데이터 경제 시대 최소 비용으로 최대효과 누리기

: 엘라스틱 데이터플랫폼으로 BI, DW, 인프라, APM, 네트워크 모니터링 그리고 보안(백신+ SIEM + EDR)까지

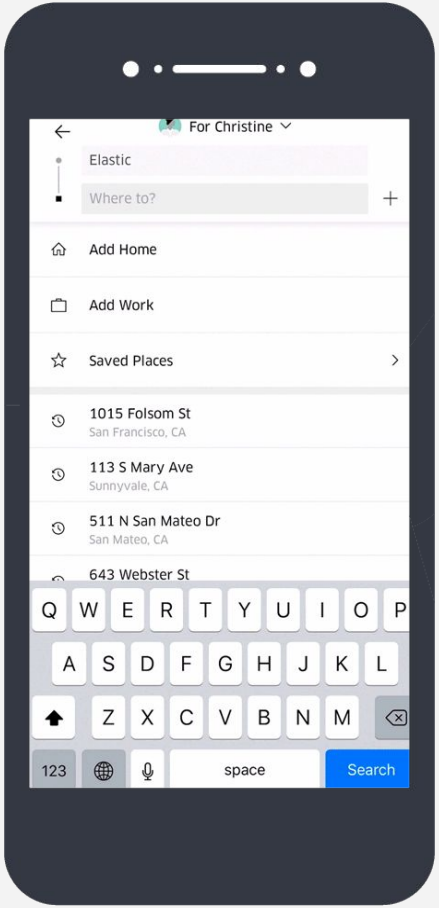
Elastic 김관호 상무

대용량 데이터 분석의 이상과 현실

Background: 국내 및 해외 주식거래가 늘어남에 따라, 고객 민원 증대로 인해 엄청난 시간과 Resource가 투입

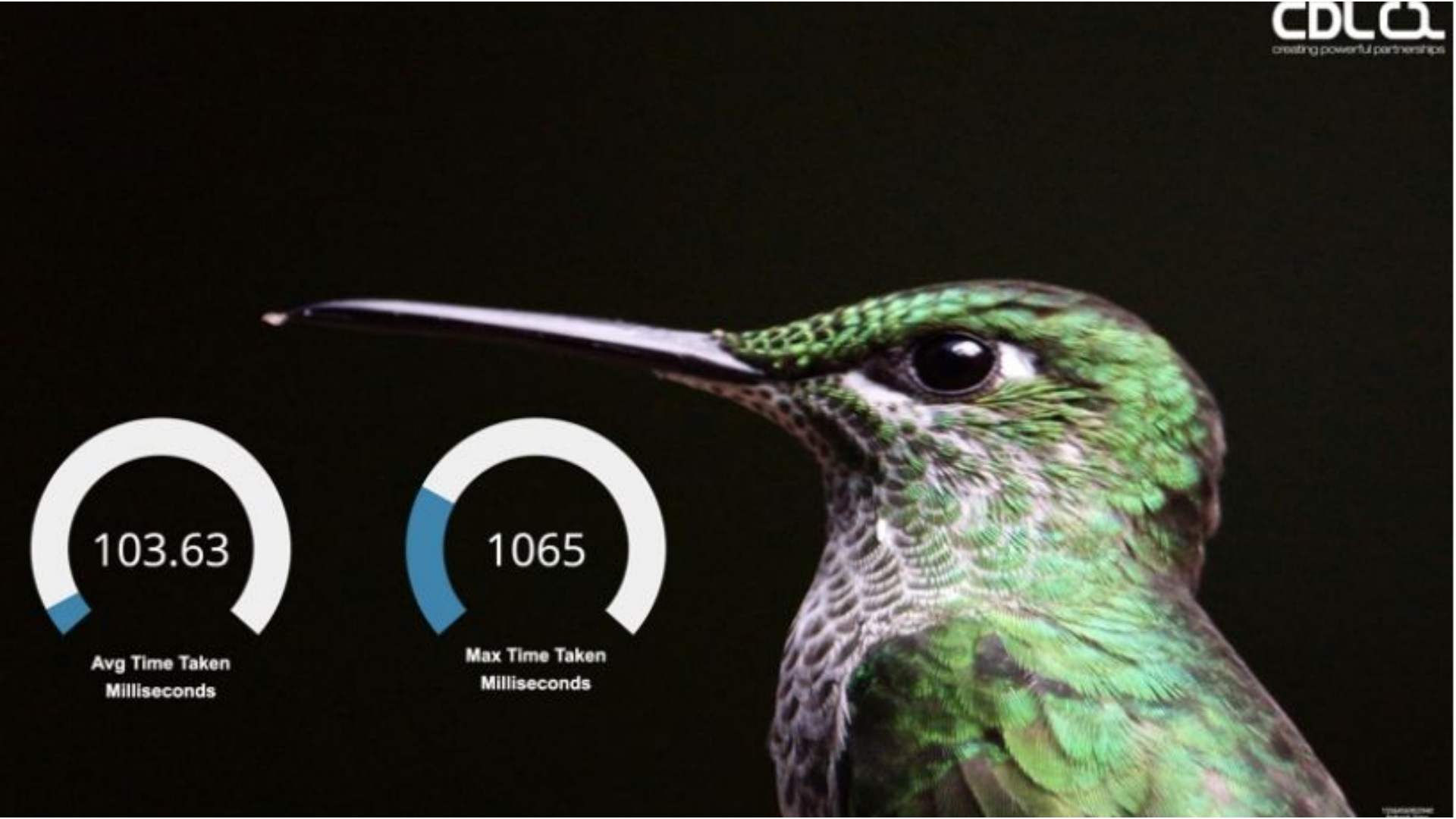
장애로 인해 매수/매도를 못하면, 보상요구가 엄청나게 밀려들어옴
이에 대한 조사를 위해,

- 하루치 고객 거래 로그 검색하는데 30분에서 1시간 소요
- 하루치 집계 데이터 같은 경우 3-4시간 소요
- 일주일 및 한달치에 대한 거래 로그를 뽑는 경우도 많은데 그런 경우 검색 결과를 뽑는데 일주일 소요
- 실제로 직원들은 장애발생시 이에 대한 민원 대응을 위해 리포트를 뽑기 위해 매일 밤샘작업을 함



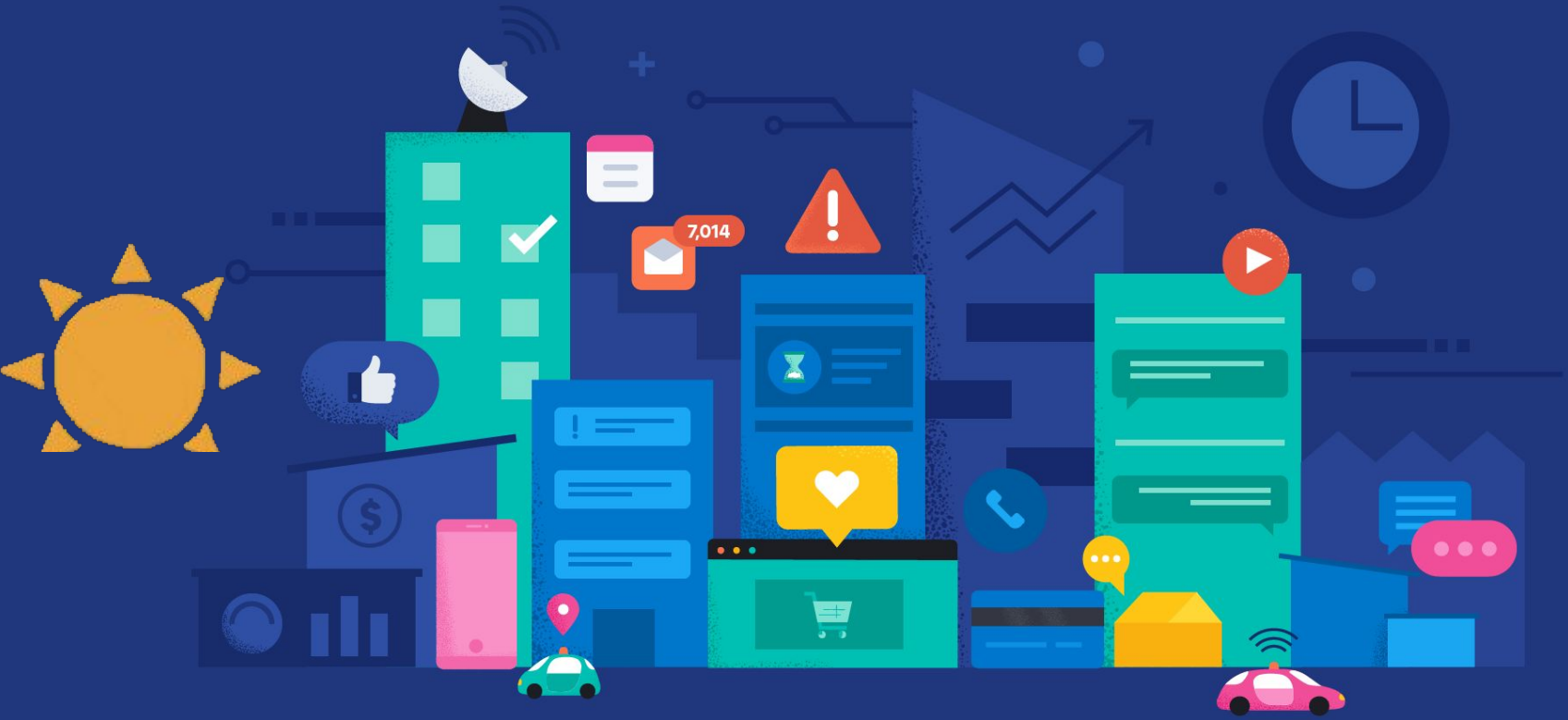
Uber

elastic


CDL
creating powerful partnerships
103.63
Avg Time Taken
Milliseconds
1065
Max Time Taken
Milliseconds

We live in an *always on world*-a world that never sleeps

엄청난 양의 데이터가 매일 매일 축적되고 있음...



This data is *only getting bigger*

480EB

1 EB = 1000 PB = 1,000,000 TB

Daily 생산되는 데이터
by 2025

IDC: Global DataSphere and StorageSphere Forecasts

elastic

비정형 데이터 > 80%*

26.8%

비정형데이터
년간 증가율**

19.6%

정형데이터
년간 증가율**

* Source: Gartner

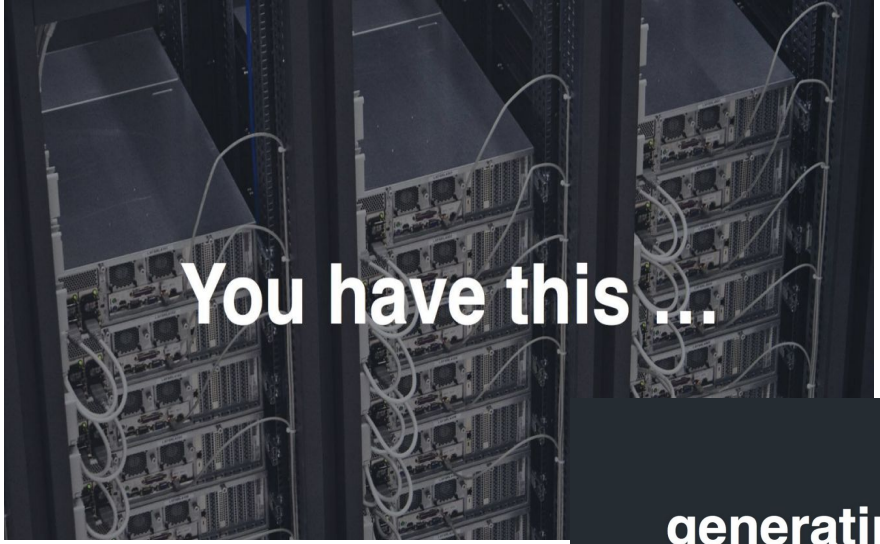
** Source: IDC

But only

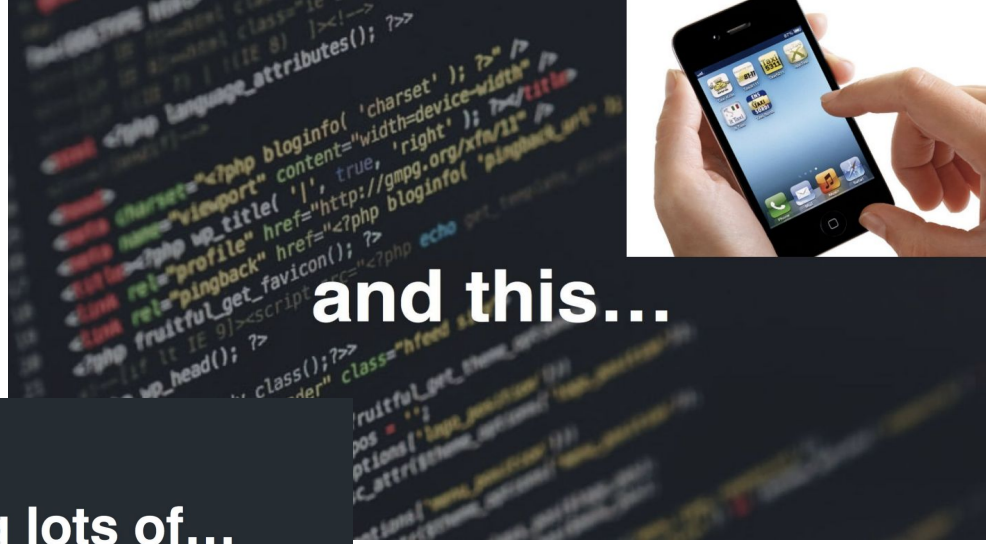
20%

기업내에서 활용되는 있는 데이터

elastic

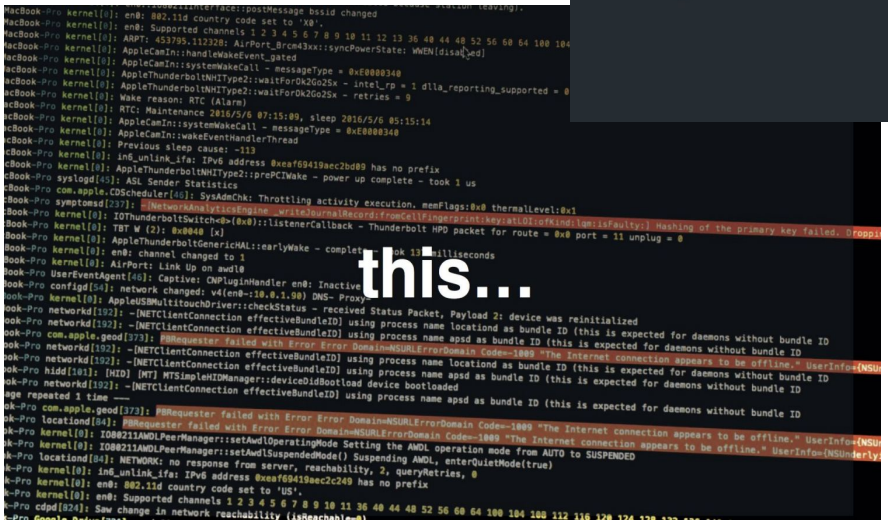


You have this …



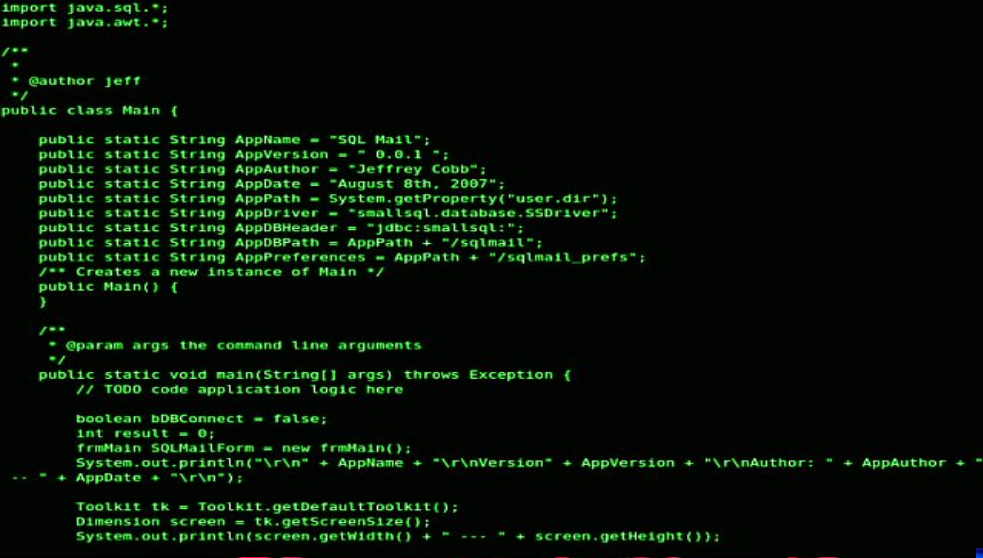
and this…

generating lots of…



this…

and this…



```
import java.sql.*;
import java.awt.*;

/**
 *
 * @author jeff
 */
public class Main {

    public static String AppName = "SQL Mail";
    public static String AppVersion = " 0.0.1 ";
    public static String AppAuthor = "Jeffrey Cobb";
    public static String AppDate = "August 8th, 2007";
    public static String AppPath = System.getProperty("user.dir");
    public static String AppDriver = "smallsql.database.SSDriver";
    public static String AppDBHeader = "jdbc:smallsql:";
    public static String AppDBPath = AppPath + "/sqlmail";
    public static String AppPreferences = AppPath + "/sqlmail_prefs";
    /** Creates a new instance of Main */
    public Main() {
    }

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) throws Exception {
        // TODO code application logic here

        boolean bDBConnect = false;
        int result = 0;
        frmMain SQLMailForm = new frmMain();
        System.out.println("\r\n" + AppName + "\r\nVersion" + AppVersion + "\r\nAuthor: " + AppAuthor + "
-- " + AppDate + "\r\n");

        Toolkit tk = Toolkit.getDefaultToolkit();
        Dimension screen = tk.getScreenSize();
        System.out.println(screen.getWidth() + " --- " + screen.getHeight());
```

```
cout << A <<
cout << Ha << "\t"

f( Re > Sc ) {
if( Re > Ha ) {
if(verbose)
status=2;
GoRetrieve(

} else {
if(verbose)
```

```
* 7015c90 - (HEAD, origin/master, origin/HEAD, master) Updated iPhones graphic with new screenshot (11 days ago) <DiNutter>
* 9bfa321 - Updated README (2 weeks ago) <DiNutter>
* dd18305 - Updated to new design (2 weeks ago) <DiNutter>
* b2e36c6 - Added fallback for missing avatar (2 weeks ago) <DiNutter>
* 8678978 - Removed Disk caching of avatar (6 weeks ago) <DiNutter>
* 39d2c3c - Preparing for App Store submission (9 weeks ago) <DiNutter>
* 4fd7261 - Fixed cell bg when user only has 1 badge. (9 weeks ago) <DiNutter>
* 13bf363 - Fix image (10 weeks ago) <DiNutter>
* 705363e - Try screenshots with transparent background (10 weeks ago) <DiNutter>
* bd4602e - Correct image location in README (10 weeks ago) <Will McKenzie>
* 483d09b - Added iPhone screenshots to README (10 weeks ago) <DiNutter>
* 2d706d7 - Adding license (10 weeks ago) <DiNutter>
* d6c6660 - Adding to .gitignore (10 weeks ago) <DiNutter>
* 0e2af71 - Still trying to ignore UserInterfaceState file (10 weeks ago) <DiNutter>
* cca3d3b - ignore interfaceState file (10 weeks ago) <DiNutter>
* 2b1e812 - Added first draft of README (10 weeks ago) <DiNutter>
* 38586ba - Bug fixes and UI Improvements. New Icons added (2 months ago) <DiNutter>
* 968da4c - Removed extra app icons (3 months ago) <DiNutter>
* ecf783d - Various updates (3 months ago) <DiNutter>
* 6ce53d3 - Removed SOURL files from root (3 months ago) <DiNutter>
* 62e0679 - Made sure images cache (3 months ago) <DiNutter>
* 1397df2 - Ran Arc conversion to improve memory management. Refactoring and bug fixes (3 months ago) <DiNutter>
* c3061b8 - Added pull to refresh functionality (3 months ago) <DiNutter>
* 92661fb - Made sure iPhone badge and accomplishments view controllers reload when user changed. (3 months ago) <DiNutter>
* 83cd921 - Stopped badges images using separate threads. (3 months ago) <DiNutter>
:_
```

RDBMS = SQL Query

Microsoft SQL Server

ORACLE

PostgreSQL

MySQL

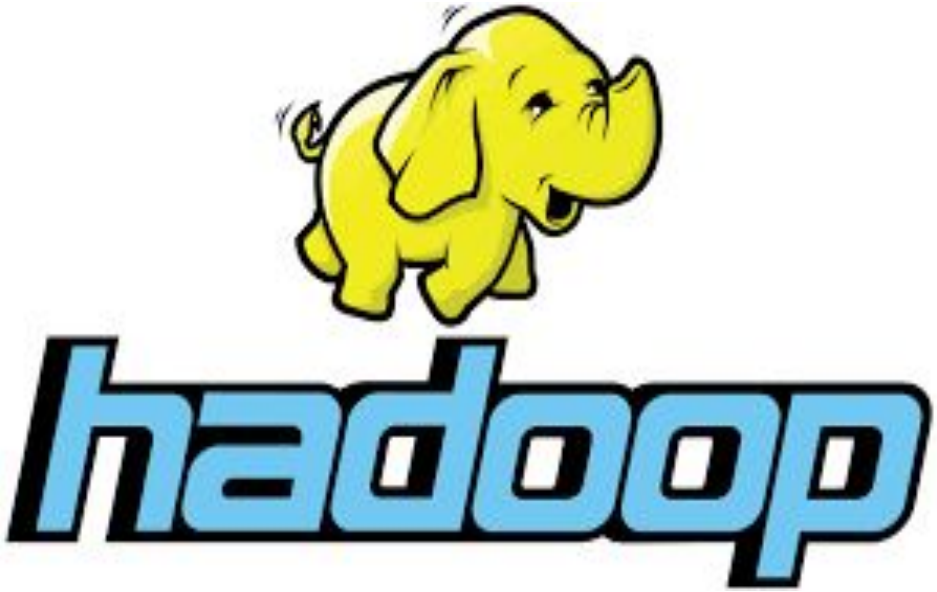
SYBASE

IBM DB2

elastic

전체 (19,466) | 정상 (1,384) | 종료 (18,082)

약정코드	구성원코...	구성원명	생애주기단...	약정상...	약정일	모금상품	납입주기	정기납입액	약정액	납입액
C21000108	2021010050	구성원 일괄5	등록	종료	2021-01-29	겨울캠페인	일시납		20,000	20,000
C21000107	2021010049	구성원 일괄4	등록	종료	2021-01-29	겨울캠페인	일시납		20,000	20,000
C21000106	2021010048	구성원 일괄3	등록	종료	2021-01-29	기업사회공헌사업	일시납		20,000	20,000
C21000105	2021010047	구성원 일괄2	등록	종료	2021-01-29	기업사회공헌사업	일시납		20,000	20,000
C21000104	2021010046	구성원 일괄1	등록	종료	2021-01-29	기업사회공헌사업	일시납		20,000	20,000
C21000103	2021010051	구성원 약정...	등록	정상	2021-01-28	TEST-데모 캠페인	정기납(무기한)	30,000/월	360,000	0
C21000102	2021010050	구성원 일괄5	등록	종료	2021-01-28	겨울캠페인	일시납		10,000	10,000
C21000101	2021010049	구성원 일괄4	등록	종료	2021-01-28	겨울캠페인	일시납		10,000	10,000
C21000100	2021010048	구성원 일괄3	등록	종료	2021-01-28	기업사회공헌사업	일시납		10,000	10,000
C21000099	2021010047	구성원 일괄2	등록	종료	2021-01-28	기업사회공헌사업	일시납		10,000	10,000



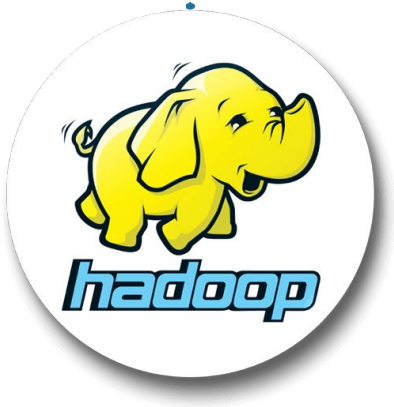
Trend of Big Data Analysis

RDBMS

과거 데이터

BIGDATA

대용량 데이터 수집



What is NEXT ?

elastic

정형 + 비정형

텍스트,

숫자,

위치데이터,

날짜,

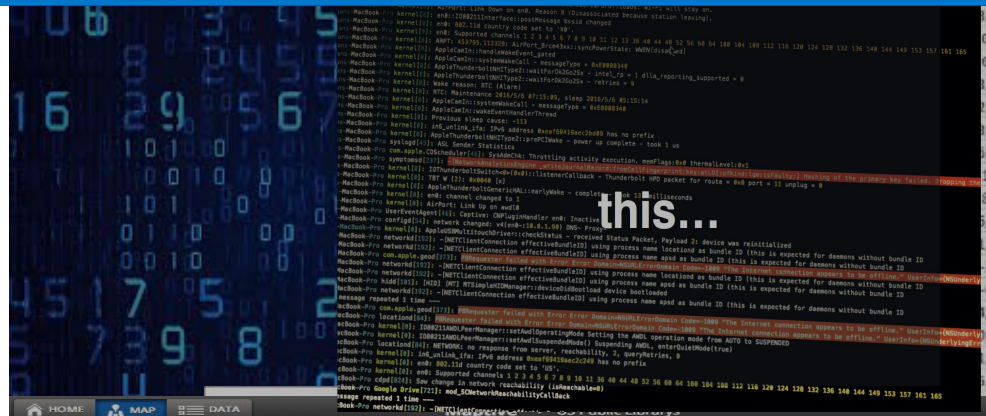
로그,

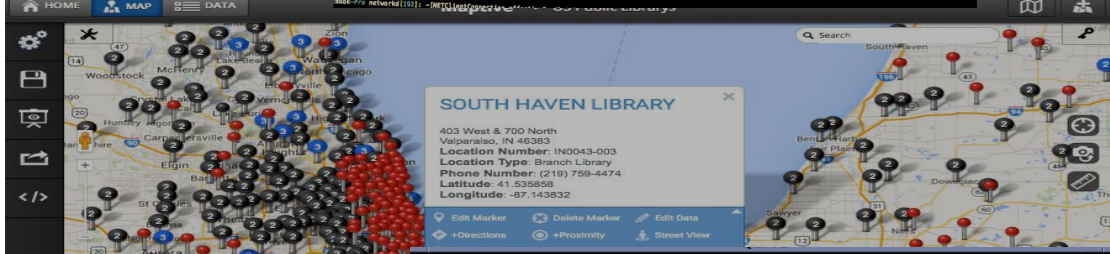
메트릭,

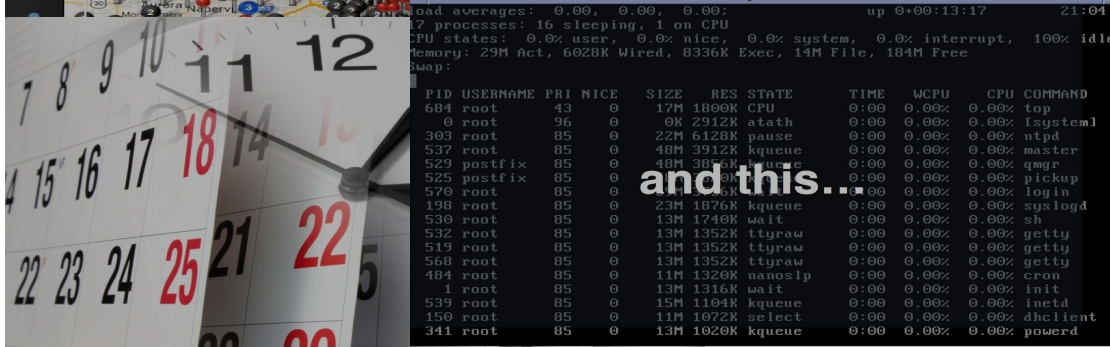
IOT,

Machine generated data,

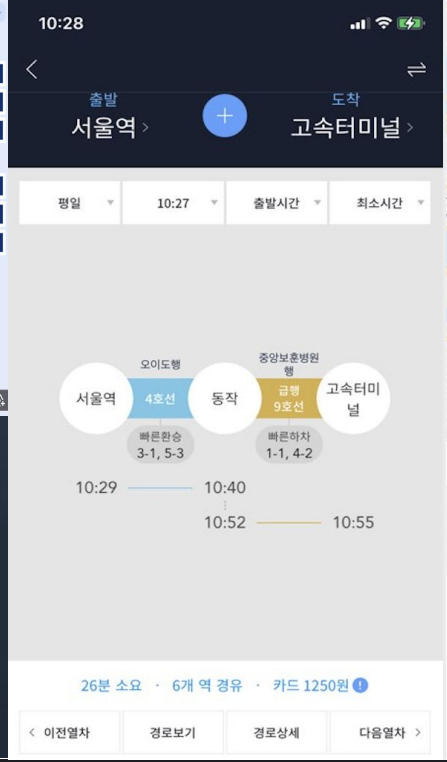
보안로그...

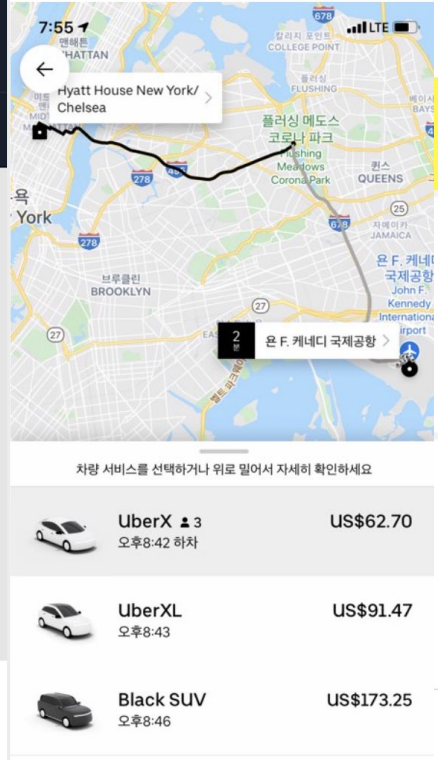






elastic



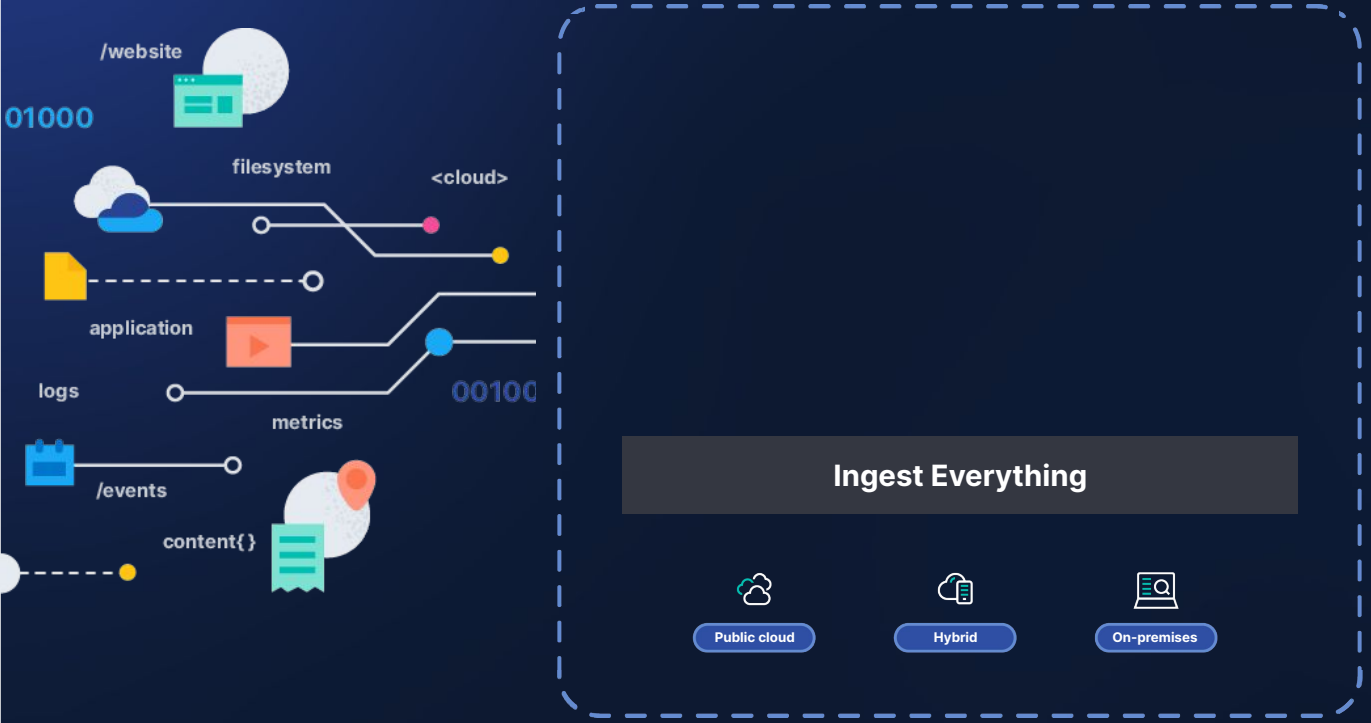


<표> II-1-1. 0000년 전 세계 대비 우리나라 가동원전 및 신규원전 건설현황 점유율: a-01

작성년도	구분	가동중 호기수	가동중 설비용량 (MW)	건설중 호기수	건설중 발전용량 (MW)	합계 호기수	합계 호기수	합계 설비용량 (MW)	Count
2,019	대한민국(6위)	24	23137	4	5360	28	28	29497	1
2,019	보유국(35개국)	445	392966	52	57073	497	497	450039	1
2,019	점유율(%)	5.39	5.89	7.69	9.39	5.63	5.63	6.55	1

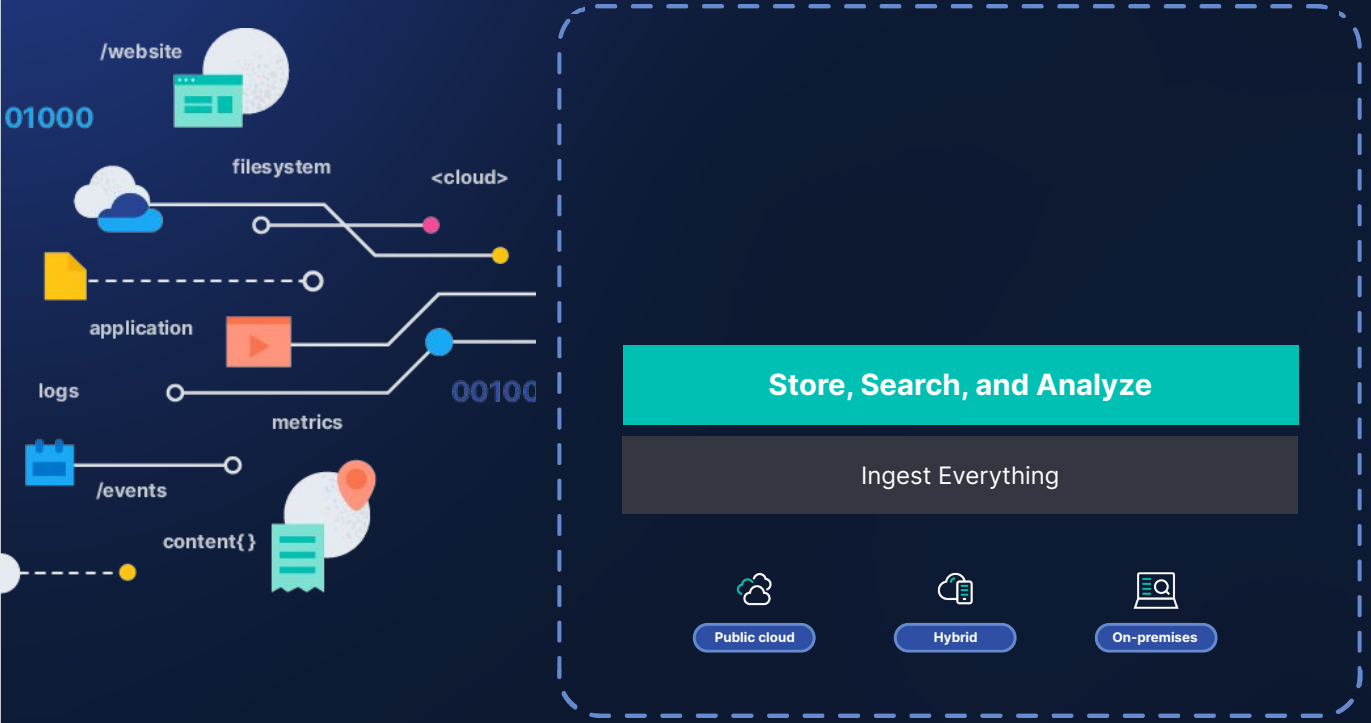
Export: Raw Formatted

Organizations need to



elastic

Organizations need to



elastic

Organizations need to

Visualize and Explore

Store, Search and Analyze

Ingest Everything

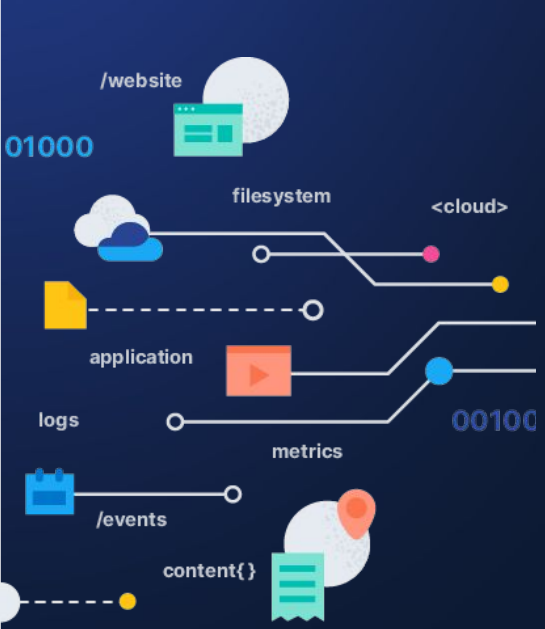
Public cloud

Hybrid

On-premises

elastic

Elastic Search Platform



Observability

Security

Enterprise Search

Kibana
Visualize and Explore

Elasticsearch
Store, Search, and Analyze

Integrations
Ingest Everything

Public cloud

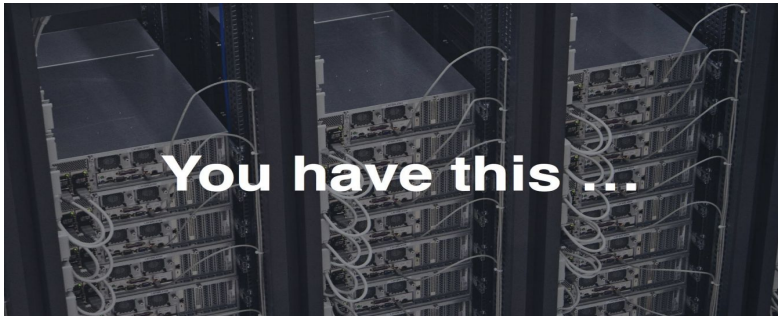
Hybrid

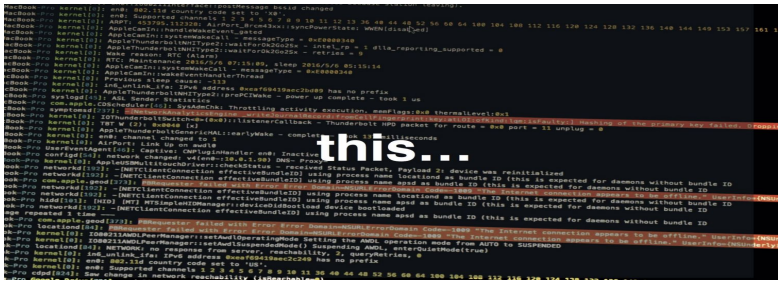
On-premises

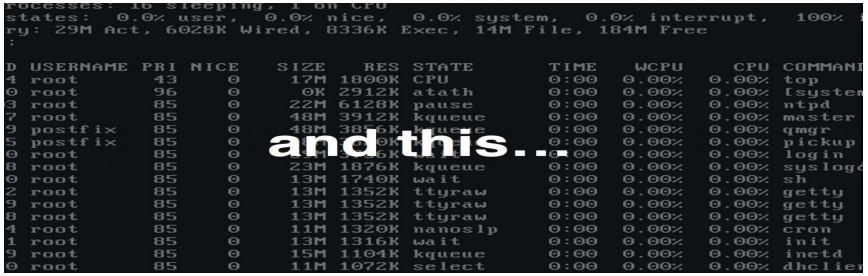
elastic

단순 정형데이터 뿐만 아닌 모든 비정형 데이터를 구글에서 검색하는 경험의 스피드로 쿼리가 가능한 기술

장비, **Application,** 네트워크 등 하루에 쏟아지는 데이터가 이제는 수**TB**에서 수십 수백 **TB**가 쏟아지고 있는것이 현실







elastic

Elastic

NYSE: “ESTC”

3,000+ employees in 40+ countries

World’s #1 database search engine (DBEngines)

elastic

All Images News Videos Shopping More Settings Tools

About 489,000,000 results (0.67 seconds)

www.elastic.co

Elastic

We're the creators of the **Elastic** (ELK) Stack -- Elasticsearch, Kibana, Beats, and Logstash. Securely and reliably search, analyze, and visualize your data in the ...

Elastic Stack and Product · Elastic · ELK stack · About

People also search for

elasticsearch download | elasticsearch vs solr
elasticsearch github | elasticsearch install
what is elasticsearch | elk stack free

People also ask

What is the elastic?

What is elastic stack used for?

What is elastic license?

Is elastic free?

Feedback

Elastic NV

Company

elastic.co

Elastic NV is an American-Dutch company that was founded in 2012 in Amsterdam, the Netherlands, and was previously known as Elasticsearch. Elastic NV is a search company that builds self-managed and SaaS offerings for search, logging, security, and analytics use cases. Wikipedia

Stock price: ESTC (NYSE) $135.00 0.00 (0.00%)
Dec 3, 4:00 PM EST - Disclaimer

Revenue: 427.6 million USD (2020)

Headquarters: Mountain View, California, United States

Founded: 2012, Amsterdam, Netherlands

정형 + 비정형

텍스트,

숫자,

위치데이터,

날짜,

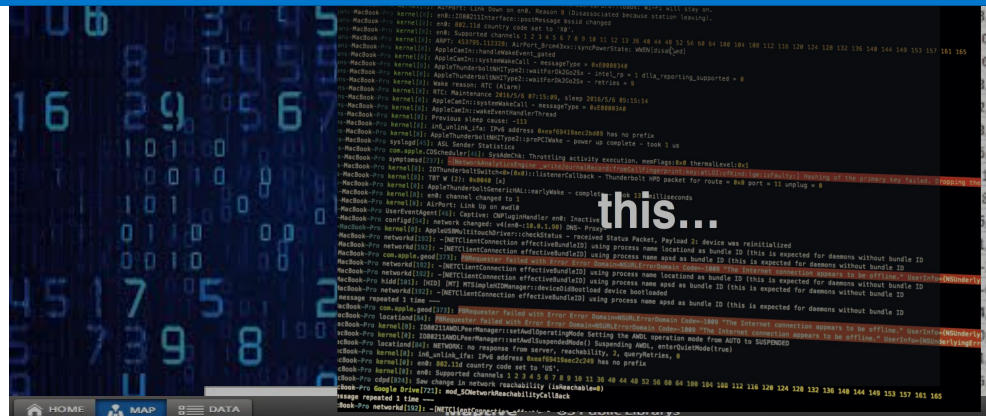
로그,

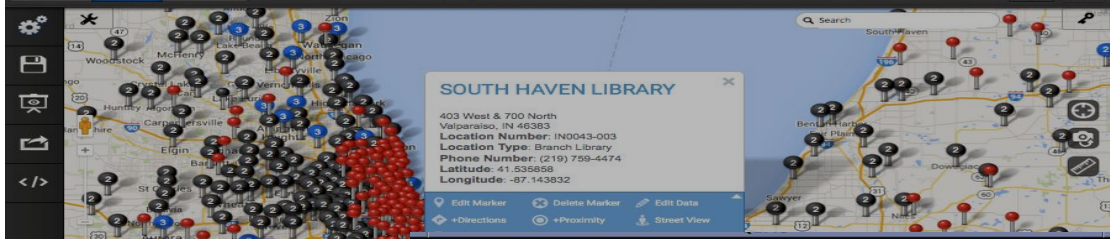
메트릭

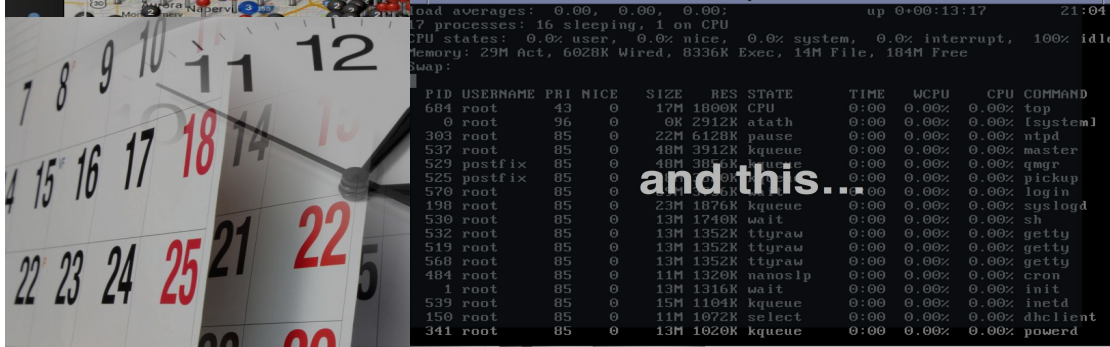
IOT

Machine generated data

보안로그...

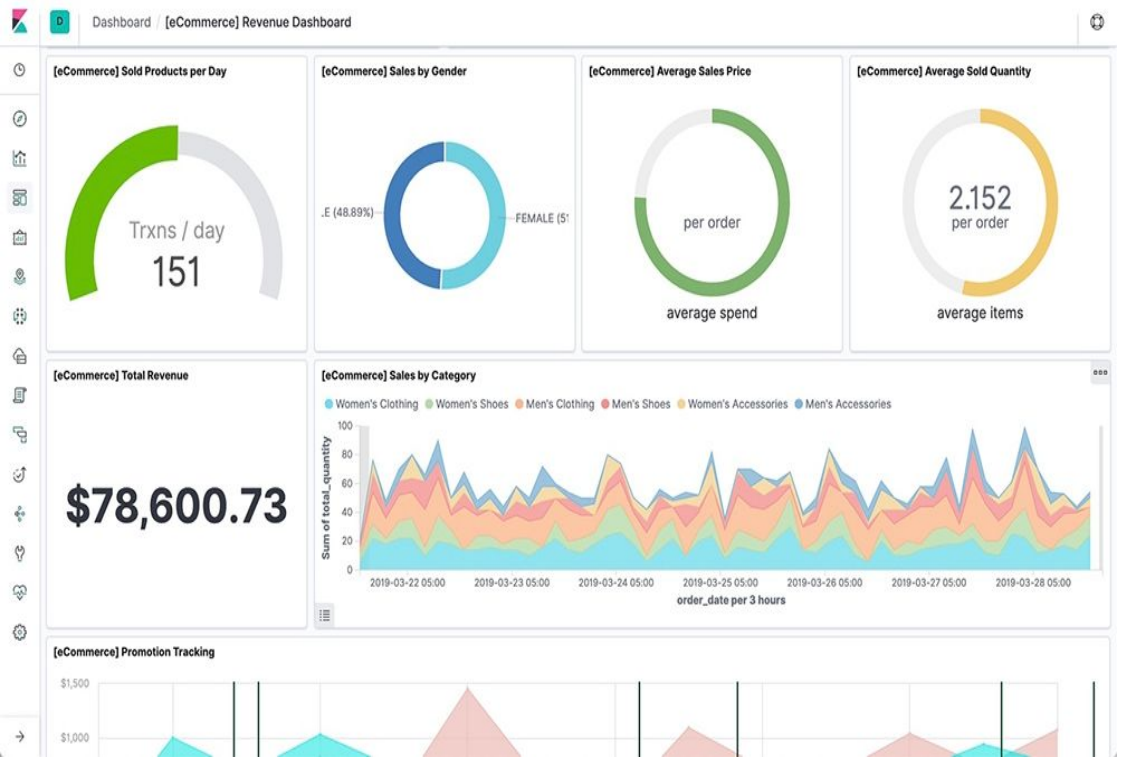


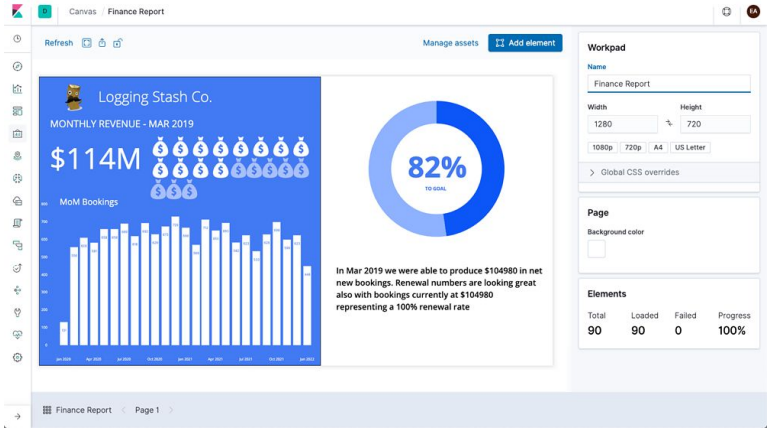


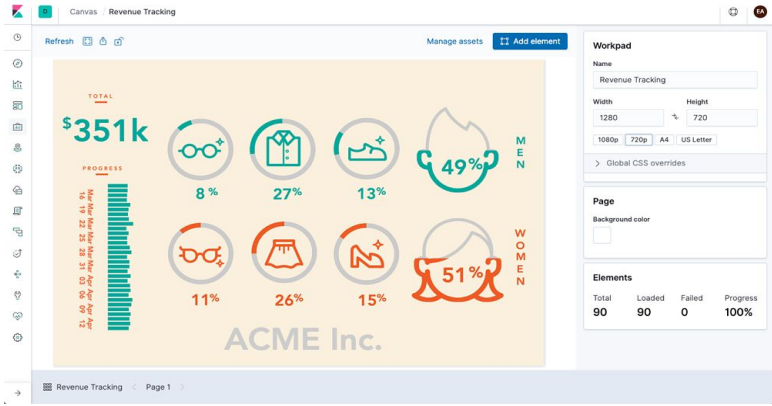


elastic

비즈니스 분석 (BI & DW)

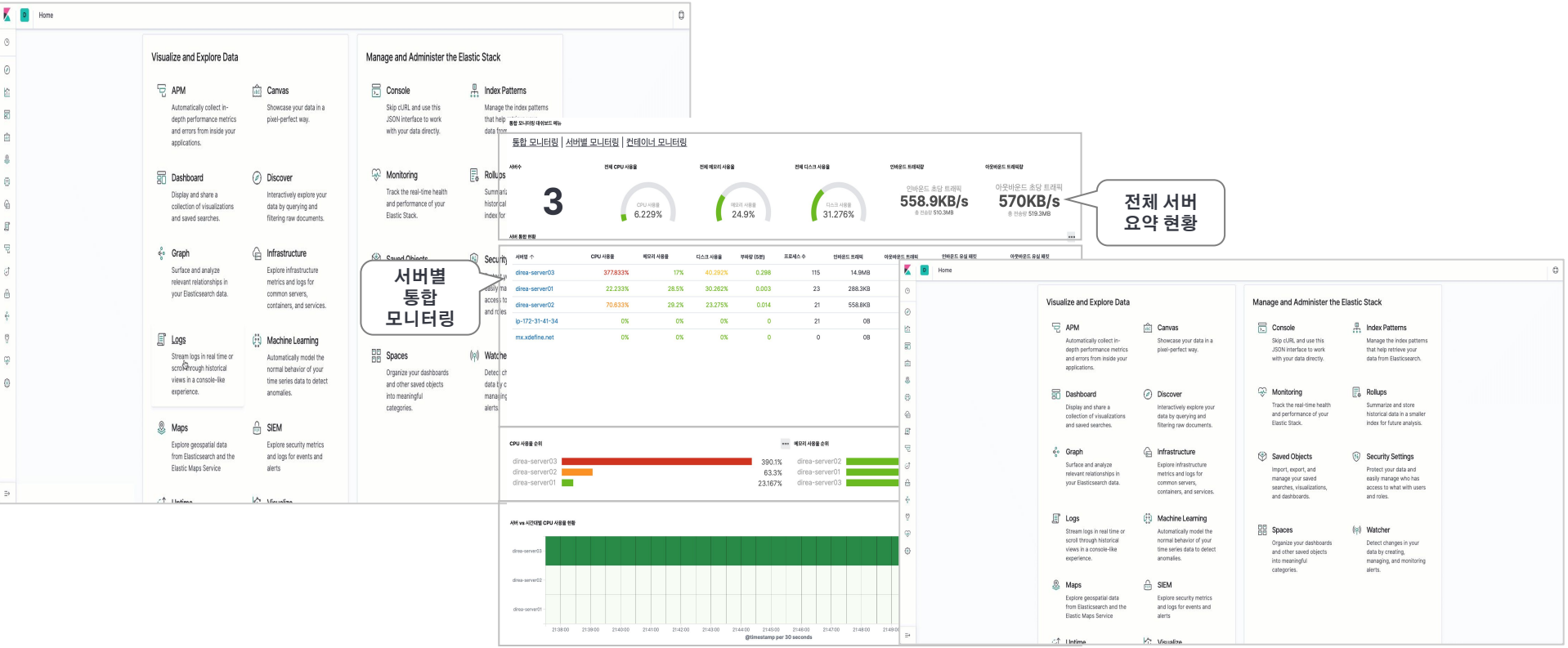




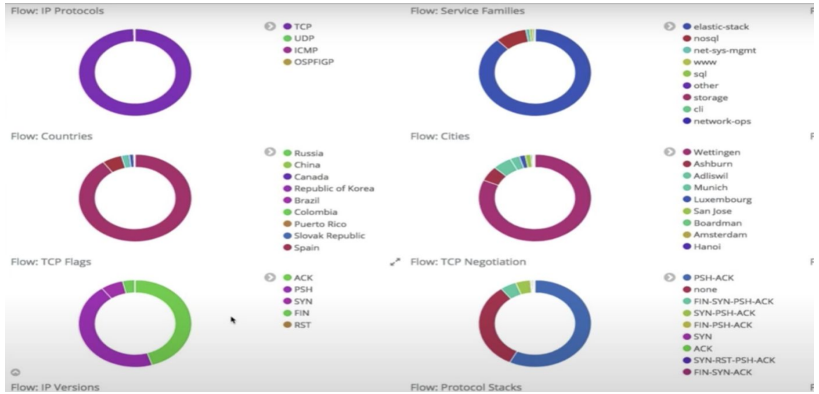


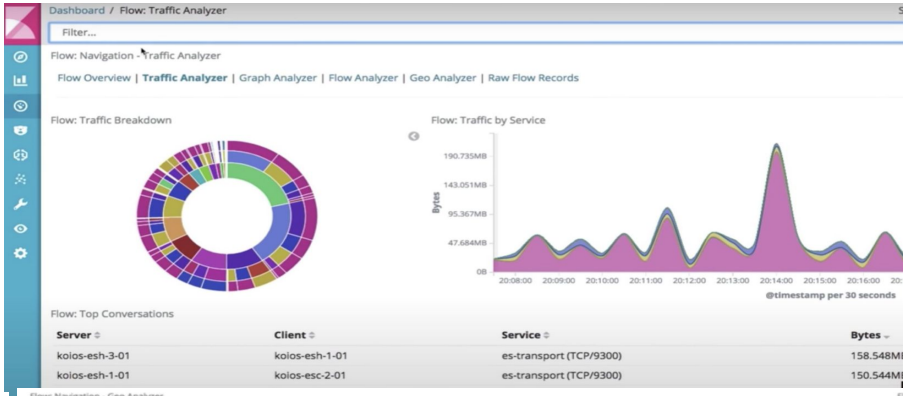
elastic

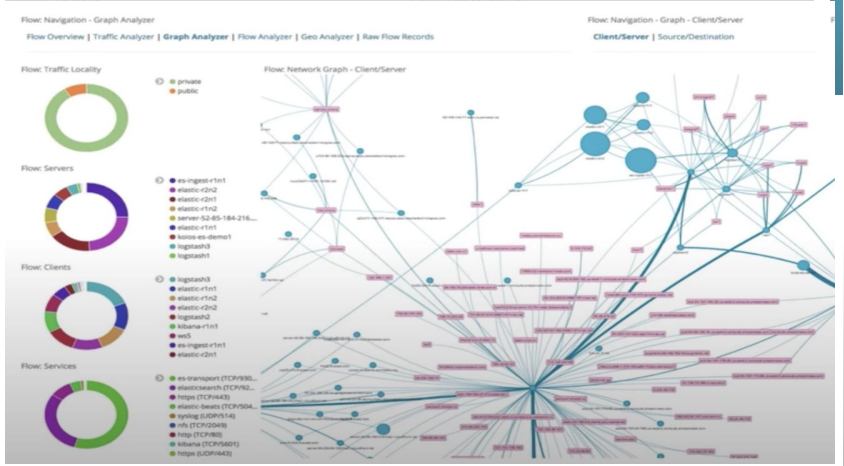
Log,Metric(시스템 성능), APM(애플리케이션 모니터링)

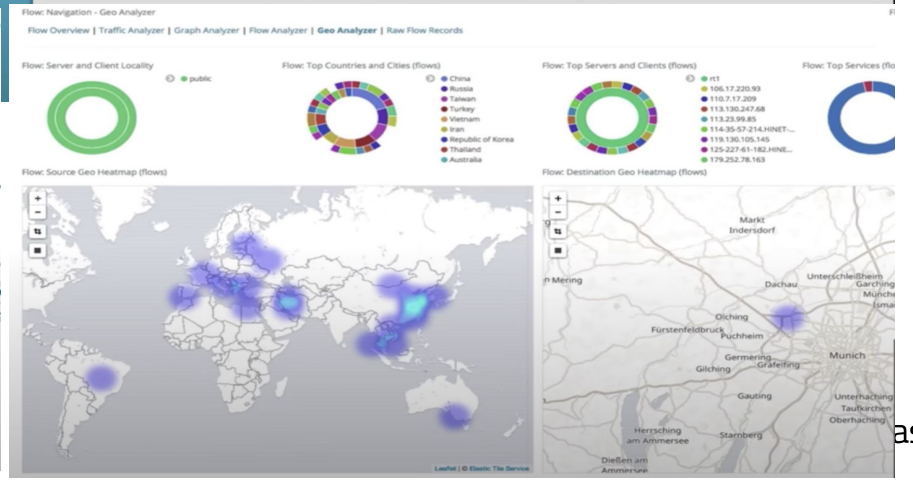


실시간 네트워크 데이터 분석 및 모니터링

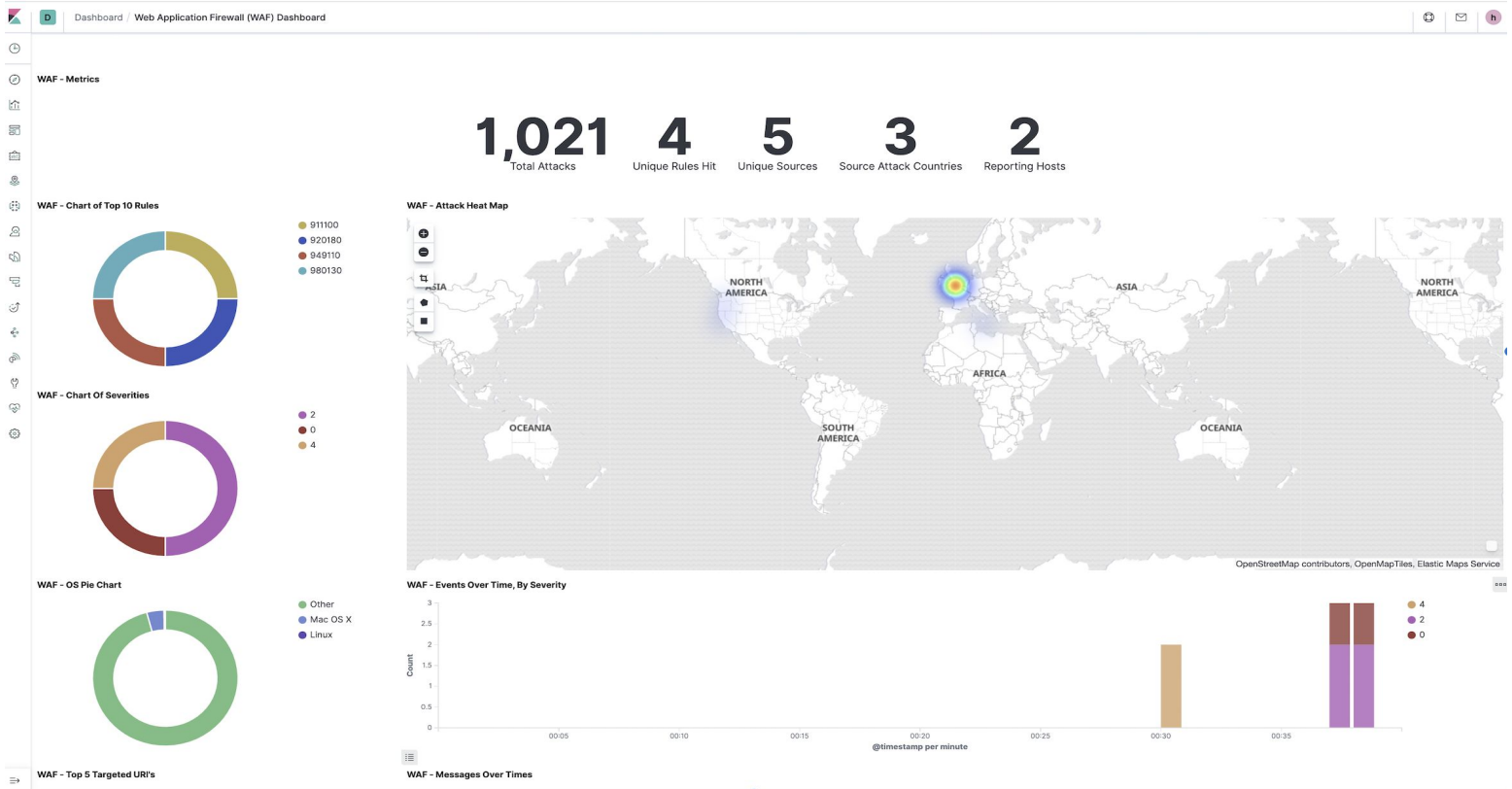




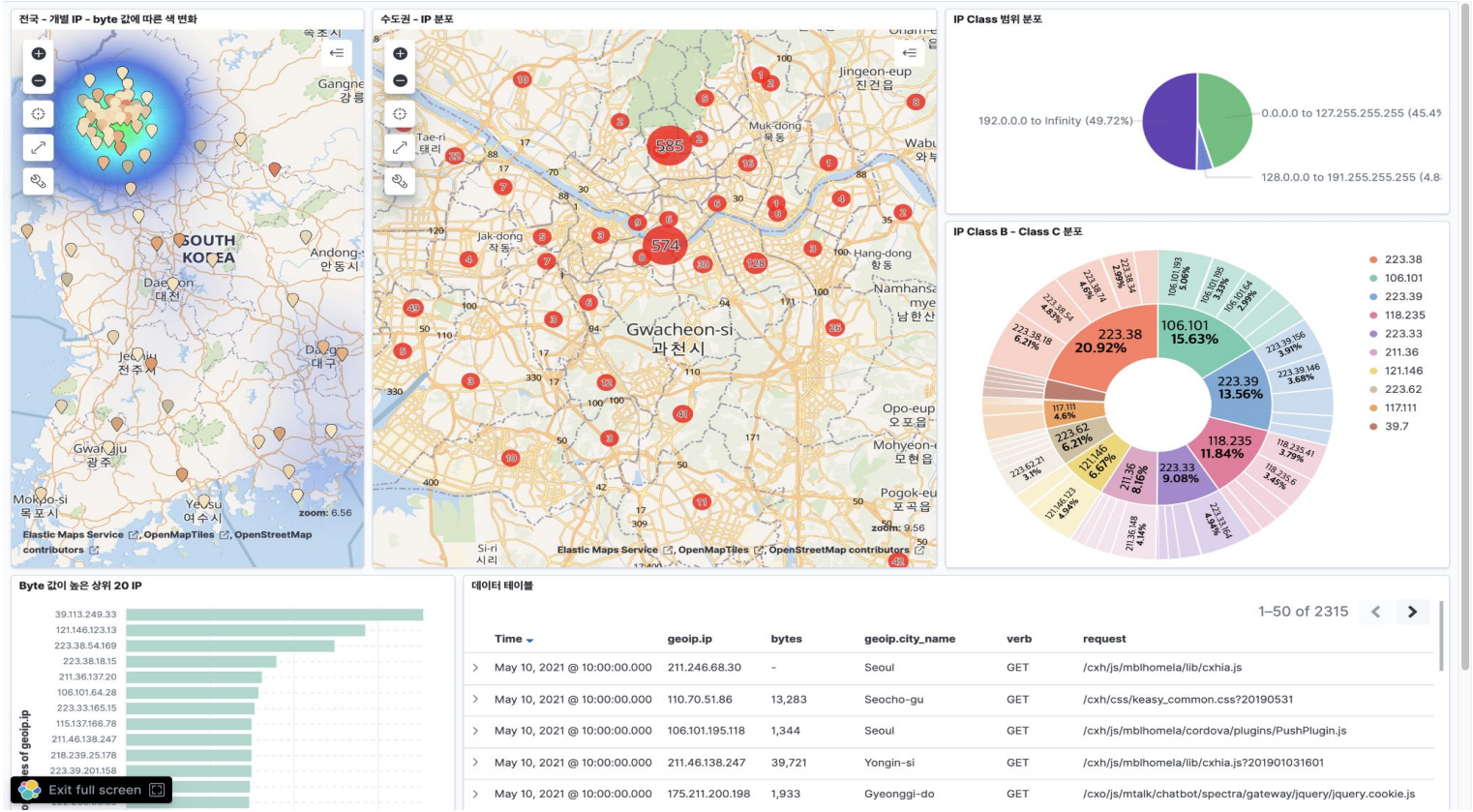




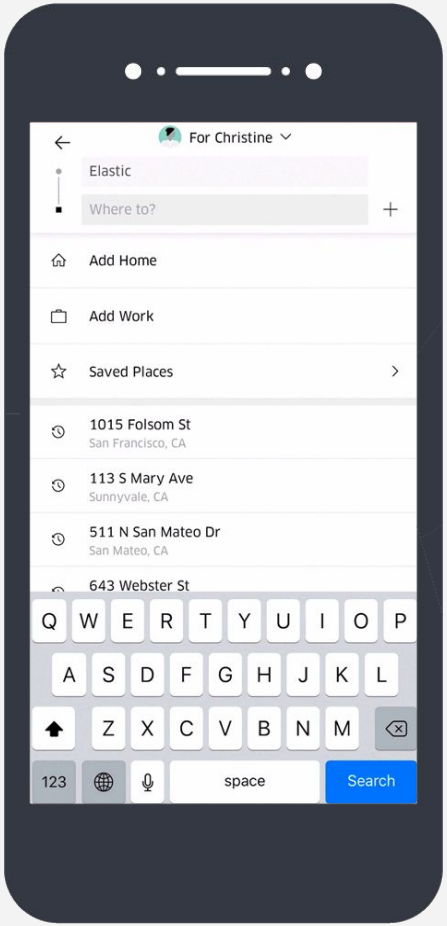
Security 대시보드 - Web Application Firewall(WAF)



Web 로그 내에 있는 IP의 출발지 위치를 지도로 시각화



elastic


For Christine
Elastic
Where to?
Add Home
Add Work
Saved Places
1015 Folsom St
San Francisco, CA
113 S Mary Ave
Sunnyvale, CA
511 N San Mateo Dr
San Mateo, CA
643 Webster St
Q W E R T Y U I O P
A S D F G H J K L
Z X C V B N M
123
space
Search

Uber

이렇게 엄청나게 오래 걸리던 업무를.....엘라스틱 도입후 모두 거의 1초 단위로 해결함

- 장애가 터진후 피해보상을 위해, 작년 2020년 5월부터 6개월간 RDB로 처리하다가 결국 다 못하고 11월에 Elastic 이 들어오며 바로 해결됨

- 타 증권사의 경우, 장애가 발생해도 백데이터 마련 및 조사에 시간이 엄청나게 걸려 확인이 거의 불가능한 상태이며, 이로 인해 보상문제도 우리 시스템에는 문제없다는 식으로 고객에게 통보하는 수준 이로인해 고객 이탈(Churn rate) 증대로 이어짐

elastic

ENTERPRISE SEARCH | 자동차 및 제조 영역

포스코 : 사용자 중심의 Enterprise search 기능 구현을 위한 검색엔진 교체

AT A GLANCE

4 만 명 의 EP 시스템 사용자

8천 5백 만 건의 컨텐츠, 약 200만 건의 등록/변경/삭제

0.9 초의 속도 개선 (더 많은 양의 데이터 관리에도 불구하고 더욱 빨라진 속도)

제공

EP 시스템은 Elasticsearch를 통해 사용자 중심의 서비스를 지원할 수 있는 유연성을 제공받았습니다.

확장 기능

Stack의 다양한 확장 기능을 통해 사용자의 요구사항을 쉽게 처리할 수 있습니다.

빠른 버전 관리

Elasticsearch의 주기적인 version up으로 사용자의 새로운 요구에 대한 대응을 쉽게 할 수 있습니다.

Share

회사 소개(포스코 그룹 EP시스템)

포스코 그룹 EP 시스템은 포스코 및 포스코 그룹사의 업무 시스템으로 기업 포털로서의 인터넷과 기업 내부의 문서, 애플리케이션 및 인터넷 서비스의 게이트 역할을 수행하는 포스코 그룹 통합 인트라넷입니다. EP 시스템의 검색 시스템 운영팀은 검색엔진의 구축 및 운영을 담당하고 있으며, 40,000명(포스코 약 2만명/그룹사 약 2만명)의 포스코 및 포스코 계열사 내의 직원들에게 서비스를 제공하고 있습니다.

포스코IT 사업부 EP운영팀은 Elasticsearch로 검색엔진을 교체하면서 사용자의 만족도에 긍정적인 영향을 미칠 것이라고 판단하고 있습니다. 그들은 Elastic Stack의 다양한 확장 기능들을 이용하면서 다량의 데이터를 컨트롤하고 안정화할 수 있다는 것에 큰 만족감을 느끼고 있습니다. 또한 향후 서버의 장애를 미리 탐지하는 장애 예방 시스템과 사용자 맞춤 검색 등 Elastic Stack의 다양한 기능을 적용하여 프로젝트들을 진행할 예정입니다.

elastic

SECURITY | 소매

위메프: AWS 클라우드 환경의 비정형 위협탐지를 위한 머신러닝 도입

제공

위메프는 보안과 머신러닝을 적용하여 위협을 사전에 탐지하고 있습니다.

머신러닝

머신러닝을 통한 비정형 위협을 사전에 탐지하고 대응할 수 있습니다.

서포트

줌으로 함께 고민하고 연구해서 운영지원을 함께 해주며 긴급 상황의 경우 1시간 내 응답을 해주기 때문에 안정적인 운영이 가능합니다.

Share

회사 소개(위메프)

올해 10주년(2020년 10월 8일)을 앞두고 있는 위메프는 나무인터넷'이라는 사명으로 설립 후 같은 해 '위메이크프라이스닷컴' 사이트를 통해 서비스를 시작했습니다. 초기 사업 모델은 소셜커머스(SNS를 통해 일정 수의 구매 희망자가 모이면, 특정 물건이나 서비스를 할인 받을 수 있는 쿠폰을 공동으로 구매할 수 있는 형태)로 레스토랑, 헤어샵 공연, 놀이동산 입장권 등을 주로 판매했습니다.

위메프는 지난 수년간 모바일 기반 이커머스 가운데 가장 안정적인 손익구조를 유지해왔습니다. 지난해 대규모 투자유치 이후 성장과 손익개선을 모두 크게 향상하기 위해 다양한 시도를 진행하고 있으며, 롱테일 시장의 영향력을 넓히고, 플랫폼을 업그레이드 시키는 등 더욱 현실적인 고객 혜택을 개발해 업계 영향력을 높이는데 집중할 계획입니다.

위메프 클라우드보안운영팀은 위메프 클라우드보안운영팀은 전략사업본부 산하의 보안팀으로서 클라우드플랫폼 서비스의 보안을 전담하는 팀입니다. 해킹과 같은 외부 사이버 공격에 대해 대응하고 내부 취약점을 개선하여 미래의 잠재위협에 대해 선제적대응을 위한 예방활동을 책임집니다. 주된 업무는 보안 수준 고도화를 위한 서비스 기획/구축과 안정적인 서비스를 위한 보안운영 활동을 하고 있습니다.

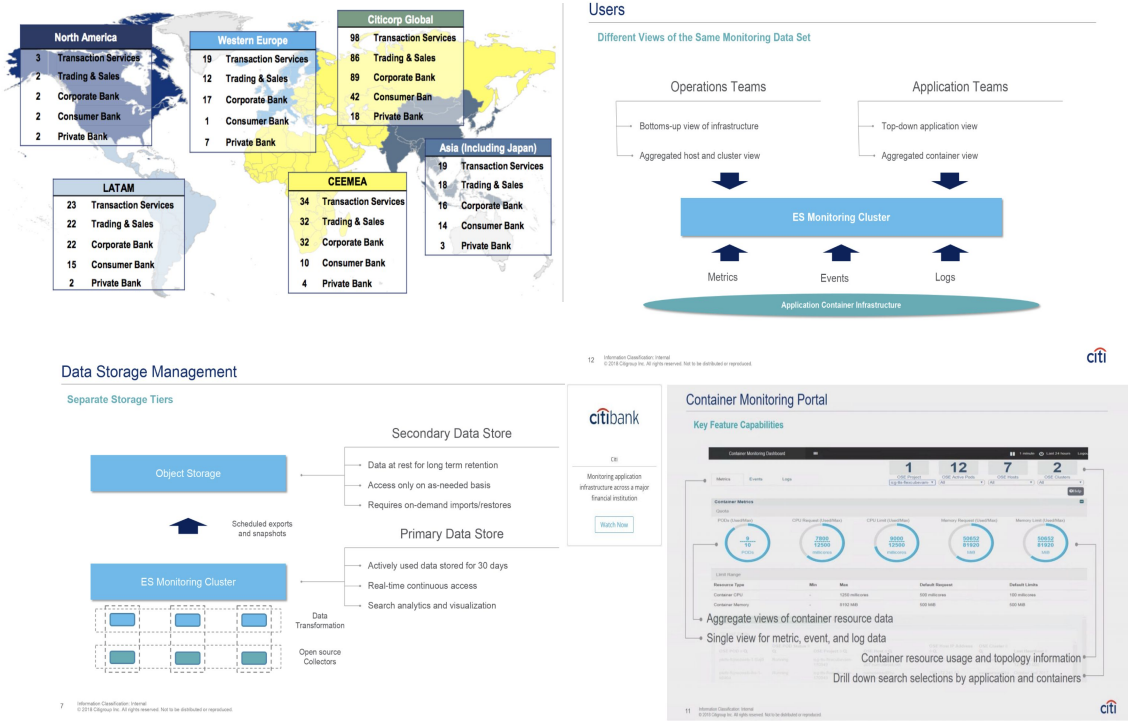
ELASTIC과 함께한 위메프의 머신러닝을 통한 비정형 위협탐지

> **"빅데이터에 대해 평소 관심이 있었고, 또 검색분야에서 Elastic을 많이 사용하는걸 보다보니 이걸 보안에 사용할 수 있지 않을까 하는 호기심에서 시작하게 되었습니다. 위메프가 도입했을 때는 보안 솔루션이라기 보다는 스택을 하나하나 배워가며 찾아가며 그렇게 Elastic을 보안에 적용할 수 있었습니다. 기술지원을 통해서 실시간 문의하고 적용하고 제공되는 문서들을 분석하면서 그렇게 Elastic에 대한 이해도를 높일 수 있었습니다."**
>
> – 정병재 팀장, 이기수 매니저, 위메프 클라우드보안운영팀

The What: 머신러닝, 보안담당자가 제대로 보안을 운영할 수 있는 환경을 분석을 제공한다.

elastic

CITI GROUP (Elastic을 사용한 통합 로그/메트릭 모니터



- 100여 개국에 진출해 있고 160여 개국에서 클라이언트를 보유하고 있는 CitiGroup 전체 시스템 로그/메트릭 데이터를 통합하여 엘라스틱에 저장(30일 보유)후 30일 지나면, 저렴한 secondary 파일시스템에 자동으로 보관

- 엘라스틱 Alerting(Rule-Engine)(이전의 Watcher)을 사용해 컨테이너 인프라 모니터링을 설정함으로써, 모든 부서를 대상으로 컨테이너 메트릭, 이벤트, 로그를 수집하는 시스템을 개발할 수 있었고, 이 정보는 감사 발견사항, 알림 관리, 티켓 발행 등 포함하는 다양하게 활용함

- Kibana를 사용해, 실시간으로 애플리케이션 상태의 집계 보기, 메트릭과 로그의 개별 보기, 컨테이너 리소스 사용 및 토폴로지 정보를 제공하는 대시보드를 생성, 사용자는 애플리케이션이나 컨테이너로 세부적으로 들어가 그 소스에서 문제를 발견할 수도 있습니다. 운영팀과 애플리케이션팀은 데이터를 보는 방법을 뒤집어, 도구 성능을

기업들이 해결해야할 다양한 **Business critical challenges**

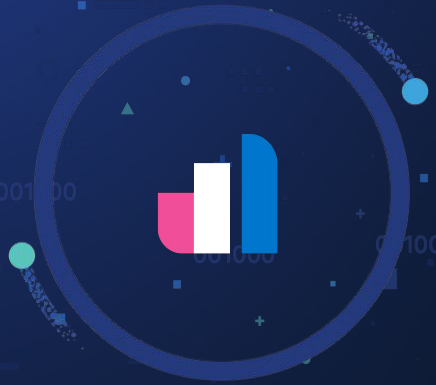
복잡한 **IT**환경의 퍼포먼스를 유지

다양한 해킹시도 및 이에 대한 강력한 방어 및 대응

흩어져있는 다양한 데이터에 대한 빠른 검색

elastic

기업들이 해결해야할 다양한 **Business critical challenges**



IT Observability
is a **data problem**

Cyber Security
is a **data problem**

Enterprise Search
is a **data problem**

elastic

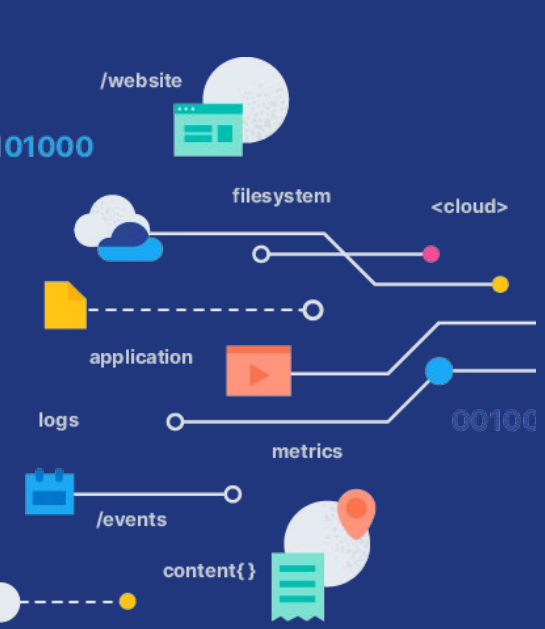
Goldman Sachs

골드만삭스는 1,000명 이상의 Elastic 개발자를 보유하고 있으며 주식매매 정보, 인사정보, 법무 행정 등 다양한 분야에 Elastic 기술을 활용 중

1,000+ developers use the Elastic Stack for use cases from trade tracking to creating new HR and compliance apps.

elastic

One Platform, Three Solutions, Available Anywhere



Observability

Security

Enterprise Search

Kibana
Explore, Visualize, Engage

Elasticsearch
Store, Search, Analyze

Integrations
Connect, Collect, Alert

Public cloud

Hybrid

On-premises

elastic

Elastic customer by Solution

Enterprise Search

Goldman Sachs
GROUPE BPCE
SoftBank Payment Service
RBC Royal Bank®
SwissLife
Rabobank
Cigna

Observability

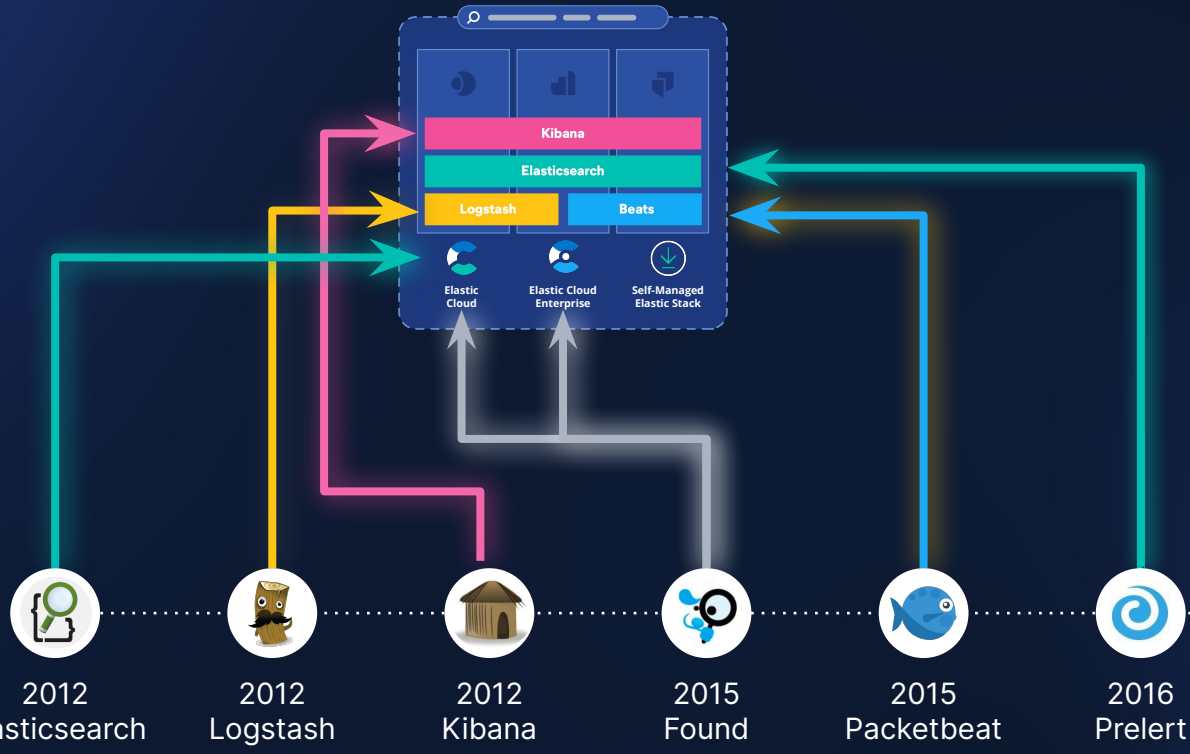
E*TRADE
SWIFT
ZURICH
PSCU
Goldman Sachs
SoftBank Payment Service
Emirates NBD

Security

PSCU
personal CAPITAL
Thought Machine
CREDIT SUISSE
wepay a CHASE company
BARCLAYS
USAA®

Elastic Stack

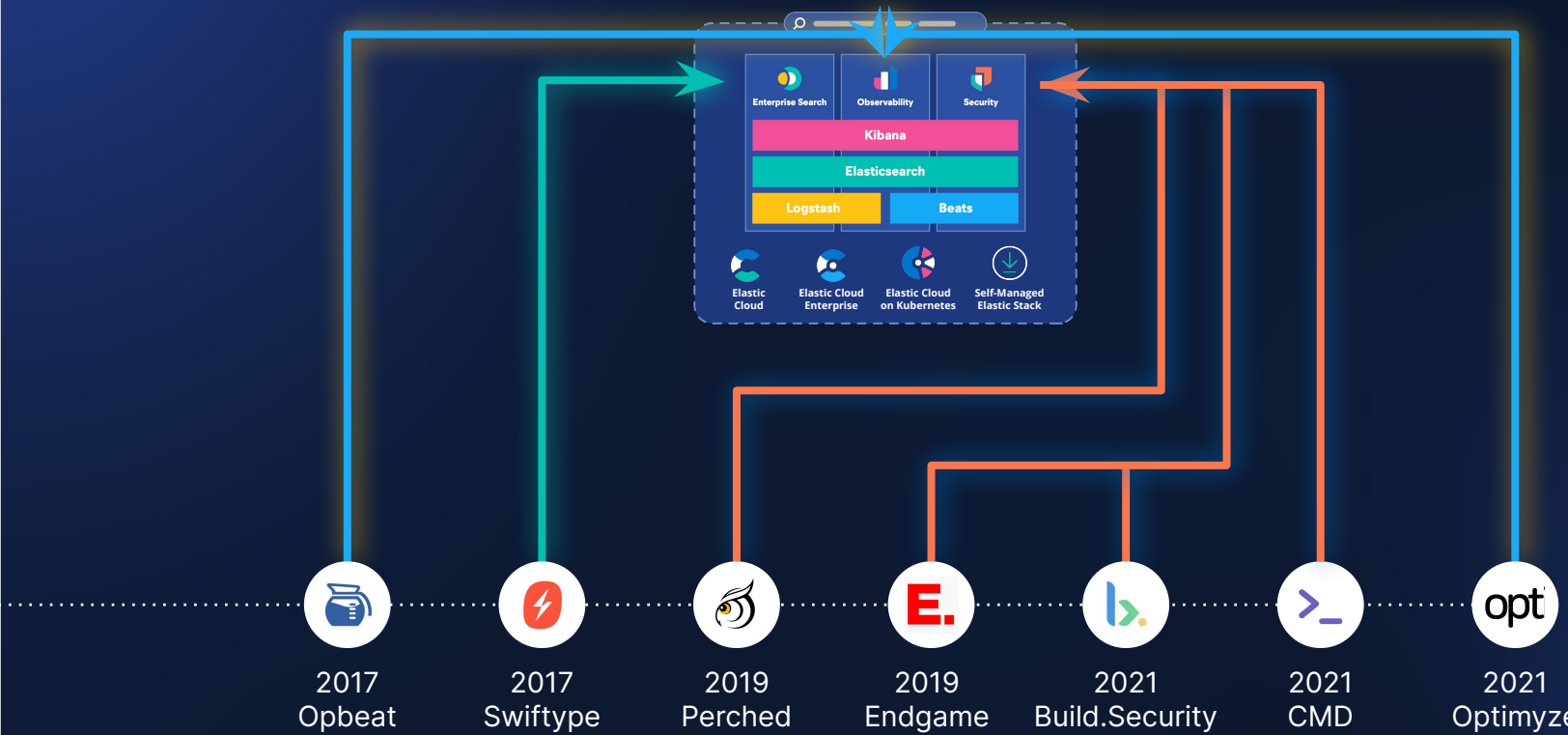
Speed. Scale. Relevance.



elastic

Elastic Solutions

Search. Observe. Protect.



elastic

Elastic named a Leader in The Forrester Wave™: Cognitive Search, Q3 2021.

elastic

Elastic recognized as a Visionary in the 2021 Gartner Magic Quadrant for APM

Figure 1: Magic Quadrant for Application Performance Monitoring

Source: Gartner (April 2021)

Gartner, Magic Quadrant for Application Performance Monitoring, Federico De Silva, Padraig Byrne, Josh Chessman, 9 April 2021

elastic

Elastic named a Visionary in the 2022 Gartner® Magic Quadrant™ for SIEM

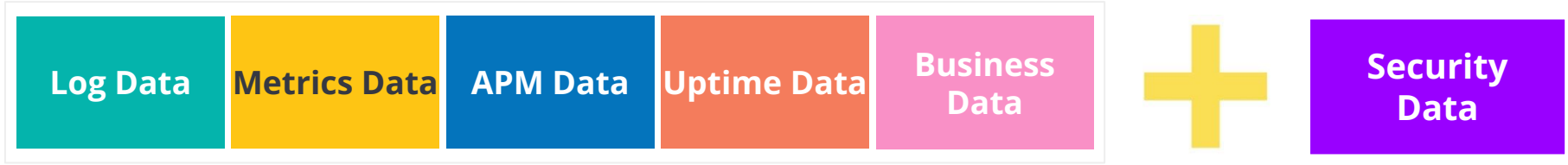
Figure 1: Magic Quadrant for Security Information and Event Management

Magic Quadrant for Security Information and Event Management, Pete Shoard, Andrew Davies, Mitchell Schneider, October 2022

This graphic was published by Gartner, Inc. as part of a larger research document and should be evaluated in the context of the entire document. The Gartner document is available upon request from Elastic.

Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER and Magic Quadrant are registered trademarks and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

elastic



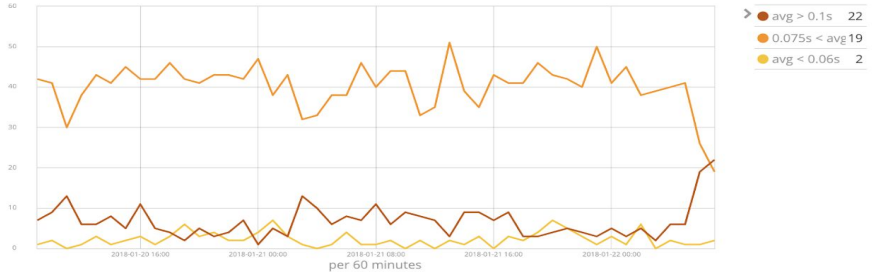
Unified Observability

보안 모니터링 시스템과 운영 모니터링 시스템 간 상호분석 및 탐지 결과 동시 제공 / Single View

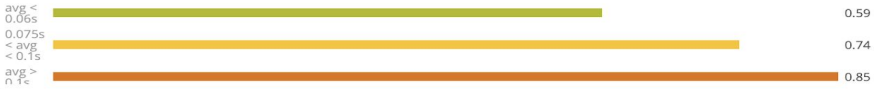
보안 이벤트 모니터링 / 분석	IT 운영 모니터링 / 분석
로그 처리, 파싱 및 저장	실시간 인프라 검색
파일 무결성 모니터링	네트워크 및 인터페이스 사용률
고유한 로그 분석	CPU, 메모리, 디스크 성능 모니터링
인시던트 관리, 티켓팅-대응	가용성 모니터링
리포팅, 컴플라이언스 – 기본/커스텀 제공	스토리지 모니터링
외부 위협 정보 통합	변경관리 모니터링 - 설치된 소프트웨어 구성 및 설정
컴플라이언스 및 보안에 관련된 사전 정의 보고서	인프라 및 사용자 어플리케이션 모니터링
비 정상 룰 및 통계 리포팅	종합 트랜잭션 모니터링

실시간 교차 연관 분석

Elastic{ON} 2018 - Abandon Counts vs Average Response Time



Elastic{ON} 2018 - Abandon Rates vs Average Response Time



Elastic{ON} 2018 - Abandoned Revenue

$186,994.9
Abandoned Revenue

Elastic{ON} 2018 - Abandoned Revenue (Slow Baskets)

$361,519.43
Abandoned Revenue

Elastic{ON} 2018 - Request Times (Converted)

0.80
Average Request Time

1.42
Max Avg. Request Time (secs)

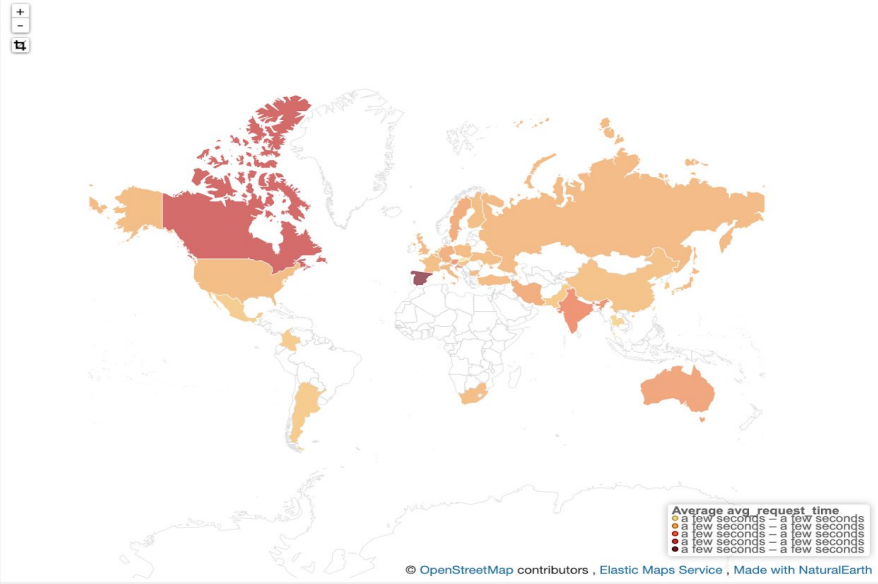
Elastic{ON} 2018 - Request Times (Abandoned)

0.87
Avg. Request Time (secs)

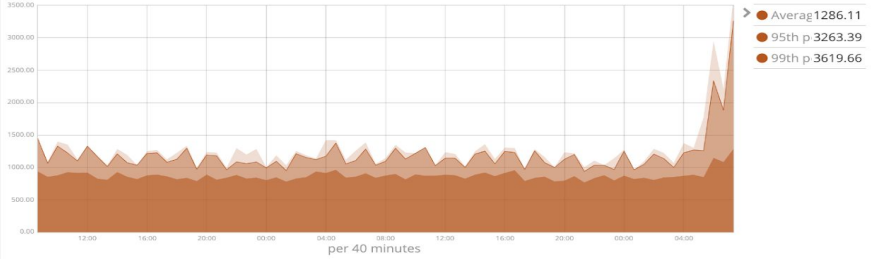
3.62
Max Avg. Request Time (secs)

Elastic{ON} 2018 - Average Request Time Distribution

Elastic{ON} 2018 - Average Performance by Country



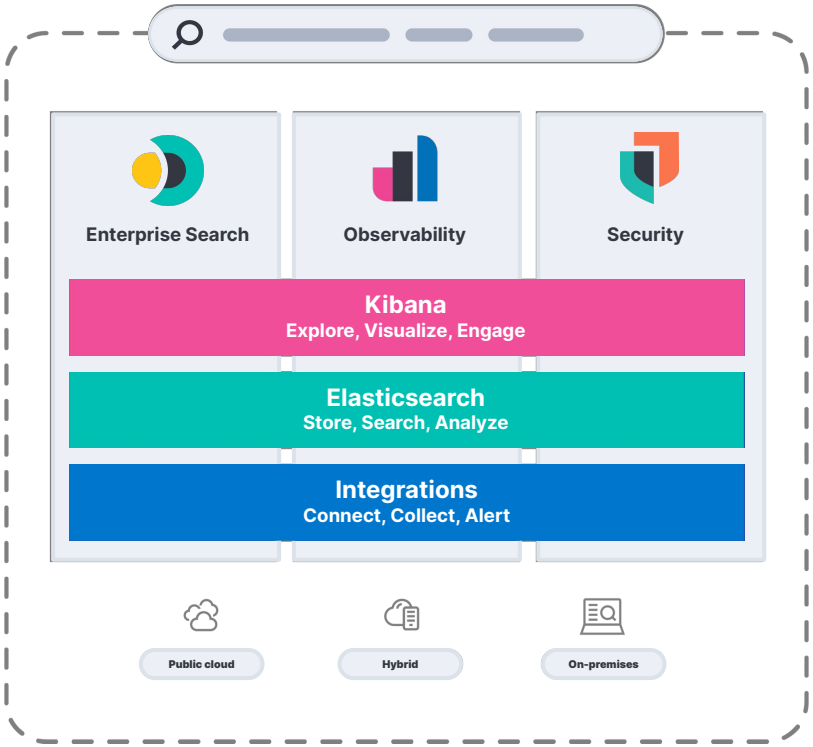
Elastic{ON} 2018 - Performance for Abandoned Baskets



Success through the power of One Platform

Compound the value of customers' data and solutions

- Reduced Total Cost of Ownership (TCO)
- Single tech stack
- Simple, resource-based pricing
- Network effect of data



Elastic Enterprise Search

The gold standard for delivering powerful, modern search experiences

Search Applications

Embedded Search | **Customer Support** | **Marketplace Search**

App Search | **Workplace Search**

Visualize and Explore

Relevance workflows,
pre-configured experiences

Search and Analyze

Vector search, adaptive relevance,
document & search analytics

Ingest Everything

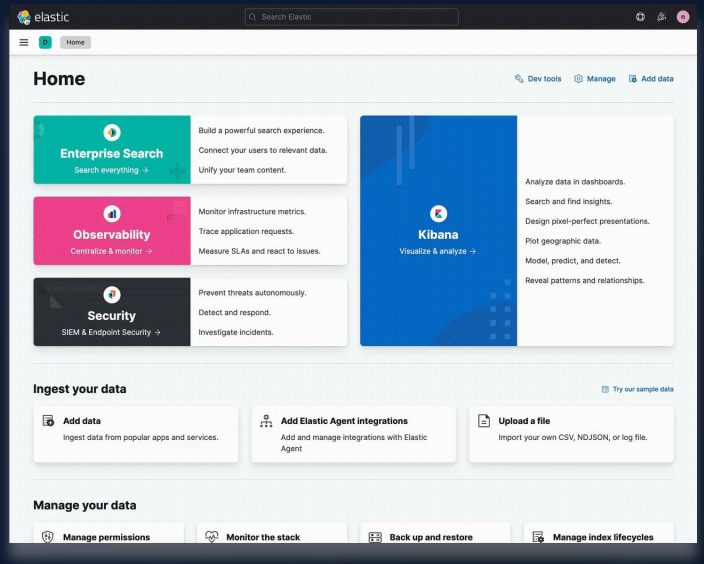
Integrations, crawlers, APIs: database,
content, website, object stores

elastic

Elastic Enterprise Search

어디서든 모든 것을
실시간으로 쉽게 검색할 수
있도록

- **Prebuilt tooling**
- 검색엔진 구축 시간 단축
- 검색 결과 최적화



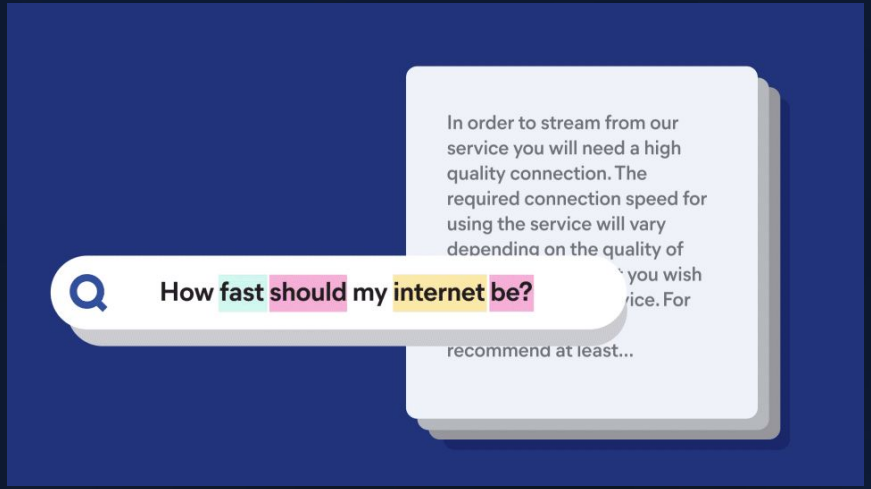
7.0 ····· 7.17

elastic

Elastic Enterprise Search

벡터 검색을 통해 더 나은 검색 결과 제공

- 더 빠르고 정확한 검색 결과
- 검색 사용 사례를 이미지, 오디오 등으로 확장
- 의미론적 의미를 기준으로 데이터 순위 매기기
- NLP(자연어 처리)



7.0 — 7.17 — 8.0 — 8.5

elastic

Elastic Security

Unified SIEM, XDR, endpoint, and cloud security on a single platform

Endpoint | **Cloud**

SIEM / Security Analytics

Continuous Monitoring | **Automated Threat Protection** | **Investigation & Incident Response** | **Threat Hunting**

Visualize and Explore

Interactive visualizations, investigation workflows, automation & response

Search and Analyze

Automated threat detection, machine learning, entity insights

Ingest Everything

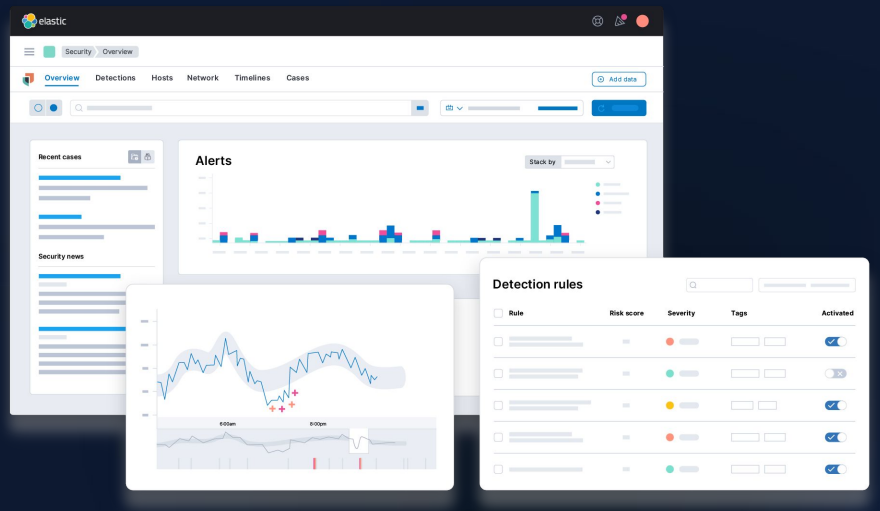
Cloud, app, network, host, user, vulnerabilities, threat intelligence

elastic

Elastic Security

SIEM과 endpoint security 통합 그리고 XDR

- 사각지대 제거
- 탐지 자동화
- 조사 및 대응 간소화
- 랜섬웨어 및 악성 프로그램 방지



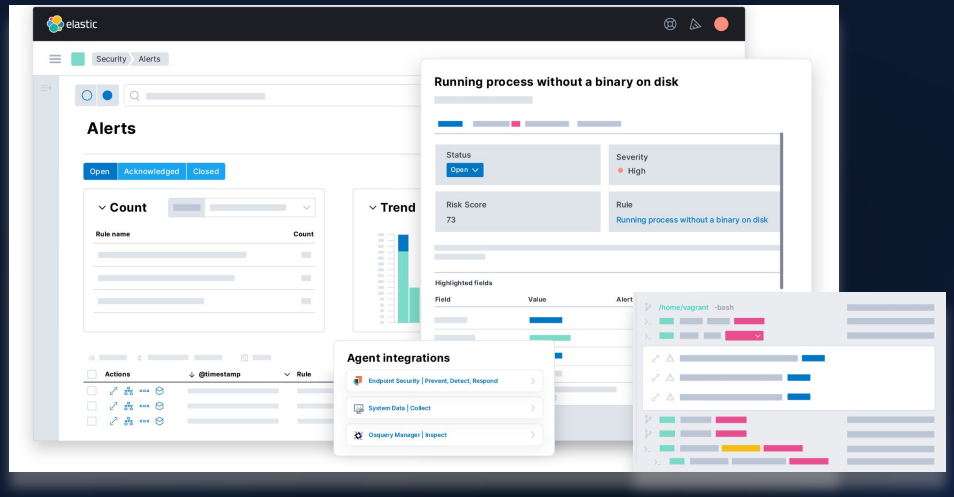
7.0 ..... 7.17

elastic

Elastic Security

위협방지
at enterprise scale

- 가시성 향상
- 분석가 워크플로우 최적화
- 체류 시간 최소화
- 보안 클라우드 워크로드 및 클라우드 보안 벤치마크
- 엔드포인트에서 지능적 위협 중지



7.0 — 7.17 — 8.0 — 8.5

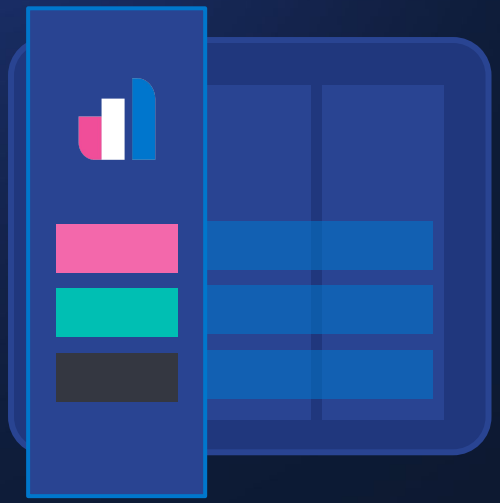
elastic

While many security vendors choose a passive, “wait-and-see” mentality, threats are constantly adapting and evolving, thereby demanding a more proactive approach

“많은 보안 공급업체가 "두고 보는" 사고방식의 수동적인 접근법을 선택하지만, 보안 위협은 지속적으로 적응하고 진화하고 있기에 보다 사전 예방적인 접근을 요구합니다”

elastic

Elastic Observability



Unified observability across your entire digital ecosystem

Logging	APM	Infrastructure Monitoring	Synthetics	RUM + Mobile Monitoring	Continuous Profiling

Visualize and Explore

Unified dev and ops interface, workflow
for accelerated root cause & response

Search and Analyze

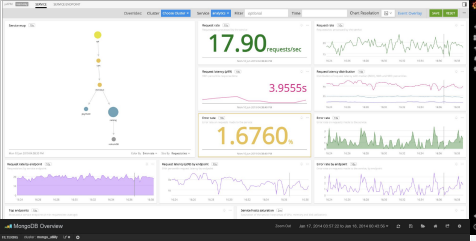
Machine learning and AIOps,
Integrated context at scale across data

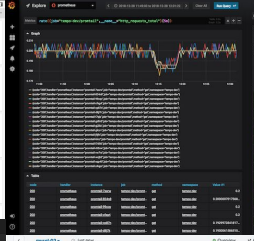
Ingest Everything

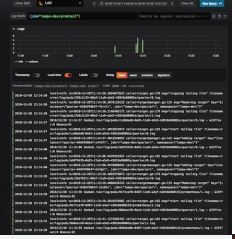
Metrics, logs, traces
OTel, eBPF, Cloud-native

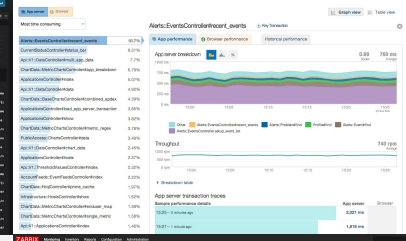
elastic

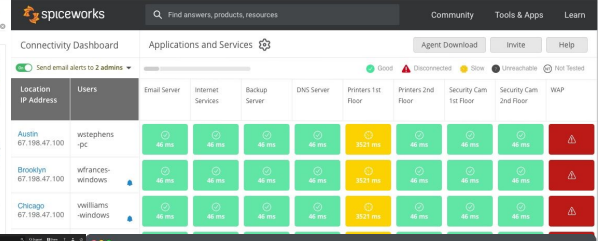
.. 이런 상황에 직면했을때...

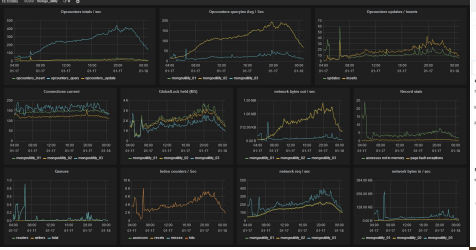

17.90 requests/sec
3.9555s
1.6760%

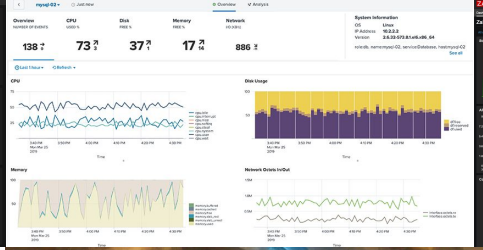


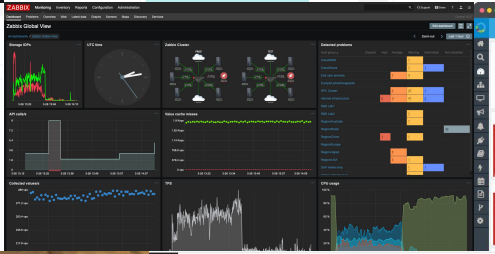


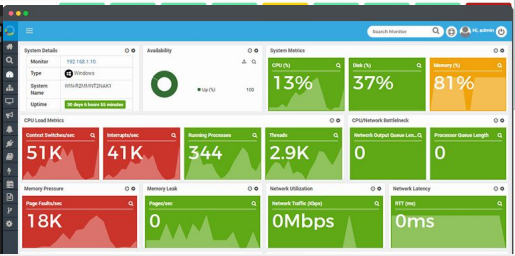



spiceworks
Find answers, products, resources
Community
Tools & Apps
Learn
Connectivity Dashboard
Applications and Services
Agent Download
Invite
Help
Send email alerts to 2 admins
Good
Disconnected
Slow
Unreachable
Not Tested
Location
IP Address
Users
Email Server
Internet Services
Backup Server
DNS Server
Printers 1st Floor
Printers 2nd Floor
Security Cam 1st Floor
Security Cam 2nd Floor
WAP
Austin
67.198.47.100
wstephens
-pc
Brooklyn
67.198.47.100
wfrances-
windows
Chicago
67.198.47.100
swilliams
-windows


MongoDB Overview

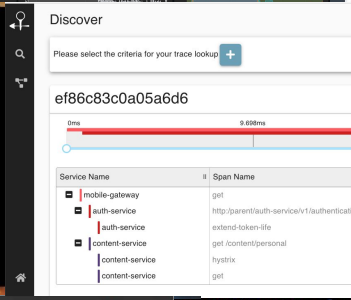


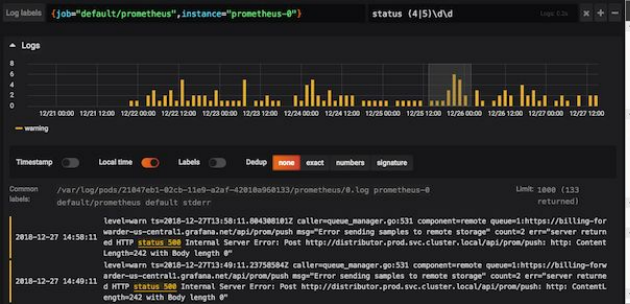

ZABBIX
Zabbix Global View

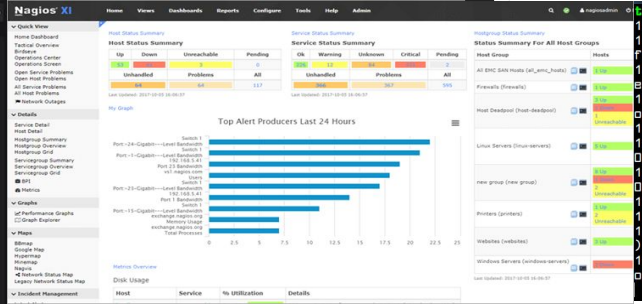

System Details
Availability
System Metrics
CPU (%)
13%
Disk (%)
37%
Memory (%)
81%
CPU Load Metrics
Context Switches/sec
51K
Interrupts/sec
41K
Running Processes
344
Threads
2.9K
Network Output Queue Len...
0
Processor Queue Length
0
Memory Pressure
Memory Leak
Network Utilization
Network Latency
Page Faults/sec
18K
Pages/sec
0
Network Traffic (Kbps)
0Mbps
RTT (ms)
0ms

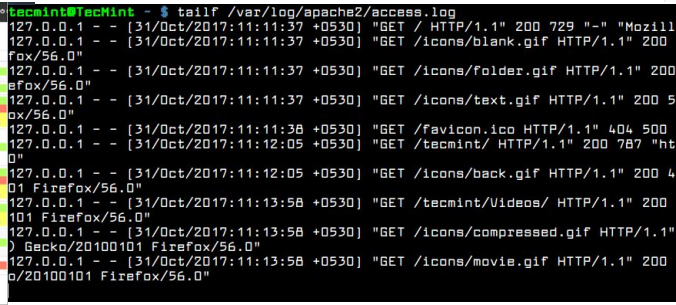

Screen Overview
1.22M
1.26M
1.26M
270.38
210.51
201.57
89.56/s
91.45/s
92.55/s
76.60M
2.15M
241.89


7015c90 (HEAD, origin/master, origin/HEAD, master) Updated iPhones graphic with new screenshot (11 days ago) <OiNutter>
9bfa521 - Updated README (2 weeks ago) <OiNutter>
dd1b895 - Updated to new design (2 weeks ago) <OiNutter>
b2e36c6 - Added fallback for missing avatar (2 weeks ago) <OiNutter>
8678978 - Removed Disk caching of avatar (6 weeks ago) <OiNutter>
39d2c3c - Preparing for App Store submission (9 weeks ago) <OiNutter>
4f6f76c - Fixed call bg when user only has 1 badge. (9 weeks ago) <OiNutter>
13bf363 - Fix image (10 weeks ago) <OiNutter>
705363e - Try screenshots with transparent background (10 weeks ago) <OiNutter>
bd4602e - Correct image location in README (10 weeks ago) <Will McKenzie>
4434b5b - Added iPhone screenshots to README (10 weeks ago) <OiNutter>
2d7d6df - Adding license (10 weeks ago) <OiNutter>
d6c6660 - Adding to .gitignore (10 weeks ago) <OiNutter>
8e2af71 - Still trying to ignore UserInterfaceState file (10 weeks ago) <OiNutter>
cca3d38 - Ignore interfaceState file (10 weeks ago) <OiNutter>
2b1e812 - Added first draft of README (10 weeks ago) <OiNutter>
38586be - Bug fixes and UI Improvements. New Icons added (2 months ago) <OiNutter>
968da0c - Removed extra app icons (3 months ago) <OiNutter>
ecf783e - Various updates (3 months ago) <OiNutter>
6ce53d3 - Removed SOURL files from root (3 months ago) <OiNutter>
62e0679 - Made sure images cache (3 months ago) <OiNutter>
1397df2 - Ran Arc conversion to improve memory management. Refactoring and bug fixes (3 months ago) <OiNutter>
c3003ab - Added pull to refresh functionality (3 months ago) <OiNutter>
9266166 - Made sure iPhone badge and accomplishments view controllers reload when user changed. (3 months ago) <OiNutter>
83cd921 - Stopped badges images using separate threads. (3 months ago) <OiNutter>


Discover
Please select the criteria for your trace lookup
Trace ID
trace id...
10
1 HOUR
ef86c83c0a05a6d6
Duration: 38.793ms
Services: 3
Depth: 3
Total Spans: 6
0ms
9.698ms
19.396ms
29.095ms
38.793ms
Service Name
Span Name
0ms
76.504s
153.009s
229.513s
306.017s
mobile-gateway
get
38.793ms
auth-service
http:/parent/auth-service/v1/authenticati...
14.077ms
auth-service
extend-token-life
1.291ms
content-service
get /content/personal
20.333ms
content-service
hystrix
863µs
content-service
get
8.965ms


Logs
warning
Timestamp
Local time
Labels
Dedup
none
exact
numbers
signature


Nagios XI
Host Status Summary
Service Status Summary
Hostgroup Status Summary
Top Alert Producers Last 24 Hours
Disk Usage


tecmint@TecMint ~ $ tailf /var/log/apache2/access.log
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET / HTTP/1.1" 200 729 "-" "Mozil
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/blank.gif HTTP/1.1" 200
fox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/folder.gif HTTP/1.1" 200
efox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:37 +0530] "GET /icons/text.gif HTTP/1.1" 200 5
ox/56.0"
127.0.0.1 - - [31/Oct/2017:11:11:38 +0530] "GET /favicon.ico HTTP/1.1" 404 500
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /tecmint/ HTTP/1.1" 200 787 "ht
0"
127.0.0.1 - - [31/Oct/2017:11:12:05 +0530] "GET /icons/back.gif HTTP/1.1" 200 4
01 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /tecmint/Videos/ HTTP/1.1" 200
101 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /icons/compressed.gif HTTP/1.1"
) Gecko/20100101 Firefox/56.0"
127.0.0.1 - - [31/Oct/2017:11:13:58 +0530] "GET /icons/movie.gif HTTP/1.1" 200
0/20100101 Firefox/56.0"

현재 모니터링 환경의 한계점 및 신규 시스템 도입 배경

- 시스템문제 발생시 DB문제인지 서버문제인지 네트웍문제인지 파악이 어렵고 파악하는데 많은 시간 소요
- 고객서비스에 장애가 10분이상 지속되면 금감원에 보고해야하고 금감원에서 시찰이 나오면 업무에 막대한 지장 초래
- DB, 서버, 네트웍, Application 등 각각의 모니터링 Tool은 갖고 있으나 통합해서 보기 어려움. 이로인해 즉각적인 대응이 어려움
- 장애가 발생하기전 이상치에 대한 가시성이 없어 실제 장애로 이어지기 전에 사전에 손을쓸수있는 환경이 마련되어 있지 않음

elastic

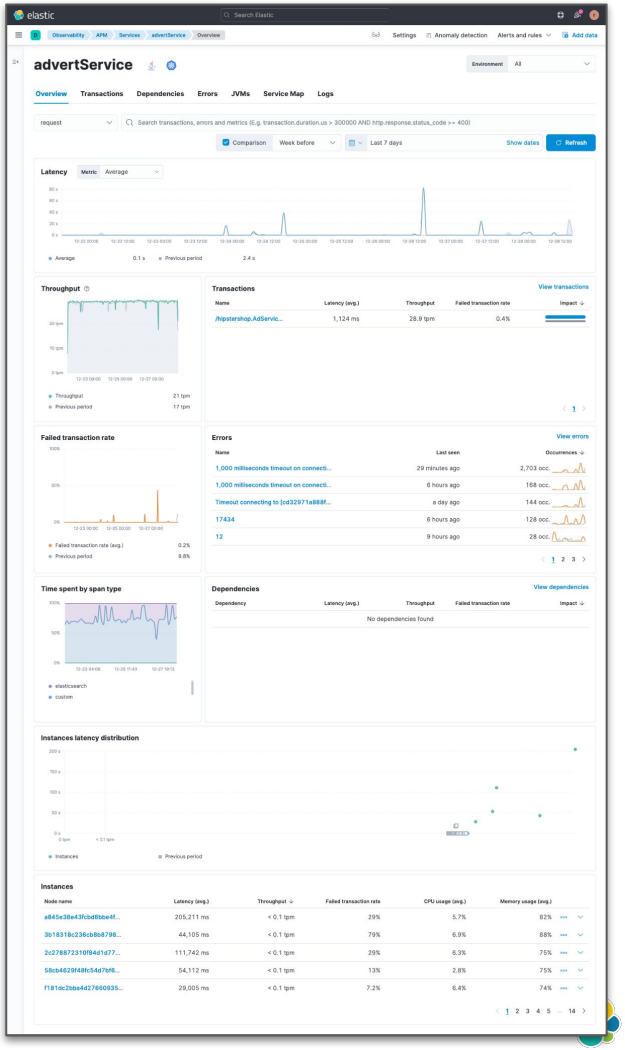

Dashboard
[System_log] Sytem_log 수집현황
Search
+ Add filter
Overview | Top 10 | Log view | 수집현황
1,038,190
log 수
63
111
linux host 수
emerg count
Emergency
0
alert count
Alert
45
critical count
Critical
54,984
error count
Informational
785,662
Debug
0
SAMPLE
DASHBOARD
호스트 이름
Count
ldsms201r 218,589
dcamws1 147,128
dcbsap1 99,080
dnibig1 83,181
lxums301r 83,037
dbcsnd1 60,018
lxums301d 24,608
dniber1 23,979
dnibws1 22,994
r_pcbsap1 21,834
Count of records
@timestamp per 3 hours
alert
warning
notice
critical
error
Informational

서비스 오버뷰

서비스와 관련된 모든 것을 한 눈에

한 서비스에 대해 다음과 같은 질문에 답을 얻음

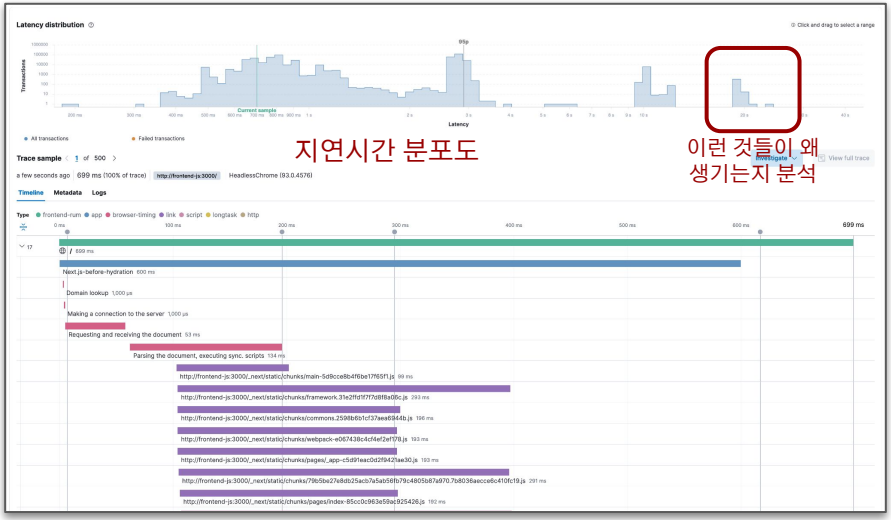
- 어떤 엔드포인트/트랜잭션에 성능 문제가 있는가?
- 서비스 전체 성능에 가장 큰 영향을 주는 트랜잭션은?
- 어떤 에러가 가장 빈번히 발생하는가?
- 이전 대비 에러 발생빈도가 어떤 차이를 보이는가?
- 서비스 기술 구성 요소 중 어디가 가장 정체인가?
- 이 서비스는 어떤 다른 서비스 또는 백엔드에 의존하는가?
- 서비스와 의존관계에 있는 다른 서비스들의 성능 상태는?



elastic

분산 트레이싱

서비스와 관련된 모든 것을 한 눈에



선택한 요청이 거쳐가는 서비스 목록

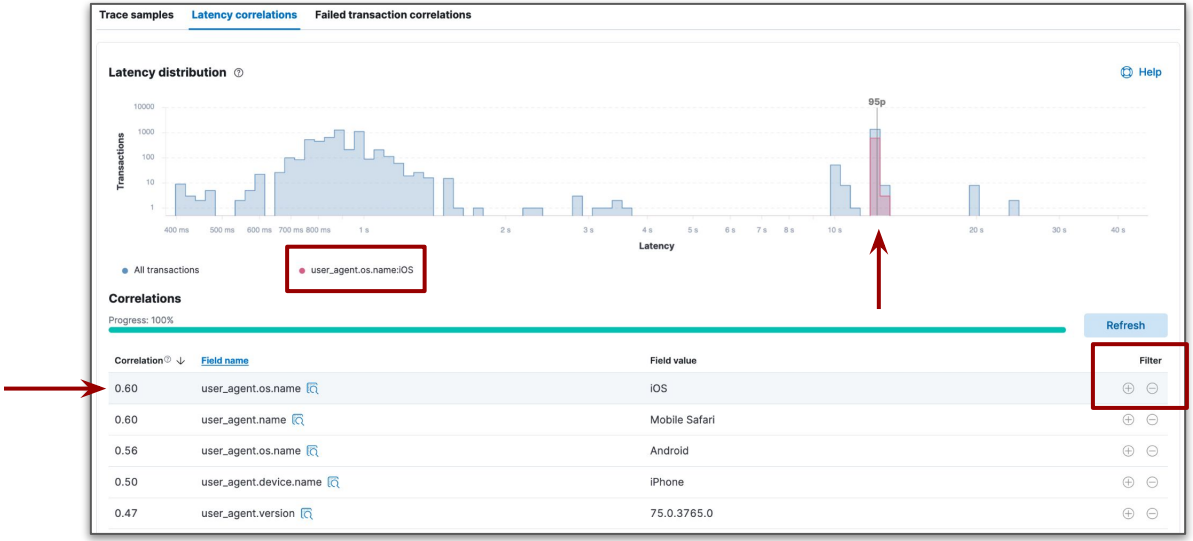
- 엔드투엔드: 사용자 요청이 전체 서비스를 어떻게 가로질러 가는지 한눈에 표시
- 연결된 다수 서비스를 색깔로 구분, 병목/지연 지점 신속 파악
- 트레이스와 관련된 파드, 컨테이너, 호스트의 로그와 메트릭 데이터 즉시 조회
- 각 트레이스 클릭시 세부 정보 표시
  - 메트릭: 지연시간, 통신 내역
  - 상세 정보: 오류 정보, DB 구분
  - 메타 정보: 인프라 정보, 프로토콜

elastic

지연시간 상관도 Latency Correlation

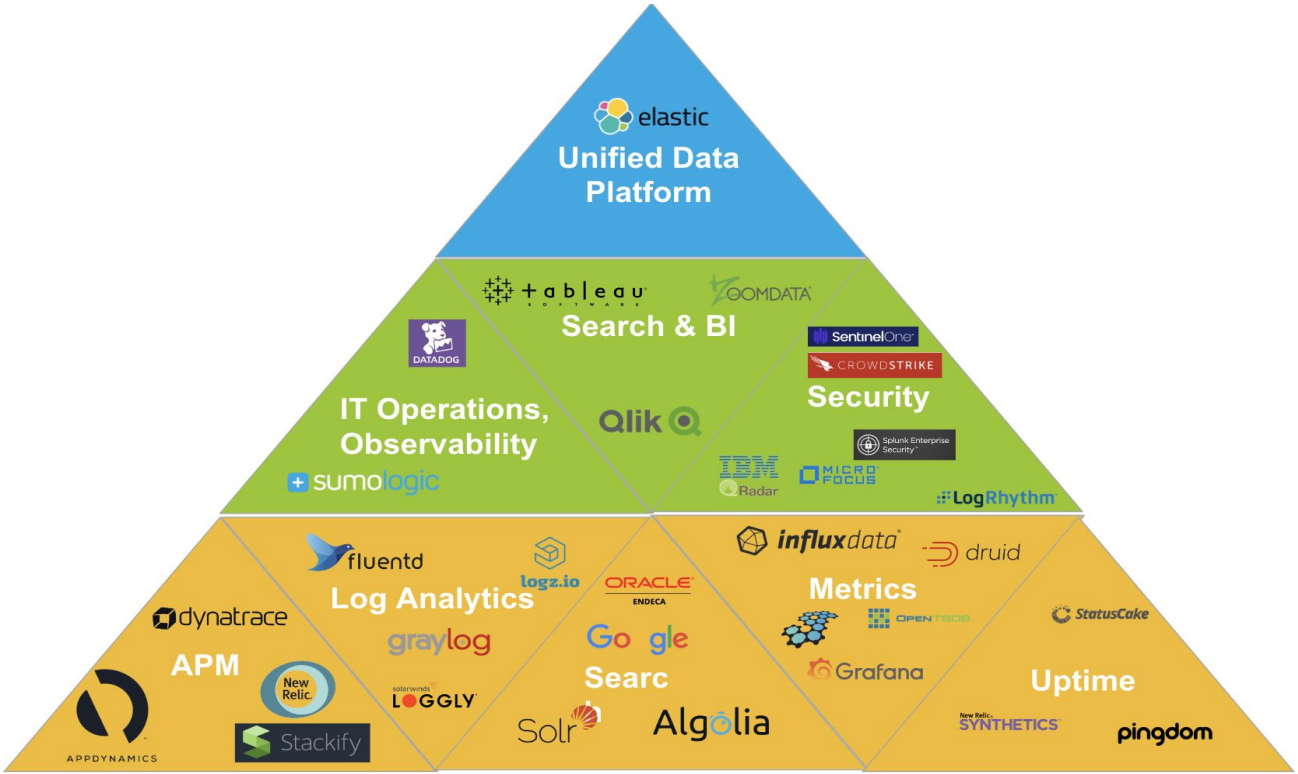
지연시간이 발생한 원인을 자동으로 분석하여 찾아 줌

- Correlation: 0~1 사이의 숫자로 클수록 지연시간에 영향을 많이 줬음을 의미
  - 어떤 변수가 성능 저하에 영향을 주는지 자동으로 찾아 시각적으로 표시
  - 문제의 변수(예, iOS에서 요청된 트랜잭션)를 필터링하여 검증
  -



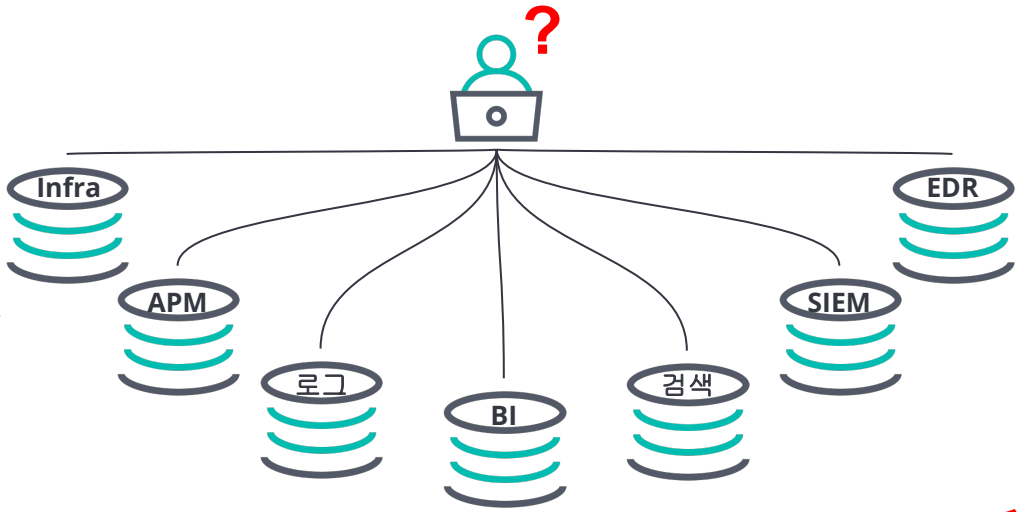
elastic

하나의 플랫폼으로 모든 종류의 데이터를 쿼리,집계,분석



elastic elastic

개별 솔루션 구축 시



- 개별 솔루션 과금 체계 상이 및 각각의 라이센스 선정 & 구매 필요
- 개별 솔루션 구축/유지보수/기술지원 비용 발생 및 솔루션 별 전문 인력 필요
- 부서별/팀별 silo 현상과 빈번한 데이터/리포트 불일치 현상 발생
- 개별 기능/ 데이터 저장 주기 추가에 따른 별도 비용 발생 및 높은 데이터 유실 가능성

VS

Elastic 도입 시

- 하나의 스택으로 구현하는 올인원 솔루션
- 데이터사이즈 과금 정책으로 무분별한 비용발생 X
- On-prem/Cloud에 상관없는 구축 형태 제공
- 라이센스 비용안에 포함된 국문 기술지원 서비스

elastic

감사합니다.

김관호 상무 (jeremy.kim@elastic.co)
Elastic
elastic.co/kr
usersuccess-kr@elastic.co