Splunk Forum

Splunk Korea – December 2020

splunk> turn data into doing™

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.

2020

70%
인터넷
사용량 증가

42%
정규직
재택 비율

76%
e-커머스 성장

5x
화상회의
솔루션 구매

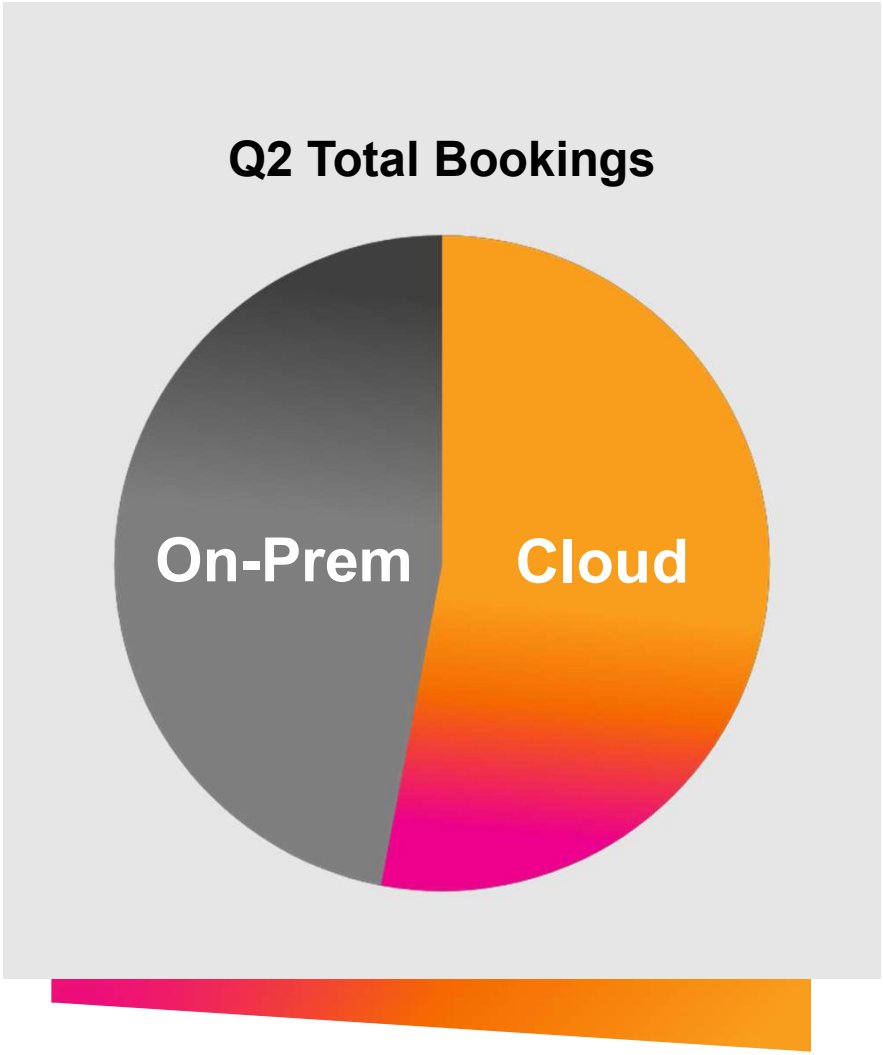
The Data Age Has Arrived

splunk> .conf20

Transformation #1

Become a World-Class Cloud Provider

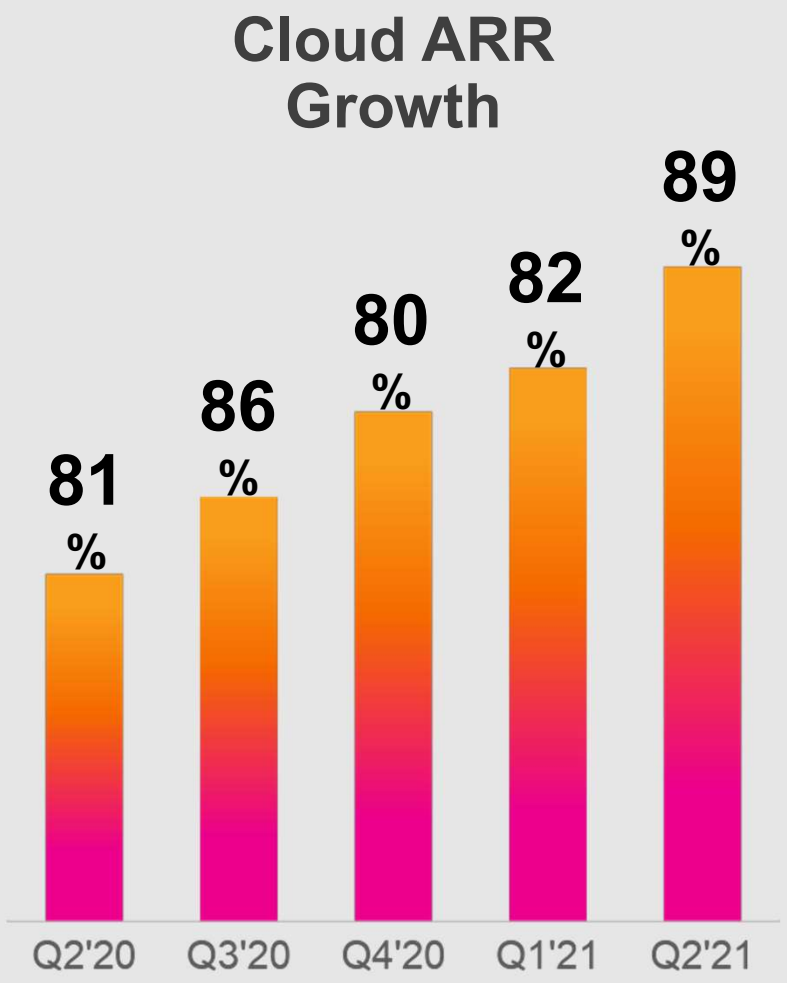
splunk> .conf20



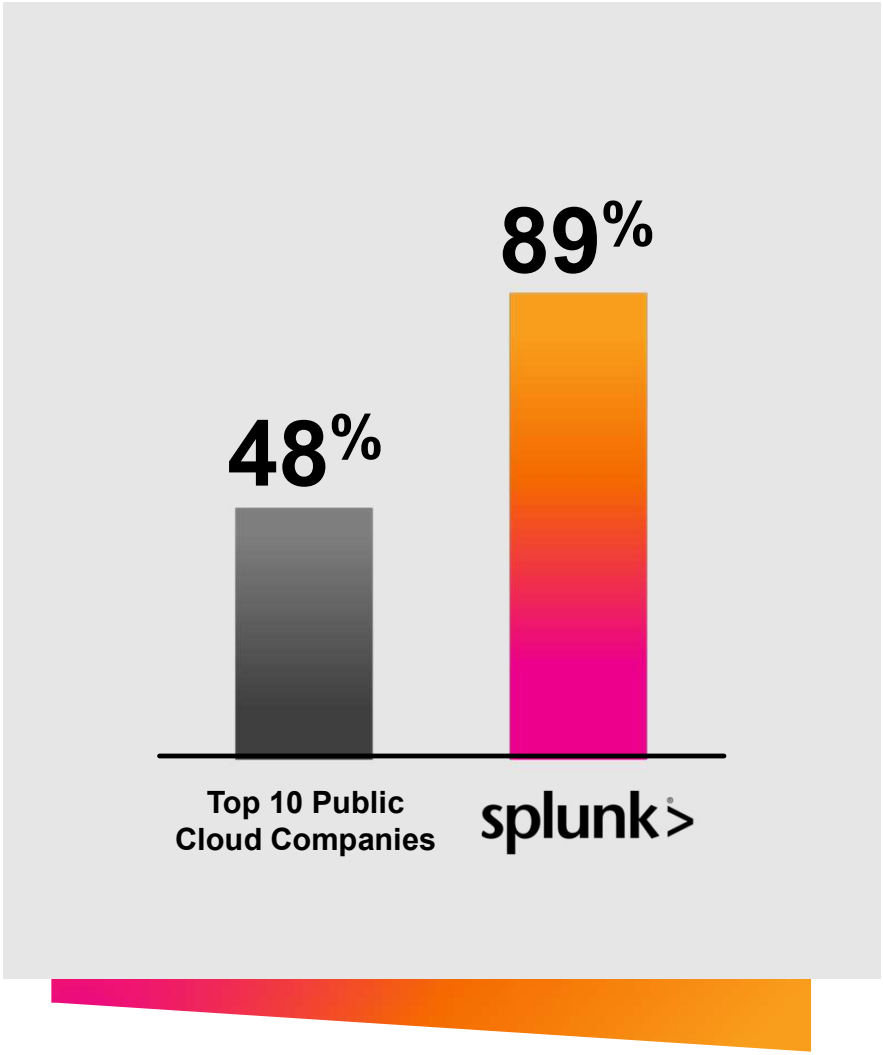
Growth in Cloud

splunk> .conf20

Growth in Cloud



Source: Splunk.com, Analyst Report. Salesforce, Workday, ServiceNow ARR based on subscription sales.



Growth in Cloud

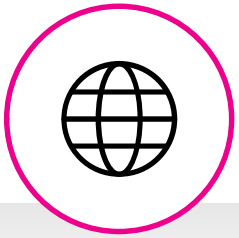
splunk> .conf20

Transformation #2

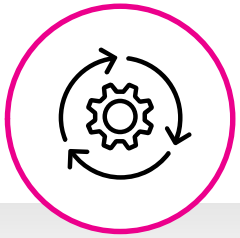
Deliver the World's First Data-to-Everything Platform

Market-Leading 포트폴리오

Security



IT



Observability

Data-to-Everything Platform

Common Work Surface, APIs, Developer Tools | Mobile and Connected Experiences

스트림 프로세싱 | 머신 러닝 | 확장 가능한 인덱스 | 페더레이트 검색 및 분석 | Collaboration & Orchestration

하이브리드와 멀티 클라우드 환경에서 수집 및 프로세싱

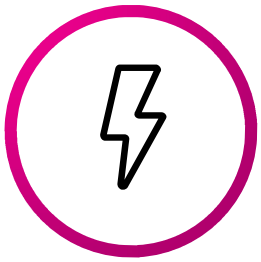
Splunk Cloud and Enterprise 8.1

splunk> turn data into doing

What's New: .conf20

Splunk Cloud and Splunk Enterprise 8.1

생산성 증대

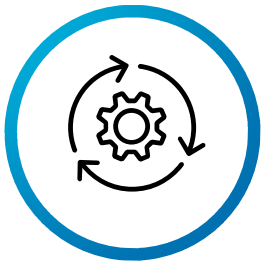


접근 & 제어

성능& 신뢰성

다양한 선택

Cloud 관리



splunk> .conf20

What's New: .conf20

Splunk Cloud and Splunk Enterprise 8.1

생산성 증대 | 접근 & 제어 | 성능& 신뢰성 | 다양한 선택 | Cloud 관리

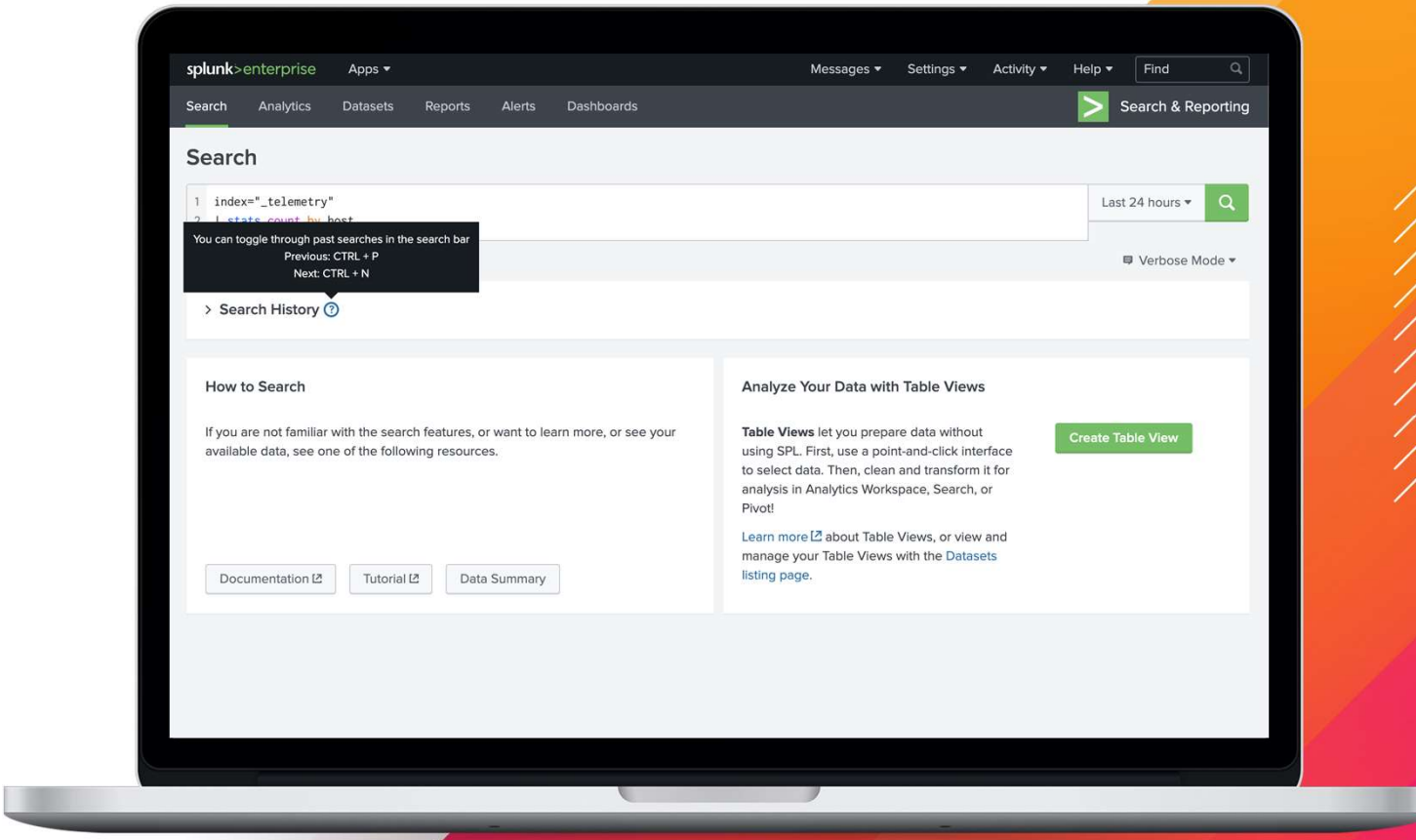
- SPL 을 검색!!
- 데이터를 바로 시각화
- Self-Service 인사이트 획득

splunk> .conf20

Search

Can you SPL?

- 검색바에서 검색 history 확인
- SPL 커멘트 지원

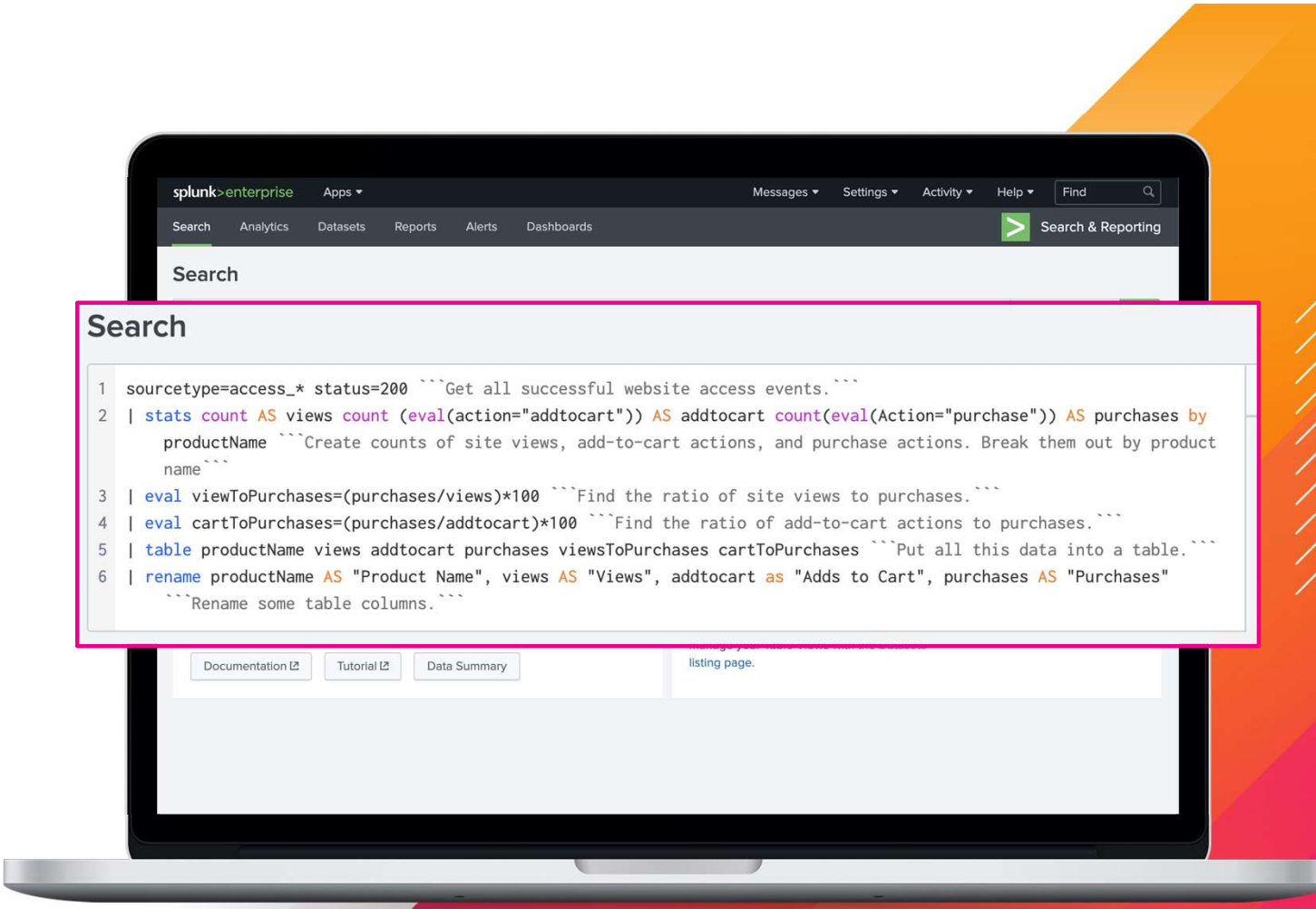


Search

Can you SPL?

- 검색바에서 검색 history 확인
- SPL 커멘트 지원

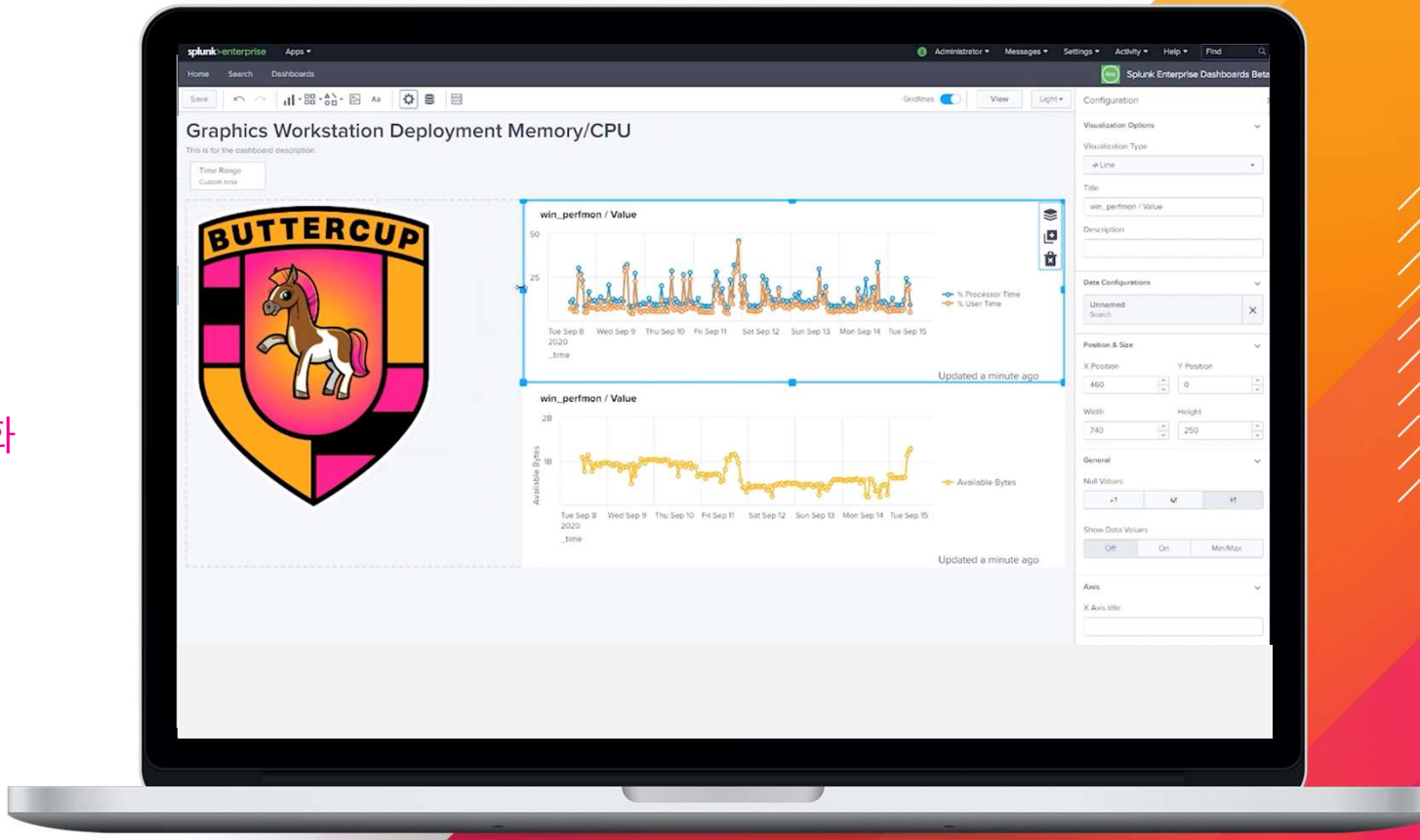
**https://ideas.splunk.com/



Self-Service 인사이트

SPL 없이 데이터를 바로 시각화

- 테이블 데이터셋과 Analytics 워크스페이스의 통합
- Analytics 워크스페이스에서 대시보드 공유: Splunk Dashboar App (beta)



What's New: .conf20

Splunk Cloud and Splunk Enterprise 8.1

생산성 증대 | **접근 & 제어** | 성능& 신뢰성 | 다양한 선택 | Cloud 관리

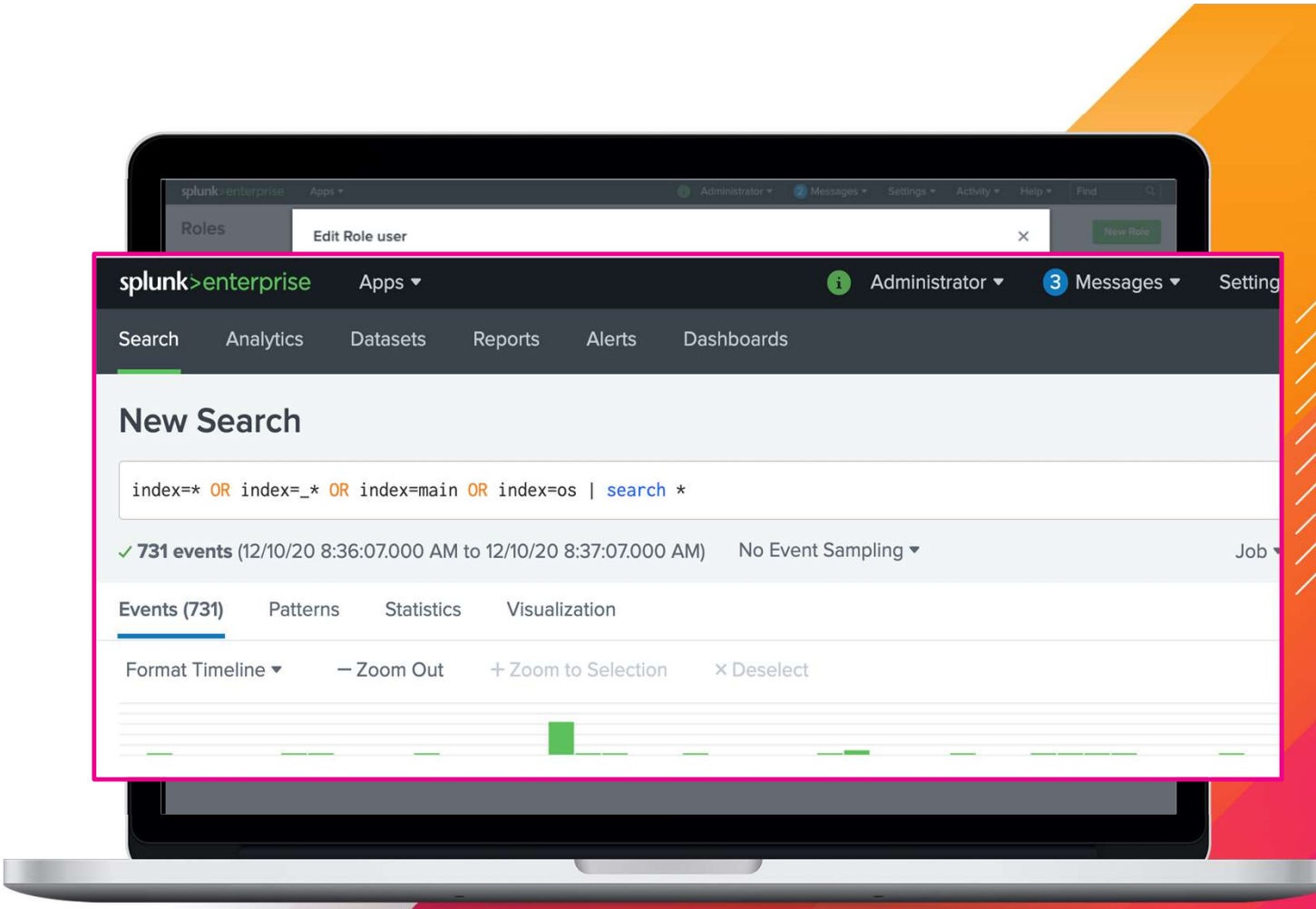
- 역할기반 접근제어
- Global Notifications
- Workload Mgmt

splunk> .conf20

역할 기반 접근 제어

잘가요 트러블슈팅

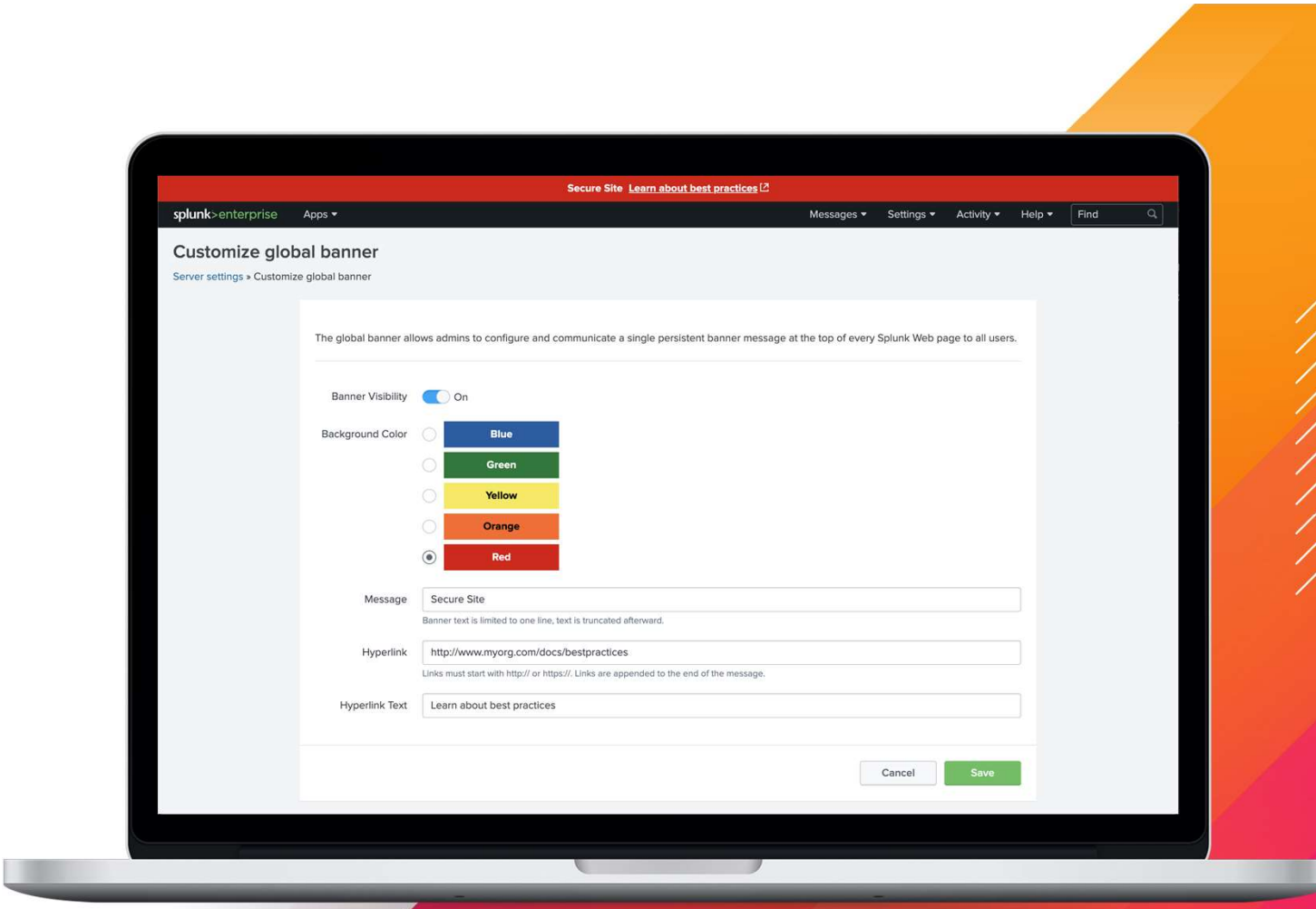
- 인덱스 상속 관계 확인
- “Search As”



커스텀 Global Notifications

Let the people know!

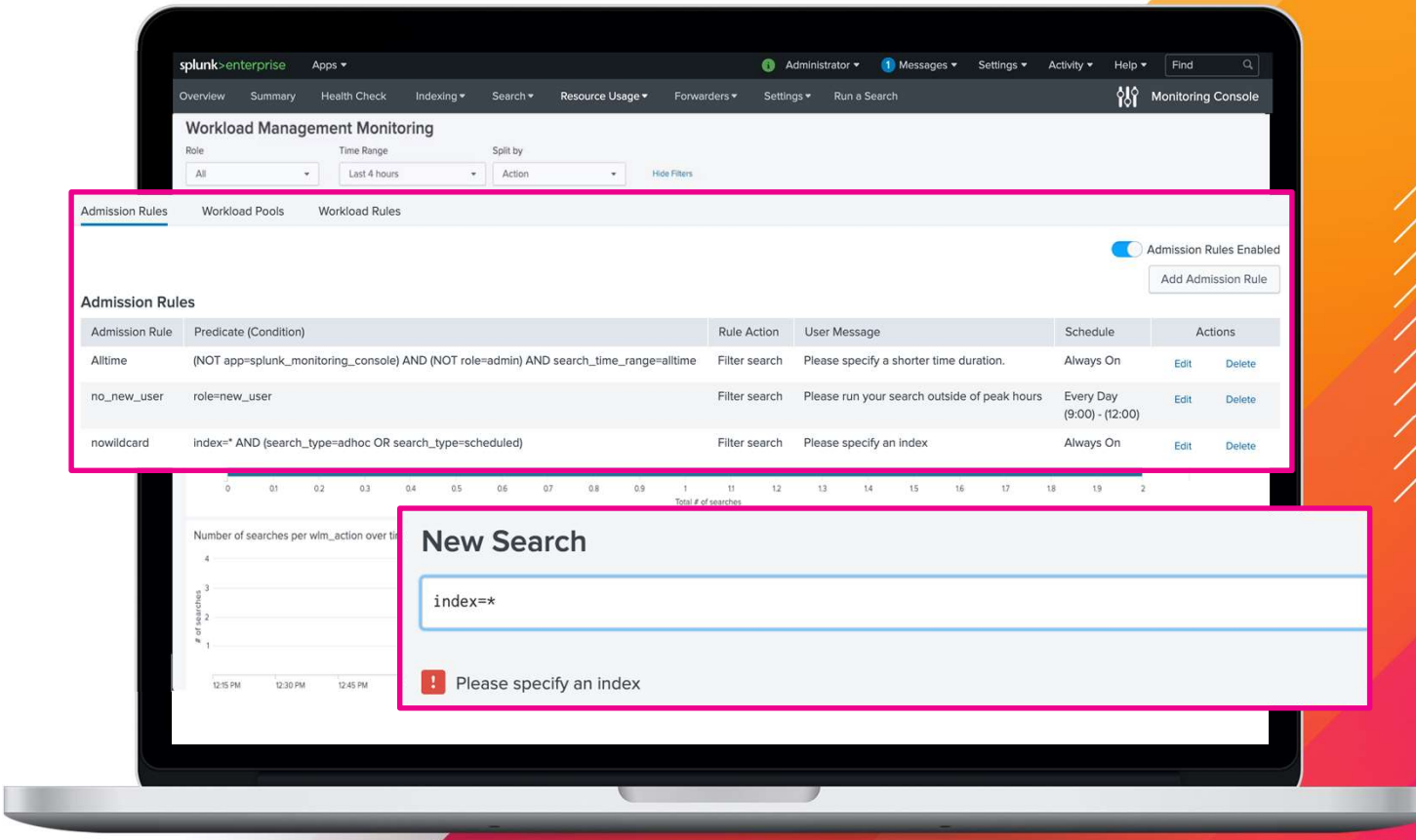
- 글로벌 배너로 공지사항 전달



Workload Management

Optimization Nation

- 검색에 대한 admission 룰 프레임워크 : 인덱스에 와일드카드를 사용 혹은 all time 을 사용한 검색 필터링
- 사용자 메시지 customization
- WL 룰 활성화/비활성화



What's New: .conf20

Splunk Cloud and Splunk Enterprise 8.1

생산성 증대

접근 & 제어

성능& 신뢰성

- 검색
- Metrics 스토어
- Rolling Restart
- Cloud 확장

다양한 선택

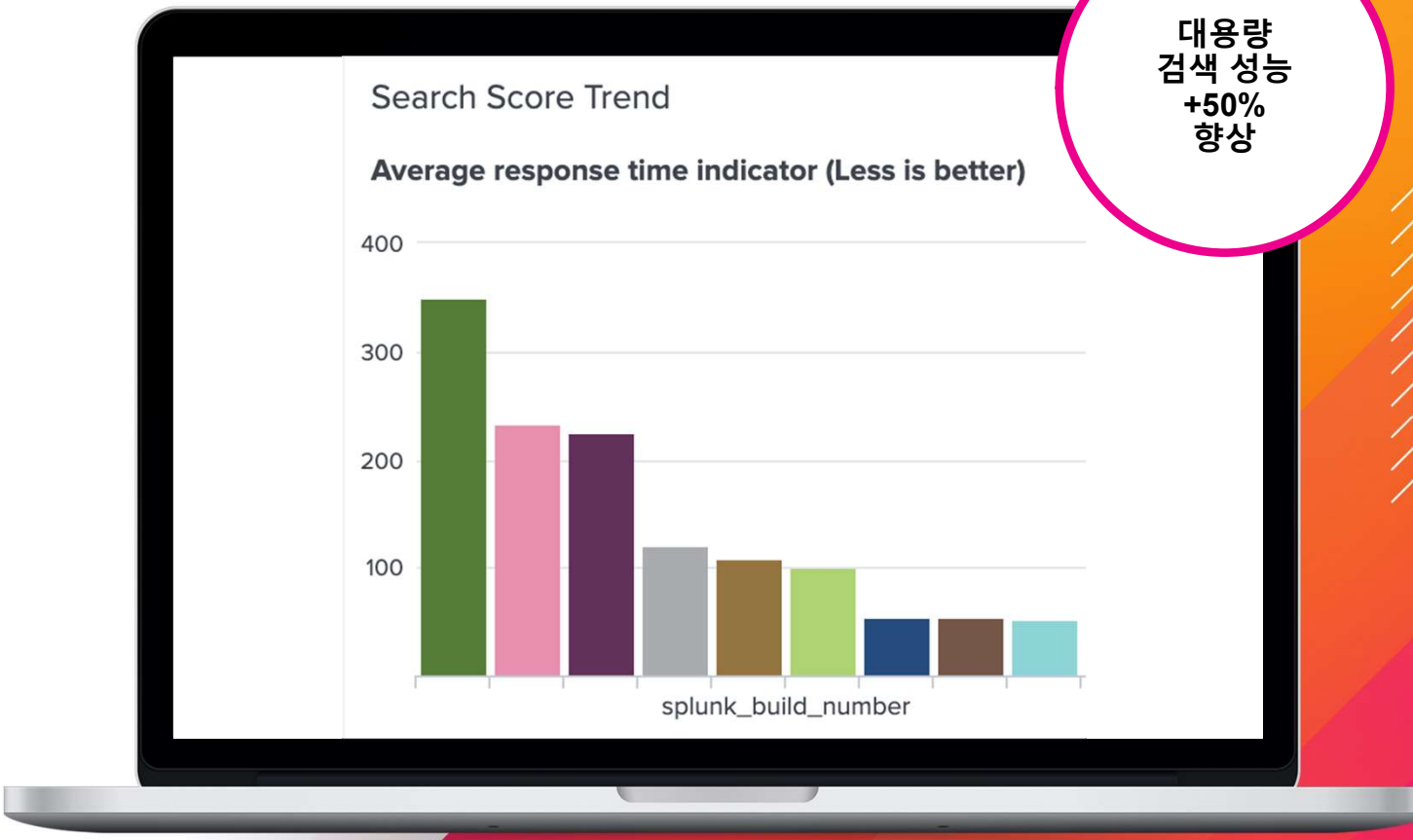
Cloud 관리

splunk> .conf20

검색 성능

We have the need for speed

- 가장 많이 사용되는 top 20 검색 커맨드 성능 최대 50% 증가
- Eval @ Ingest Time (On-Prem)

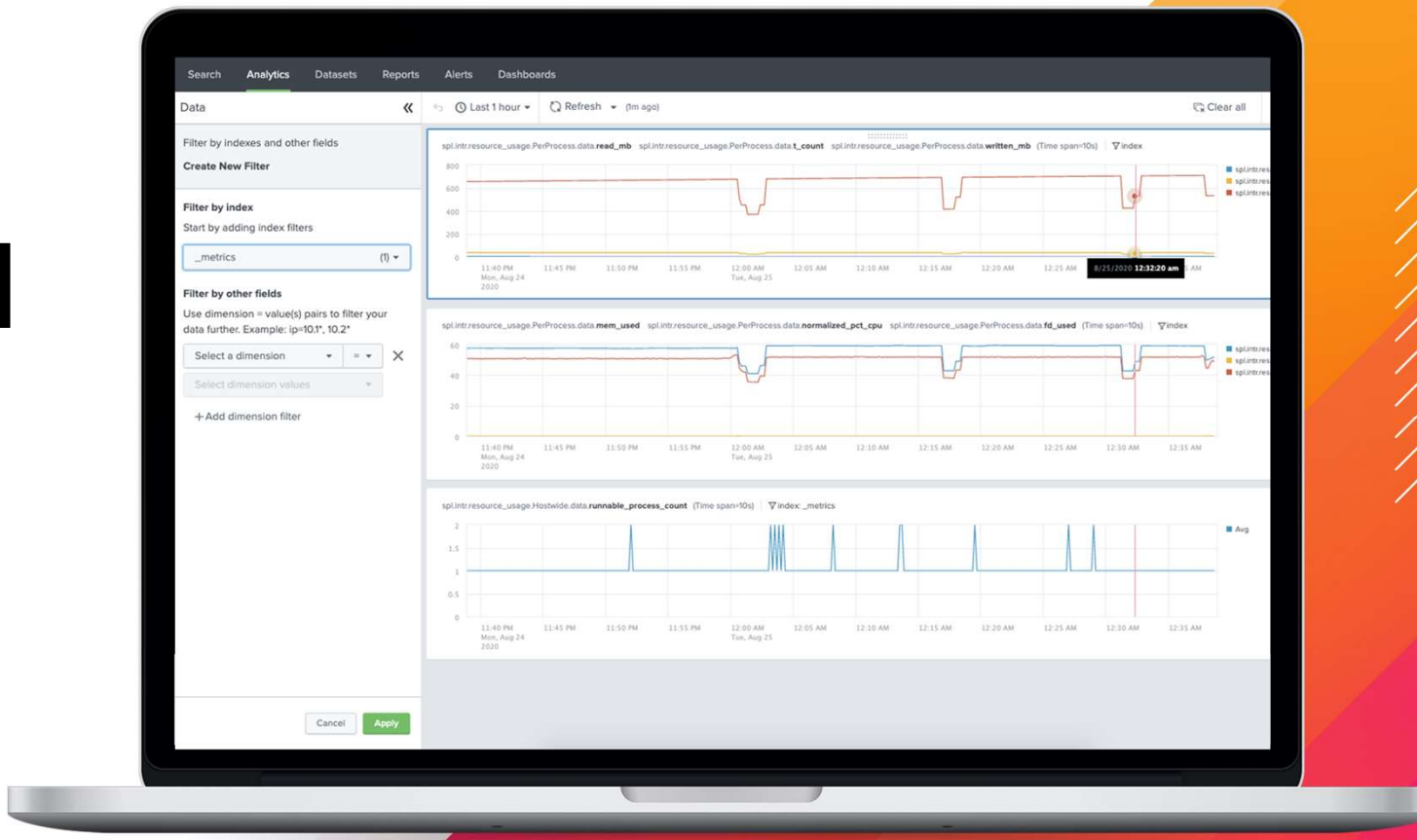


대용량
검색 성능
+50%
향상

메트릭 스토어

Metrics made easier

- 메트릭 검색 속도 증가 & 밀리세컨드 단위 지원 (Cloud only)
- 초당 2M+ 메트릭 처리 (Both)
- Analytics 워크스페이스에서 메트릭 필터링



Rolling Restarts

Re-something, not restart!

발생 감소

75% 

Splunk Cloud 에서 발생한
rolling restart

Self-service 앱

Top 25 Cloud Apps

Rolling restart 없이
직접 설치 가능

Cloud 에서의 확장성

100TB

100TB

Elastically 확장

Scale for Cloud @ 100TB, for Core, ES, and ITSI

3X

KV Store

Improvements yields 3X reduction in storage requirements

0

Zero-impact

Elastically scale up or down

What's New: .conf20

Splunk Cloud and Splunk Enterprise 8.1

생산성 증대

접근 & 제어

성능& 신뢰성

다양한 선택

- GCP & AWS 리전
- Kubernetes
- Workload pricing

Cloud 관리

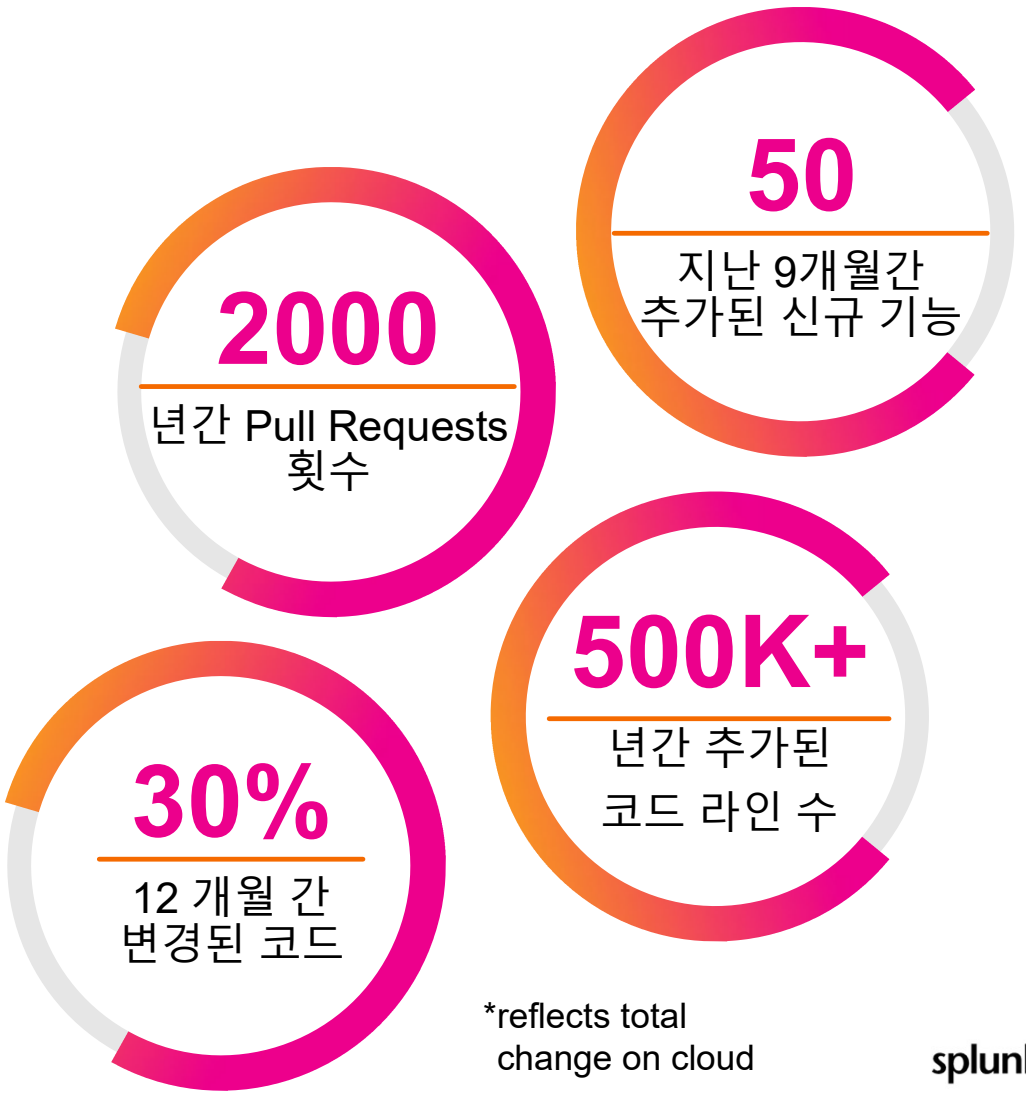
splunk> .conf20

Splunk Cloud
on AWS or Google

New Regions
(Seoul)

Generally
Available
(New)

Reinventing
for Cloud



*reflects total change on cloud

splunk> .conf20

Splunk Cloud 가격 정책

가격이 데이터에서 가치를 얻는 것을 막는 요소가 되어서는 안됩니다.

Workload Pricing

- 수집 용량 기준은 싫어요..
- 복합적인 사용 시나리오에 대한 비용 조정
- 워크로드 컨트롤

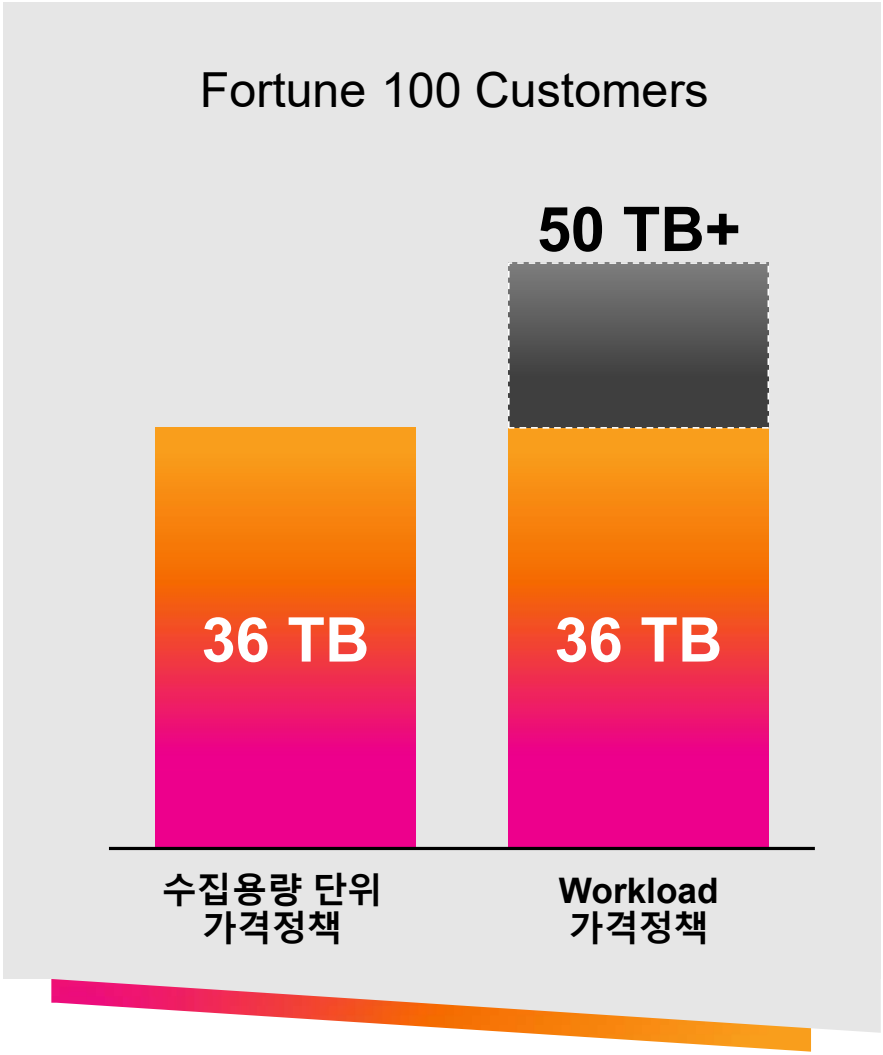
Ingest (per Gig) Pricing

- 잘 알려진 가격 정책
- 이해하기 쉽고 명확함
- 아키텍처와 무관

Rapid Adoption Packages

- 25GB 이하 수집 기준
- 가장 일반적인 use cases 에 집중
- 새로운 고객에게 적합

splunk> .conf20



왜?
Workload Pricing
이 더 유리할까요?

What's New: .conf20

Splunk Cloud and Splunk Enterprise 8.1

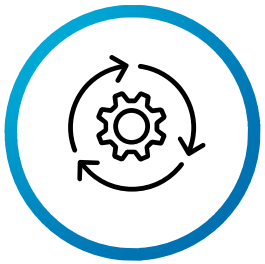
생산성 증대

접근 & 제어

성능& 신뢰성

다양한 선택

Cloud 관리



- 통합 모니터링
- New SaaS launch
- Self-Service Config

splunk> .conf20

The All New Splunk Cloud:
더 빠른 서비스
더 높은 가용성

- 4주 간격으로 릴리즈
- 업그레이드 시간 3x 감소
- 일 수집 용량 100TB 확장
- Private App 인증 자동화
- 75% 앱 Self-Installable

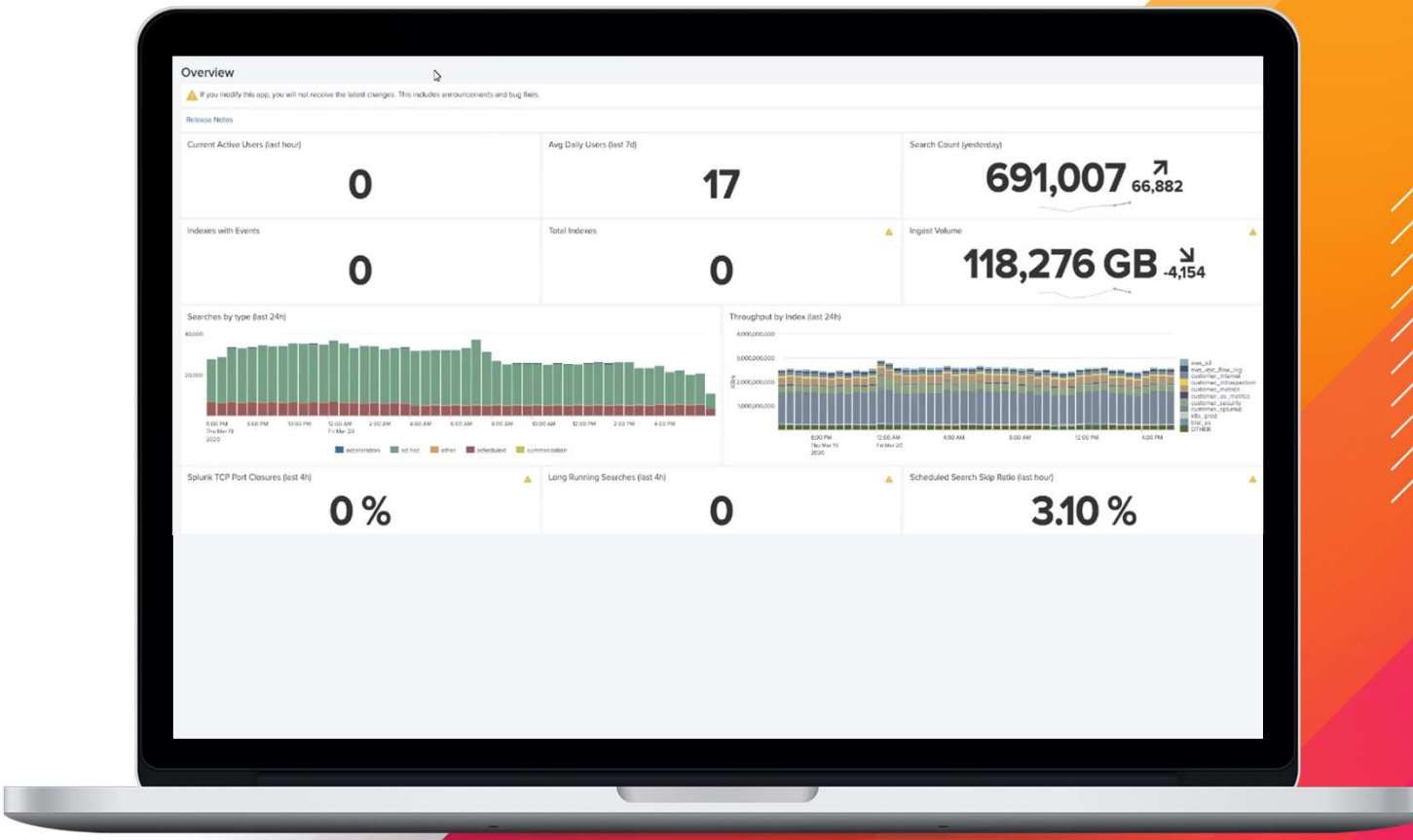
Cloud Monitoring Console (CMC)

Monitor all the things

Splunk Cloud 상태와 성능에 대한 인사이트 획득

새로운 대시보드에는..

- 라이센스 사용량: Cloud 리소스 사용량 관리
- 업그레이드 Readiness : 업그레이드로 인한 문제를 방지(App compatibility, etc.)
- 워크로드 관리 & 메모리 사용량이 높은 Top 20 검색 : 최적화해야 할 검색 결정



Cloud Admin Experience (CAE)

Stack the deck

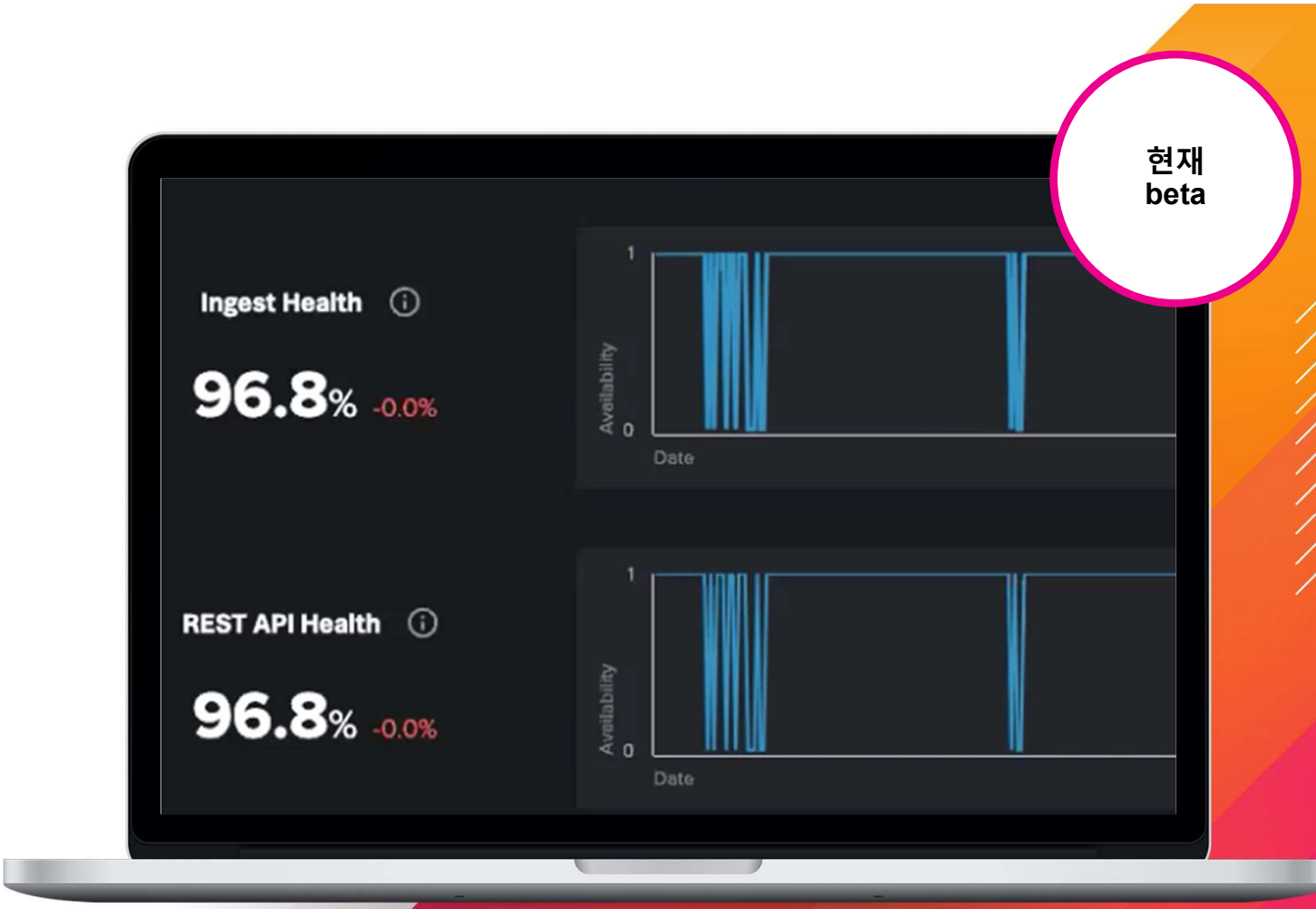
CMC 를 보완하는, 클라우드 관리자를 위한 새로운 SaaS

현재버전

- 현재 상태 페이지 (SLA, SLI)
- 라이센스 사용량, entitlement
- CMC 링크

다음버전

- Maintenance 스케줄
- 서포트 케이스
- 간단한 사용 방법
- Multi-stack 가시화



Admin Config Service

Self-service at your service

CMC 를 보완하는, 클라우드 관리자를 위한 새로운 SaaS

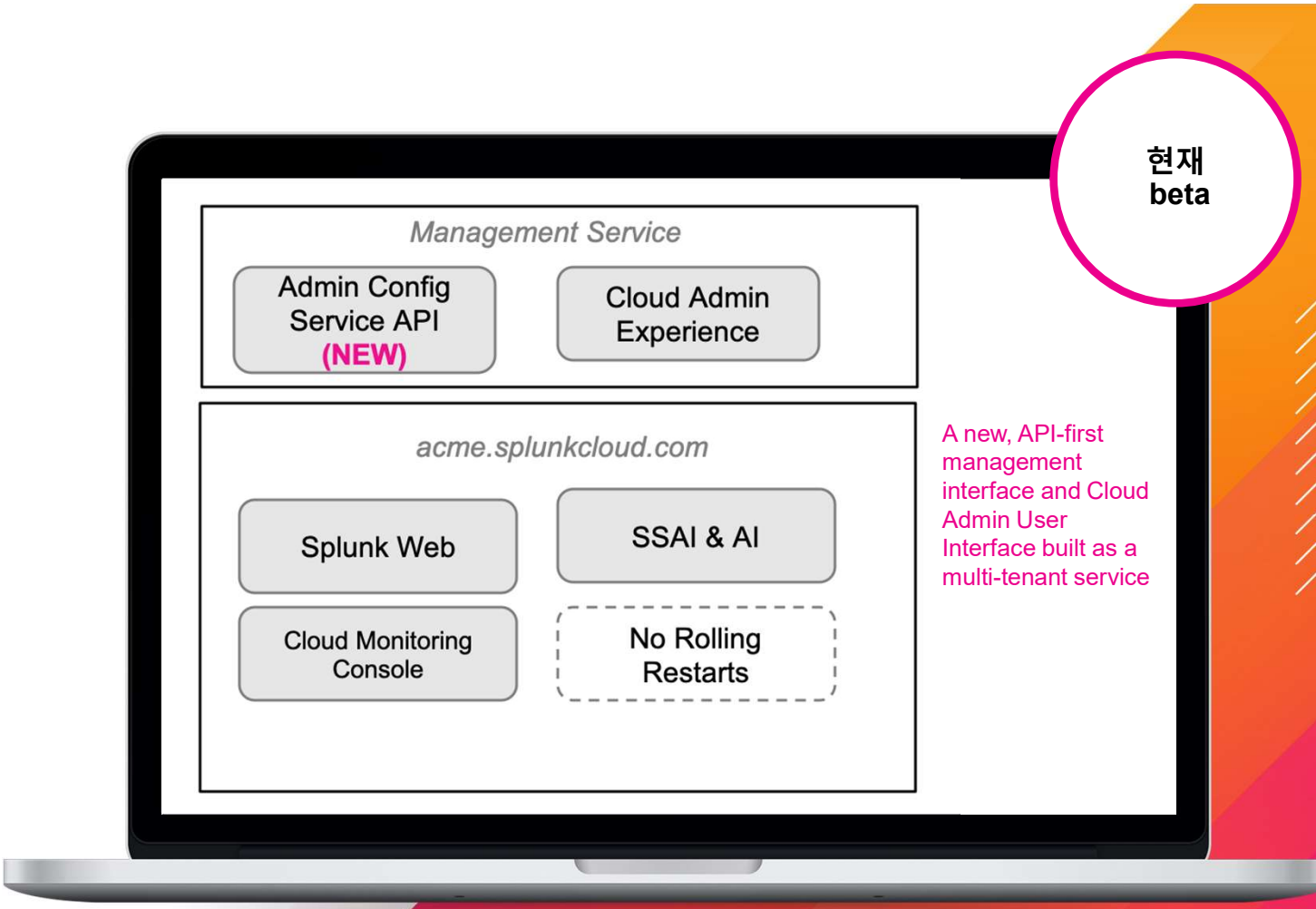
다음 관리 작업을 지원

현재버전

- IP Allow List

다음버전

- Index 관리
- HEC Token 관리
- Private & Splunkbase App 앱 설치
- 배치 작업들

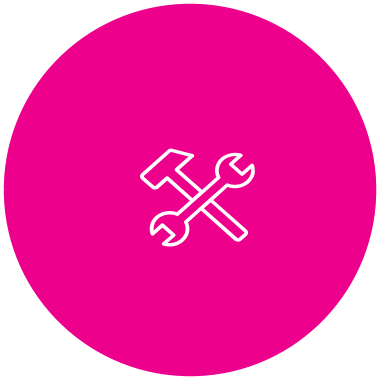


Splunk
Data Stream Processor 1.2

Our customers want...

Pre-Ingest 플랫폼

대용량의 수집 Data를 실시간으로 관리하고 처리할 수 있는 플랫폼



Pre-Ingest Data 변경

수집 Data 를 구조화하고 불필요하거나 민감한 Data를 제거

의미 있는 Data만 최종 사용자에게 전달

Data 전달 제어

Right Data를 Right User 에게 전달

실시간 Data 통찰력

Data가 최종 사용자에게 전달되기 전에 특정 조건 또는 패턴을 탐지

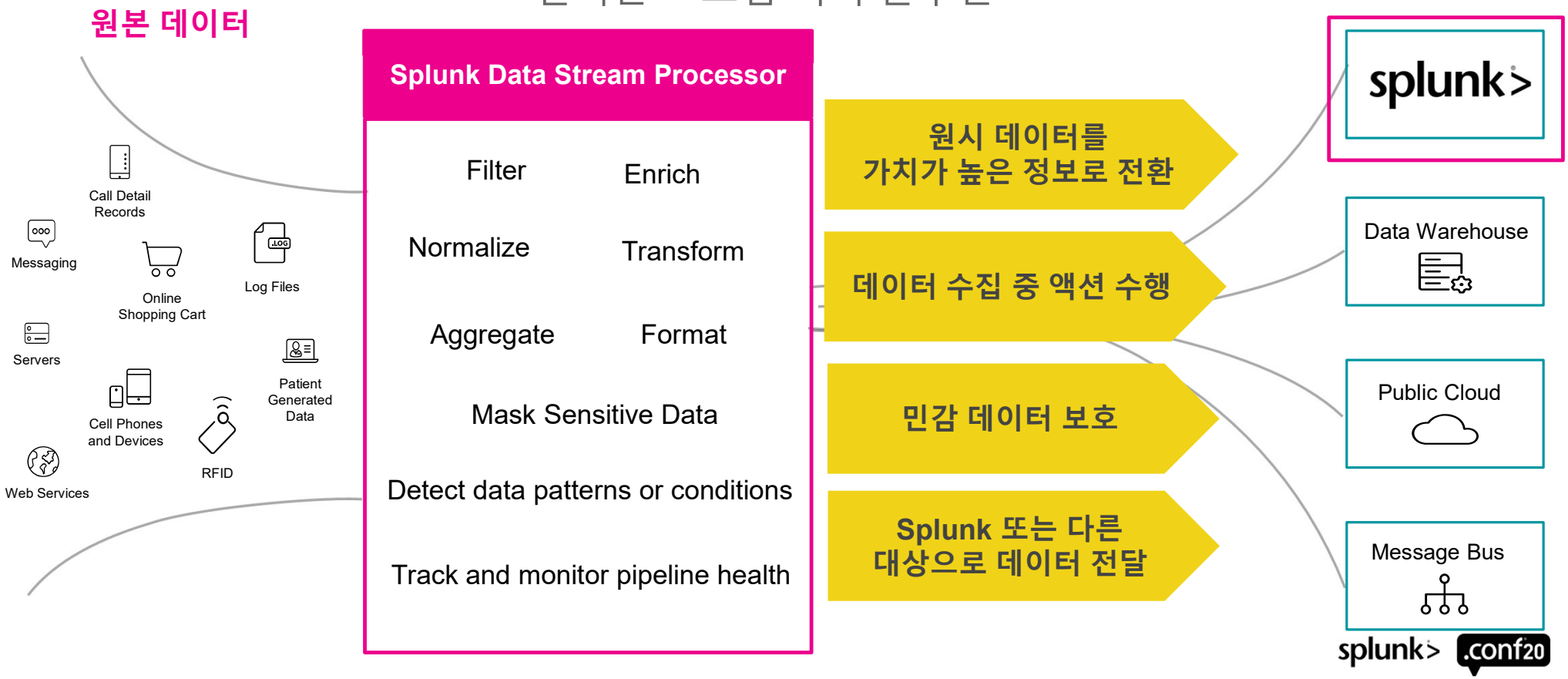
Splunk Data Stream Processor

- Apache Top Level Project
- 주요 사용 고객 : Verizon, Comcast, Tencent 등
- 최신 버전 : 2.6.1
- 최초 Release 일자 : 2016년 8월
- 주요 기능 :
  - Topic 기반의 메시징 미들웨어
  - 메시징(이벤트)의 안정적인 저장 및 전달을 담당

- Apache Top Level Project
- 주요 사용 고객 : Uber, Ericsson, ebay 등
- 최신 버전 : 1.11.2
- 최초 Release 일자 : 2015년 6월
- 주요 기능 :
  - Streaming / Batch processing 을 위한 분산 처리 엔진
  - 실시간 이벤트 수신 및 처리를 위한 다양한 기능 제공

Splunk Data Stream Processor

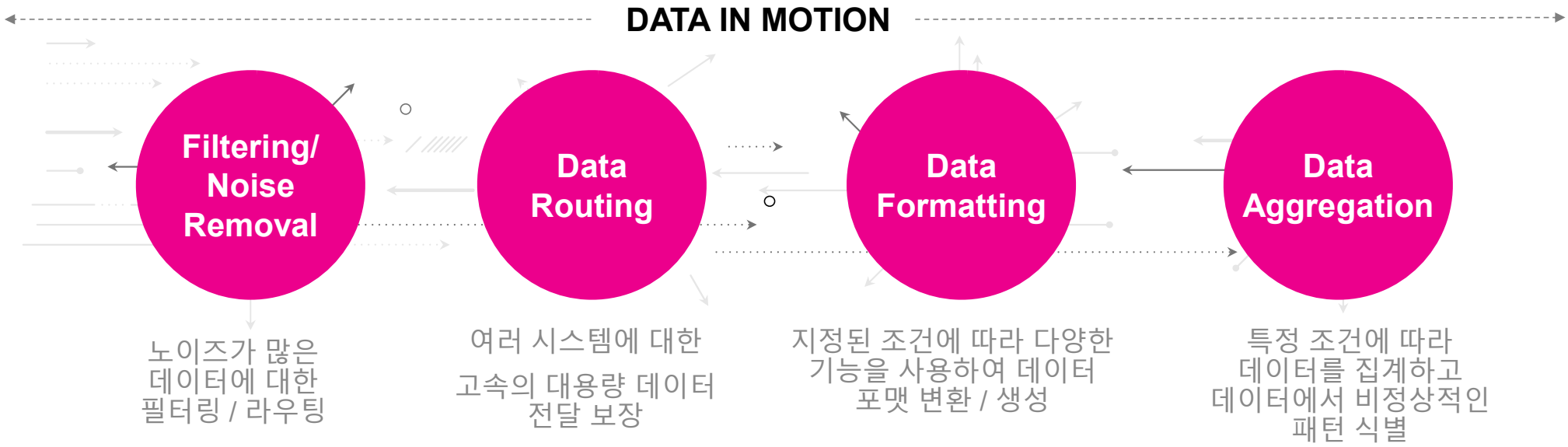
다양한 대상의 데이터를 밀리초 내에 수집, 가공, 전달을 수행할 수 있는
실시간 스트림 처리 솔루션



주요 사용처

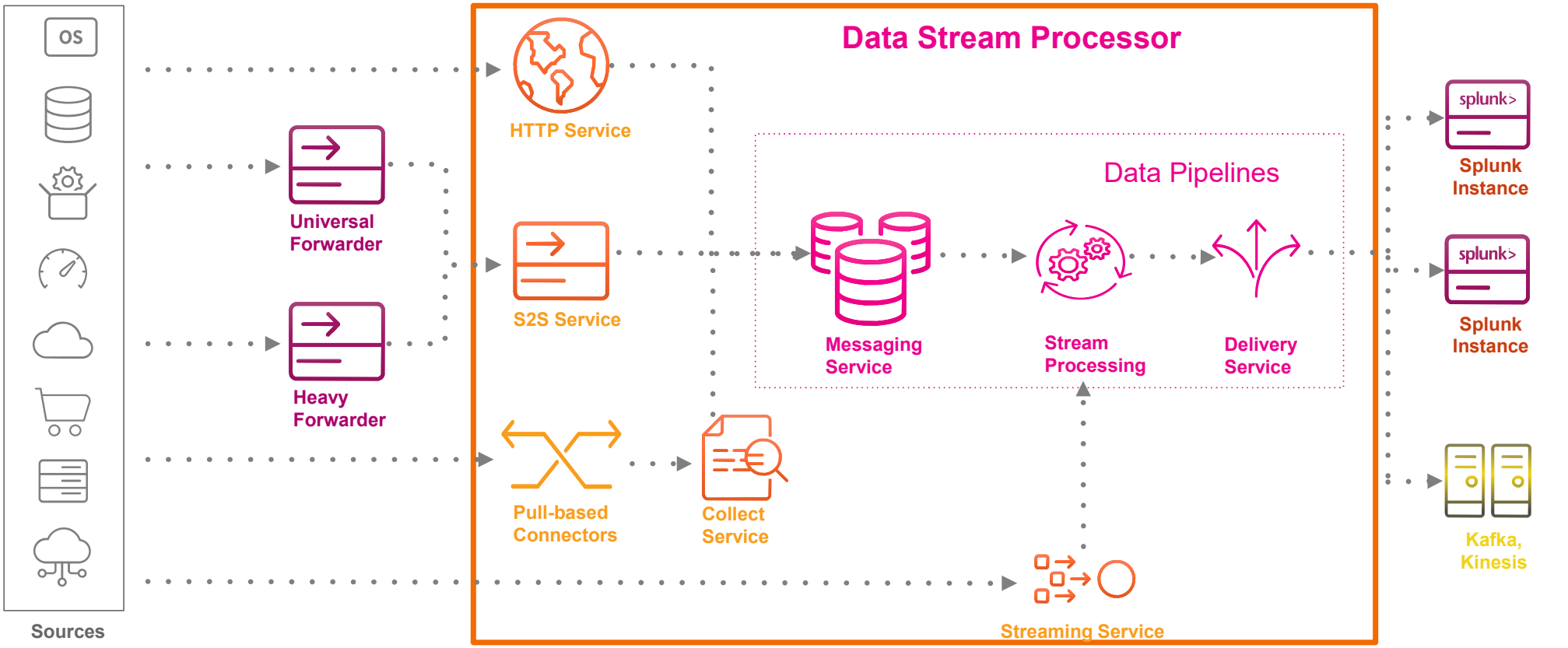
컴플라이언스 & 데이터 보호	GDPR과 같은 데이터 관련 규정 준수 개선 민간 데이터에 대한 비식별화 처리	**사용자 식별 정보** 또는 **신용카드 정보** 등 중요한 데이터에 대한 **마스킹**
즉각적인 비즈니스 통찰력 확보	데이터 수집 / 이동 중일 때 비정상적인 활동 또는 동작 감지	**특정 임계값** 또는 **조건을 초과하는 개별 이벤트를 요약**하여 분석가에게 즉시 전송하여 추가 조가
데이터 수집 운영 효율성 향상	사용자가 중요한 데이터 분석에 더 많은 시간을 할애할 수 있는 전사 단일 데이터 교환 플랫폼	**다양한 소스에서 데이터를 수집**하고, 데이터를 가치 있는 정보나 통찰력을 바꾼 후, **다양한 시스템에 결과를 전달**하는 **단일 플랫폼**

Technical Use Cases



DSP Architecture

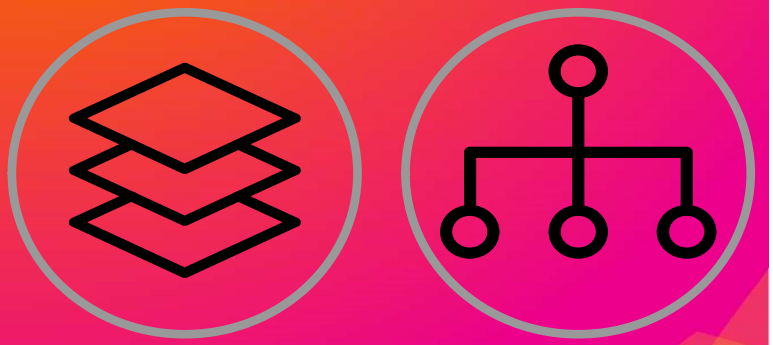
Splunk Solution



Sources / Sinks

Data collection sources offered in multi cloud + on premises environments

Data destinations



Sources

Connectors

- AWS S3 Connector
- AWS Metadata Connector
- AWS Cloud Watch Metrics Connector
- Azure Monitor Metrics Connector
- MS Office 365 Connector
- Splunk Connect for Syslog (SC4S)
- GCP Stack-Driver metrics Connector
- GCP Monitoring metrics Connector

Splunk

- Splunk Forwarder + Heavy Forwarder S2S
- HTTP Event Collector (HEC)

Message Bus

- Read from Message bus-clients
  - Kinesis
  - Kafka two way SSL
  - Azure Event Hubs

REST API

Sinks

Splunk Enterprise + Splunk Cloud

Send data to multiple splunk instances and indexes

SignalFx

Send metrics data to SignalFx

Amazon S3

Lower storage costs by sending data to S3

Kafka + Kinesis + Event Hubs

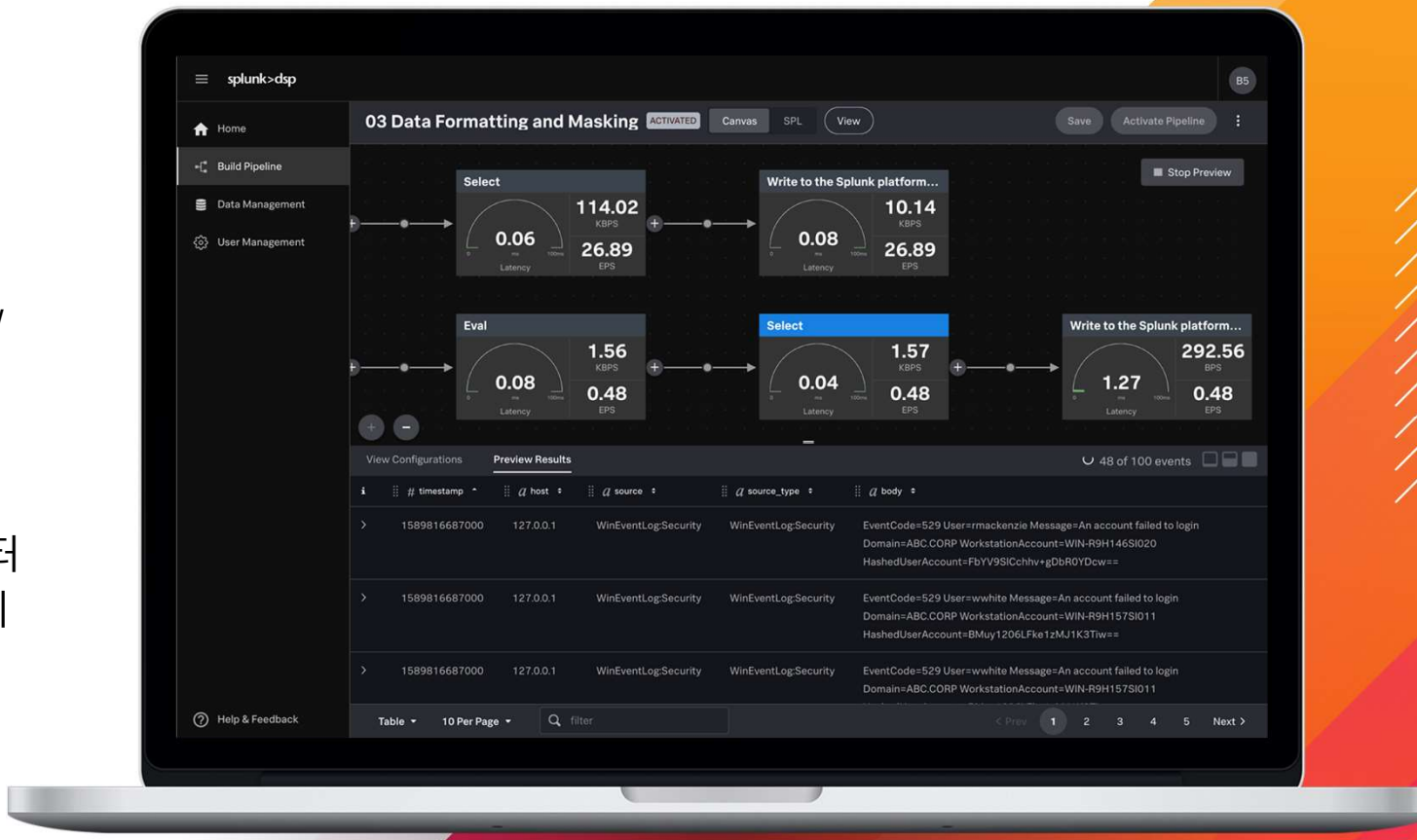
Write data back to your preferred message brokers whether it be Apache Kafka, Amazon Kinesis or Azure Event Hubs

Data Pipelines

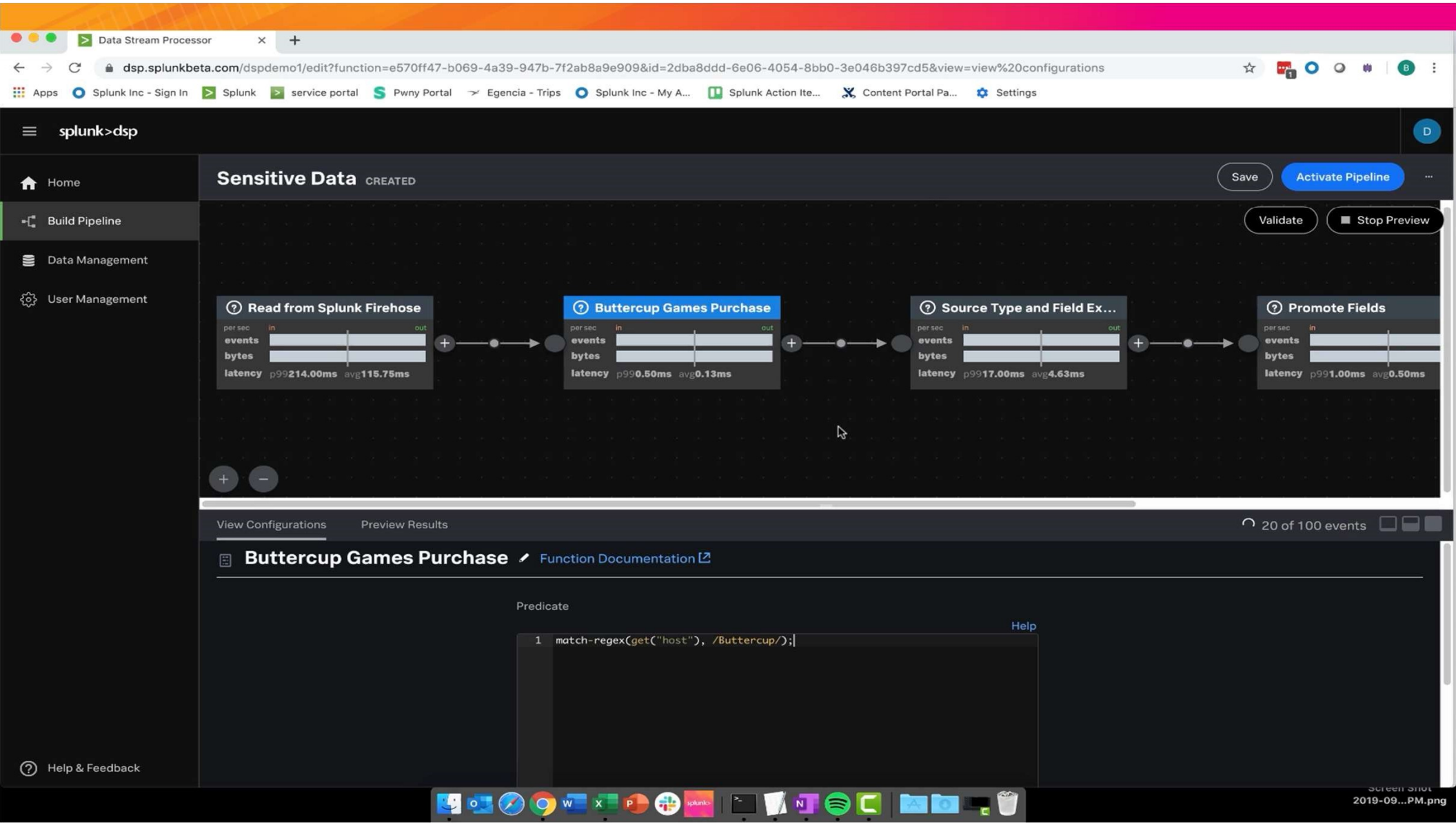
WHAT IT IS

실시간 데이터에 대한 필터링 / 변환 / 마스킹 등을 시각적으로 정의한 플로우

사용자 요구사항에 맞춰 데이터 처리에 대한 흐름을 손쉽게 정의



splunk> turn data into doing


Data Stream Processor
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 p99 214.00ms avg 115.75ms
Buttercup Games Purchase
per sec in out
events
bytes
latency p99 0.50ms avg 0.13ms
Source Type and Field Ex...
per sec in out
events
bytes
latency p99 17.00ms avg 4.63ms
Promote Fields
per sec in
events
bytes
latency p99 1.00ms avg 0.50ms
View Configurations
Preview Results
20 of 100 events
Buttercup Games Purchase
Function Documentation
Predicate
Help
1 match-regex(get("host"), /Buttercup/);

SPLUNK CLOUD

CUSTOMER MANAGED

What's New

Data Stream Processor

멀티 클라우드 환경을 위한 Source 추가

- GCP Pub/Sub source
- Azure Event Hub sink

Data 제어 기능 확장

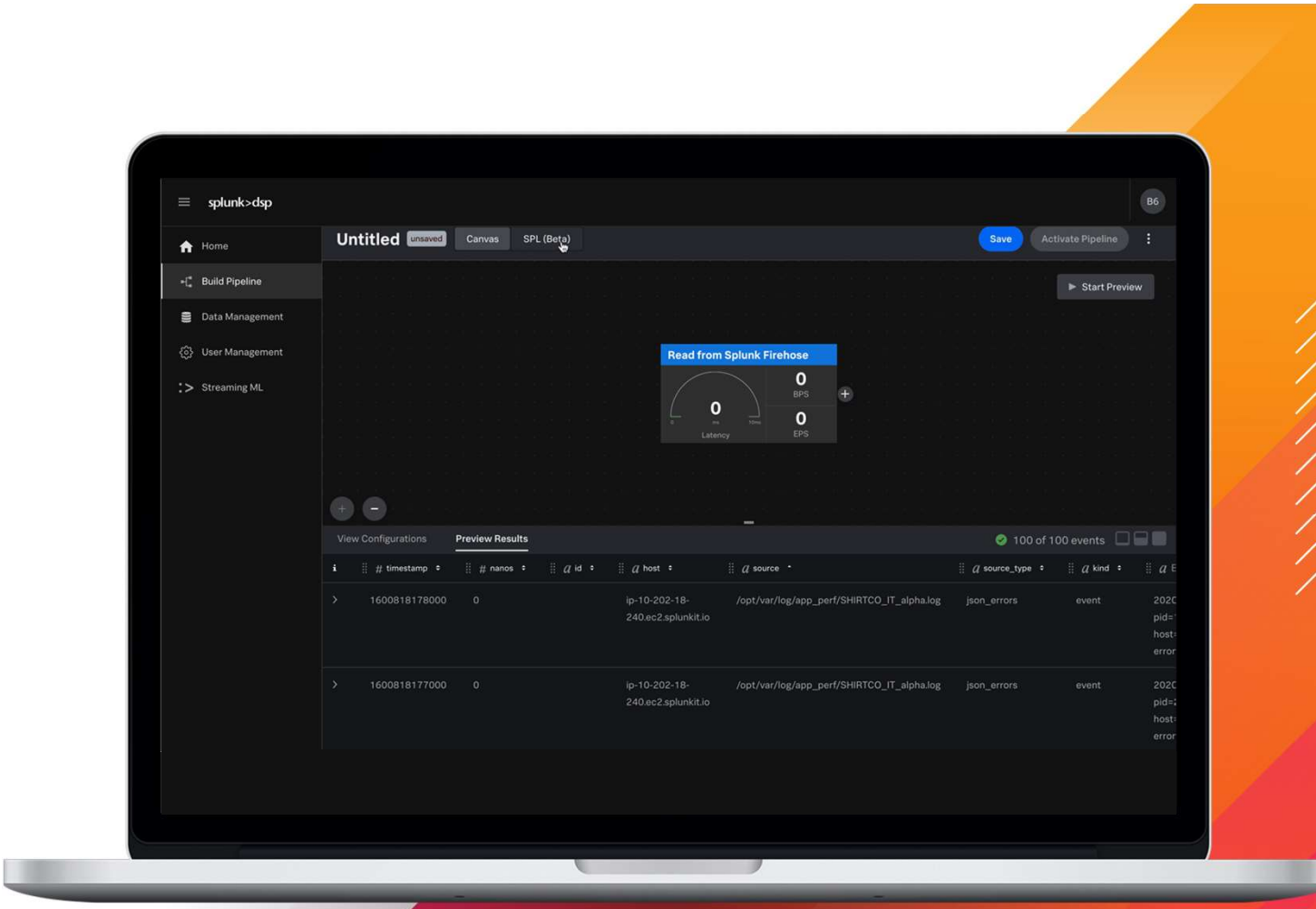
- 로그 데이터를 지표 및 트레이스 데이터로 변환
- 비표준 데이터를 표준 포맷으로 변환
- 여러 목적지 시스템으로 라우팅

Enrichment 기능 추가

- 룩업 기능을 통한 수집 데이터에 대한 Enrichment
- Unbounded ML on the stream

Announcing

SPL in Data Stream Processor



SPLUNK CLOUD

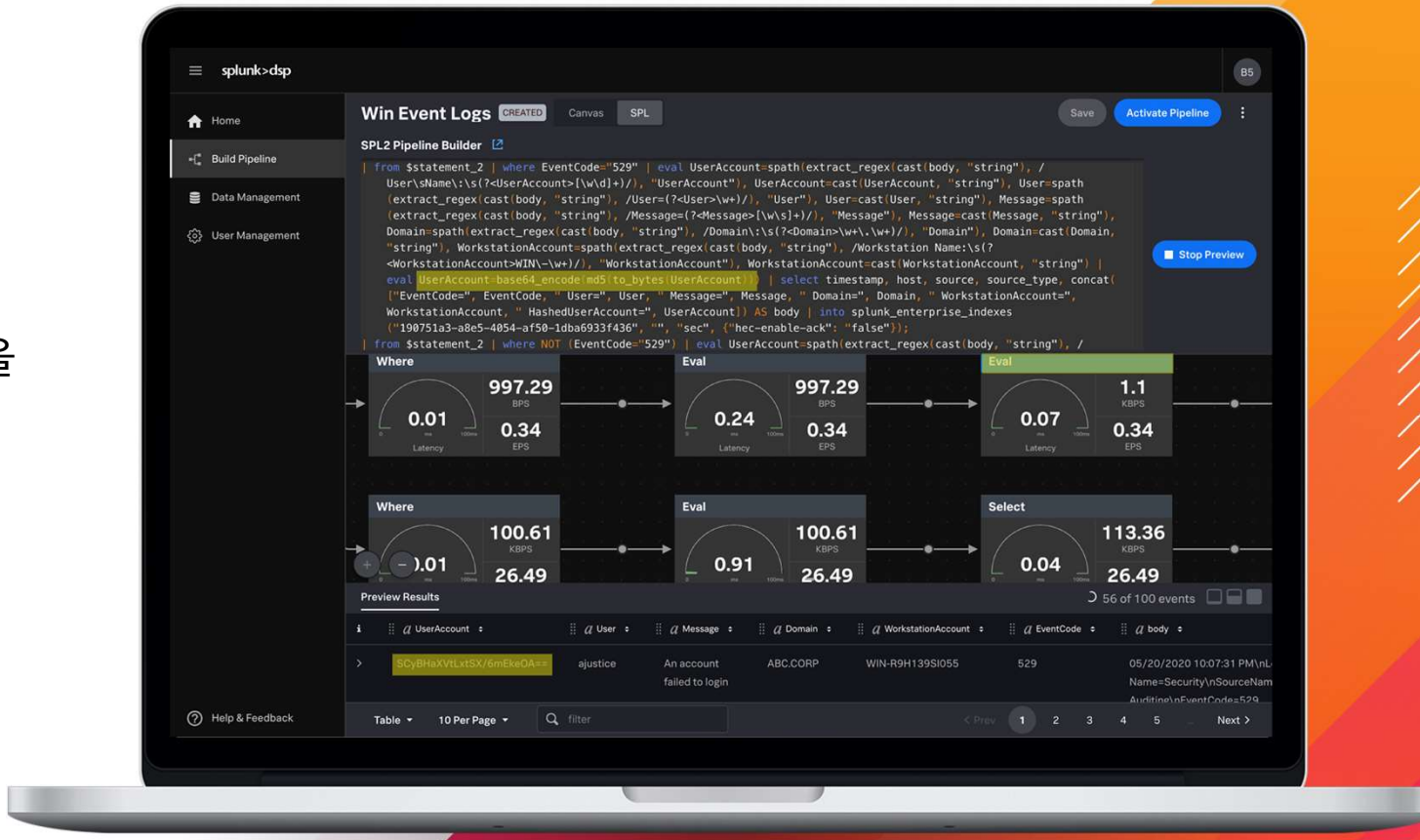
CUSTOMER MANAGED

splunk> turn data into doing

Eval Function

WHAT IT IS

데이터에 대한 다양한 변환을 수행할 수 있는 함수

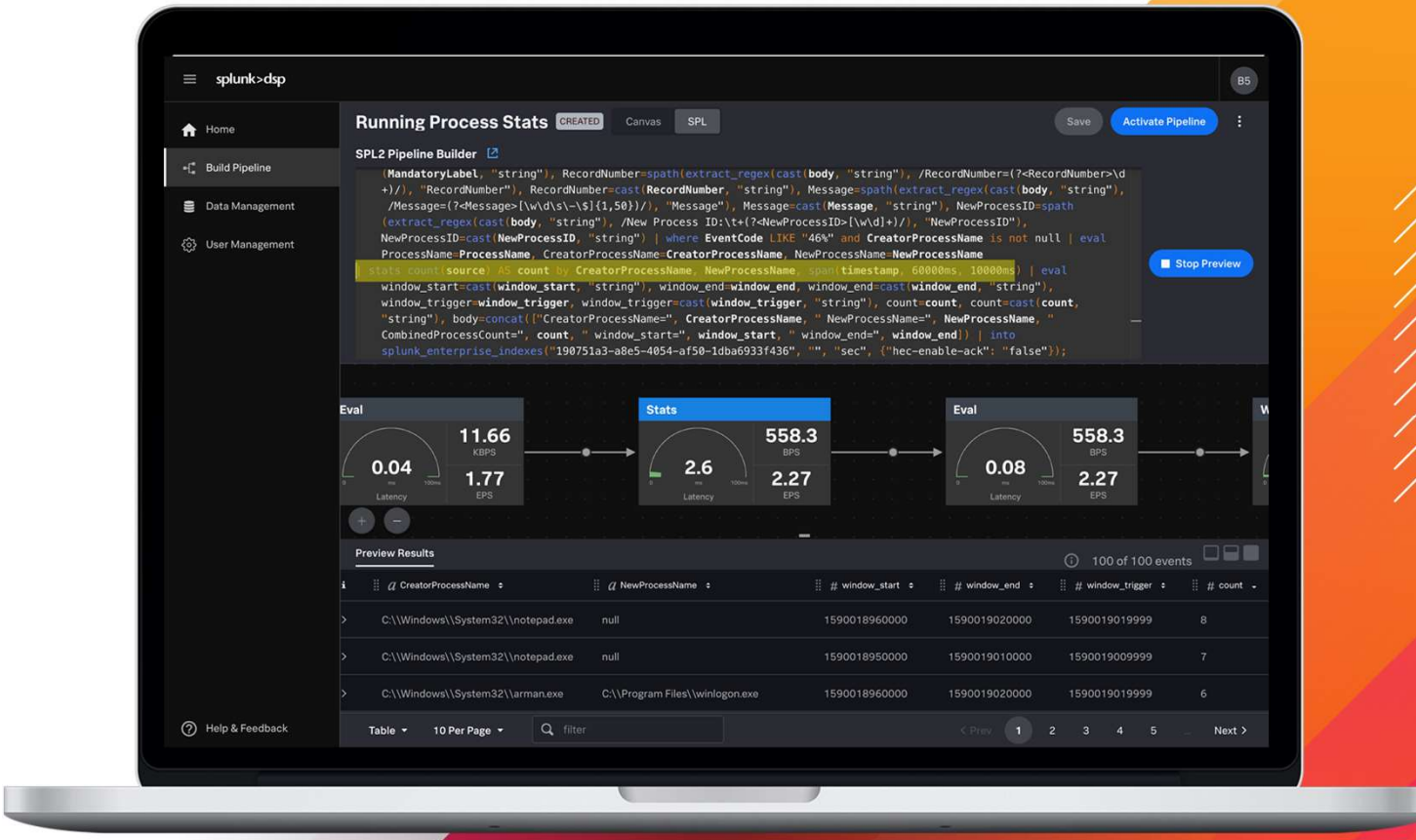


splunk> turn data into doing

Stats Function

WHAT IT IS

평균 / 최소 / 최대값 등을 계산하기 위한 집합 함수



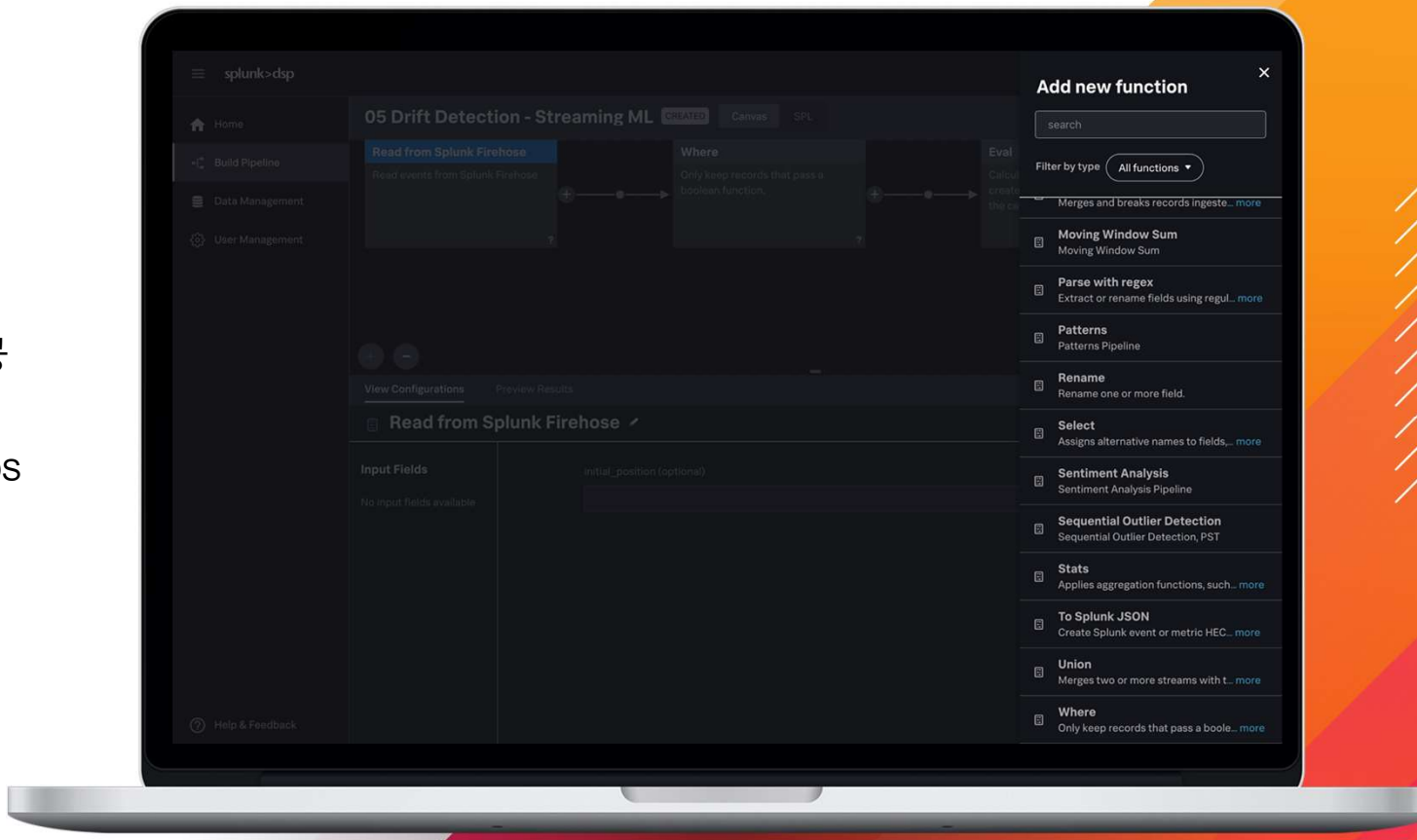
splunk> turn data into doing

And many more...

Functions Library

약 60여종의 Pre-Buillt 함수 제공

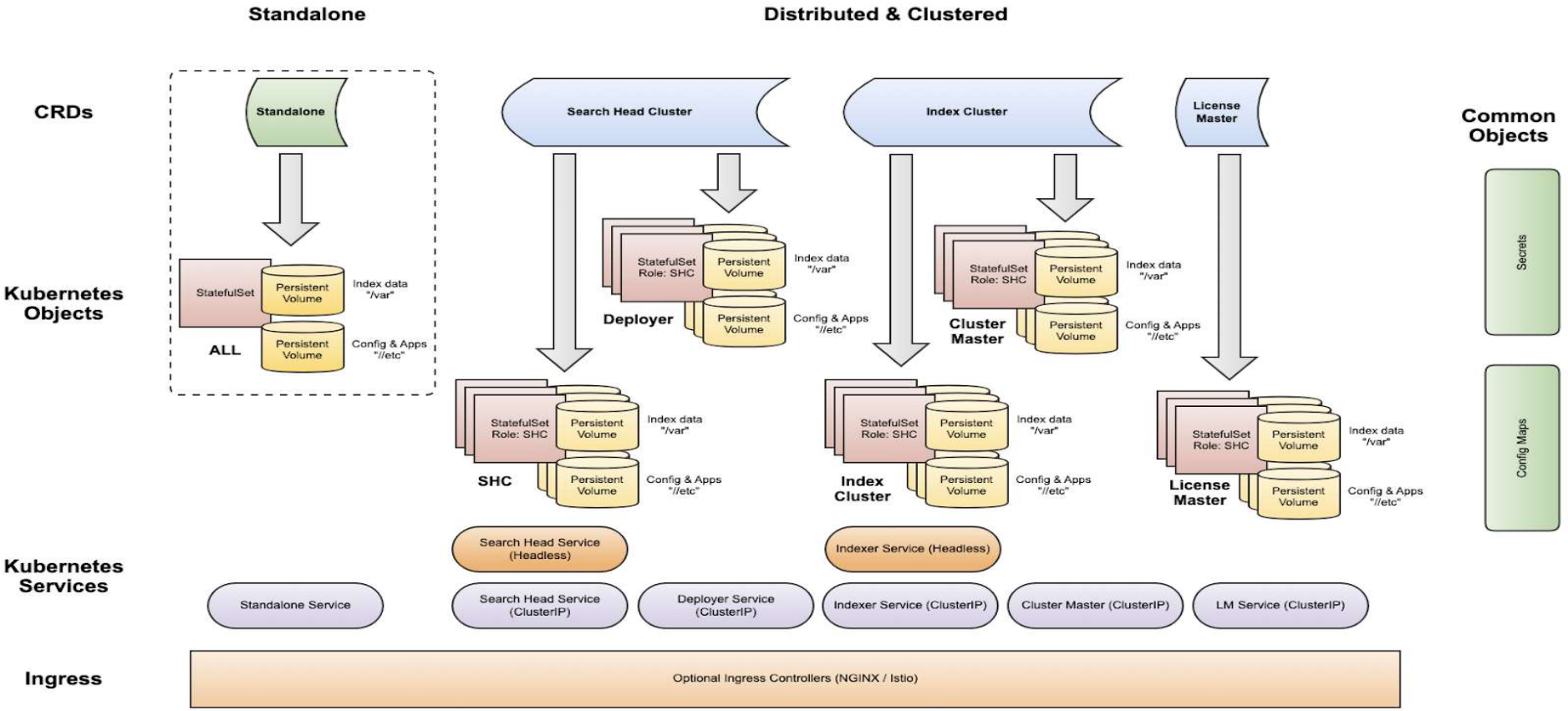
https://docs.splunk.com/Documentation/DSP/1.2.0/FunctionReference/Howtouse



splunk> turn data into doing

Splunk Enterprise Operator for Kubernetes

Splunk Operator for Kubernetes



splunk> .conf20

BETA

Announcing

Splunk Enterprise Operator for Kubernetes

고객사 상황에 맞는 Public / Private 클라우드 환경에 배포

Push-Button 배포

SmartStore 사용

Multi-Site 지원

https://github.com/splunk/splunk-operator

Splunk Machine Learning Environment

Splunk ML

Reasons to bring your compute to where the data is …

SMLE Studio Experience

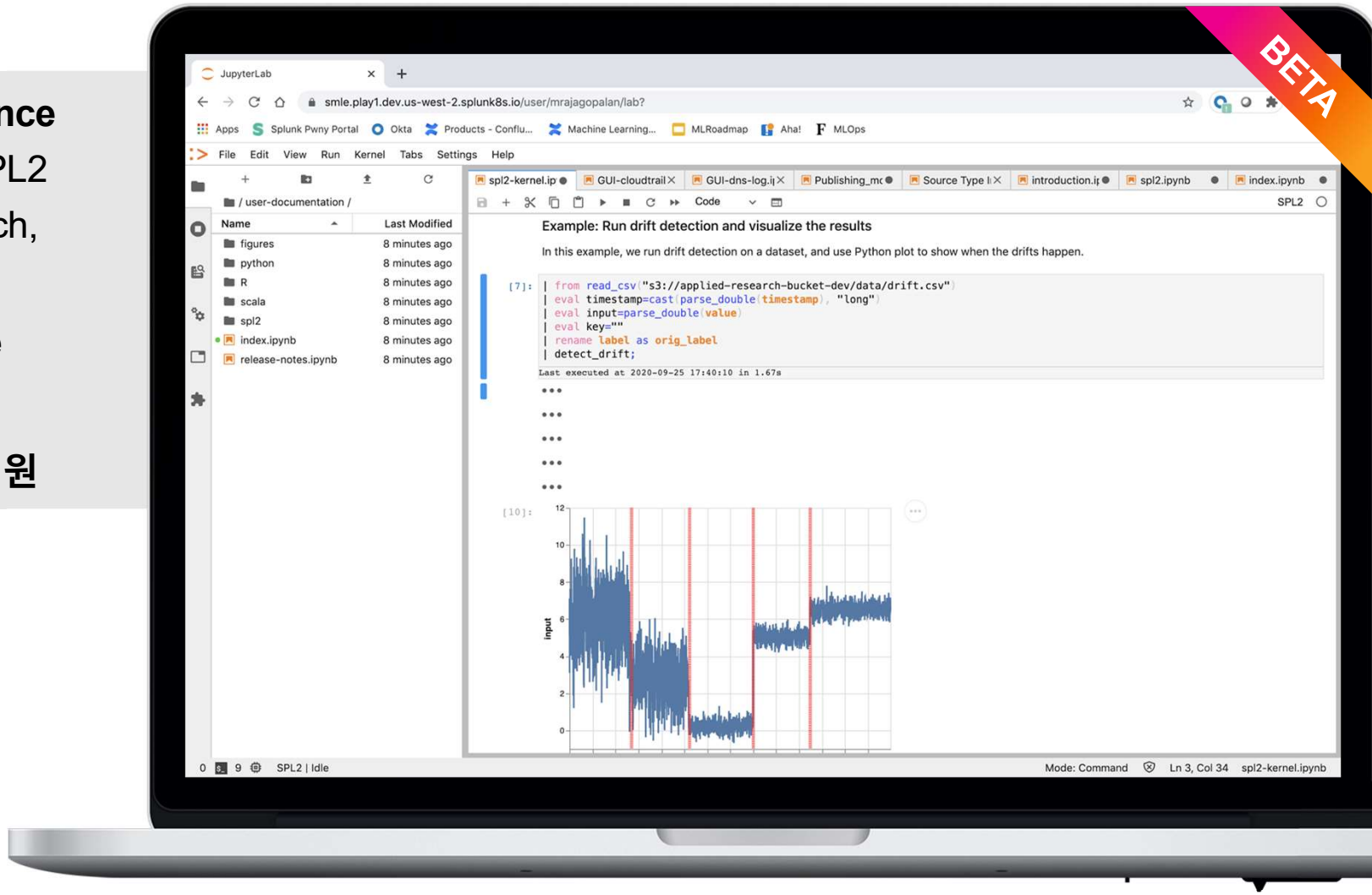
- R, Python, Scala, SPL2
- TensorFlow, PyThorch, Propeht, etc.

Smart MLOps Service

- 배포, 관리, 모니터링

배치 & 스트리밍 ML 지원

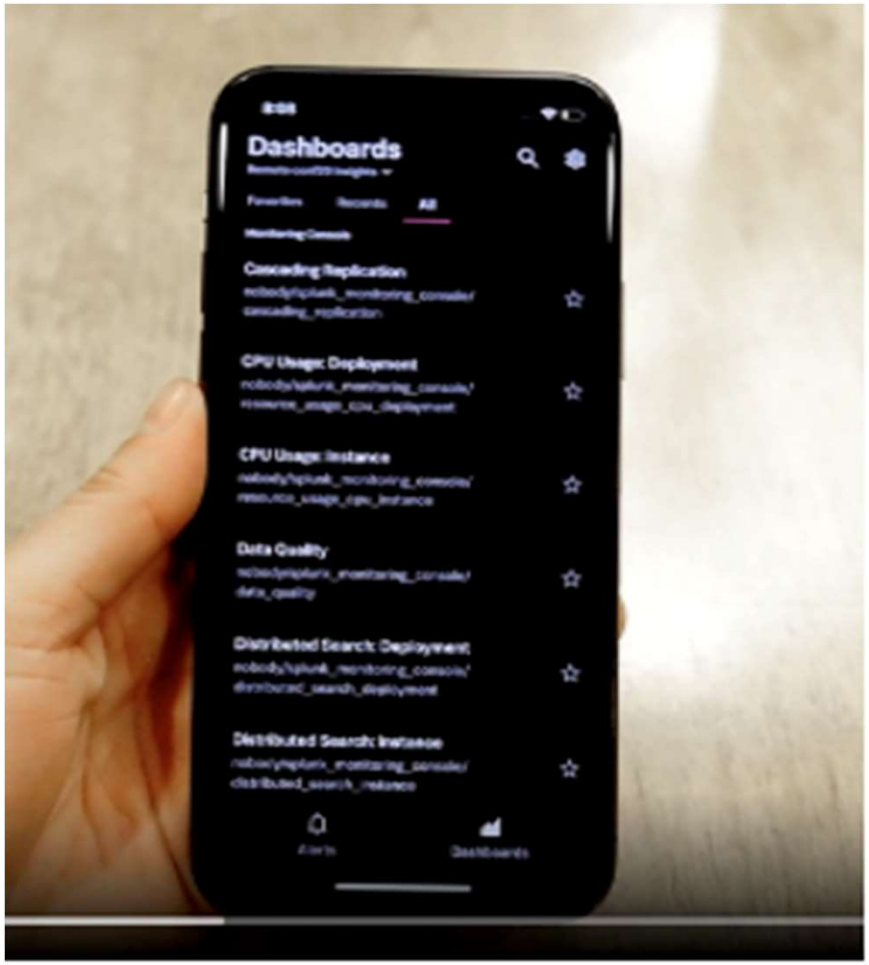
smle



Splunk Connected Experience

Splunk® Mobile

- Splunk Secure Gateway
- Splunk Dashboard 를 모바일 화면에 딱 맞게!
- 알람 수신
- Slack 등 화면 공유
- MDM 으로 배포 및 관리



Splunk® AR

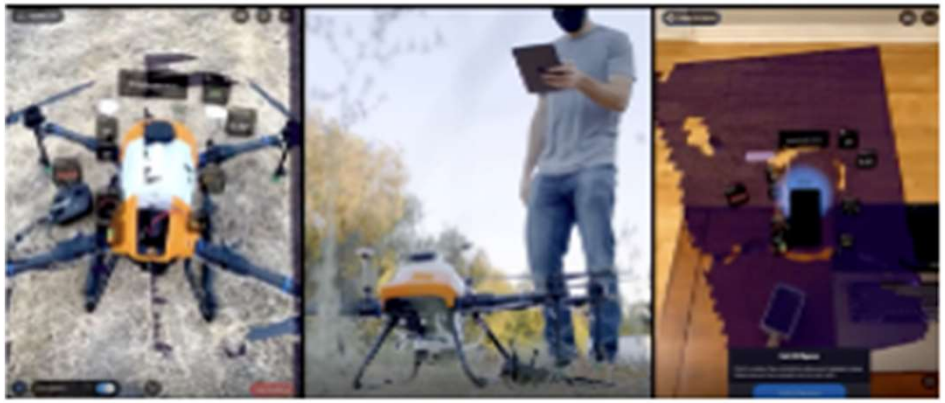
- 대시보드, 문서, 메시지 추가
- Workspace Editor
- 원격 collaboration
- 텍스트 & 로고 인식

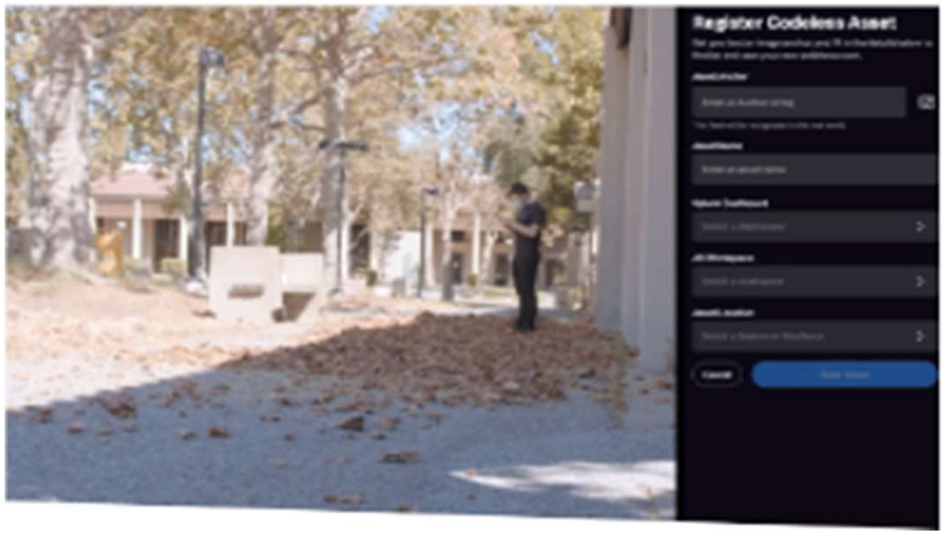
Splunk® VR

- Hololens 지원

Splunk® TV

- Android TV & Fire TV 지원

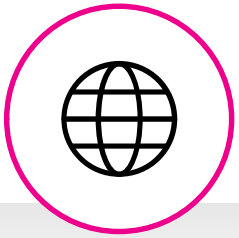




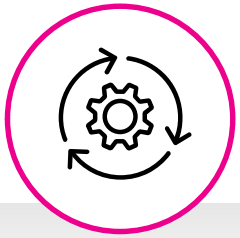
Day1. Summary

Market-Leading 포트폴리오

Security



IT



Observability

Data-to-Everything Platform

Common Work Surface, APIs, Developer Tools | Mobile and Connected Experiences

스트림 프로세싱 | 머신 러닝 | 확장 가능한 인덱스 | 페더레이트 검색 및 분석 | Collaboration & Orchestration

하이브리드와 멀티 클라우드 환경에서 수집 및 프로세싱

Splunk 설문 이벤트

splunk> .conf20

Splunk Korea 카카오 채널

- 프로모션
- 가장 최신의 업데이트
- Splunk Korea 행사 소식
- 월간 뉴스레터
- 워크샵 안내 등

Splunk의 주요 소식을 가장 빠르게

찾아볼 수 있는 방법입니다.

감사합니다