

# What's New in Splunk

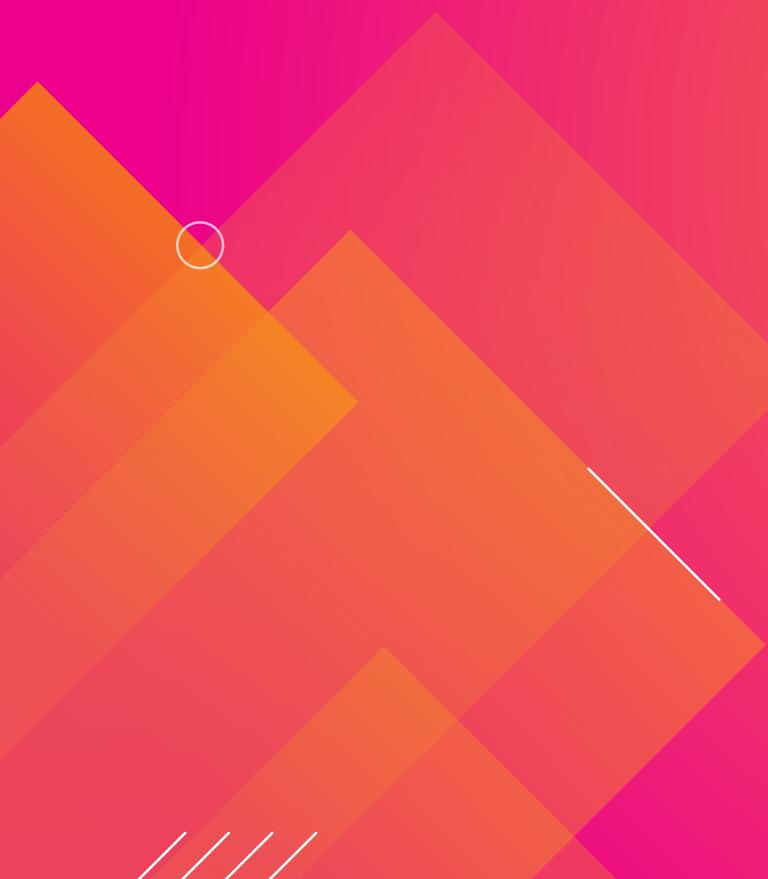
2019년 Data to Everything Platform 의 새로운 기능들

최승돈 / 이미정 매니저  
스플렁크 코리아

December 12, 2019

splunk>Forum

# Forward-Looking Statements

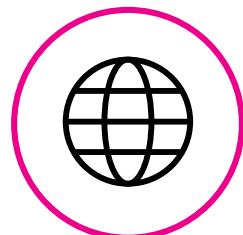


During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. 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.

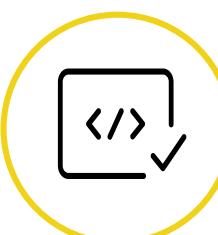
# 스플렁크의 데이터를 비지니스 결과로 바꾸는 종합적인 접근법



IT



Security



DevOps

Business  
Analytics

Developers



On-Premises



Analyze with differentiated AI and ML

**Splunk Data-to-Everything Platform**

Investigate the expanding data universe

Deployment



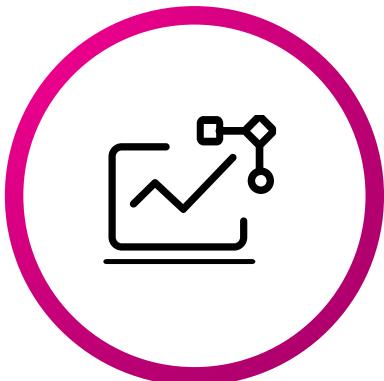
Cloud



# What's New in .conf2019

2019년 스플렁크의 새로운 기술 포트폴리오

## Platform



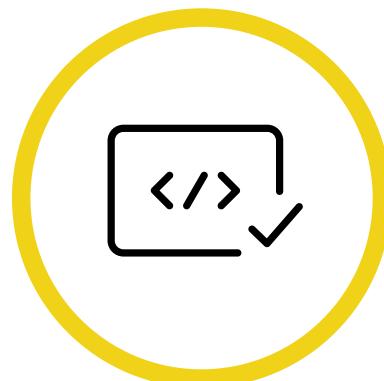
Splunk Enterprise  
Connected Experiences  
Splunk Machine Learning Toolkit  
Splunk Cloud FedRAMP  
Data Fabric Search  
Data Stream Processor

## IT Operations



Splunk IT Service Intelligence  
Splunk App for Infrastructure  
Splunk Business Flow  
VictorOps  
SignalFX

## DevOps



SignalFX  
Splunk Investigate  
VictorOps  
Splunk Developer Cloud

## Security



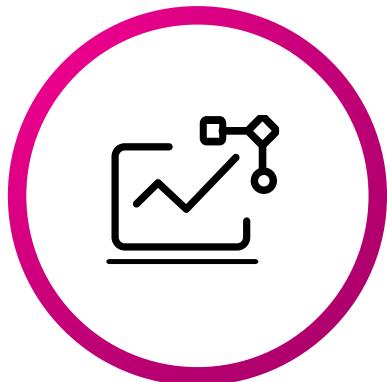
Splunk Enterprise Security  
Splunk User Behavior Analytics  
Splunk Phantom  
Splunk Mission Control

**splunk>Forum**

# What's New in .conf2019

2019년 스플렁크의 새로운 기술 포트폴리오

## Platform



Splunk Enterprise  
Connected Experiences  
Splunk Machine Learning Toolkit  
Splunk Cloud FedRAMP  
Data Fabric Search  
Data Stream Processor

## IT Operations



Splunk IT Service Intelligence  
Splunk App for Infrastructure  
Splunk Business Flow  
VictorOps  
SignalFX

## DevOps



SignalFX  
Splunk Investigate  
VictorOps  
Splunk Developer Cloud

## Security



Splunk Enterprise Security  
Splunk User Behavior Analytics  
Splunk Phantom  
Splunk Mission Control

**splunk>Forum**



거대충 넘어갑니다

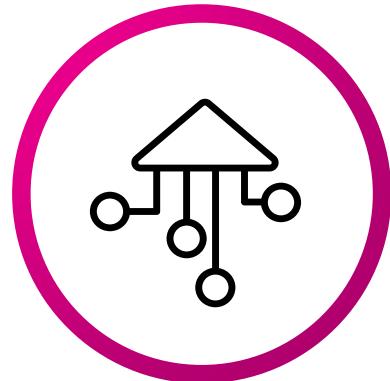
ANNOUNCING

# Splunk Enterprise 8.0

# Splunk Enterprise 8.0

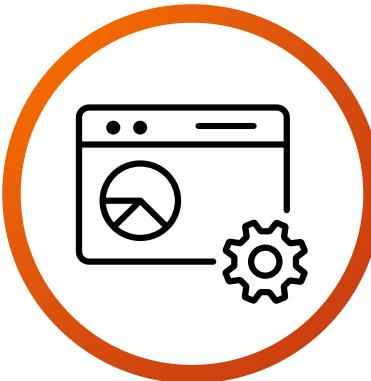
Delivers management at scale for a fully observable enterprise

계속되는 성능  
향상과 데이터 확장



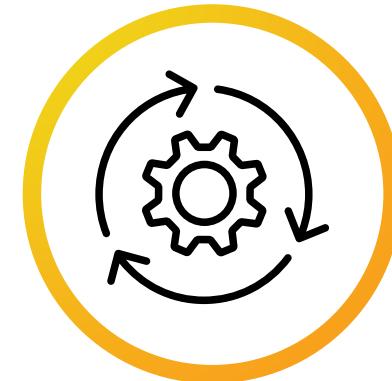
Search  
Metrics and Events  
Performance Enhancement  
Shared DMA Summaries

보다 빠르고, 쉽고,  
직관적인 분석



Analytics Workspace  
Connected Experience  
Natural Language Platform  
New Dashboards  
Machine Learning Toolkit

확장되고 향상된  
관리 기능

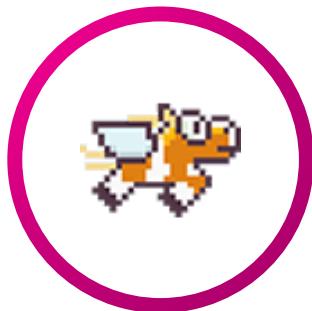


Monitoring SmartStore  
Workload Management  
Security Access & Control  
Operator for Kubernetes  
Python 3.7 Migration

# 보다 빠른 검색

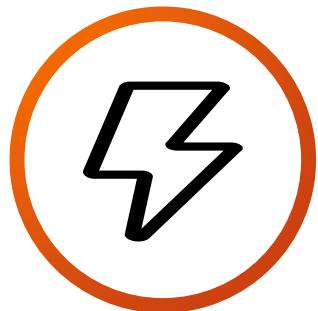
Faster Searches. Automatically.

**Tstats  
Optimizer**



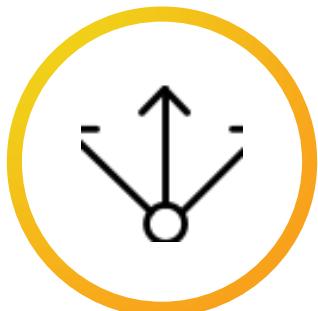
Index-Field 사용시  
자동으로 stats →  
tstats으로 최적화  
**99.8% 성능 개선**

**Shared  
Lookup**



자동으로 Search  
Process 내  
Lookup 재사용  
메모리 사용량  
감소 및 성능 증가  
**65% 성능 개선**

**Bundle Rep  
속도 개선**



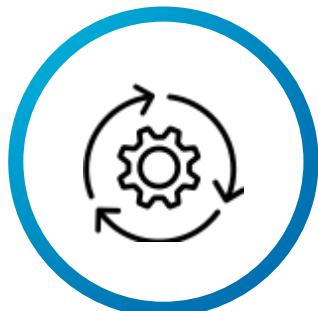
SHC 번들 복제,  
SH-SP 번들  
복제 시간  
**10배 이상의 향상**  
빠르고 보다  
정확한 검색

**MetricStore  
v3**



메트릭 인덱스  
저장 공간 최적화  
성능 향상

**DMA  
Summary  
Sharing**

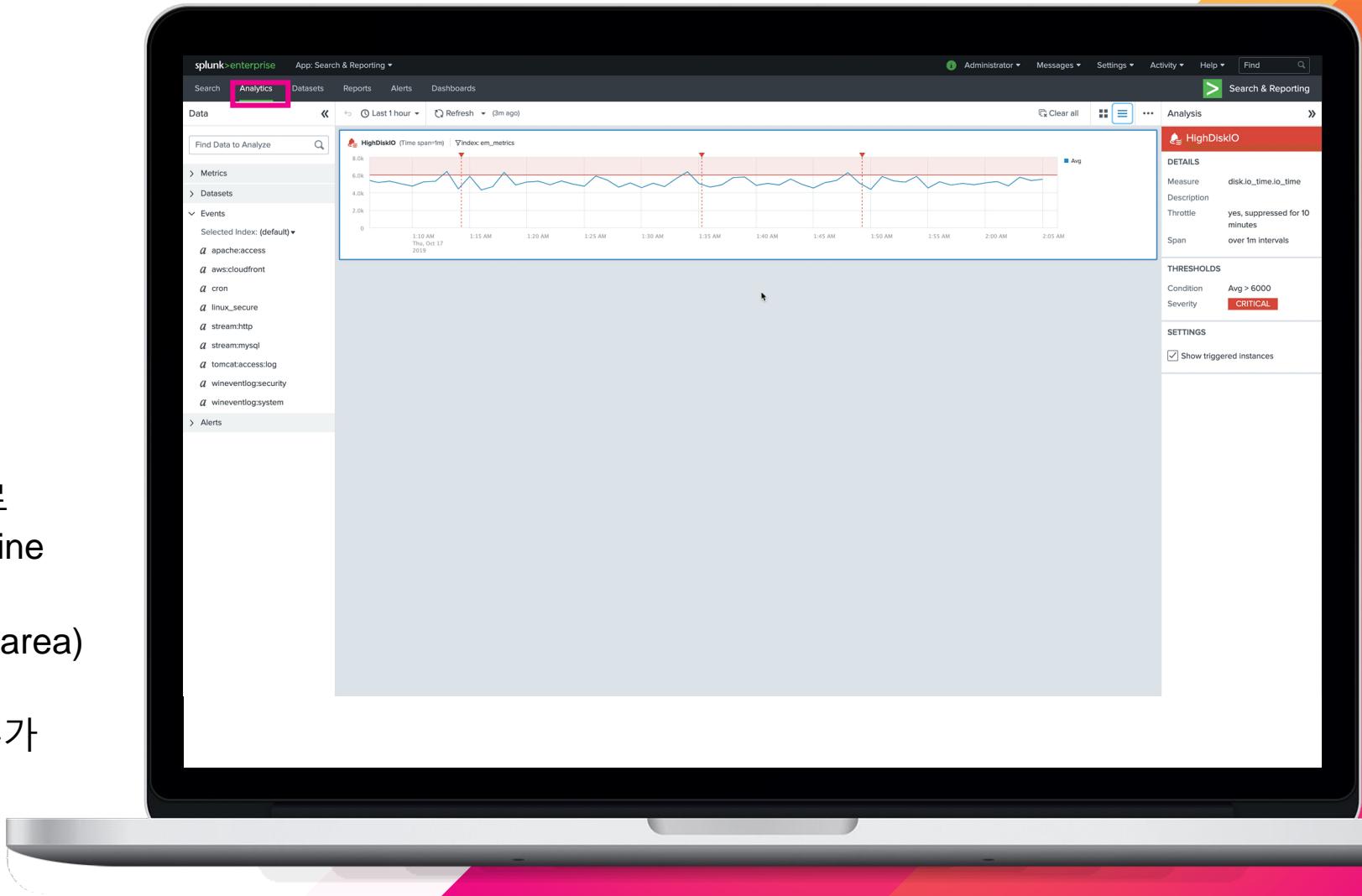


DMA  
summary 정보를  
여러 SH/SHC 간의  
공유

# Analytics Workspace

Self Service Insight. No SPL

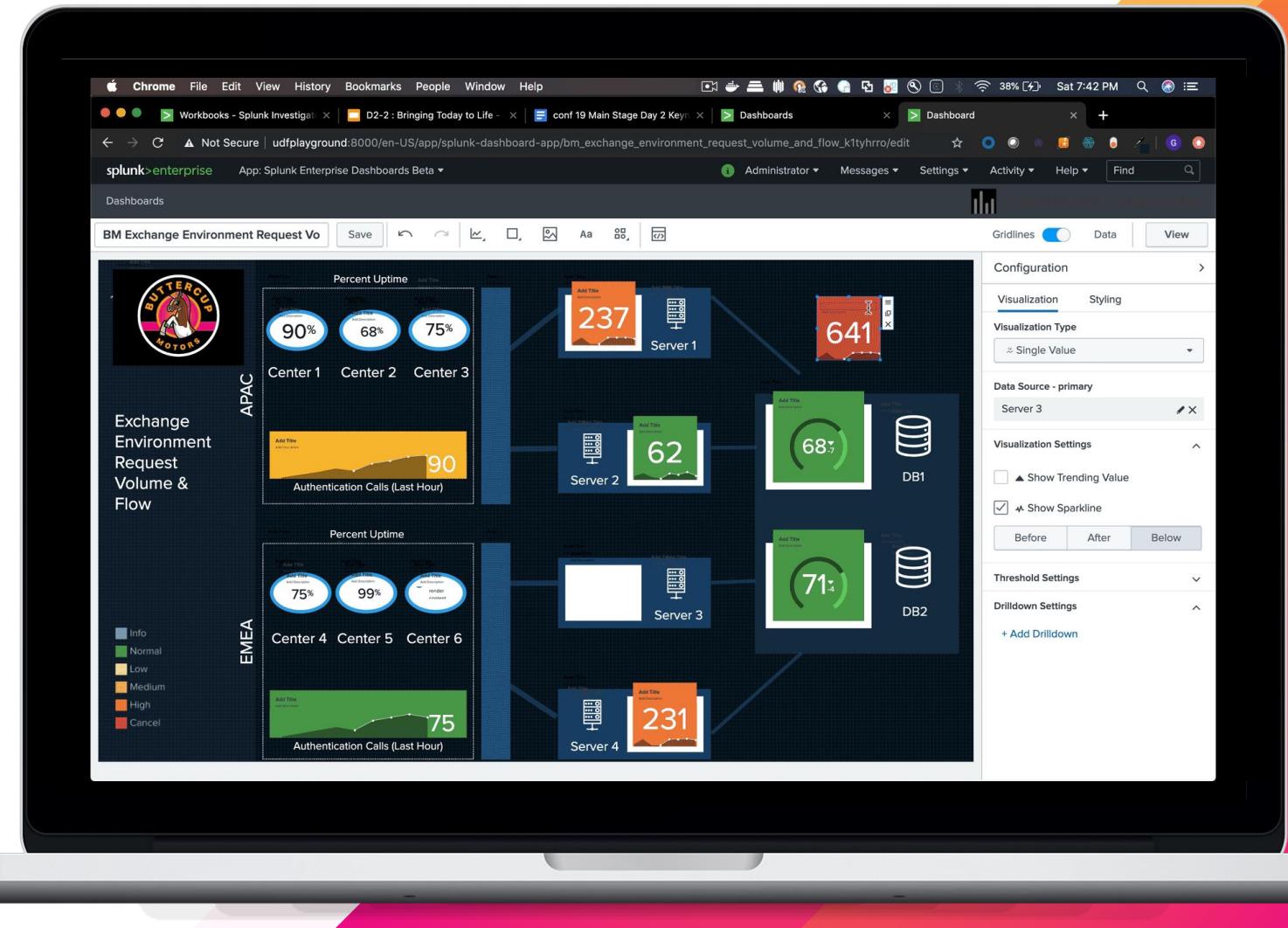
- 사용하기 쉬운 직관적인 UI.
- Drag-in Drop 방식으로 시각화  
프로세스 간소화
- Time Picker 개선, 클릭 한번으로  
다른 Metric에 대한 Reference Line  
추가
- Categorical Chart (bar, column, area)  
시각화 추가
- Streaming Metrics Alert 기능 추가  
더 빠른 성능의 경보 생성
- Events + Metrics + Alerts  
in Single UI



# Splunk Dashboard App<sup>beta</sup> 새로운 대시보드

빠르고 직관적인 새로운  
대시보드 경험

- 픽셀단위까지 정확한 자유로운 커스터마이징 대시보드 제공
- 레이아웃과 UI를 통한 대시보드 변경 가능
- Image, Background, Icon의 손쉬운 추가로 고객의 비즈니스 업무에 좀더 직관적인 시각화 제공



# Machine Learning Toolkit 5.0



## 머신러닝을 보다 손쉽게

- 새롭고 현대적인 쇼케이스 레이아웃으로 손쉬운 ML 접근
- 새로운 Smart Outlier Detection Assistant를 통한 이상치 탐지 모델 생성 간편화
- 다중변수 예측(Multivariate Forecasts)과 특정일자(Special Days Effect) 기능 추가로 보다 정확한 ML 모델 생성

The screenshot shows the Splunk Machine Learning Toolkit interface. The top navigation bar includes links for Showcase, Experiments, Search, Models, Classic, Settings, Docs, and Video Tutorials. The main title is "Smart Outlier Detection: Anomalies in Supermarket Purchases". On the left, there's a sidebar with tabs for Define, Learn, Review, and Operationalize, with "Define" currently selected. Below the title, a search bar contains the query "inputlookup supermarket.csv". A "Data Preview" section shows a table with columns: customer\_id, distance, price, product\_id, quantity, and shop\_id. The table lists 20 rows of data from the supermarket CSV file. The interface has a dark theme with orange and white highlights.

| customer_id | distance      | price   | product_id | quantity | shop_id |
|-------------|---------------|---------|------------|----------|---------|
| u1          | 4882.52216298 | 0.334   | p112       | 3        | s1      |
| u1          | 4882.52216298 | 1.048   | p133       | 1        | s1      |
| u1          | 4882.52216298 | 263.234 | p248       | 2        | s1      |
| u1          | 4882.52216298 | 1.429   | p318       | 1        | s1      |
| u1          | 4882.52216298 | 0.465   | p326       | 1        | s1      |
| u1          | 4882.52216298 | 21.639  | p336       | 1        | s1      |
| u1          | 4882.52216298 | 6.356   | p338       | 2        | s1      |
| u1          | 4882.52216298 | 0.989   | p356       | 2        | s1      |
| u1          | 4882.52216298 | 1.171   | p379       | 1        | s1      |
| u1          | 4882.52216298 | 1.368   | p380       | 1        | s1      |
| u1          | 4882.52216298 | 1.883   | p442       | 1        | s1      |
| u1          | 4882.52216298 | 1.605   | p446       | 3        | s1      |
| u1          | 4882.52216298 | 1.817   | p458       | 1        | s1      |
| u1          | 4882.52216298 | 1.826   | p453       | 1        | s1      |
| u1          | 4882.52216298 | 1.726   | p485       | 1        | s1      |
| u1          | 4882.52216298 | 2.245   | p488       | 1        | s1      |
| u1          | 4882.52216298 | 6.256   | p495       | 2        | s1      |
| u1          | 4882.52216298 | 1.133   | p497       | 2        | s1      |
| u1          | 4882.52216298 | 1.462   | p582       | 1        | s1      |
| u1          | 4882.52216298 | 2.167   | p585       | 1        | s1      |

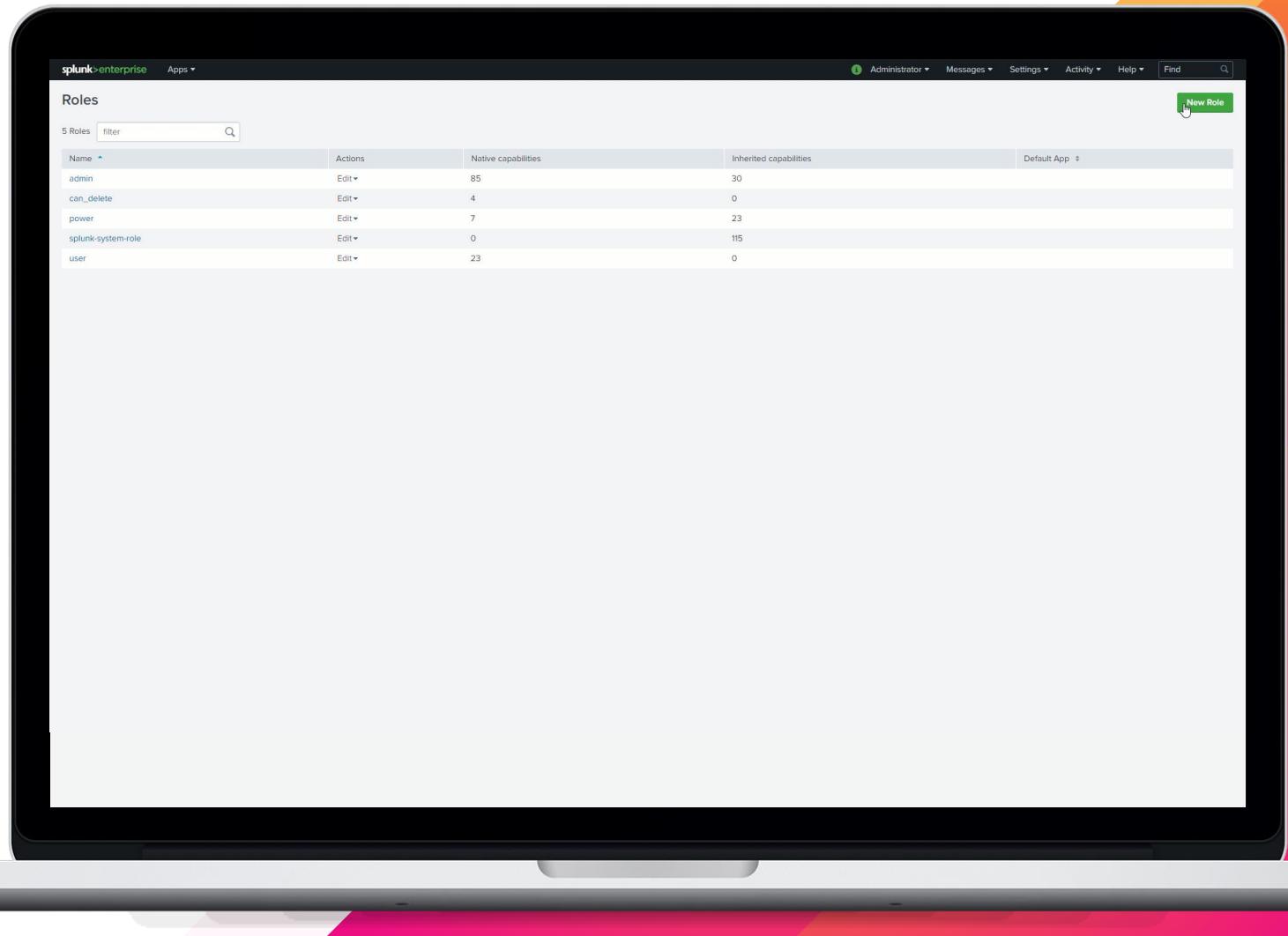
# 강화된 보안 기능

## Indexed Fields Access Controls

보다 정교한 접근 제어

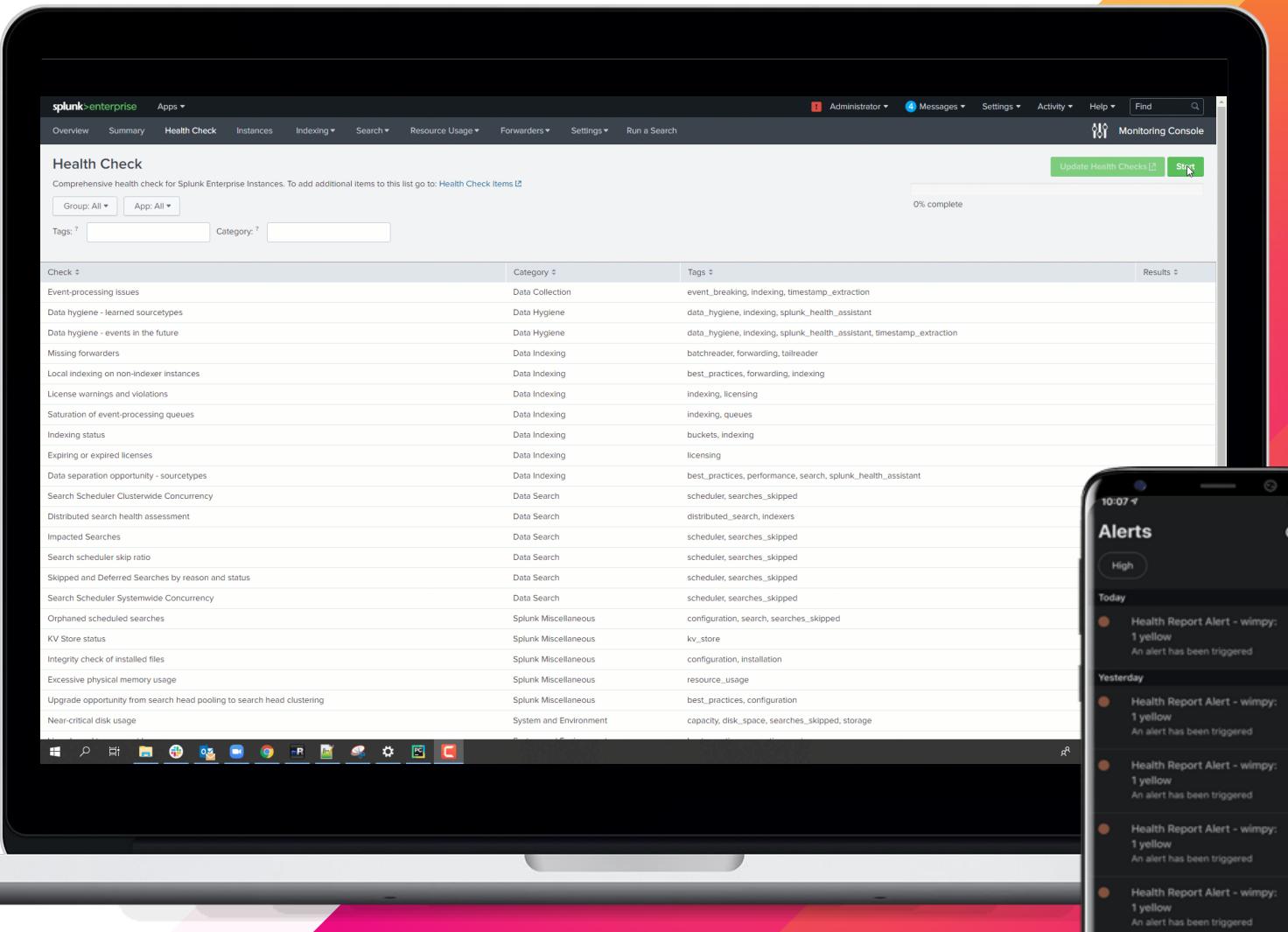
인증 토큰 사용으로 보안성 강화

- 새로운 룰 관리 UI
- 동적 검색 필터 생성기를 통한  
**동일 인덱스 데이터를 유저 룰별로  
접근 권한 부여**
- REST, CLI, Mobile App을 위한 새로운  
인증 토큰으로 보안성 강화



# 강화된 스플렁크 모니터링 콘솔

- 스플렁크 디플로이에 대한 실시간 모니터링 제공
- 분산 환경의 단일 뷰 및 헬스 리포트 제공
- Splunk Health Assistant Add-on 을 통해 스플렁크의 고객 지원 센터의 최신 best practice를 proactive하게 제공
- Splunk Mobile를 통한 실시간 Alert



# Workload Management

## 효율적인 스플렁크 리소스 관리

- 검색과 수집의 리소스 우선순위 설정으로 리소스 및 작업 최적화
- 룰 프레임워크 개선 - 서치 타입별/모드별 룰 설정 가능
- 좀비 프로세스 자동 처리
- 시간대별 스케줄 기반 룰 관리 가능

The screenshot shows the Splunk Cloud Workload Management interface. At the top, there's a navigation bar with 'splunk>cloud' and various dropdown menus like 'Apps', 'Messages', 'Settings', 'Activity', 'Find', and a search bar. On the right, there are buttons for 'Splunk Administrator', 'Support & Services', and toggle switches for 'Enabled', 'Add Workload Pool', and 'Add Workload Rule'. Below the navigation is a section titled 'Workload Management' with a sub-section 'Categories'. It displays three categories: 'Search Category' (CPU Weight: 50 / 100, Memory Limit %: 65%), 'Ingest Category' (CPU Weight: 45 / 100, Memory Limit %: 100%), and 'Misc Category' (CPU Weight: 5 / 100, Memory Limit %: 5%). A note says 'There are no workload rules. Use the Add Workload Rule button to create new workload rules.' Below this is a table titled 'Categories' with columns for Category, Configured CPU Weight, Allocated CPU %, Configured Memory Limit %, Allocated Memory Limit %, and Actions. It lists 'search' with values 50, 50.00%, 65%, 65.00%, and 'edit' link. It also lists 'ingest' with values 45, 45.00%, 100%, 100.00%, and 'edit' link. Finally, it lists 'misc' with values 5, 5.00%, 5%, 5.00%, and 'edit' link. At the bottom, there's a section titled 'Search Pools' with a table showing 'Category', 'Workload Pool', 'Configured CPU Weight', 'Allocated CPU %', 'Configured Memory Limit %', 'Allocated Memory Limit %', 'Default Pool', and 'Actions'. It lists three pools: 'search' in 'high\_perf' pool with values 60, 30.00%, 100%, 65.00%, and 'edit' and 'delete' links; 'search' in 'limited\_perf' pool with values 5, 2.50%, 100%, 65.00%, and 'edit' and 'delete' links; and 'search' in 'standard\_perf' pool with values 35, 17.50%, 100%, 65.00%, checked as default pool, and 'edit' and 'delete' links.

# Splunk Operator for Kubernetes beta

스플렁크의 쿠버네티스 환경 설치 간편화

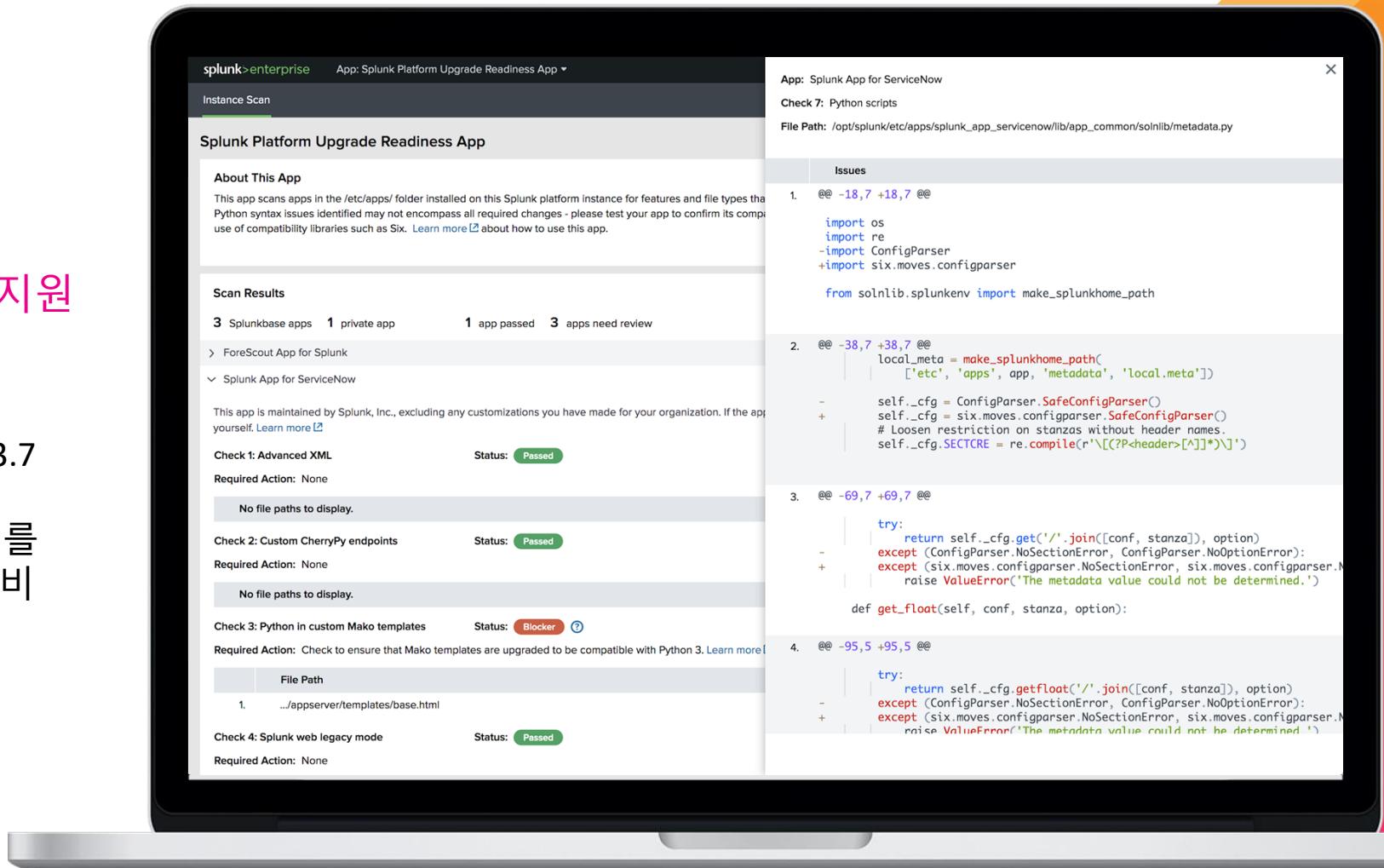
- 쿠버네티스 환경에 스플렁크 엔터프라이즈 설치 및 설정을 자동화/단순화
- DockerHub와 Redhat registry 에 등록된 새로운 컨테이너
- 싱글노드에서 멀티 노드 클러스터 환경까지 손쉽게 디플로이
- EKS, GKE, Openshift, Docker Enterprise , OSS K8s 상에서 테스트
- Learn more on [Github](#)



# Python 3 Upgrade

Python 3.7로 업그레이드  
Python 2.7과 3.7 런타임 동시 지원

- 2020년 1월 Python 2.7 EOL
- 8.0 버전은 Python 2.7과 Python 3.7 두개의 런타임 동시 지원
- Platform Upgrade Readiness app 를 사용하여 업그레이드를 사전 준비



Monitoring Splunk Health.  
Proactive.

2x faster stats command

# Splunk Enterprise 8.0

**Faster Searches. Automatically.**

**Splunk Dashboards App**

Splunk Tokens for REST API

**Metrics Optimizations**

Workload Management  
Enhancements

Smart Store  
Enhancements

Sub-Index Access Controls

SH to Search Peer Bundle Rep  
Performance Improvement

**Analytics Workspace**

**Splunk Enterprise Kubernetes Operator**

SHC Deployer Bundle Push  
Performance Enhancements

DMA Summary Sharing

**Python 3 Support**

**Splunk Cloud FedRAMP**

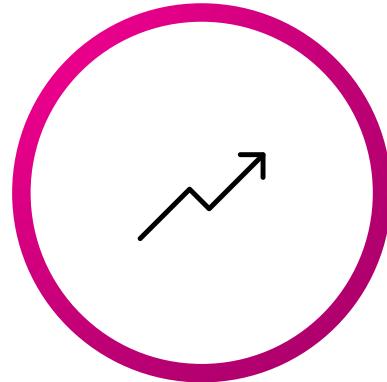
DMA Monitoring  
splunk>Forum

ANNOUNCING

# Data Stream Processor

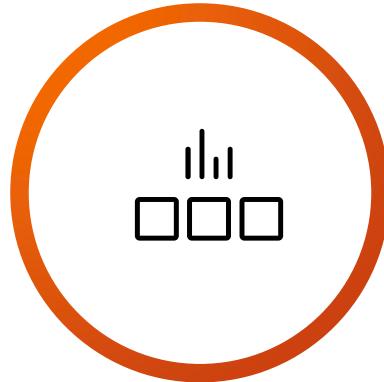
# 실시간 스트림 데이터의 처리

**Fast**



밀리세컨드 단위의 실시간  
전송

**Proceed**



전송 중 특정 조건, 패턴에 따른  
실시간 데이터 처리.

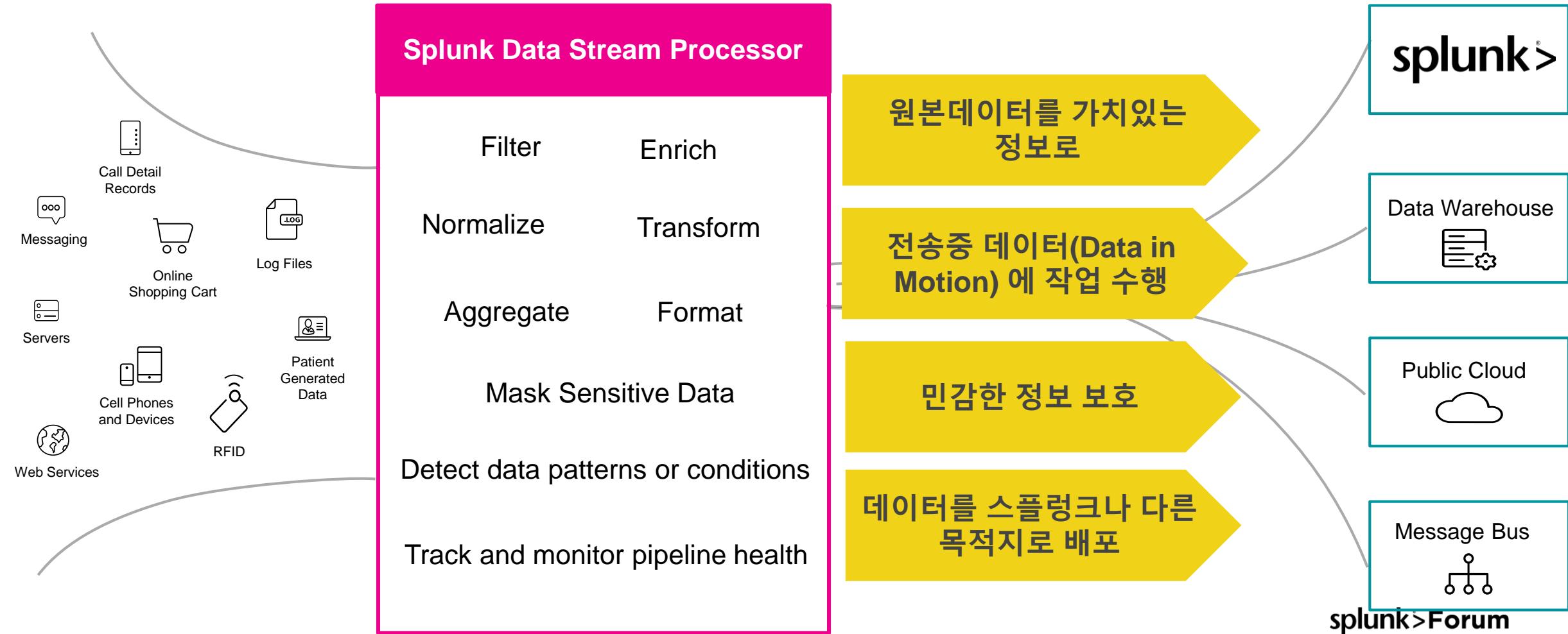
**At Scale**



대용량, 고속의 데이터의  
여러 목적지 시스템들에  
대한 전송 보장

# Splunk Data Stream Processor

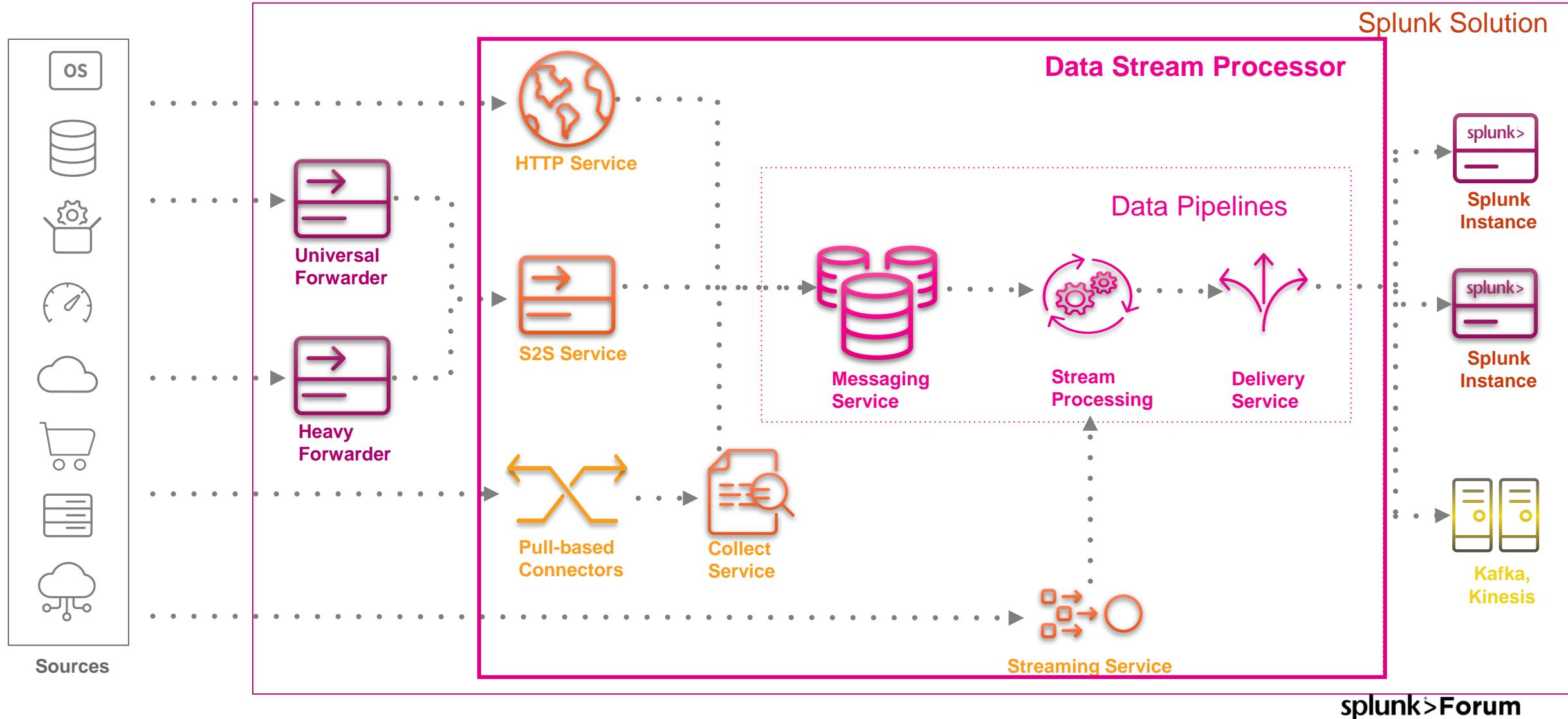
A real-time stream processing solution that collects, processes and delivers data to Splunk and other destinations **in milliseconds**





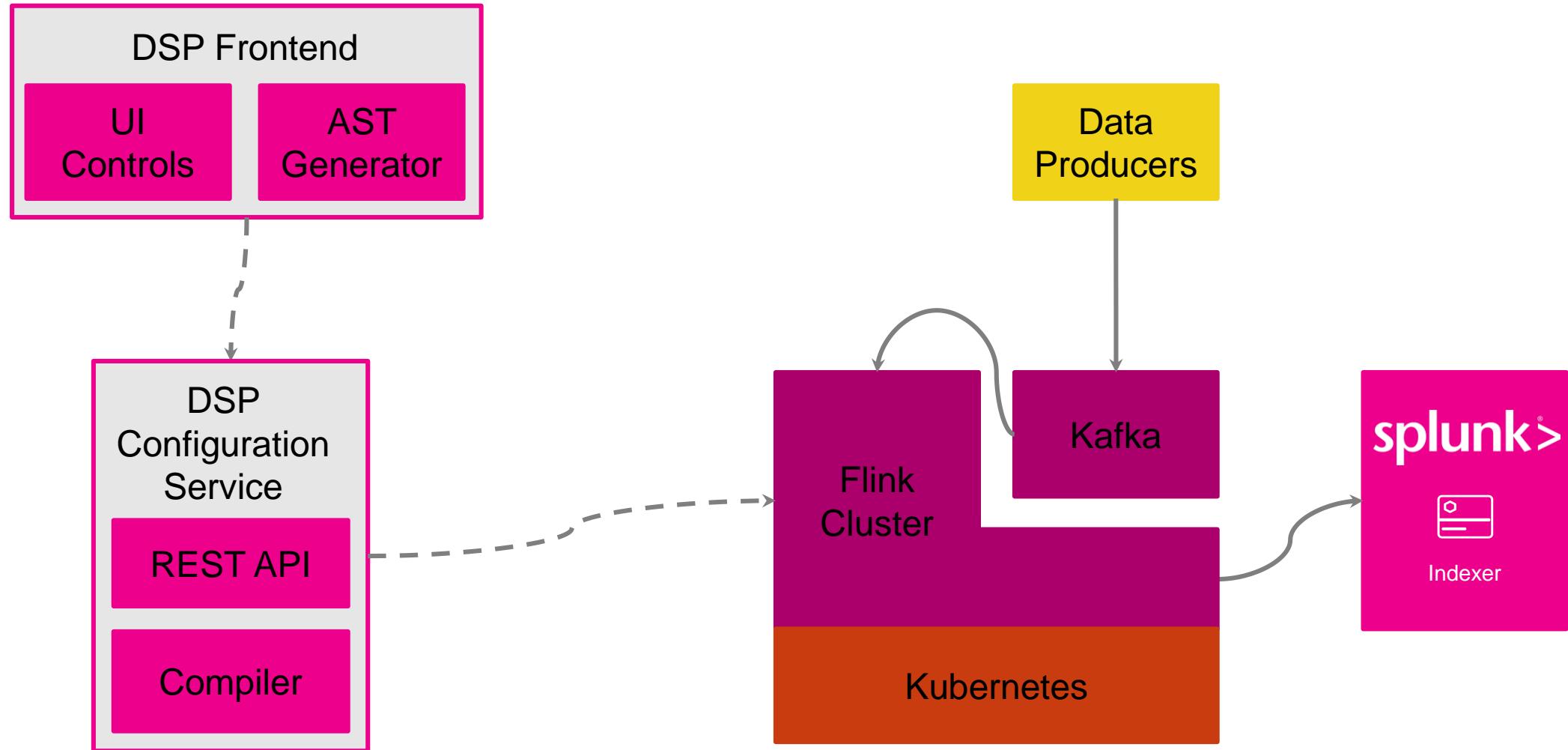
# DSP 아키텍처

실시간 데이터 프로세싱 스플렁크 솔루션



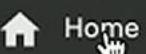
# Overall system

다양한 OSS 를 활용한 Enterprise 급의 Splunk Solution

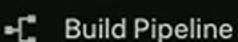


splunk&gt;dsp

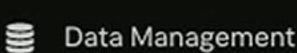
D



Home



Build Pipeline



Data Management



User Management

# Welcome to DSP!

Build pipeline

## Resources

### Data Stream Processor Concepts

Learn more about data stream processor concepts and terminology

[DSP Concepts](#)

### Getting Started

Start here to quickly get up and running with a pipeline

[Get Started](#)

### Functions

Learn about what functions are and what you can do with them

[Functions](#)

## Recently Created

Pipelines ▾

| i | Name                        | Last Modified  | Modified By       | Status  | Created Date   | Created By        | ⋮ |
|---|-----------------------------|----------------|-------------------|---------|----------------|-------------------|---|
| > | Real-time Aggregation-clone | Oct 22nd, 2019 | pdubey@splunk.com | CREATED | Oct 22nd, 2019 | pdubey@splunk.com | ⋮ |
| > | tespipeline                 | Oct 22nd, 2019 | pdubey@splunk.com | CREATED | Oct 22nd, 2019 | pdubey@splunk.com | ⋮ |

← → ⌂ [dsp.splunkbeta.com/dspdemo1/edit?function=e570ff47-b069-4a39-947b-7f2ab8a9e909&id=2dba8ddd-6e06-4054-8bb0-3e046b397cd5&view=view%20configurations](https://dsp.splunkbeta.com/dspdemo1/edit?function=e570ff47-b069-4a39-947b-7f2ab8a9e909&id=2dba8ddd-6e06-4054-8bb0-3e046b397cd5&view=view%20configurations)

Apps Splunk Inc - Sign In > Splunk > service portal S Pwny Portal Egencia - Trips Splunk Inc - My A... Splunk Action Ite... Content Portal Pa... Settings

splunk>dsp

Sensitive Data CREATED

Save Activate Pipeline Validate Stop Preview

Build Pipeline Data Management User Management

Read from Splunk Firehose Buttercup Games Purchase Source Type and Field Ex... Promote Fields

per sec in out events bytes latency per sec in out events bytes latency per sec in out events bytes latency per sec in out events bytes latency

events bytes latency events bytes latency events bytes latency events bytes latency

p99214.00ms avg115.75ms p990.50ms avg0.13ms p9917.00ms avg4.63ms p991.00ms avg0.50ms

+ -

View Configurations Preview Results 20 of 100 events

Buttercup Games Purchase Function Documentation

Predicate

```
1 match-regex(get("host"), /Buttercup/);
```

Help

Help & Feedback

```
graph LR; A[Read from Splunk Firehose] --> B[Buttercup Games Purchase]; B --> C[Source Type and Field Ex...]; C --> D[Promote Fields]
```

# Use Data Stream Processor to help make data driven decisions

DESTINATIONS

splunk>

Kafka

AWS

Syslog

USE CASES

Noise removal &  
Data shaping

Real-time data  
enrichment

Real-time  
alerting

Data routing

Compliance &  
data privacy

REAL-TIME  
STREAM  
PROCESSING

## Splunk Data Stream Processor

DATA SOURCES



Mainframe  
Data



Kafka



Syslog/  
TCP



Mobile



IoT  
Devices



Network  
Wire Data

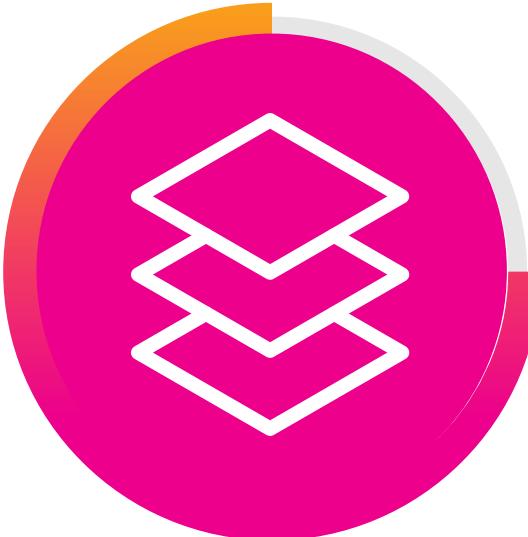
ANNOUNCING  
**Data Fabric Search**

# Big Data Problem



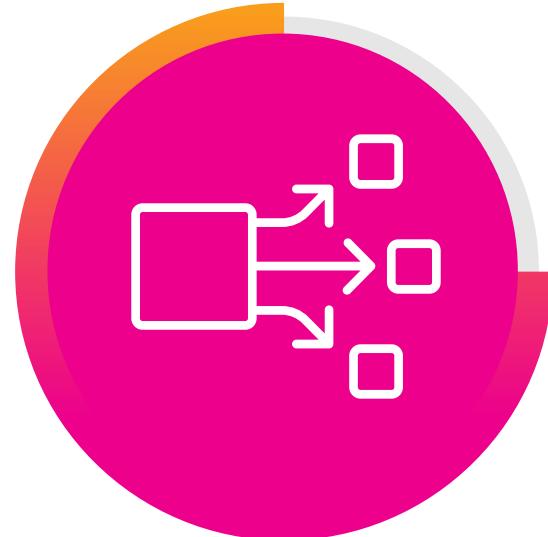
**Volume**

엄청난 크기의 데이터셋



**Variability**

다양한 종류



**Variety**

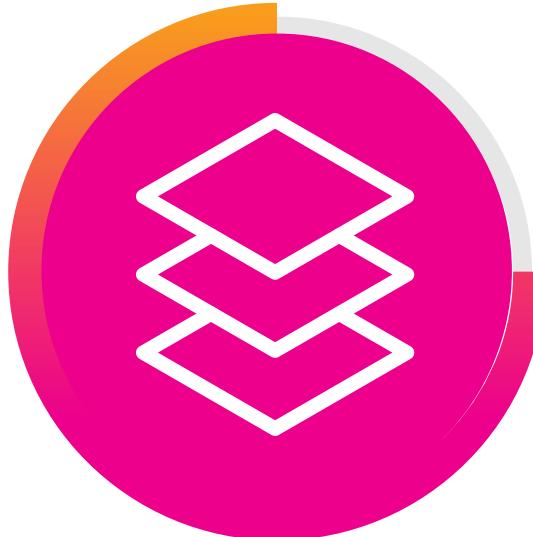
상이한 위치, 사용법

# How to Solve Big Data Problem with DFS



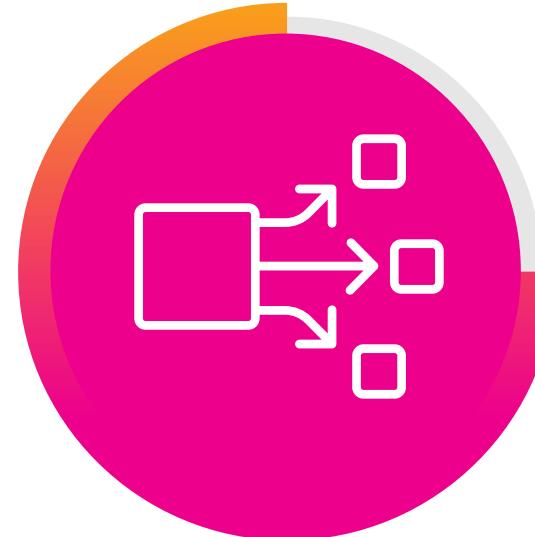
## Big Data Analysis

High Cardinality 대량의  
데이터 셋에 대한 빠른 장기  
배치 분석



## Limitless Join

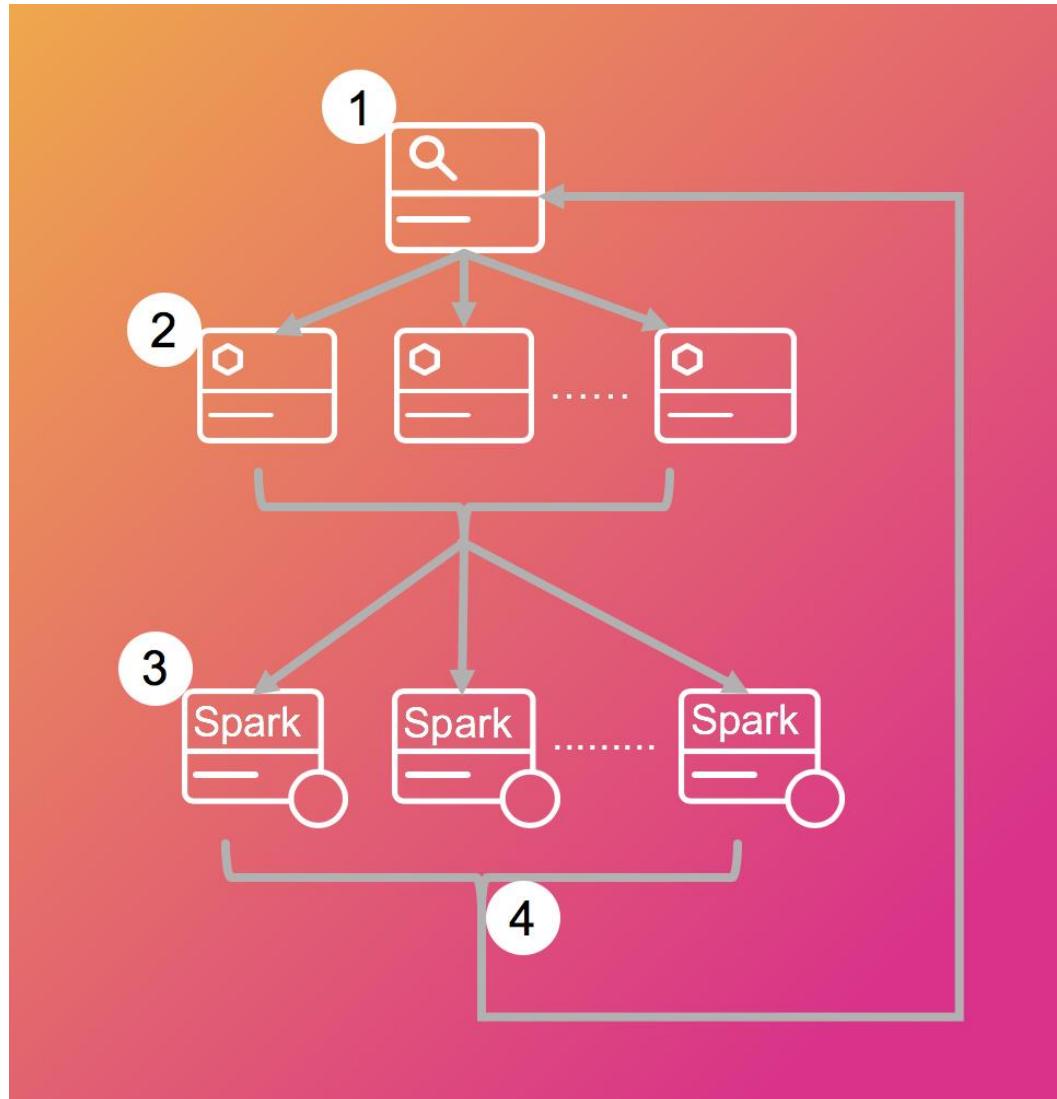
메모리 증가 없이도 대량의  
데이터셋에 대한 제한없는  
조인



## Federated Search

다양한 데이터스토어에 대한  
통합 분석 엔진  
**splunk>Forum**

# Data Fabric Search 의 동작 방식



1. 서치헤드에서 쿼리 수행
  2. 인덱서에서 preprocess된 데이터를 DFS 워커노드에 전송
  3. DFS워커노드에서 분산 프로세싱 수행
  4. 최종 결과를 서치헤드에 전달
- 새로운 문법  
`|dfsjob [search <map>|<reduce> ] [<sh>]`
  - 지원 명령어  
stats, join, sort, head, tail, reverse, dedup, rename, fields, union, from, eval, where
  - DFS Manager를 통한 손쉬운 관리

## splunk>enterprise

Search Datasets Reports Alerts Dashboards DFS Comparison > Search

### Search

```
index=idx_bc_mobile | stats count by clientip,status | sort -count
```

from Dec 1 through Dec 21, 2018

No Event Sampling ▾ Smart Mode ▾

#### How to Search

If you are not familiar with the search features, or want to learn more, see one of the following resources.

[Documentation](#) [Tutorial](#)

#### What to Search

**13,034 Events** **2 days ago** **30 minutes ago**

INDEXED EARLIEST EVENT LATEST EVENT

[Data Summary](#)

> [Search History](#)

## splunk>enterprise

Search Datasets Reports Alerts Dashboards DFS Comparison > Search

### Search

```
| dfsjob [ search index=idx_bc_mobile | stats count by clientip,status | sort -count ]
```

from Dec 1 through Dec 21, 2018

No Event Sampling ▾ Smart Mode ▾

#### How to Search

If you are not familiar with the search features, or want to learn more, see one of the following resources.

[Documentation](#) [Tutorial](#)

#### What to Search

**13,034 Events** **2 days ago** **30 minutes ago**

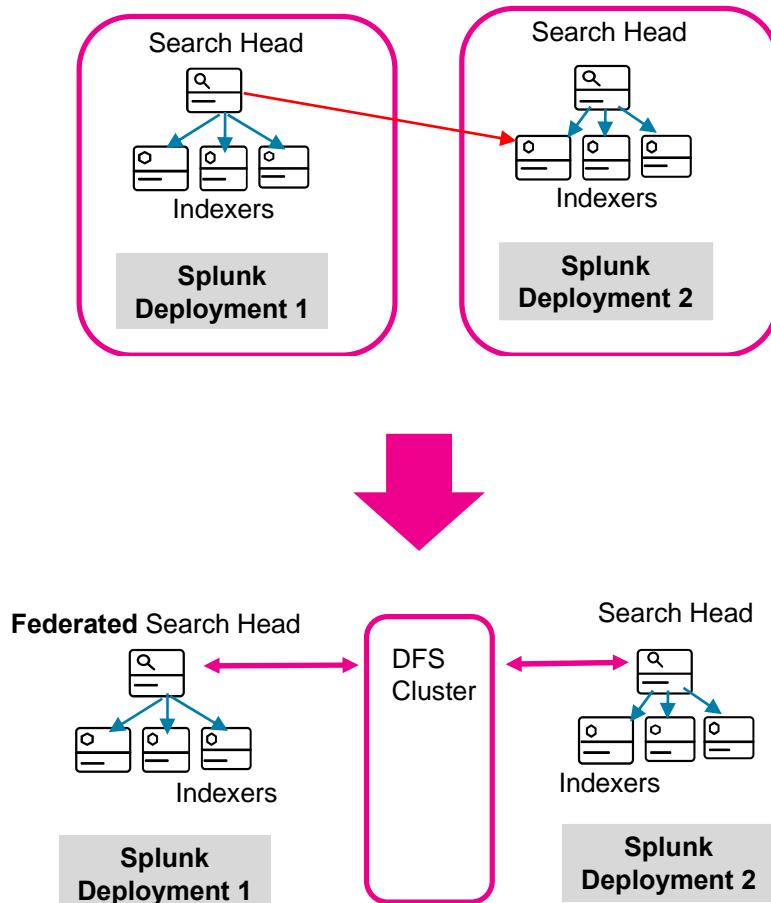
INDEXED EARLIEST EVENT LATEST EVENT

[Data Summary](#)

> [Search History](#)

# Federated Search

여러 스플렁크 deployment 에 대한 통합 검색



Search Datasets Reports Alerts Dashboards DFS Comparison > Search & R Save As ▾ Last 15 minutes ▾

New Search

```
| dfsjob
  [| union
    [| from federated:buttercup_mobile_americas]
    [| from federated:buttercup_mobile_asia]
    [| from federated:buttercup_mobile_emea]
    [| from federated:buttercup_mobile_australia]
    [| from federated:buttercup_mobile_remaining_all]
  ]
  | stats sum(totalCount) by status,clientip |
```

✓ 5,948,740 events (9/21/18 2:40:17.000 PM to 9/21/18 2:55:17.000 PM) No Event Sampling ▾ Job ▾ II ⏪ ⏩ ⏴ Smart N

Events Patterns Statistics (2,000) Visualization

20 Per Page ▾ Format < Prev 1 2 3 4 5 6 7 8 ...

| status | clientip   | sum(totalC) |
|--------|------------|-------------|
| 200    | 10.2.1.101 |             |
| 200    | 10.2.1.2   |             |

# Federated Search

3rd party datastore(pre-release)

스플렁크에 인덱싱할 필요 없이 데이터가 있는 곳에서 통합 검색/분석/조인 수행

New Search Save As ▾ Close

```
|dfsjob
union[|from federated:deployment_hdfs:" search index=car | stats sum(voltage) as sum_voltage,count as count_vin by vin"]
[search index=cardatainfo | stats sum(voltage) as sum_voltage,count as count_vin by vin ]
|stats sum(sum_voltage) as sum_voltage,sum(count_vin) as count_vin by vin | eval avg_voltage =sum_voltage/count_vin| where avg_voltage< 798|fields vin, avg_voltage
|join type=inner usetime=f left=L right=R where L.vin=R.vin
[|from federated:s3_deployment:" index=vendorMap | stats count as count_vin_vendorId by vin,
vendorId, vendorName, location"]
|rename L.vin as vin, L.avg_voltage as voltage, R.location as location, R.vendorId as vendorId, R.vendorName as vendorName | fields vin, vendorId, vendorName, location
]
```

All time 🔍

✓ 1,130,221,241 events (before 10/21/19 4:20:15.000 AM) No Event Sampling Job ▾ Smart Mode ▾

Events Patterns Statistics (250) Visualization

100 Per Page Format < Prev 1 2 3 Next >

| vin                | vendorId | vendorName            | location  |
|--------------------|----------|-----------------------|-----------|
| 1BMAA38743LLB08454 | 00003938 | Advanced Batteries CN | Monterey  |
| 1BMAA38743LLB01302 | 00003938 | Advanced Batteries CN | Sunnyvale |
| 1BMAA38743LLB02712 | 00003938 | Advanced Batteries CN | Fremont   |



# Splunk 환경

Yahoo / AOL mail 데이터:

|                   |  |
|-------------------|--|
| Ingestion Rate    | Over 1 Petabyte/day ingestion                            |
| Events            | Over 2 Trillion events/day processed                     |
| Indexers          | 1600 indexers in 7 index clusters                        |
| Search Heads      | SHC with 6 heads   |
| DFS Compute Nodes | 300 Spark nodes  |
| Users             | Hundreds of development and production engineering users |



# Classic VS DFS 성능 비교

| Job size    | Classic SPL   | DFS Improvement                         | Analysis query   |
|-------------|---|---|--|
| 4B events   | Auto-finalizes due to time<br>Search very slow                    | Complete, accurate,<br>>10x faster      | Rewrote Classic to remove join   |
| 3.5B Events | Auto-finalizes<br>Incomplete results                              | Complete, accurate,<br>12x faster       | Simple stats in both Classic and DFS   |
| 4B Events   | Auto-finalizes<br>Incomplete results                              | Complete, accurate<br>2x faster         | Used stats of multi-valued fields<br>that didn't scale well with DFS                                       |
| 115M events | Subsearch that auto-finalized<br><br>Search had only 3% of events | Complete and accurate<br><br>Same speed | Complicated query with join of two indexes over lots of data.<br><br>24 hours of data produced 115M events |



# Verizon Media

잠재적 고객 이슈에 대한 감지 및 응답 시간 감소

*With Splunk's new Data Fabric Search, we can detect and respond to potential issues within minutes, not hours, so our teams can focus on delivering innovative and personalized products for our customers. Data Fabric Search harnesses the power of multiple Splunk deployments to gain operational insights about billions of events with optimized, scalable queries.*

—Jon Prall, VP Communications Production Engineering, Verizon Media

# 하나의 플랫폼 - Data Fabric Search

USE CASES



ADVANCED ANALYTICS SOLUTION

## Data Fabric Search

DATA STORES

**Business Operations****Security****IT**

DATA SOURCES



Mainframe Data



Forwarders

Syslog/  
TCP

Mobile

IoT  
DevicesNetwork  
Wire DataRelational  
Databases

ANNOUNCING

# Splunk Connected Experiences

70억 인구 중 모바일 기기 사용자

60억

“밀레니얼 세대의 **90%**가 모바일  
폰을 손에서 놓지 못해...” *by Forbes*

모바일 환경 덕분에 비지니스

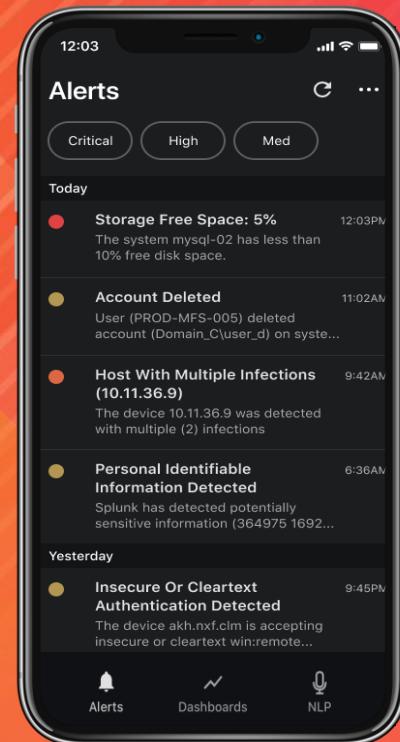
프로세스 효율성 **30%** 개선, 업무

생산성은 **23%** 높아져...*by TechJini*

**splunk** > turn data into doing™

# Splunk® Connected Experiences

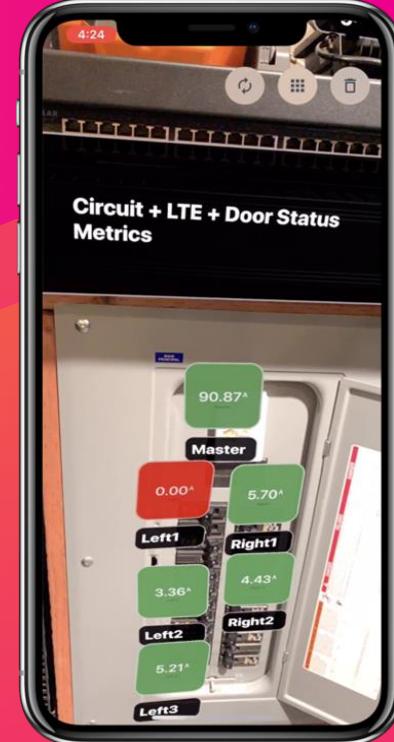
더 빠른 의사 결정을 위한 insights 를 전달합니다.



Stay connected with  
on-the-go visibility



Empower non-technical  
users to access data

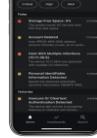


Provide contextual  
insights that inspire action

# Connected Experiences Apps

언제 어디서든 가능합니다.

## Splunk® Mobile



## Splunk® TV



## Splunk® AR



## Splunk® VR



## Splunk® NLP



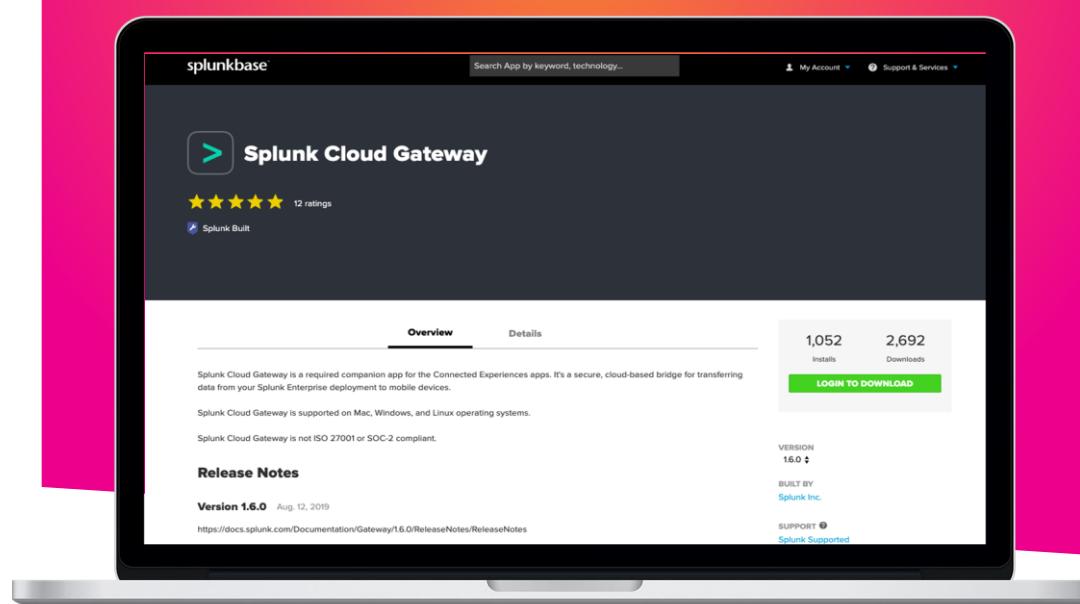
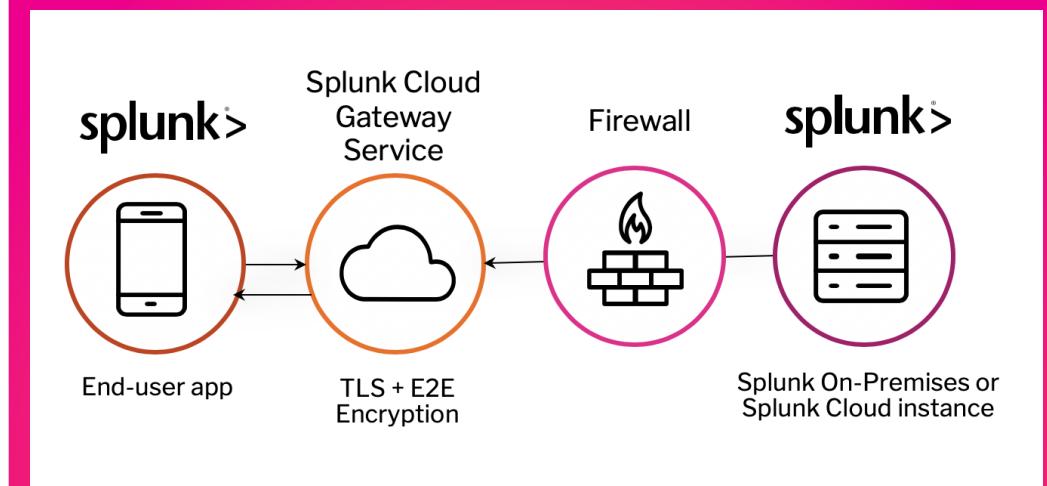
## Splunk® Cloud Gateway

splunk>enterprise

splunk>Forum

# Splunk® Cloud Gateway

ConnEx 기술을 위한 안전한 인증 서비스

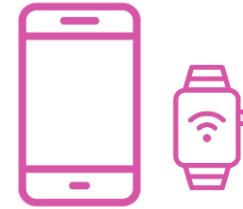


- 안전한 엔드-투-엔드 암호화를 지원하는 클라우드 서비스로 Splunk® Enterprise 및 Splunk® Cloud 인스턴스와 연결
- 쉽고 간편한 인증 방식으로 Easy Mobile Engagement



# Splunk® Mobile

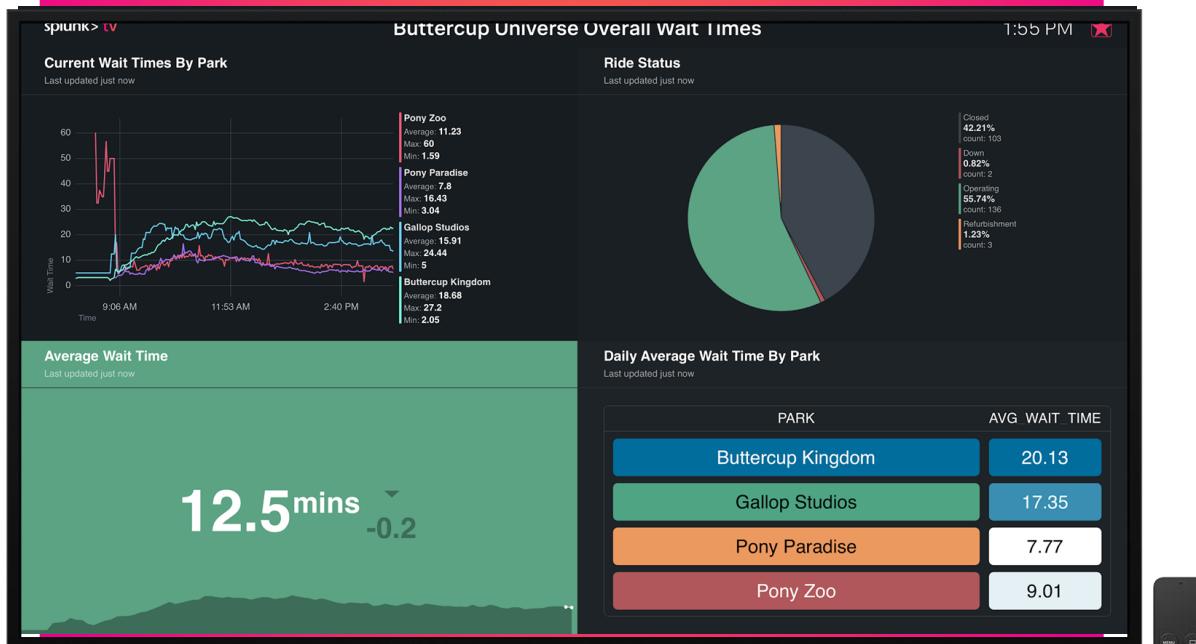
모바일 기기를 위한 최적의 대시보드



- Splunk® Platform 기능을 확장함으로써  
지속적인 인사이트 획득
- iPhone, Android 모바일 기기, Apple 스마트  
워치에서 알람을 처리하고 데이터를 확인
- iPhone 에서는 Phantom® platform 과  
연동되며 MDM 을 통한 앱 배포 및 관리

# Splunk® TV

고급스런 고해상도 대시보드 화면



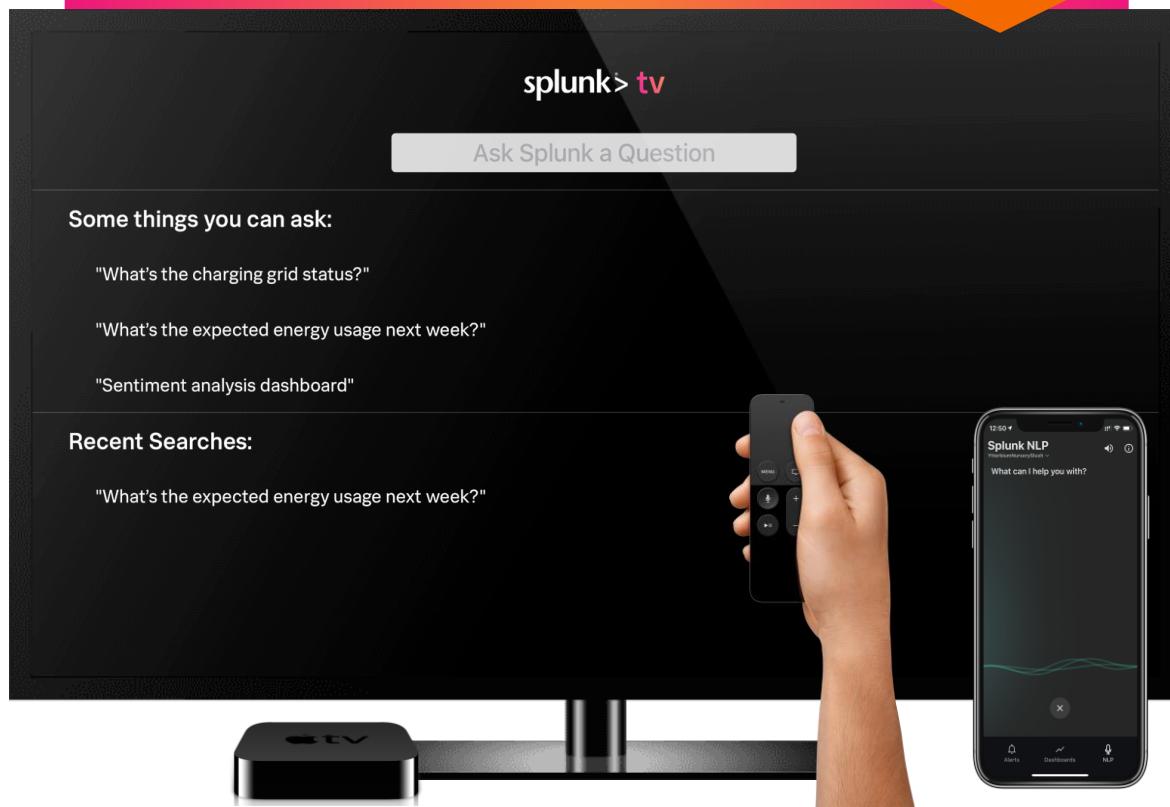
- NOC 과 SOC, 시니어 리더쉽을 위한 최상의 디스플레이 환경
- Apple TVs 에서 높은 해상도로 Splunk® Enterprise 와 Splunk® Cloud 대시보드 디스플레이

# Splunk® NLP

말로 하는 검색

*"What were our sales  
from last month?"*

*"What percentage of incidents were  
flagged as 'critical' last quarter?"*

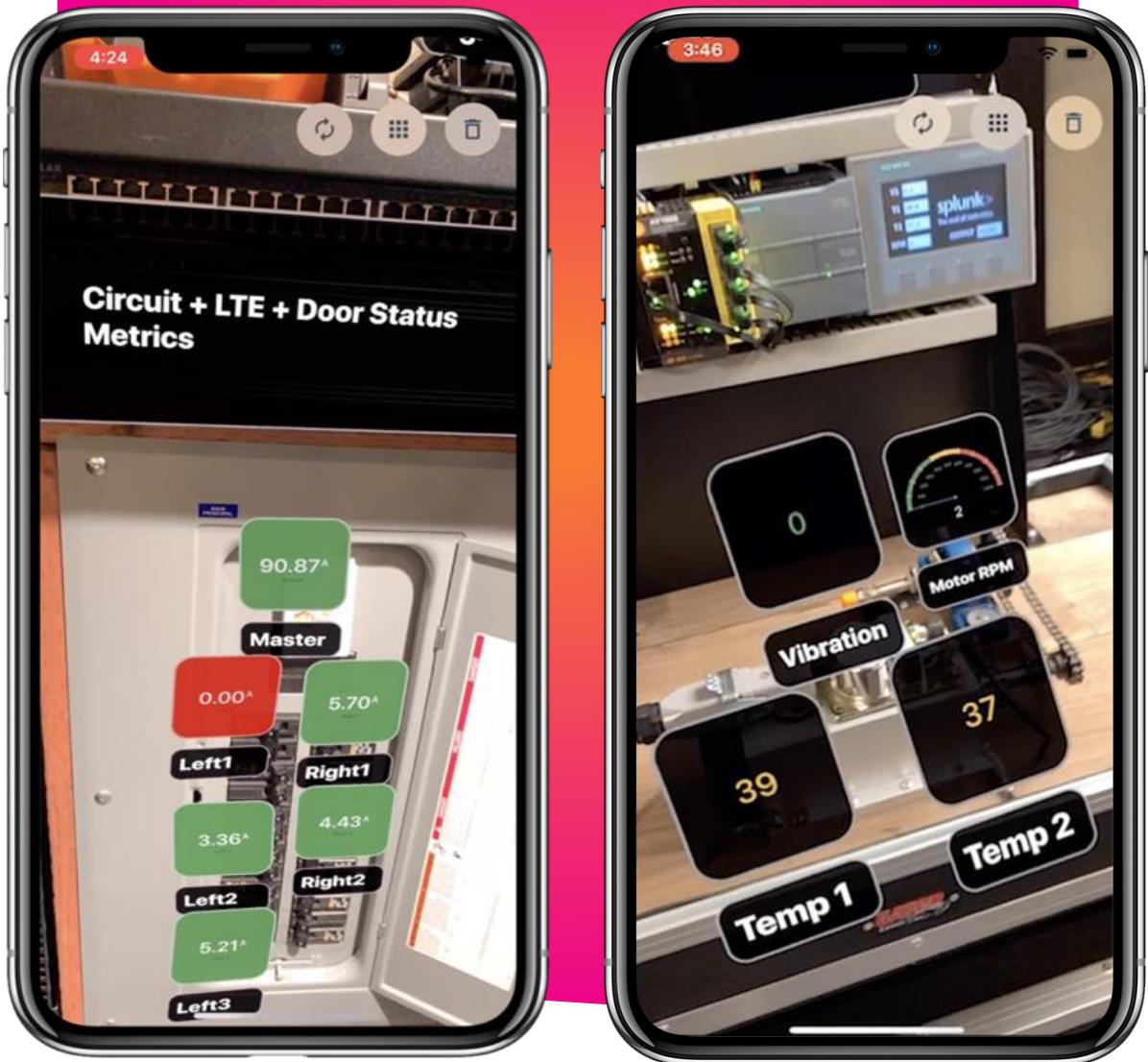


- Splunk® Mobile 과 Splunk® TV 를 통한 자연어 처리 기반의 말로 하는 검색
- Splunk SPL 작성 없이 비지니스 사용자가 쉽게 질문하고 답을 획득

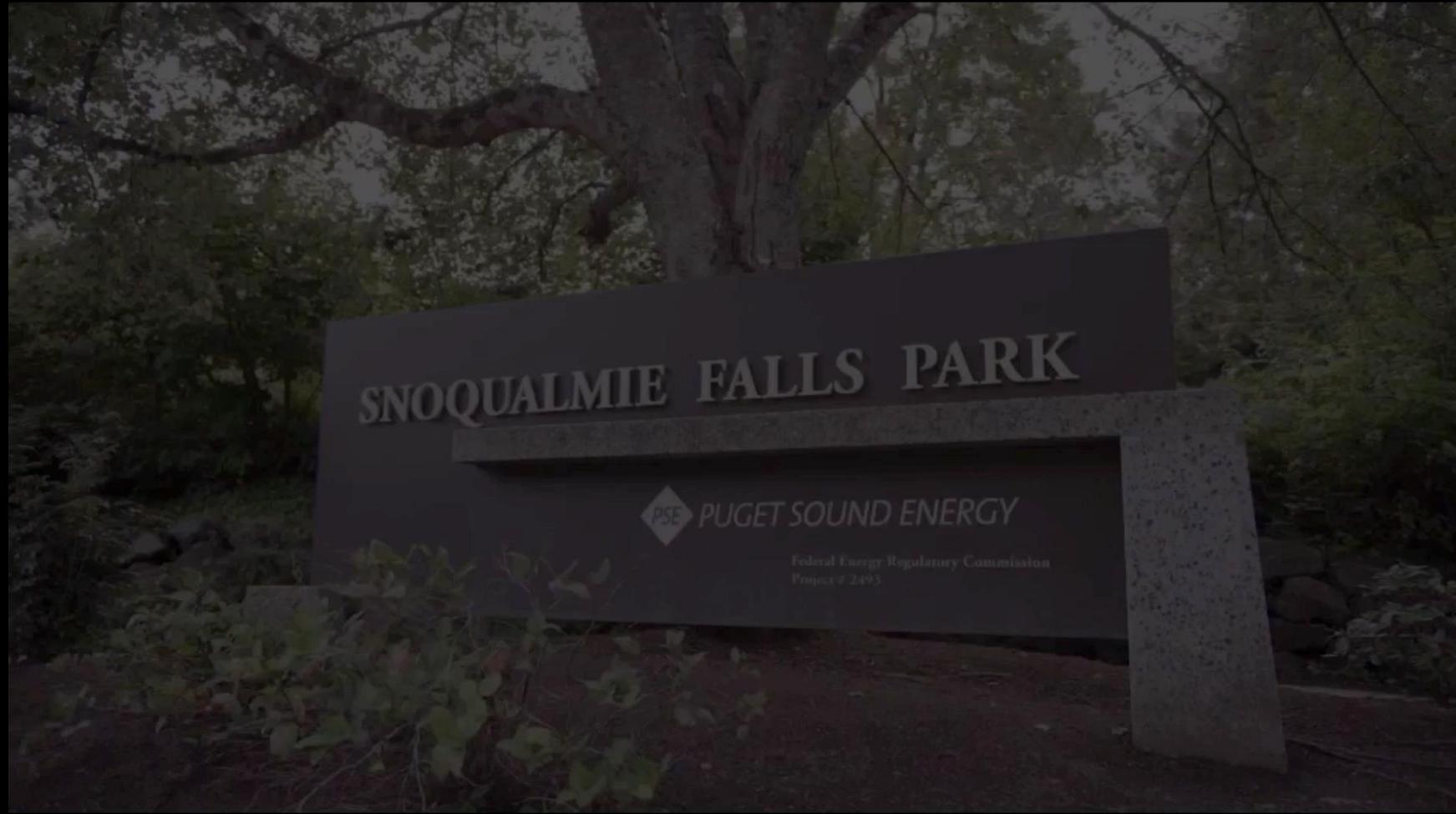
splunk>**Forum**

# Splunk® AR

## 증강현실을 통해 데이터를 경험



- 모바일 기기를 통해 온디맨드 방식으로 인사이트를 획득하고 신속하게 데이터를 확인
- Splunk® AR 은 IT 뿐만 아니라 IoT 에도 활발하게 활용 가능: 어플리케이션 혹은 플랜트 다운에 영향을 미치는 데이터를 관제



# Splunk® VR

## 가상 현실을 통한 데이터 경험



- 3D 공간에서 전체적이고 직관적인 정보 확인
- 주변 공간을 최대한 활용하면서 간편하게 트렌트를 확인하고 다수의 대시보드를 동시에 확인

# Connected Experiences 가 선사하는 Benefits



Cloud  
Gateway



Mobile



TV



NLP



AR



VR



For you

Stay connected with  
on-the-go visibility

Empower non-technical  
users to access data

Provide contextual insights  
that inspire action

- For your business
- Faster collaboration
  - Better productivity

- Faster time to insight
- Better knowledge sharing

- Faster time to resolution
- Better decision making

# Splunk® Connected Experiences

더 빠르게 지속적으로  
양질의 인사이트 획득



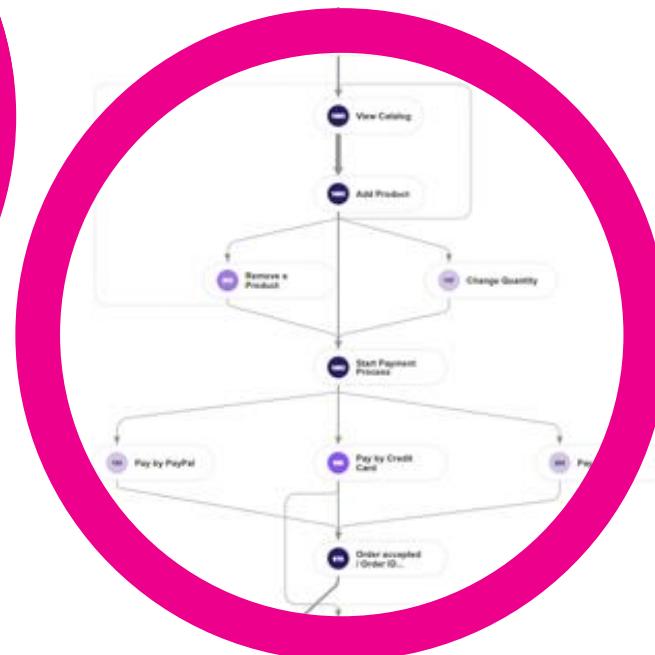
ANNOUNCING

# Splunk Business Flow

Splunk Business Flow 는  
비지니스 프로세스상의 비효율 지점을  
파악하기 위한 **프로세스 마이닝** 툴입니다.

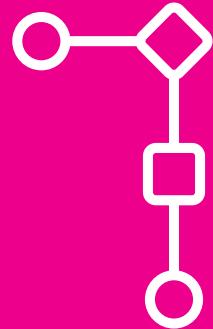
# Process Mining

## 프로세스 분석 기법



- 이벤트 로그를 기반으로 비즈니스 프로세스 분석을 지원하는 프로세스 관리 분야의 기술로, 특정 데이터 마이닝 알고리즘이 이벤트 로그에 적용되어 이벤트 로그에 포함된 트렌드, 패턴, 상세정보를 찾아내는 기법. -*Wikipedia*
- 공항 승객 입출국 프로세스, 상품 거래 프로세스 등 비지니스 프로세스 분석

# Splunk Business Flow 기능



End-to-end process  
discovery through  
event stitching



Investigate  
drill-down with  
exploration interface



Side-by-side  
A/B comparison  
of process flows



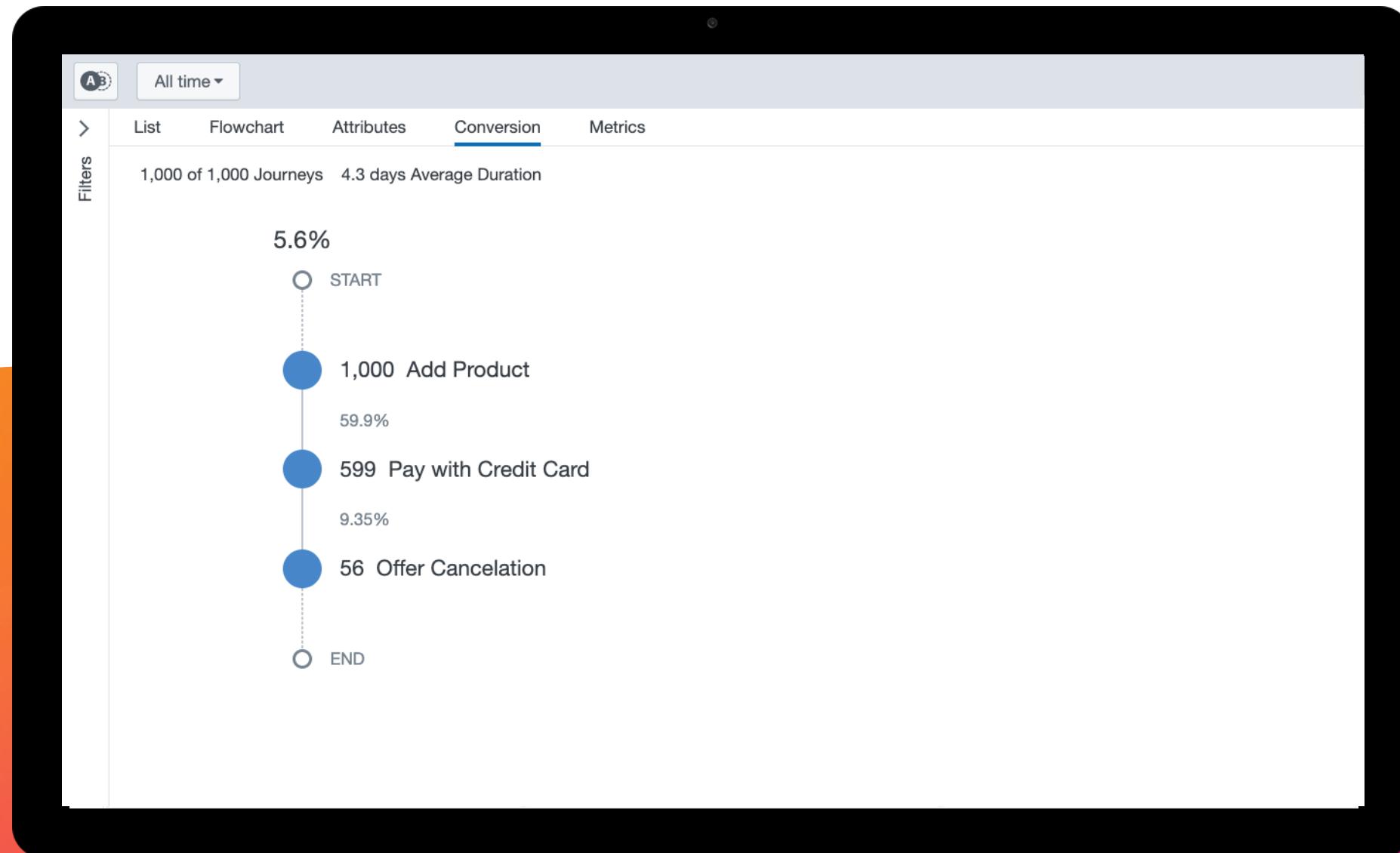
Conformance  
checking and  
deviation notifications

## SPLUNK BUSINESS FLOW

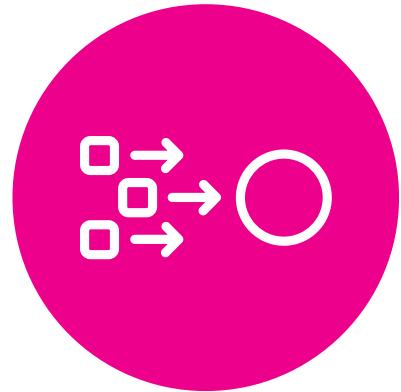
splunk >enterprise

splunk >cloud

splunk>Forum

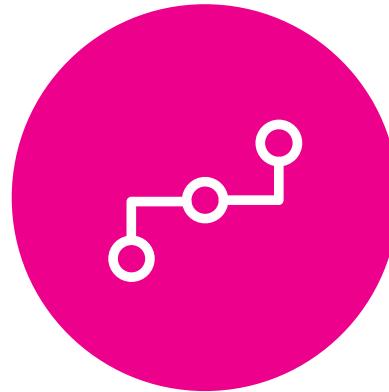


# 3 단계로 끝!



1

이벤트 데이터  
소스에서 프로세스를  
정의하는 공통  
identifiers 확인



2

이벤트 스트림을  
정의하고 identifiers 를  
correlating 함으로써  
플로우 모델을 디자인



3

비지니스 사용자는  
스스로 프로세스를  
탐색하고 시각화

Splunk > enterprise App: Splunk Business Flow ▾ MJ Lee ▾ Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

## Preview: Retail - Online Shop End-to-End 🛍

All time ▾

Filters 1

Top Clusters

| Cluster   | Percentage |
|-----------|------------|
| Cluster 1 | 6%         |
| Cluster 2 | 4%         |
| Cluster 3 | 3%         |
| Cluster 4 | 2%         |
| Cluster 5 | 2%         |
| Cluster 6 | 2%         |
| Cluster 7 | 2%         |
| Cluster 8 | 2%         |
| Cluster 9 | 2%         |
| Others    | 75%        |

Attributes

- > basket\_id
- > client\_ip
- > product\_id
- > shipping\_id
- > stage

Step

Search steps... showing 27 of 27

| Action             | Count |
|--------------------|-------|
| Add Product        | 1,000 |
| Change Quantity    | 158   |
| Check Availability | 976   |

List Flowchart Attributes Conversion Metrics

1,000 of 1,000 Journeys 4.3 days Average Duration

zoom Reset Layout

Properties 1

Layout

- Circuit
- Lanes

Noise

Step Count

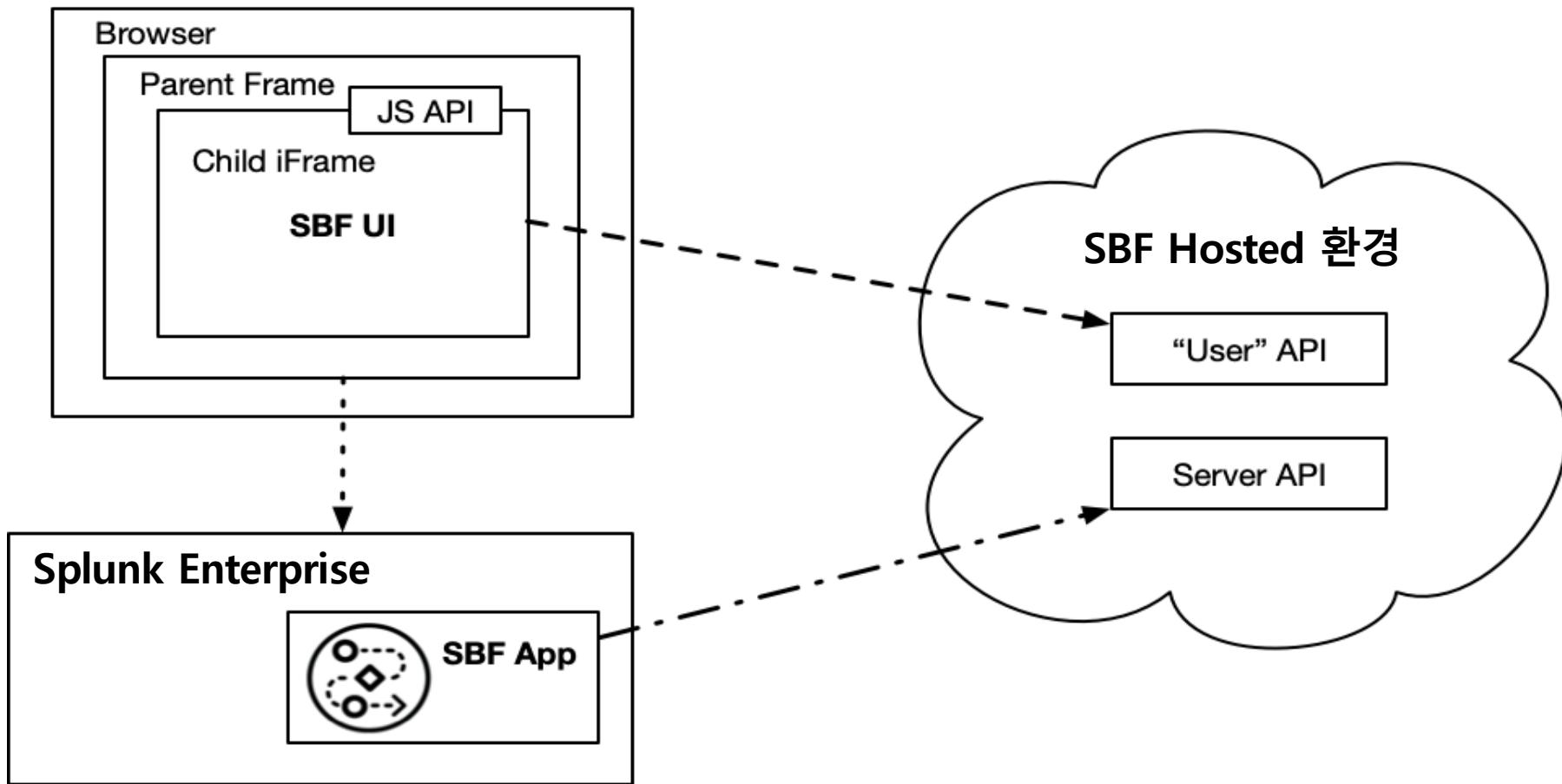
- Journey Step Count
- Absolute Step Count
- None

Path Performance

- Path Avg. Duration
- Path Avg. Duration ±2σ
- Path Count
- None

# SBF 하이브리드 어플리케이션 아키텍처

SBF의 개념적인 전체 아키텍처





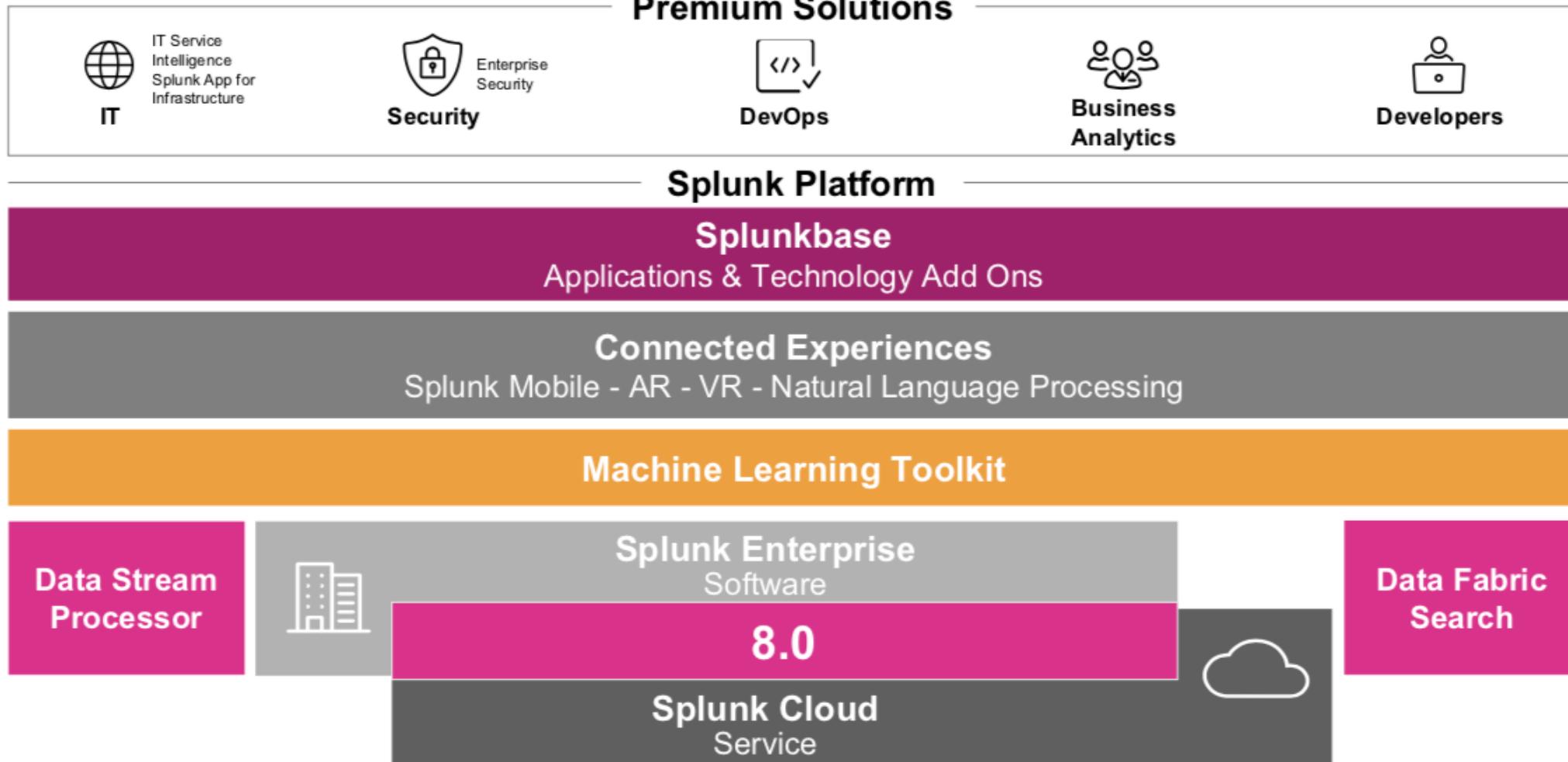
# Splunk® Business Flow

비지니스 프로세스를 시각화하고 분석하고 개선함으로써  
최적의 프로세스를 찾아보세요!

# Summary

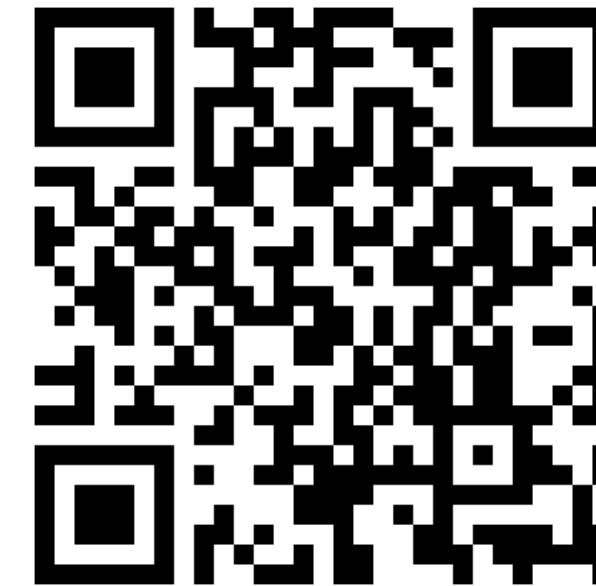
splunk>Forum

# Splunk Delivers a complete Portfolio for tuning Data into Business Outcomes



# 스플렁크 코리아 카카오톡 플러스친구 OPEN EVENT!

‘스플렁크 코리아’ 카카오톡 채널 등록하고  
스타벅스 커피 상품권 받으세요!



감사합니다