Key points of the services needed to achieve Zero Trust and the Future of Enterprise IT Systems realized by IIJ Omnibus

IIJ
Internet Initiative Japan

October 29, 2020
Internet Initiative Japan Inc.
Hajime Shironouchi
Network Cloud Division, Division Director

Ongoing Innovation

Agenda

1. Services needed by enterprises to realize Zero Trust
2. IIJ Omnibus that achieves Zero Trust
3. Future vision of Zero Trust to be achieved with IIJ Omnibus
4. New digital workplace

1. Services needed by enterprises to realize Zero Trust

◆ Issues regarding Zero Trust promotion

It's not easy to achieve Zero Trust

→ Drastic change from the current architecture is needed

It doesn't end when services are products are installed

→ Must continue to look after against new threats and/or periodic change in policies

1. Services needed by enterprises to realize Zero Trust

- ◆ Zero Trust Model that IIJ targets
  - □ Approval and authentication based on combined information about users, devices, place, time, access points, application, data etc.
  - □ High security realized with comprehensive functions such as endpoint, gateway security etc.
  - □ Environment to continuously execute counter security measures and to support continuous operation and maintenance realized

IIJ Omnibus that achieves Zero Trust

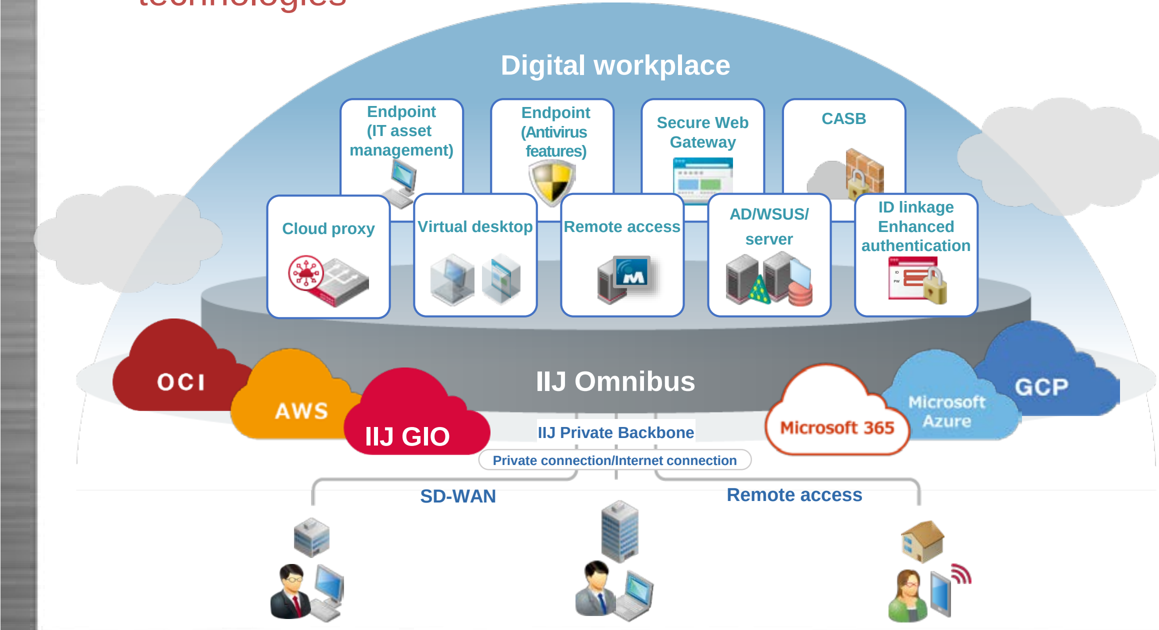
Models Available Now

2. IIJ Omnibus that achieves Zero Trust

◆ What is IIJ Omnibus?

Digital workplace

A world where diverse workstyles, which are free from constraints of time and place, are enabled using digital technologies



IIJ Omnibus

A platform service that conveniently supports the digital workplace:

1. Cloud environment
   - Internet connection and direct cloud connection
2. Network environment
   - Seamless connection of head office, branches, and others via SD-WAN
   - Compatible with diverse network environments (leased line, mobile network, internet)
   - Stable remote access environment
3. Office IT environment
   - Virtual desktop, Active Directory and server

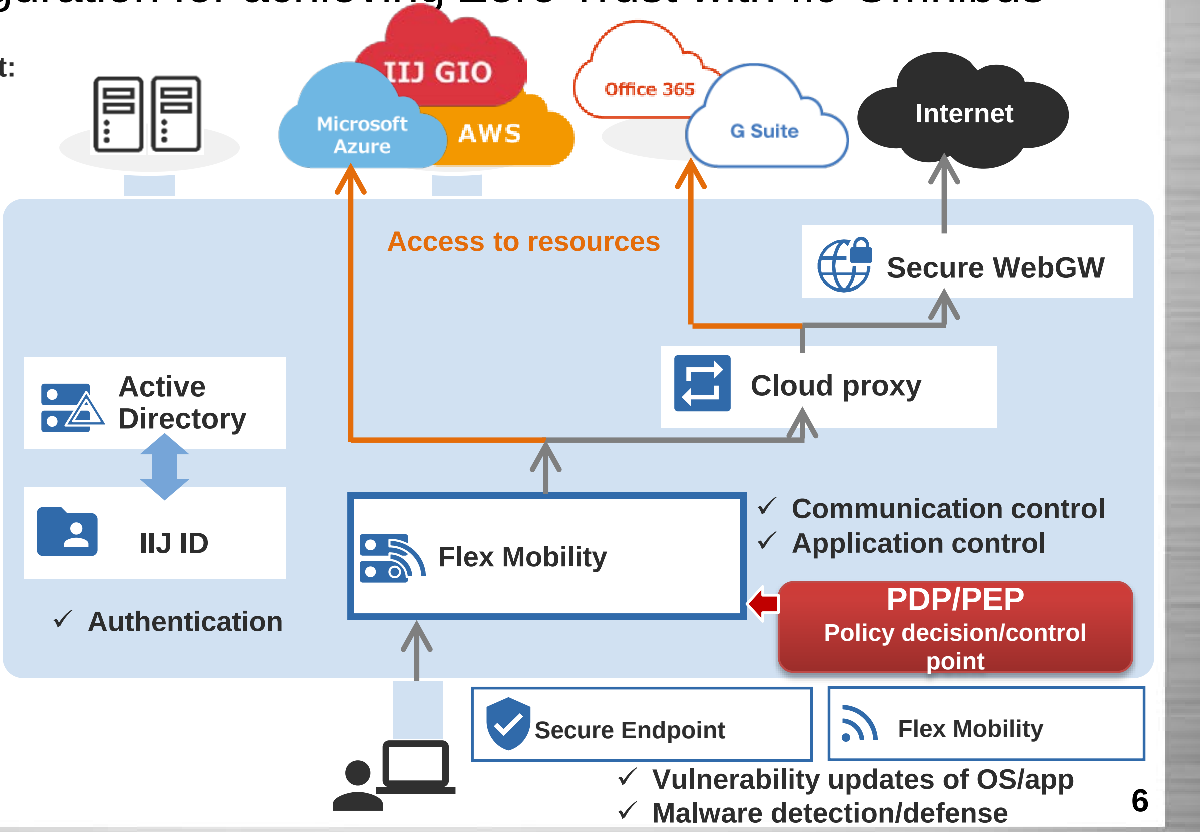
Models Available Now

2. IIJ Omnibus that achieves Zero Trust

◆ Example of service configuration for achieving Zero Trust with IIJ Omnibus

Part of a group of services that achieve Zero Trust:

- **IIJ Secure End Point Service**
  Antivirus features, IT asset management
- **IIJ Flex Mobility Service**
  Comfortable remote access
- **IIJ Virtual Desktop Service**
  VDI, web separation
- **IIJ Directory Service for Microsoft**
  AD, WSUS, AADC
- **IIJ ID Service**
  SSO, multi-factor authentication, FIDO
- **IIJ Secure Web Gateway Service**
  URL filter, antivirus features, log storage



Models Available Now

2. IIJ Omnibus that achieves Zero Trust

◆ Select services by business configuration or employment type.

Terminals for business use provided by the company

With agents

Achieved using Flex Mobility (mentioned above)

For terminals for business use managed by the company, Flex Mobility, asset management agent, and antivirus agent are installed on the devices. Use of an app is permitted or rejected **according to the device’s condition** with this approach.

Policy examples

- Limit apps for business use to attendance app, business management app, Teams, and browser (Chrome).
- Set business hours as 9:00 to 17:30.
- Check the devices’ condition by confirming that they are computers provided by the company and by checking the version of the virus detection software.
- Configure a VPN tunnel at the time of login and authorize use of privately owned computers other than the above.

Brought-in terminals and unofficial users

for specific tasks only

Without agents

Achieved using virtual desktop

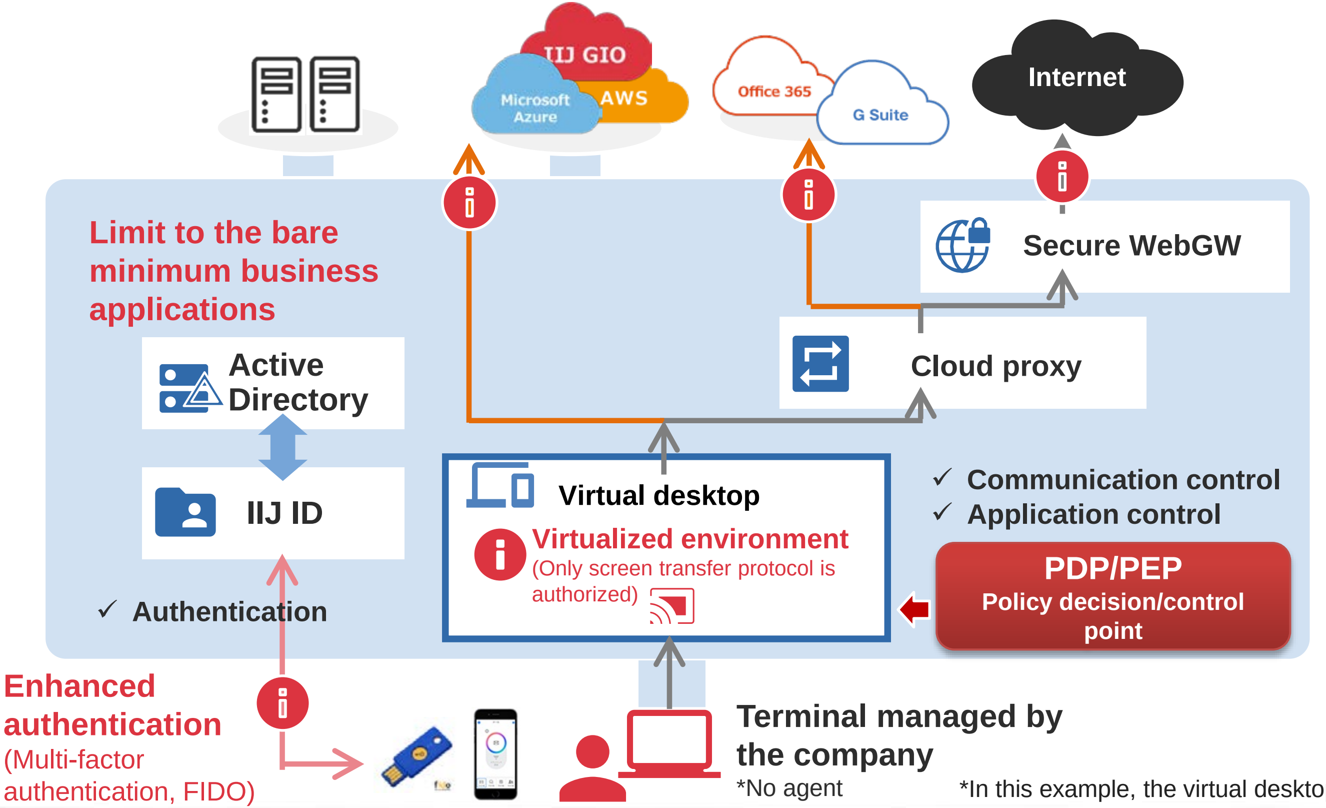
Apps authorized under specific conditions are distributed from the server to a user/a group of users in advance. Only screen transfer protocol is authorized, and the apps are used in a **virtual environment that is completely separated from the device.**

- Work can only be done via the browser and Teams on the virtual desktop that is separated from the device.
- Two-factor authentication is required for login.

Models Available Now

2. IIJ Omnibus that achieves Zero Trust

- Illustration of a configuration in which network agents are not distributed



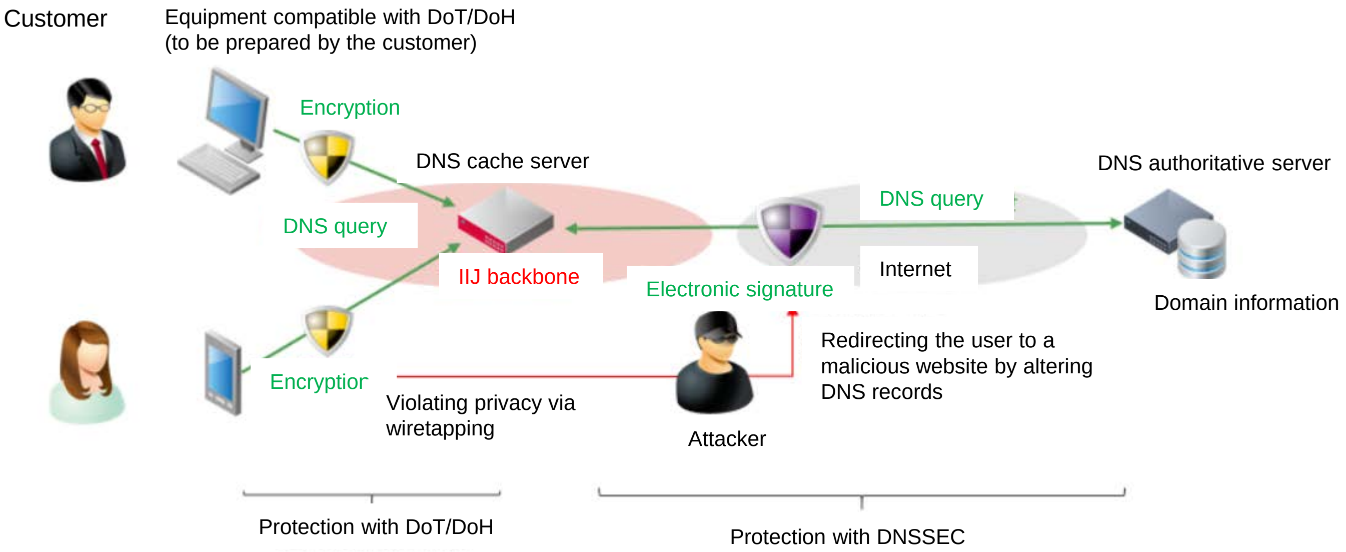
*In this example, the virtual desktop is PDP/PEP.

Internet threats from the ISP perspective

Threat of DNS spoofing

DNS encryption: A countermeasure against DNS spoofing, to which there exists unexpected vulnerability

* DNS over TLS (DoT), DNS over HTTPS (DoH), and DNS Security Extensions (DNSSEC)



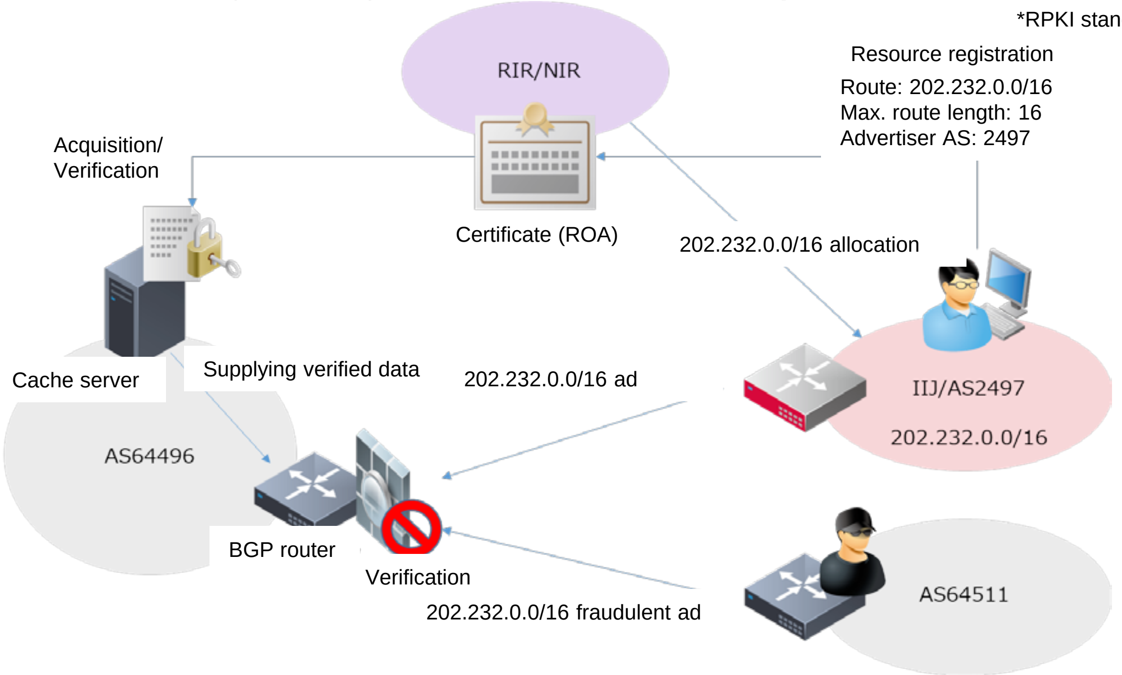
References: Engineer blog titled "*IIJ-no DNS angoka-e-no torikumi* (IIJ's DNS encryption initiatives)," https://eng-blog.iij.ad.jp/archives/5298
Press release from IIJ dated January 16, 2020, titled "*IIJ Improves the DNS Security of its Connectivity Services",* https://www.iij.ad.jp/en/news/pressrelease/2020/0116-2.html

Internet threats from the ISP perspective

Threat of internet route hijacking

Prevention of hijacking of internet routes (≒ IP addresses) with **RPKI**

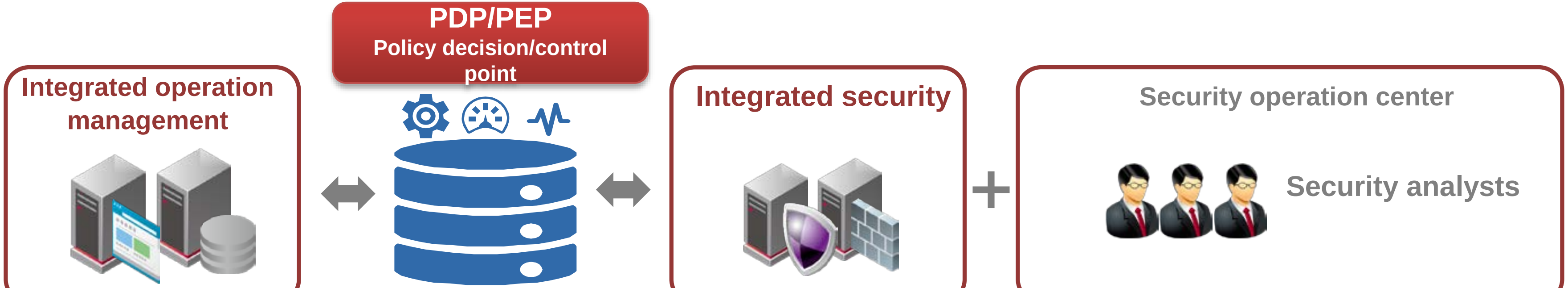
*RPKI stands for Resource Public Key Infrastructure.



Reference: Engineer blog titled “*Internet-wo yori robust ni. RPKI hajimemasu.* (Make the internet more robust. We will begin RPKI.)”
https://eng-blog.iij.ad.jp/archives/6861

3. Future vision of Zero Trust to be achieved with IIJ Omnibus

◆ Integrated operation management and security enabled by monitoring all points



PDP/PEP
Policy decision/control point

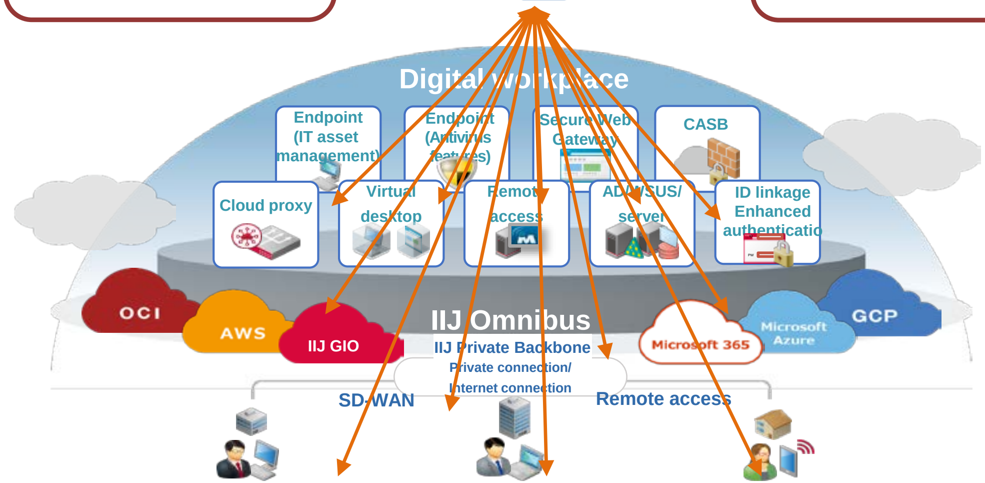
Integrated operation management

Integrated security

+

Security operation center

Security analysts



Digital workplace

Endpoint (IT asset management)

Endpoint (Antivirus features)

Secure Web Gateway

CASB

Cloud proxy

Virtual desktop

Remote access

AD/WSUS/ server

ID linkage Enhanced authenticatio

OCI

AWS

IIJ GIO

IIJ Omnibus

IIJ Private Backbone

Private connection/ Internet connection

Microsoft 365

Microsoft Azure

GCP

SD-WAN

Remote access

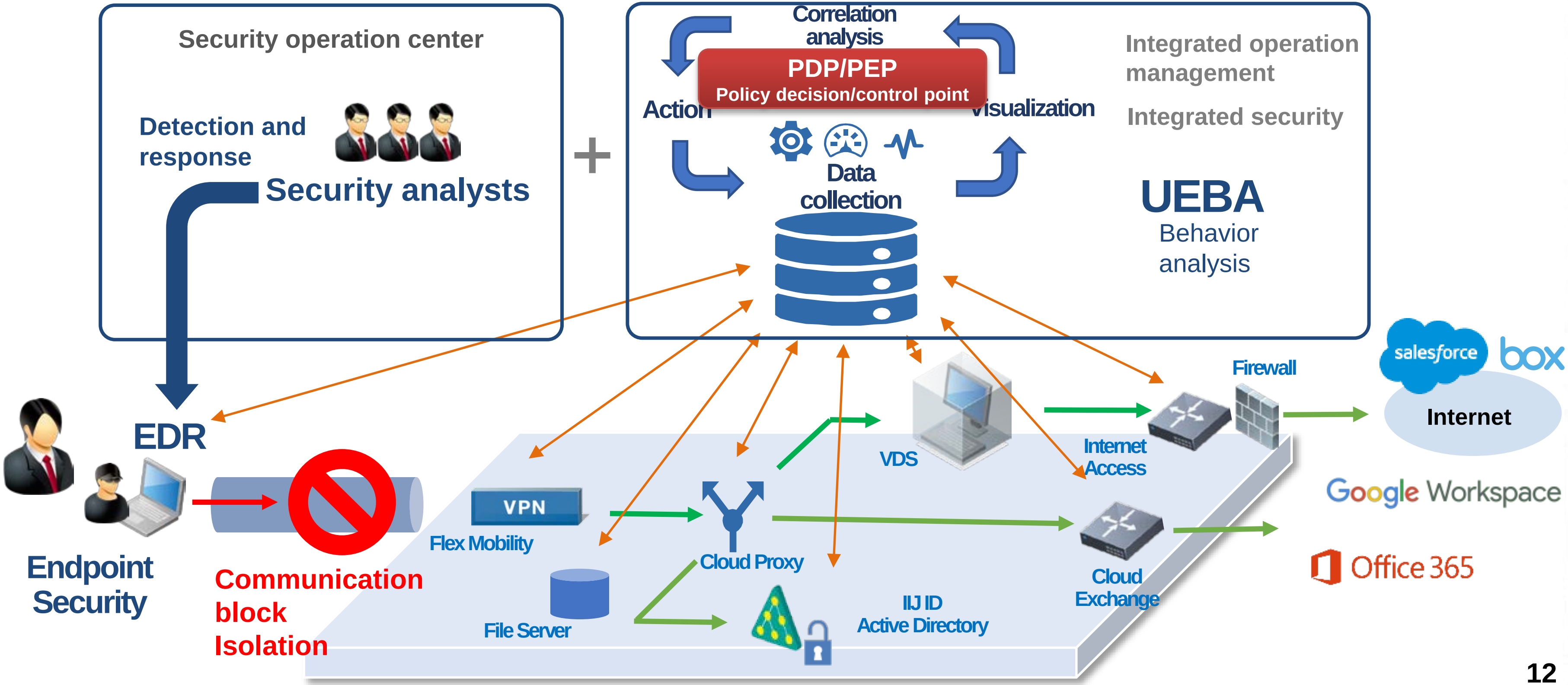
Point 1.
Authentication and authorization based on complex information, including information about the user, device, place, time, communication destination, application, and data

Point 2.
High level of security ensured by complex functions, including endpoint and gateway security

Point 3.
Provision of an environment that permits security measures to be followed continuously and an environment that enables continuous operation management

3. Future vision of Zero Trust to be achieved with IIJ Omnibus

- Use case: Early detection and blocking of security incidents



Security operation center

Detection and response

Security analysts

EDR

Endpoint Security

Communication block Isolation

Correlation analysis

PDP/PEP

Policy decision/control point

Action

Visualization

Data collection

Integrated operation management

Integrated security

UEBA

Behavior analysis

VPN

Flex Mobility

File Server

Cloud Proxy

IIJ ID

Active Directory

VDS

Internet Access

Firewall

Cloud Exchange

Internet

salesforce

box

Google Workspace

Office 365

3. Future vision of Zero Trust to be achieved with IIJ Omnibus

- □ Approval and authentication based on combined information about users, devices, place, time, access points, application, data etc.
- □ High security realized with comprehensive functions such as endpoint, gateway security etc.
- □ Environment to execute continuous counter security measures and to operate and manage continuous

IIJ Omnibus that achieves Zero Trust

New digital workplace

4. New digital workplace

◆ What is a digital workplace?

What to achieve:

Digital workplace

A world where diverse workstyles, which are free from the constraints of time and place, are enabled using digital technologies

Service that achieves a digital workplace:

IIJ Omnibus

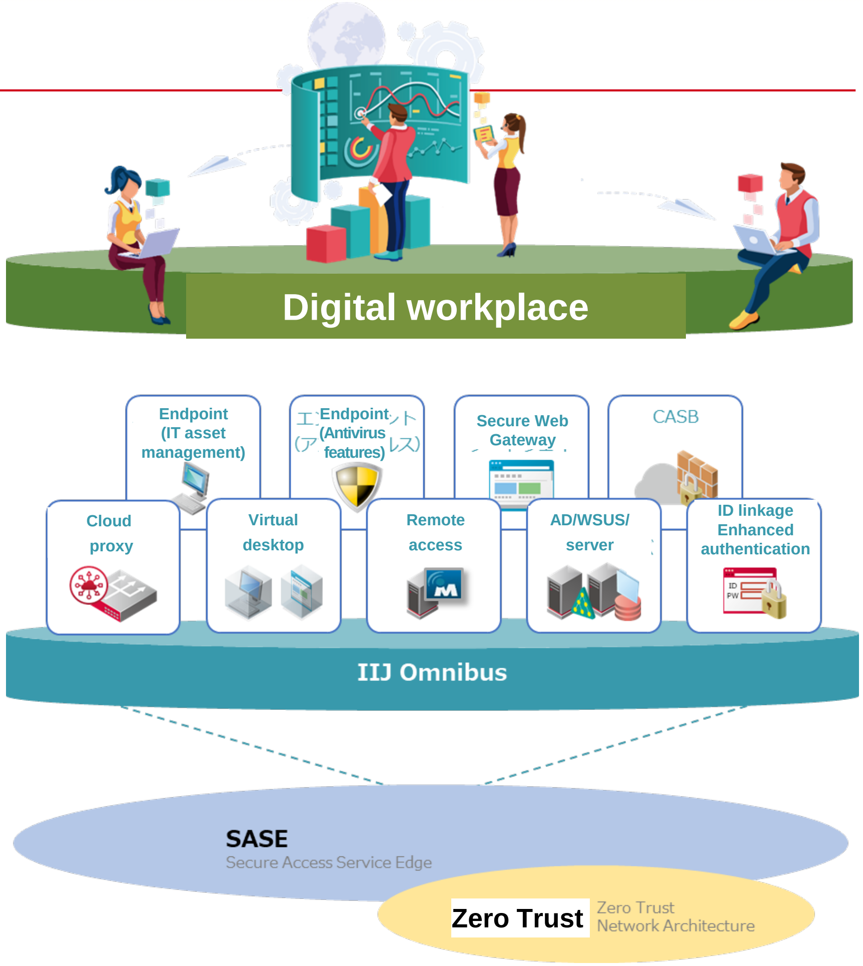
Functions needed for the platform of a digital workplace are provided as cloud services.

Concept model as the base:

Zero Trust, SASE

Network and security services are integrated, consolidated, and provided on the cloud.

A configuration based on the idea that border defense is insufficient for ensuring safety, and no access source or network is trusted



4. New digital workplace

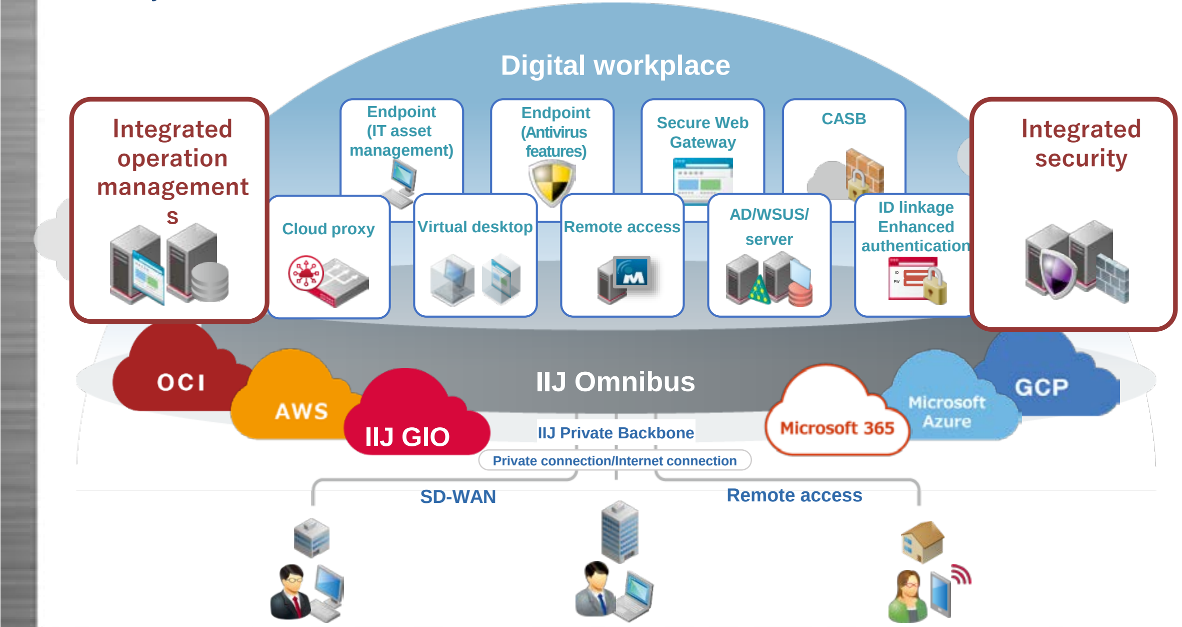
◆ Four elements that achieve the new digital workplace

Convenient telework environment
An environment that enables convenient use of IT systems, as if you were in the office

Safe, secure telework environment
Eliminating malware and other threats to internet use

Business management
Visualizing attendance status and operational status

High productivity
Productivity improvement through integrated data analysis



IIJ Omnibus

1. Convenient environment for using cloud
2. Convenient network environment
3. Convenient office IT environment

4. **Global distribution**
   - Convenient execution of operation possible globally
5. **Integrated operation management**
   - Integrated management of complex IT systems
   - Early detection and handling of bottlenecks and problems
6. **Integrated security**
   - Complex security functions without dependence on a single security function
   - Complete security from internet threats, which is enabled by the Zero Trust model

IIJ

Internet Initiative Japan

The internet started in Japan in 1992, along with IIJ. Since that time, the IIJ Group has been building the infrastructure for a networked society, and with our technical expertise, we have continued to support its development. We have also continued to evolve our vision for the future and innovate to make it a reality. As an internet pioneer, IIJ has blazed the trail so that others could realize the full potential of a networked society, and that will never change. The middle "I" in "IIJ" stands for "initiative," and IIJ alway starts with the future.

Disclaimer

Statements made in this presentation regarding IIJ’s or managements’ intentions, beliefs, expectations, or predictions for the future are forward-looking statements that are based on IIJ’s and managements’ current expectations, assumptions, estimates and projections about its business and the industry. These forward-looking statements, such as statements regarding revenues, operating and net profitability are subject to various risks, uncertainties and other factors that could cause IIJ’s actual results to differ materially from those contained in any forward-looking statement.