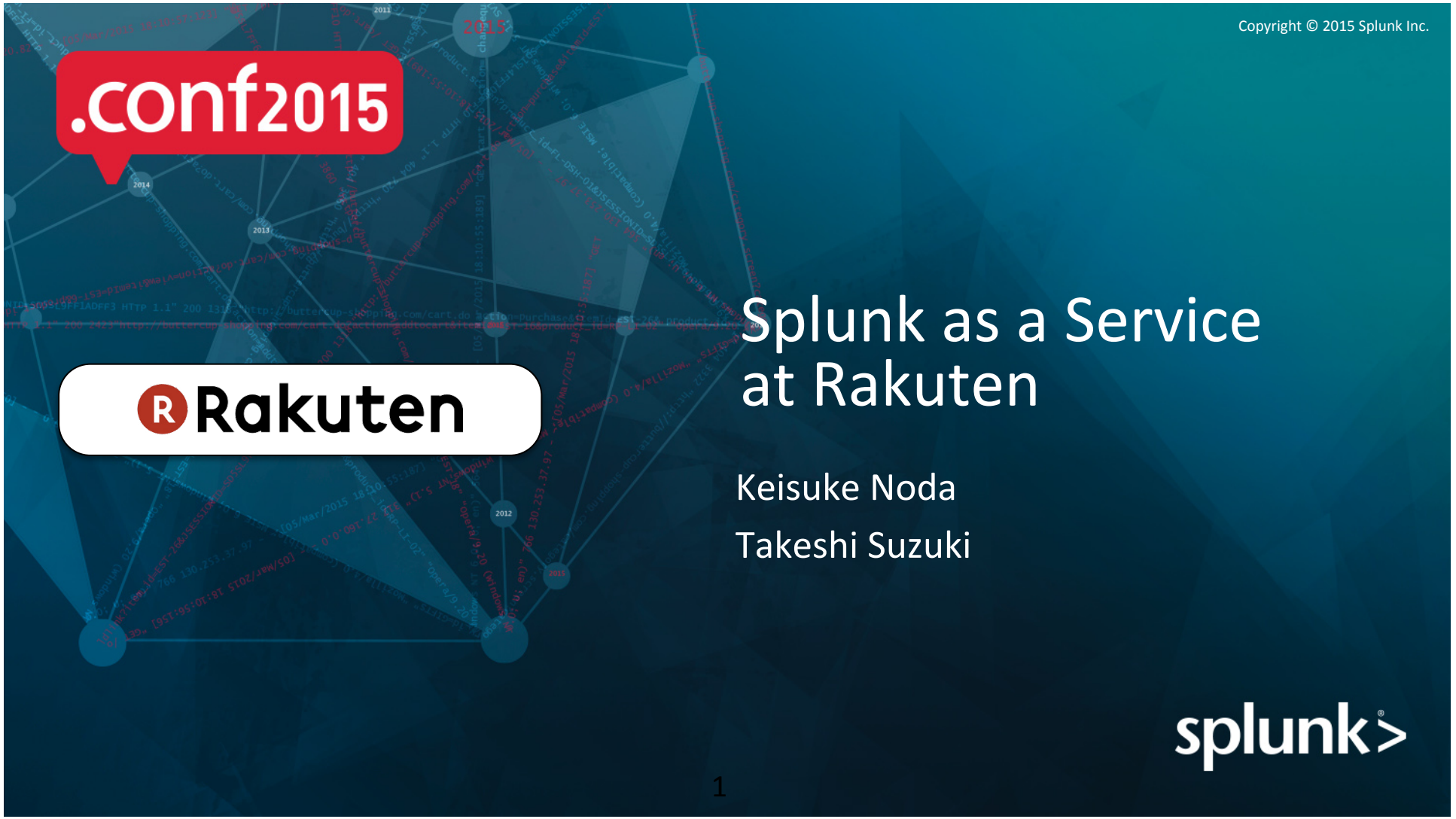


Splunk as a Service at Rakuten

Keisuke Noda

Takeshi Suzuki

splunk>

Disclaimer

During the course of this presentation, we may make forward looking statements regarding future events or the expected performance 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 could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC. 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, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward looking statements we may make.

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 functionality described or to include any such feature or functionality in a future release.

About Us

- Name
  - Keisuke Noda
  - 野田 啓介
- Position
  - Architect / Manager
  - Data Store Platform Group
- Background
  - Application engineer
  - Database engineer

About Us

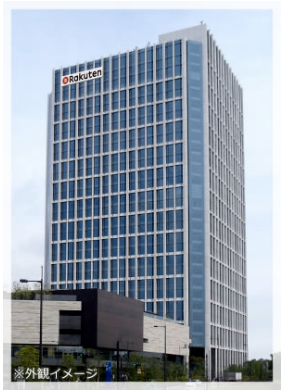
Rakuten

- Takeshi Suzuki
- 鈴木　武
- Tokyo

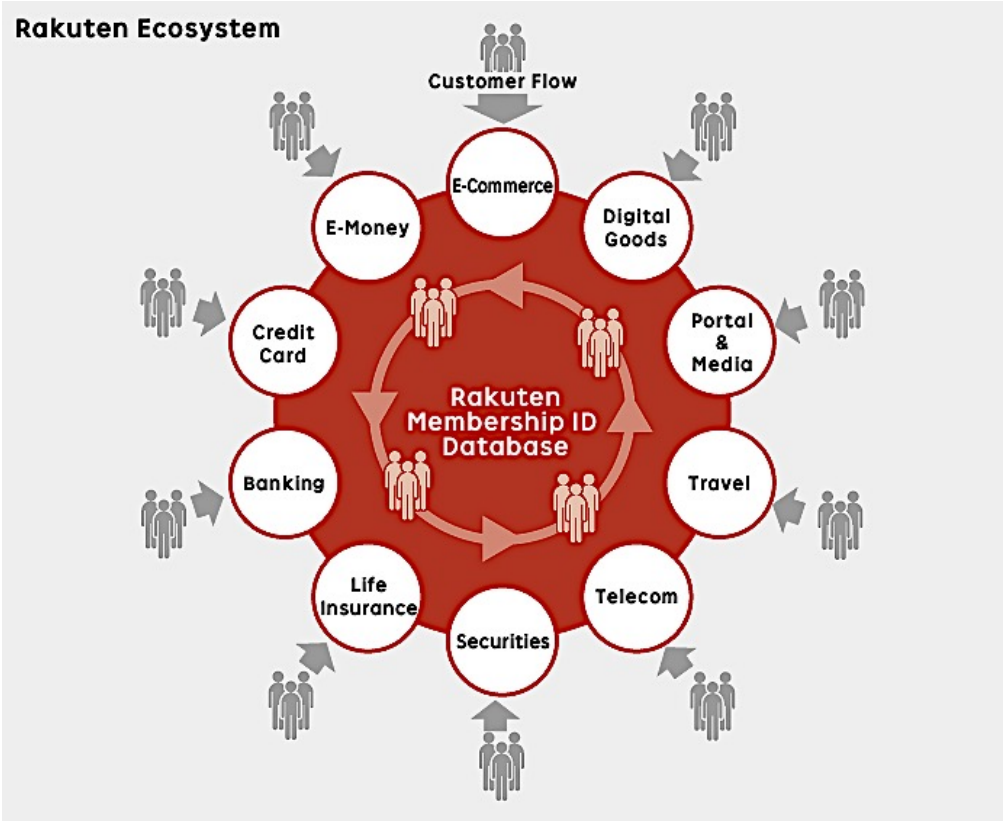
- Rakuten, Inc.
- Security Operations Group
- Security engineer / Manager

About Company

Founded:	**February 7, 1997**
IPO:	**April 19, 2000 (JASDAQ Stock Exchange)**
Office:	**Rakuten Tower (Tokyo, Japan)**
Employees:	**12,288 (as of June, 2015)**
Market Cap:	**JPY 214,701 million (as of Sep 15, 2015)**



About Company



Going Global

Agenda

- Why Splunk?
- Why is Splunk offered as a Service?
- Service Overview
- Our Challenges
- Current Status
- Case Studies
- What's Next?
- Wrap up
- Q and A

Why Splunk?
Why is Splunk offered as a Service?

splunk>

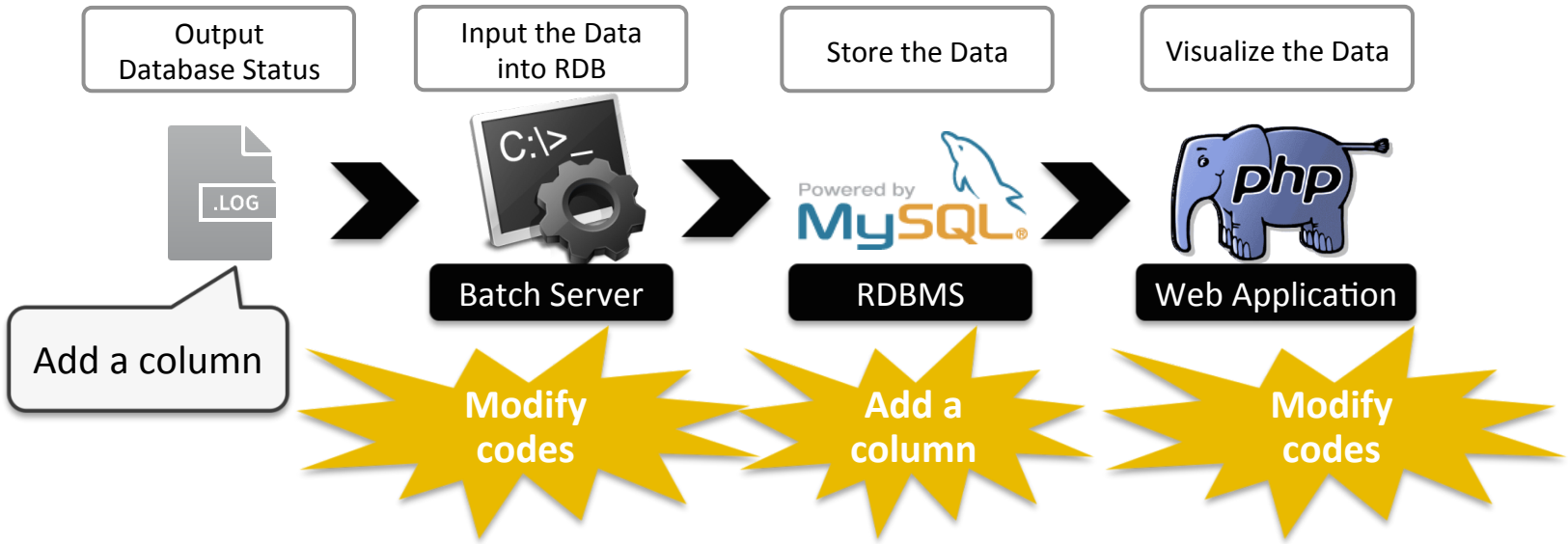
Why Splunk?

- Summer 2011… I discovered Splunk
  - Cool visuals
  - Looks interesting

Why Splunk?

Before

- Self-made database monitoring system
  - Legacy and complex system



Why Splunk?

After

- Self-made database monitoring system
  - One Splunk is simple

Then, Splunk began to be used in various groups…

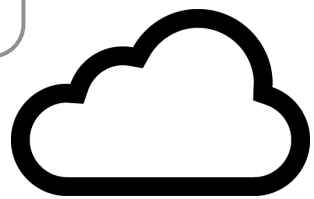
Why is Splunk offered as a Service?

- Splunk began to be used in various groups
  - There were so many repetitive operations
    (such as license management, system constructions, operations …etc)

If there is one big platform and everyone can use it without management, the problem will be solved.

In addition, it may have many other benefits…

. . . Splunk as a Service was born

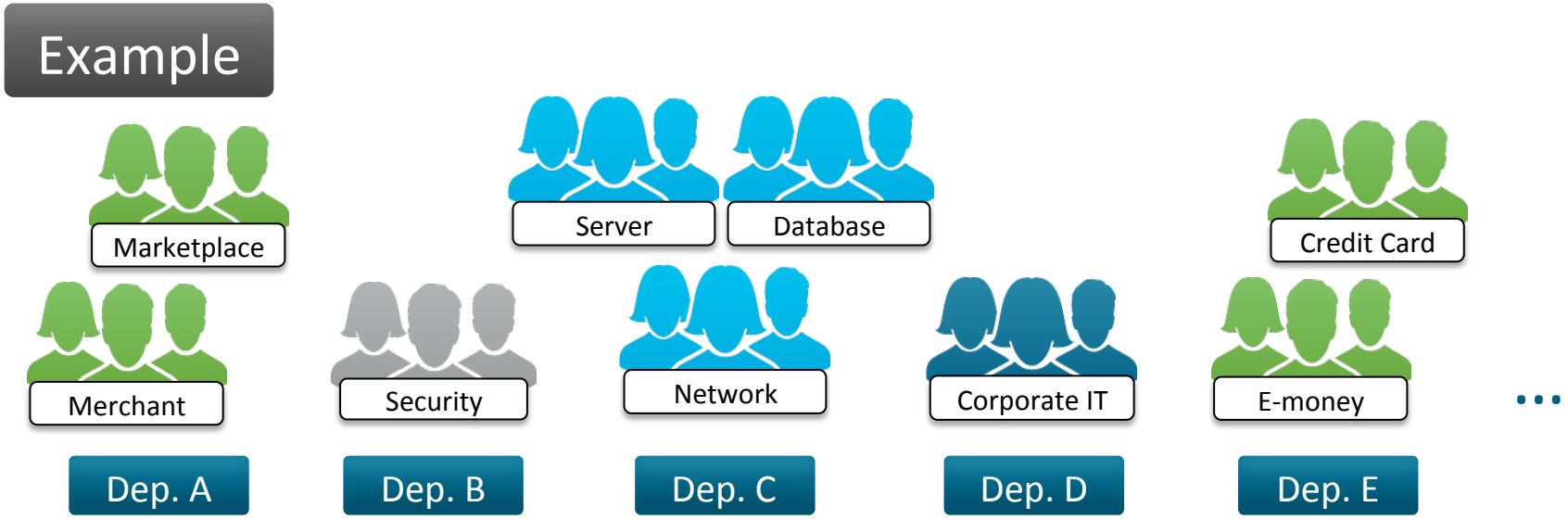


Service Overview

splunk>

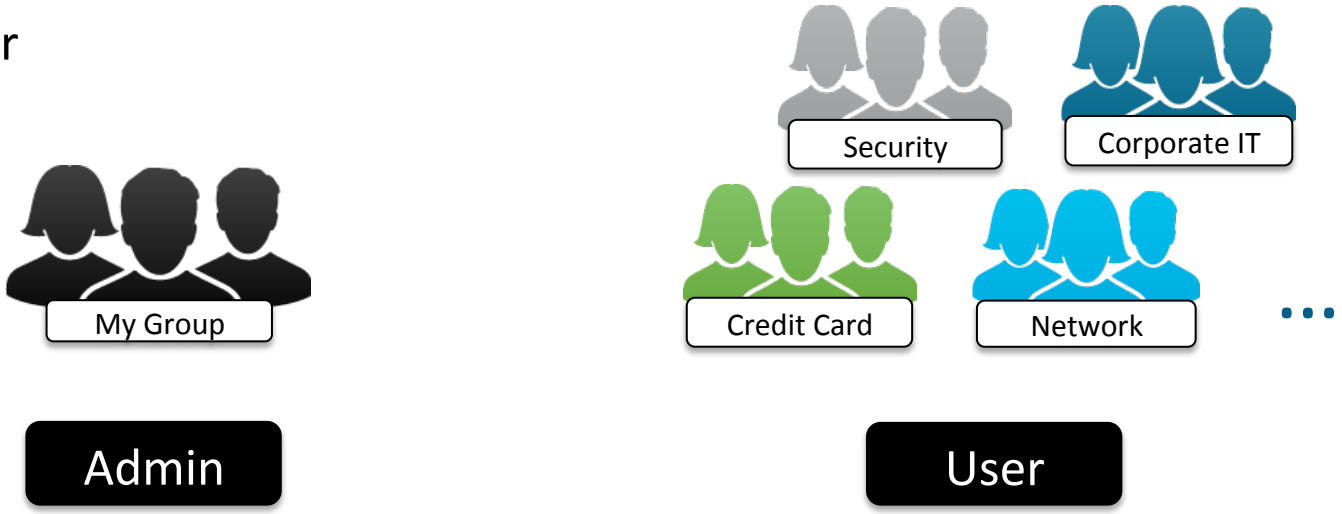
Service Overview

- Rakuten's organization
  - There are so many departments and groups



Service Overview

- Groups of Splunk as a Service
  - Admin
  - User



Service Overview

For user

- No need to manage Infrastructure
  - Design, construction, monitoring, operation and license
- Easy to start Splunking in a few minutes without detailed configuration
- Charged by measured rate
- High availability
  - 99.99% uptime

Will be talked details later

Rakuten

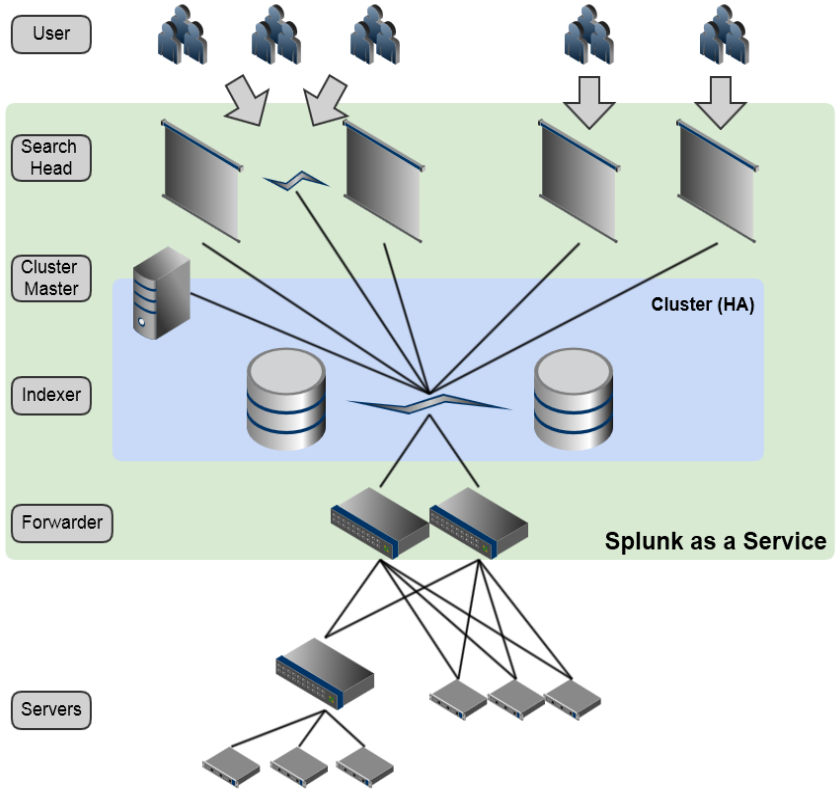
Splunk as a Service

Service Design

- Environment
  - Private Cloud
    - High availability
    - On time delivery
    - Flexibility

Service Design

- System configuration
  - v6.2.X
  - Using an indexer cluster
  - Full components
  - Newer data on Low latency Storage (Hotdb), Older data on Low Cost Storage (Colddb)



Service Design

- Other specifications
  - Splunk account is created for each user
    - 1 user = 1 group, 1 service, or 1 project
  - Each user has his/her own App
  - Basically a user can see only his/her own data
    - Accesses are controlled by tags
  - Users can choose the term of storage retention from 1 day to 6 years for each input
  - Admin does not do backups
  - Dedicated Search Head is ready for users who need

Service Operations

Admin side

- System operations
  - Create user accounts (rolls, users and Apps)
  - Set up inputs
  - Install external Apps
  - Irregular configuration (props.conf, transforms.conf, limits.conf, …etc)
- Service operations
  - User support / Consultation
- Monitoring
  - Input size
  - System resources (SoS / Unix App / PandoraFMS)

Our Challenges

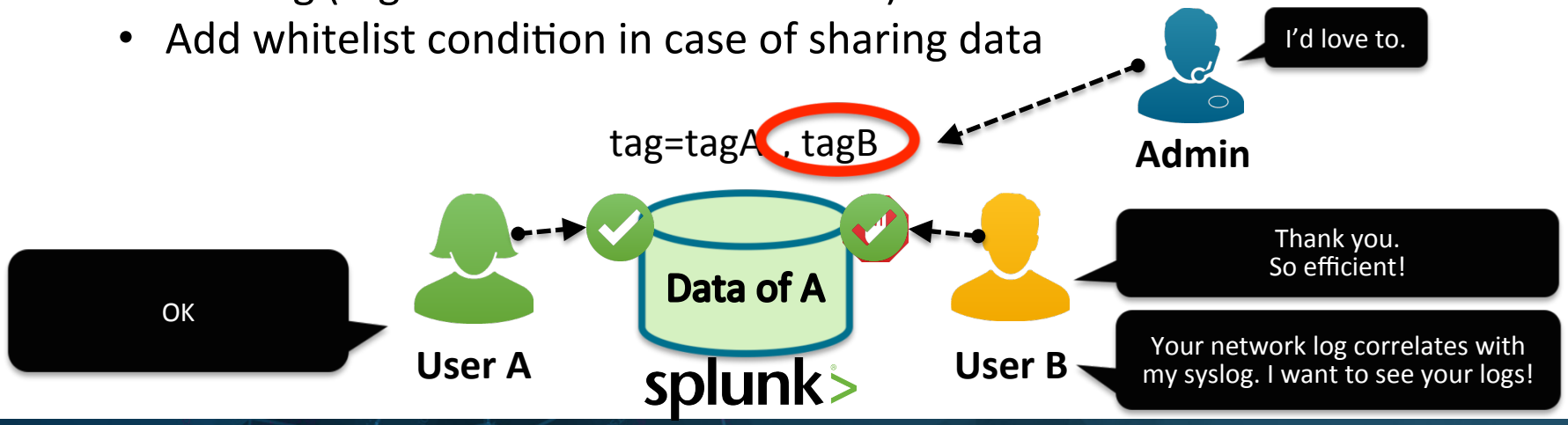
splunk>

Our Challenges

1. Easy data access control
2. Collaboration with internal tools
3. Collaboration with global group companies
4. Operation improvements by Rakuten Splunk Portal Site with API

Easy Data Access Control

- **Demand**
  - Users want to see other user's data
- **Measure**
  - Use Tag (tagUser:: host=<user's host>)
  - Add whitelist condition in case of sharing data

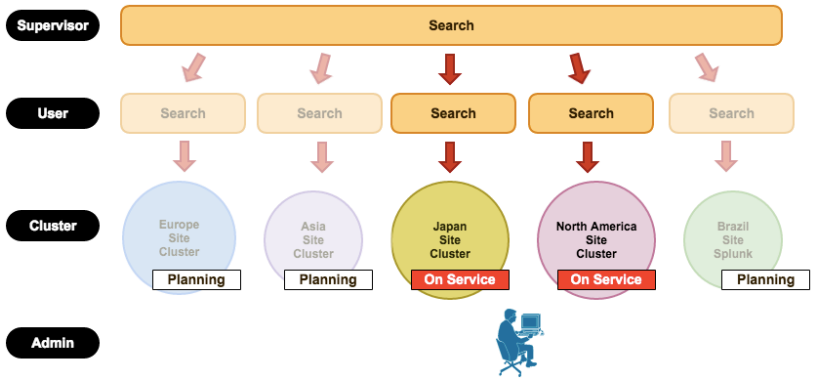


Collaboration with Internal Tools

- **Demand**
  - Users want to use some internal tools and information from Splunk
- **Measure**
  - Import CMDB data (lookup)
  - Can receive direct phone calls from DC staff (alert script)
  - Can call Hipchat/Slack web hooks (alert script)

Collaboration with global group companies

- **Demand**
  - Users want to access global companies' data through Splunk
- **Measure**
  - Splunk as a Service in the USA is ready
  - Supervisors can see the whole data of each region

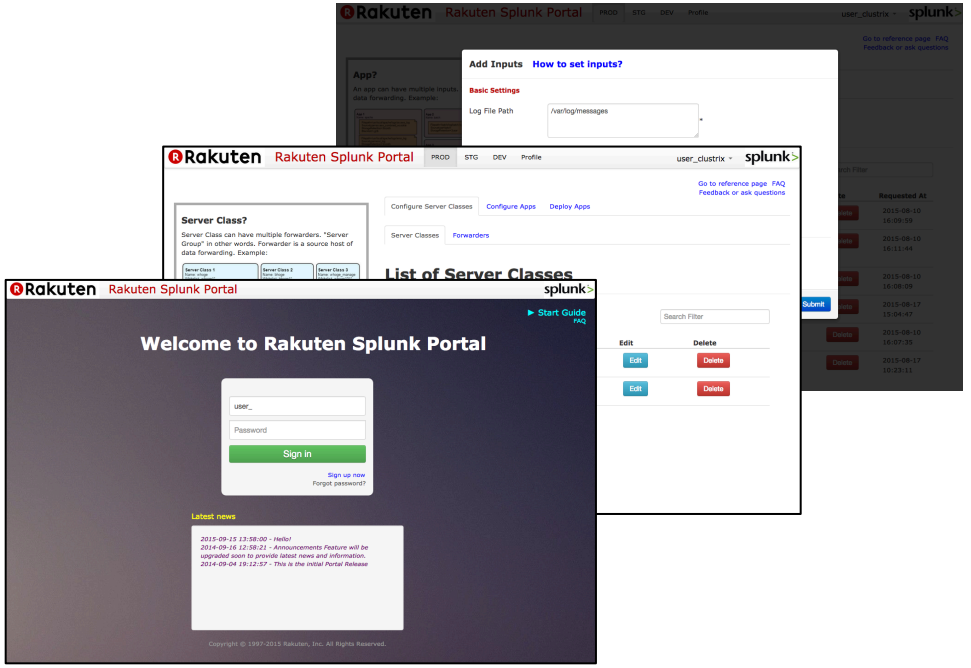


Operation Improvements

- **Demand**
  - Users want to start Splunking easily in a short time
  - Admin wants to make regular operations more efficient
- **Measure**
  - Made Rakuten Splunk Portal Site for operation improvements using Splunk REST API!
  - Easy to start Splunking in just a few minutes

Rakuten Splunk Portal Site

- Demonstration
  - Easy to start Splunking
  1. Create Splunk web account
  2. Install a forwarder
  3. Set up & deploy Apps



Rakuten Splunk Portal Site

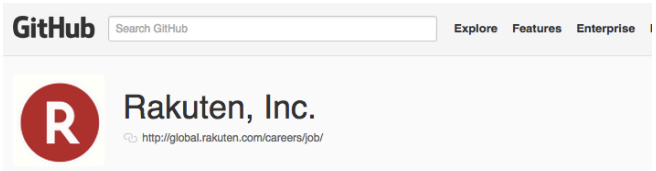
- Current main features
  - Manages user's information (organization, emails, etc..)
  - Creates Splunk web accounts (create roles, users, and Apps)
  - Manages forwarders, server classes, inputs and Apps
  - Deploys Apps to users' forwarders
  - Alerts users when users' forwarders are down

Good reputation

Rakuten Splunk Portal Site

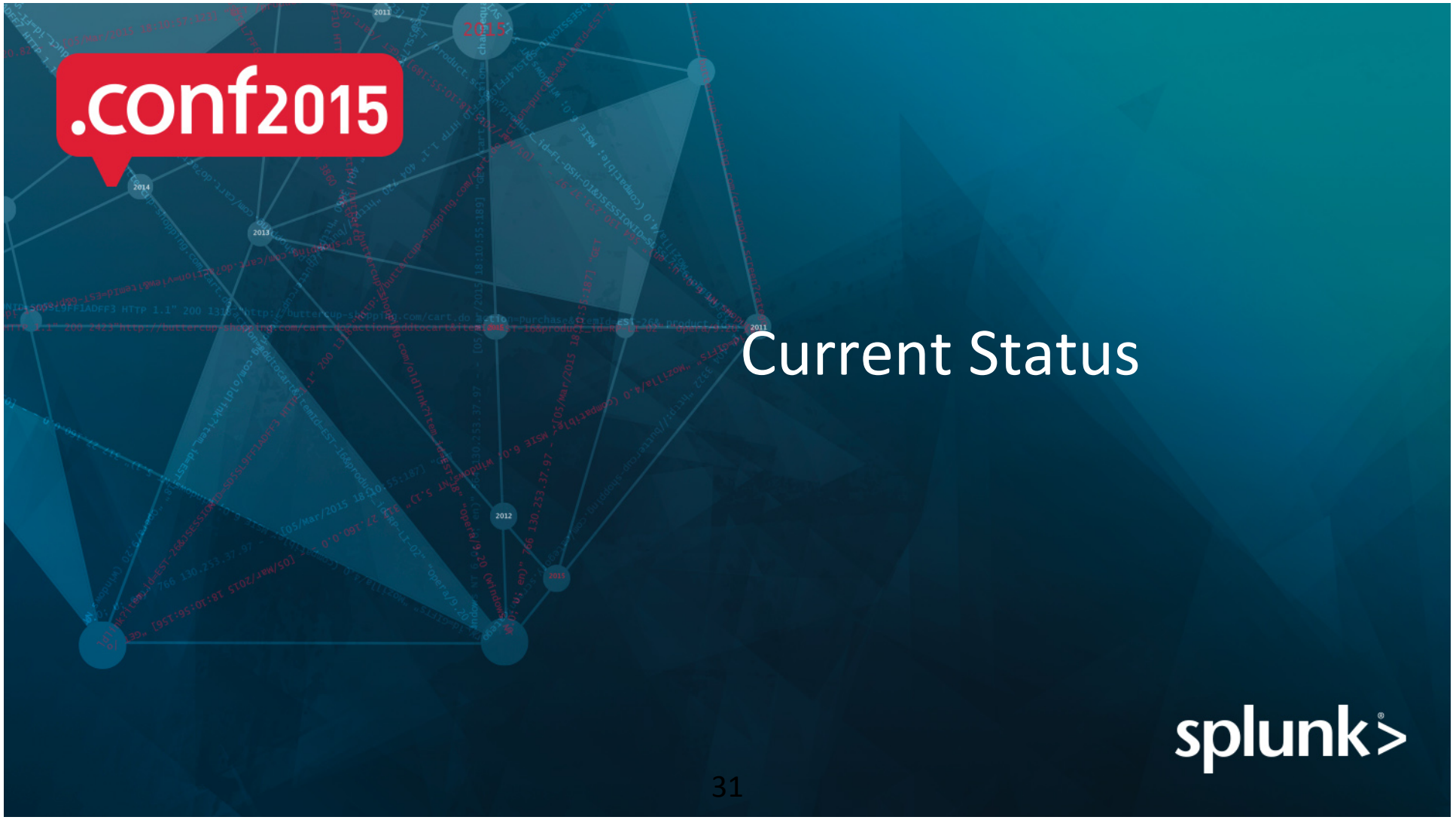
- Do you want to try the Portal Site on your environment?

We are currently developing it as an open-source project!!



To be prepared!!

Please read README before using it.

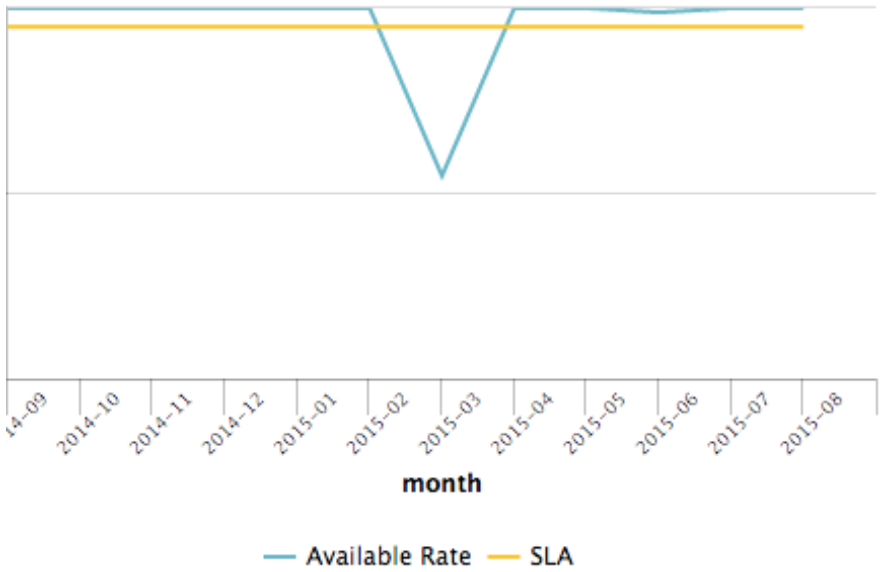


Current Status

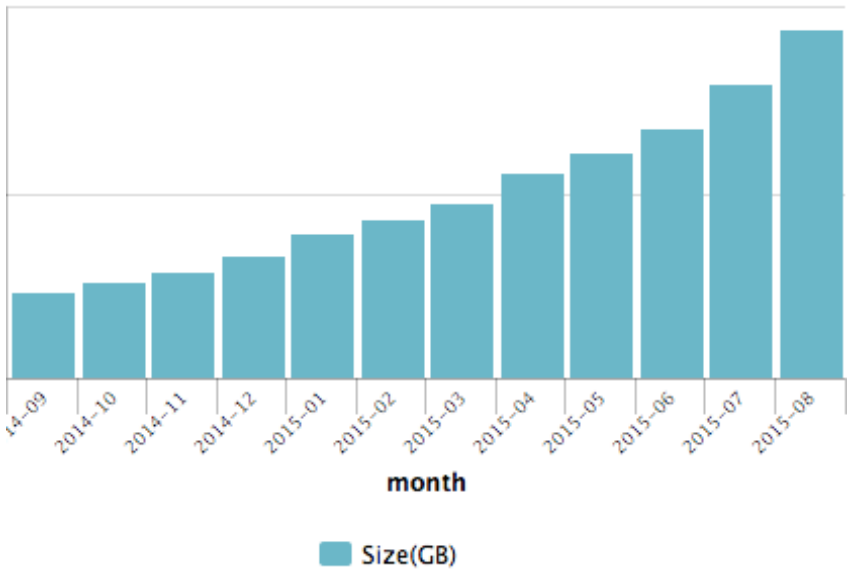
splunk>

Current Status

Availability Rate

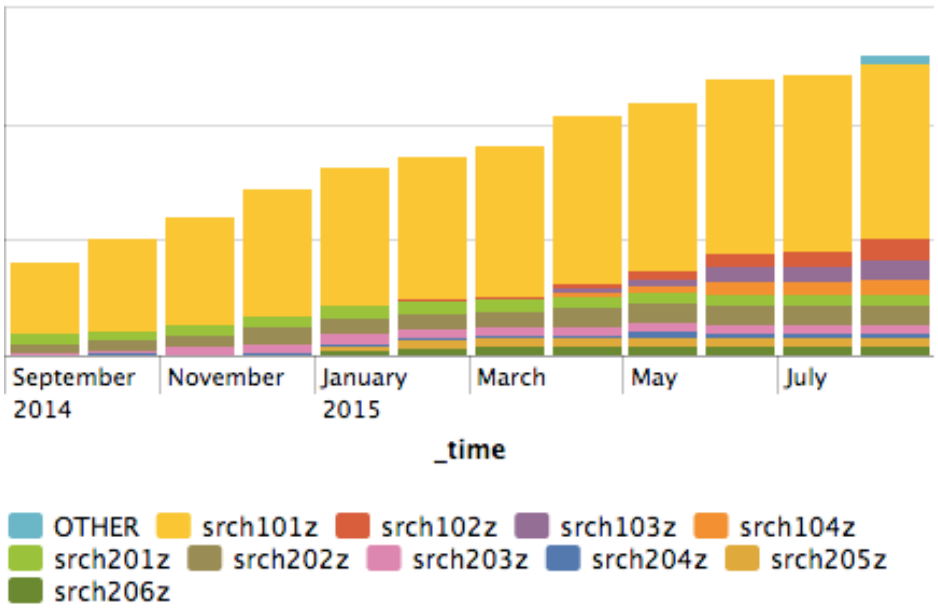


Indexed Data Size

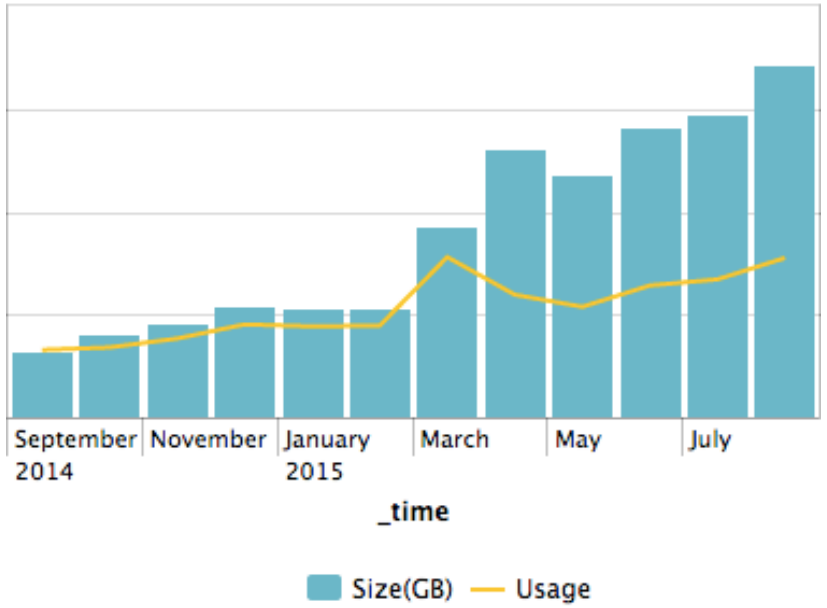


Current Status

# of Accounts



Input Size



Case Studies

splunk>

Case Studies

Server
Real-time monitoring
Troubleshooting
Usage report

Database
Real-time monitoring
Troubleshooting
Usage report
Service KPI management

Security
IDS real-time monitoring
Fraud detection

Private Cloud (RIaaS)
Real-time monitoring
Resource management

Application
Real-time monitoring
Service KPI management
Performance management

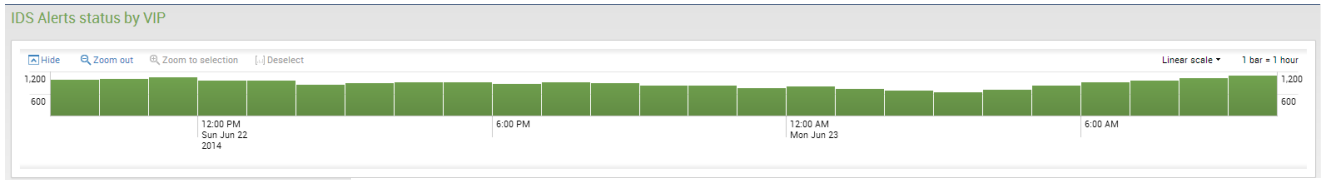
Storage
Real-time monitoring
Resource management
Service KPI management

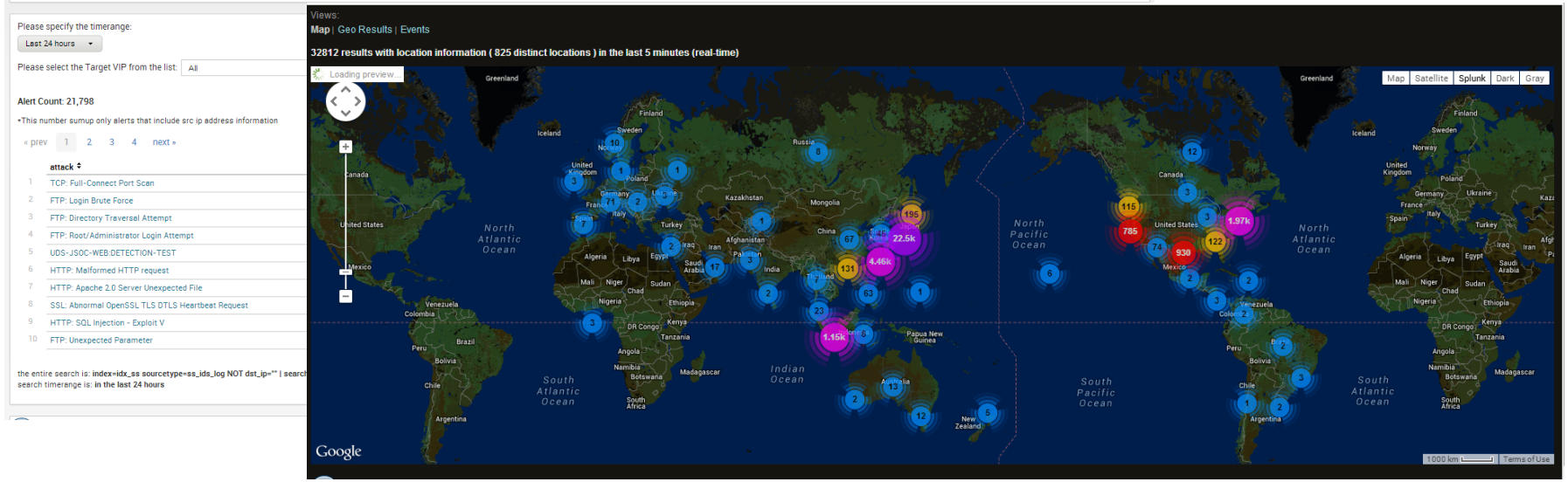
Network
Real-time monitoring
Troubleshooting
Trend analysis

More…

Security Monitoring

Security





Alert Email

Security

Today at 10:05 AM
splunk

To:
Scripted Alert from SS IDS monitor on Splunk

IDS Alert

Hi,
Could you please check the IDS alerts as below.
If you find something, please conatact System Security team (@ com)
Thank you for your cooperation.

The number of matched events:1
Link to result URL:
sid=scheduler__admin_c3NvcHNfYXBw__RMD5fb80bb8954048322_at_1441069500_17126

email	emergency1	tel	severity	time	attack	src_ip	vip	dst_ip	cve_id
			Medium	2015-09-01 09:53:34 JST	HTTP: SQL Injection - Exploit				

description	This alert indicates that someone attempted to submit a crafted URL to inject a SQL command, which could then be run by the SQL server. "SQL injection" occurs when an attacker is able to insert a SQL statement into a SQL query generated by a trusted Web server. These injected SQL queries can be used to execute commands and possibly compromise the database.
packetdata	``` ``^`````E4`@`Ξ& 4P`Ib`.K`D`` ``` `^`````E4`@`Ξ& 4P`Ib`0``P`A ``` `^`````E4`@`Ξ& 4P`Iw`0``P`` ``` `^`````E``@`QΞ& 4P`Ib`0``P:` ``` `HTTP/1.1 200 OK X-YQL-Host: X-Content-Type-Options: nosniff Access-Control-Allow-Origin: * Cache-Control: no-cache Content-Type: text/xml;charset=utf-8 Date: Mon, 31 Aug 2015 09:35:35 GMT Server: ATS Content-Encoding: gzip Vary: Accept-Encoding Age: 0 Transfer-Encoding: chunked Connection: close ```

Data comes from other systems

Point of contact

Description of attack

Actual attack payload

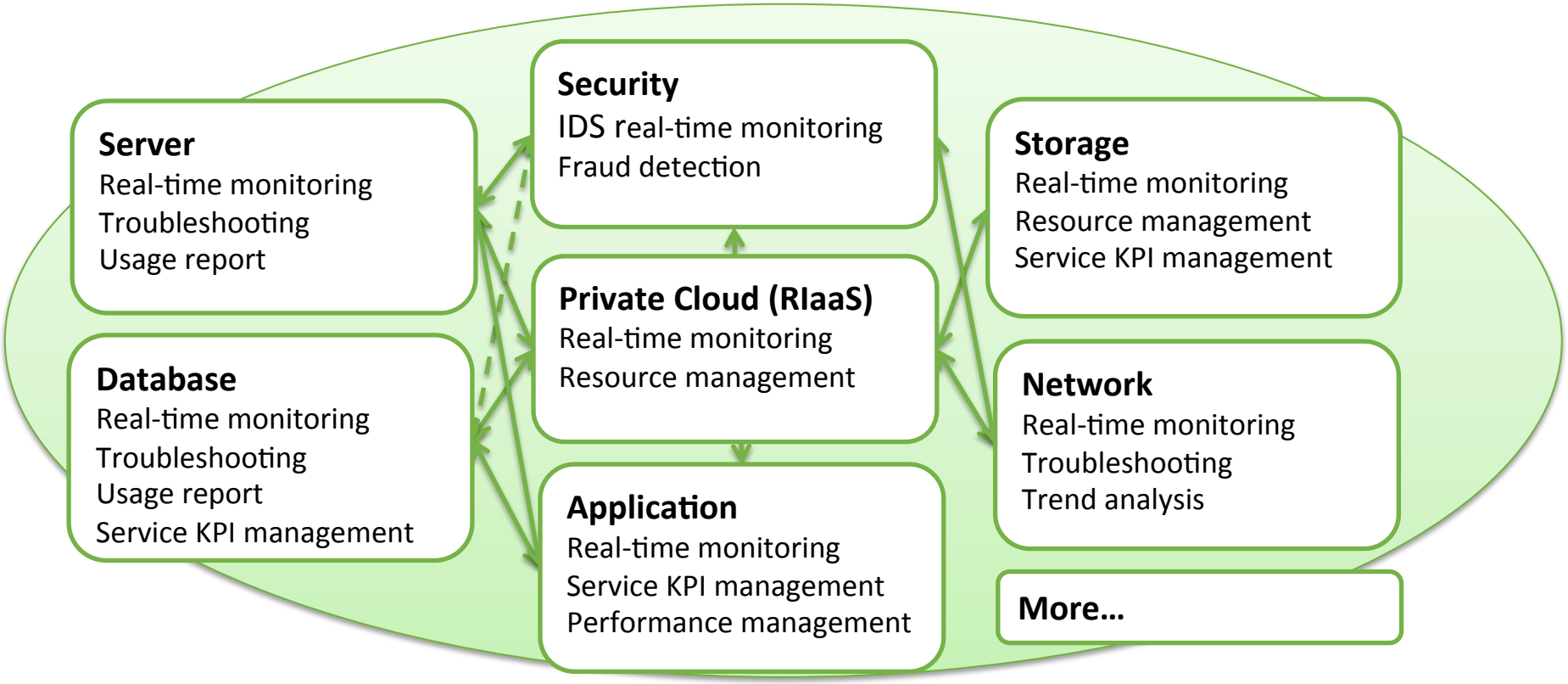
Security Monitoring

Security

- Before
  - Analyze by Managed Security Service Portal
  - Make sure the right person handles the incident

- After
  - By CMDB, streamlined escalation flow
  - Shorten time for initializing action
  - Detect irregular accesses

Case Studies



Quote

"You can't connect the dots looking forward; you can only connect them looking backward. So you have to trust that the dots will somehow connect in your future. You have to trust in something"

- Steve Jobs

Wrap up

splunk>

What's Next?

- Make it easier to get Splunk started
  - Complete automation
- Make regular operations more efficient
  - Change frequent operations automatically
- Upgrade to v6.3
- Enhance Rakuten Splunk Portal Site
- Have more collaboration with global group companies

Wrap up

- Rakuten is using one big Splunk as a Service
  - Positive advantages for user
    - No need to manage Infrastructure, License, and detailed configuration
    - Can use data of crossing organization
  - Positive advantages for admin
    - Can manage operations and license efficiently
    - Have many satisfied users
- Operation improvements by Splunk Portal Site with API
  - Can start Splunking easily in a few minutes
- Many different types of users are using Splunk, and hopefully it will expand globally

Questions?

THANK YOU

splunk>