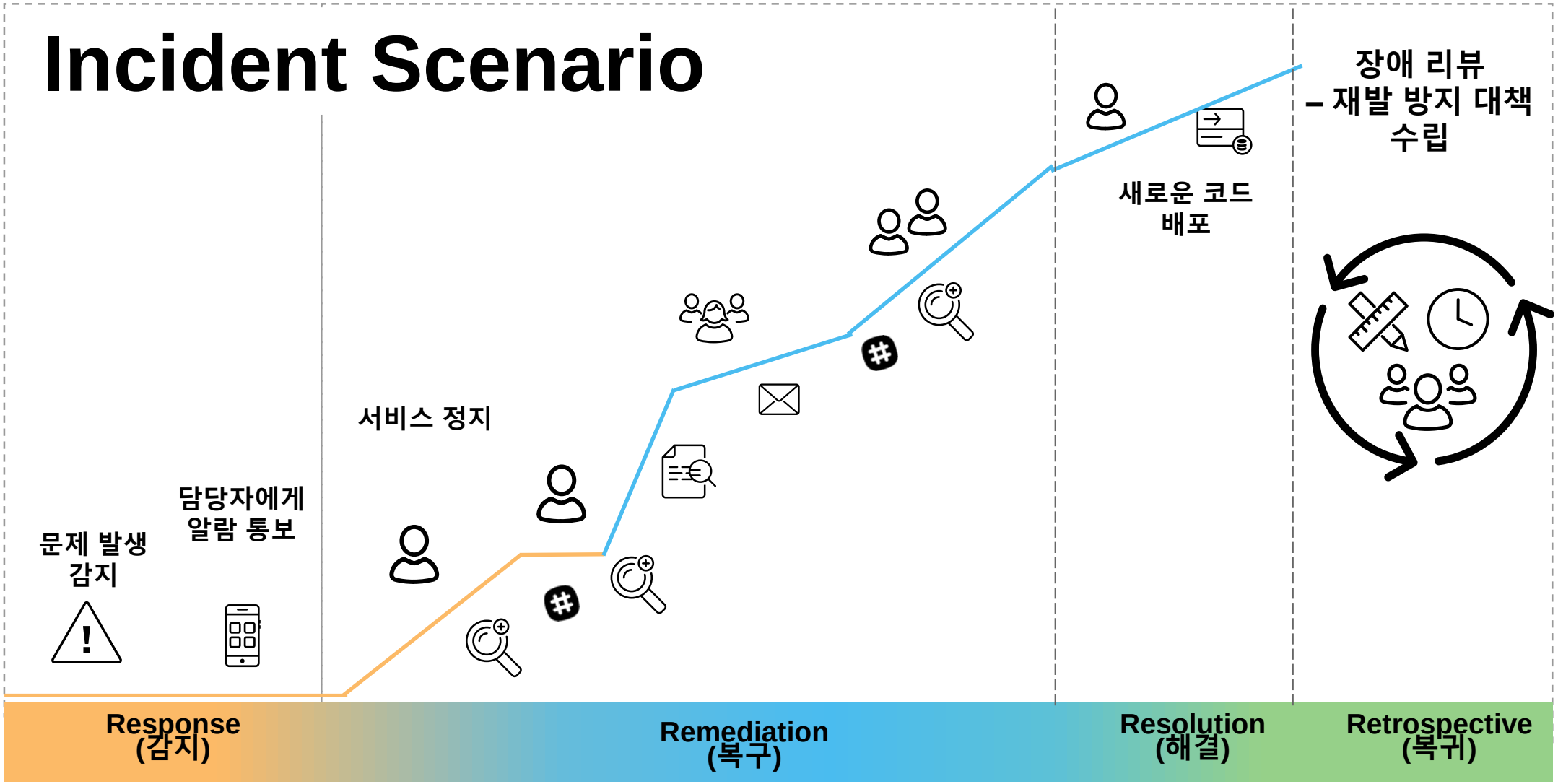
SignalFx 구조



Splunk Investigate

splunk>Forum

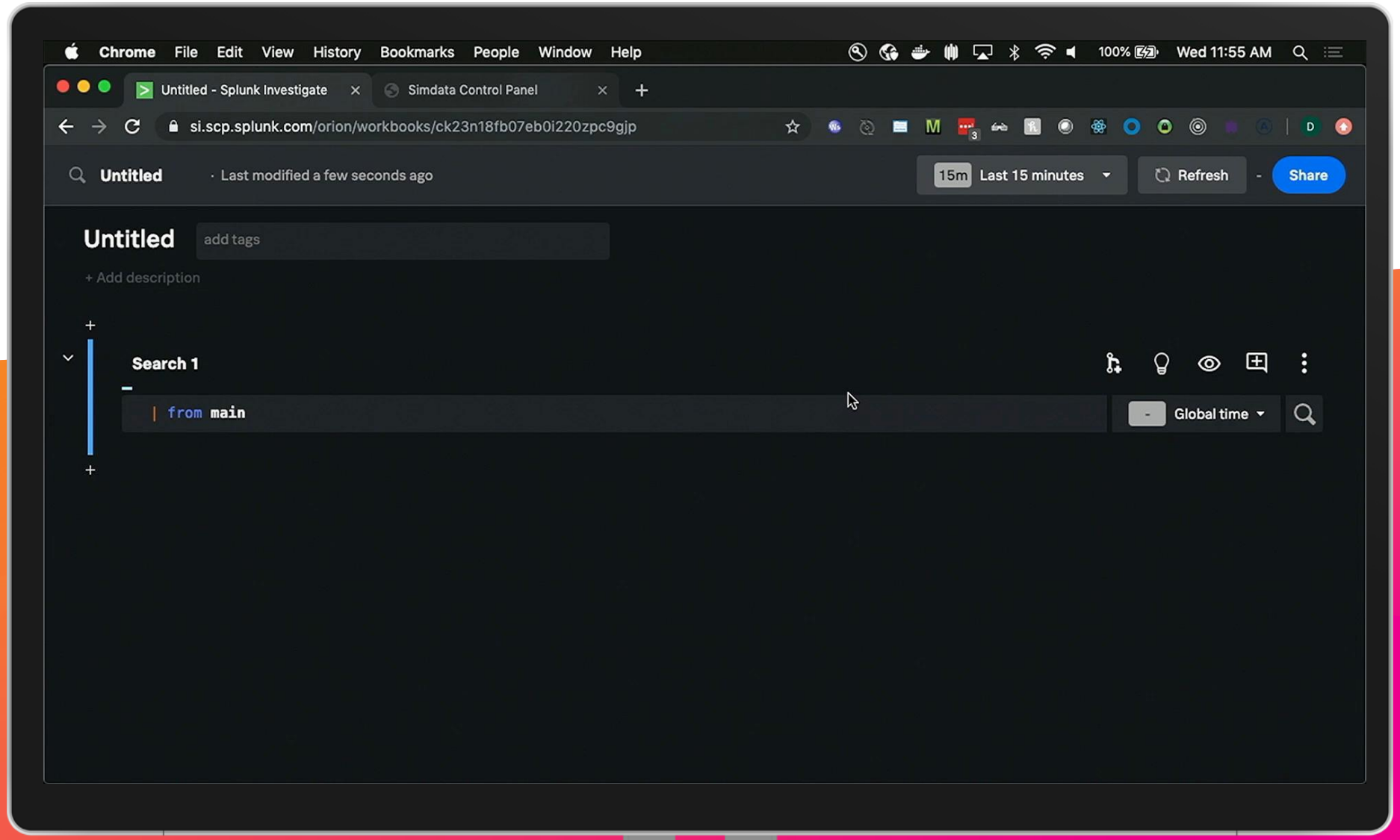
Incident Scenario



8 명 + 6 시간 => $ 2백만

splunk> investigate

*"A **cloud-based** solution with a collaborative interface for **remediating** and **resolving** incidents"*



splunk> turn data into doing

핵심 기능

협업 인터페이스 워크북

Smart Knowledge Object Library

스토리텔링 대시보드

데이터 추가와 정제 워크플로우

신속한 문제 해결을 위한 최적의 솔루션

Multiple Data Sources

Real Time Streaming

Single place to collect + process data

Default connectors: AWS-S3, Cloudwatch, Kinesis

Local Universal Forwarder

Modern Infrastructure

Kubernetes 기반으로 동적 스케일링

멀티 테넌트 아키텍쳐

지속적인 신규 기능 개발

Use-Cases

- ✔ **Remediation (복구)**
- ✔ **Resolution (해결)**
- ✔ **Retrospective (복귀)**

Business Outcomes

장애 처리 시간 경감

빠른 원인 탐색

재발방지

Across Disparate Teams…

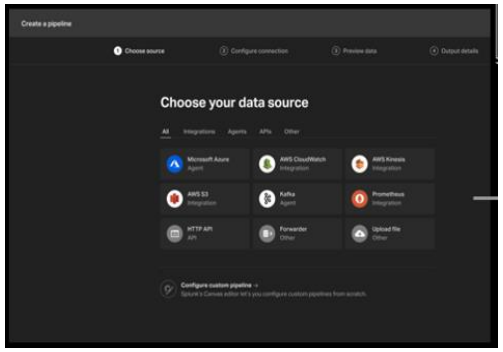
개발자

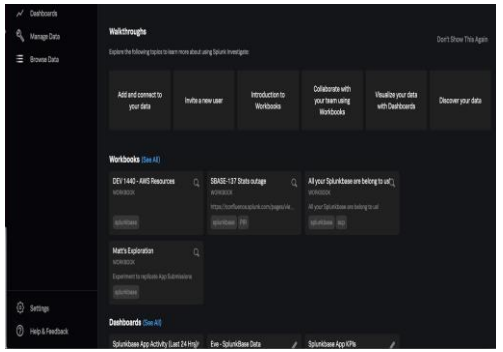
SREs

PM

경영자

Splunk Investigate
지금 바로 시작하세요





Step 1.

http://si.scp.splunk.com/

에서 무료사용 등록

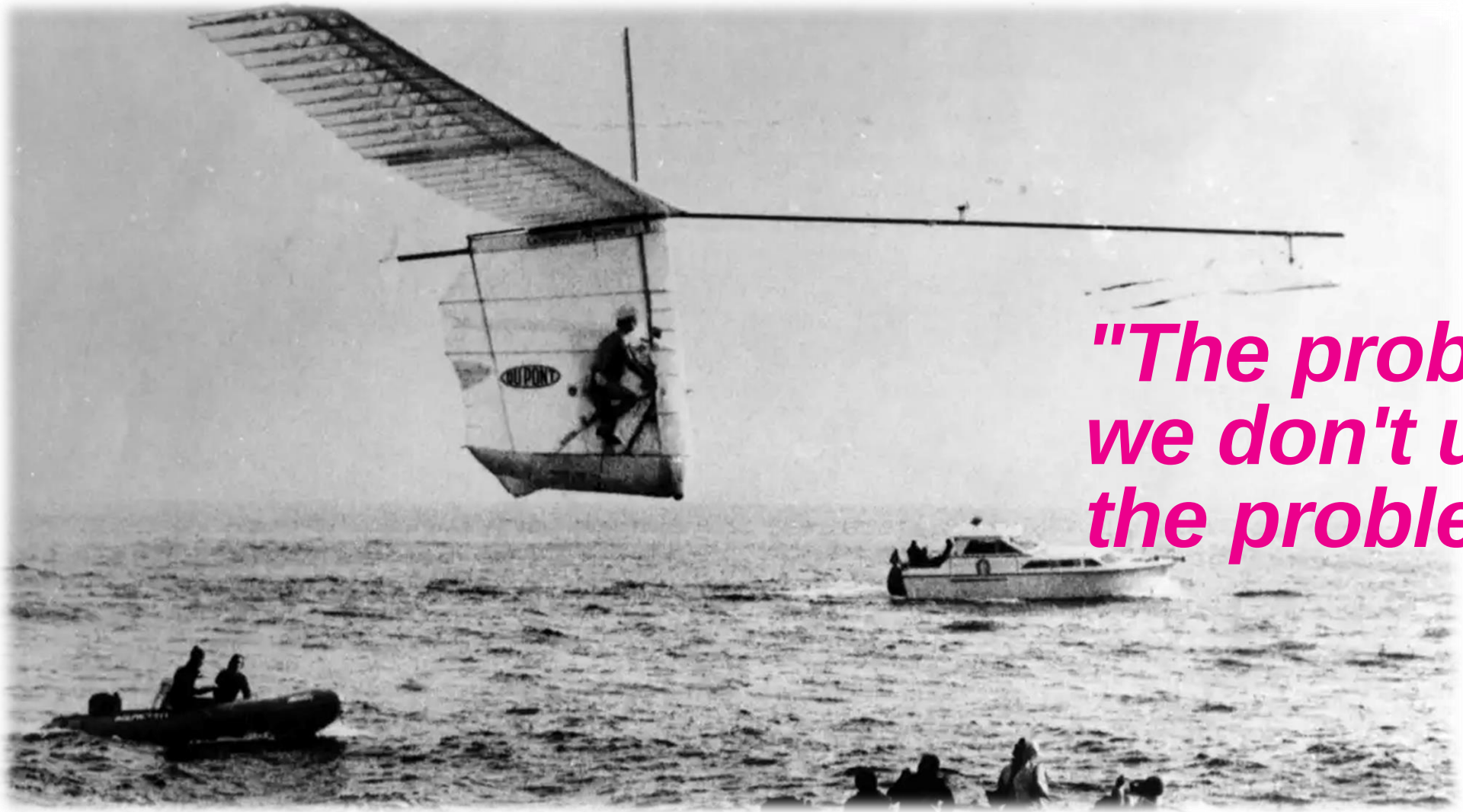
Step 2.

데이터 업로드

Step 3.

Splunk
Investigate 시작

splunk> turn data into doing

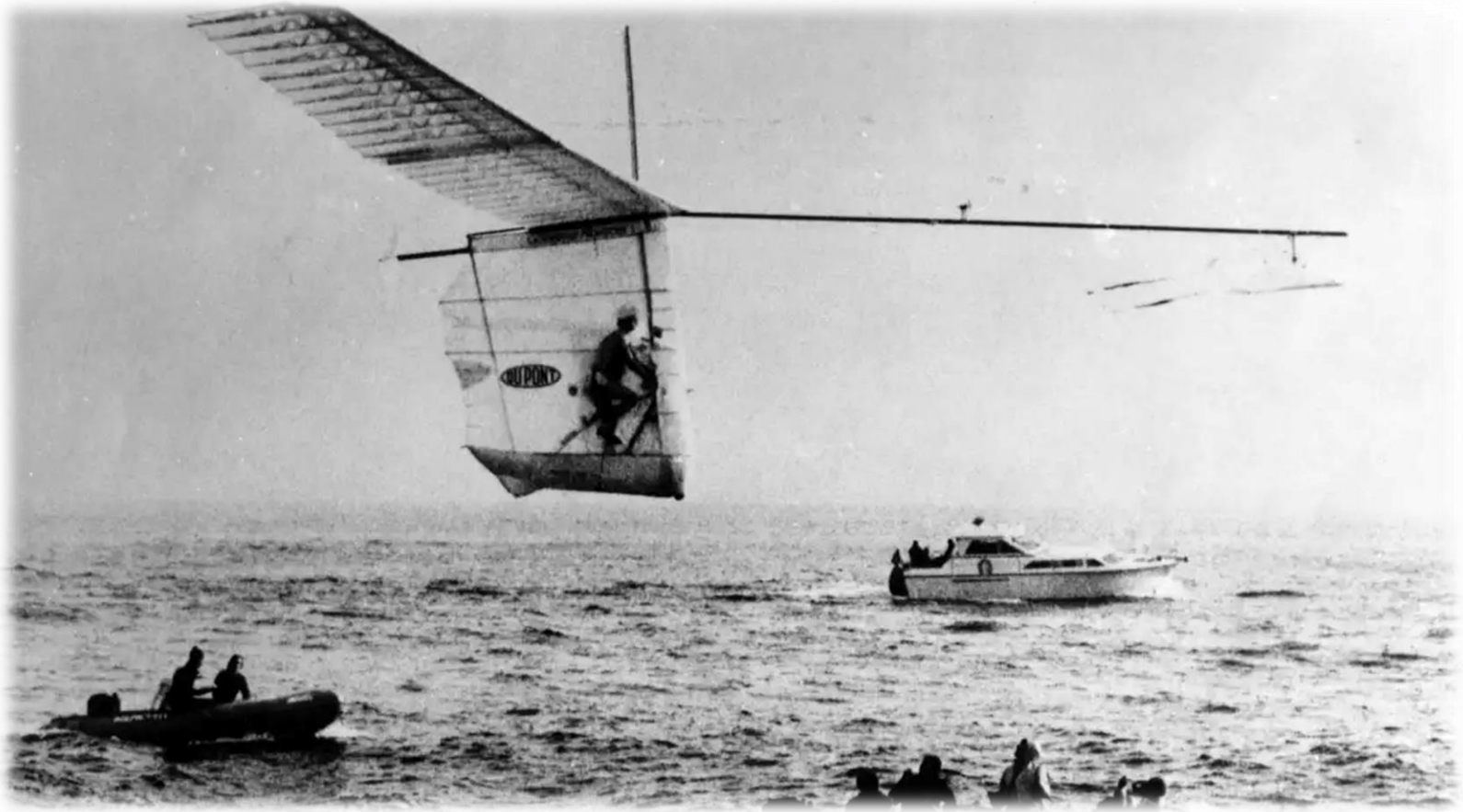


"The problem is that we don't understand the problem."

1979년 영국 해협을 횡단한 Paul McCready의 Gossamer Albatross

감사합니다

왜 Micro Service 인가?



1979년 영국 도버 해협을 횡단한 Paul McCready의 Gossamer Albatross

1959 Henry Kremer

사람의 힘만으로 움직이는 항공기

50,000

17

Paul McCready

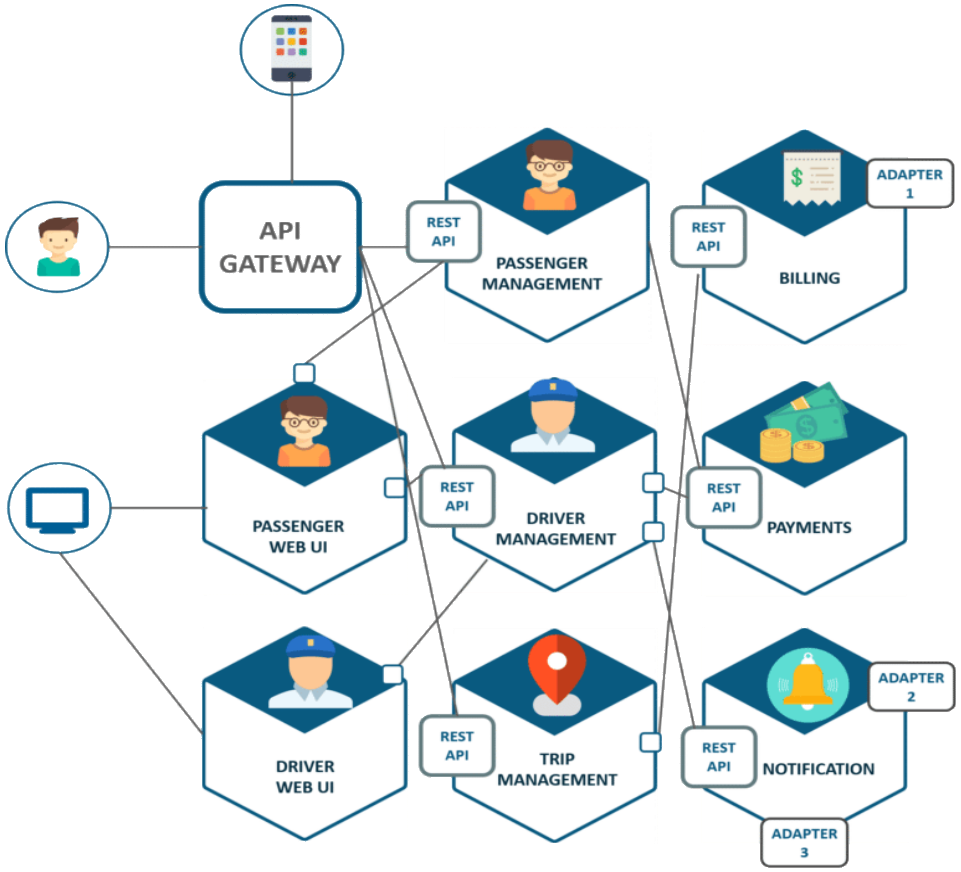
1977

Gossamer Condor

223

4

Microservice 예제 (UBER)



https://medium.com/edureka/microservice-architecture-5e7f056b90f1