

New IT Data World for You...

splunk[®] > *Operational Intelligence*

August, 2012

V Hankuk *valence* (주)한국밸런스

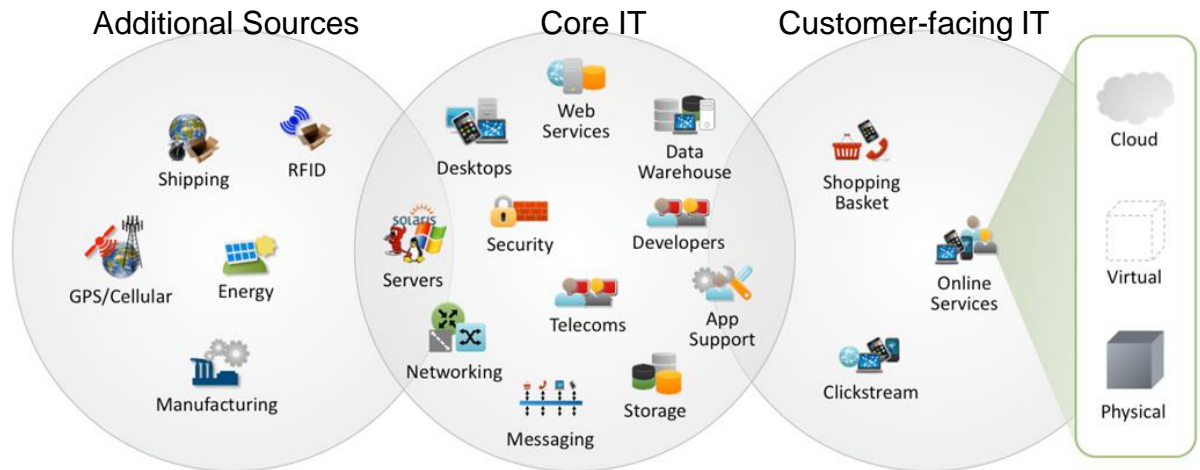
현 IT의 문제점?

IT의 현실

IT에 대한 대부분의 비용은 현재 IT를 유지하는데 지불되며, 다양한 IT 인프라에서 발생하는 여러 data가 급증하고 복잡해짐에 따라 이를 적절하게 활용하거나 이용하고 있지 못하고 있습니다.

Gartner®

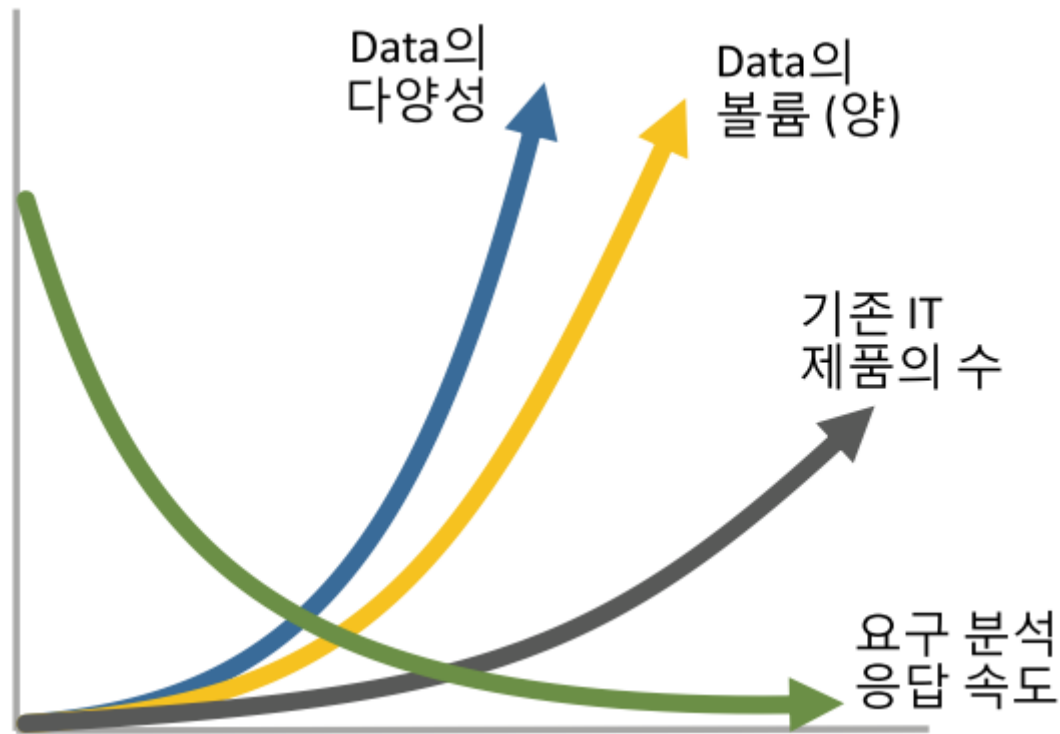
“약 70%의 IT 비용이 Business를 성장시키거나 개선시키기보다 유지하는데 사용된다.”



- ▶ IT 데이터의 양과 종류의 폭발적 증가
- ▶ 80~95%의 데이터가 비구조적 (unstructured)
- ▶ 저장 되더라도, 대부분 특정 영역에만 존재함
- ▶ 새로운 기술로 인한 복잡성의 증대 (가상화, 클라우드, Web 2.0, Mobility, SOA)
- ▶ 최근의 비즈니스 경향(e.g. always-on business)으로 인한 IT 데이터 가치의 비약적 증대

IT Data의 성장 추이 및 전망

향후 Data는 그 양과 다양성에서 급증할 것이나 이를 활용하기 위한 분석 및 응답 속도는 현저히 떨어질 것으로 전망됩니다.



“2009년과 2020년도 사이 디지털 데이터의 규모는 XX배로 증가”

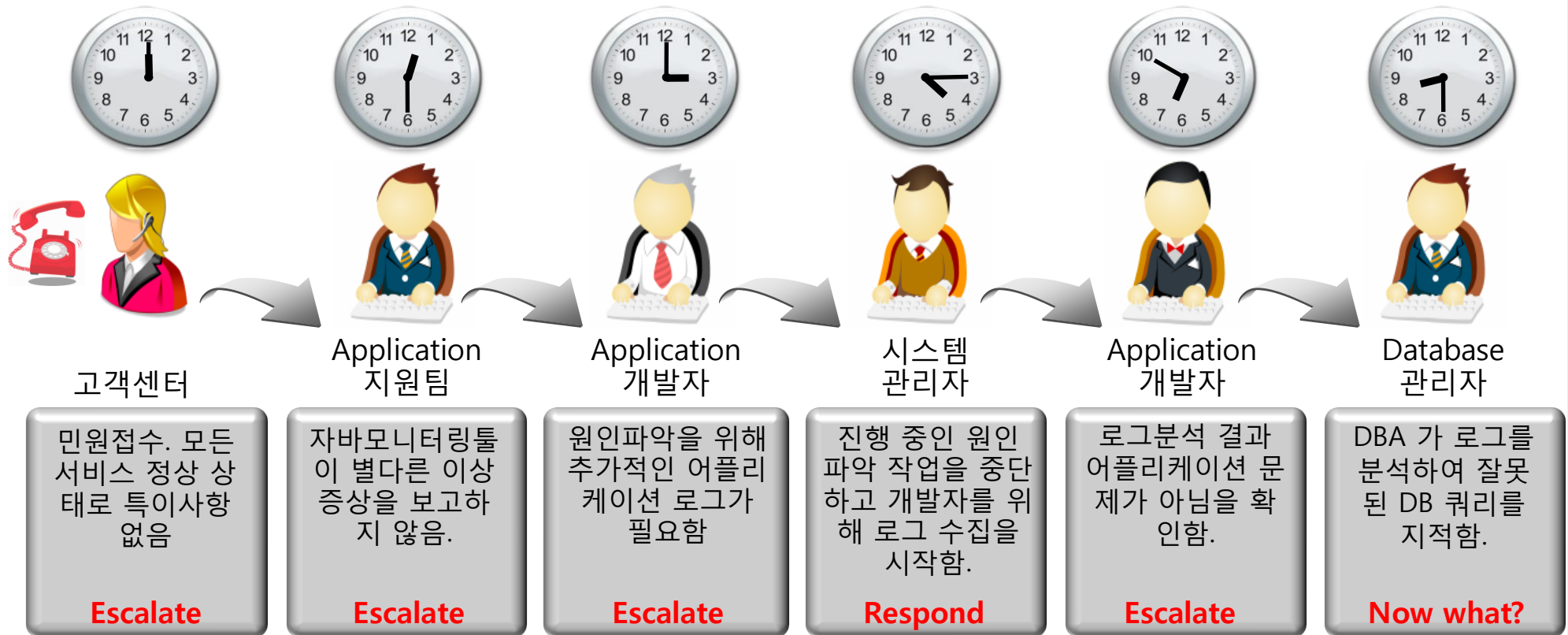
[IDC 2010 Storage Market View](#)

“비정량 IT 데이터만의 순수 증가가 90%의 전체 디지털 데이터 시장”

[IDC 2011 Digital Universe Study :
Extracting Value from Chaos](#)

IT 관련 민원 대응

각 업무별 담당자가 전문화되어 있어 해당 업무의 전문성은 높아졌으나 부서간, 업무간 상호 협조가 원활하지 않아 민원 등에 대한 업무 처리 효율성이 떨어지고 종합적인 판단에서부터 대응까지의 시간이 늘어나고 있습니다.



비즈니스(CxO) 요구사항에 대한 IT 대응

비즈니스 측면에서는 지속적으로 다양하고 신속한 정보를 요구하고 있으나 현 IT에서 이를 지원하는데 많은 한계가 존재합니다.



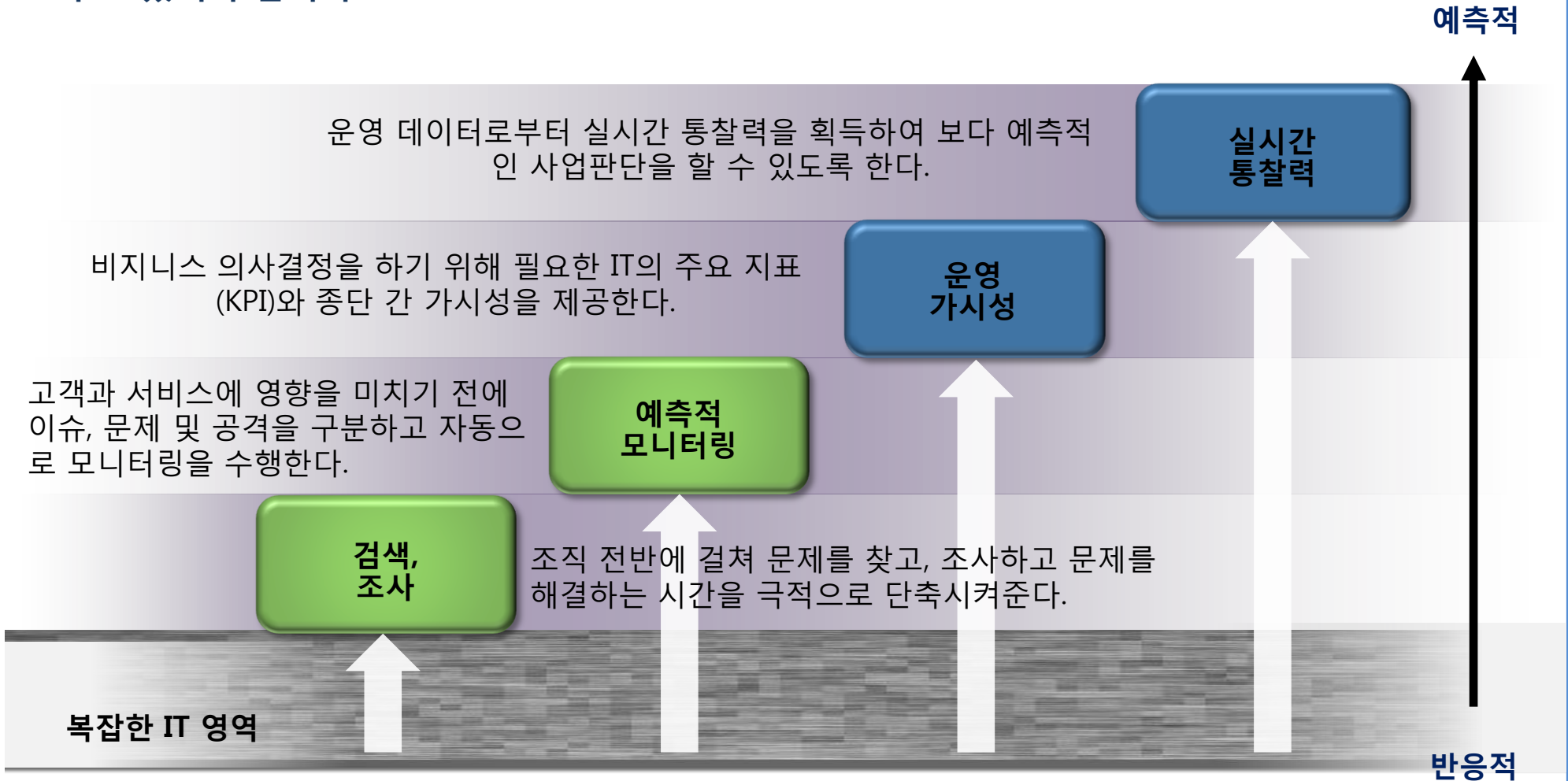
앞선 문제들을 해결하기 위해...

여러 다양한 시스템(Machine)들이 생성한 IT 데이터를 수집하고 Indexing하여 문제/위험은 물론 기회까지 식별한 후, IT는 물론 비즈니스에 대한 보다 직관적이고 신속한 통찰력을 제공해야 한다.

이러한 **Operational Intelligence(OI)**가 필수.

Operational Intelligence가 갖춰야 할 조건/기능

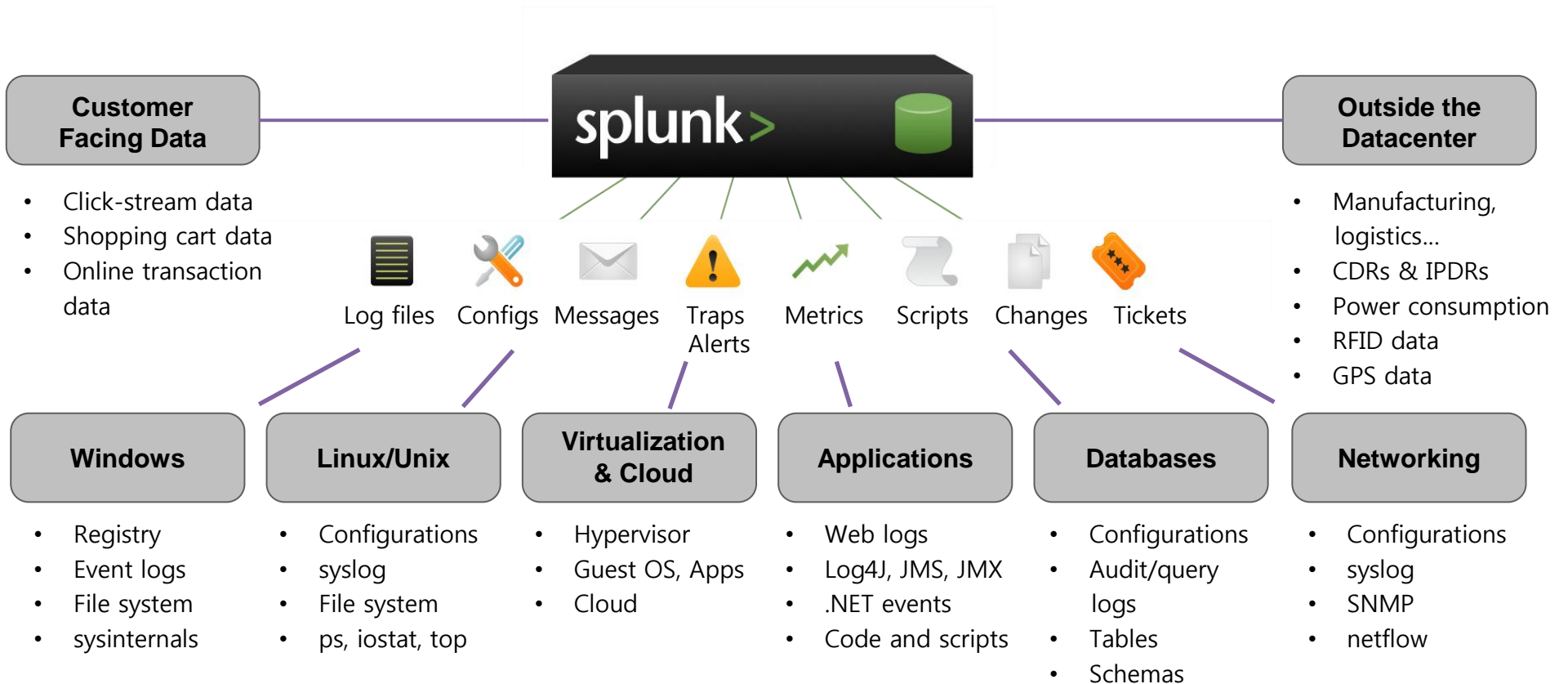
앞선 문제해결을 위한 Operational Intelligence가 되기 위해서는 아래의 4가지 조건/기능을 갖추고 있어야 합니다.



SPLUNK는 어떤 솔루션?

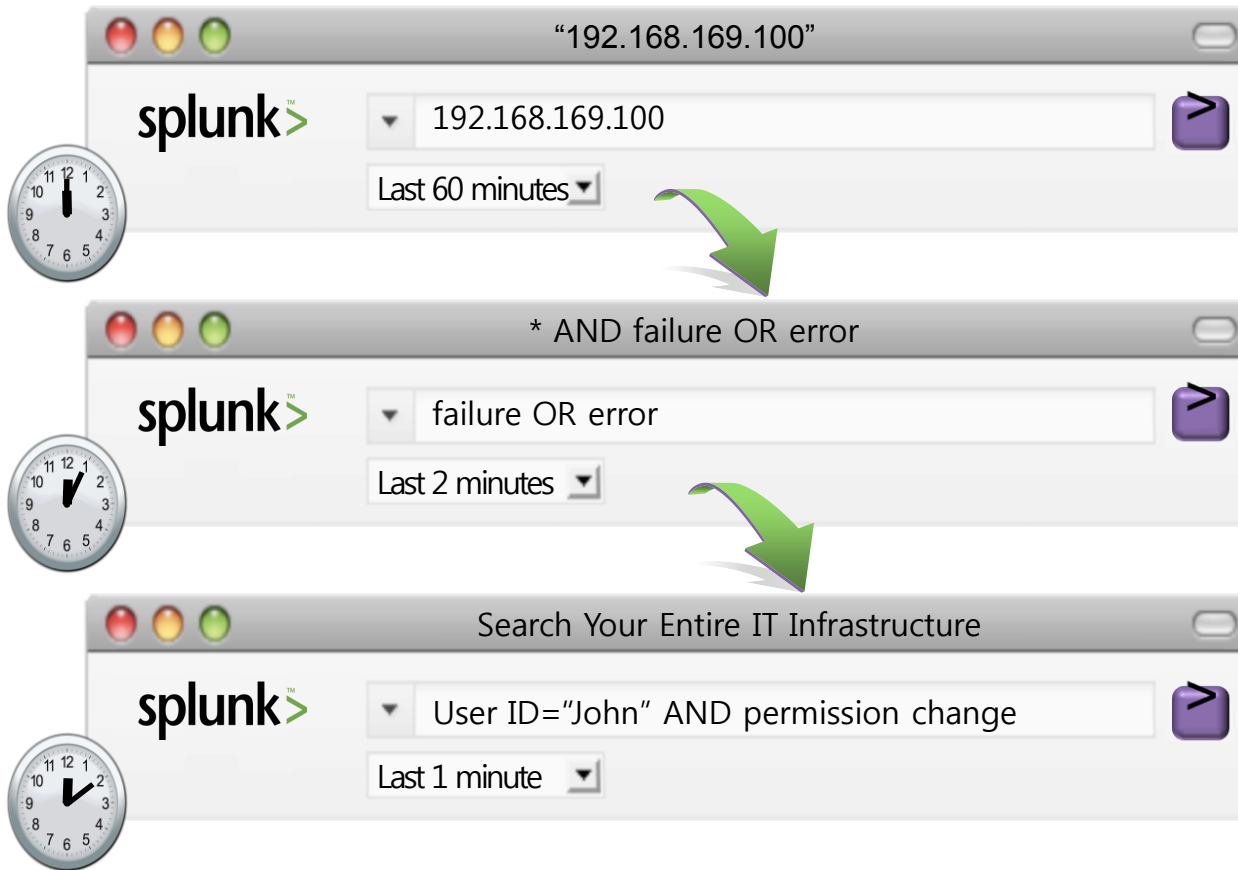
IT Data Engine

기존의 IT 환경에서와는 달리 미리 정의된 스키마, RDB, 별도의 connector(agent) 등이 필요 없이 Data를 수집, 검색할 수 있습니다.



IT 문제 해결을 위한 Tool

각종 시스템 및 어플리케이션에서 발생한 문제를 파악하고 연관하여 분석하는데 단지 몇 분만이 소요됩니다.



IP 검색으로 관련된 웹 세션과 ID 정보를 알아낸다.

DB 에러와 권한 획득 실패가 동시에 발생한 것을 발견한다.

ID와 권한 변경을 상관 검색하여 Order 없는 권한 변경을 발견한다.

기존의 방식과의 차이점

기존의 RDB를 사용하는 방식과는 달리 비구조적(Unstructured) 데이터 및 대용량의 데이터(Big Data)를 빠르고 정확하게 연관 검색할 수 있습니다.



Relational Databases



Multidimensional Databases



IT Data Engine

- 금융거래, 제조 및 물류 정보, 개인정보 등
- 구조적 데이터 — 구조적 데이터베이스
- 유연하지 않은 스키마, 긴 운영/구축 사이클

- 비즈니스 관리 및 통계정보
- 수학적/연산 처리에 강함- 고밀도의 데이터
- 유연한 금융정보 분석을 위한 피벗(pivot) 데이터
- 월간(주기적) 보고에 적합, 실시간 처리에 부적합

Human Generated Data

- 정의된 스키마 없이 연속적이고 비구조적인 데이터
- 모든 IT 시스템에서 생성, 표준화 되지 않고 예측하지 못한 포맷
- 대용량, 빠른 탐색과 탁월한 연관 검색

Machine Generated Data

Operational Intelligence로서의 Splunk

단일 데이터 저장소

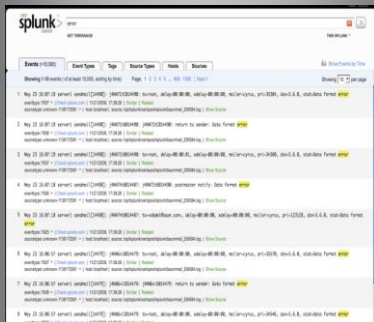
단일 인터페이스

다양한 용도

세 가지 핵심 역량

검색 / 탐색

- 데이터 Drill-down
- "덤불에서 바늘 찾기"
- 문제의 근원 분석 / Trouble Shooting
- 즉각적/실시간 조사



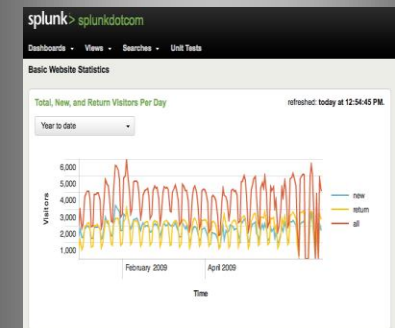
실시간 가시성

- 실시간 대시보드
- 이벤트 상관분석
- 모니터링과 경보
- 성능관리
- 트랜잭션의 수준
- SLA 트래킹



데이터 분석능력

- 베이스라인 및 임계값
- 추이 (Trending)
- 직관적 도식화
- 과거 패턴분석
- 규정준수용 리포트



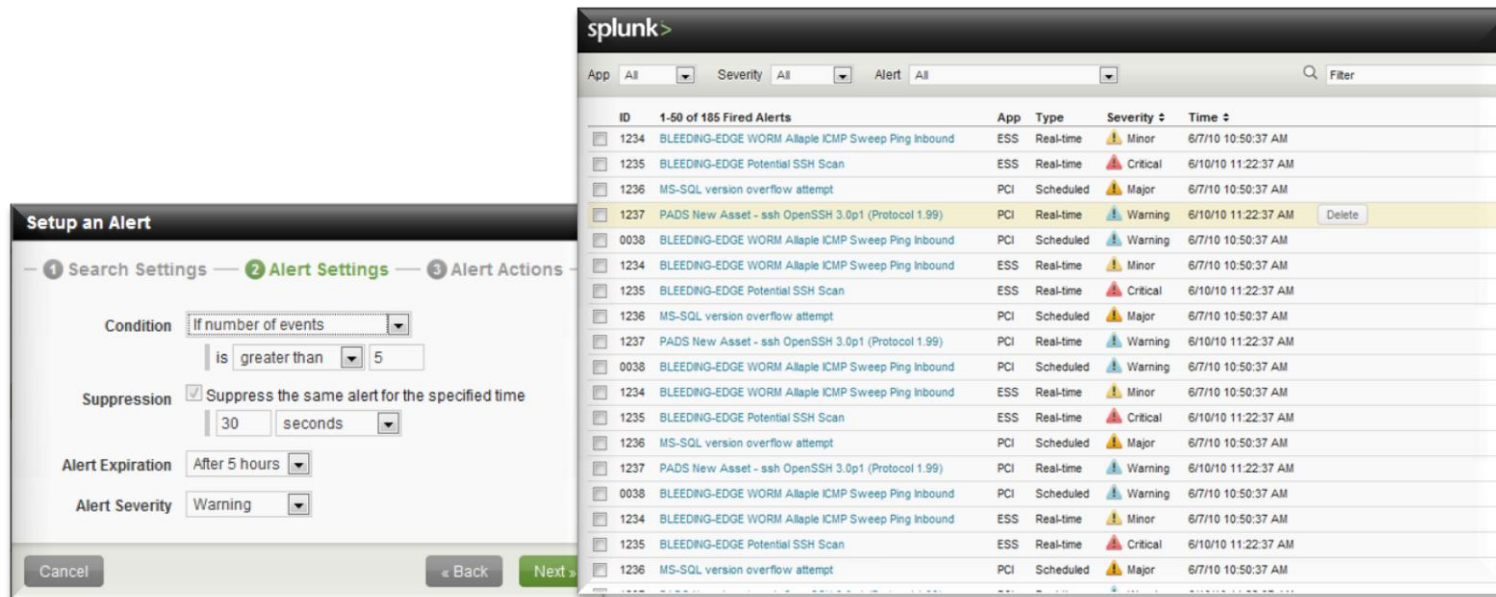
IT Data를 위한 검색 엔진 기능

Splunk는 인터넷 검색엔진(Google, Naver 등)을 통해 원하는 정보를 빠르고 정확하게 찾아내듯이 각종 IT Machine에서 생성되는 Data를 쉽고, 빠르고, 정확하게 검색하여 줍니다.



사전인식(예측) 기능

Splunk에는 Alert 설정 기능이 있어 고객이나 서비스, 시스템 등에 영향을 미칠 수 있는 문제 또는 공격 징후 등을 사전에 IT 전반적인 영역에 걸쳐 자동적으로 모니터링 할 수 있습니다.



The image shows two parts of the Splunk interface. On the left is the 'Setup an Alert' dialog box, and on the right is a list of 'Fired Alerts'.

Setup an Alert Dialog:

- Tab: **Alert Settings**
- Condition: If number of events is greater than 5
- Suppression: ☒ Suppress the same alert for the specified time (30 seconds)
- Alert Expiration: After 5 hours
- Alert Severity: Warning

Fired Alerts Table:

ID	Alert Name	App	Type	Severity	Time
1234	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound	ESS	Real-time	Minor	6/7/10 10:50:37 AM
1235	BLEEDING-EDGE Potential SSH Scan	ESS	Real-time	Critical	6/10/10 11:22:37 AM
1236	MS-SQL version overflow attempt	PCI	Scheduled	Major	6/7/10 10:50:37 AM
1237	PADS New Asset - ssh OpenSSH 3.0p1 (Protocol 1.99)	PCI	Real-time	Warning	6/10/10 11:22:37 AM
0038	BLEEDING-EDGE WORM Allaple ICMP Sweep Ping Inbound	PCI	Scheduled	Warning	6/7/10 10:50:37 AM

RSS



Email



SNMP

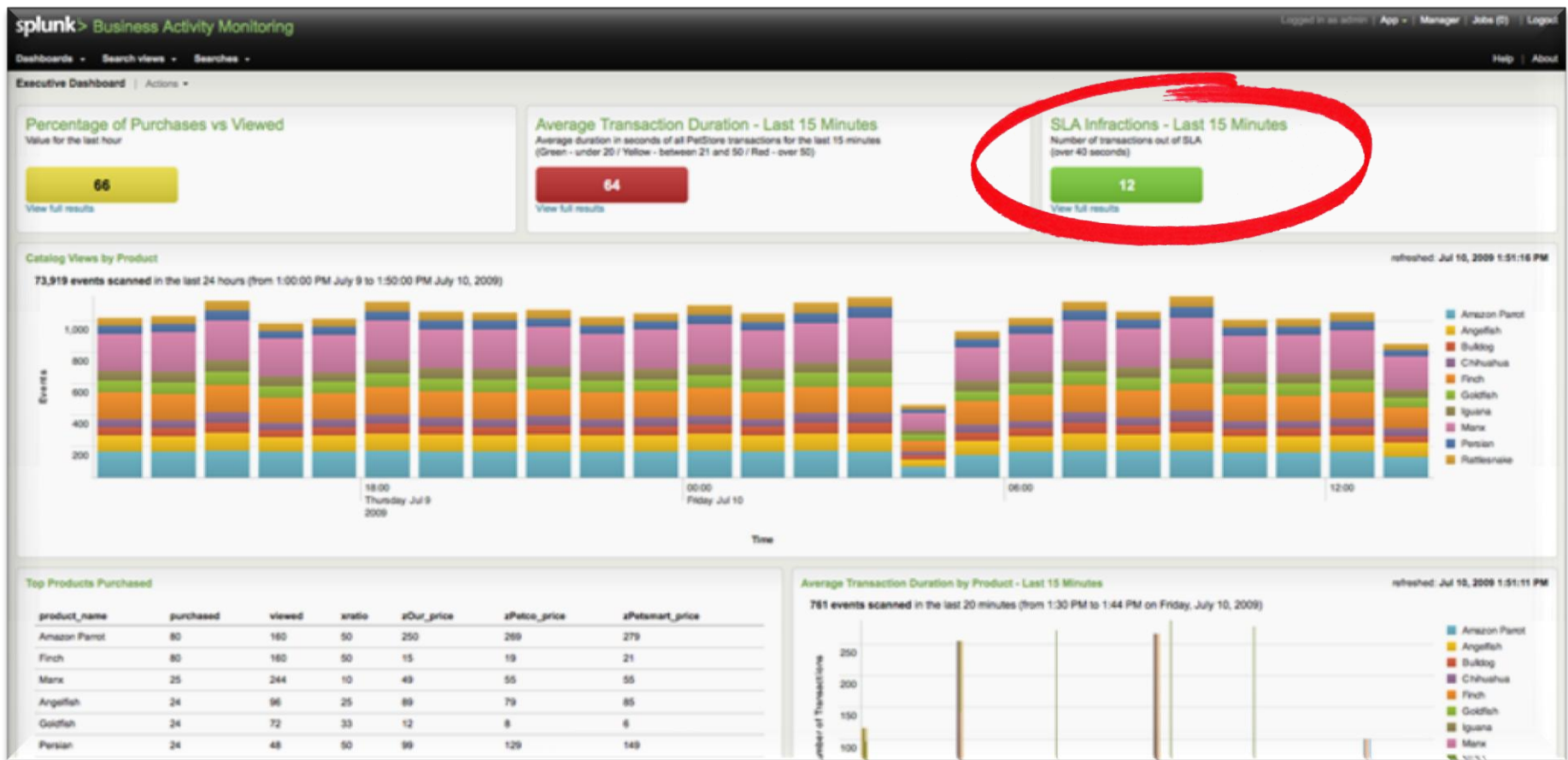


Trouble ticket



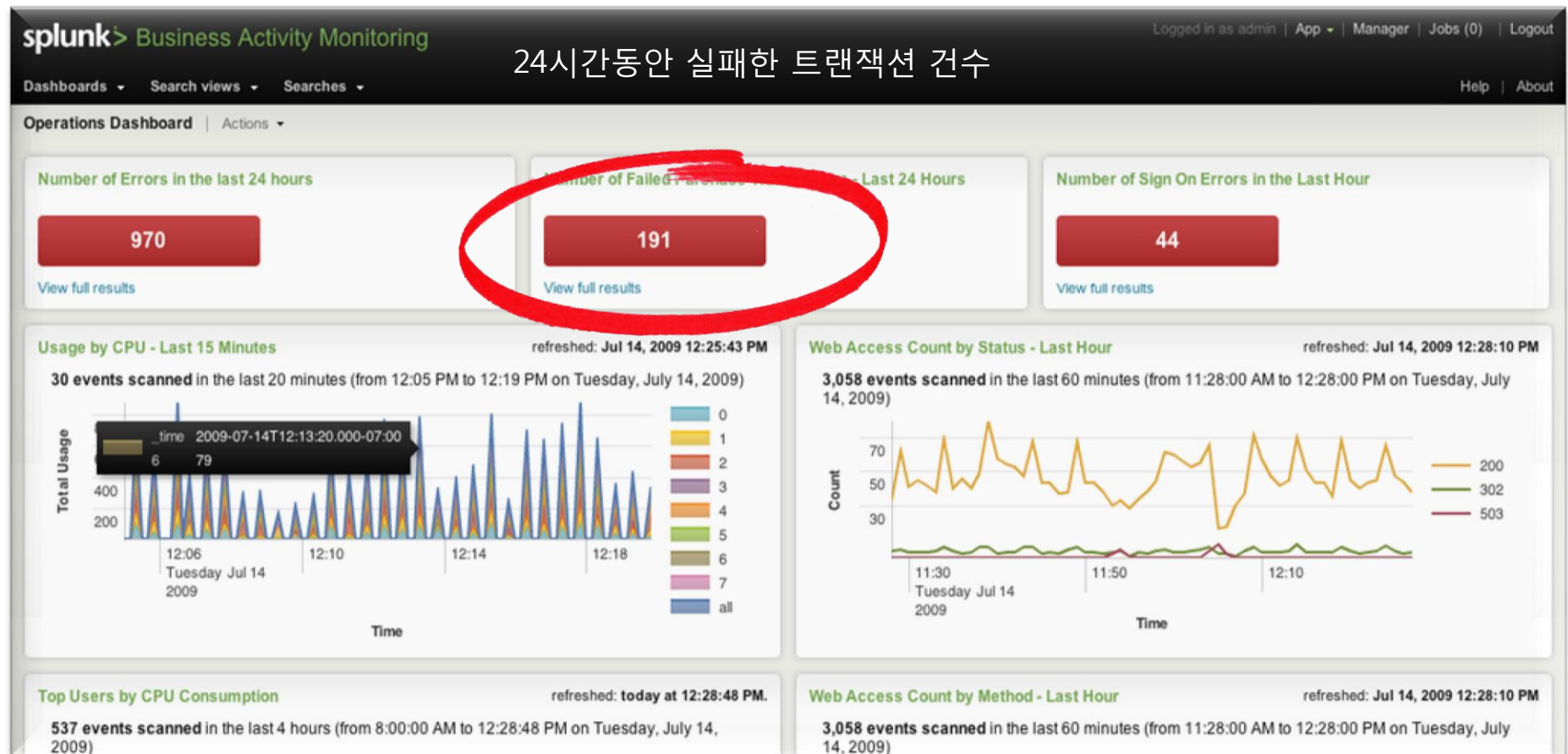
가시성 제공

Splunk는 IT 전 영역에 걸쳐 주요 성과지표는 물론, 가시성을 제공하여 좀더 나은 Business 의사결정 도구로 활용될 수 있습니다.



Business 통찰력 제공

Splunk는 IT 운영데이터로부터 새로운 비즈니스의 통찰력을 제공합니다.



대상 사용자

Splunk는 IT, non-IT 분야에서 일하고 있는 모든 사용자들이 업무 수행 및 의사결정에 도움이 될 수 있는 가치있는 정보를 제공할 수 있기 때문에 각 분야에 있는 모든 사용자들을 위한 솔루션이라고 할 수 있습니다.



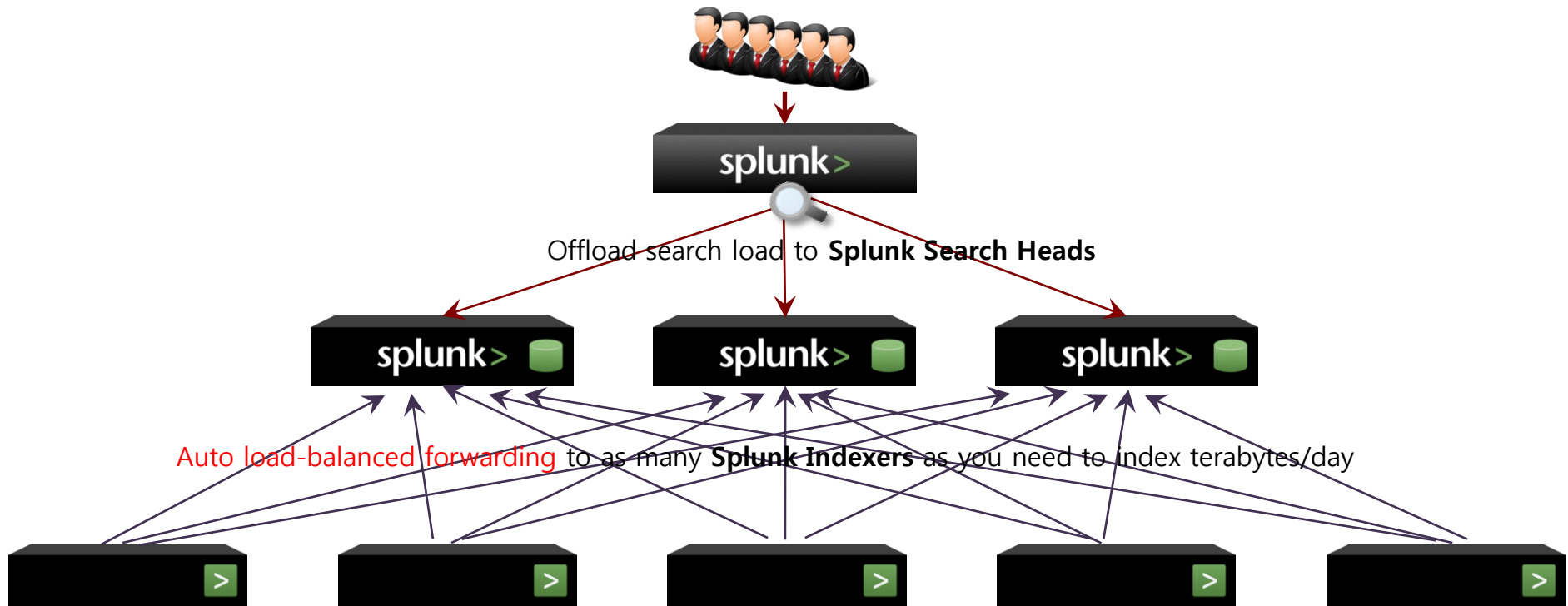
사용자별 Dashboards 및 Reports

Splunk는 모든 사용자들이 업무 수행 및 의사결정에 도움이 될 수 있는 가치있는 정보를 제공하기 위해 사용자별 Dashboard 및 Report를 구성하여 제공할 수 있습니다.



확장성

Splunk는 특유의 분산처리 기술이 있어 전체 네트워크의 성능에 영향을 주지 않고 보다 많은 Data를 빠르고 정확하게 수집하기 위해 Forwarder, Indexer, Search Head 등으로 구성할 수 있습니다.



Send data from 1000s of servers using combination of **Splunk Forwarders**, syslog, WMI, message queues, or other remote protocols

쉬운 사용법

Splunk는 Software 제품으로 설치할 Hardware의 OS별로 간단히 download 받아 설치할 수 있으며 바로 Data 수집 및 분석이 가능합니다.

1. Download



2. Eat your IT Data



3. Start Splunking



Splunk의 특징점

Splunk는 수집하는 데이터에 제한이 없으며, 활용방안도 유연하며, 대용량의 데이터도 빠른 분석 및 다양한 결과 reporting이 가능합니다.

제한없는 데이터

- ▶ 모든 소스에서 발생하는 모든 포맷의 데이터
- ▶ 필터링 되지 않은 모든 데이터 수집/보관/검색
- ▶ 데이터 관리의 모든 생명주기를 만족

완벽한 유연성

- ▶ IT 전 영역에 걸친 제한없는 분석, 모니터링 및 리포팅
- ▶ 모든 사용자를 만족시키는 고도로 유연한 대시보드
- ▶ 새롭고 생소한 데이터 수용이 매우 쉽고 직관적 (필드 추출 마법사)

즉각적 결과

- ▶ OS별 다운로드, 빠른 설치
- ▶ Laptop부터 데이터센터급까지 필요한 만큼의 Sizing으로 모든 기능을 즉각적으로 활용
- ▶ 몇 시간에, 며칠 만에 즉각적인 결과를 도출할 수 있음

Splunk : the IT Data Engine

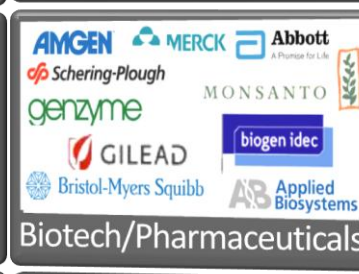
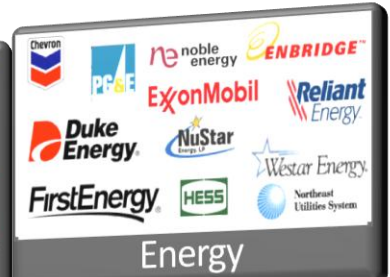
splunk>

Splunk의 ROI

Splunk를 도입하여 활용함으로써 예측을 통한 보안사고 감소, Compliance 준수 등을 통해 다양한 ROI 결과를 얻을 수 있습니다.

매출증대	Macys.com proactively monitor website, e-commerce and application infrastructure. Eliminated downtime during peak periods, avoiding revenue loss of \$300,000/incident
가용성 증대	TransUnion decreased average downtime per incident by 90%, saving millions of dollars per year in extra revenue.
생산성 향상	HealthTrans used to take 7-8 hours to trace a transaction. Now it takes 5 minutes.
비용절감	Large mutual fund is using Splunk for compliance review. Through greater efficiency, Splunk paid for itself in 60 days.
누수비용 절감	Large telecoms company eliminate service abusers. ROI gained on fraud detection in the first month paid for Splunk
사업성 향상	Top five US wireless carrier optimizes call routing, saving hundreds of thousands of dollars per month

전 세계 80개국 3,000 이상 고객



국내 Splunk 고객

hynix

CJ 파워캐스트

kt 미디어본부

kt EPC (클라우드 사업)

kt powertel

LG U+

한화증권

Smartro
Payment Biz Best Provider

한양대학교의료원
HANYANG UNIVERSITY MEDICAL CENTER

KISA 한국인터넷진흥원
Korea Internet & Security Agency

한국교직원공제회
THE KOREAN TEACHERS' CREDIT UNION

MANDO

SAMSUNG 삼성SDS

Hyundai Card

예금보험공사
KOREA DEPOSIT INSURANCE CORPORATION

HanbitSoft

KIER 한국에너지기술연구원
KOREA INSTITUTE OF ENERGY RESEARCH

기획재정부
MINISTRY OF STRATEGY AND FINANCE

국방과학연구소
Agency for Defense Development

관세청
KOREA CUSTOMS SERVICE

KERIS 한국교육학술정보원

KICT

Daum

SPLUNK를 어디에 활용하나?

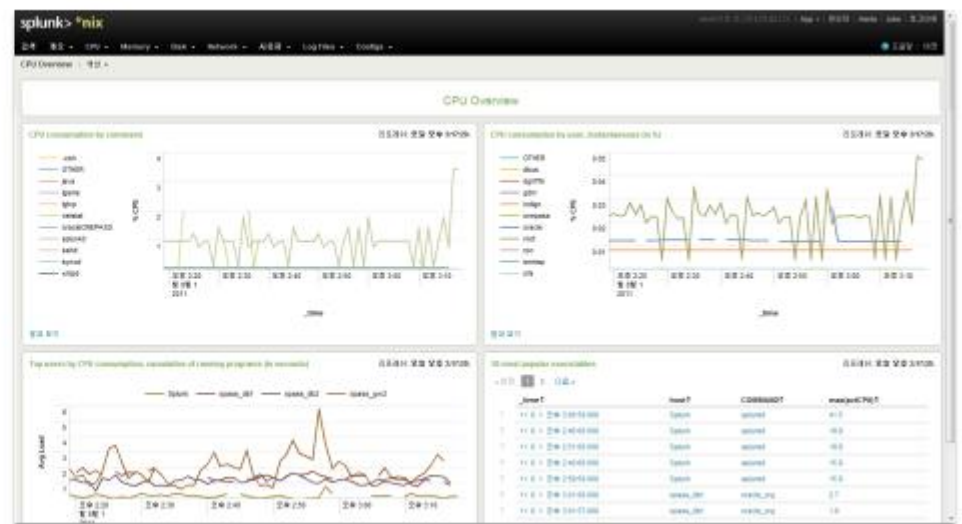
신규 Business 분석

새롭게 시작한 Business의 성과 등을 파악하기 위해 Business 시스템과 운용 시스템에서 발생하는 IT Data를 수집/분석하여 실시간 가시성을 확보할 수 있습니다.



Server/Network 실시간 관리

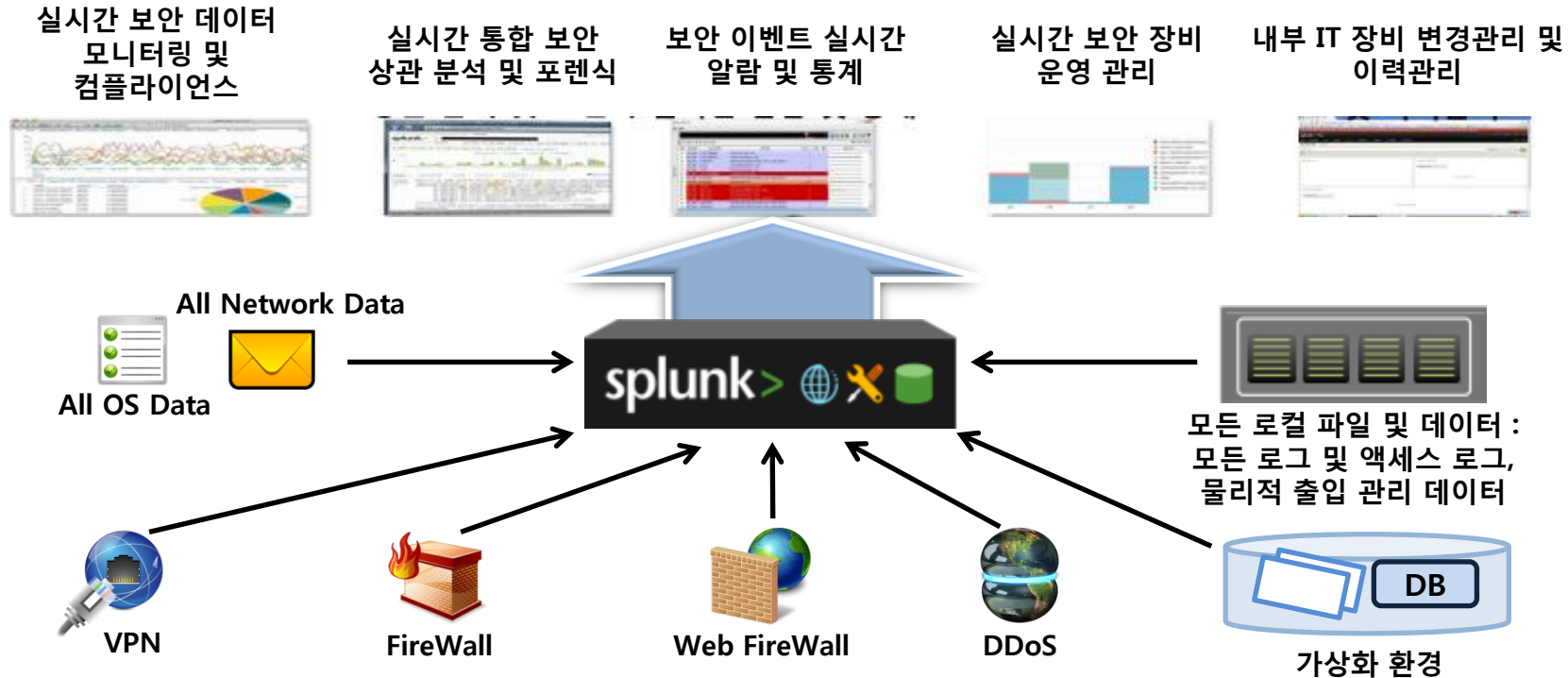
Splunk를 이용하여 Server/Network를 관리하게 되면 기존의 SMS, NMS와 동일한 기능을 수행하면서 alert 등이 발생하였을 때 그 원인을 파악할 수 있습니다.



- Splunk 변경관리와 서버/NW 보안 제품의 기능을 통합하여 관제
- 서버/NW에서 일어나는 모든 일들을 실시간으로 모니터링 및 경고 발생
- 방대한 양의 데이터를 보유한 고객을 위한 IT 감사 시스템

통합 보안 관제

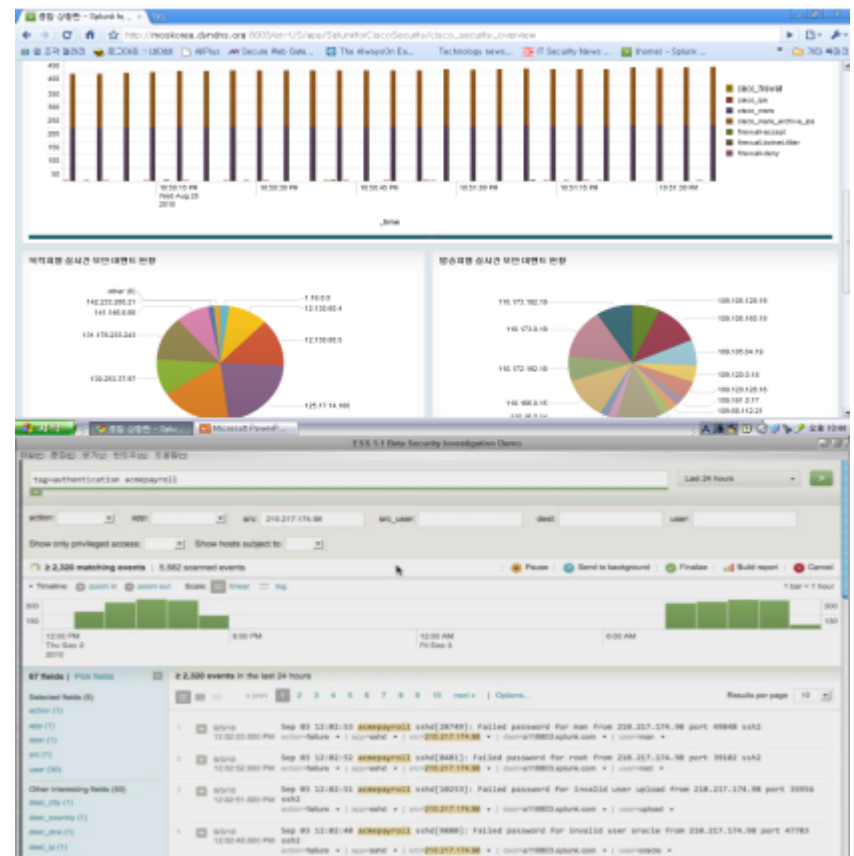
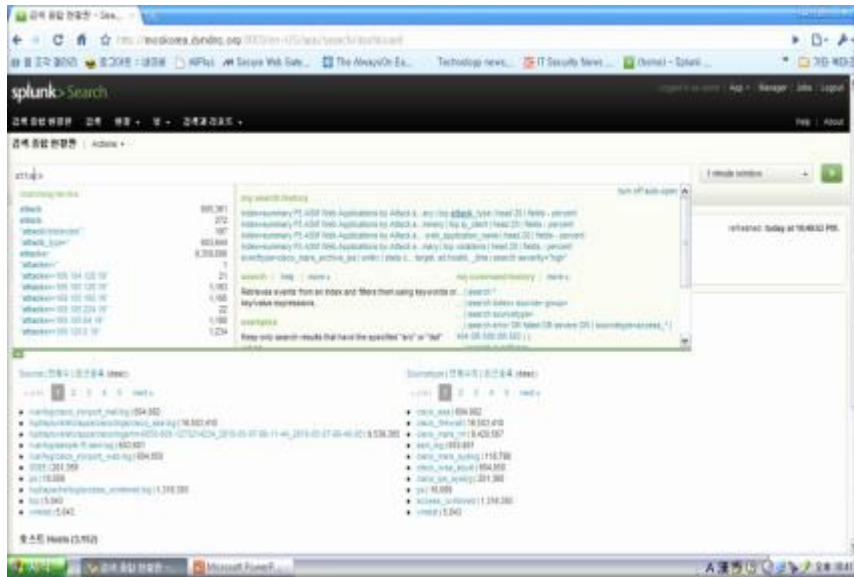
기존과는 달리 시스템, 보안시스템, 물리적 보안 등을 포괄한 통합 보안 관제를 수행할 수 있습니다.



- 물리적인 보안과 논리적인 보안 데이터를 한자리에서 모두 관제
- 내/외부 데이터 유출 시 빠른 추적과 분석 가능
- 단순한 관제가 아니라 추적, 분석, 장비들 간의 데이터를 Cross Check 하는 차세대 관제

통합로그관리 및 ESM

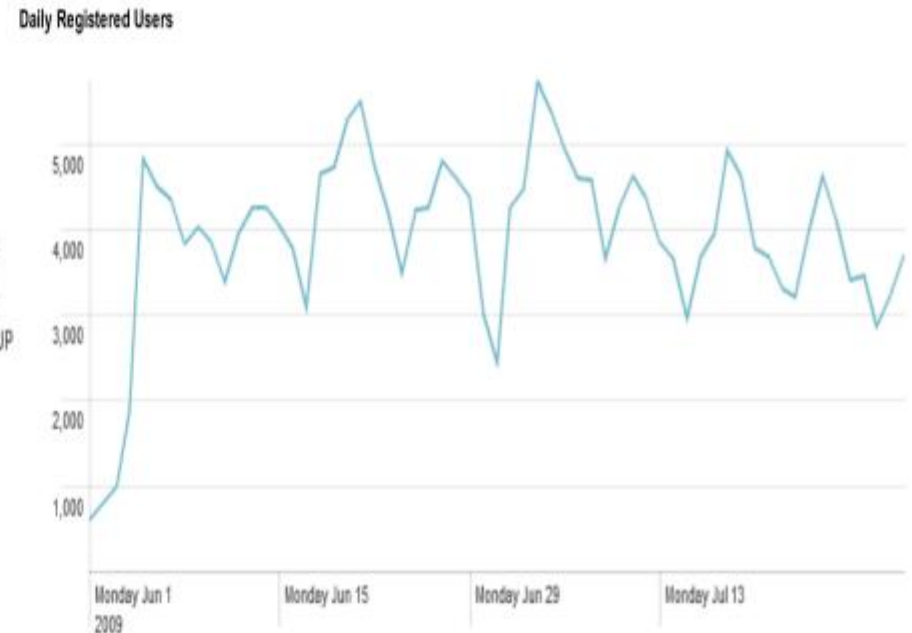
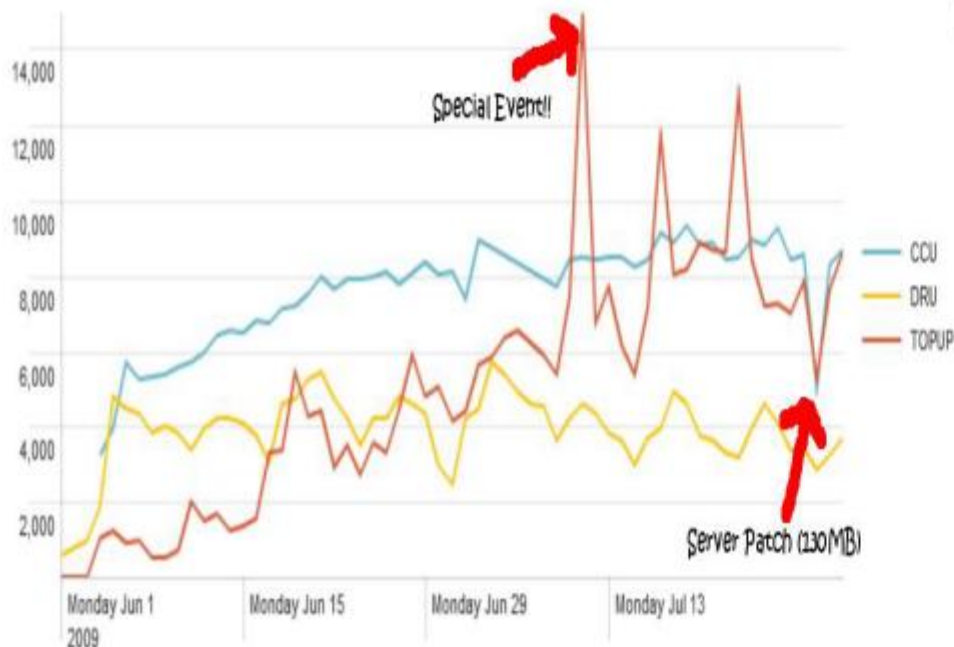
기존 로그관리시스템과 ESM의 조합 또는 SIEM 솔루션에 비해 실시간성, 분석능력 등에서 보다 앞선 성능 및 편리성 등을 제공할 수 있습니다.



- 통합 로그관리와 ESM을 하나의 제품으로 구현
- 모든 로그를 저장, 검색, 분석, 모니터링 가능
- 연관분석 및 시계열 분석 등을 통한 정확한 분석 가능

Business Intelligence(BI)

Splunk를 통해 조직 내 다양한 Data를 통합하여 분석할 수 있고 그 결과를 즉각적으로 제공할 수 있음에 따라 직관적인 정보를 적시에 제공할 수 있습니다.



- 매우 느린 MS 리포팅 툴과 사람의 힘으로 의존하던 BI를 Splunk를 통해 실시간으로 분석 가능
- 단일 시스템으로 조직 내 관련 부서에서 활용함으로써 보다 정확한 의사결정을 내릴 수 있는 통찰력 제공 가능



Thank You !!

영업 Contact :
(주)한국밸런스
영업대표 김 형덕
Mobile) 010-7138-8889
Email) hdkim@valence.co.kr