

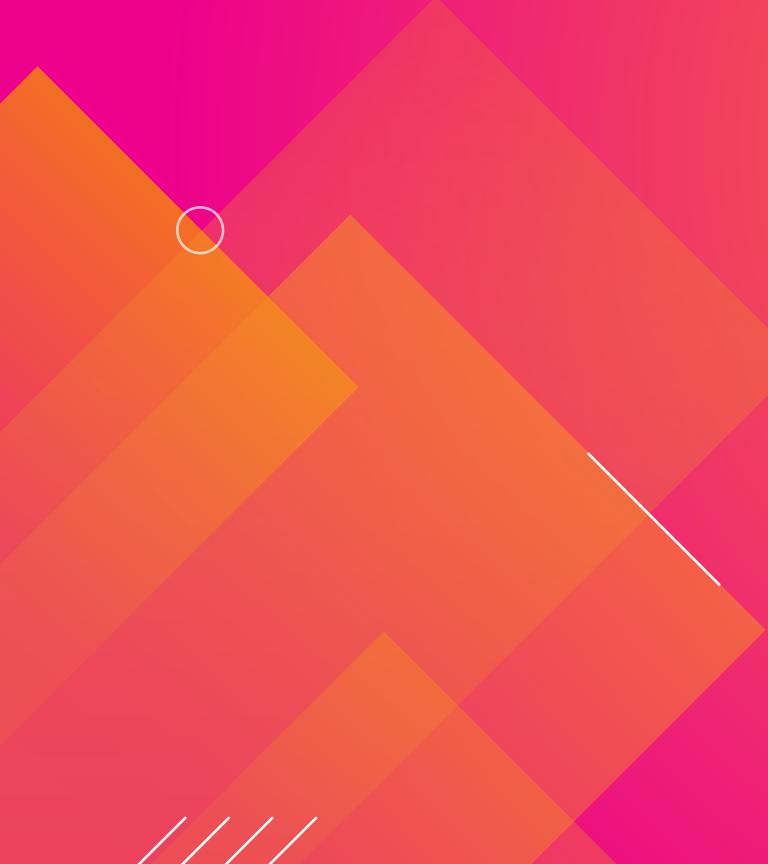
# Splunk for ITOps + DevOps

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 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. © 2019 Splunk Inc. All rights reserved.

# Agenda

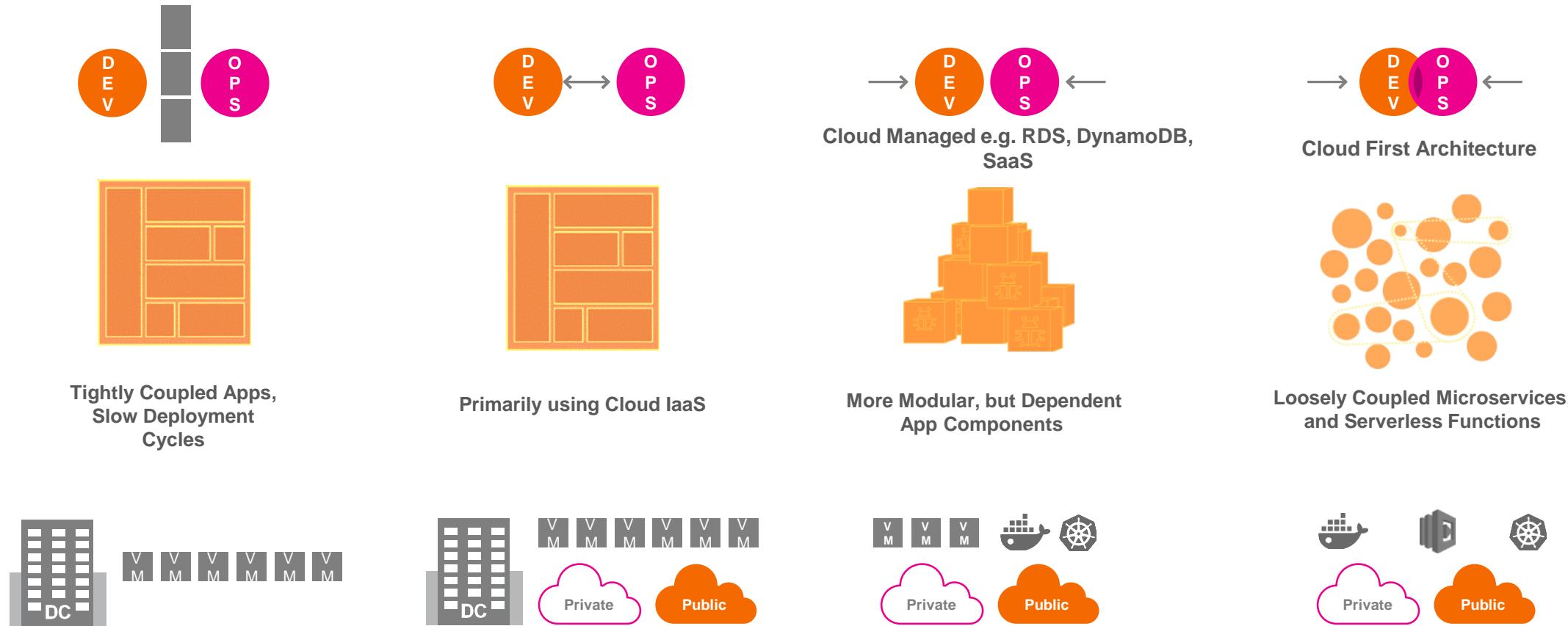
- 1) Splunk's Vision for New IT**
- 2) Splunk for IT Ops**
- 3) SignalFX**
- 4) Splunk Investigate**

# Splunk's Vision for New IT

splunk>Forum

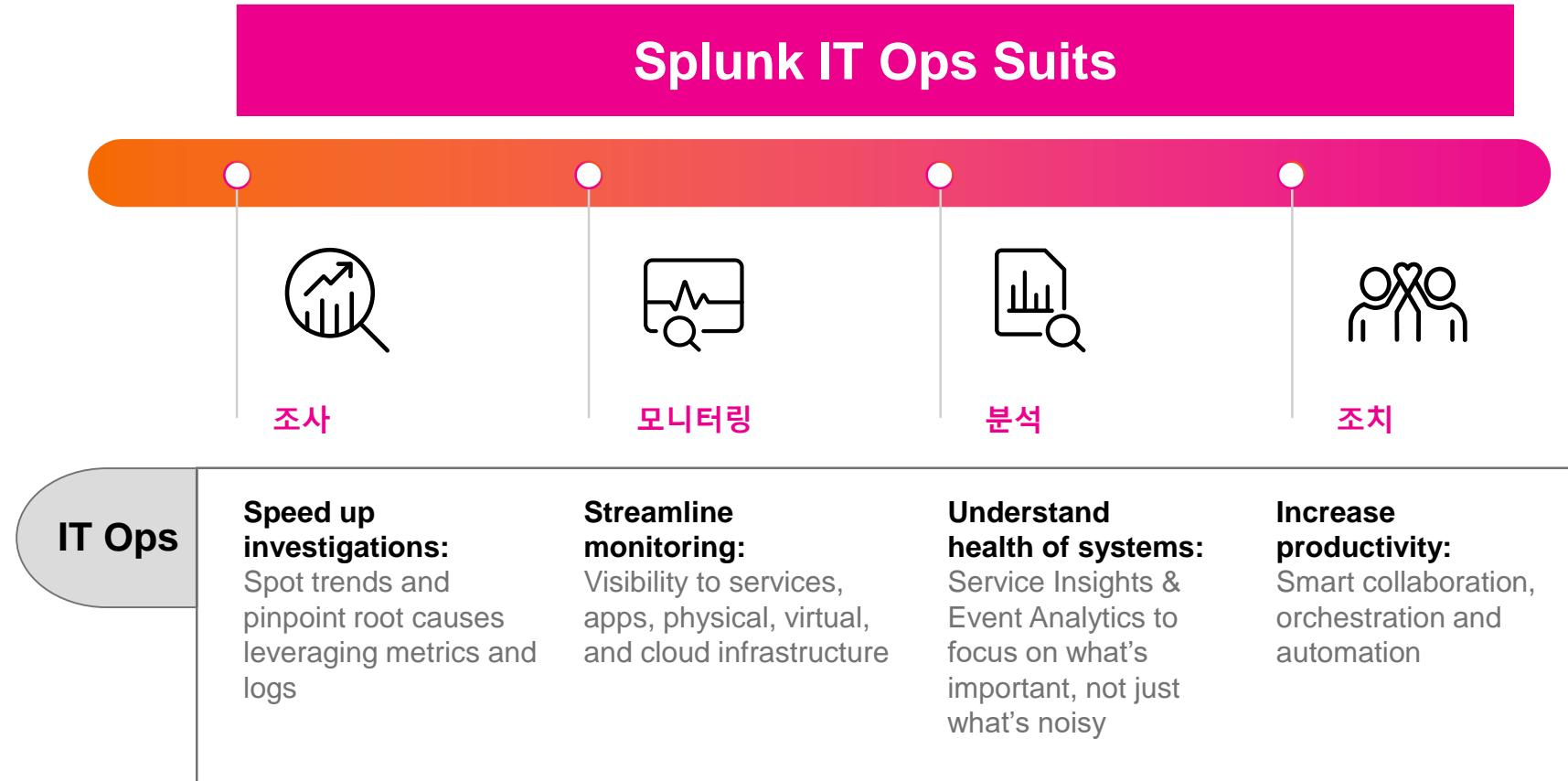
# App 개발과 운영을 위한 환경은 변하고 있습니다

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



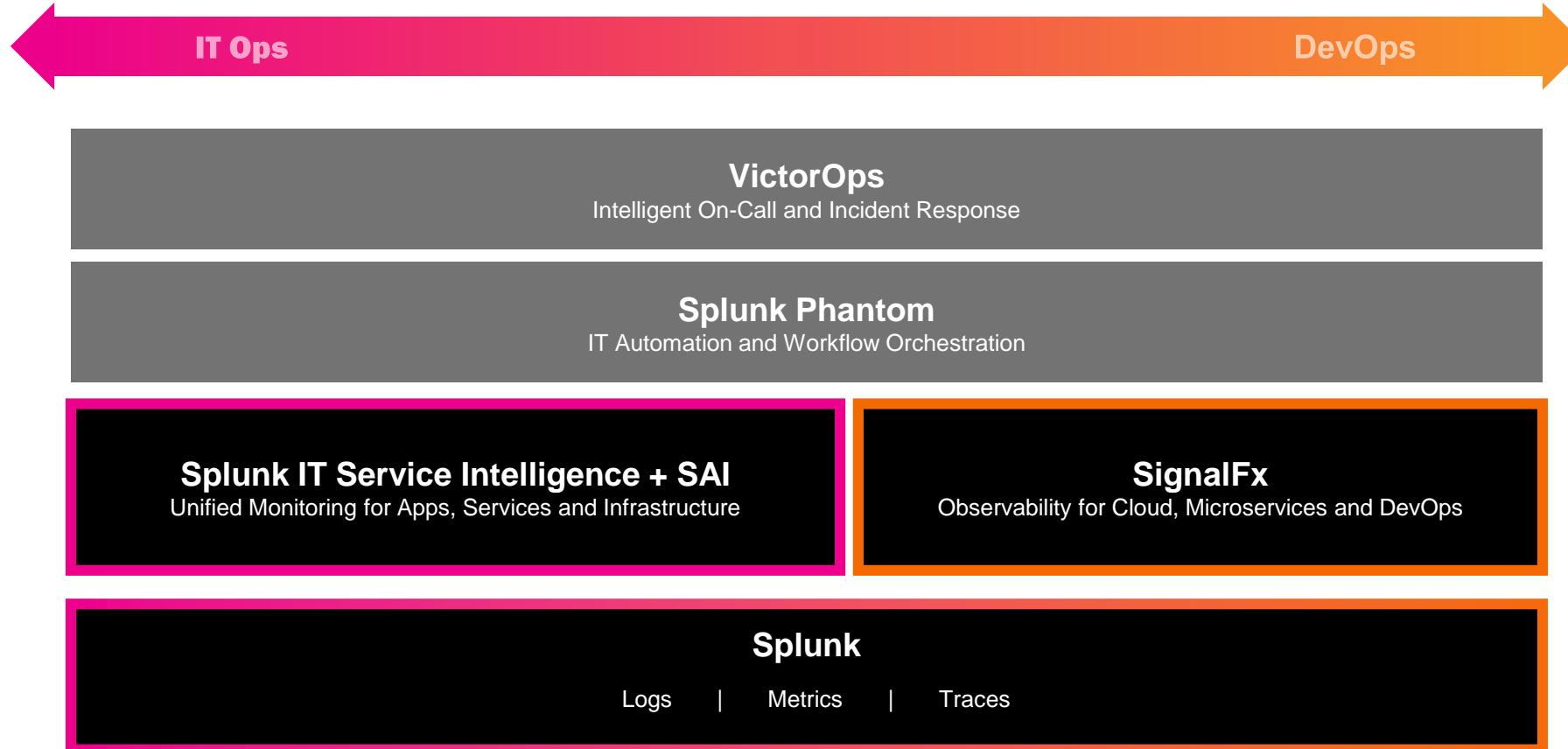
# Data-to-Everything for IT Ops

Faster time to business outcomes



# NEW IT / DEV 환경을 위한 SPLUNK 포트폴리오

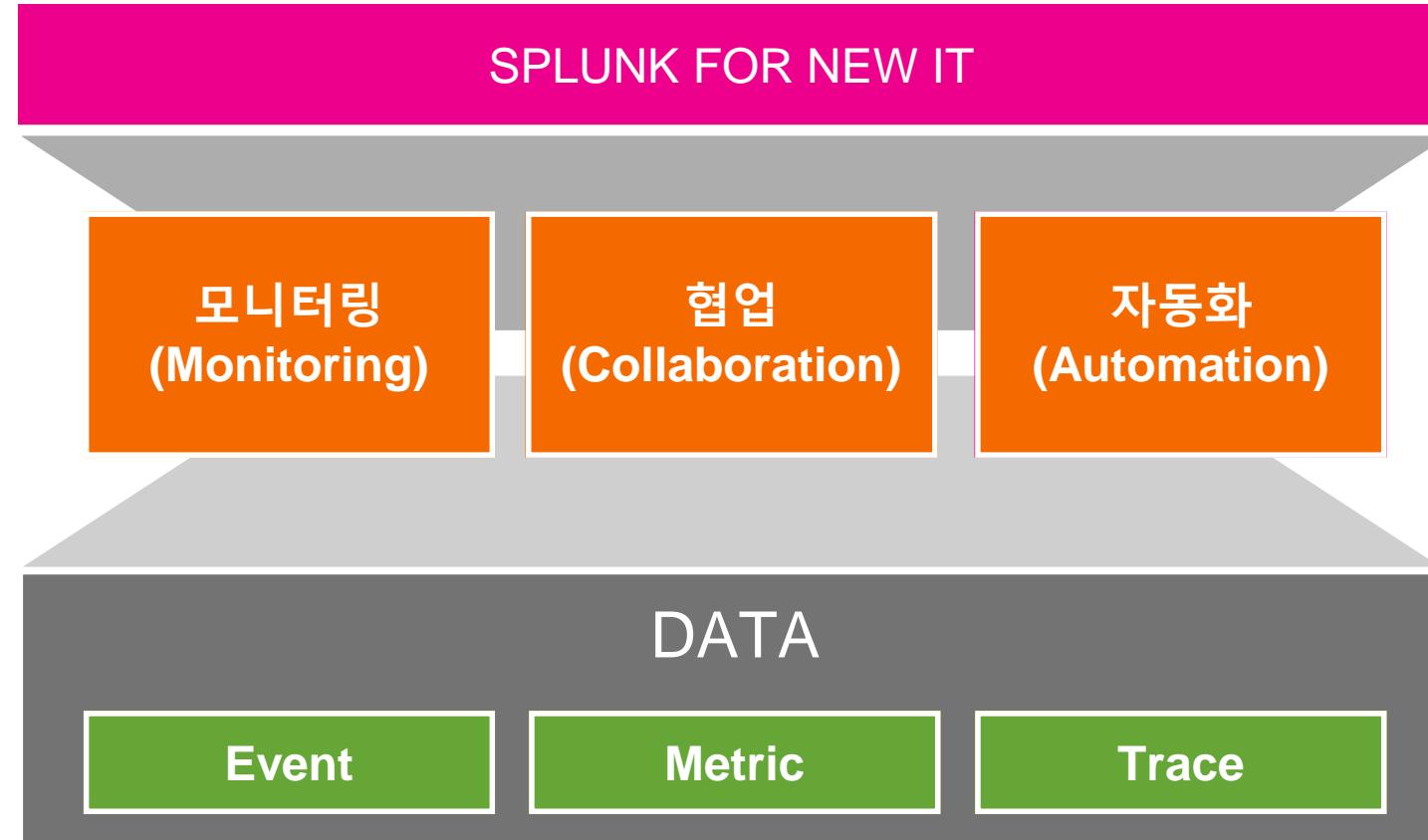
The only platform for monitoring, observability & AIOps - every app, every team



# Splunk for IT Ops

splunk>Forum

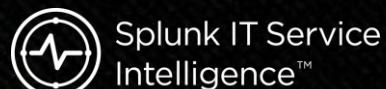
# New IT 환경을 위한 Splunk의 세가지 주요 기능



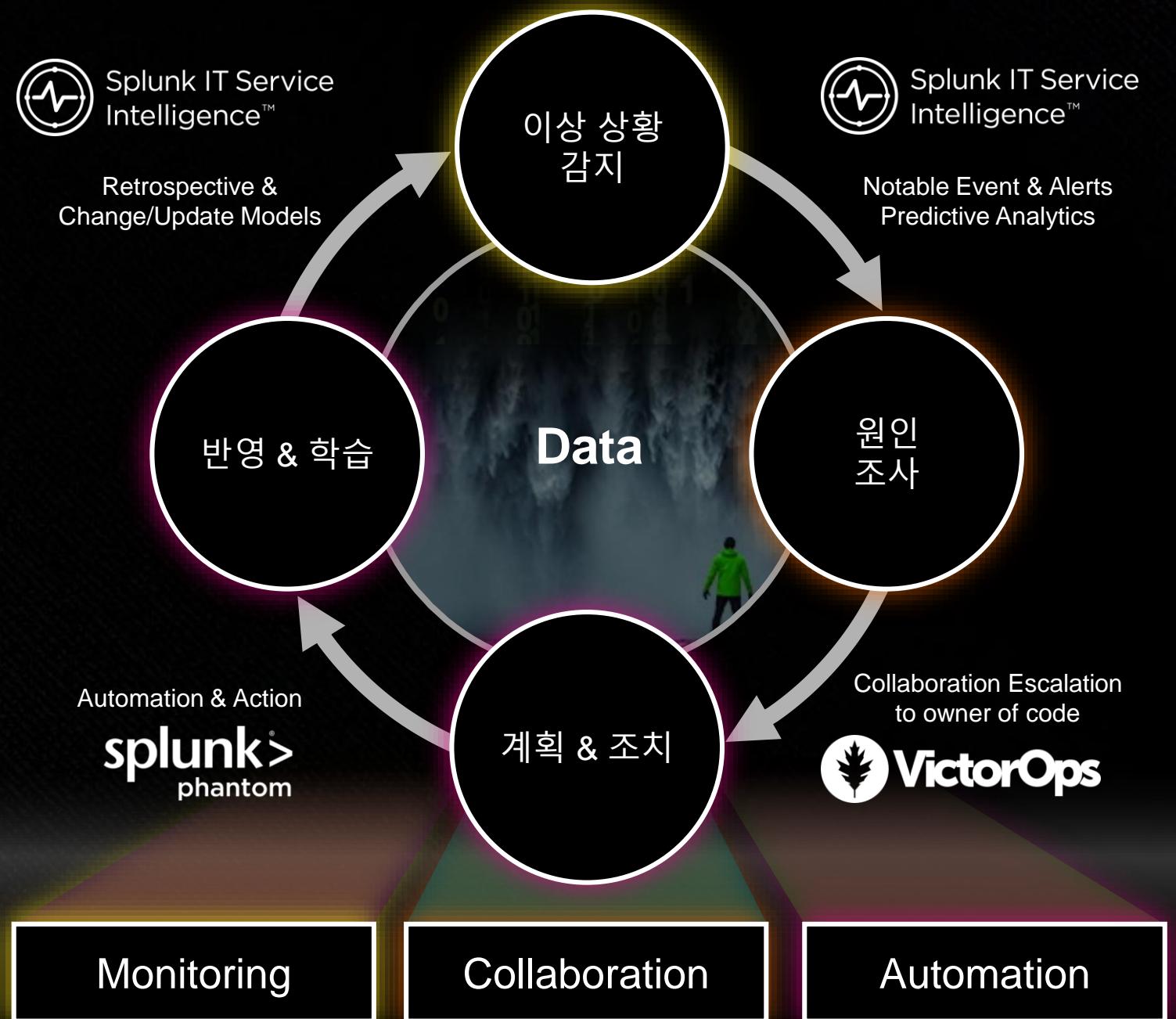
# Splunk for ITOps

The Modern Suite of Solutions  
for the New IT Operations

splunk®



splunk®  
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

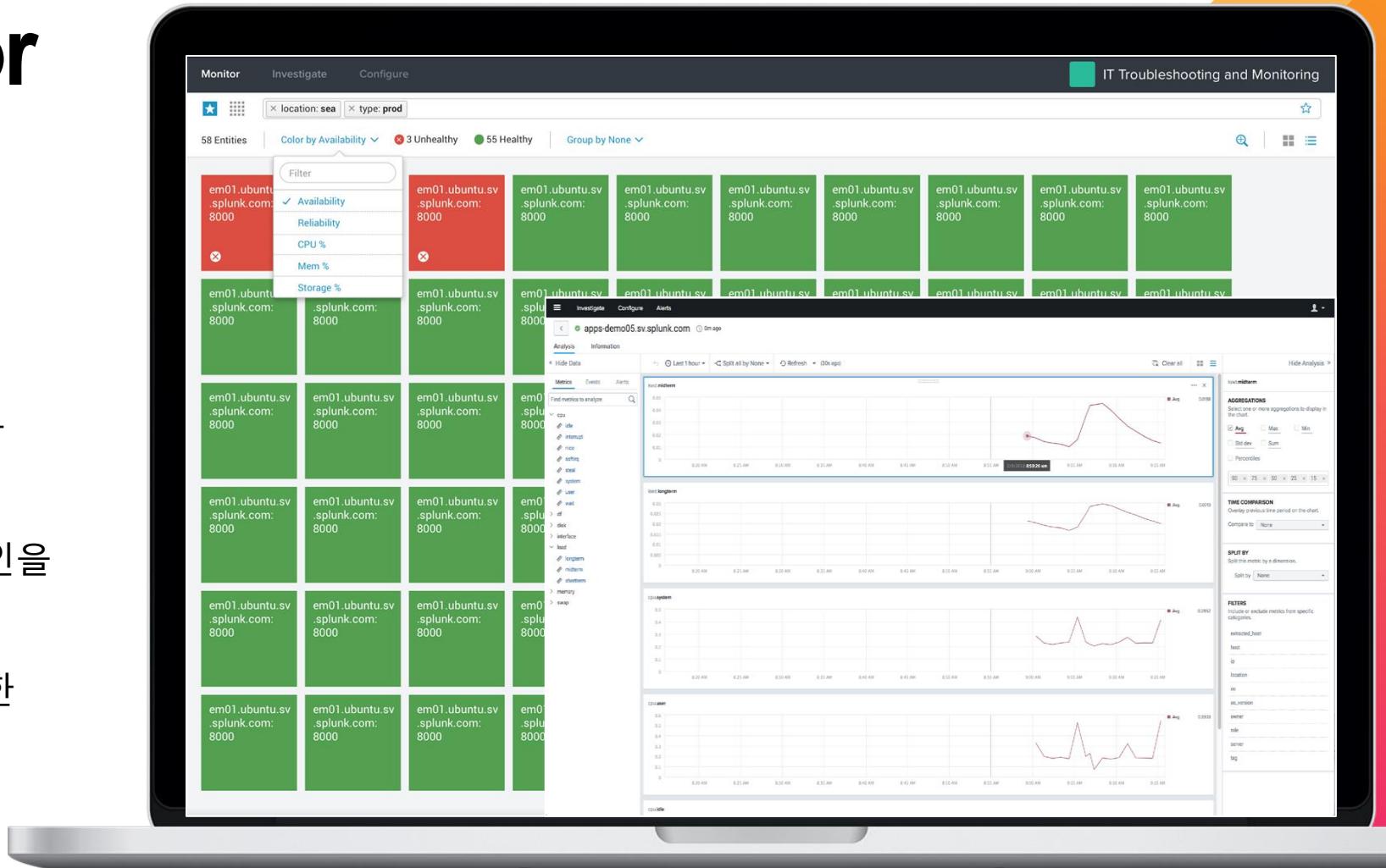
## AIOps On-Prem & Cloud Platform

확장 가능하고 최신 아키텍처를 지원하는 AIOps 플랫폼



# Splunk App for Infrastructure

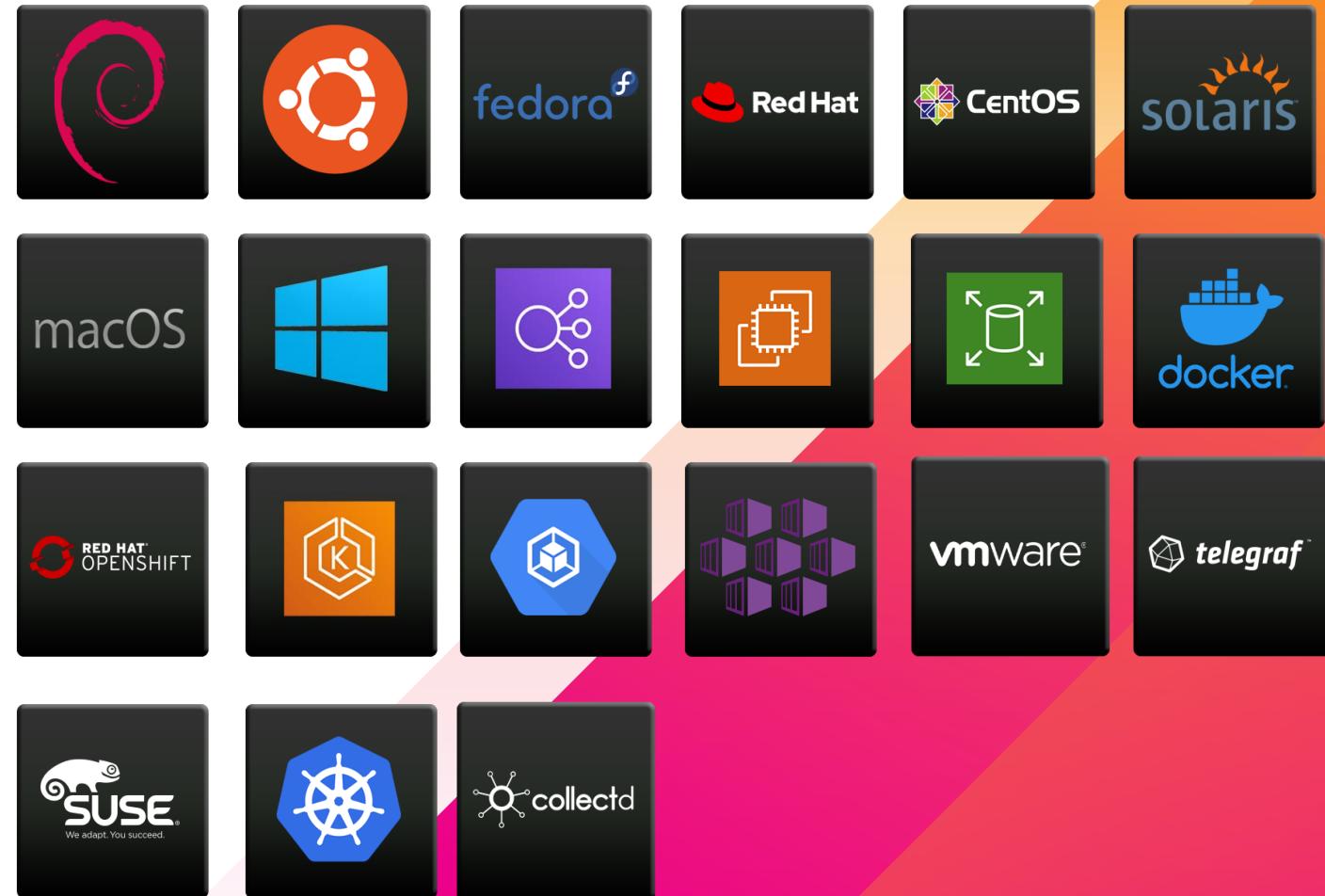
- 다양한 OS, VM, 클라우드, 컨테이너 모니터링을 위한 앱
- 빠른 가치 실현 : 손쉬운 설정을 통한 데이터 수집
- 가이드 기반으로 트렌드와 장애 원인을 빠르게 조사할 수 있도록 지원
- 지표와 로그에 대한 유연하고 다양한 형태로 분석할 수 있는 기능 지원
- ITSI 통합 기능 제공
- Splunk Cloud 지원



# 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

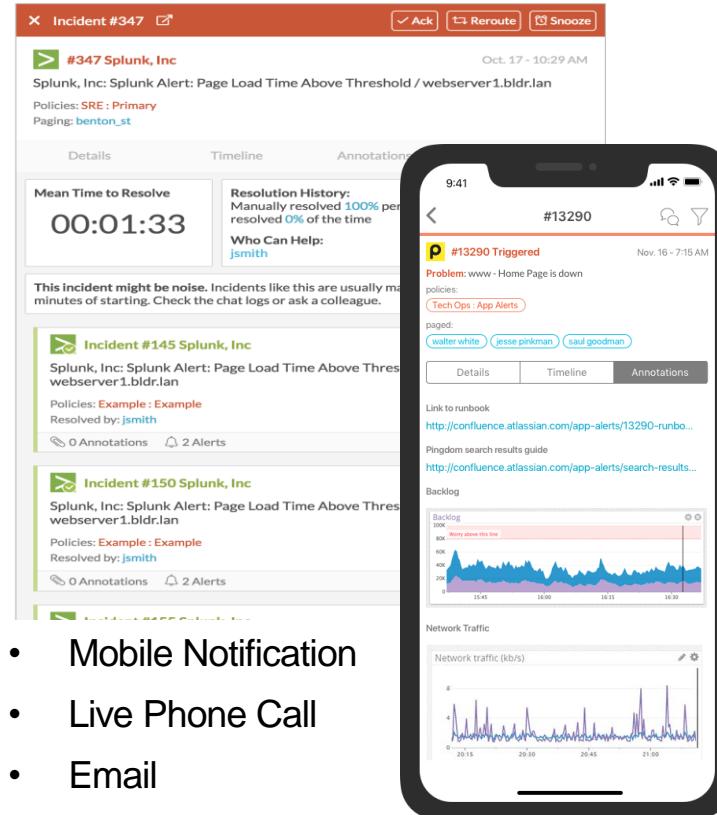
Splunk 포함 다양한 모니터링 툴에서 발생한 경고를 Right Team / People 이 처리 가능토록 지원

## Alarm



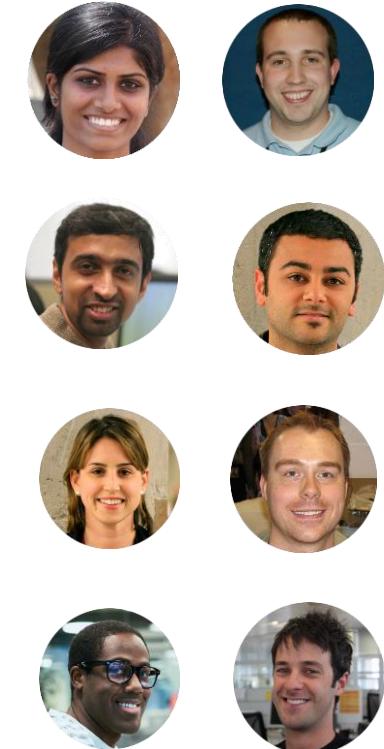
모니터링 툴에서 경고 발생 시  
해당 정보를 VictorOps로 전달

## Routing / Collaboration



VictorOps는 해당 경고를 처리하기  
위한 적합한 팀/사람을 할당

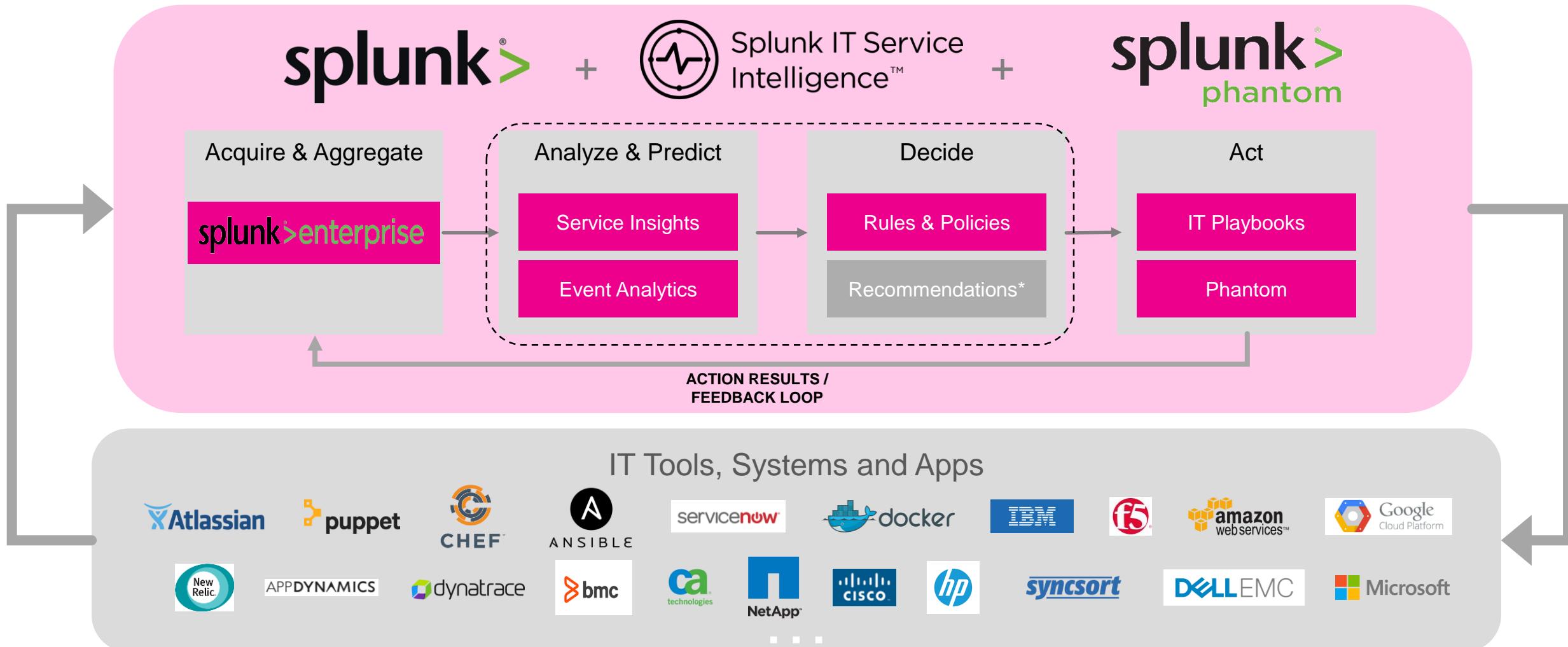
## Action



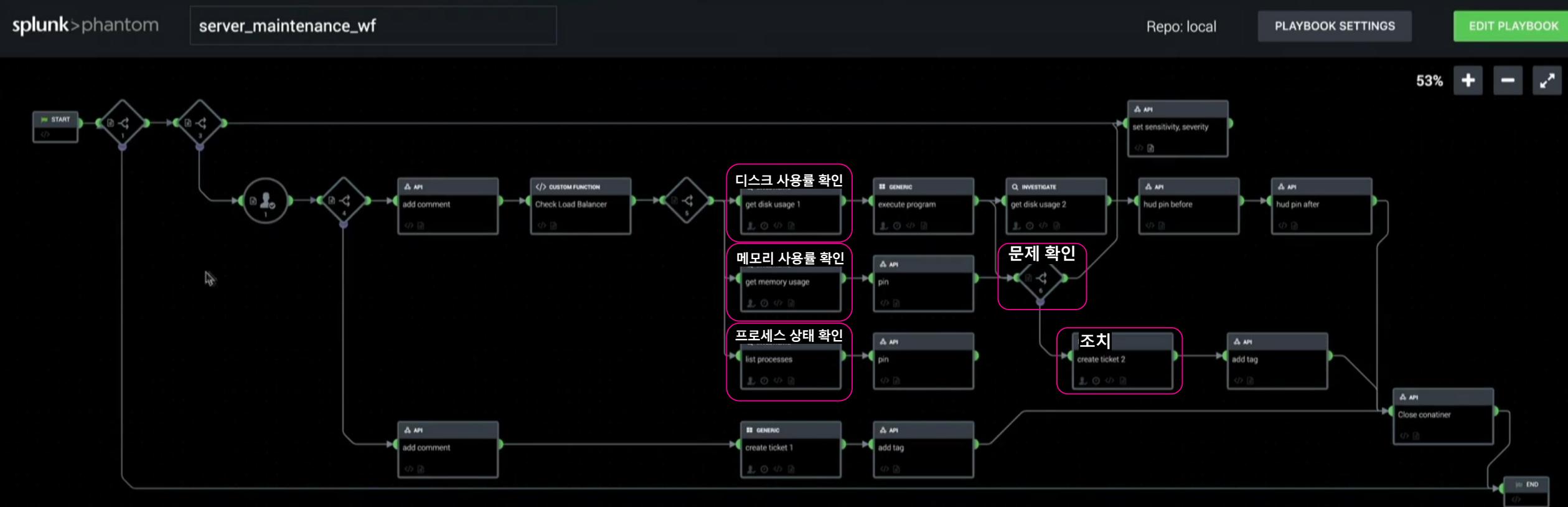
팀/사람은 VictorOps의 협업 기능을  
통하여 장애 처리 수행

**splunk** > turn data into doing

# Phantom – ITOps Automation



# Phantom – Playbook for ITOps



# Key IT Apps & Actions

Available in Phantom v4.3

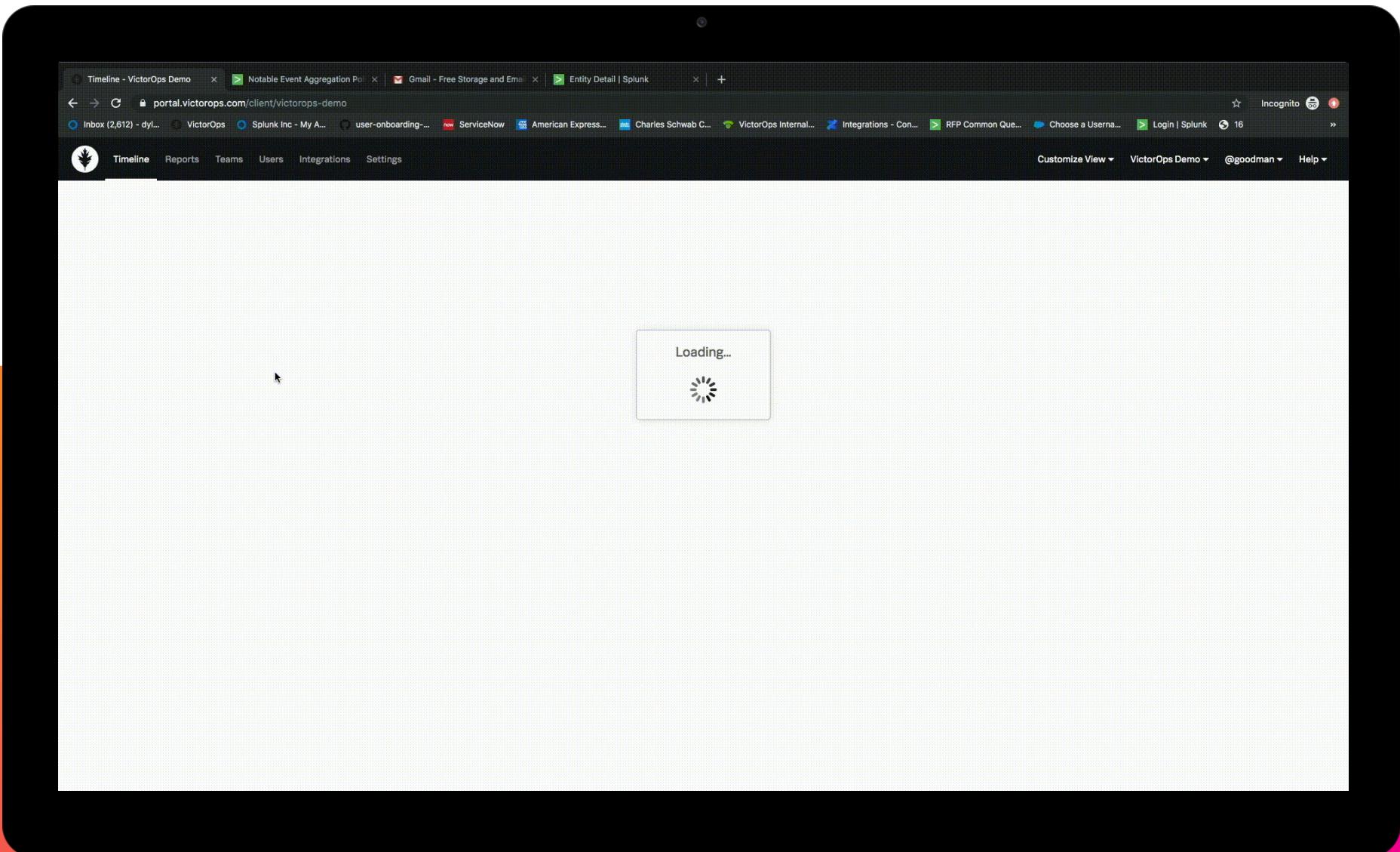
70+  
Apps

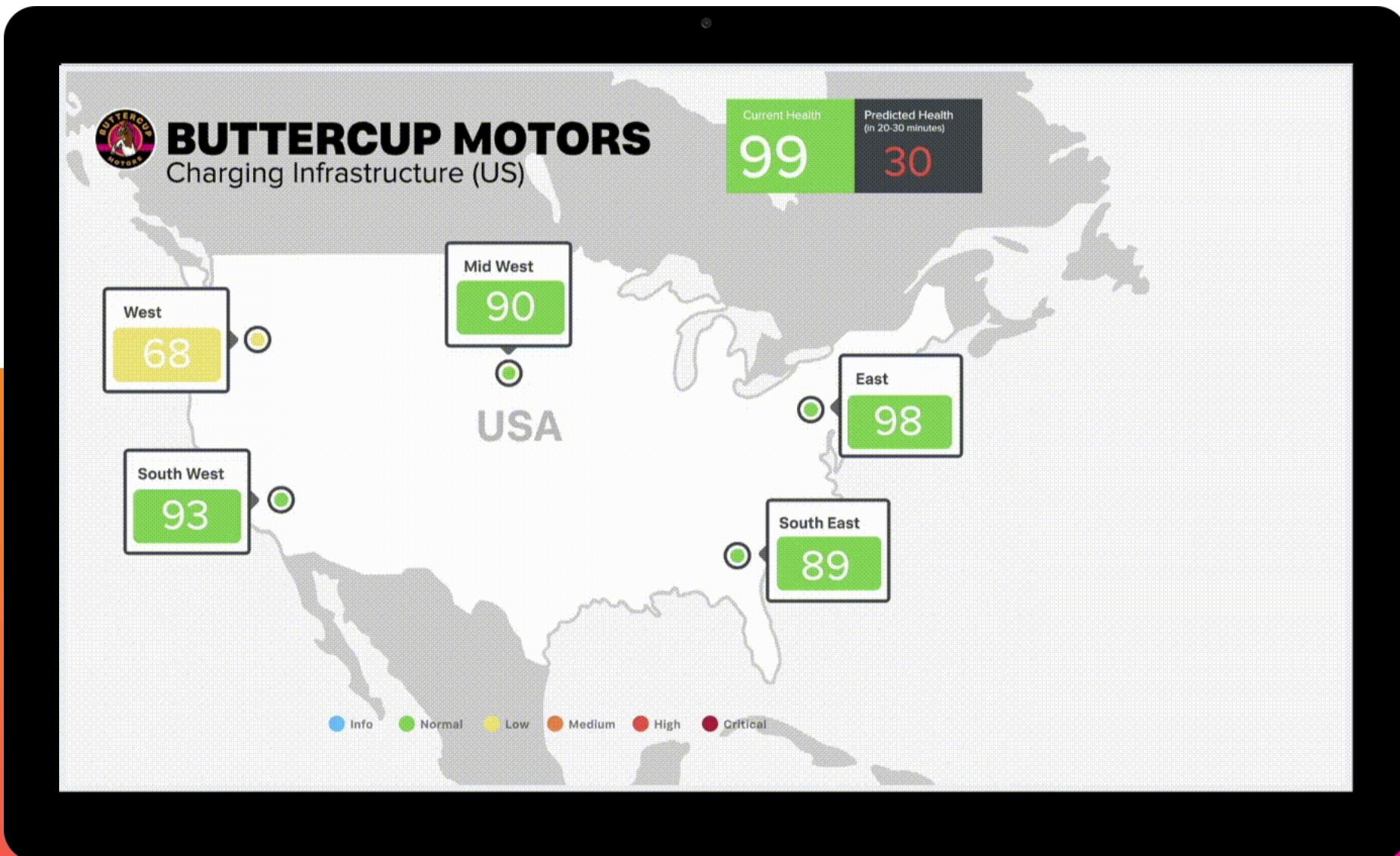
500+  
Actions

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









The screenshot displays the VictorOps platform interface, which integrates with Splunk for event aggregation and management. The top navigation bar includes links for Customer Transactions, Notable Event Aggregation, Gmail, Entity Detail, and various Splunk and external service links. The main menu features Timeline, Reports, Teams, Users, Integrations, and Settings.

**Timeline View:** This section shows a feed of recent activity. It includes a search bar, filters, and a list of events. One event from Nagios is highlighted, detailing a CFEngine Runlog warning on a host named haproxy2.pr.bldr01. The output shows a FILE\_AGE WARNING for a log file that is 305 seconds old and 9665030 bytes large. The host is UP, and the output indicates PING OK with a low RTA.

**Incident View:** This view is for Incident #79914, triggered on Oct 22, 2019, at 3:03 PM. It shows the incident details, including the API (Customer Transaction Issue), policies (Database: Primary, Infrastructure: Infrastructure, Database: On-call), and acknowledgments (goodman). It also lists the paging contact (pinkman) and a note stating the incident will stay triggered until all parties have acknowledged. The annotations tab is selected, listing eight specific annotations related to the incident.

# ITOps 강화를 위한 지속적인 투자



**VictorOps**

Incident Management



**phantom<sup>®</sup>**

Automation

# SignalFx

DevOps & Container Monitoring

**omnition**

Distributed Tracing

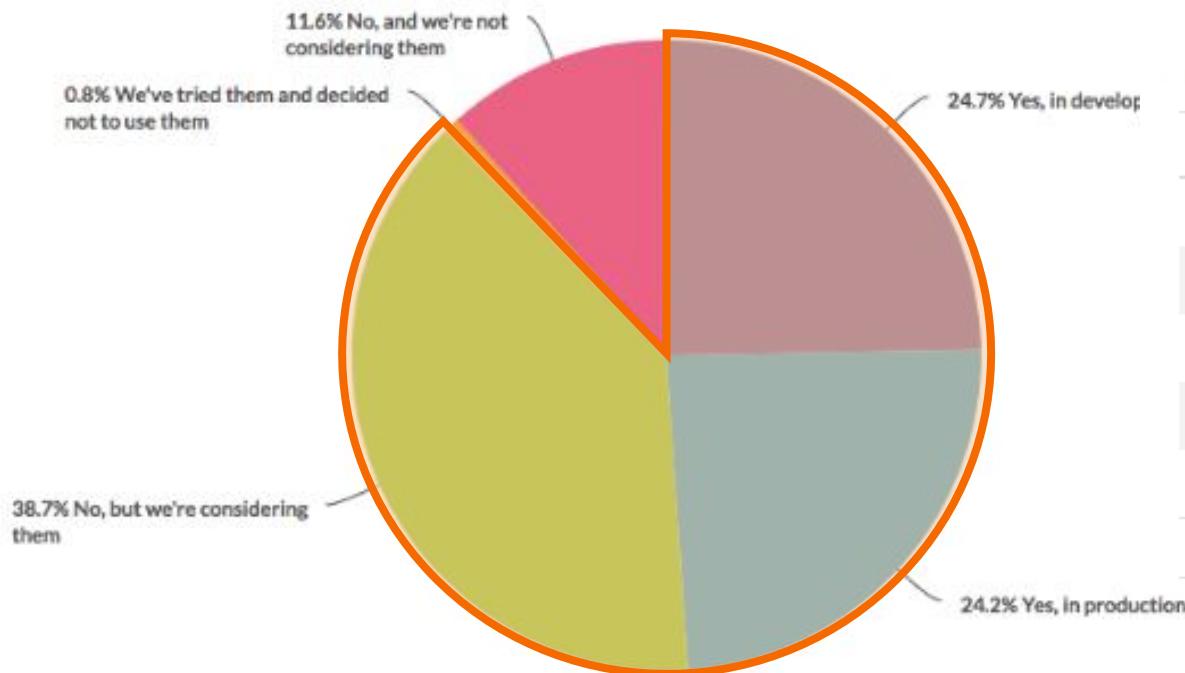
**streamlio**

Real time stream processing

# SignalFX

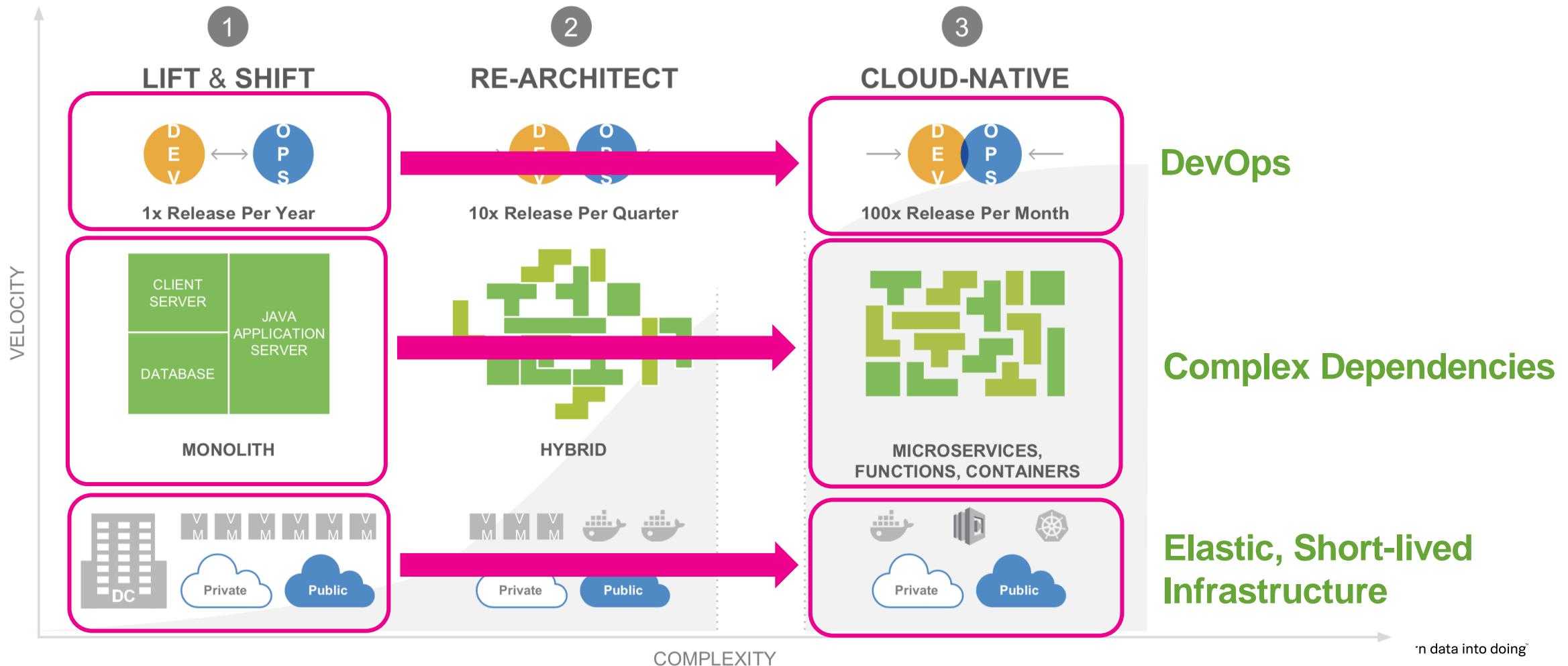
splunk>Forum

# Micro Service 인기

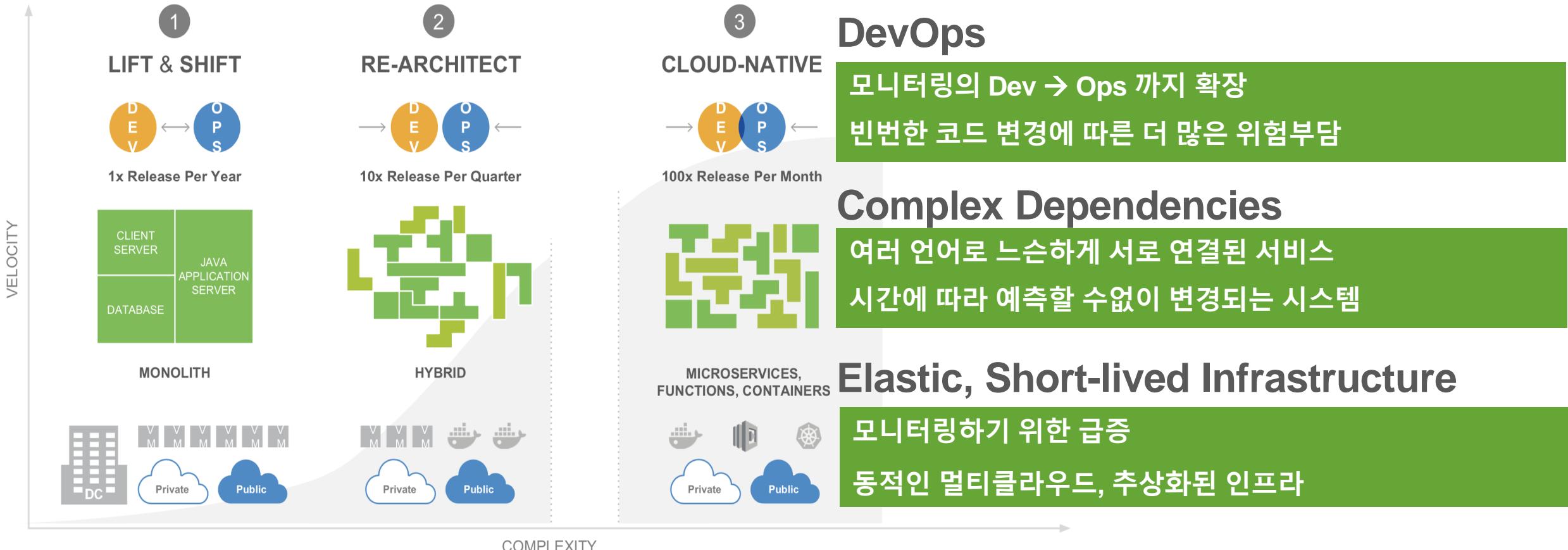


[출처: 2018 DZone Research]

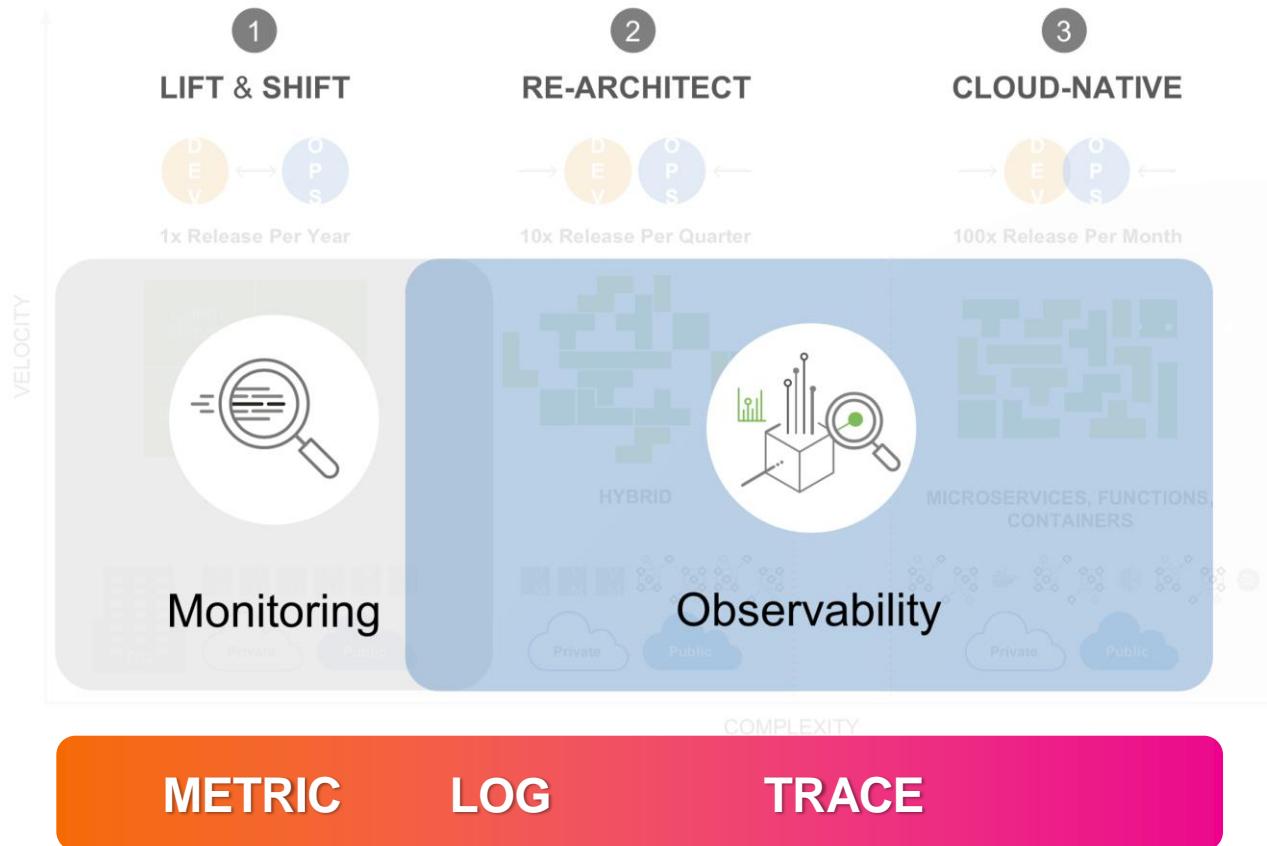
# Cloud-Native 로의 전환



# Cloud-Native 와 모니터링 도전



# 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?

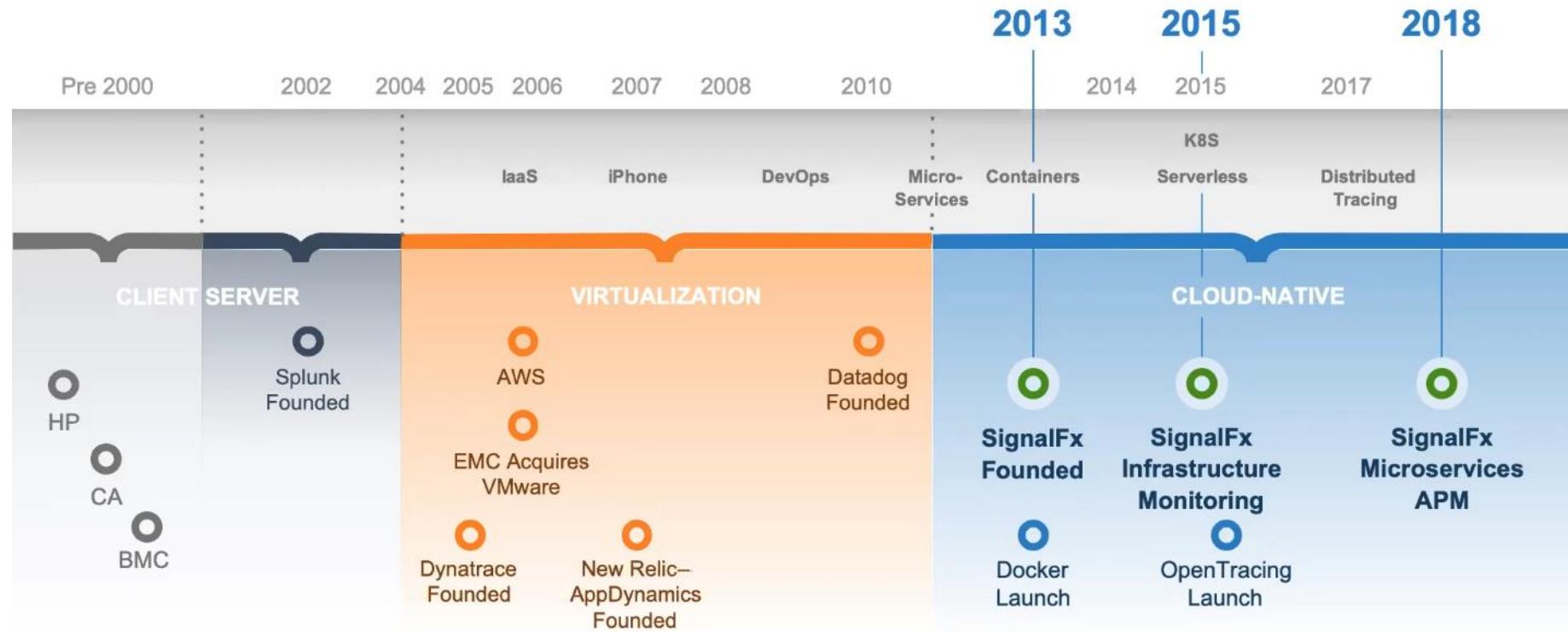
The screenshot shows the official Splunk website homepage on the left and the Network tab of the browser's developer tools on the right. The homepage features a pink-to-white gradient background with the text "The Data-to-Everything Platform", "Bring data to every question, decision and action.", "Find Out How", and "See What's New". Below this, it says "Turn Data Into Doing™" and "Know what is happening in real time". The developer tools Network tab shows a list of network requests from "source...." to "source...." with various status codes (200, 204) and types (te...). A tooltip for one request details its duration: "Queued at 1.15 s", "Started at 1.15 s", "Resource Scheduling" (2.23 ms), "Connection Start" (0.41 ms), "DNS Lookup" (6.36 ms), "Initial connection" (400.65 ms), "SSL" (201.51 ms), "Request/Response" (0.71 ms), "Waiting (TTFB)" (202.79 ms), "Content Download" (0.29 ms), and an "Explanation" of 614.00 ms.



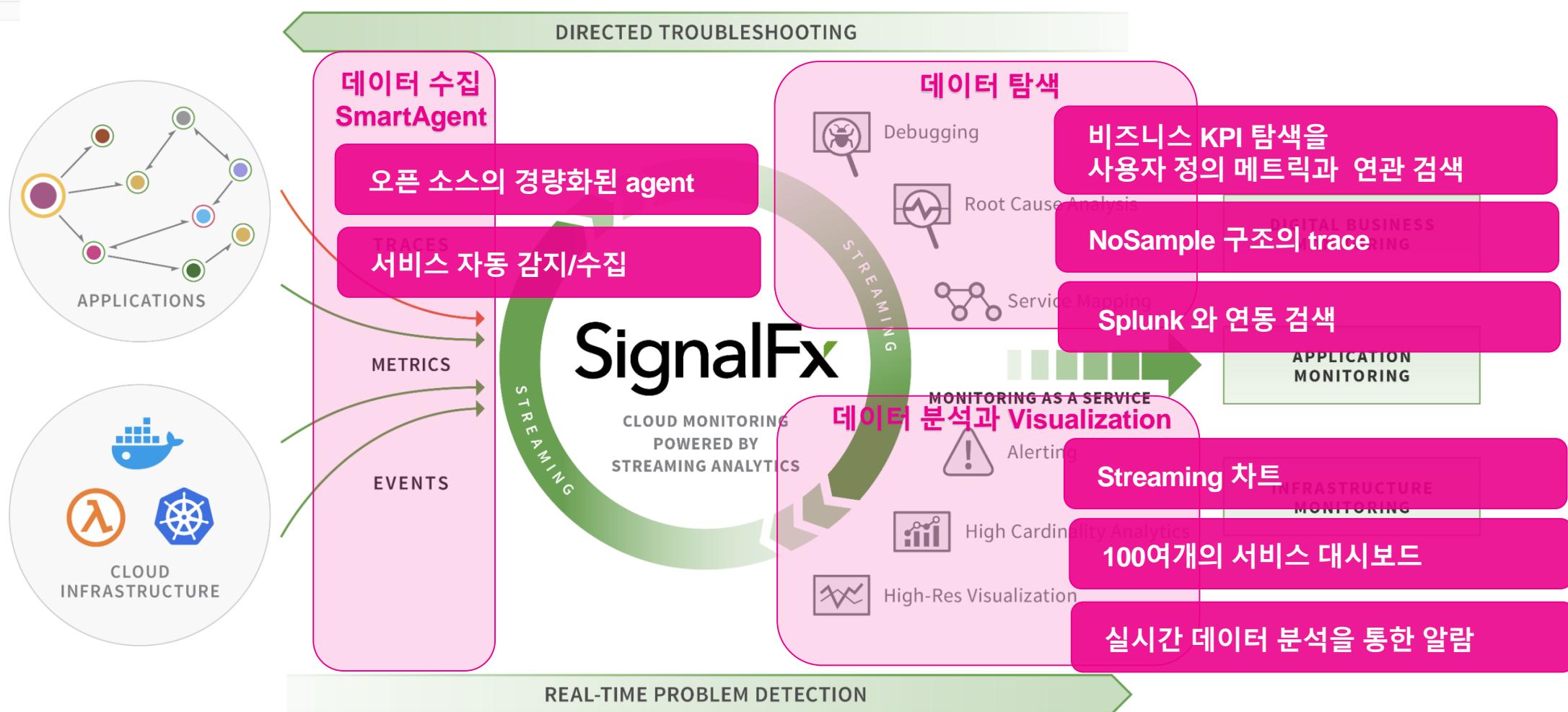
# SignalFx

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

# Cloud-Native 시대와 SignalFx



# SignalFx 기능



# Infrastructure Monitoring

The screenshot shows a SignalFx Infrastructure monitoring interface. At the top, there's a navigation bar with tabs for DASHBOARDS, μAPM, INFRASTRUCTURE (which is selected), ALERTS, METRICS, and INTEGRATIONS. Below the navigation is a search bar and a 'RESET' button. The main area features a large heatmap representing host utilization across multiple hosts. Below the heatmap, there are five circular summary metrics: 1K+ Critical (red), 41 Major (orange), 1 Minor (yellow), 420 Warning (purple), and 0 Info (white). Further down, a table lists detector rules with columns for Rule Name and Source, Detector Name, and Duration. The table includes several entries related to disk space and CPU utilization.

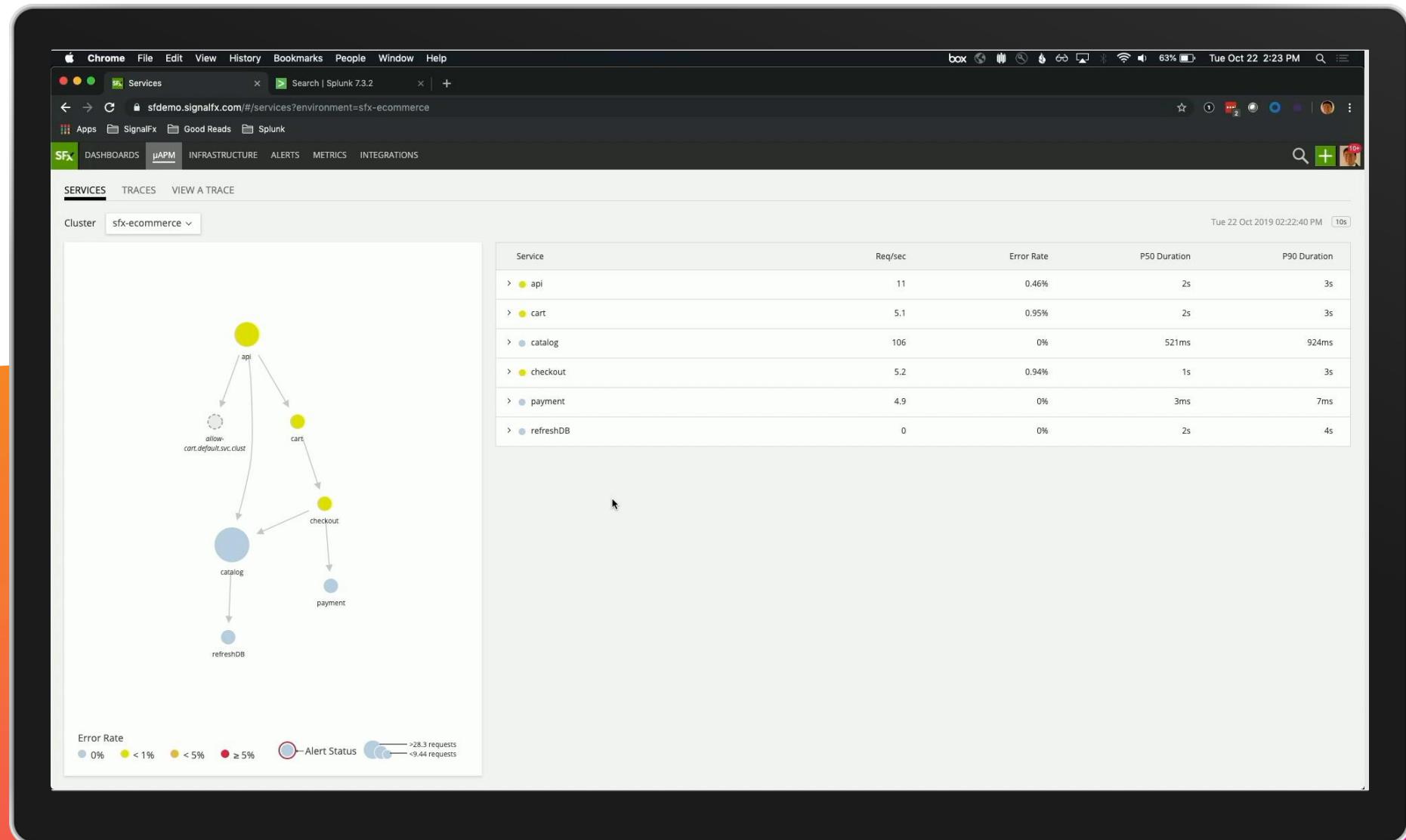
Rule Name and Source	Detector Name	Duration
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-cassandra-3.0-2 disk.summary_utilization i-0...	Zero available disk space within 24 hours	2 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-kafka-0.8.2.1-2 disk.summary_utilization i-0cf...	Zero available disk space within 24 hours	2 minutes
▲ CPU utilization is significantly greater than normal, and increasing - utilization signalfx-metadata value i-0bc4e18c39b42f599 cpu.utilization	CPU utilization % greater than historical norm	2 minutes
▲ CPU utilization is significantly greater than normal, and increasing - utilization signalfx-metadata value i-0dc499e4ba60b9345 cpu.utilization	CPU utilization % greater than historical norm	2 minutes
▲ Disk space utilization is significantly greater than normal, and increasing - utilization signalfx-metadata value i-07f73e2798779405f disk.summary_utilization	Disk space utilization % greater than historical n...	3 minutes
▲ Memory utilization is significantly greater than normal, and increasing - utilization signalfx-metadata value i-0c881742d22eb0a89 memory.utilization	Memory utilization % greater than historical norm	3 minutes
▲ Disk space utilization is significantly greater than normal, and increasing - utilization signalfx-metadata value i-01ef1e5b283e4309a disk.summary_utilization	Disk space utilization % greater than historical n...	3 minutes
▲ Disk space utilization is significantly greater than normal, and increasing - utilization signalfx-metadata value i-07f73e2798779405f disk.summary_utilization	Disk space utilization % greater than historical n...	3 minutes

# Alert

The screenshot shows a browser window with the URL [sf демо.signalfx.com/#/navigator/CO5Uf1QAcAA/collectd%20hosts?colorBy=collectd.cpu.utilization&outlierStrategy=off&tab=Alerts](https://sf демо.signalfx.com/#/navigator/CO5Uf1QAcAA/collectd%20hosts?colorBy=collectd.cpu.utilization&outlierStrategy=off&tab=Alerts). The dashboard has tabs for LIST, ALERTS (selected), SYSTEM METRICS, and INSIGHTS (Beta). Below the tabs is a heatmap of host utilization. To the right of the heatmap are five circular summary metrics: 1K+ Critical (red), 41 Major (orange), 2 Minor (yellow), 422 Warning (purple), and 0 Info (white).

Rule Name and Source	Detector Name	Duration
▲ majorAlert - utilization signalfx-metadata value i-0034e783797ac4c41 cpu.utilization	Signalflow Custom CPU Growth	a minute
▲ Disk space utilization is significantly greater than normal, and increasing - utilization signalfx-metadata value i-024fa3f9010520612 disk.summary_utilization	Disk space utilization % greater than historical n...	3 minutes
▲ Disk space utilization is significantly greater than normal, and increasing - utilization signalfx-metadata value i-024fa3f9010520612 disk.summary_utilization	Disk space utilization % greater than historical n...	3 minutes
▲ CPU utilization is significantly greater than normal, and increasing - utilization signalfx-metadata value i-0bc4e18c39b42f599 cpu.utilization	CPU utilization % greater than historical norm	5 minutes
▲ CPU utilization is significantly greater than normal, and increasing - utilization signalfx-metadata value i-0bc4e18c39b42f599 cpu.utilization	CPU utilization % greater than historical norm	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-flip_flop-5.ONE disk.summary_utilization i-0cf...	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-flip_flop-2.TWO disk.summary_utilization i-0cf...	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-apache-2.4.10-2 disk.summary_utilization i-0...	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-mysql-5.6-2 disk.summary_utilization i-0cf...	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-mongodb-2.6-2 disk.summary_utilization i-0cf...	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-zookeeper-3.4.10-2 disk.summary_utilizat...	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-couchbase-server-4.1-2 disk.summary_utilizat...	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-varnish-4.1.1-1-2 disk.summary_utilization i-0...	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-haproxy-1.6-2 disk.summary_utilization i-0cf...	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-activemq-5.14.5-2 disk.summary_utilization i-...	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value i-0cfabe05a72505b32 disk.summary_utilization	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-mesos-0.27.0-2 disk.summary_utilization i-0cf...	Zero available disk space within 24 hours	5 minutes
▲ Disk space utilization is projected to reach 100% within 24 hours - utilization signalfx-metadata value integration-test-nginx-1.10.3-2 disk.summary_utilization i-0cf...	Zero available disk space within 24 hours	5 minutes

# Micro APM



# SPLUNK 와 연동

**Container Latency Outlier Detector (Critical rule)**

Detector view as of Oct 22, 2019 2:24:03 PM (a minute ago) — [View traces from this time window](#)

Initiating Rollback for jlo@signalfx.com

[View more details](#)

user:jlo@signalfx.com >  
canary:true >  
containerId:b6231a6a9409 >  
customer:Hooli >

**\_S13**

Statement	Sources	Value
population_median + num_MAD * population_MAD	user: jlo@signalfx.com ...	77

[View all alerts from jlo@signalfx.com](#)

**\_S26**

Statement	Sources	Value
population_stream.promote(group_by_property)	canary: true ... containerId: b6231a6a9409 ... customer: Hooli ... sf_metric: requests.latency user: jlo@signalfx.com ...	503

[View all alerts from true](#)

[View all alerts from b6231a6a9409](#)

[View all alerts from Hooli](#)

[View all alerts from requests.latency](#)

[View all alerts from jlo@signalfx.com](#)

**\_S7**

Statement	Sources	Value
population_median + num_MAD * population_MAD	user: jlo@signalfx.com ...	77

[View all alerts from jlo@signalfx.com](#)

**Event Feed**

- Custom Event a few seconds ago
- Automated Rollback initiated user: jlo@signalfx.com
- Critical Container Latency Outlier Detector (Service - Latency Population Outlier) user: jlo@signalfx.com canary: true containerId: b6231a6a9409 customer: Hooli sf\_metric: requests.latency
- Custom Event a few seconds ago
- canary push event user: jlo@signalfx.com

**Requests processed per container**

999  
c4acec3a28c7 | jlo@signalfx.com |  
aee95f126d1b  
62bbb26270d4 | jlo@signalfx.com |

# Observability & Stack Trace

Container Latency Outlier Detector (Critical rule)

Detector view as of Oct 22, 2019 2:24:03 PM (a minute ago) — [View traces from this time window](#)

Initiating Rollback for jlo@signalfx.com

[View more details](#)

\_S13

Statement: population\_median + num\_MAD \* population\_MAD  
Sources: user: jlo@signalfx.com ...  
Value: 77

[View all alerts from jlo@signalfx.com](#)

\_S26

Statement: population\_stream.promote(group\_by\_property)  
Sources: canary: true ...  
containerId: b6231a6a9409 ...  
customer: Hooli ...  
sf\_metric: requests.latency  
user: jlo@signalfx.com ...  
Value: 503

[View all alerts from true](#)  
[View all alerts from b6231a6a9409](#)  
[View all alerts from Hooli](#)  
[View all alerts from requests.latency](#)  
[View all alerts from jlo@signalfx.com](#)

\_S7

Statement: population\_median + num\_MAD \* population\_MAD  
Sources: user: jlo@signalfx.com ...  
Value: 77

[View all alerts from jlo@signalfx.com](#)

Event Feed

- Custom Event a few seconds ago  
Automated Rollback initiated user: jlo@signalfx.com
- Critical a few seconds ago  
Container Latency Outlier Detector (Service - Latency Population Outlier)  
user: jlo@signalfx.com  
canary: true  
containerId: b6231a6a9409  
customer: Hooli  
sf\_metric: requests.latency
- Custom Event a few seconds ago  
canary push event user: jlo@signalfx.com

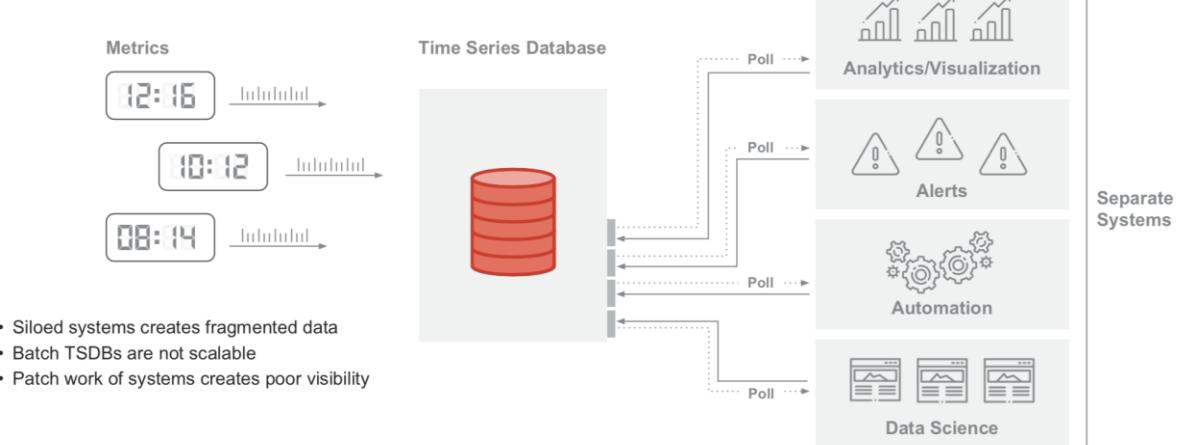
Requests processed per container

986

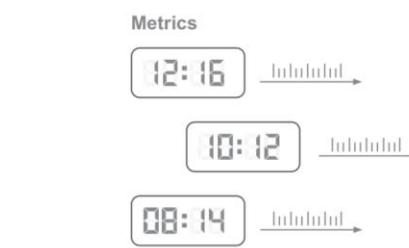
715511e58aa | jlo@signalfx.com | a6be9eb883d0 | 62bb26270d4 | jlo@signalfx.com |

# SingalFX 차별성 1/2

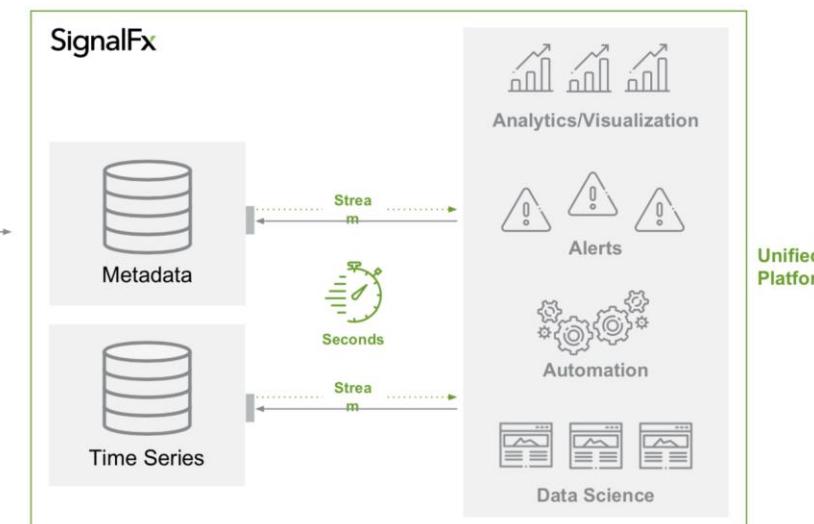
초 단위의 stream 모니터링



Separate Systems

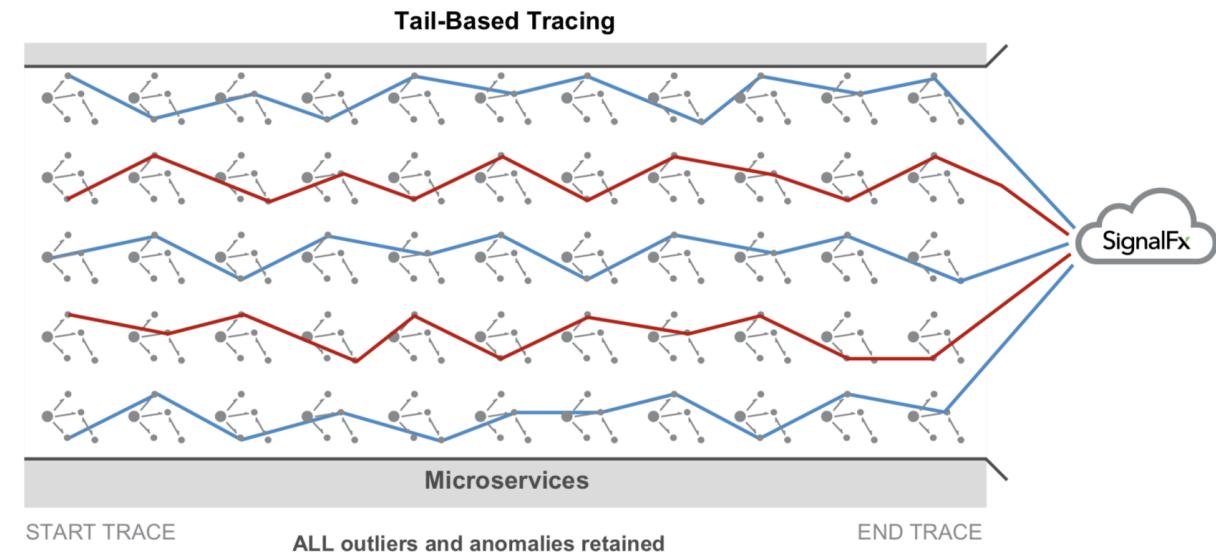
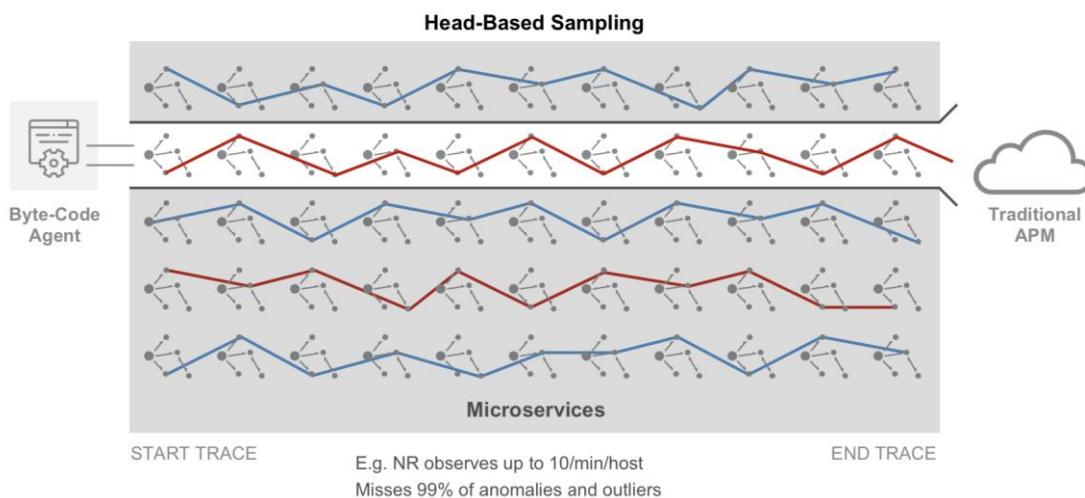


- Two separate DBs for high scalability
- Streaming system for instant visibility
- Unified platform for a single source of truth

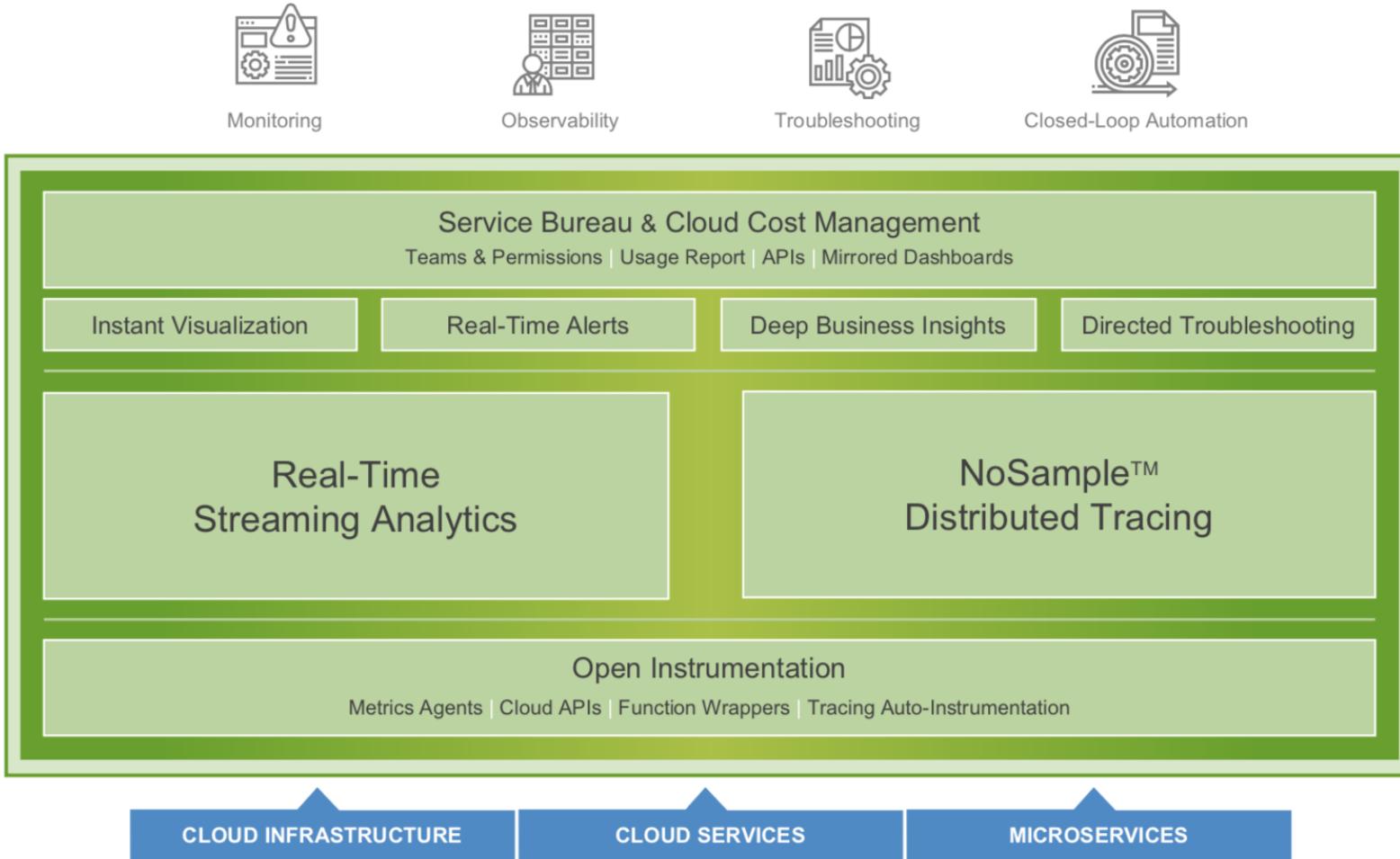


# SingalFX 차별성 2/2

## NoSample Tail-Based Tracing



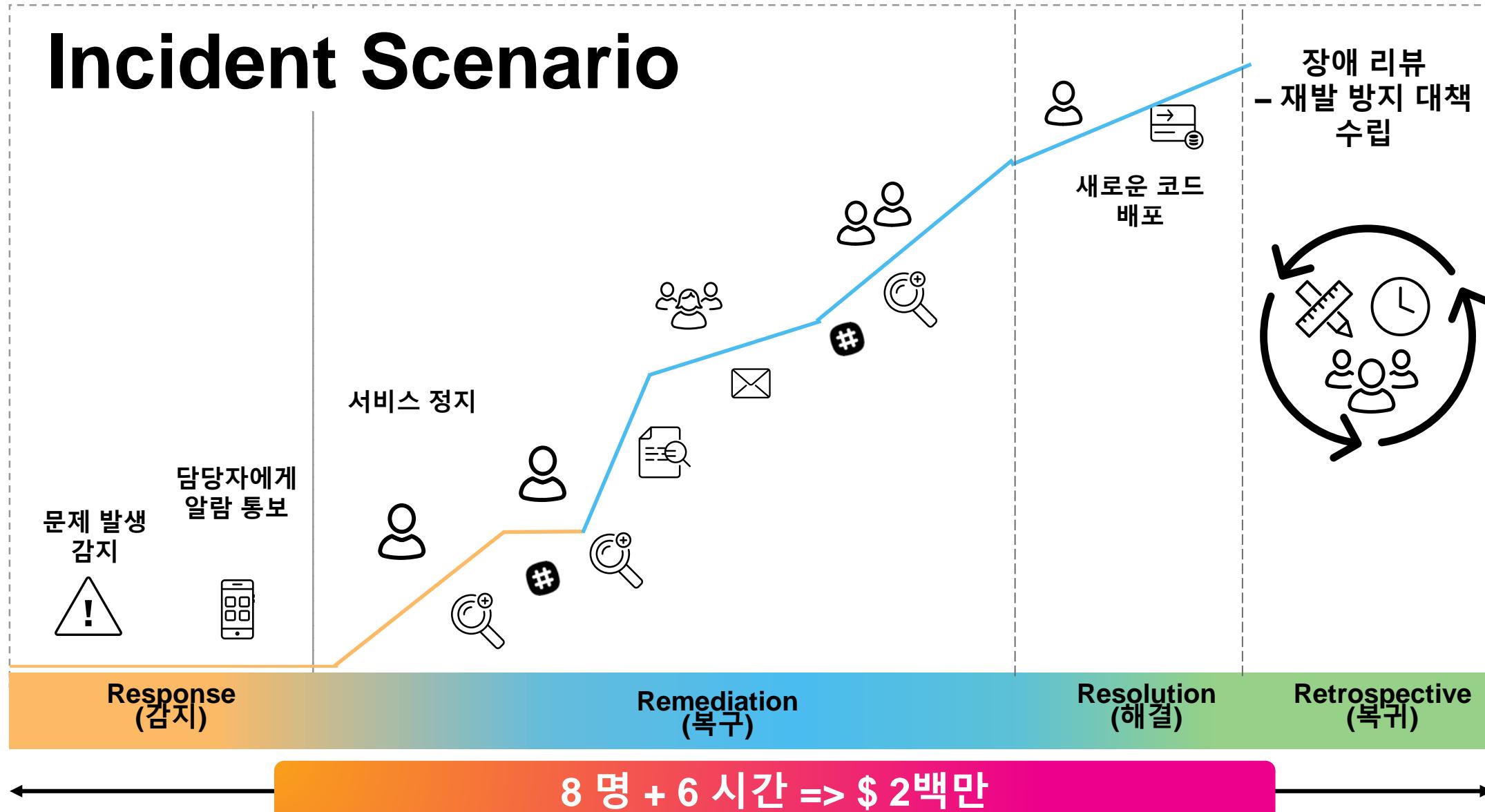
# SignalFx 구조



# Splunk Investigate

splunk>Forum

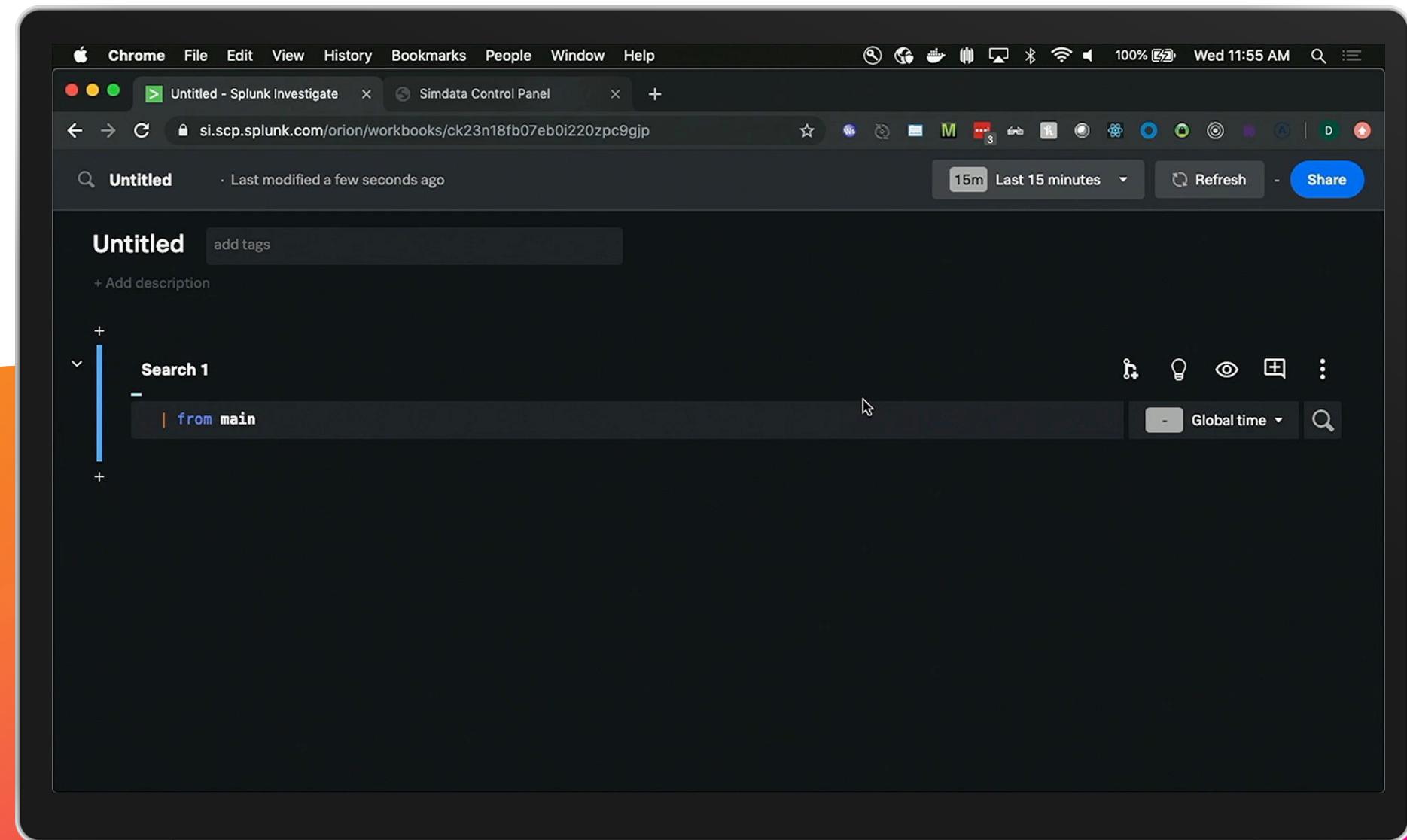
# Incident Scenario





splunk®  
investigate

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



# 핵심 기능

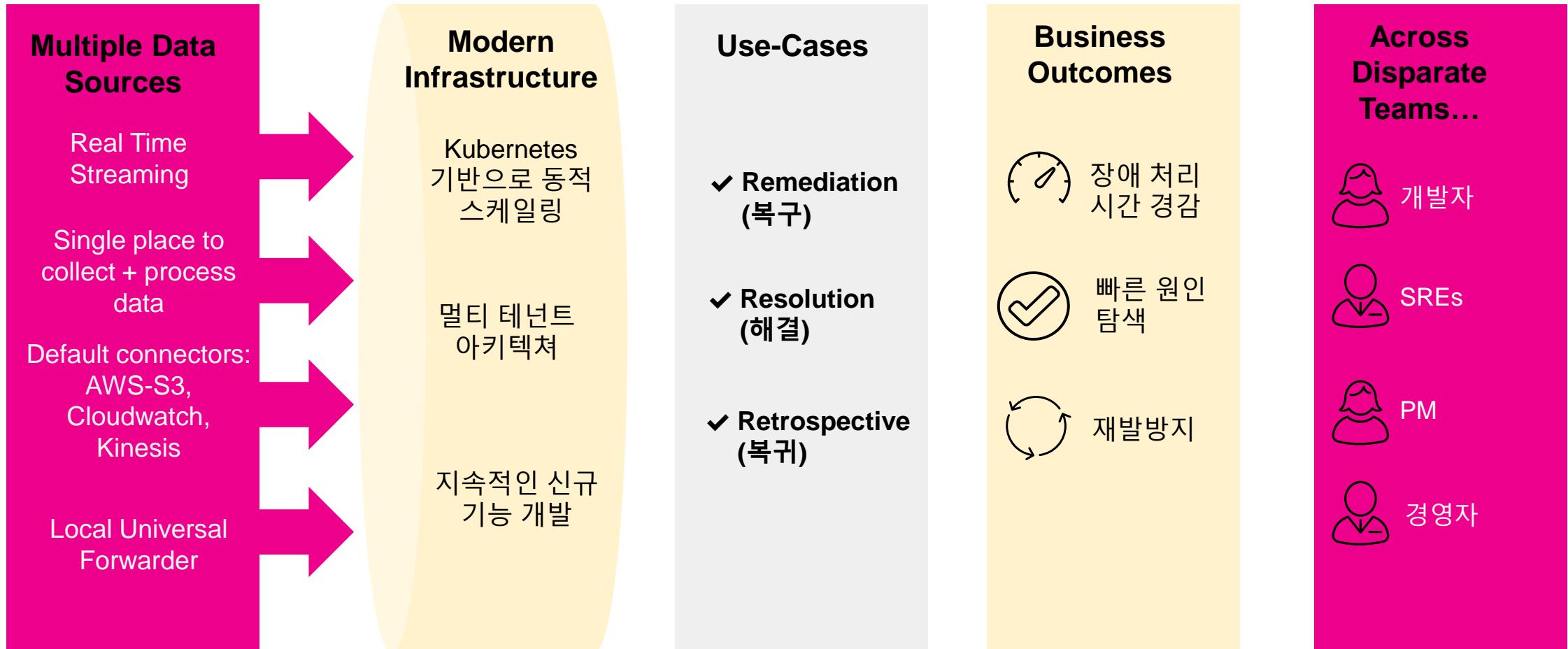
협업 인터페이스 워크북

Smart Knowledge Object Library

스토리텔링 대시보드

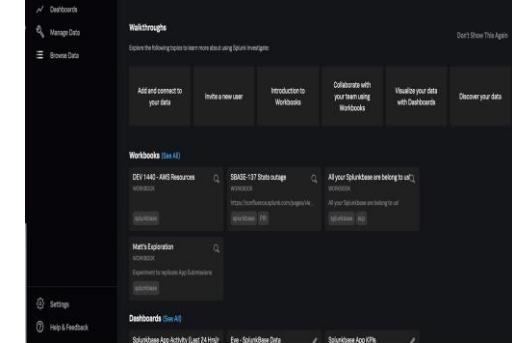
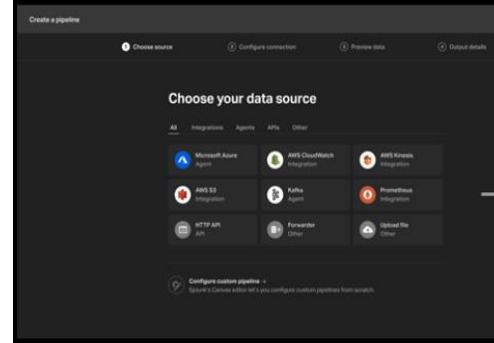
데이터 추가와 정제 워크플로우

# 신속한 문제 해결을 위한 최적의 솔루션



# Splunk Investigate

## 지금 바로 시작하세요



### Step 1.

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

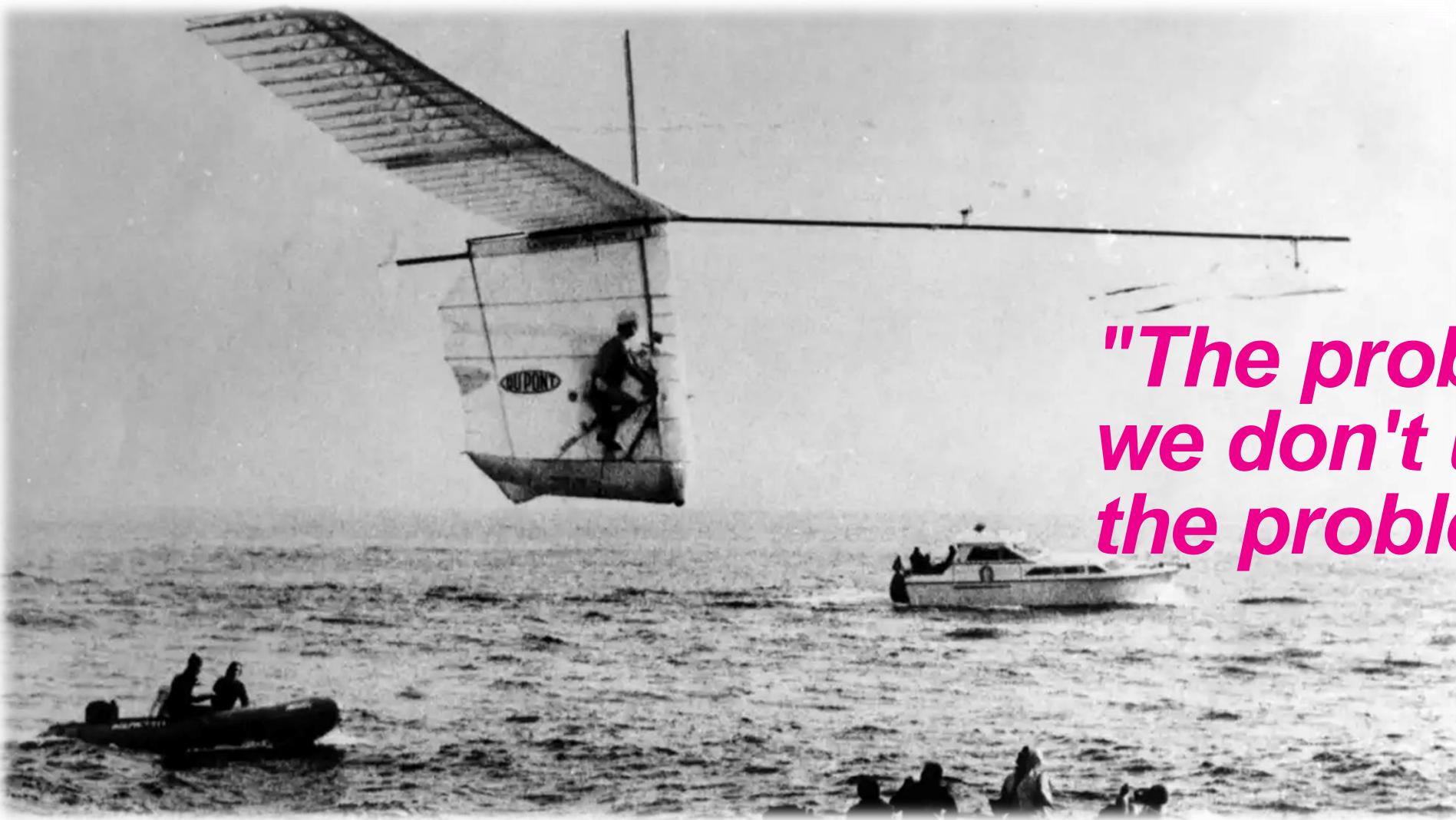
에서 무료사용 등록

### Step 2.

데이터 업로드

### Step 3.

Splunk  
Investigate 시작

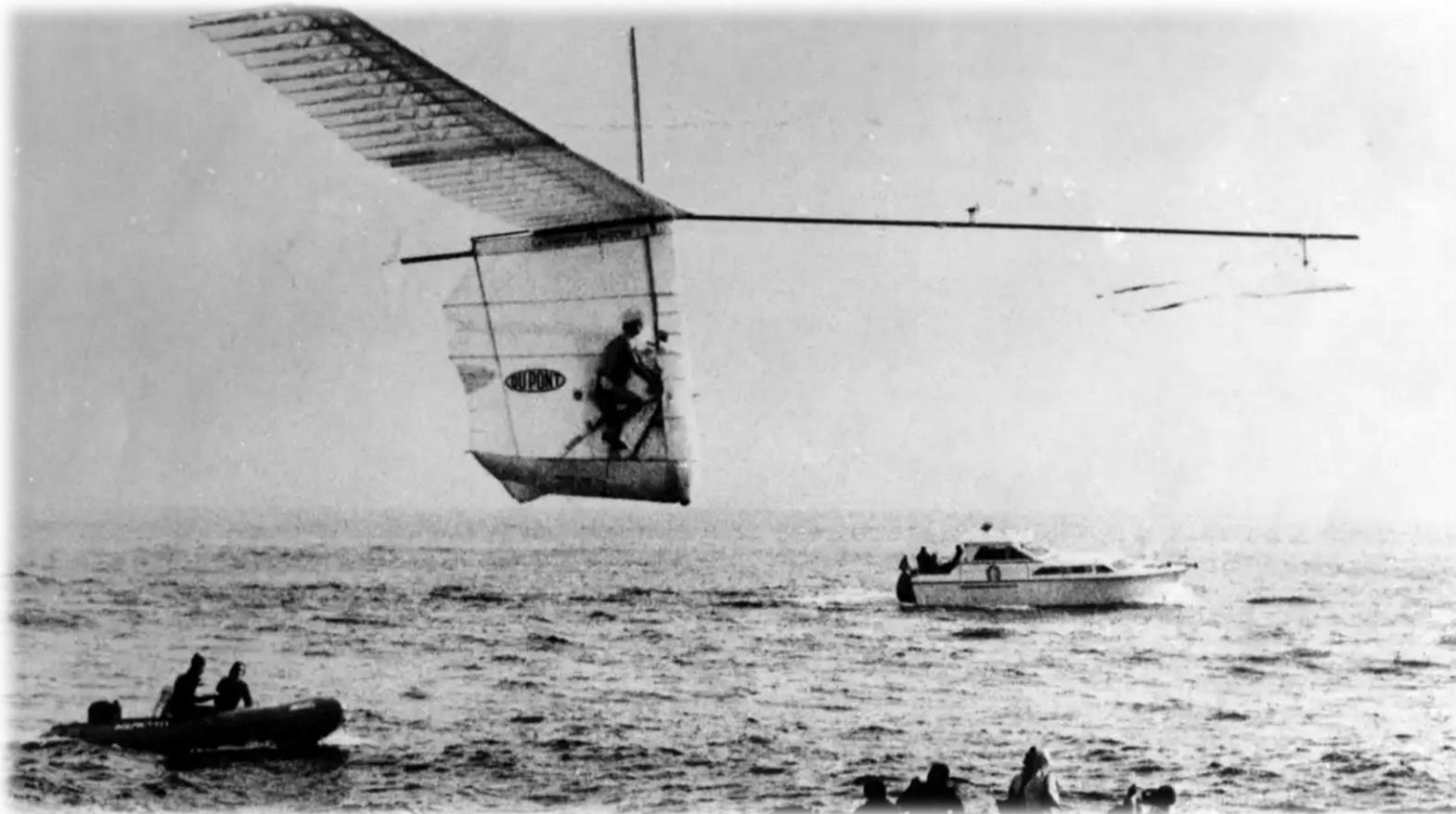


*"The problem is that  
we don't understand  
the problem."*

1979년 영국 해협을 횡단한 Paul McCready의 Gossamer Albatross

감사합니다

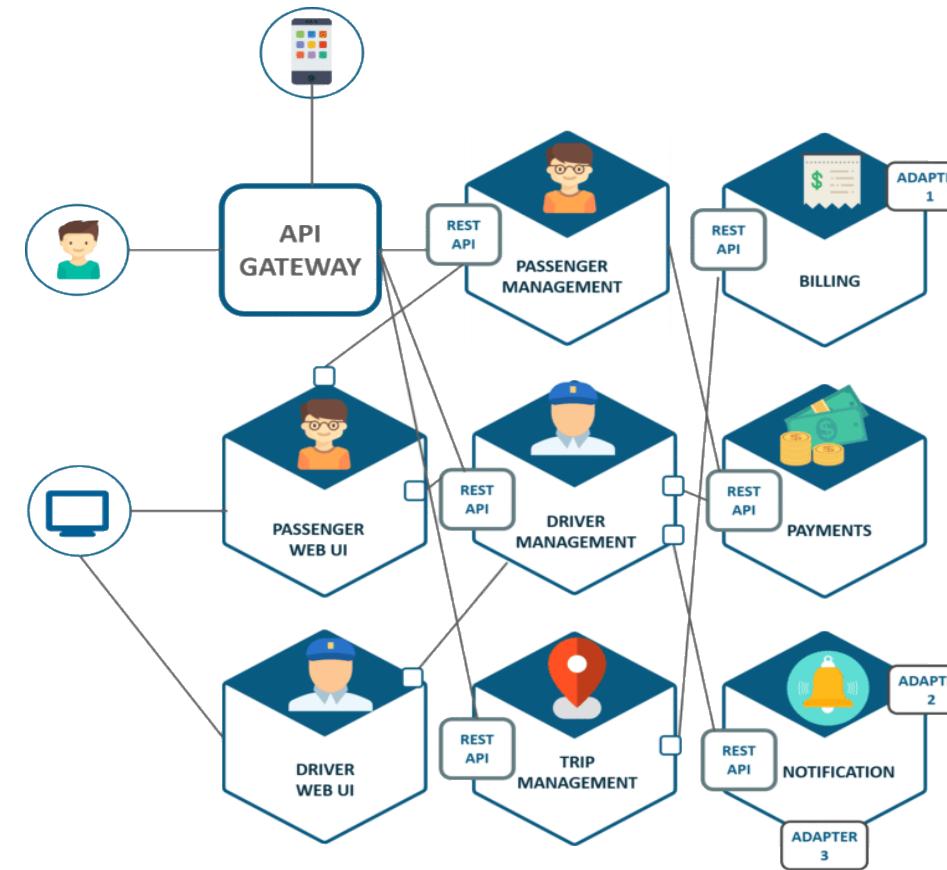
# 왜 Micro Service 인가?



1979년 영국 도버 해협을 횡단한 Paul McCready의 Gossamer Albatross

- |                   |                        |
|-------------------|------------------------|
| <b>1959</b>       | <b>Henry Kremer</b>    |
| 사람의 힘만으로 움직이는 항공기 |                        |
| <b>17</b>         | <b>50,000</b>          |
| Paul McCready     |                        |
| <b>1977</b>       | <b>Gossamer Condor</b> |
| <b>223</b>        | <b>4</b>               |

# Microservice 예제 (UBER)



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