Splunk 소개

머신데이터 플랫폼

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.

Who is Splunk?

- **글로벌 HQs:**
  - 샌프란시스코(AMER)
  - 런던(EMEA)
  - 홍콩(APAC)
- **직원수 전세계 6,000+명**
- **연 매출 약 2조 4천억원 ($1,803 YoY +30%)**
- **나스닥 상장 : SPLK**

- **2003년 시작**
- **제품 구성:**
  - Splunk Enterprise
  - Splunk Cloud
  - Premium Solutions
    - Enterprise Security
    - IT Service Intelligence
  - UBA, Phantom, SignalFX

- **고객사 (전체): 16,000+**
- **국가기준: 110개국+**
- **Fortune 100대 기업: 92+**
- **고객사 (한국): 400+**
  - 중소기업, 대기업, 그룹 계열사
- **최대 라이센스: 10+ PB/일**

Every Company Has a Universe of Real-time Data

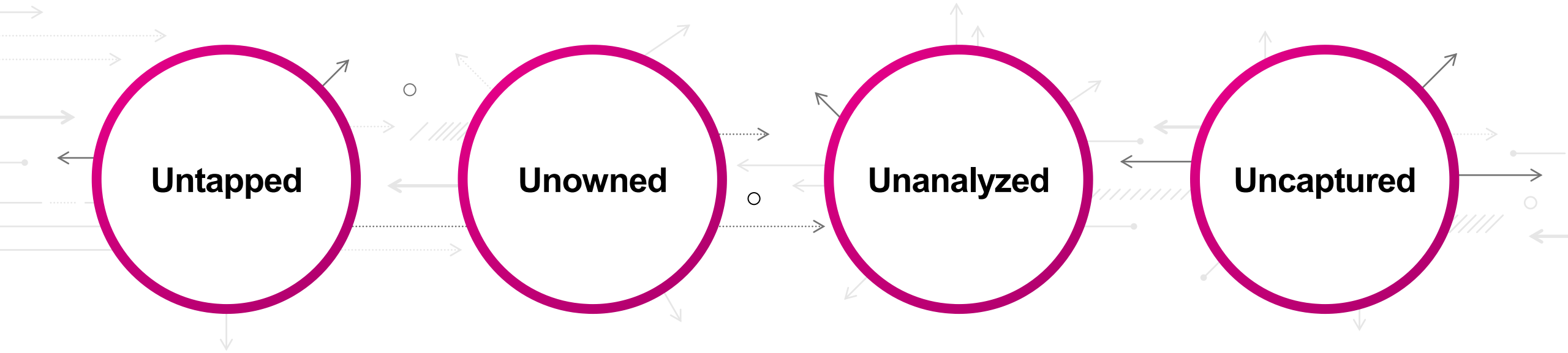
Creating More Opportunities and Threats than Ever Before

- Inventory RFID'S
- Assembly Robots
- Databases
- Business Apps
- Warehouse Utilization Systems
- Control Units
- New Technology
- New Data Streams
- Networks
- New Devices

splunk> turn data into doing™

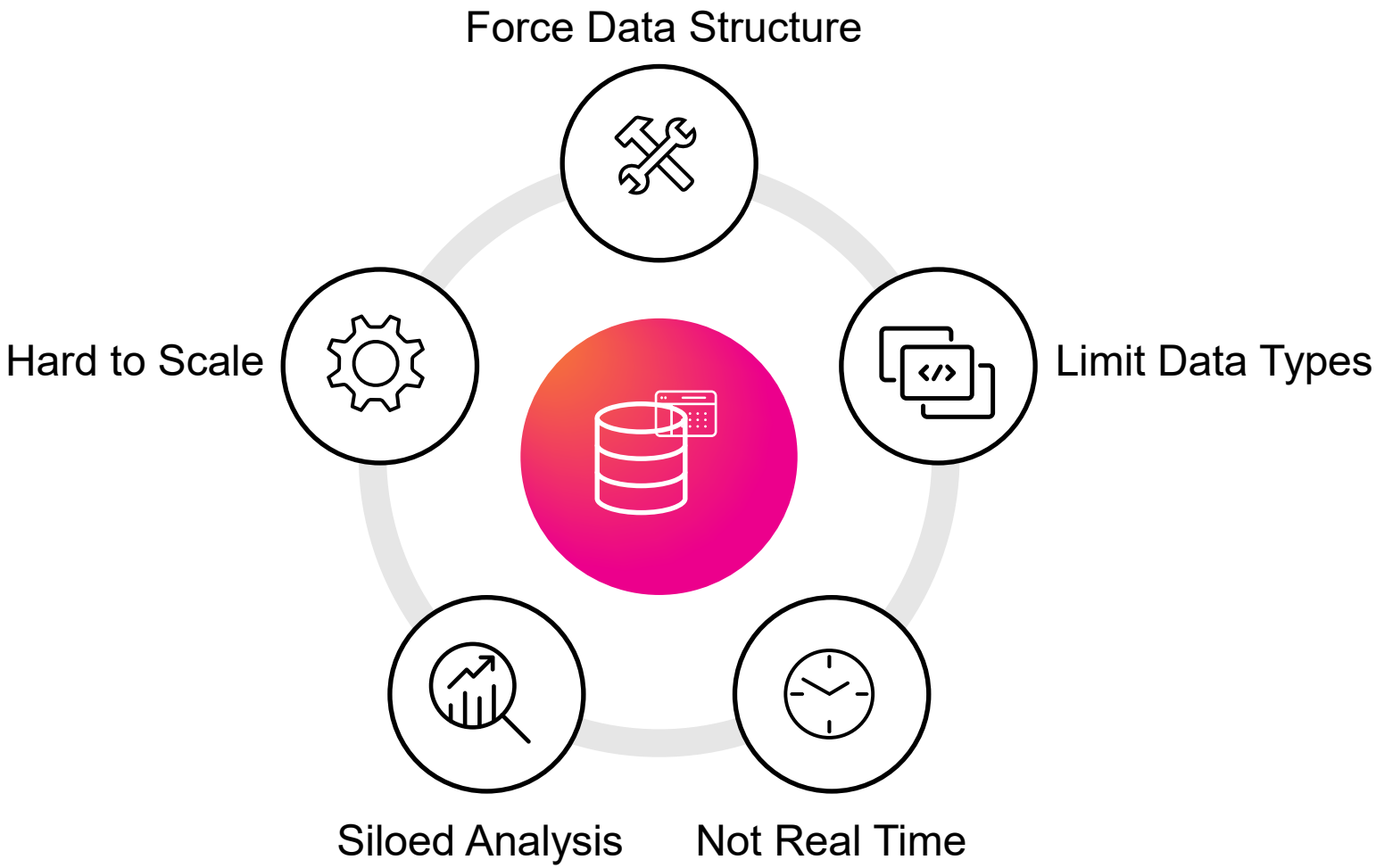
Most Organizations' Data is Still Dark Data

60% 기업은 자사가 보유한 데이터의 대부분이 여전히 다크 데이터라고 응답*

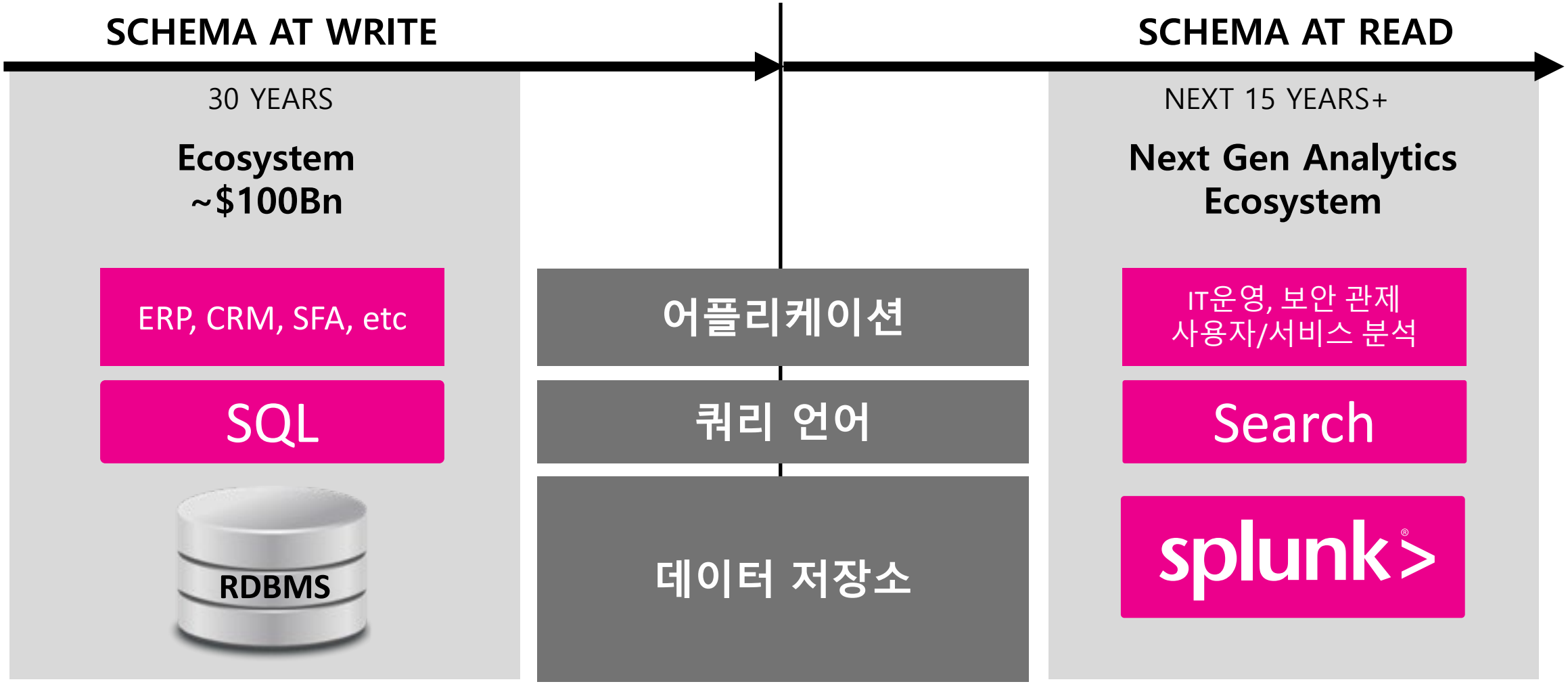


*Splunk Inc., "State of Dark Data Report", May 2019

전통적인 데이터 & 분석 솔루션으로는 더이상 문제를 해결할 수 없습니다.



머신데이터 분석 환경의 새로운 패러다임



splunk>

The Data-to-Everything Platform

IT

Security

IoT

Biz Analytics

splunk> turn data into doing

splunk>

turn data into doing™

"**머신데이터**를 아무런 **제약 없이** **수집>저장>분석>시각화** 할 수 있는 **실시간 분산** **플랫폼**"

머신데이터
(Machine Data)

- 서버/NW 로그
- 각종 설비 데이터
- 애플리케이션 로그
- 기타 **모든 텍스트 형태의 데이터**

제약 없음
(No Limits)

- 반정형/정형 데이터
- 데이터 **포맷 무관**
- 데이터 **용량 무관**
- 데이터 속도 무관
- 제약 없이 수용

엔드 투 엔드
(End-to-End)

- 별도의 외부 솔루션불필요
- 복잡한 코딩 및 SI 개발이 **필요 없음**
- 데이터의 생성부터 가치 획득까지 모두

실시간 및 분산
(Real-time)

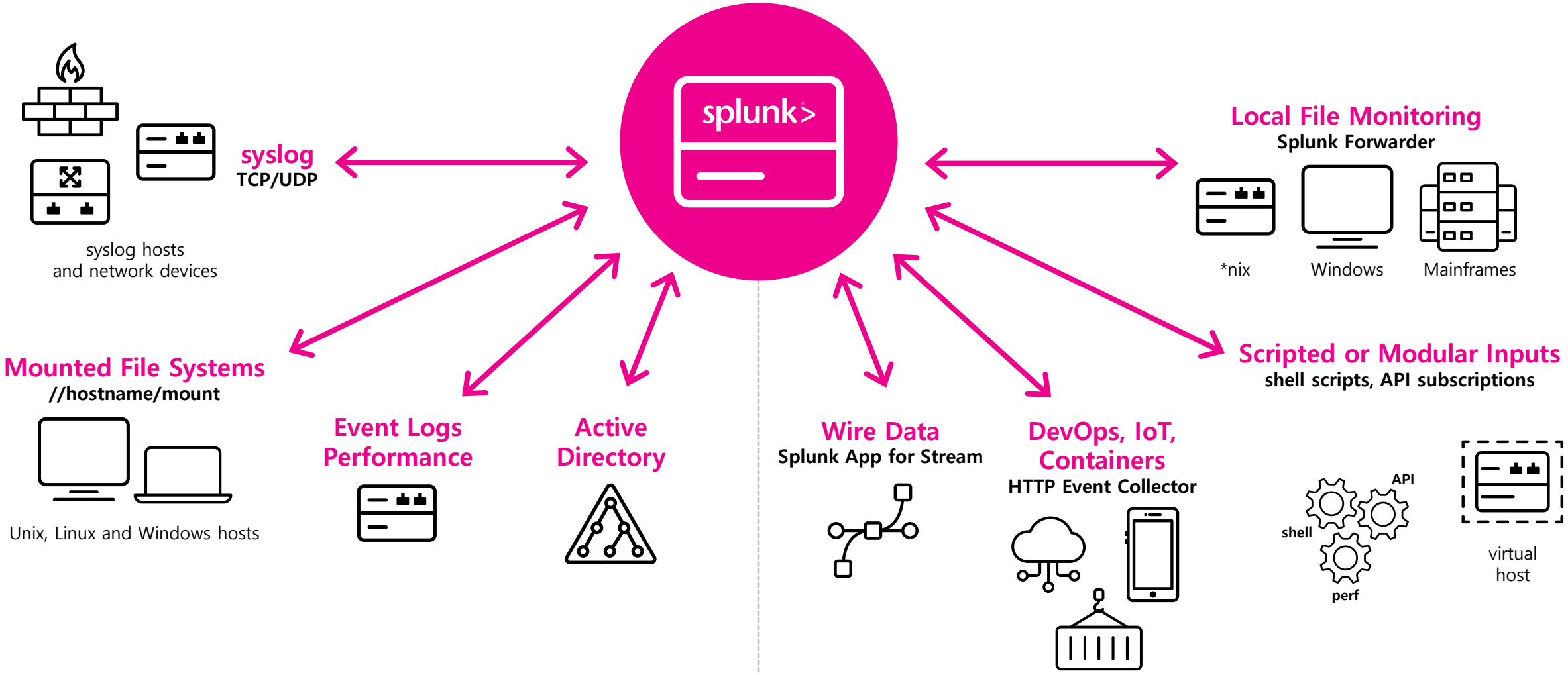
- 모든 데이터 **실시간** 처리, 즉시 결과 확인
- **분산 저장, 분산 검색**
- 성능 및 용량의 선형적 확장

플랫폼
(Platform)

- 커스터마이징 용이
- 외부 시스템과 손쉬운 연동
- **1900여 무료 앱**을 통한 기능 확장

1. 다양한 이기종 데이터 소스로부터 제약 없는 수집

에이전트/에이전트리스 방식 제공으로 유연성과 최적화된 수집 기능 제공



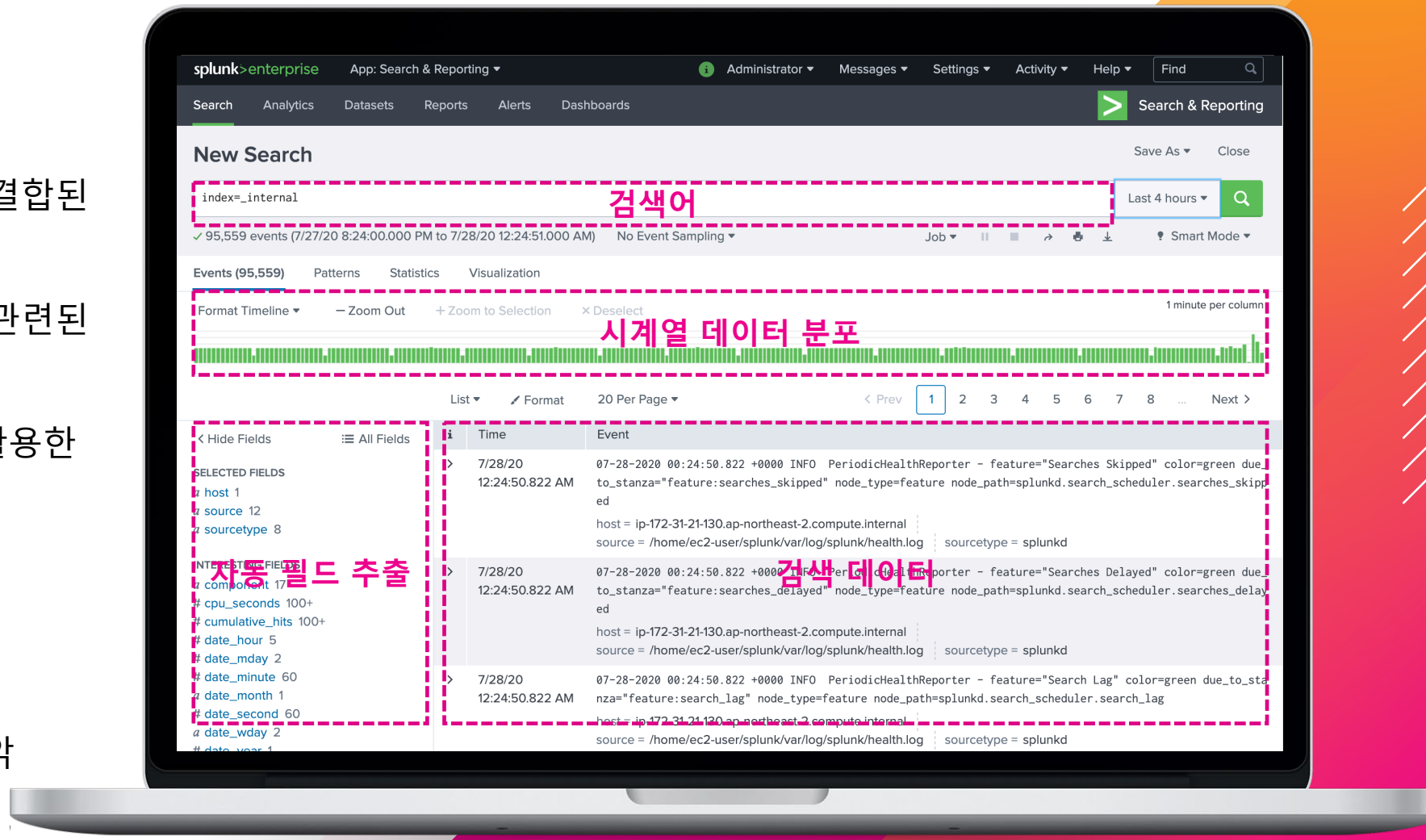
splunk> turn data into doing

2. 하루 수백 TB 수집까지 횡적 확장

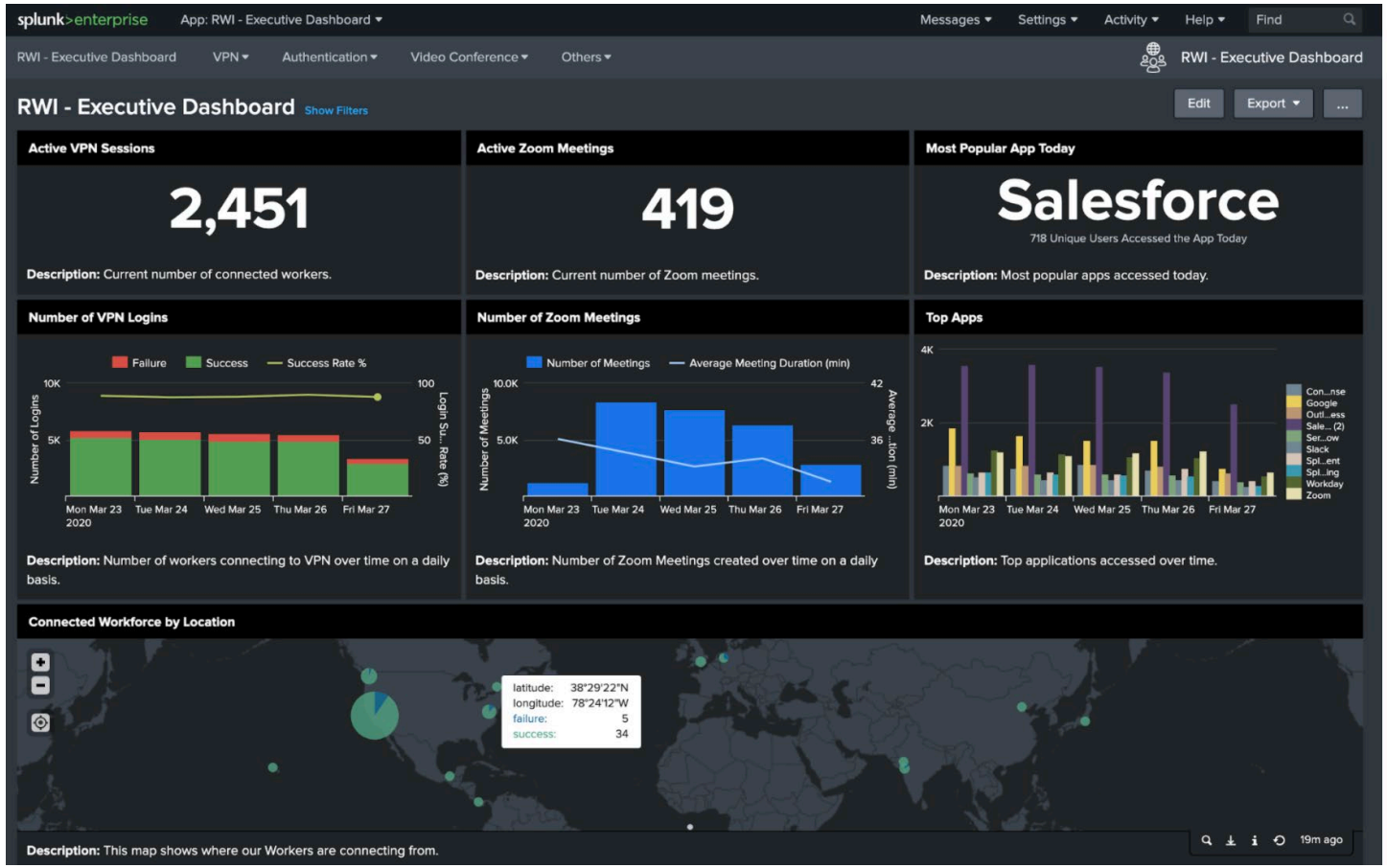
엔터프라이즈급 확장성, 장애 복구, 및 통합성 제공

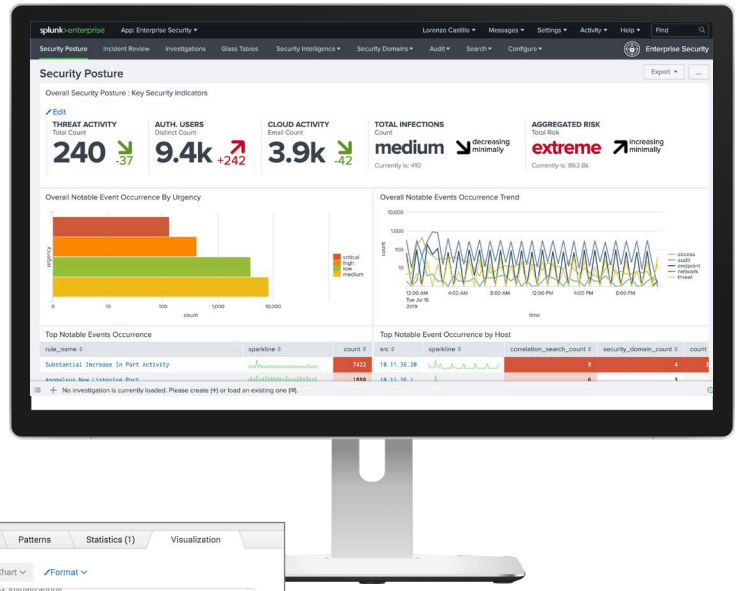
3. 강력한 검색 기능

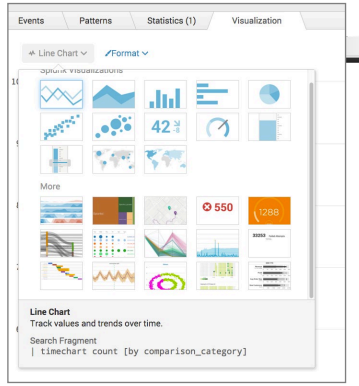
- SQL 과 Unix 파이프라인 구문이 결합된 최적의 검색 언어 SPL
- 검색, 상호 연관, 분석 및 시각화 관련된 140개 이상의 명령어
- 통계, 그래프, 각종 연산 함수를 활용한 분석
- 별도의 correlation key 설정 없이 상관관계 분석
- 신속하게 필요한 데이터를 찾아 분석하여 사고의 근본 원인을 파악



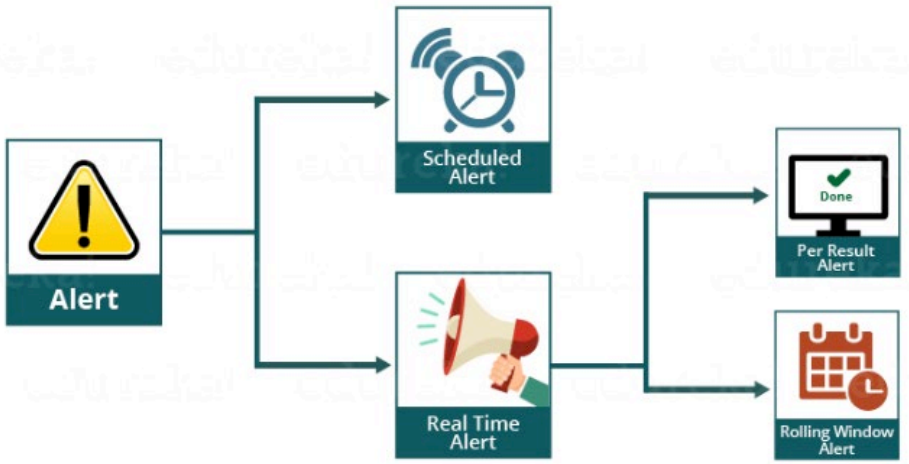
4. 내장 UI 컴포넌트를 활용한 쉽고 빠른 대시보드 제작



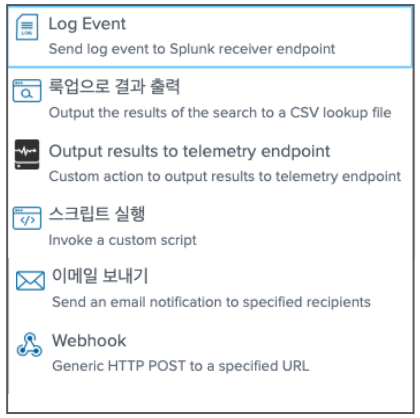




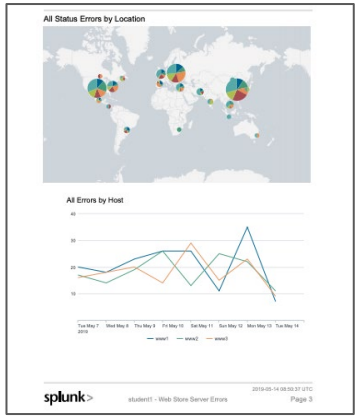
5. 실시간 감시 및 알람



경고 트리거 옵션



PDF 예약 전송



- 실시간 모니터링 및 알람 등록
- 검색 쿼리 저장 후 실시간/주기적인 실행을 통한 모니터링
- 자동 대응을 위한 각종 프로그램/스크립트 실행
- RSS, Email 통지 및 NMS/SNS 연동
- PDF 스케줄 전송 기능을 통한 보고서 이메일 발송

6. 다양한 App 생태계 및 커뮤니티

앱 생태계를 활용하여 최소의 리소스로 빠르게 요구사항을 구현

splunkbase.com **1900+** 개 이상의 다양한 앱

Answers.splunk.com **9만건**의 Q&A

전세계 **85**개 user groups

400 여개의 partners

World-wide

주요 고객사

클라우드 & 온라인 서비스

Google, SONIFI, Zillow, mindtouch, PEXA, Facebook, CONCUR, SurveyMonkey

교육

Penn State, Duke University, University of Exeter, Imperial College London, The George Washington University, Stanford University, USC University of Southern California, The University of Texas at Austin

에너지 & 공공

PG&E, TRANE, ENERNOC, ENGIE, TransAlta

금융 & 보험

Aflac, TransUnion, FINRA, Nasdaq, AAA, Japan Net Bank, NCCoE, PSCU, PROGRESSIVE

정부기관

헬스케어

Pfizer, imprivata, RECURSION, UCLA Health, myriad, CardinalHealth, OhioHealth, AstraZeneca

제조

BMW, ASICS, MBDA, Shaw Floors, BOSCH, P&G, JABIL, Northrop Grumman, YOKOGAWA

미디어 & 엔터테인먼트

Discovery Communications, ESPN, CenturyLink, UBISOFT

유통

amazon, Coca-Cola, GROUPON, REI co-op, zulily, 7-Eleven, TESCO

기술

Adobe, hp, Symantec, AUTODESK, rackspace, INTUIT, TiVO, leidos, Viasat

통신

COMCAST, Telstra, verizon, telenor, CISCO, yelp, vodafone

여행 & 운송

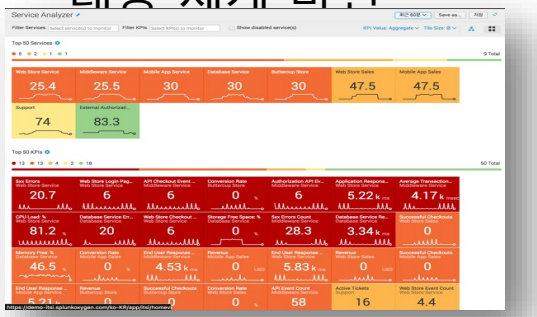
FedEx, lyft, eTravel, SNCF, Dubai Airports, Expedia, Carnival, MTR, HYATT

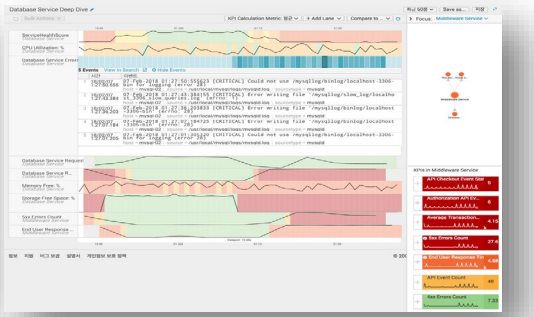
국내 A제조사

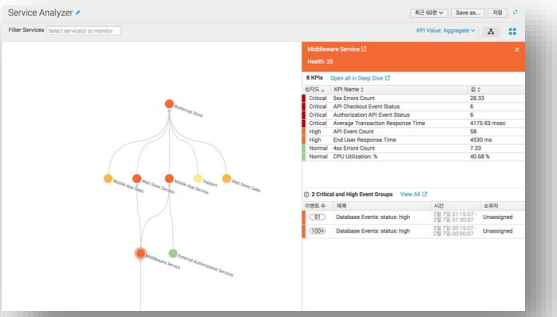
IT 통합 관제 시스템

Splunk Enterprise + ITSI

- Silo 상태의 장애 대응 환경을 **통합 관제 및 실시간 탐지, 분석 환경**으로 전환
- 전체 시스템 상태에 대한 **Single-View** 통합 대시보드 구축
- 핵심 리소스에 대한 통합 **실시간 관제** 환경 구현
- 서비스 및 KPI 기반 장애 영향도 및 상관 관계 분석 환경 구축
- Root-Cause 에 대한 빠른 대응 및 분석이 가능한 빅데이터 기반 실시간 대응 체계 마련







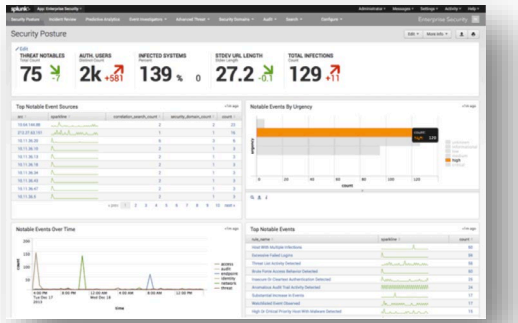
splunk> turn data into doing

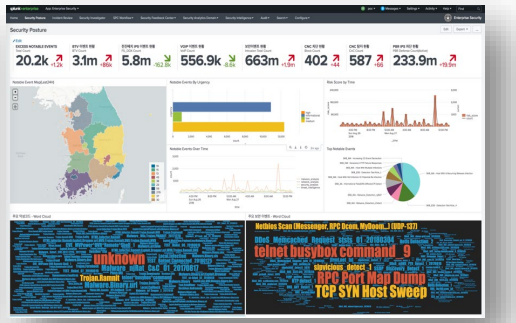
국내 B 은행

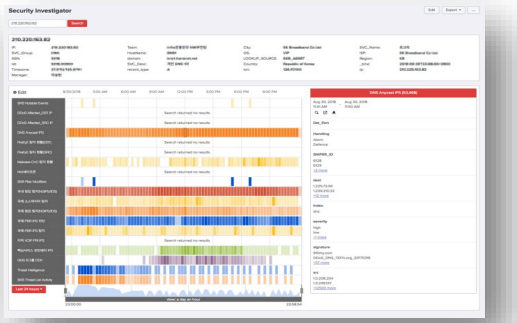
통합 보안 관제 시스템 (SIEM)

Splunk Enterprise + ES

- 보안 장비 로그 기반의 단순 패턴, 시그니처 중심 단기간 탐지에서 보안 로그 포함 모든 로그와 트래픽을 분석 가능한 **통합 보안 빅데이터 플랫폼** 확보
- **유연한** 아키텍처
- 보안 위협 인텔리전스 플랫폼으로 **위협 탐지 기능 강화**
- 이기종 데이터 **상관 관계 분석**으로 보안 관제 고도화







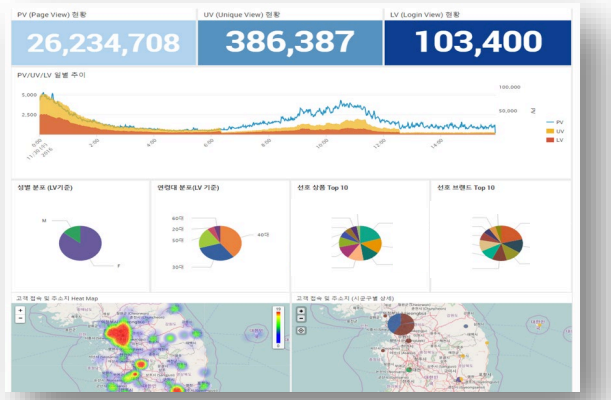
splunk> turn data into doing

국내 C
e커머스

빅데이터 분석 시스템

Splunk Enterprise

- 고객 접속 이력, 관심사 분석, 구매 내역 분석을 통한 **마케팅 전략** 수립
- 주문, 구매 전환율, 채널별 주문 현황 **실시간 파악**
- 분석 인프라 구축으로 데이터 활용성 증대 및 **실시간 분석** 역량 강화
- 광범위한 기업 내/외부 데이터 기반으로 **의사결정 정확도 향상**
- 객관적인 **지표를 의사 결정에 활용**



splunk> turn data into doing

Thank You

splunk> turn data into doing™