

# FUJITSU Software Systemwalker Desktop Keeper V15 Introducing

March 2018  
Fujitsu Limited

## ■ Introduction

- What is Systemwalker Desktop Keeper?

## ■ Operation Log Collection (View/Trace)

- Flow of Operation Log Collection
- Log Collection
- Log Management (Trace Operations)
- Log Management (Back Up the Original File)

## ■ Operation Prohibition

- Flow of Operation Prohibition
- Operation Prohibition
- Operation Prohibition (Permit Use of Media)

## ■ Report Feature

- Output Report

## ■ Product Information

- Examples (for Reference)
- Trademarks

# Introduction

- What is Systemwalker Desktop Keeper?

# What is Systemwalker Desktop Keeper?

## ■ Importance of operation log collection (view/trace) and operation prohibition

It is impossible to prevent information leakage only by recording operations performed on corporate PCs such as access to files not related to business, printing of confidential information, or copying of the information to USB memory.

Prohibiting printing or copying in order to lower the risk of information leakage may affect business.

To protect confidential information, it is vital to have measures for information leakage not only from PCs, but smart devices as well, which are now commonly used for business.

## ■ Systemwalker Desktop Keeper solutions!

Operation log  
collection (view/trace)

Operations on PCs or smart devices, or operations using a printer or USB memory are recorded, making it possible to take action promptly after an issue occurs.

Operation prohibition

Determines security policies that meet the needs of the entire company or a department and prohibits operations unnecessary for business.

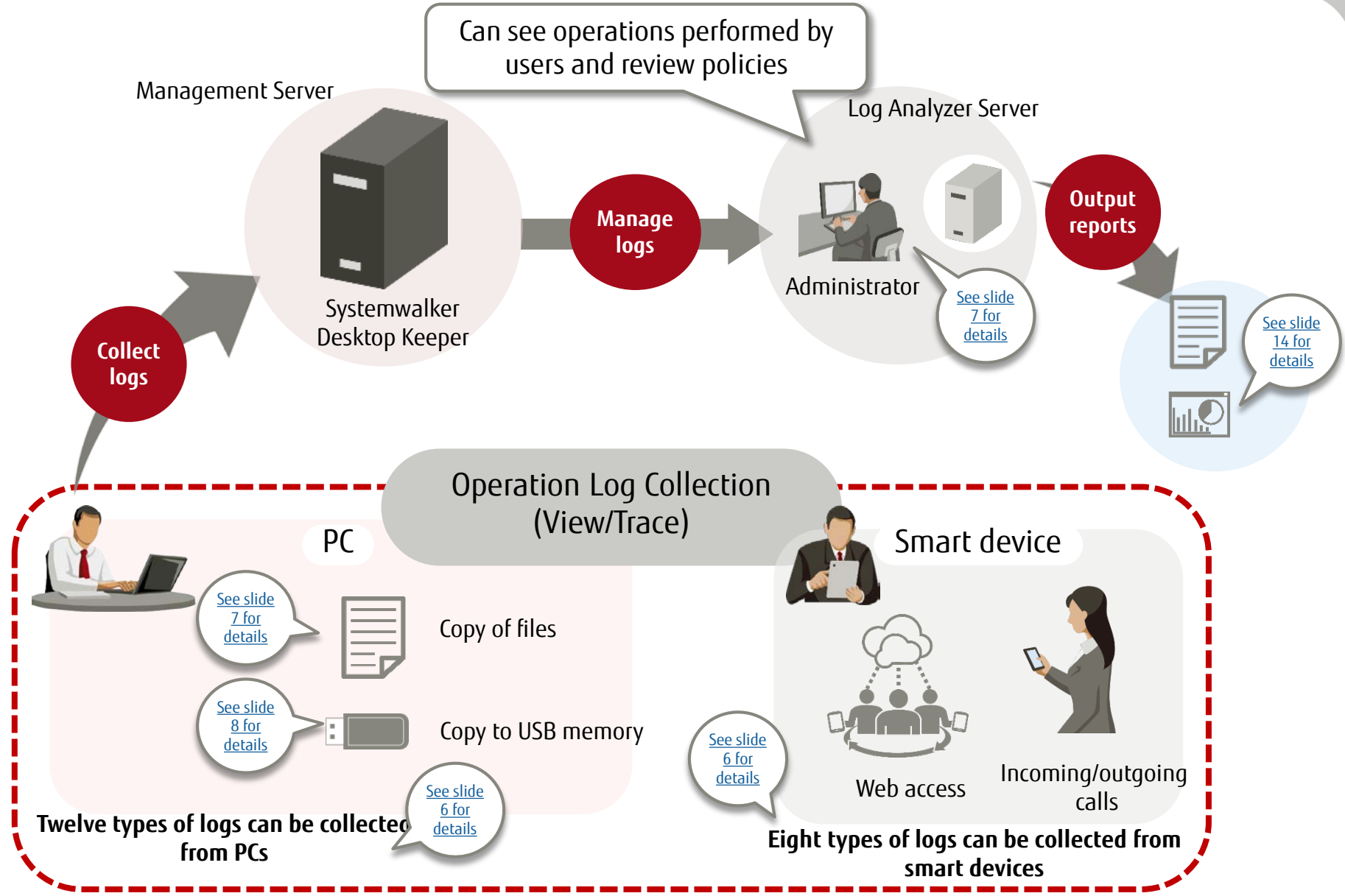
Report feature

The diagnosis result of the security status within an organization and the internal compliance status can be printed as a report or output to file.

# Operation Log Collection (View/Trace)

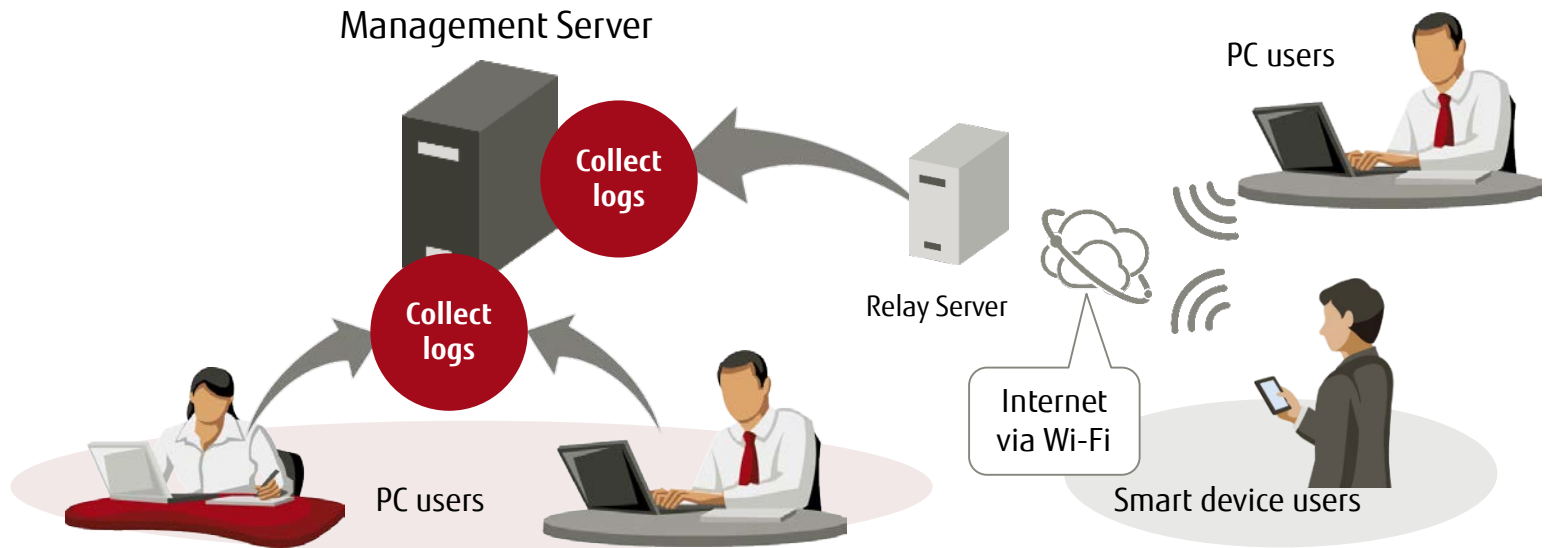
- Flow of Operation Log Collection
- Log Collection
- Log Management (Trace Operations)
- Log Management (Backup Up the Original File)

# Flow of Operation Log Collection



# Log Collection

■ Operation records of PCs or smart devices per user can be centrally managed.



## Logs collected from PCs<sup>\*1</sup>

- |  |  |                               |
|--|--|-------------------------------|
| ■ Application startup/termination          | ■ File export                            | ■ Logon, Logoff <sup>*3</sup> |
| ■ Window title collection (Web access log) | ■ PrintScreen key operation              | ■ Environment change          |
| ■ E-mail sending                           | ■ Web operation (upload/download)        | ■ Linkage application         |
| ■ E-mail receiving                         | ■ Clipboard operation <sup>*2</sup>      |                               |
| ■ Device configuration changes             | ■ FTP server operation (upload/download) |                               |
| ■ Printing operation                       | ■ File operation                         |                               |
- (15 types of logs)

## Logs collected from smart devices<sup>\*4</sup>

- |                          |                           |                                    |
|--------------------------|---------------------------|------------------------------------|
| ■ Web access             | ■ Wi-Fi connection        | ■ Application usage                |
| ■ SD card mount/unmount  | ■ Bluetooth connection    | ■ Application configuration change |
| ■ SIM card mount/unmount | ■ Incoming/outgoing calls |                                    |
- (8 types of logs)

\*1: There are also logs that cannot be collected in a virtual environment. Refer to the relevant documents that describe the feature for details.

\*2: Collect logs of copy operation via Clipboard between a virtual PC (Citrix XenDesktop/VMware View) and PC.

\*3: Also collect logs for power on/off of PCs.

\*4: Smart devices with iOS are not supported.

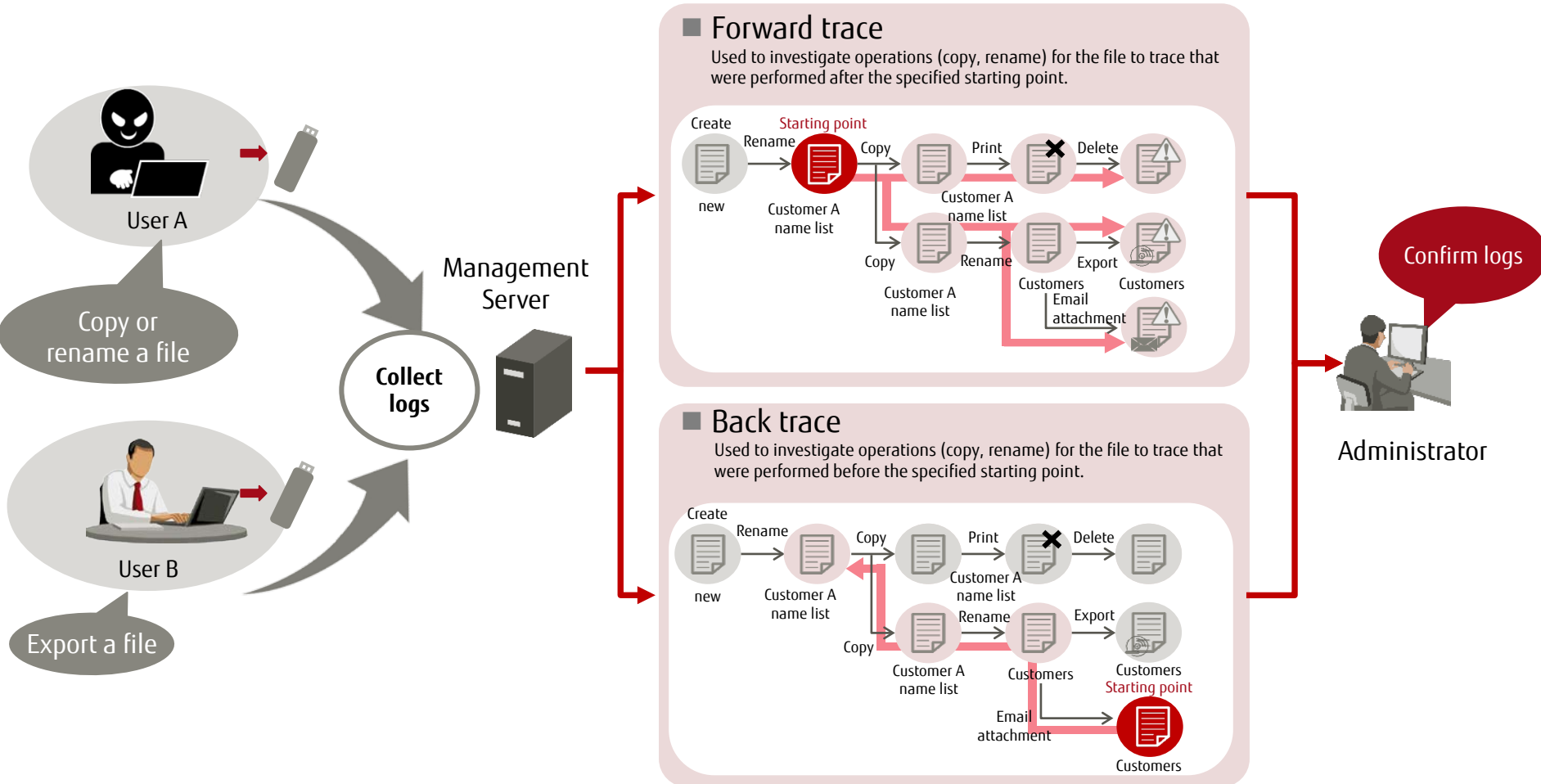
# Log Management (Trace Operations)



Operation log  
collection  
(view/trace)



- Operations performed before or after the filtered operation can be traced by searching logs, using keywords or period of time.

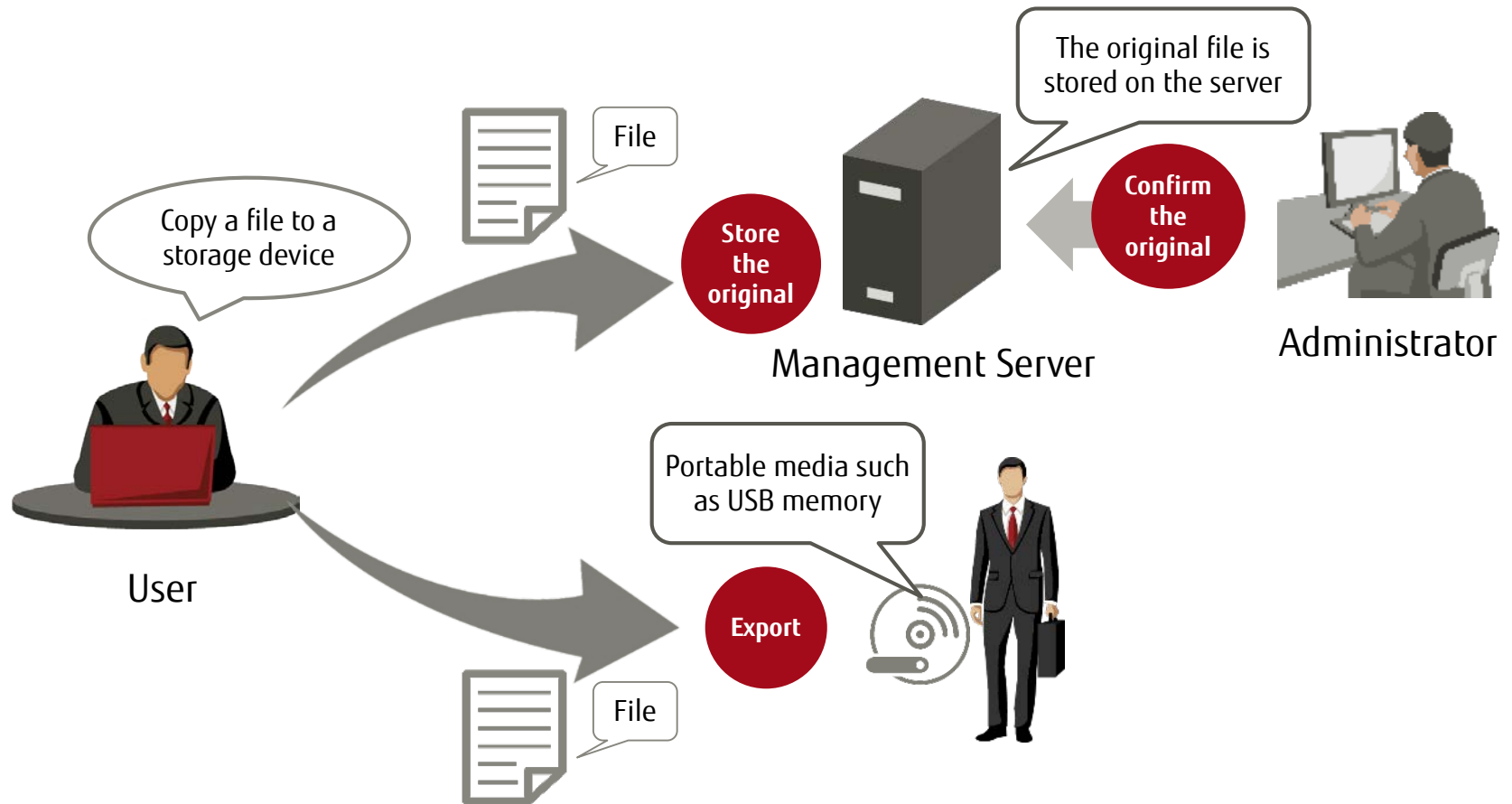


Search operation logs to trace operation history in case of an emergency, allowing prompt action.



# Log Management (Back Up the Original File)

- A file (the original file) can be stored with operation logs when it is exported to a portable storage device. Fujitsu proprietary

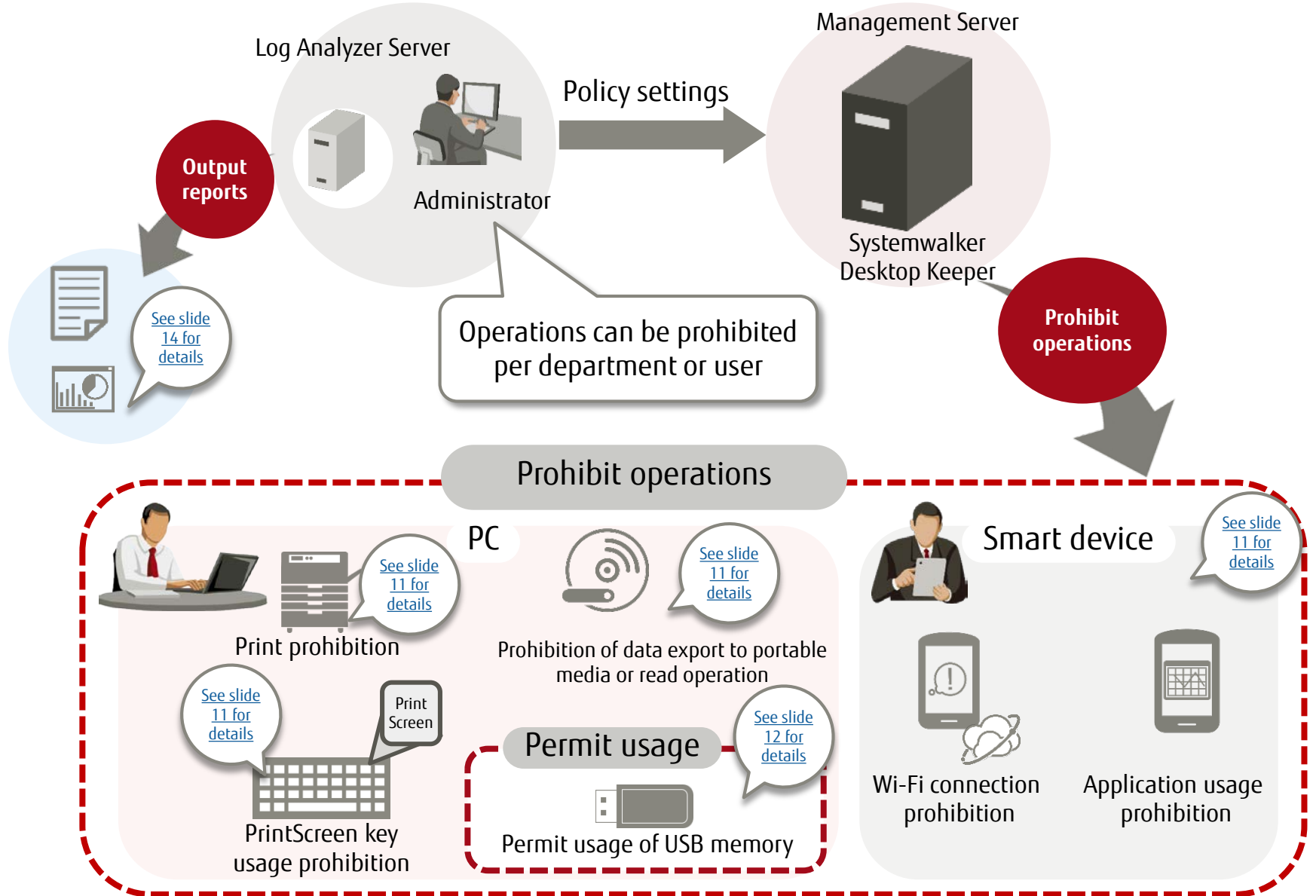


Even if the file is leaked, the administrator can plan actions to take according to the stored original file.

# Operation Prohibition

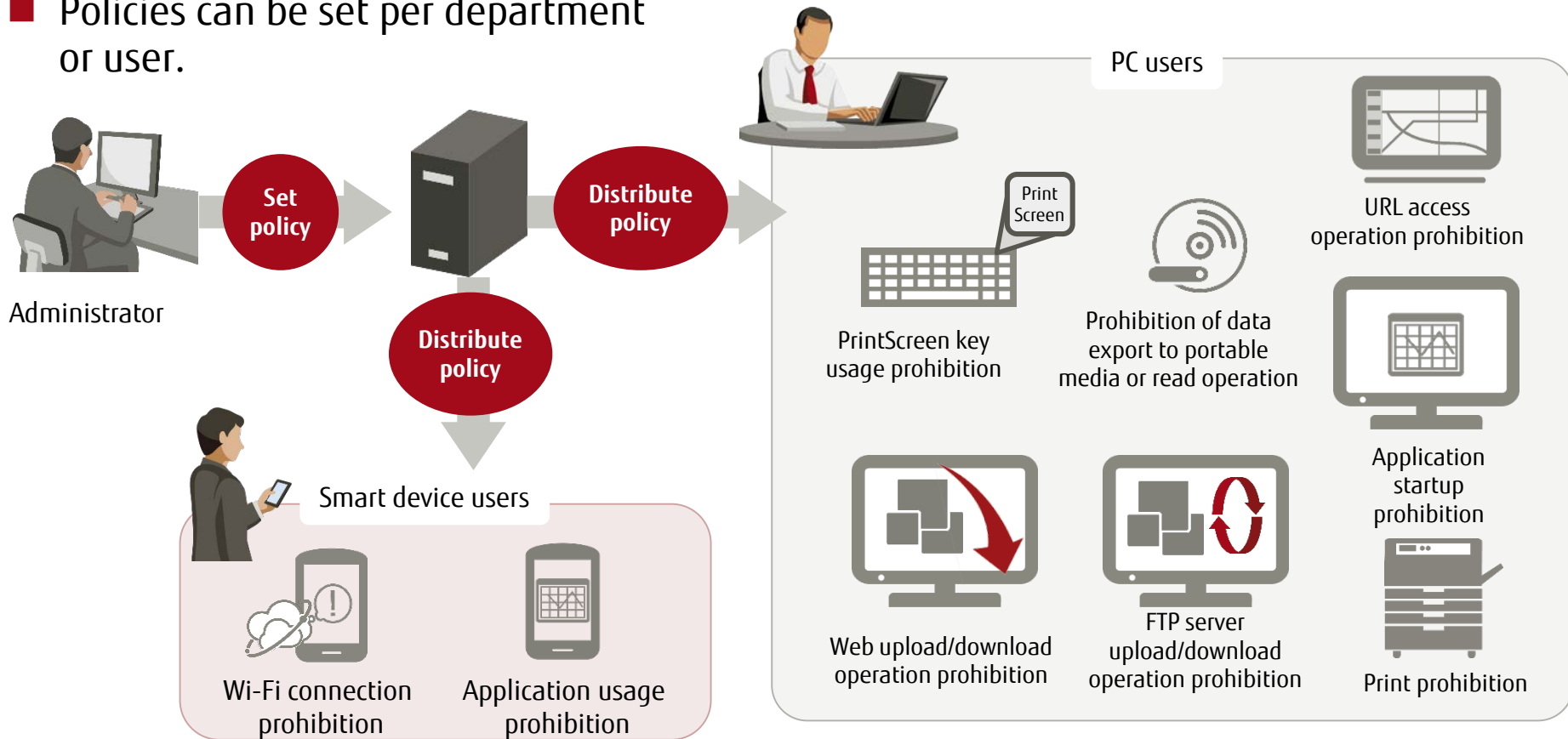
- Flow of Operation Prohibition
- Operation Prohibition
- Operation Prohibition (Permit Use of Media)

# Flow of Operation Prohibition



# Operation Prohibition

- Operations that have a risk of information leakage can be prohibited.
- Prohibits operations unnecessary for business according to security policies.
- Policies can be set per department or user.

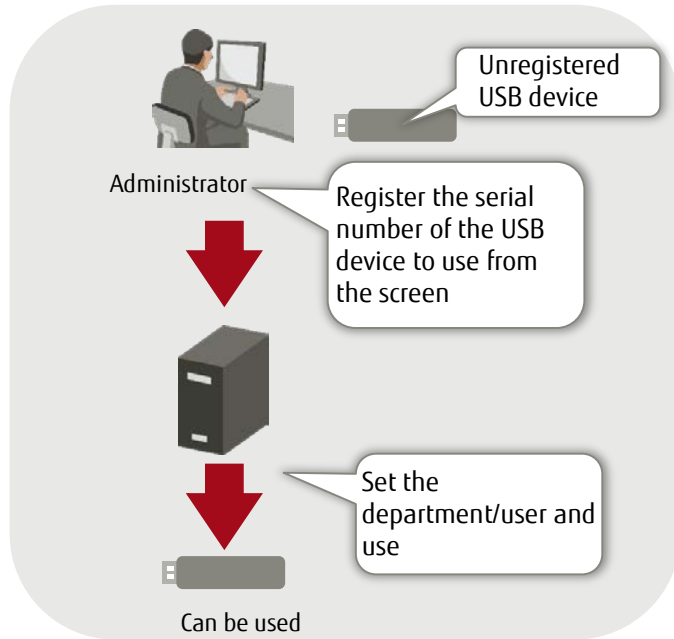


PC or smart device operations that have a risk of information leakage can be prohibited.

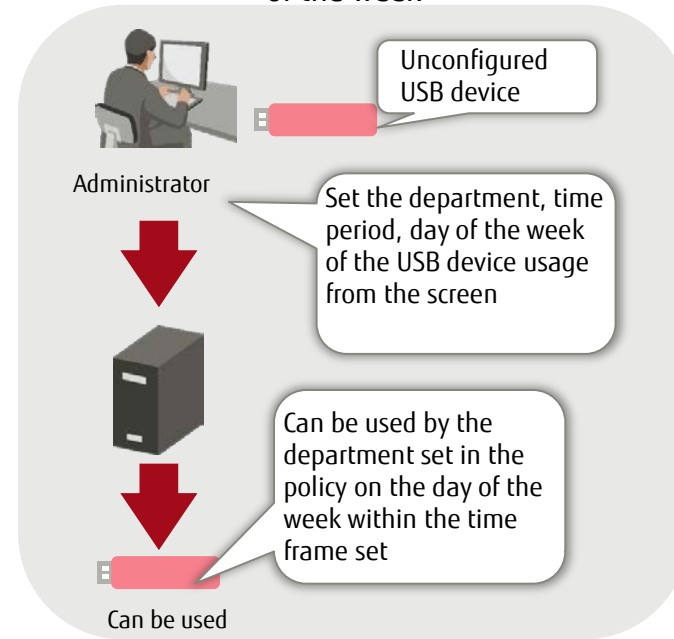
- The individual media identification feature allows export only for a specific person or device for business purposes.
- Export can be permitted by specifying time or day of the week.

Fujitsu proprietary

## USB device individual identification feature



## Specifying time or day of the week



The following devices can be controlled in addition to USB memory:

- Android device\*<sup>1</sup> (portable/imaging)
- iOS media (portable)
- Digital camera (portable)
- Scanner (portable)
- SD card, mini SD card, micro SD card

\*1: For smart devices etc., a different file transfer method (PTP/MTP\*<sup>2</sup>) from the USB memory is used to avoid file corruption during transfer.

\*2: PTP: Picture Transfer Protocol, MTP: Media Transfer Protocol

Individual file usage can be permitted according to the security policy when the files are exported.

# Report Feature

- Output Report

# Output Report



Report  
feature

FUJITSU

- Security measures, security risk status, and PC usage can be confirmed by using the Report Output Tool.

Log Analyzer Server



Administrator



Create analysis reports using  
the Report Output Tool



## Reports that can be output (24 types)

- Information leakage analysis report: 8 types
- Device usage analysis report: 4 types
- Violation operation analysis report: 6 types
- Comprehensive analysis report: 1 type
- Print volume monitoring report: 5 types



Regular evaluation/analysis results are visualized and can be used to review policies.

# Product Information

- Examples (for Reference)
- Trademarks



# Example 1 - Telecom Carrier (for Reference)



Store the original

FUJITSU

- Enhance security measures for products under development when they are exported to portable media.

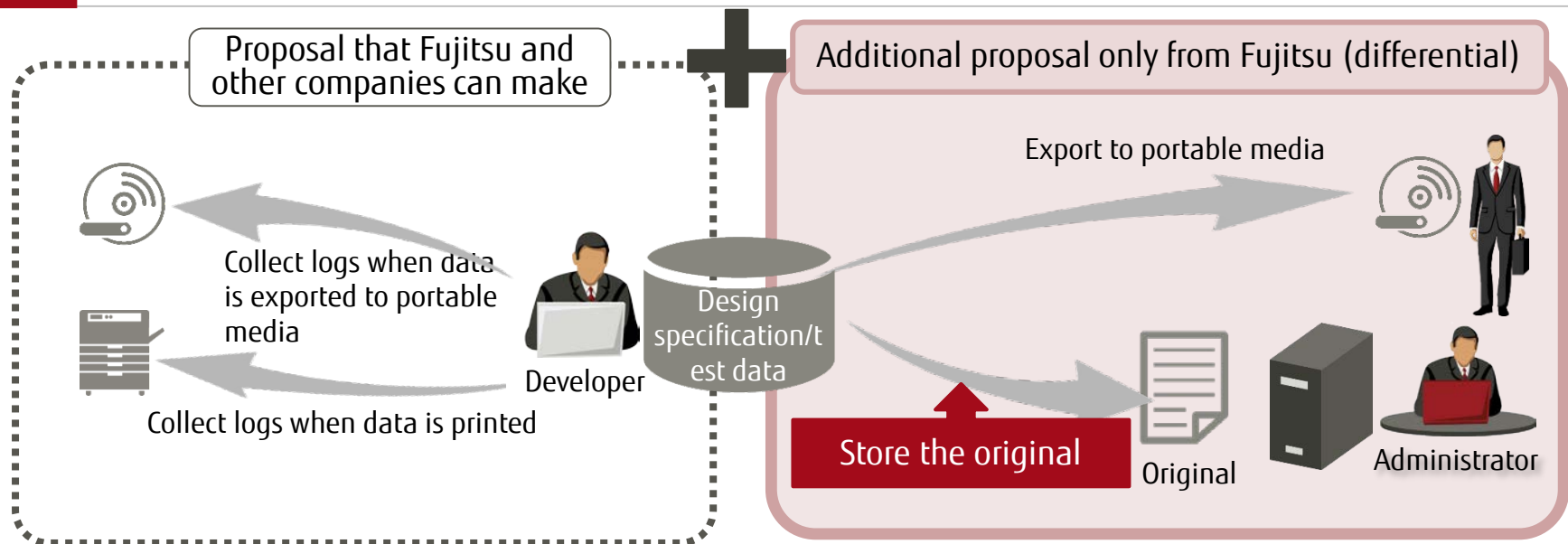
Requirement: Information leakage measures without compromising the work efficiency of system developers.

## Challenges

- There is a concern of information leakage due to the loss of media when system developers export design specifications or test data to portable media.
- Want to understand the status of operation log collections or exported files.

## Solutions

- Using a feature of Systemwalker Desktop Keeper, original files are forcibly and automatically stored on the server when they are exported to portable media. When the media is lost, prompt action can be taken because the file content can be confirmed from the original file.
- By collecting operation logs of the terminals used by system developers, any operations that violate the security policy can be traced.

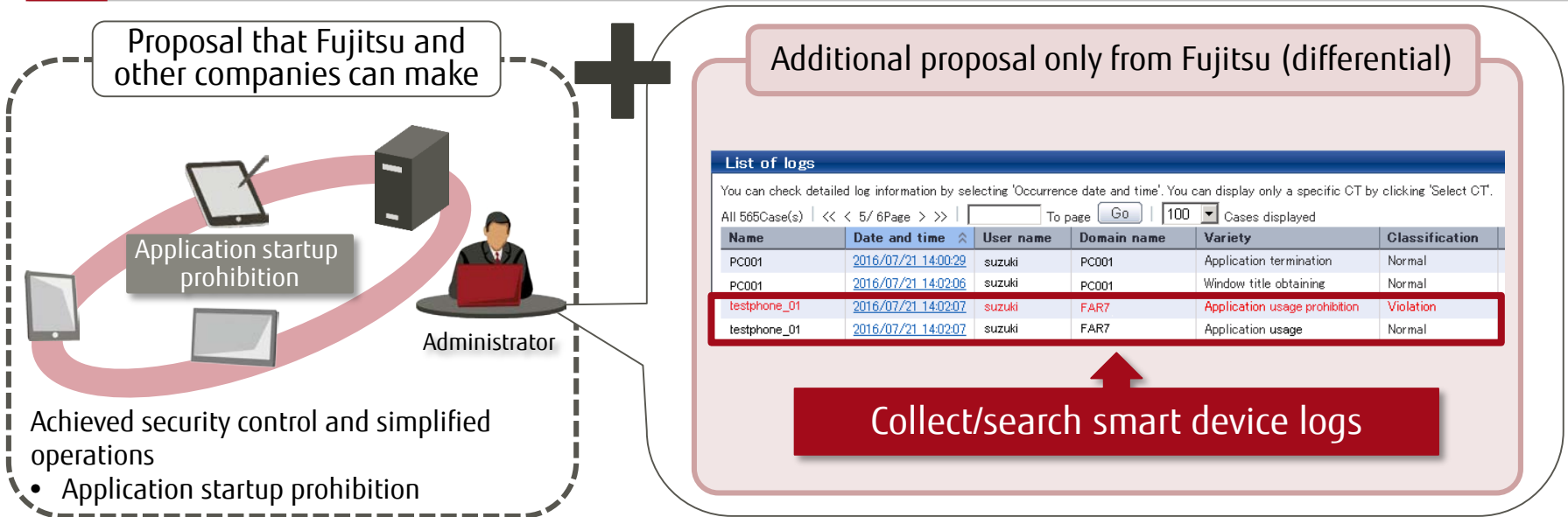


# Example 2 - Oil Company (for Reference)

## Smart device operation logs can be centrally managed.

Requirement: Smart devices are introduced to gas stations to start selling subscriptions for credit cards and car insurance. Want to ensure security prohibiting the unauthorized use of smart devices.

Challenges	<ul style="list-style-type: none"> <li>Prohibit the use of applications unnecessary for business</li> <li>Understand how the devices are used to determine other operations to be prohibited</li> </ul>
Solutions	<ul style="list-style-type: none"> <li>Distribute applications or explanatory materials necessary for selling subscriptions to the outlets via smart devices (Android)</li> <li>Using the Systemwalker Desktop Keeper application startup prohibition feature, prohibit the startup of unnecessary applications</li> <li>Using the log collection feature, user operation logs are collected to understand how devices are used. Consider if any operations should be prohibited.</li> </ul>



# Example 3 - Metal Company (for Reference)

## Security control to domestic/overseas sites using the same policy

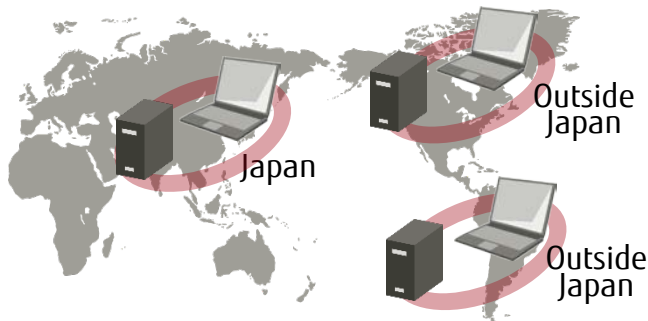
Requirement: Want to use the same security policy as the domestic one in overseas sites and centrally manage PC logs

- Challenges**
- Administrators are different for domestic sites and overseas sites in five countries (Thailand, Vietnam, China, Singapore, and Malaysia), and the security policy is not followed in overseas sites as strictly as in the domestic sites.
  - Want to maintain the same security level over the entire company by distributing security policies to overseas sites as well as domestic sites from a central location.

- Solutions**
- Systemwalker Desktop Keeper also supports client operations on non-Japanese operating systems, so it is possible to centrally manage overseas PCs from a domestic site.
  - Can achieve the same level of security policy operation between domestic and overseas sites.

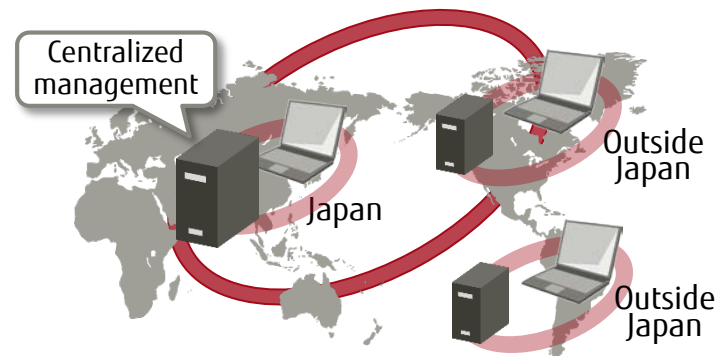
### Proposal that other companies can make

Distribute policies and collect logs using different administrators and servers for domestic and overseas sites




### Proposal from Fujitsu

Distribute policies and collect logs at each site and perform centralized management in Japan



- Microsoft, Windows, Windows NT, Windows Vista, Windows Server or other Microsoft product names are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries.
- Citrix, Xen Citrix XenApp, Citrix XenServer, Citrix XenDesktop and Citrix Presentation Server are trademarks or registered trademarks of Citrix Systems, Inc in the United States and other countries.
- VMware is a trademark or registered trademark of VMware, Inc in the United States and other countries.
- Android is a trademark or registered trademark of Google Inc.
- Bluetooth is a registered trademark of Bluetooth SIG, and is licensed to Fujitsu.
- Wi-Fi and Wi-Fi Logo are registered trademarks of Wi-Fi Alliance.
- IOS trademark is used based on the license of Cisco in the United States and other countries.
- Apple, Apple Logo and Mac OS are registered trademarks of Apple Inc. in the United States and other countries.
- Other product names are trademarks or registered trademarks of their respective holders.



**FUJITSU**

shaping tomorrow with you