Splunk 소개

빅데이터 머신 데이터 플랫폼

Splunk Korea / 2019
May 2019 | Version 1.0

목차

Splunk 회사 소개

회 사

- 글로벌 HQs:
  - 샌프란시스코(AMER)
  - 런던(EMEA)
  - 홍콩(APAC)
- 직수 전세계 4,500+명
- 연 매출 약 1조2천억원 ($950YoY +42%)
- 나스닥 상장 : SPLK

제 품

- 무료 버전에서 시작, 대규모 분산 확장
- 스플렁크 제품:
  - Splunk Enterprise
  - Splunk Cloud
  - Premium Solutions
    - Enterprise Security
    - IT Service Intelligence
    - UBA
  - Phantom, VictorOps

고 객

- 고객사(전체): 16,000+
- 고객사(한국): 400+
- 국가기준: 110개국+
- 중소기업, 대기업 그룹 계열사
- 포춘 100대 기업: 89+
- 최대 라이센스:
  10+ PB/일

머신 데이터란?

어플리케이션 데이터
모바일 앱 & 웹사이트 데이터
*일일 평균 3시간 모바일 앱 사용**

IT 인프라 데이터
네트워크 서버 & 클라우드 서비스
*데이터 센터의 다운타임으로 인한 손실은 평균 시간당 $300,000**

보안 데이터
방화벽 데이터 & 엔드포인트 보안 솔루션 데이터
*2021년에 이르면 사이버 범죄로 인한 손실 비용이 연간 $6 조에 이를 것으로 예상**

고객 생성 데이터
소셜 미디어 데이터 & 콜 로그
*전세계적으로 28 억 건의 소셜 미디어 데이터 존재**

IoT 데이터
온도 제어 & 속도 측정 장치
*2017년 기준으로 장치(Thing)에서 발생하는 84 억 건의 데이터가 존재**

splunk> listen to your data

머신데이터를 사업적 가치로 전환

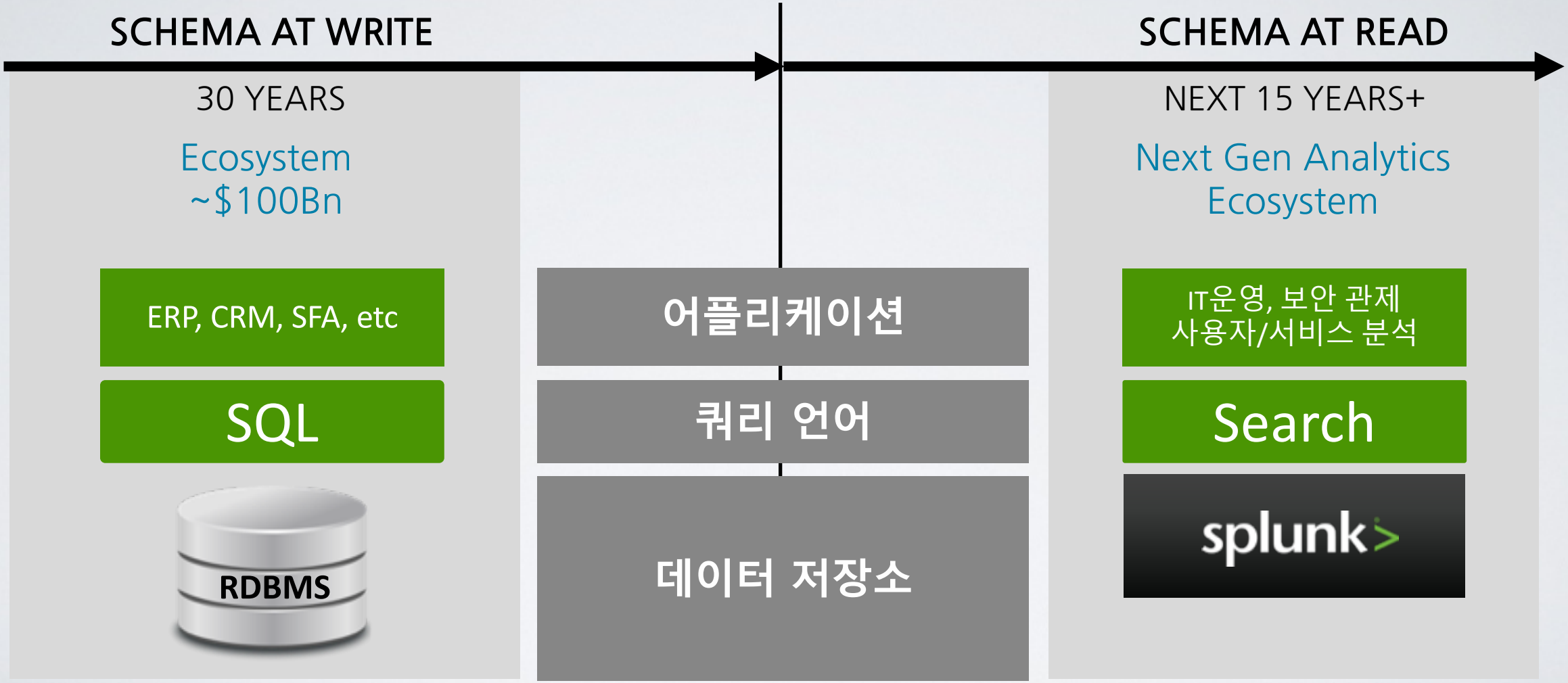
원시 데이터 그대로 수집 : 위치, 형태, 규모에 상관 없이!

splunk>

어떠한 질문도 OK!

- 어플리케이션 개발
- IT 운영
- 보안, 규정 준수, 사기 방지
- 비지니스 분석
- 산업 데이터 및 사물 인터넷(IoT)

머신데이터 분석 환경의 새로운 패러다임



Database 중심의 분석 프로젝트 Pain-points

Human Generated Data
SNS data Like Twitter >

Machine Generated Data
CDR >
Packets >
Sensor data >
Security data >
Log files >
Server Status >
Virtualization Mgmt >
Application Monitoring >
Web Logs >
Transaction Data >
Scripts >
Metrics >
Configuration Data >

?

Custom Adapters

3rd Party
IT
MES
ERP
Database

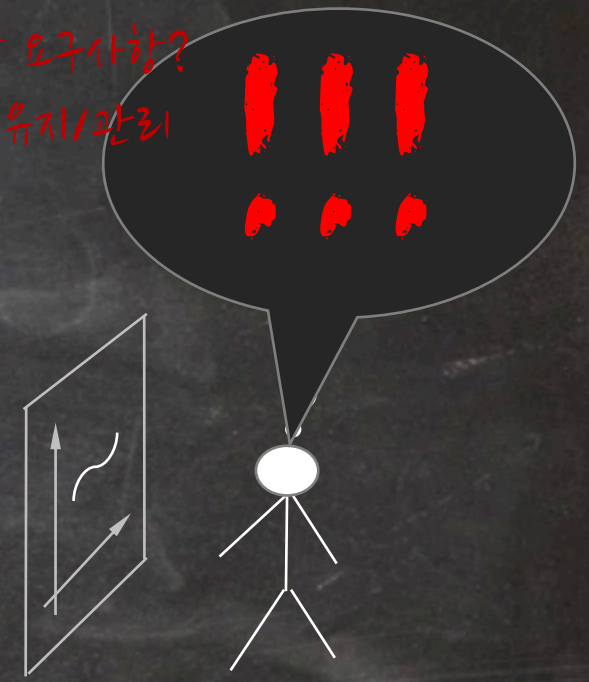
E.T.L
DB

Schema

Database
DW / DM

BI solutions

- 어댑터를 만들고 유지하기 어렵다
- E.T.L과 스키마 디자인
- end-to-end 실시간 요구사항?
- 대용량 데이터베이스 유지/관리
- summarization
- NOT AGILE!



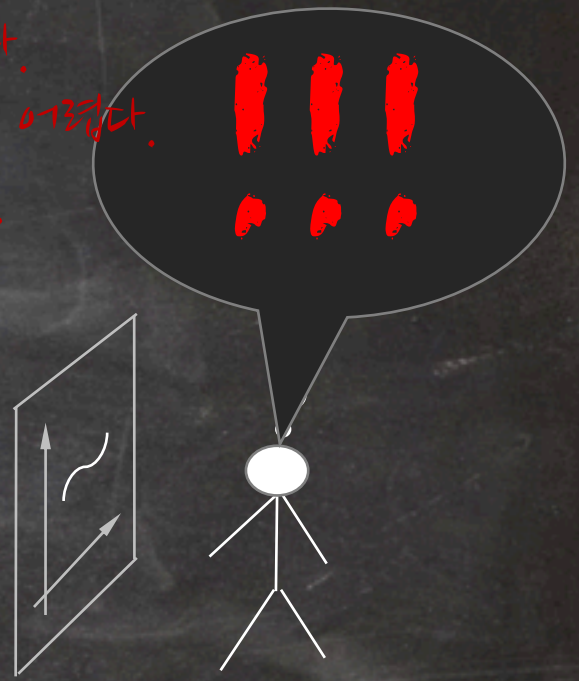
하둡 프로젝트의 pain-points

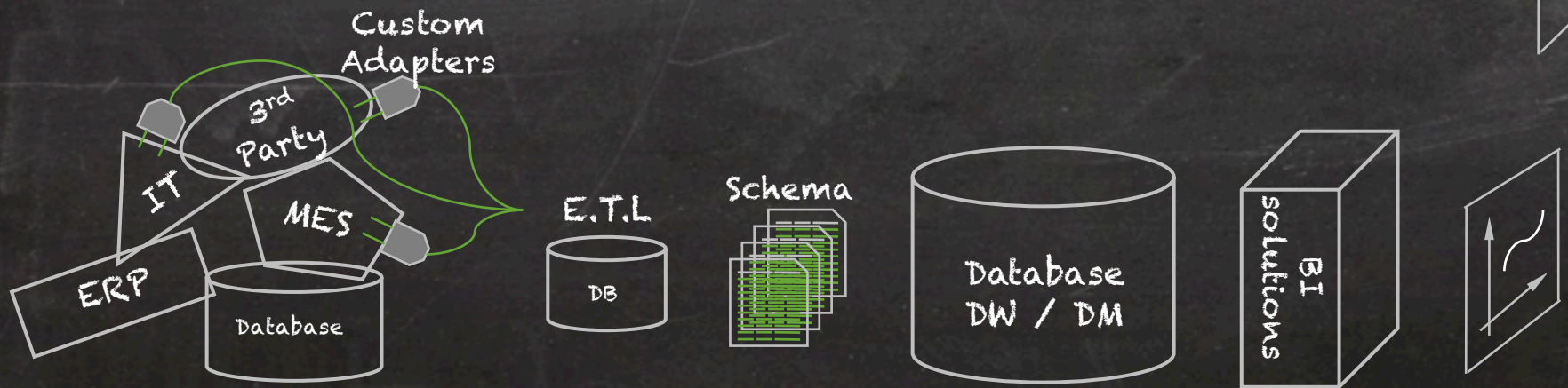
Human Generated Data
SNS data like Twitter >

Machine Generated Data
CDR >
Packets >
Sensor data >
Security data >
Log files >
Server Status >
Virtualization Mgmt >
Application Monitoring >
Web Logs >
Transaction Data >
Scripts >
Metrics >
Configuration Data >

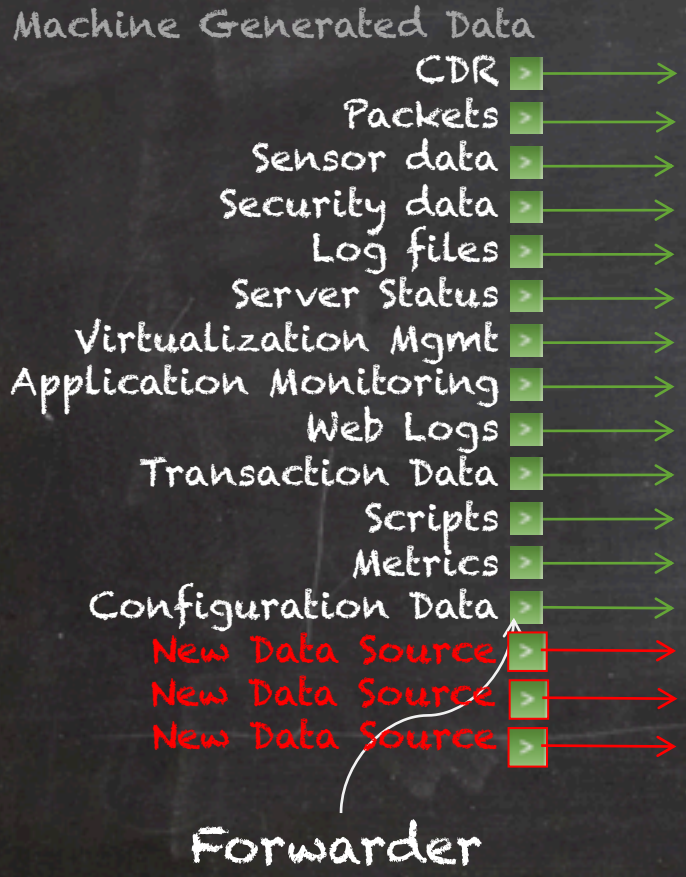
Zookeeper
Mahout
Snappy
Whirr
HBase
Oozie
Hive, Pig
Hadoop
Sqoop
Flume
HDFS
Map Reduce

- 조금만 바뀌어도 새로운 모듈 개발 프로젝트
- 관리할 컴포넌트가 너무 많다.
- 전문가를 구하기 어렵다.
- 실시간 운영사항 수동이 어렵다.
- 장애 대처가 어렵다.
- NOT AGILE!



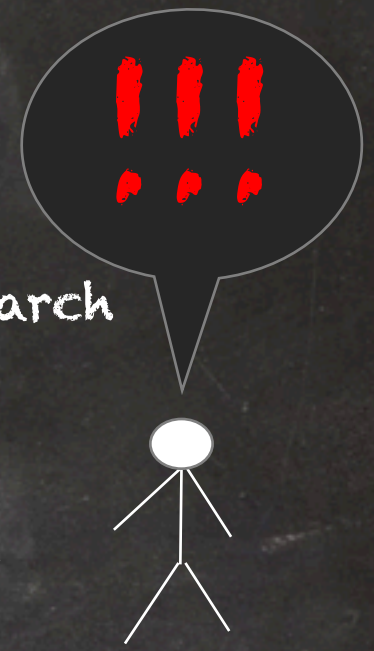


SPLUNK 는 다릅니다



splunk>

- ~~Adaptor?~~
- ~~E.T.L?~~
- ~~DB Schema?~~
- ~~DB Mgmt?~~
- ~~Limit?~~



splunk> = 머신데이터 플랫폼

"**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)

- 비정형/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

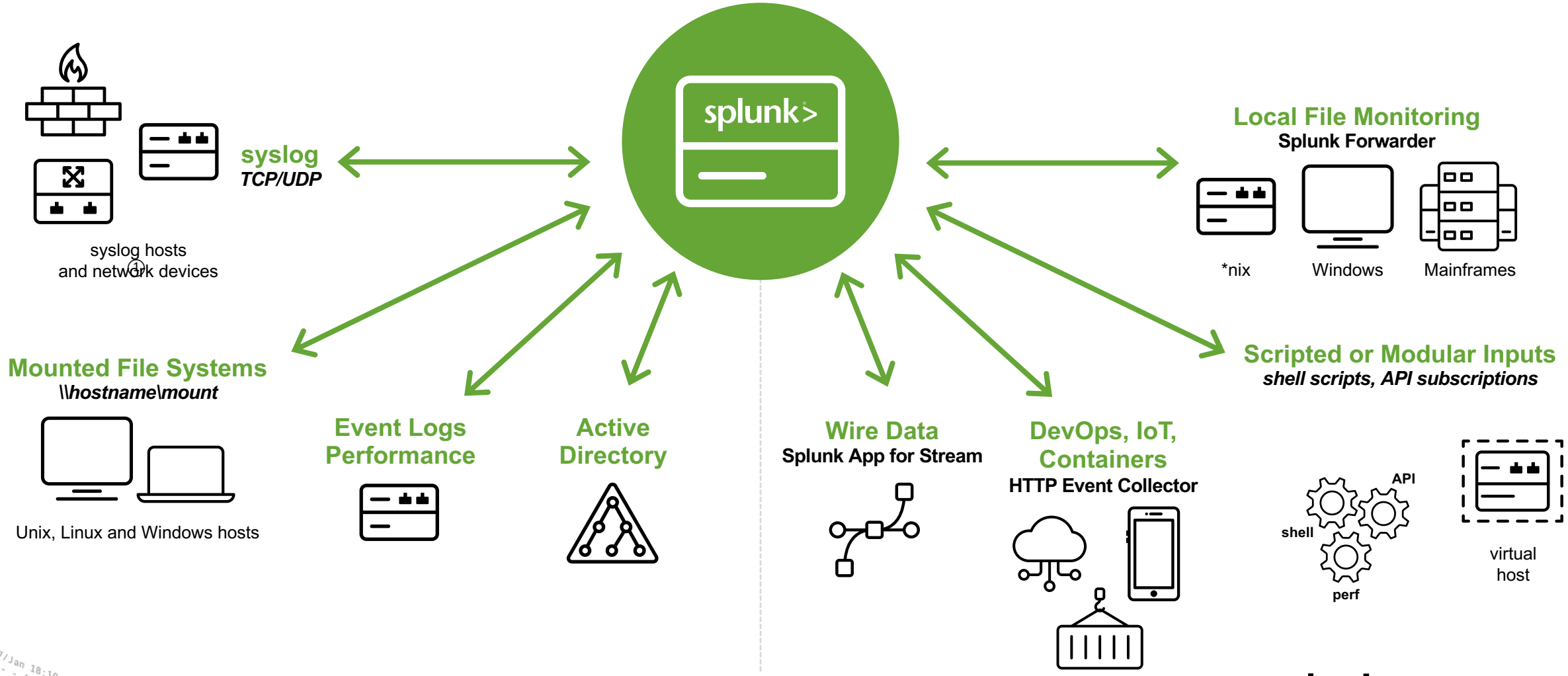
플랫폼
(Platform)

- 커스터마이징 용이
- 외부 시스템과 손쉬운 연동
- **1500여 무료 앱**을 통한 기능 확장
- 개발 프레임워크

목차

1. 다양한 이기종 데이터 소스로부터 제약 없는 수집

에이전트/에이전트리스 방식 제공으로 유연성과 최적화된 수집 기능 제공

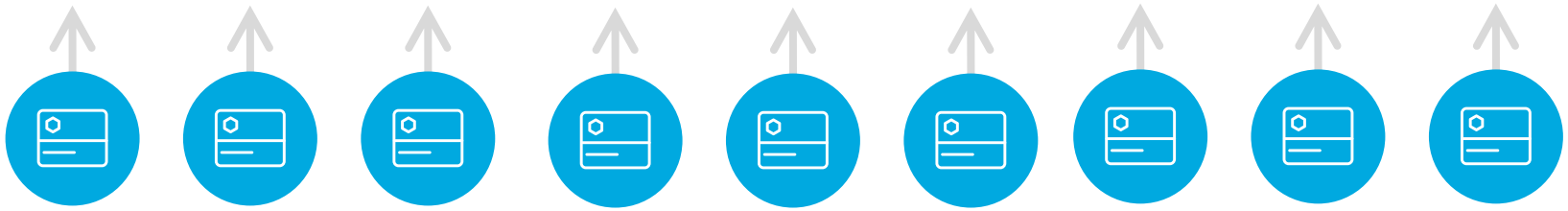


splunk> listen to your data®

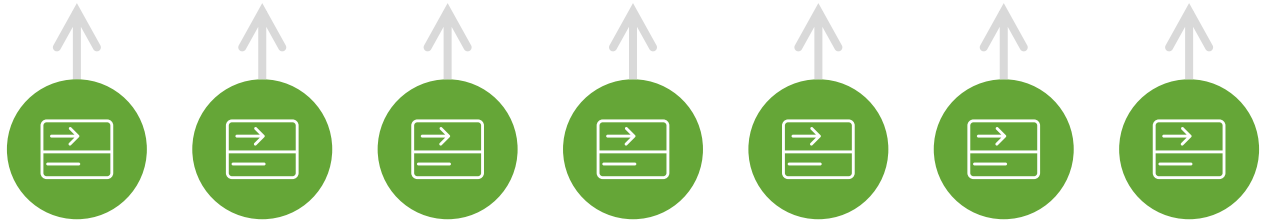
2. 하루 수백 TB 수집까지 횡적 확장

엔터프라이즈급 확장성, 장애 복구, 및 통합성 제공

Search head로 검색 워크로드 오프로딩



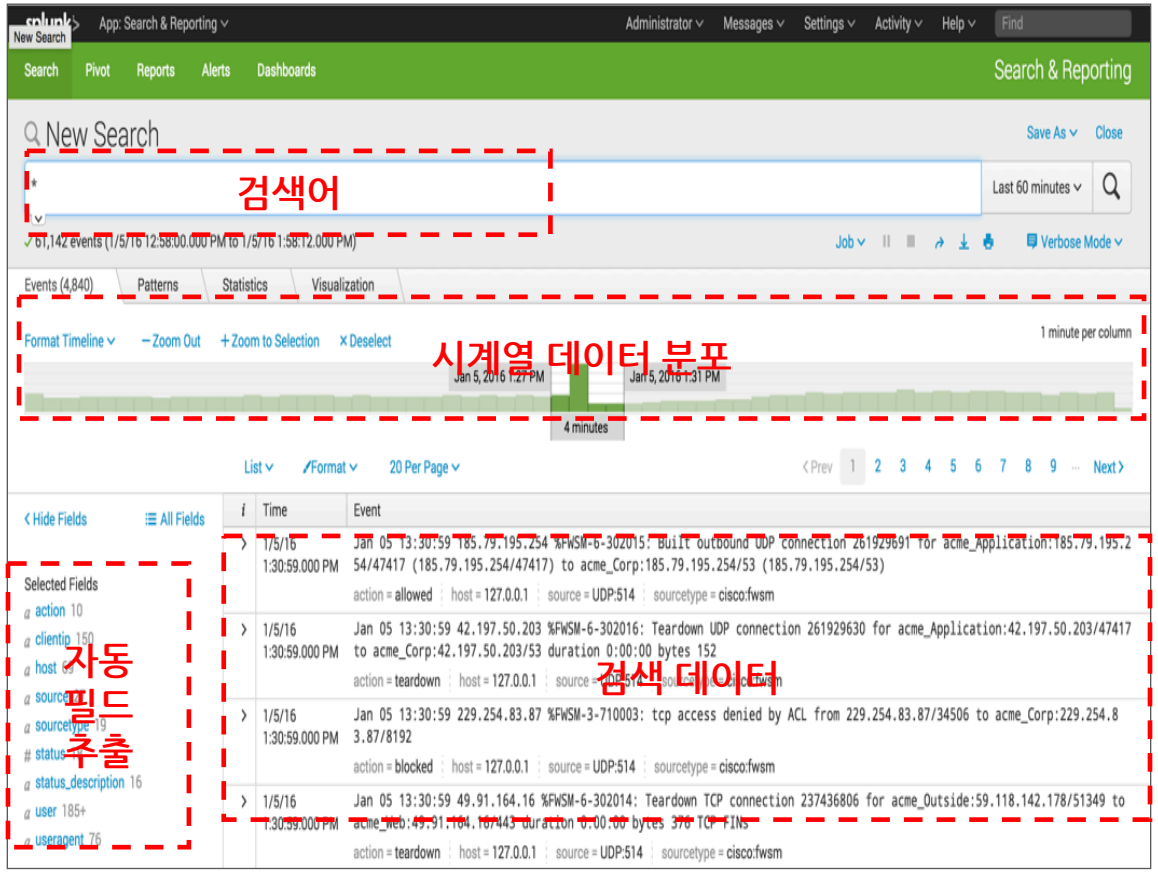
Splunk Indexer 들로 자동 부하분산하여 균등하게 데이터 압축 저장



Splunk Forwarder 를 통해 수천대 서버에서 데이터를 전송

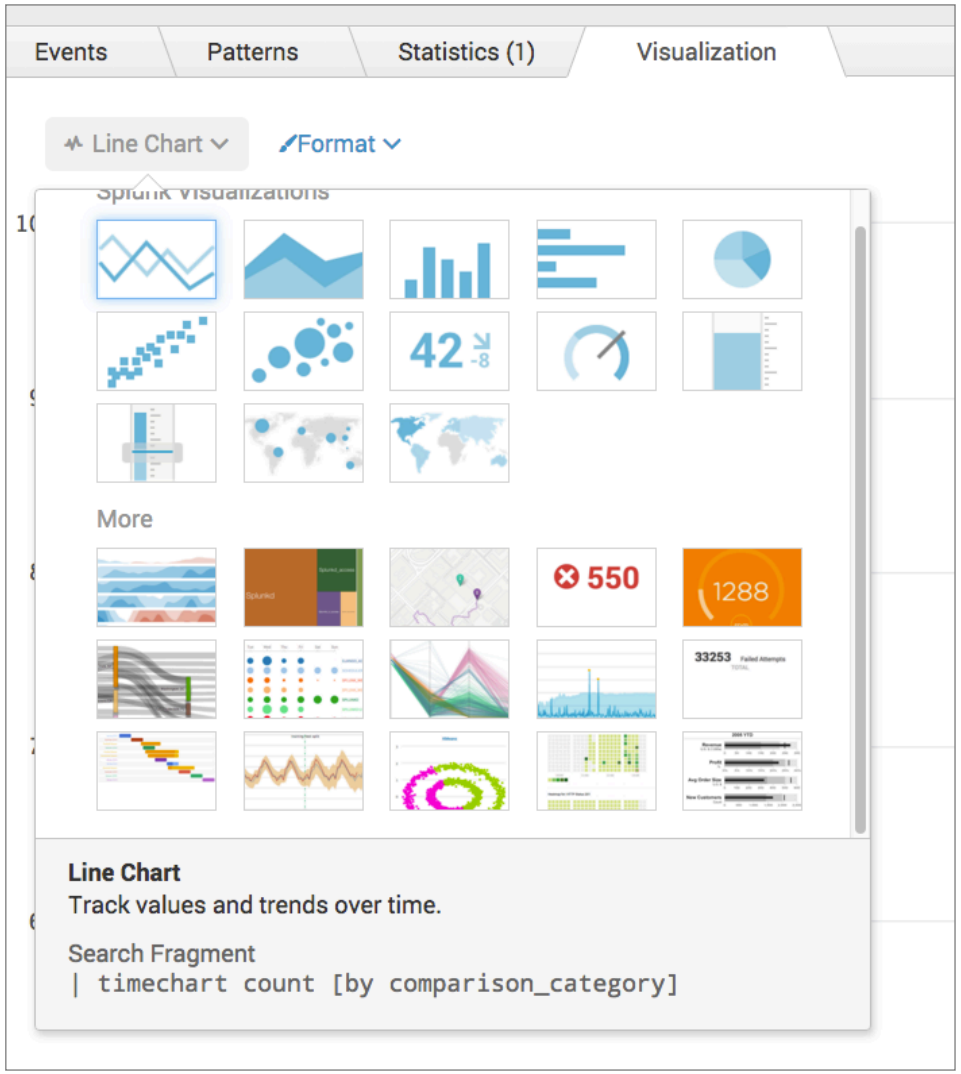
3. 강력한 검색 기능

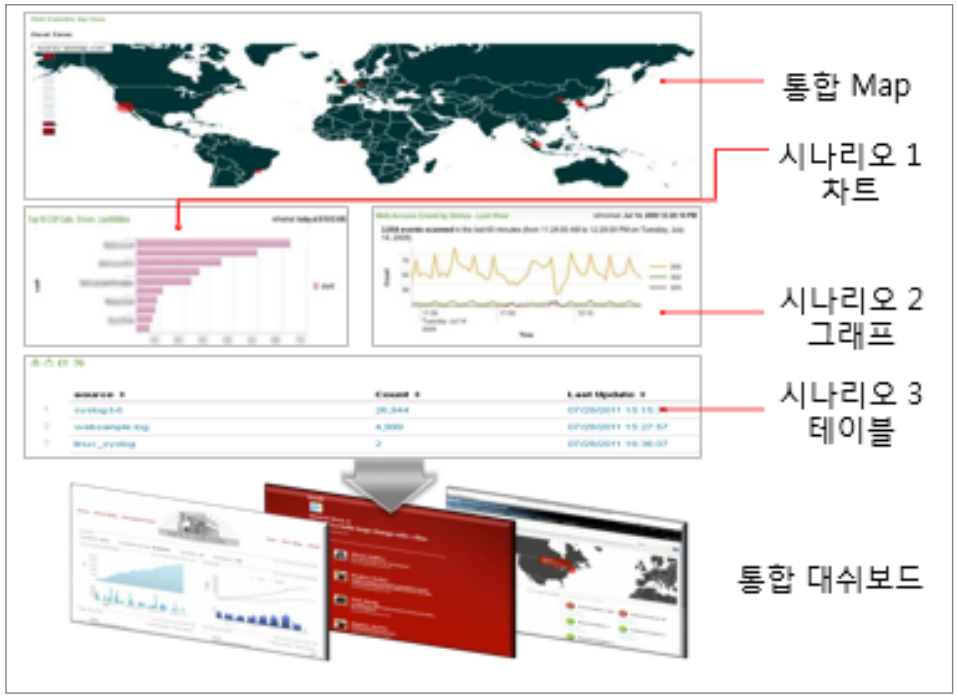
머신 데이터 검색에 최적화된 Splunk 자체 검색 언어인 SPL을 활용한 검색



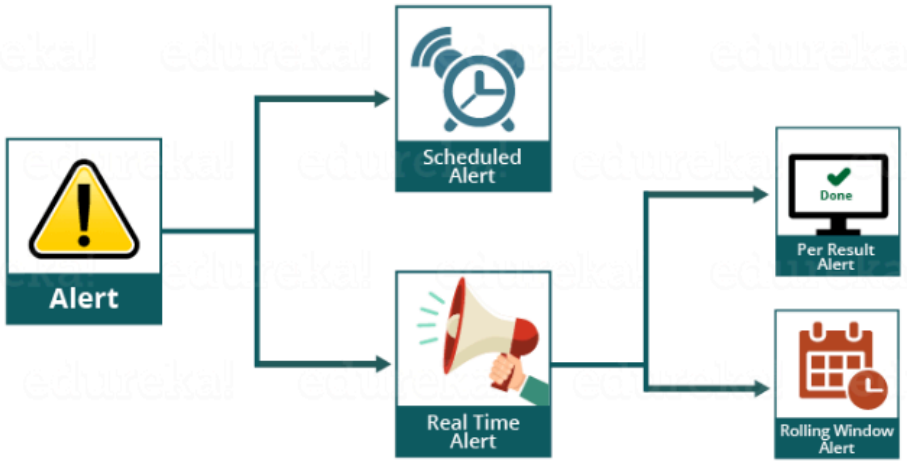
- SQL 기능과 Unix 파이프라인 구문이 결합된 최적의 검색 언어인 SPL 지원
- 검색, 상호 연관, 분석 및 시각화 관련된 140개 이상의 명령어 제공
- 통계, 그래프, 각종 연산 함수를 활용한 분석
- 별도의 correlation key 설정 없이 상관관계 분석 가능
- 신속하게 필요한 데이터를 찾아 분석하여 사고의 근본 원인을 파악

4. 내장 UI 컴포넌트를 활용한 쉽고 빠른 대시보드 제작

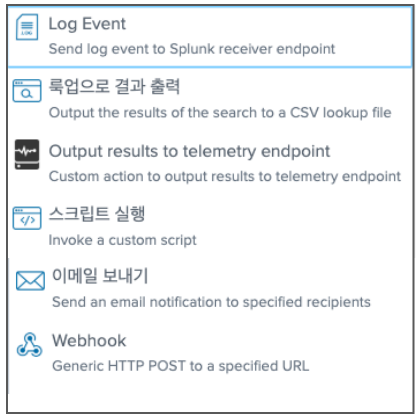




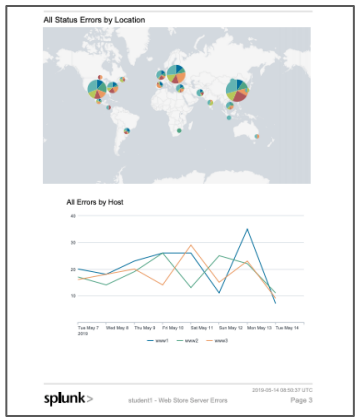
5. 실시간 감시 및 알람



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 실행가능
- RSS, Email 통지 및 NMS/SNS 연동 가능
- PDF 스케줄 전송 기능을 통한 보고서 이메일 발송

6. 다양한 App 생태계 및 커뮤니티

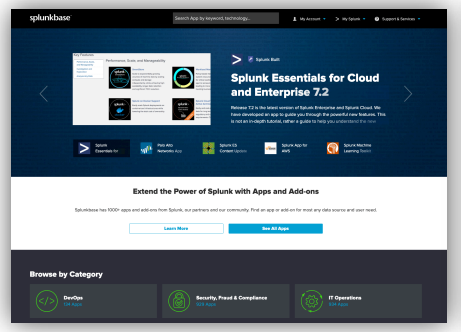
앱 생태계를 활용하여 최소의 리소스로 빠르게 요구사항을 구현

1500+이상의 다양한 앱 생태계

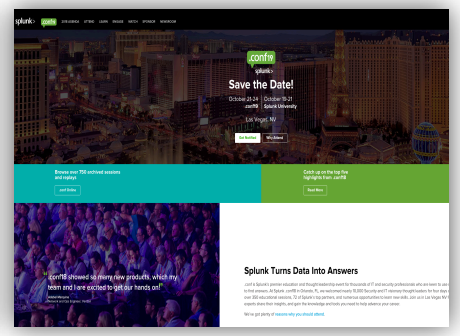
Weather	BigFix	Sendmail	PDF Report Server	F5	Radio Stations	WebSphere	XenDesktop NetScaler	Multicast	MS Exchange
Ruby on Rails	Google Maps	Whois lookup	PCI Compliance	Puppet Conf. Mgt	Python Mail	NetFlow	Audible Alerts	Stock Quote	FISMA Monitoring
Twitter	Windows	Nagios	Unix and Linux	Sourcefire	Splunk Monitoring	SNORT	FireEye Malware	POST/GET Rqsts	Citrix NetScaler
Security	Javamail	BlueCoat ProxySG	Solera DeepSee	IMAP	YouTube	Encrypt/Decrypt	Enterprise Security	AS/400 - iSeries	Transaction Profiling
Security	SCOM	TCP/UDP Sending	IronPort WSA	RSS Input	JMS receiver	Geo Location	VMware	Fin. Inf. eXchange	Splunk Mobile

splunk>enterprise

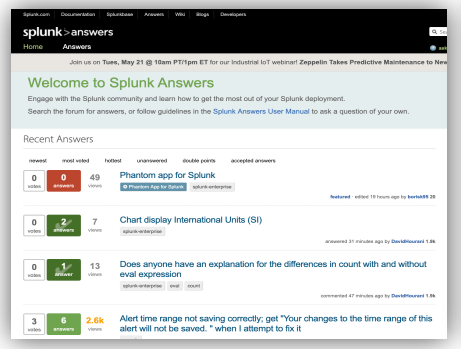
splunkbase.splunk.com



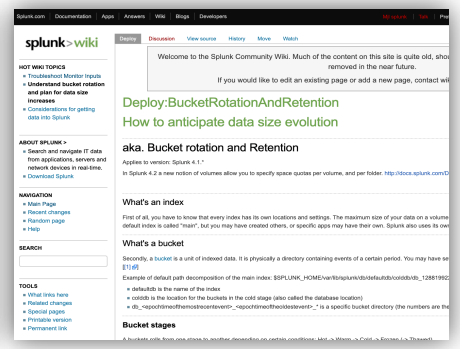
conf.splunk.com



answers.splunk.com



wiki.splunk.com



splunk> listen to your data®

목차

국내 Splunk 고객사

400여 국내 고객사들이 IT운영, 보안, OT등 다양한 분야에서 활용

고객명	내역	고객명	내역	고객명	내역	고객명	내역
삼성전자 모바일	Samsung Account 갤럭시 펌웨어 관제 모니터링	삼성전자 반도체	실시간 반도체 제조공정 모니터링/분석 시스템 IT 운영관제, 보안(내부자 통제)	신한은행	이상징후탐지시스템 모바일 거래분석 시스템	신한금융지주/신한생명/신한금투	이상징후탐지시스템(개인정보 유출방지) 시스템
삼성전자 VD	빌드로그 분석, devops	LG전자	SmartData팀 마케팅분석 전사보안관제	하나은행	FDS 시스템, 통합보안관제 시스템 - 금감원 선정 가장 FDS구축이 잘 된 기관 선정	동양증권	통합보안관제 시스템, FDS, 업무 분석 시스템
삼성전자 R&D	Devops, CI/CD 모니터링	현대기아차	전사SIEM	외환은행	FDS 시스템	현대카드	통합보안관제 시스템, 콜센터 분석 시스템
삼성화재	애니카 다이렉트 사용자 패턴 분석 시스템	SKT	통신망 통합품질관리시스템 IT보안관제 네트워크 보안관제	제일은행	로그통합 , SIEM,FDS 프로젝트	한화증권	통합보안관제 시스템, FDS
삼성전기	제조센서데이터 수율 분석	KT	uCloud 운영관제 네트워크 보안관제 내부자통제	대신증권	FDS, 업무 관제, 내부정보 유출방지 시스템	KB증권	서비스 통합 관제 시스템
삼성카드	보안로그 분석 시스템	LGU+	전자결제시스템관제모니터링	현대해상	로그기반 보안 관제 시스템	증권 예탁 결제원	Safe Plus 데이터 분석 시스템
삼성증권	이상징후탐지시스템(FDS)	KTnet	전자무역시스템 통합OP센터	NH 농협은행	차세대 보안관제 시스템(SIEM)	우리은행, IBK	FDS 시스템
호텔신라	내부자통제	SK브로드밴드	ISP 보안관제 , IPTV 품질 분석 모니터링	금융결제원	IT운영관제 시스템	금융보안원	차세대 보안 관제 시스템(SIEM)
롯데	보안관제	Nexon	게임사기행위탐지	롯데홈쇼핑	CallCenter 통합고객분석	우리은행	차세대 보안 관제 시스템(SIEM)
NS홈쇼핑	콜센터분석	NCsoft	보안관제	CJMall	서비스모니터링, 실시간마케팅분석	KB증권	서비스 통합 관제 시스템

감사합니다