© 2019 SPLUNK INC.

What's New in Splunk

2019년 Data to Everything Platform 의 새로운 기능들

최승돈 / 이미정 매니저
스플렁크 코리아

December 12, 2019

splunk>Forum

© 2019 SPLUNK INC.

Forward-Looking Statements

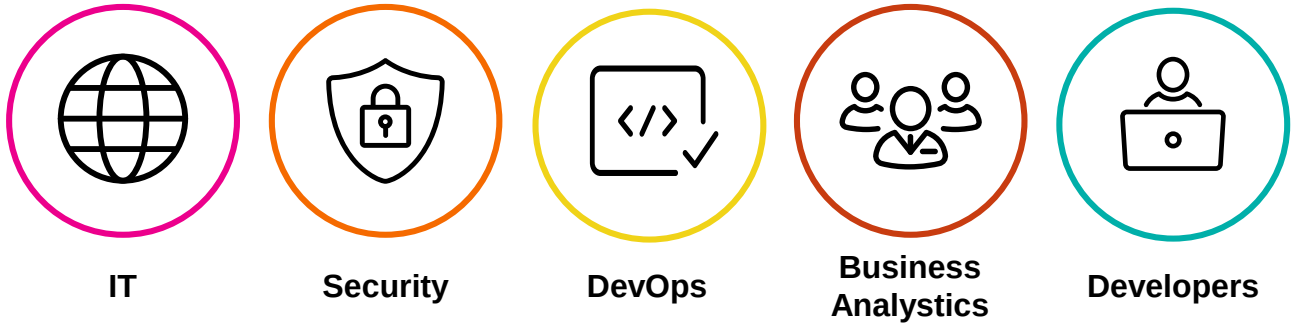
During the course of this presentation, we may make forward-looking statements regarding future events or plans of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results may differ materially. 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. © 2019 Splunk Inc. All rights reserved.

© 2019 SPLUNK INC.

스플렁크의 데이터를 비지니스 결과로 바꾸는 종합적인 접근법



Analyze with differentiated AI and ML

Splunk Data-to-Everything Platform

Investigate the expanding data universe

On-Premises

Cloud

Deployment

splunk>Forum

© 2019 SPLUNK INC.

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

© 2019 SPLUNK INC.

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


거 대충 넘어갑시다

© 2019 SPLUNK INC.

ANNOUNCING

Splunk Enterprise 8.0

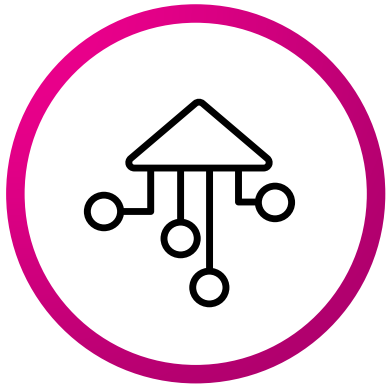
splunk> turn data into doing®

© 2019 SPLUNK INC.

Splunk Enterprise 8.0

Delivers management at scale for a fully observable enterprise

계속되는 성능 향상과 데이터 확장

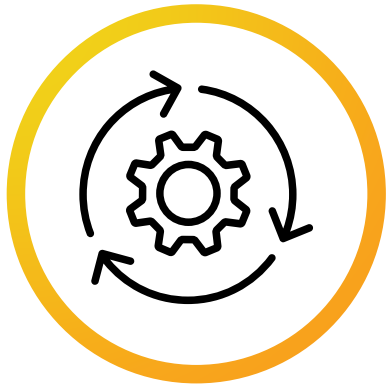


Search
Metrics and Events
Performance Enhancement
Shared DMA Summaries

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

© 2019 SPLUNK INC.

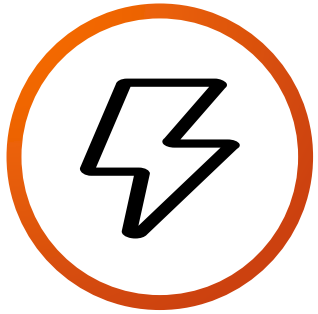
보다 빠른 검색

Faster Searches. Automatically.

Tstats Optimizer

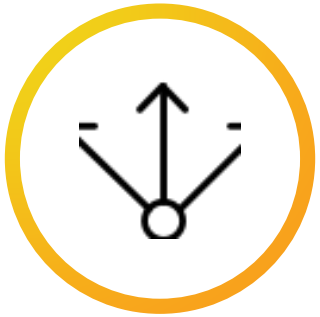
Index-Field사용시
자동으로 stats → tstats으로 최적화
99.8% 성능 개선

Shared Lookup



자동으로 Search Process내 Lookup 재사용
메모리 사용량 감소 및 성능 증가
65% 성능 개선

Bundle Rep 속도 개선

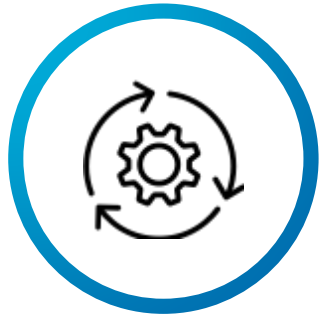


SHC 번들 복제,
SH – SP 번들 복제 시간
10배 이상의 향상
빠르고 보다 정확한 검색

MetricStore v3

메트릭 인덱스 저장 공간 최적화
성능 향상

DMA Summary Sharing



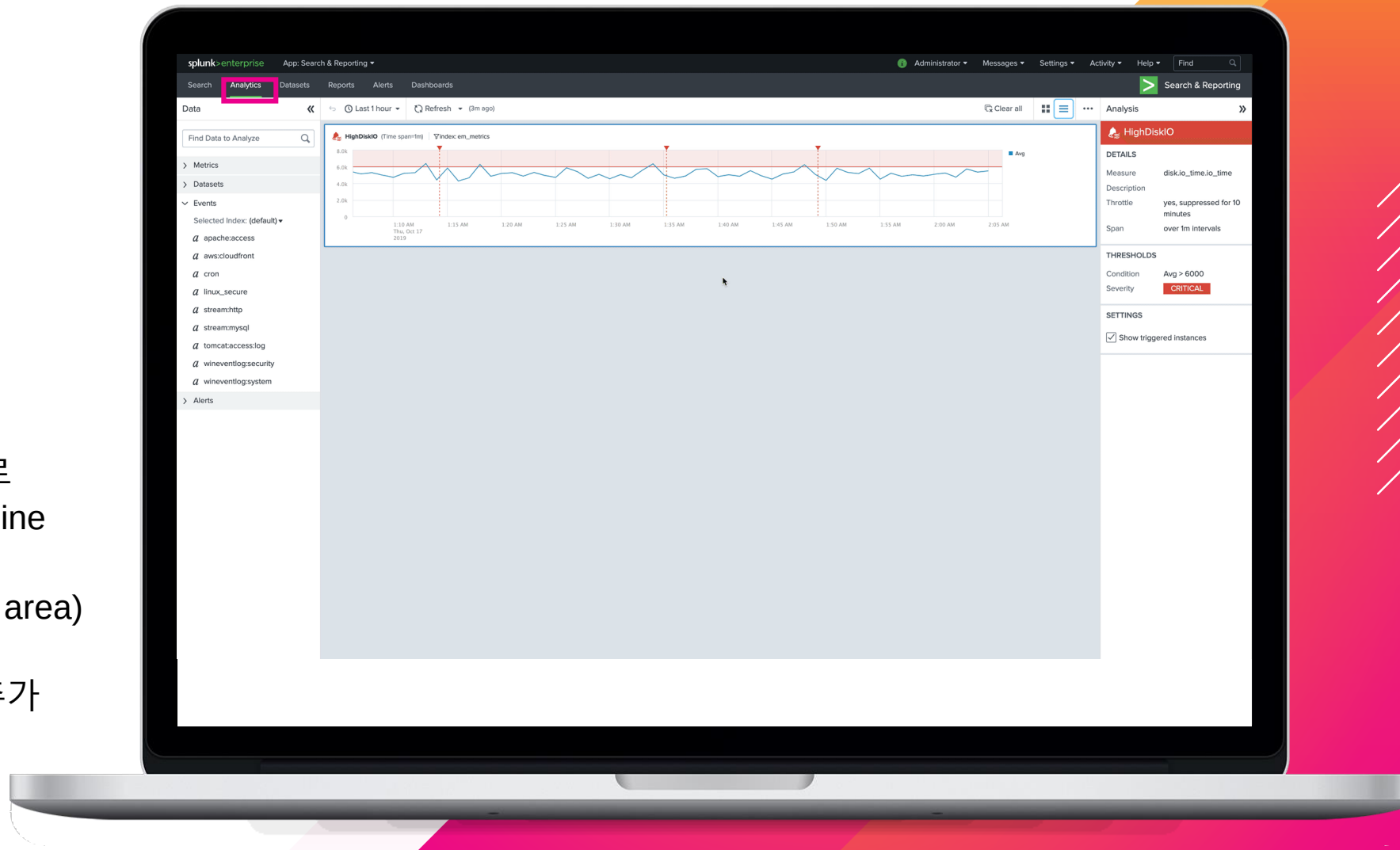
DMA summary정보를
여러 SH/SHC간의 공유

splunk>Forum

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> turn data into doing

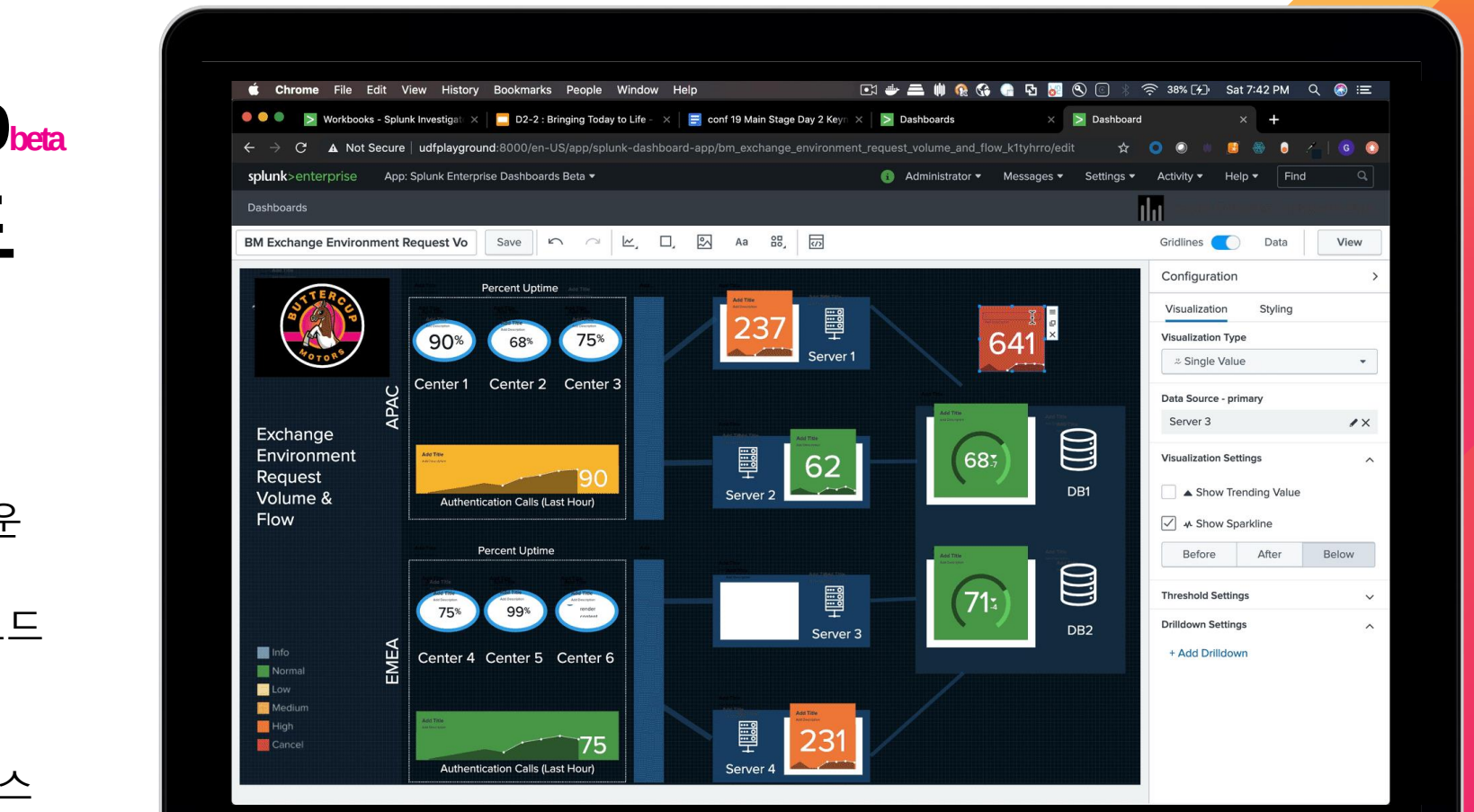
© 2019 SPLUNK INC.

Splunk Dashboard App beta

새로운 대시보드

빠르고 직관적인 새로운 대시보드 경험

- 픽셀단위까지 정확한 자유로운 커스터마이징 대시보드 제공
- 레이아웃과 UI 를 통한 대시보드 변경 기능
- Image, Background, Icon의 손쉬운 추가로 고객의 비지니스 업무에 좀더 직관적인 시각화 제공



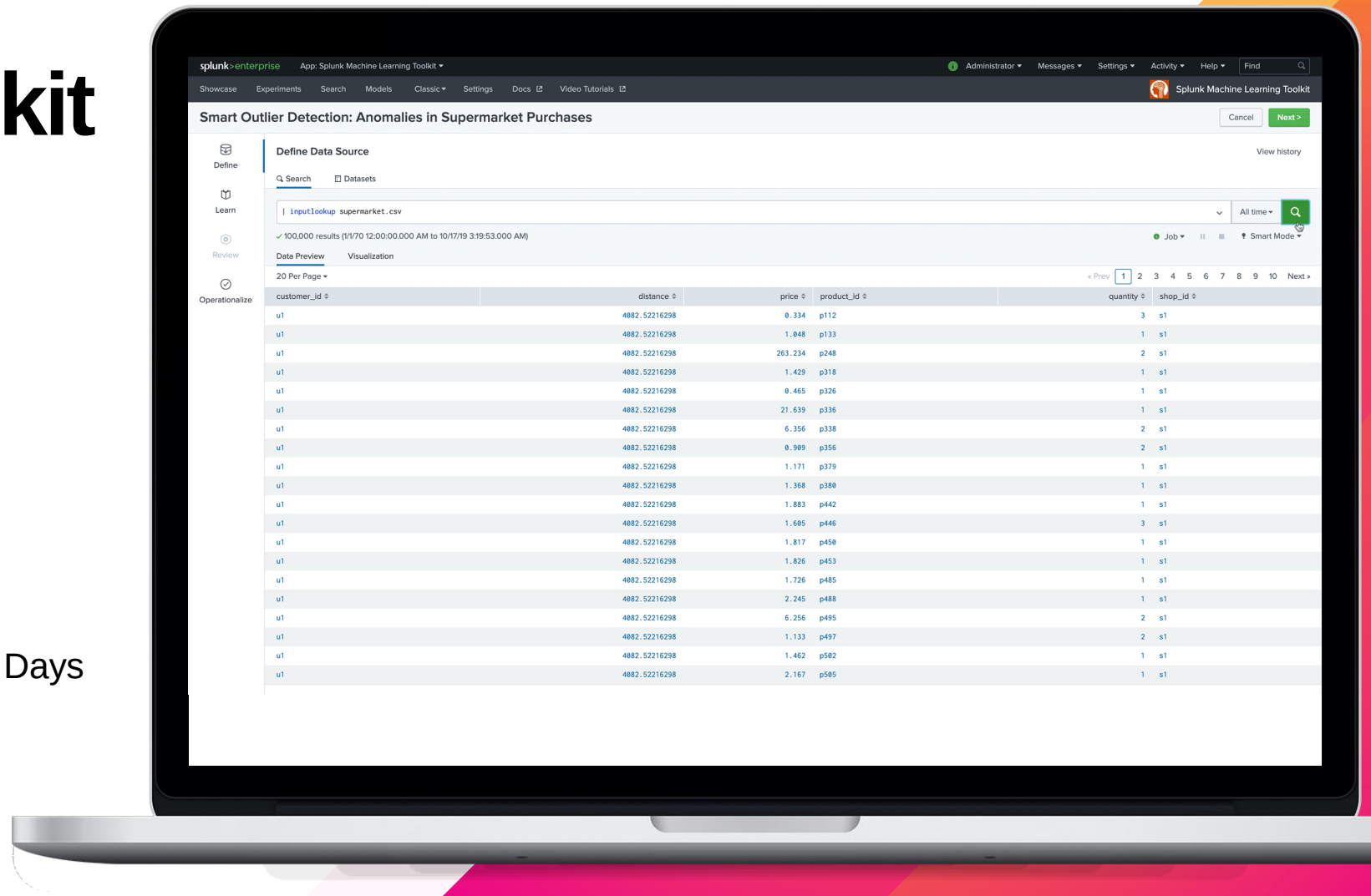
© 2019 SPLUNK INC.

splunk> turn data into doing

Machine Learning Toolkit 5.0

머신러닝을 보다 손쉽게

- 새롭고 현대적인 쇼케이스 레이아웃으로 손쉬운 ML접근
- 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



splunk> turn data into doing

© 2019 SPLUNK INC.

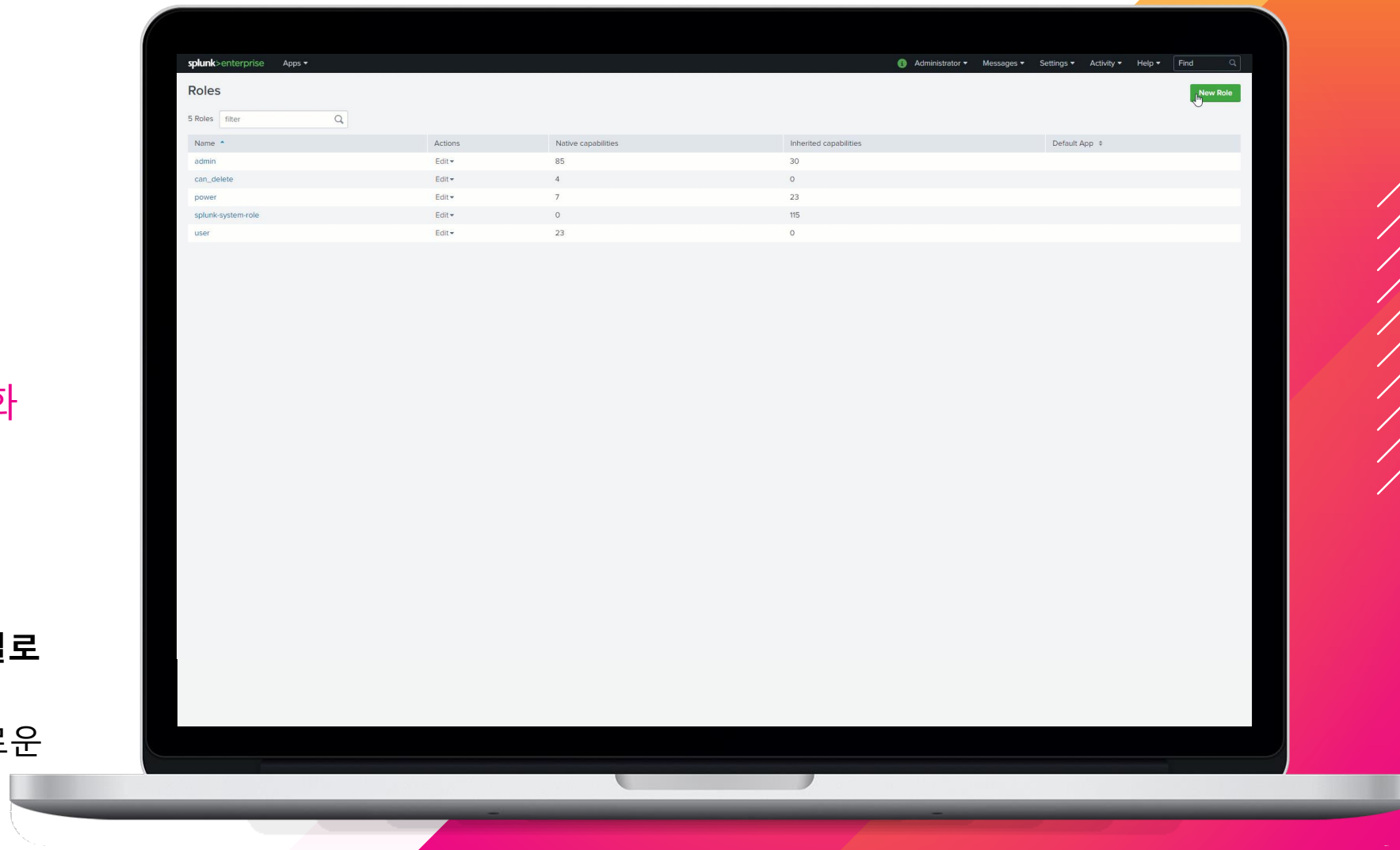
강화된 보안 기능

Indexed Fields Access Controls

보다 정교한 접근 제어

인증 토큰 사용으로 보안성 강화

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

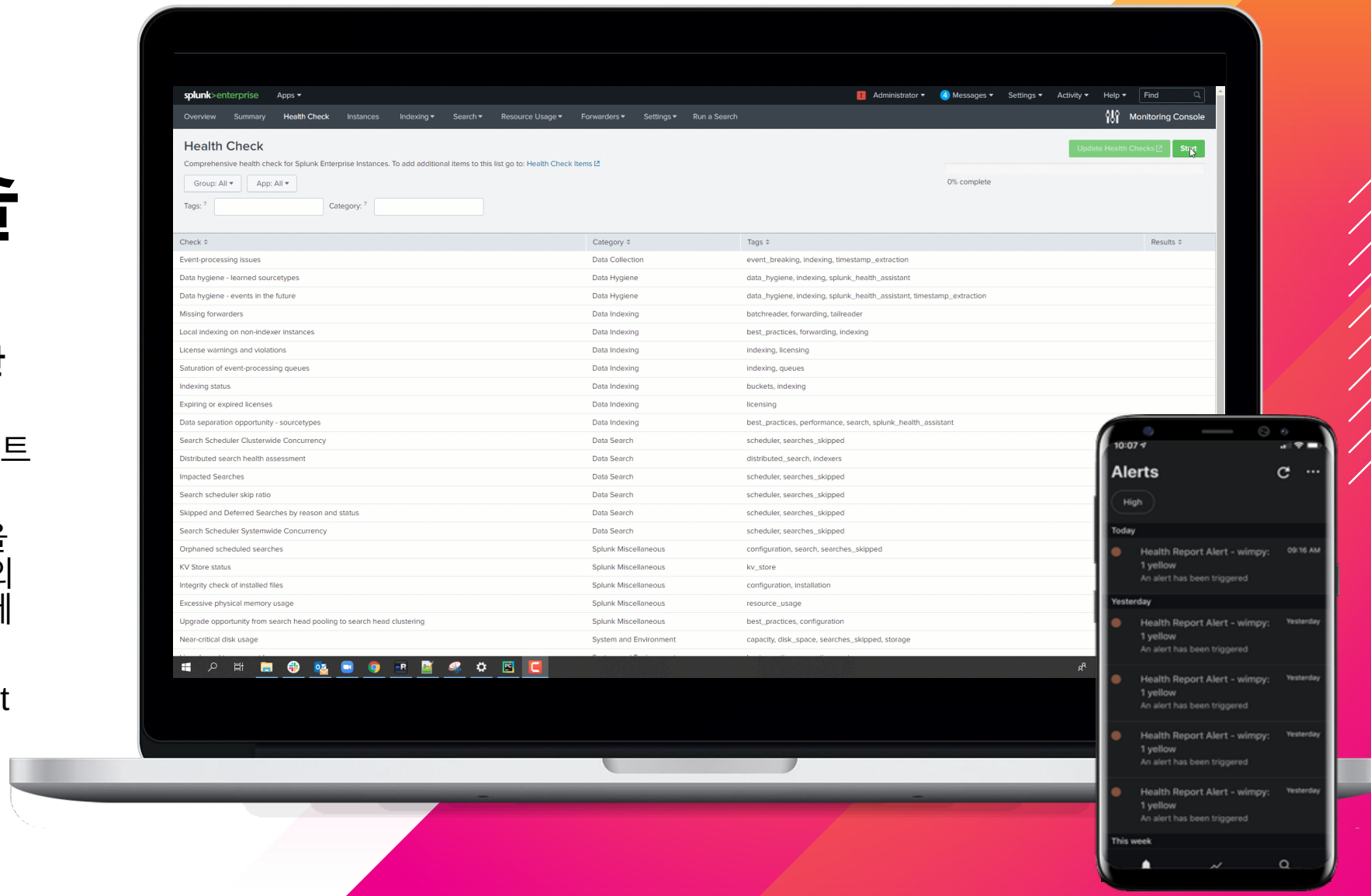


splunk> turn data into doing

© 2019 SPLUNK INC.

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



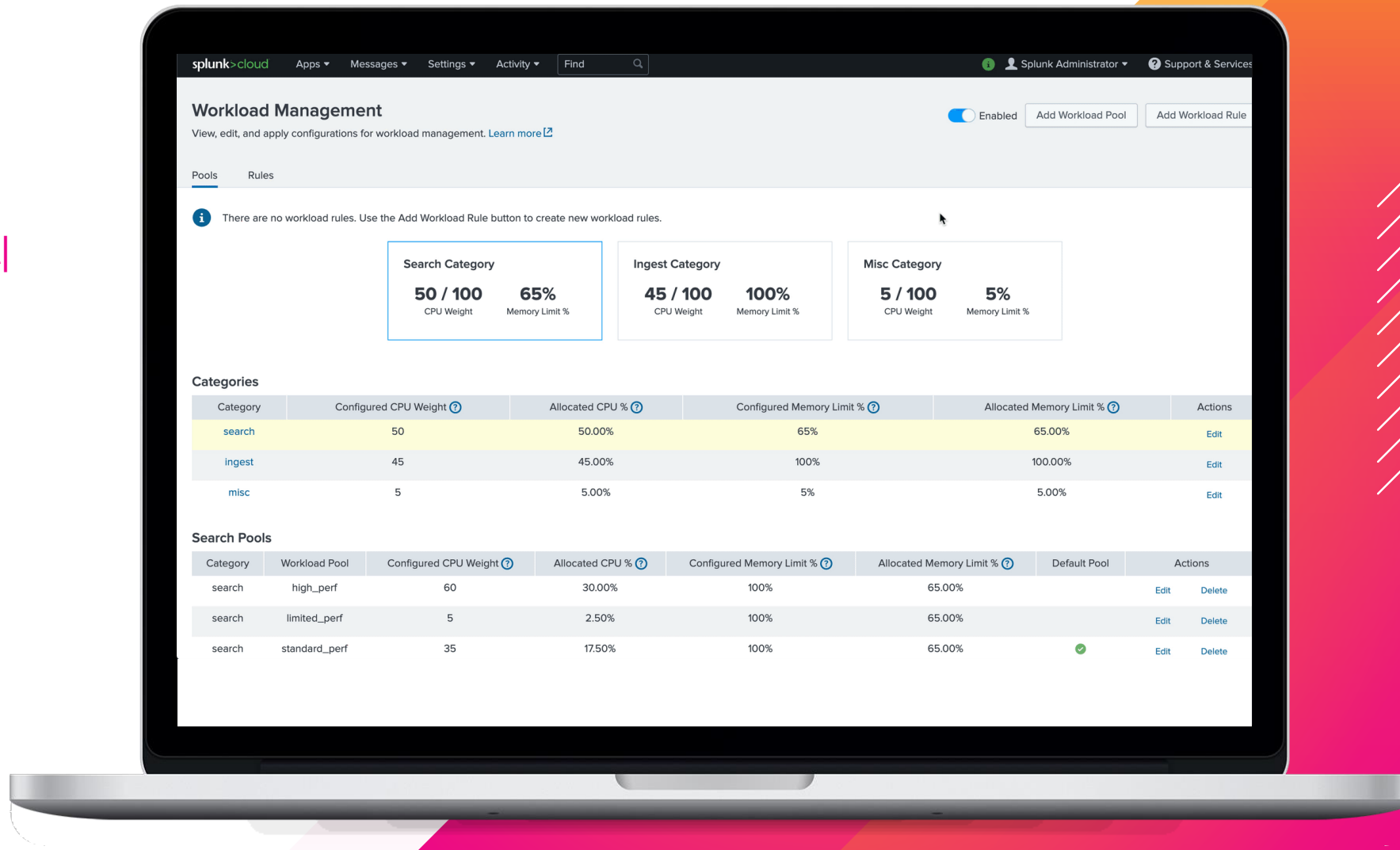
splunk> turn data into doing

© 2019 SPLUNK INC.

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 스케쥴 기반 룰 관리 가능



splunk> turn data into doing

© 2019 SPLUNK INC.

Splunk Operator for Kubernetes beta

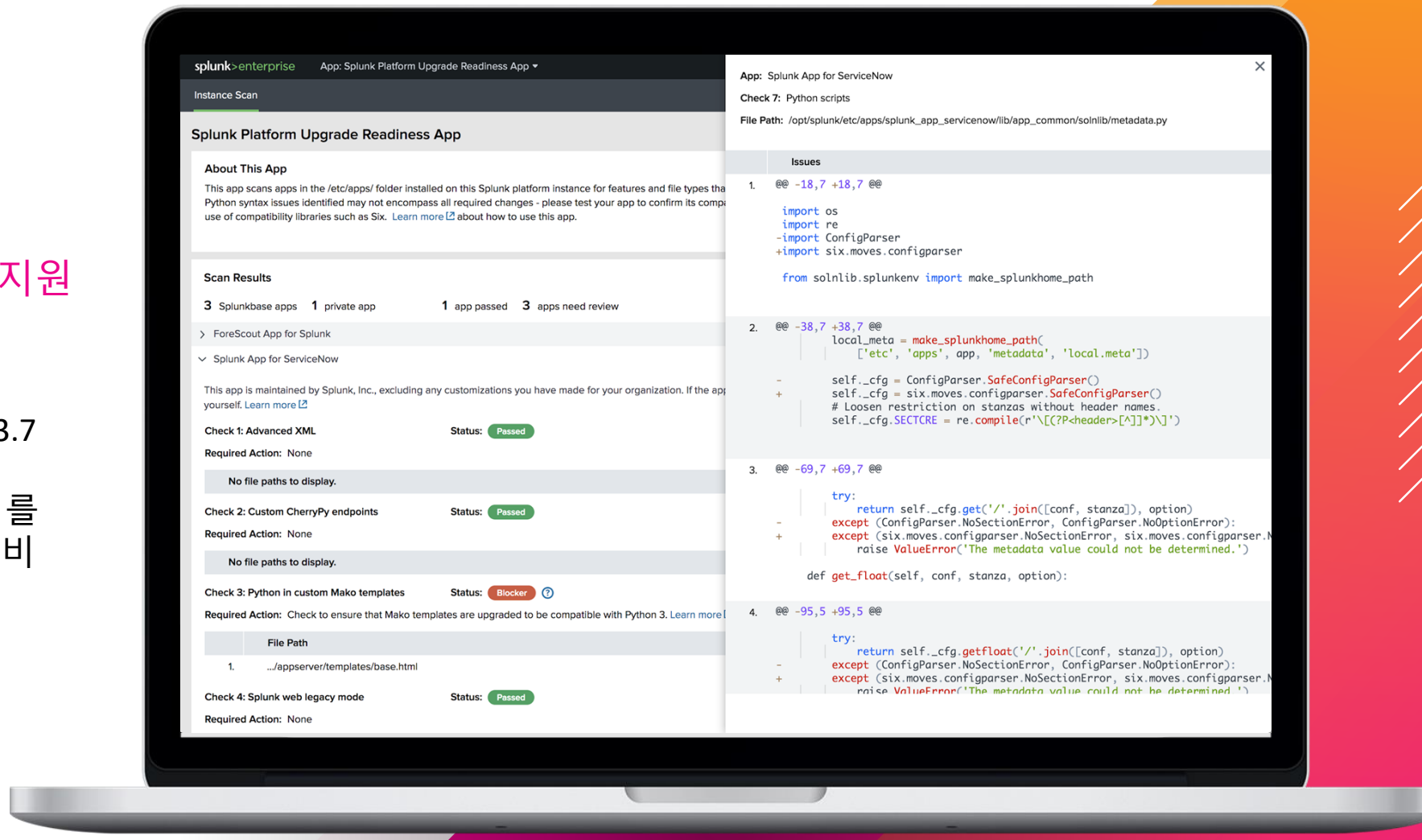
스플렁크의 쿠버네티스 환경 설치 간편화

- 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 3.7 로 업그레이드
Python 2.7 과 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



© 2019 SPLUNK INC.

2x faster stats command

Monitoring Splunk Health.
Proactive.

Sub-Index Access Controls

Splunk Enterprise 8.0

SH to Search Peer Bundle Rep
Performance Improvement

Faster Searches. Automatically.

Analytics Workspace

Splunk Dashboards App

Splunk Enterprise Kubernetes Operator

Splunk Tokens for REST API

SHC Deployer Bundle Push
Performance Enhancements

Metrics Optimizations

DMA Summary Sharing

Workload Management
Enhancements

Python 3 Support

Smart Store
Enhancements

Splunk Cloud FedRAMP

DMA Monitoring

splunk>Forum

© 2019 SPLUNK INC.

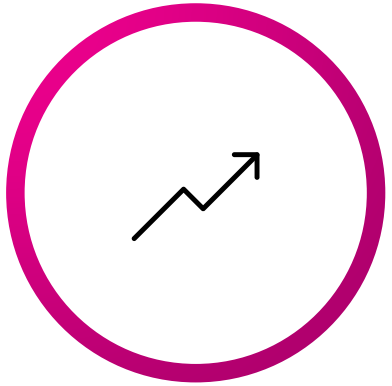
ANNOUNCING

Data Stream Processor

© 2019 SPLUNK INC.

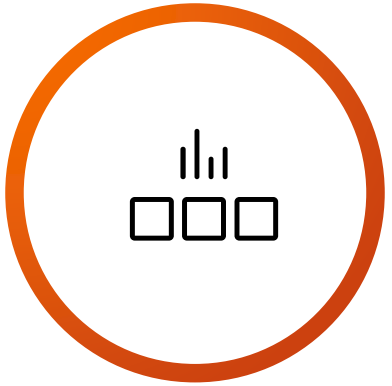
실시간 스트림 데이터의 처리

Fast



밀리세컨드단위의 실시간 전송

Proceed



전송중 실시간 데이터 처리. 특정 조건, 패턴에 따른 실시간 감지

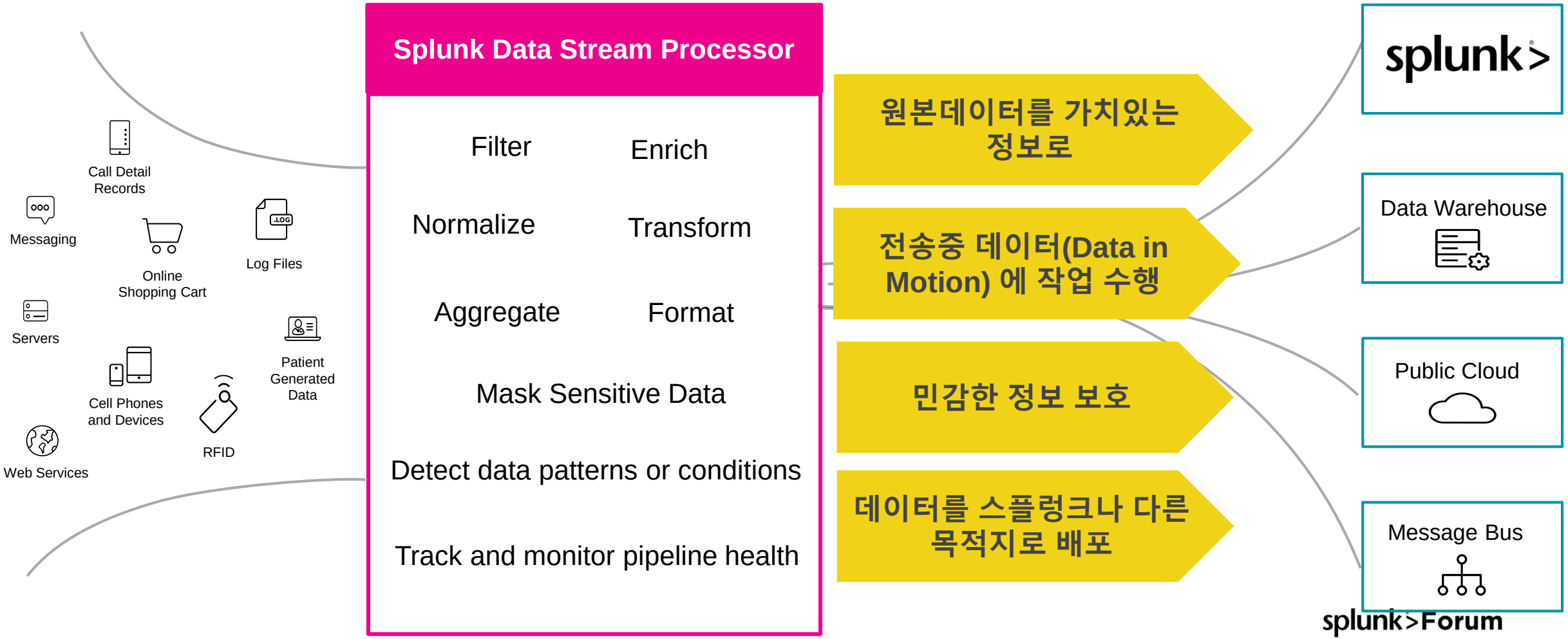
At Scale

대용량, 고속의 데이터의 여러 목적지 시스템들에 대한 전송 보장

© 2019 SPLUNK INC.

Splunk Data Stream Processor

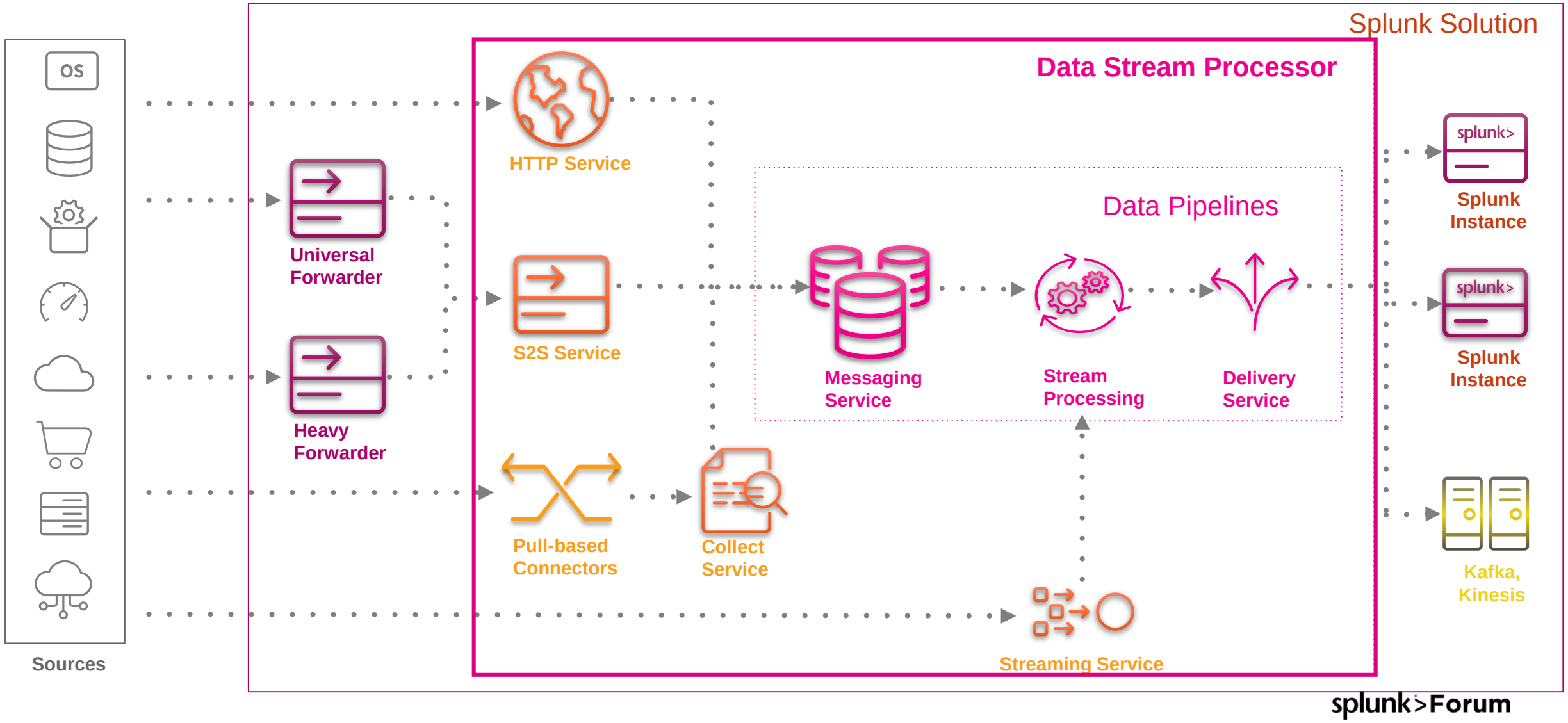
A real-time stream processing solution that collects, processes and delivers data to Splunk and other destinations **in milliseconds**



© 2019 SPLUNK INC.

DSP 아키텍처

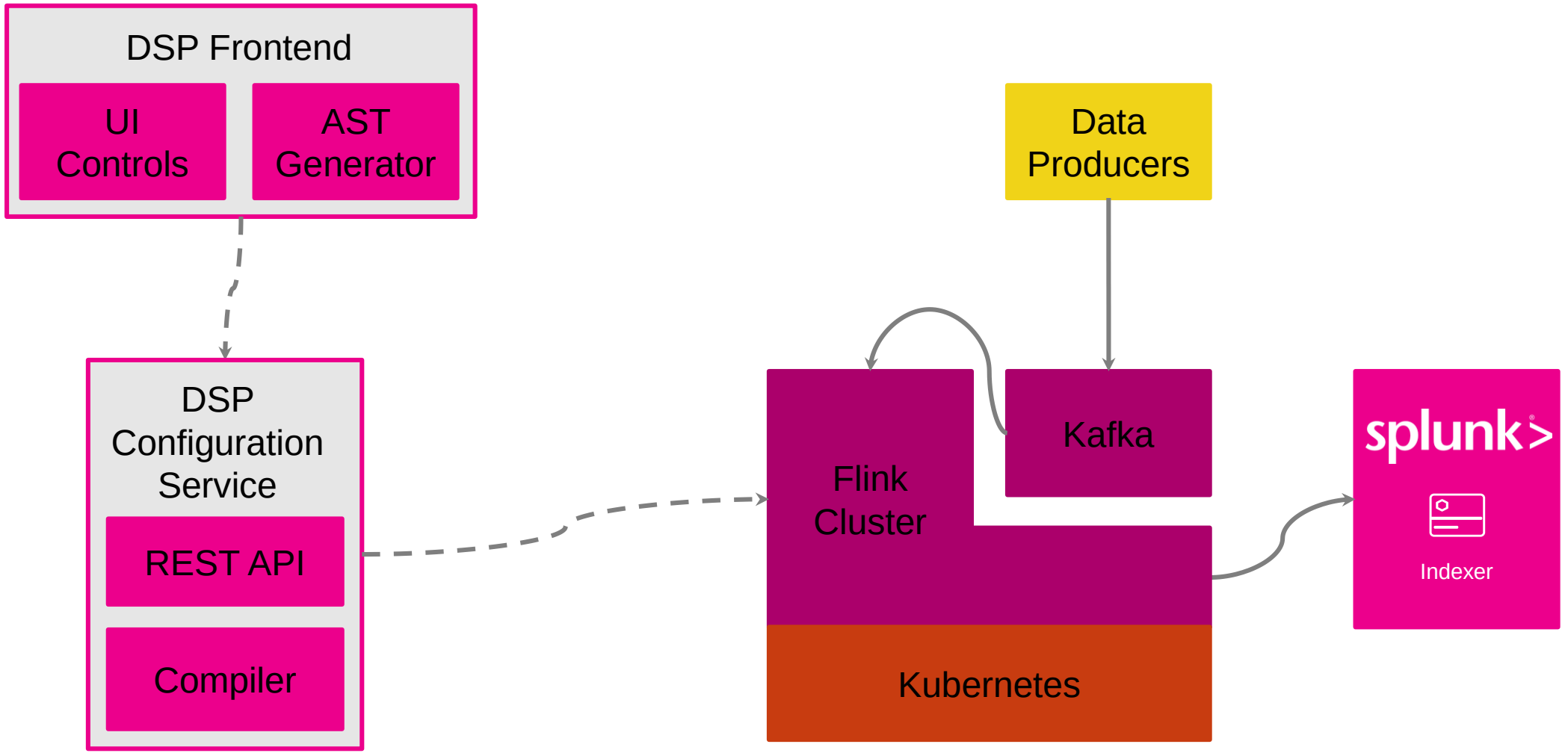
실시간 데이터 프로세싱 스플렁크 솔루션



© 2019 SPLUNK INC.

Overall system

다양한 OSS 를 활용한 Enterprise 급의 Splunk Solution



splunk>dsp

D

- Home
- Build Pipeline
- Data Management
- User Management
- Help & Feedback

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

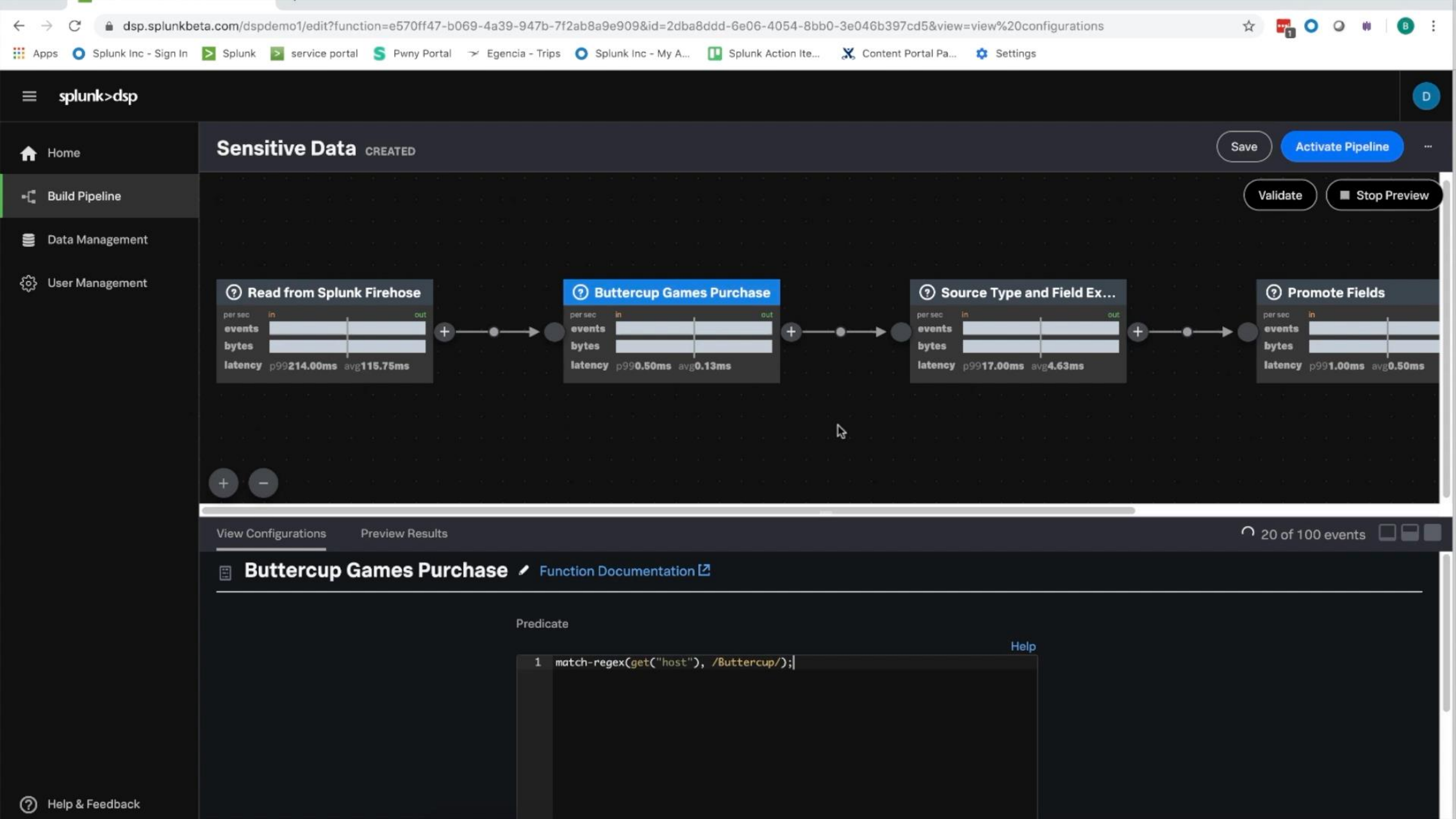
Learn about what functions are and what you can do with them

Functions

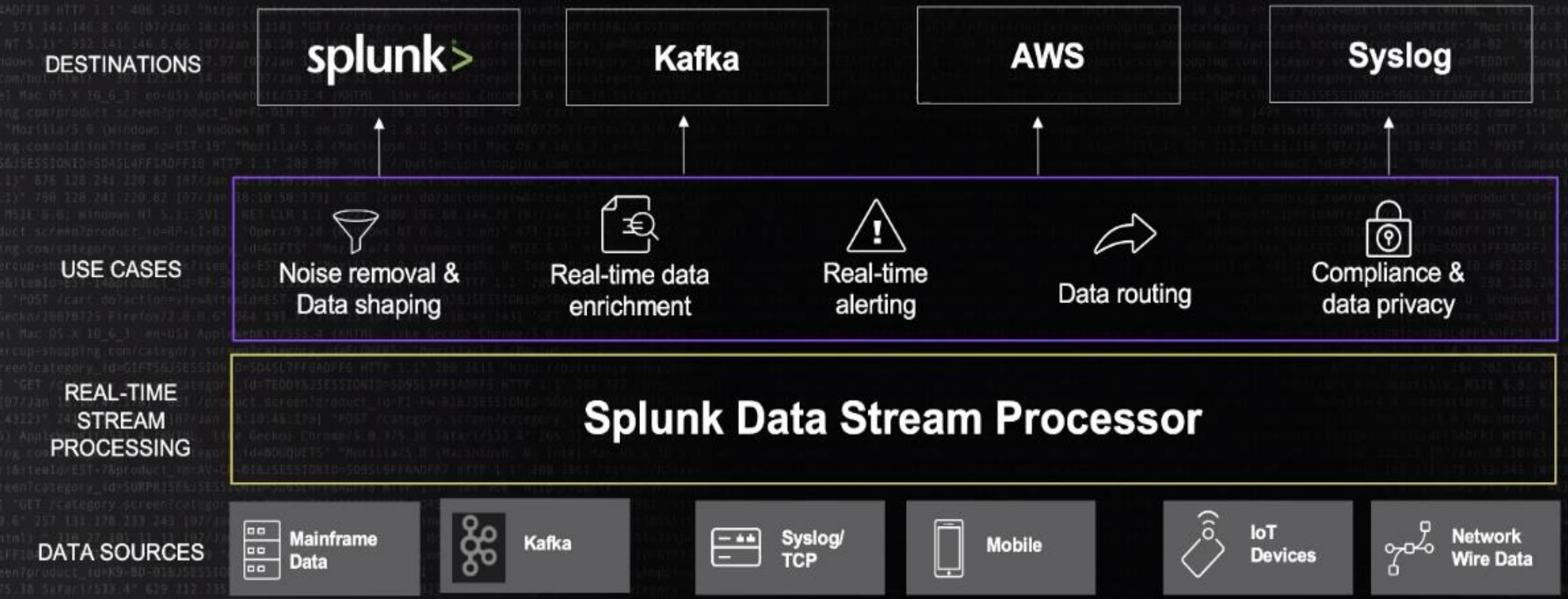
Recently Created

Pipelines

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
Apps
Splunk Inc - Sign In
Splunk
service portal
Pwny Portal
Egencia - Trips
Splunk Inc - My A...
Splunk Action Ite...
Content Portal Pa...
Settings
splunk>dsp
Home
Build Pipeline
Data Management
User Management
Help & Feedback
Sensitive Data CREATED
Save
Activate Pipeline
Validate
Stop Preview
Read from Splunk Firehose
per sec in out
events
bytes
latency p99214.00ms avg115.75ms
Buttercup Games Purchase
per sec in out
events
bytes
latency p990.50ms avg0.13ms
Source Type and Field Ex...
per sec in out
events
bytes
latency p9917.00ms avg4.63ms
Promote Fields
per sec in
events
bytes
latency p991.00ms avg0.50ms
View Configurations
Preview Results
20 of 100 events
Buttercup Games Purchase
Function Documentation
Predicate
Help
1 match-regex(get("host"), /Buttercup/);

Use Data Stream Processor to help make data driven decisions



© 2019 SPLUNK INC.

ANNOUNCING

Data Fabric Search

© 2019 SPLUNK INC.

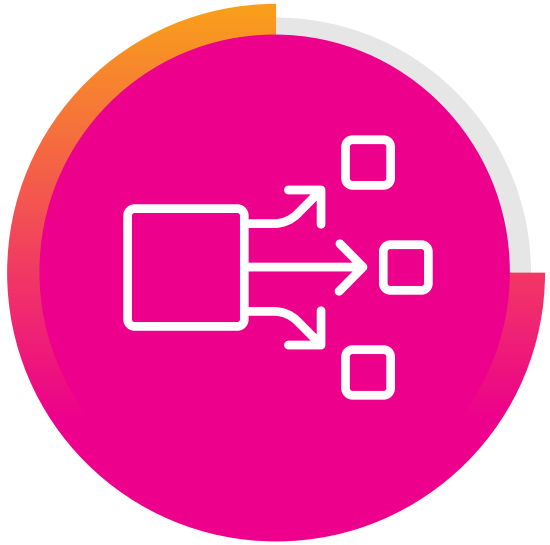
Big Data Problem

Volume

엄청난 크기의 데이터셋

Variability

다양한 종류



Variety

상이한 위치, 사용법

© 2019 SPLUNK INC.

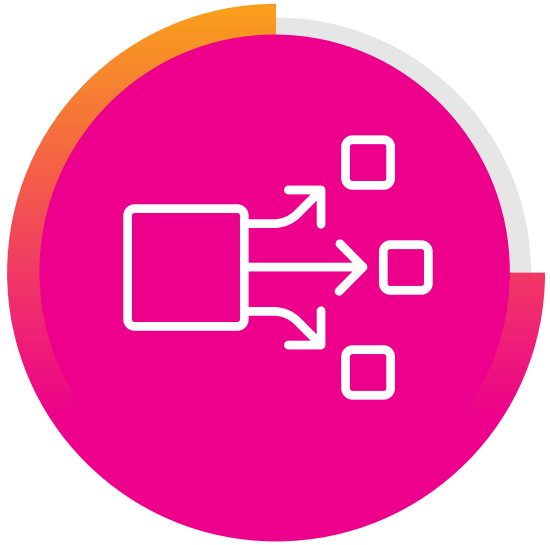
How to Solve Big Data Problem with DFS

Big Data Analysis

High Cardinality 대량의 데이터 셋에 대한 빠른 장기 배치 분석

Limitless Join

메모리 증가 없이도 대량의 데이터셋에 대한 제한없는 조인

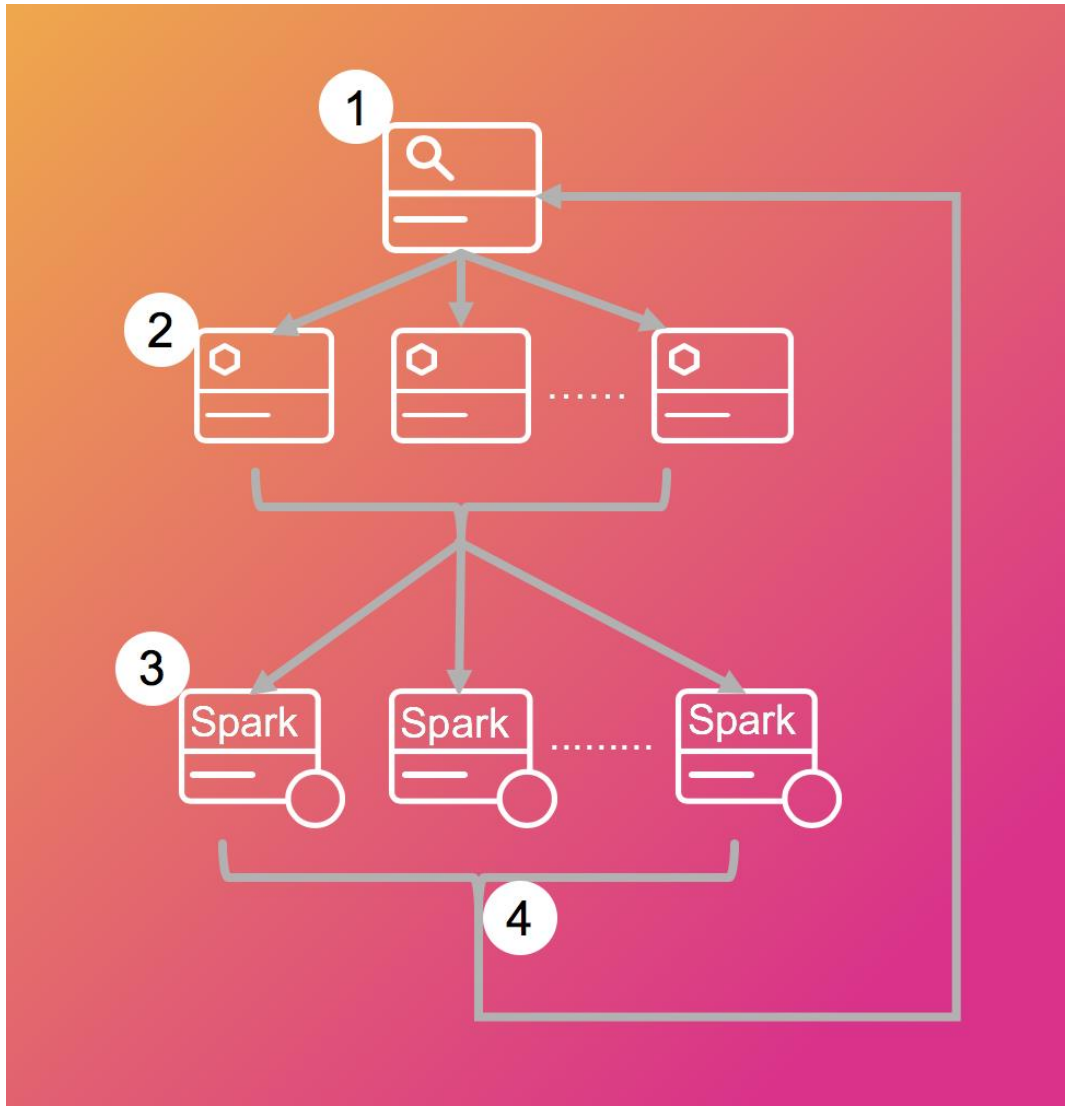


Federated Search

다양한 데이터스토어에 대한 통합 분석 엔진

© 2019 SPLUNK INC.

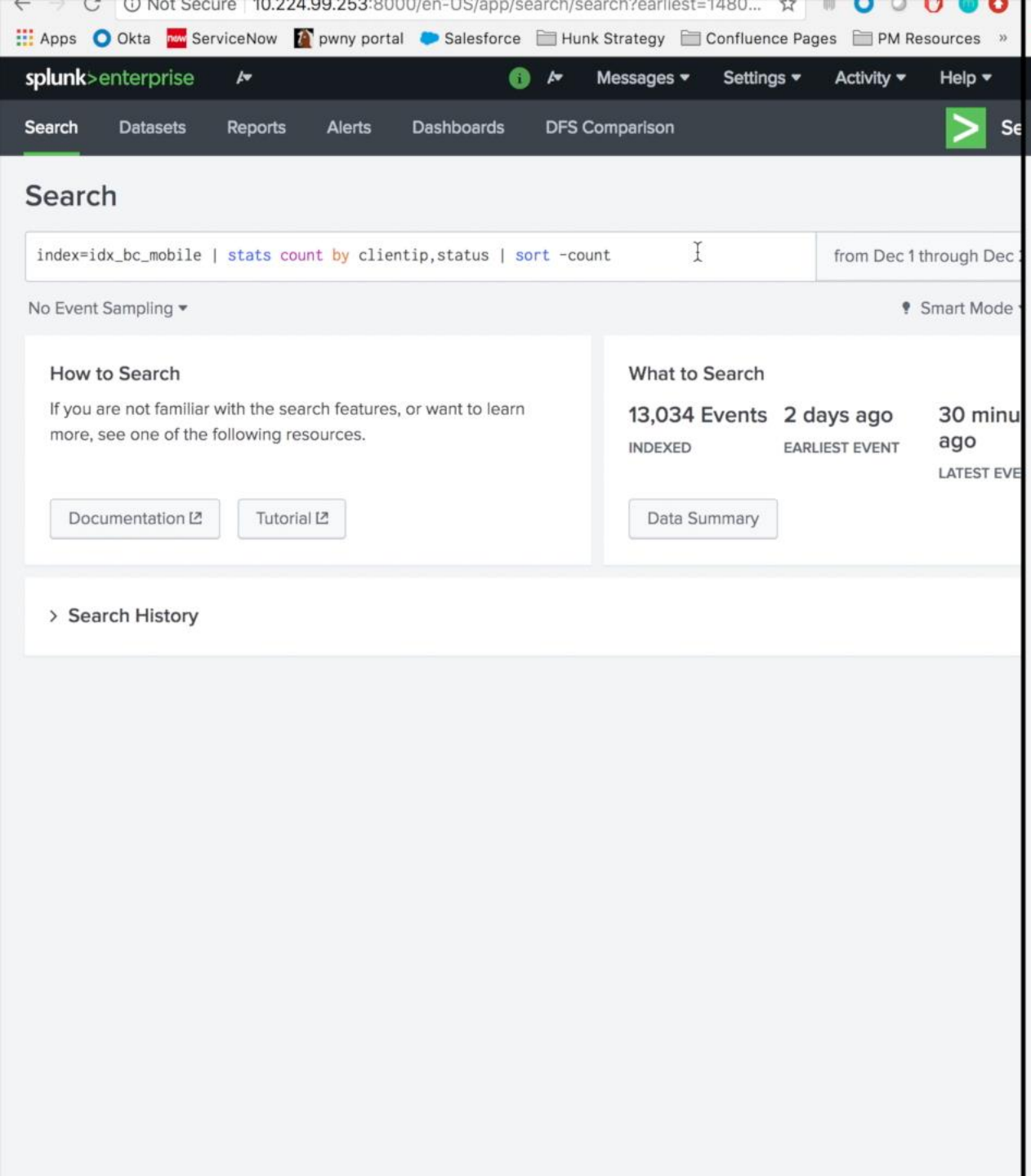
Data Fabric Search 의 동작 방식

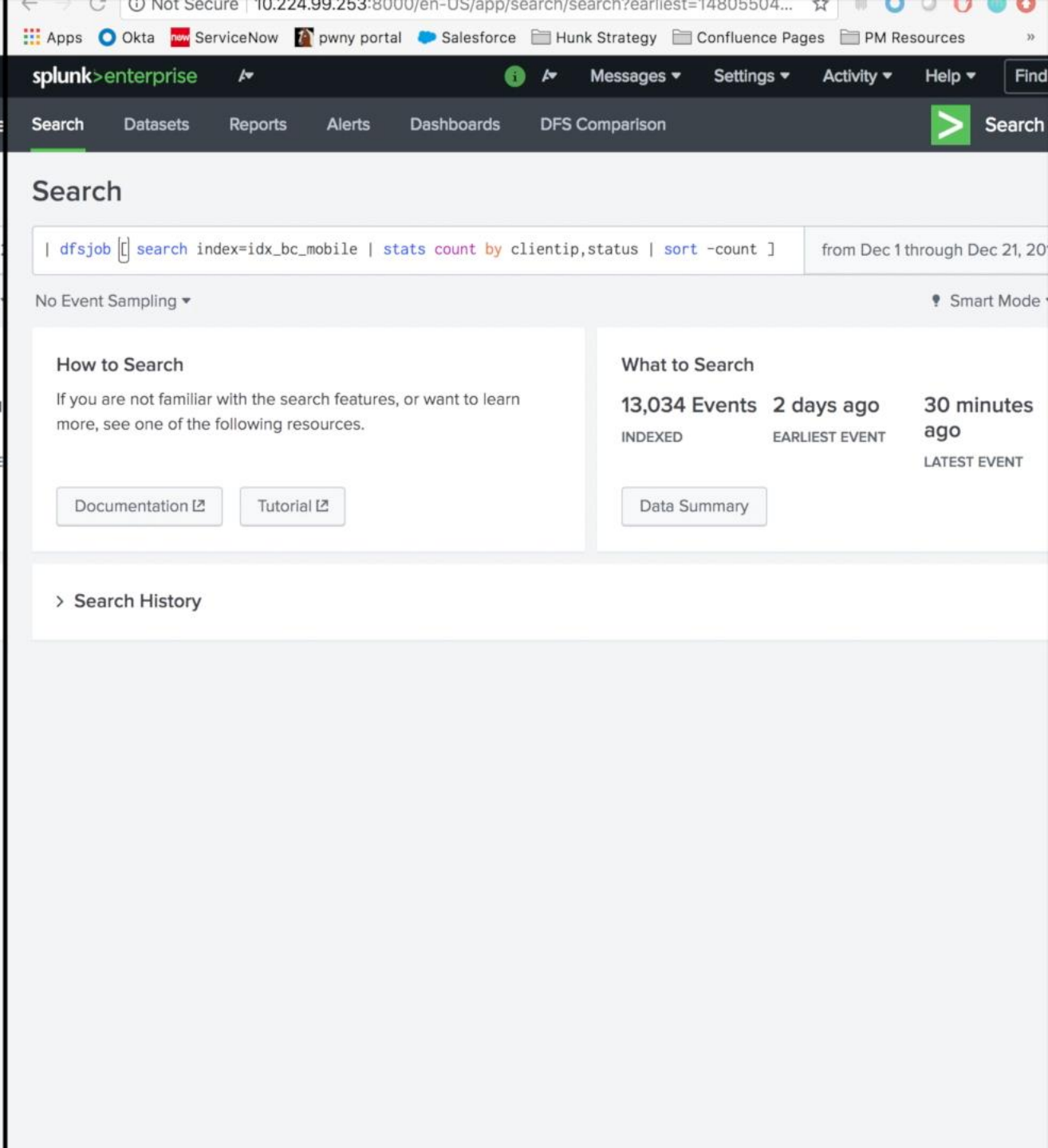


1. 서치헤드에서 쿼리 수행
2. 인덱서에서 preprocess된 데이터를 DFS 워커노드에 전송
3. DFS워커노드에서 분산 프로세싱 수행
4. 최종 결과를 서치헤드에 전달

- 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

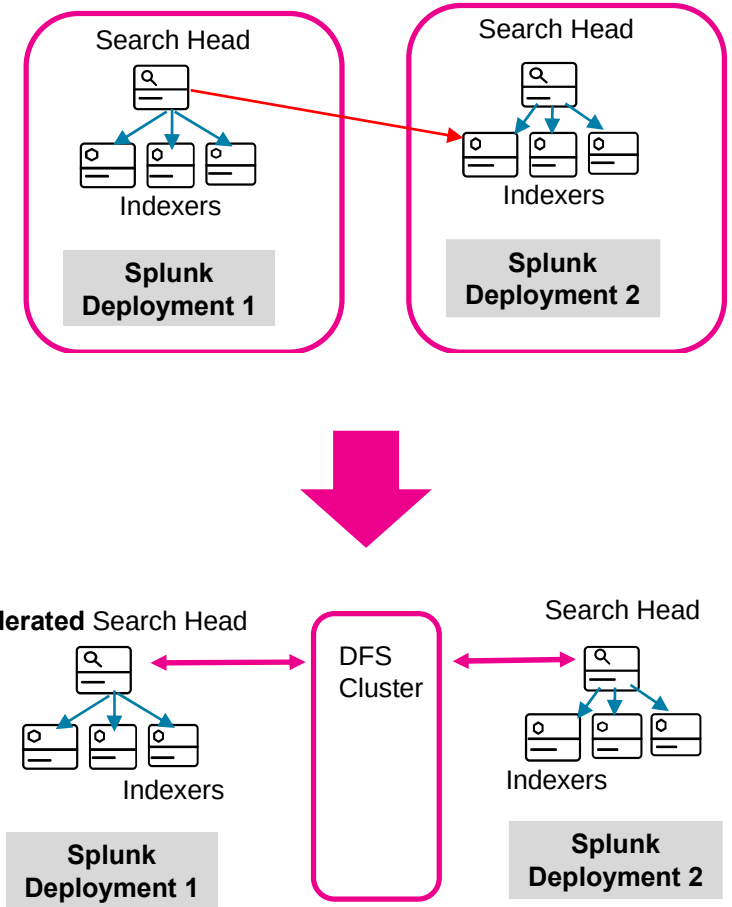

Not Secure 10.224.99.253:8000/en-US/app/search/search?earliest=1480...
Apps Okta ServiceNow pwny portal Salesforce Hunk Strategy Confluence Pages PM Resources
splunk>enterprise
Messages Settings Activity Help
Search Datasets Reports Alerts Dashboards DFS Comparison
Search
index=idx_bc_mobile | stats count by clientip,status | sort -count
from Dec 1 through Dec
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
INDEXED
2 days ago
EARLIEST EVENT
30 minu ago
LATEST EVE
Data Summary
Search History


Not Secure 10.224.99.253:8000/en-US/app/search/search?earliest=14805504...
Apps Okta ServiceNow pwny portal Salesforce Hunk Strategy Confluence Pages PM Resources
splunk>enterprise
Messages Settings Activity Help
Search Datasets Reports Alerts Dashboards DFS Comparison
Search
| dfsjob [search index=idx_bc_mobile | stats count by clientip,status | sort -count]
from Dec 1 through Dec 21, 20
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
INDEXED
2 days ago
EARLIEST EVENT
30 minutes ago
LATEST EVENT
Data Summary
Search History

© 2019 SPLUNK INC.

Federated Search

여러 스플렁크 deployment 에 대한 통합 검색



Search | Datasets | Reports | Alerts | Dashboards | DFS Comparison | Search & R

New Search

Save As

```
| 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
```

Last 15 minutes

✓ 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 | Smart M

Events | Patterns | Statistics (2,000) | Visualization

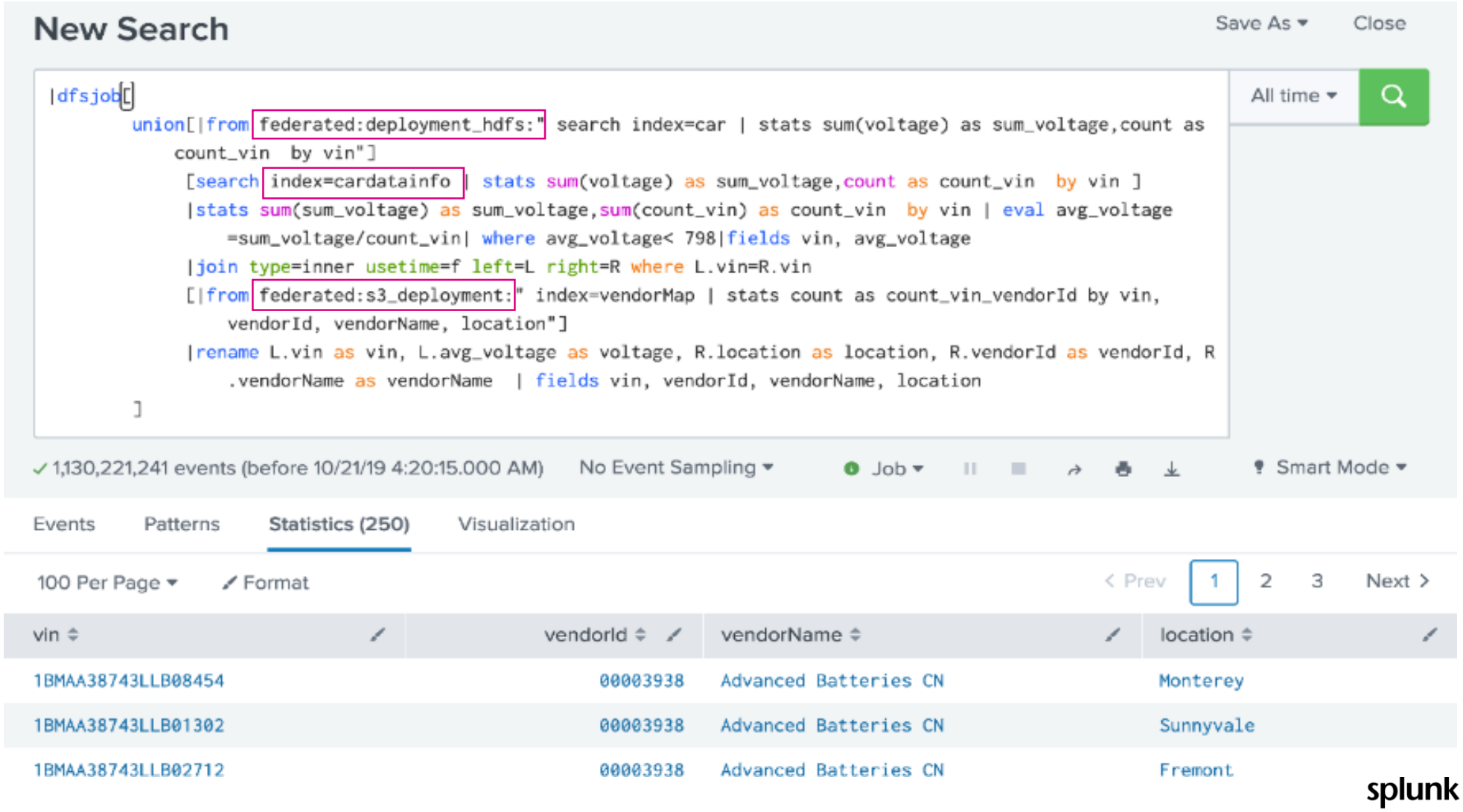
20 Per Page | Format | Prev 1 2 3 4 5 6 7 8 ...

status	clientip	sum(totalCo
200	10.2.1.101	
200	10.2.1.2	

© 2019 SPLUNK INC.

Federated Search 3rd party datastore(pre-release)

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



© 2019 SPLUNK INC.

verizon media

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

© 2019 SPLUNK INC.

verizon media

Classic VS DFS 성능 비교

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

© 2019 SPLUNK INC.

Verizon Media

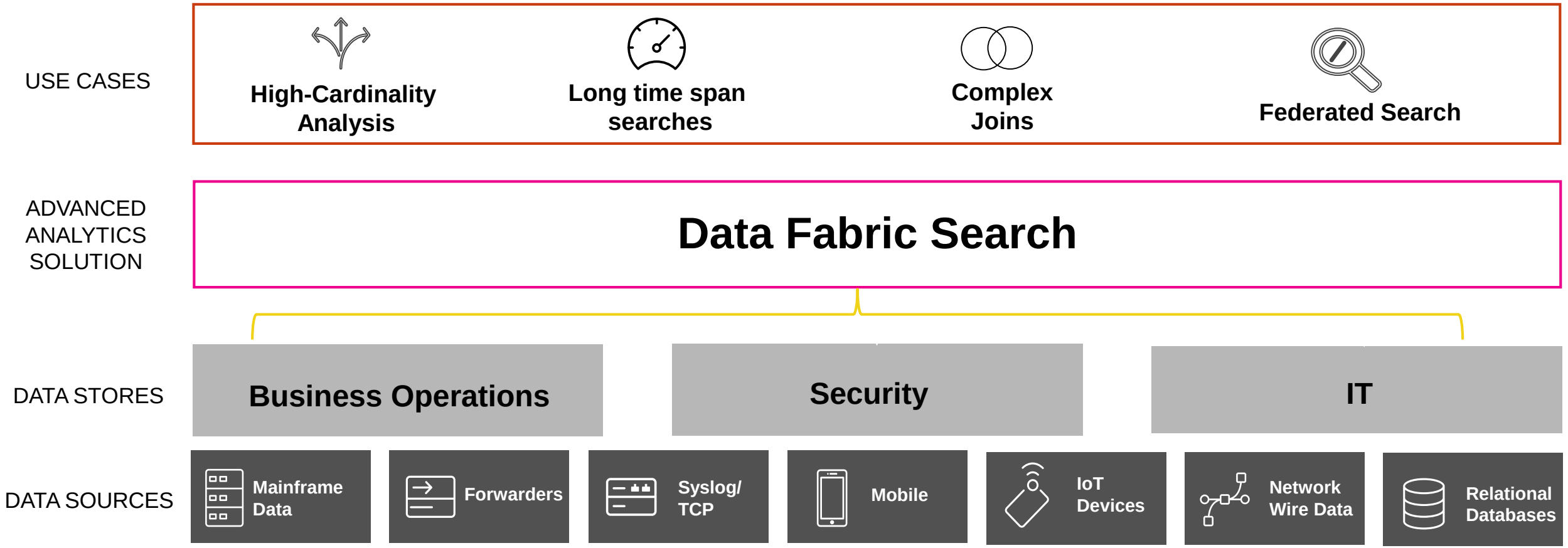
잠재적 고객 이슈에 대한 감지 및 응답 시간 감소

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

© 2019 SPLUNK INC.

하나의 플랫폼 - Data Fabric Search



© 2019 SPLUNK INC.

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™

Source: Forbes

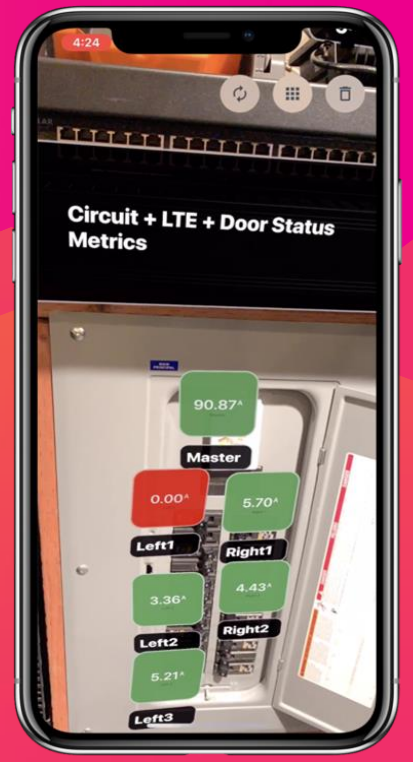
© 2019 SPLUNK INC.

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

© 2019 SPLUNK INC.

Connected Experiences Apps

언제 어디서든 가능합니다.

Splunk® Mobile

Splunk® TV

Splunk® AR

Splunk® VR

Splunk® NLP

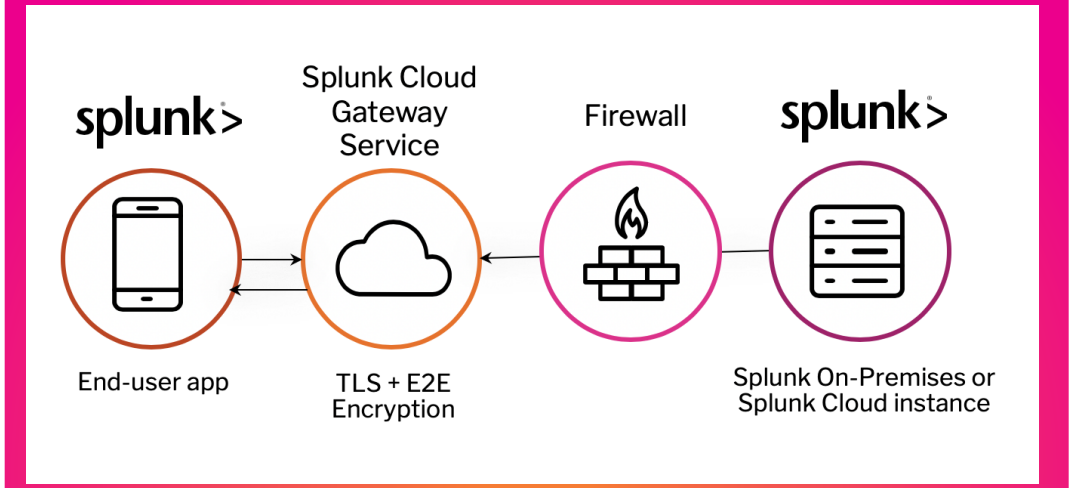
Splunk® Cloud Gateway

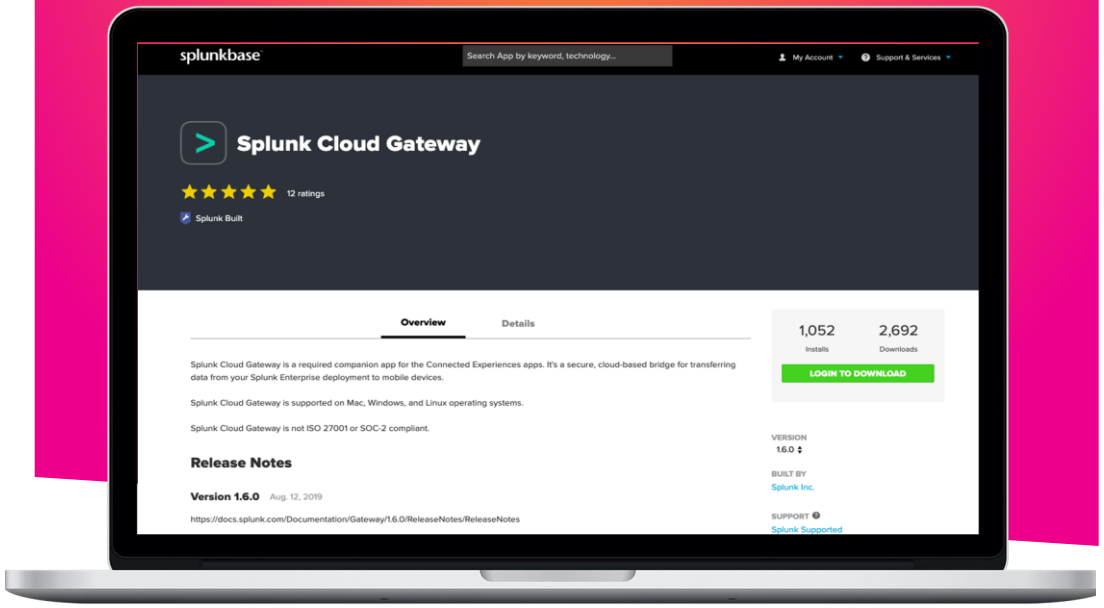
splunk>enterprise

© 2019 SPLUNK INC.

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

© 2019 SPLUNK INC.

Splunk® Mobile

모바일 기기를 위한 최적의 대시보드

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

© 2019 SPLUNK INC.

Splunk® TV

고급스런 고해상도 대시보드 화면

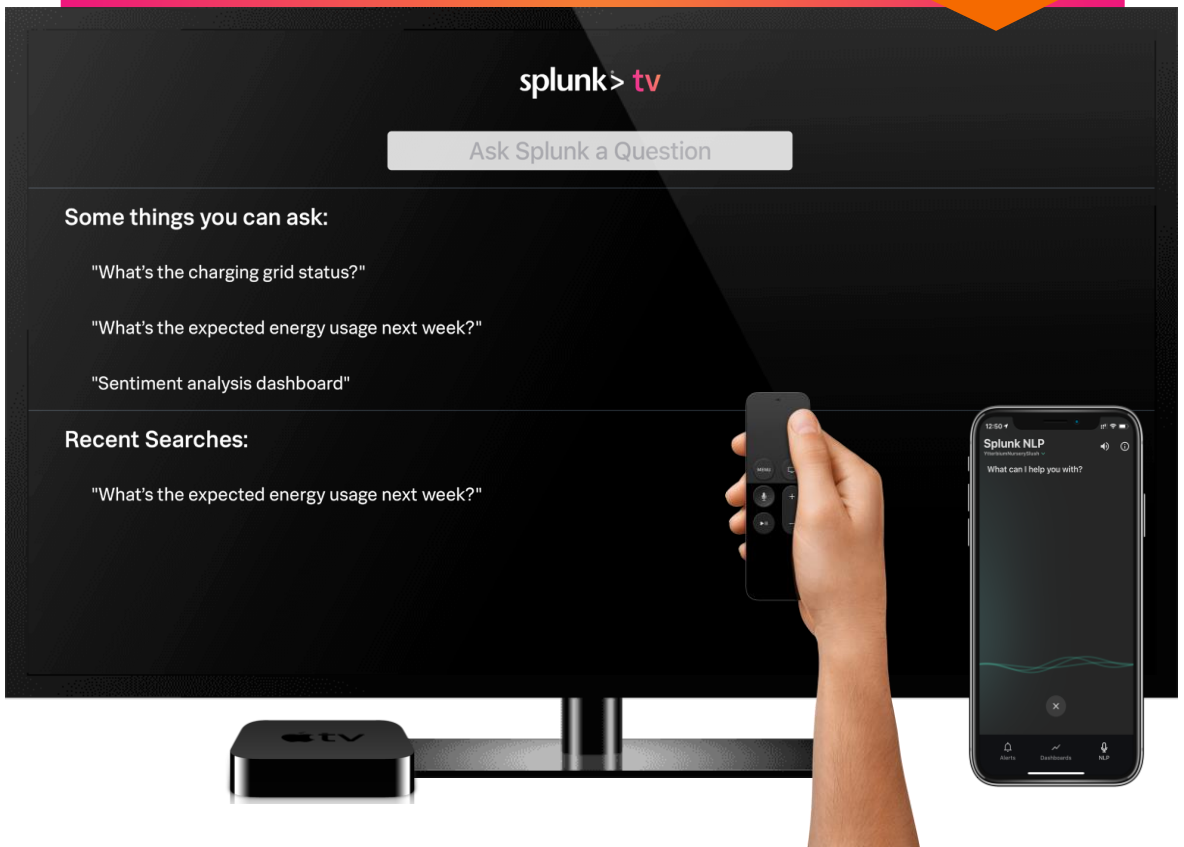
- NOC 과 SOC, 시니어 리더쉽을 위한 최상의 디스플레이 환경
- Apple TVs 에서 높은 해상도로 Splunk® Enterprise 와 Splunk® Cloud 대시보드 디스플레이

© 2019 SPLUNK INC.

Splunk® NLP

말로 하는 검색

- 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

© 2019 SPLUNK INC.

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

© 2019 SPLUNK INC.

© 2019 SPLUNK INC.

Splunk® VR

가상 현실을 통한 데이터 경험

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

© 2019 SPLUNK INC.

Connected Experiences 가 선사하는 Benefits

Cloud Gateway

Mobile

TV

NLP

AR

VR

oculus

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

© 2019 SPLUNK INC.

ANNOUNCING

Splunk Business Flow

splunk> turn data into doing®

© 2019 SPLUNK INC.

Splunk Business Flow 는

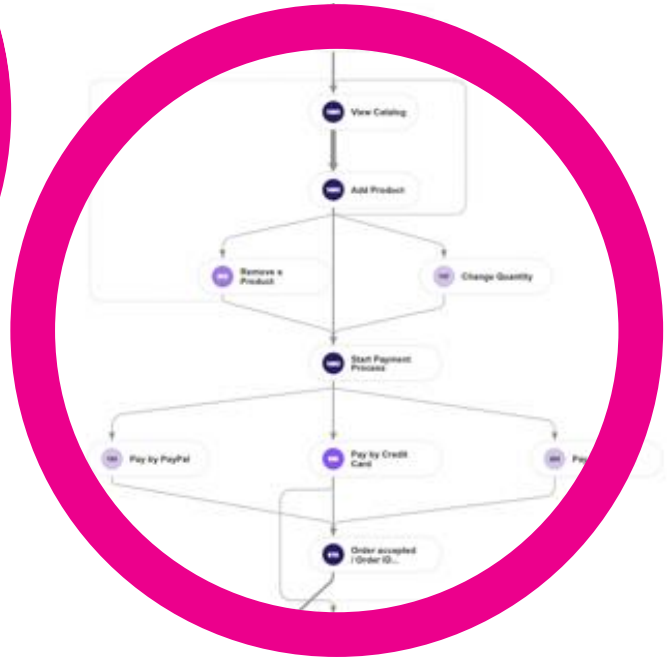
비지니스 프로세스상의 비효율 지점을

파악하기 위한 **프로세스 마이닝** 툴입니다.

© 2019 SPLUNK INC.

Process Mining

프로세스 분석 기법

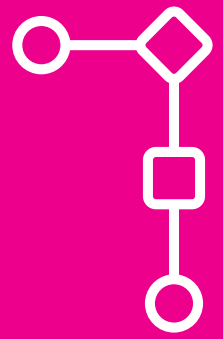


- 이벤트 로그를 기반으로 비즈니스 프로세스 분석을 지원하는 프로세스 관리 분야의 기술로, 특정 데이터 마이닝 알고리즘이 이벤트 로그에 적용되어 이벤트 로그에 포함된 트렌드, 패턴, 상세정보를 찾아내는 기법. *–Wikipedia*

- 공항 승객 입출국 프로세스, 상품 거래 프로세스 등 비지니스 프로세스 분석

© 2019 SPLUNK INC.

Splunk Business Flow 기능



End-to-end process discovery through event stitching

Investigate drill-down with exploration interface

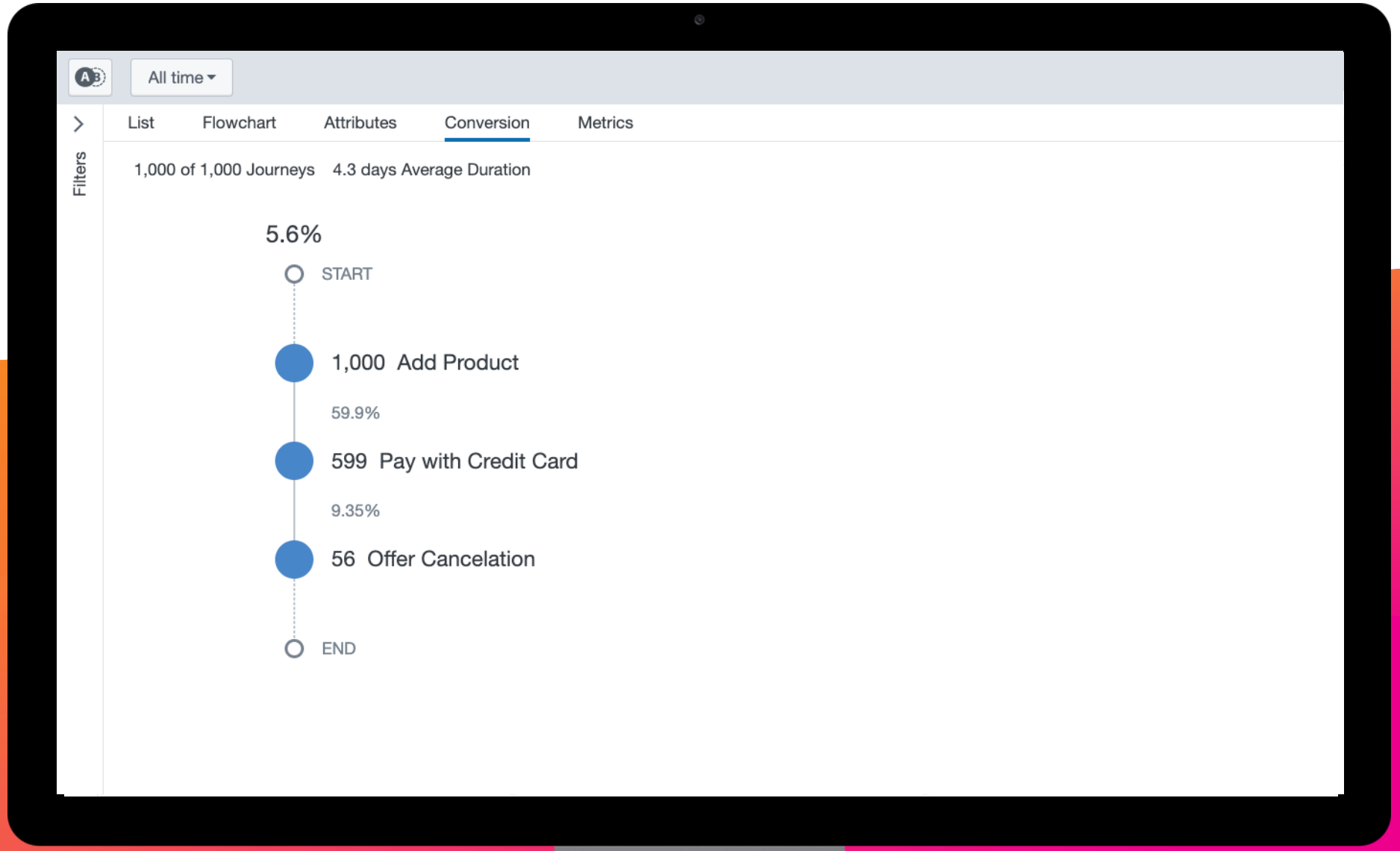
Side-by-side A/B comparison of process flows

Conformance checking and deviation notifications

SPLUNK BUSINESS FLOW

splunk>enterprise splunk>cloud

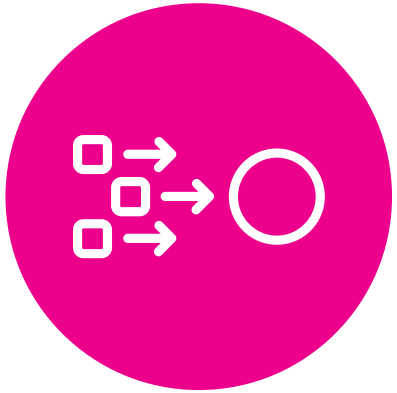
© 2019 SPLUNK INC.



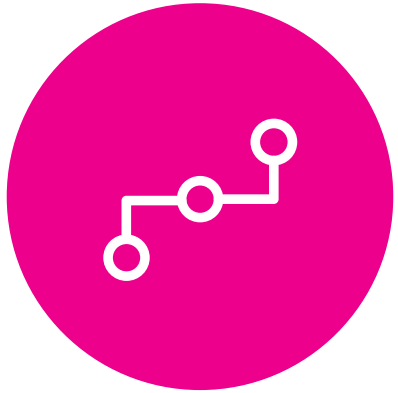
splunk> turn data into doing®

3 단계로 끝!

© 2019 SPLUNK INC.



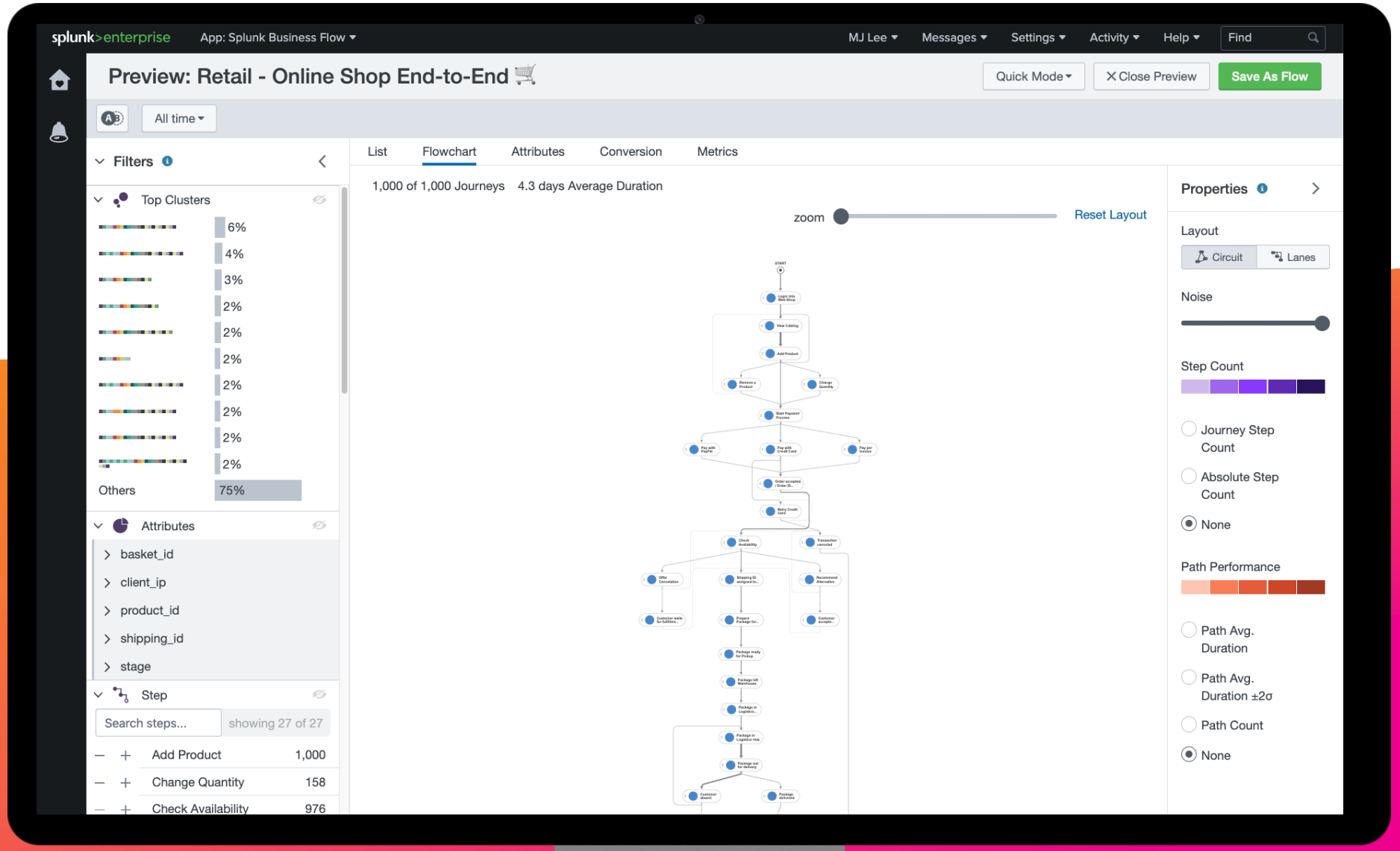
1 이벤트 데이터 소스에서 프로세스를 정의하는 공통 identifiers 확인



2 이벤트 스트림을 정의하고 identifiers 를 correlating 함으로써 플로우 모델을 디자인

3 비지니스 사용자는 스스로 프로세스를 탐색하고 시각화

© 2019 SPLUNK INC.

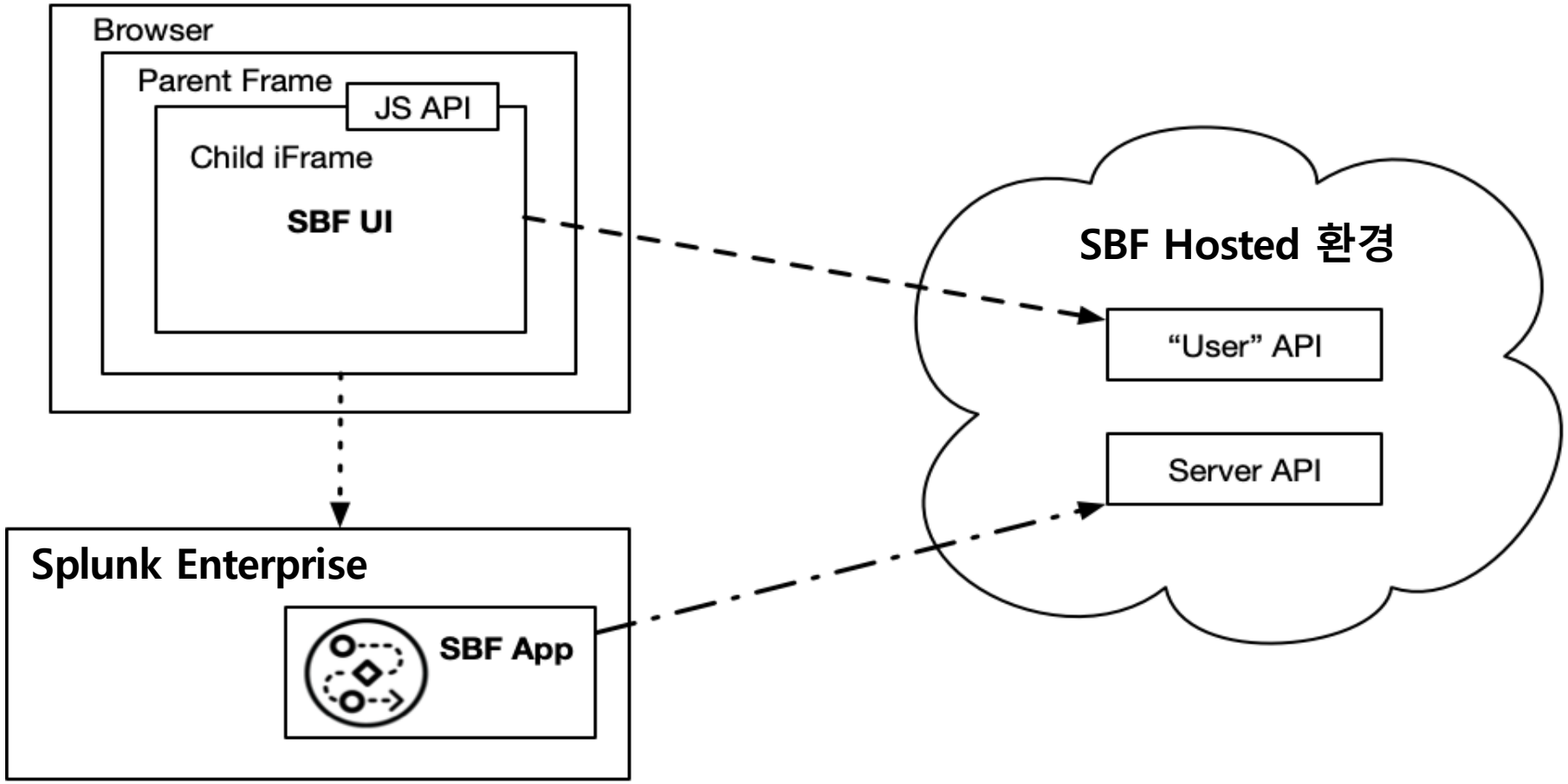


splunk> turn data into doing®

© 2019 SPLUNK INC.

SBF 하이브리드 어플리케이션 아키텍처

SBF의 개념적인 전체 아키텍처



© 2019 SPLUNK INC.

Splunk®
Business Flow

비지니스 프로세스를 시각화 하고 분석하고 개선함으로써

최적의 프로세스를 찾아보세요!

splunk>Forum

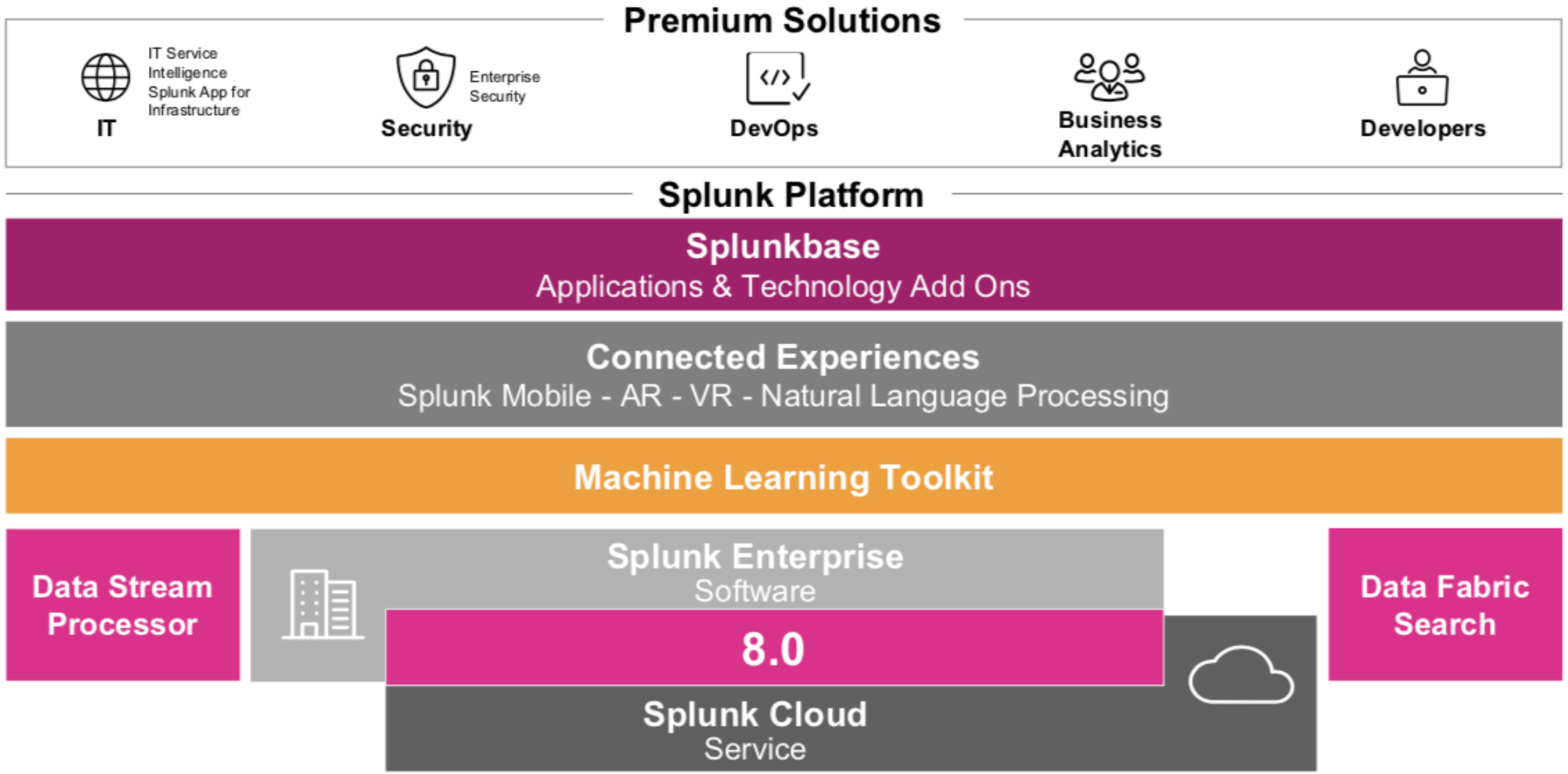
© 2019 SPLUNK INC.

Summary

splunk>Forum

© 2019 SPLUNK INC.

Splunk Delivers a complete Portfolio
for tuning Data into Business Outcomes



© 2019 SPLUNK INC.

스플렁크 코리아 카카오톡 플러스친구 OPEN EVENT!

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

splunk> turn data into doing

© 2019 SPLUNK INC.

감사합니다

splunk> turn data into doing®