# Security Required in the New Normal Era
## –Points on New Challenges and Measures–

Ken Saito Takeshi Tagawa

**The new normal era has arrived as a result of the spread of COVID-19. People are shifting to styles of working that do not depend on location, such as working from home. At the same time, this phenomenon has brought into relief a variety of challenges, including increased cyber attacks and concerns around the risk of data leaks enabled by working from home. This article describes the necessary security measures for responding to the changes brought about by this new normal era.**

## 1. Introduction

A year has passed since COVID-19 began to spread throughout society. In that year, the environments and systems required to allow for working from home have advanced rapidly, and a new style of working that does not require employees to go to the office has permeated society as the new normal era. Until recently, office work has been concentrated in major cities. But now, depending on the work in question, this is not always necessary. Real events have been replaced with virtual ones, while meetings have gone online [1].

The security measures required by working from home, however, have been an afterthought for no small number of businesses. Consequently, those businesses are now faced with the pressing task of implementing the security measures and constructing secure environments for working from home.

This article aims to present ways of thinking about the newly required IT security, and measures to meet the challenges that have arisen as part of this new normal era, as well as a range of Fujitsu's security measures that can help implement the above.

## 2. Security Measures Required in the New Normal Era

This section describes how to think about security in a way that is suitable for the new normal era.

Through the use of the cloud, there has been an increase in cases where data that was previously protected by internal networks (i.e. data that was stored in internal servers) is stored externally. The risk of data leaks has also risen, with staff taking home devices, which were previously protected by firewalls and other measures inside company networks, as part of the promotion of working from home brought about by the COVID-19 crisis. Here we describe the main security points that need to be addressed to solve these issues.

### 2.1 Device Security

This section covers the device security measures that need to be taken in the new normal era. **Figure 1** shows the base security that is normally required, and the device security that has become requisite during the new normal era.

#### *2.1.1 Current Challenges*

With the number of occasions on which staff use devices at home and otherwise off premises increasing, managing those devices appropriately has become more challenging, giving rise to the following issues:

- With devices not under the original business management system, there is a need for a structure that allows devices to be controlled in accordance with company policy at all times.
- Devices may be used in ways that businesses cannot oversee, so the heightened risk of malware infection needs to be reduced.

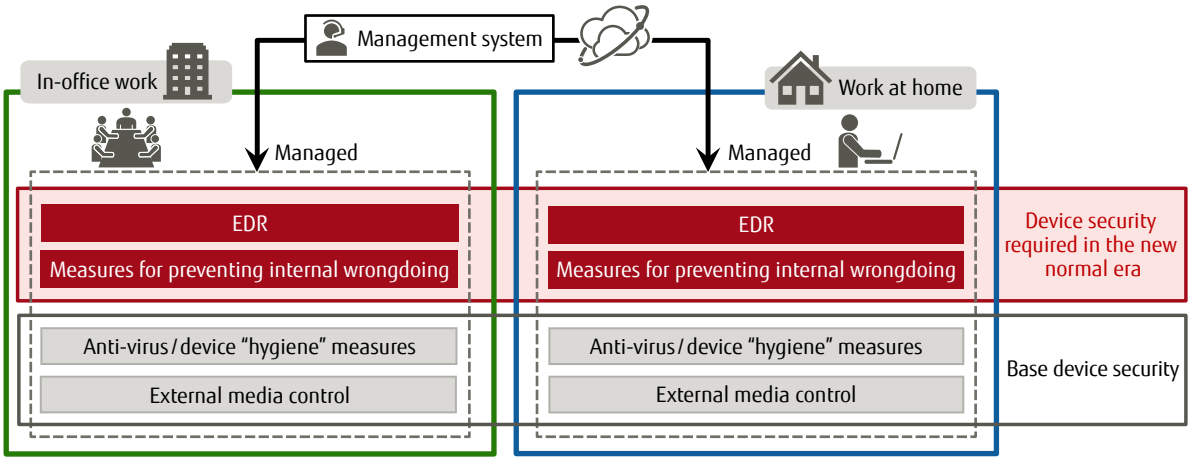



**Figure 1**
**Device security required in the new normal era.**

- At private residences, all kinds of things can be done to devices without anyone seeing, so there is a need for a structure that does not rely on individual morals.

### *2.1.2 Device Security Required in the New Normal Era*

In order to ensure consistent device security both on and off premises, the base security must first be unified both internally and externally. Building on that, companies must handle working from home through the addition of requisite security measures. (Figure 1).

1) Implementing a Base Security

The first priority for companies is to thoroughly implement a base security in both their internal and external environments.

A base security can be thought of as IT "hygiene" that includes such things as the installation of antivirus software, controls on USB devices and other external media, and the application of appropriate patches. Under work from home conditions, there are situations that cannot be covered by management systems, so security may come to be neglected. Thus it is crucial to first establish a work from home environment of the same kind as exists at the company.

2) Newly Required Measures to Prevent Cyber Attacks

Under work from home conditions, it may be difficult to implement defensive measures in line with company policy, while the use of devices in ways that are not regulated by the company increase the risk of infection with malware.

In order to meet these challenges, measures need to be taken to trace cyber attacks in devices. Measures for detecting and countering cyber attacks from the logs and other evidence left by attackers are called endpoint detection and response (EDR). They have come to greater prominence in recent years.

3) Measures to Prevent Data Leaks by Insiders

Under work from home conditions, it is more difficult to supervise the behavior of staff. Consequently, companies need security measures to minimize the risk of harm from internal threats.

The former wisdom on security focused on restricting and controlling access. Now, it is more important to detect the signs of internal corruption before it occurs, and to connect this with revisions in the education and training implemented for staff.

## 2.2 Network Security

This section describes the network security measures required in the new normal era.

### *2.2.1 Current Challenges*

As the move to working from home continues, external networks are accessed more frequently through the security gateways installed in data centers (such as firewalls and VPNs), which leads to a squeeze on bandwidth due to limits on functionality. In order to avoid

this, devices should access the cloud directly, without going through the security gateways provided by companies. On the other hand, this presents the challenge of finding measures to deal with the risk of malware infection from directly accessing dangerous clouds.

### 2.2.2 Network Security Required in the New Normal Era

This section describes the security measures required in the new normal era in order to ensure secure networks without straining bandwidth. **Figure 2** shows the network security measures that can be considered essential for achieving this.

1) Internet Breakouts

The risk of malware infections is increased due to people working from home directly accessing external clouds. To avert this risk, companies need to partition cloud access such that only clouds recognized by the company as being safe may be accessed without passing through security gateways. This type of partition is termed an "internet breakout." It is an important part of how we think about security during the new normal era, as it allows us to reduce the burden on security gateways.

2) Putting Security Functionality on the Cloud

The overconcentration of access through security gateways is one cause of the strain placed on security gateways that has come about with the rise in the number of people working from home. As a strategy for resolving this, security measures can be put on the cloud to allow for dynamic secure access. This method is termed secure access service edge (SASE). In the new normal era, companies need to provide secure internet access consistently across all locations, by putting security functionality that has previously been concentrated in data centers onto the cloud.

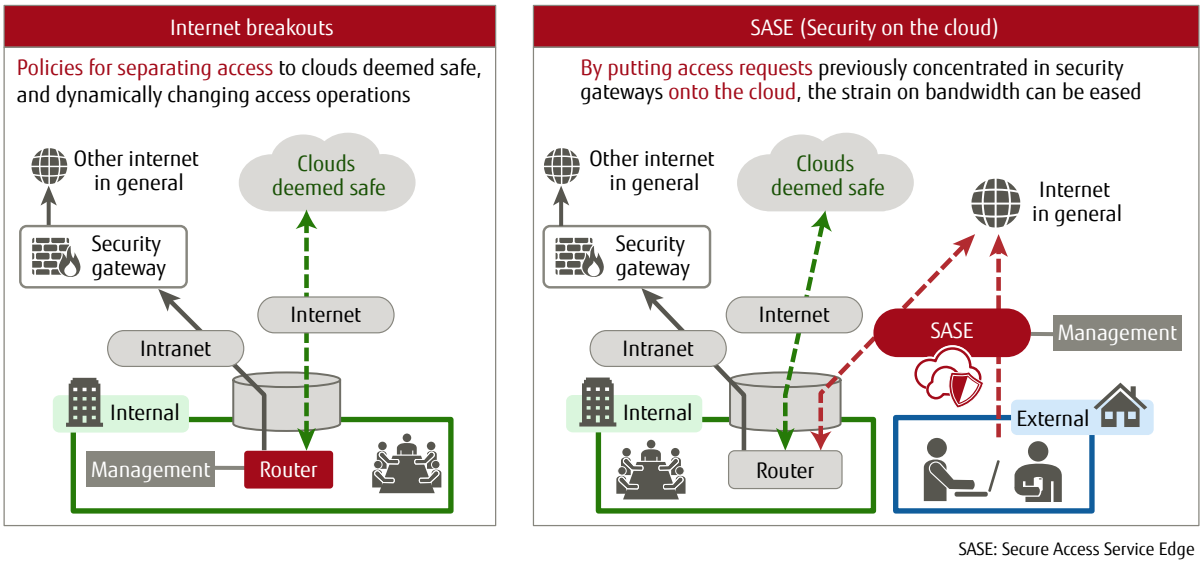
## 2.3 Cloud Security

This section describes the security measures to be taken in using the cloud.

### 2.3.1 Cloud Security Challenges

Sharing data using the cloud has become a requirement in the new normal era. With the consequent rapid increase in cloud usage, the management of the cloud has become a challenge for businesses.

One particular challenge is that management of staff is made difficult in the work from home environment, where staff are working from home or other locations, since this means that staff cannot be supervised. One possible risk that might result from this could be that staff could access a variety of websites, or make use of a variety of clouds beyond the control of company security.




SASE: Secure Access Service Edge

**Figure 2**
**Network security required in the new normal era.**

### *2.3.2 Cloud Security Required in the New Normal Era*

1) Visualizing the Status of Cloud Utilization

The risk of leaking data is increased as staff make use, on their own, of a variety of clouds (particularly consumer-oriented services), thus potentially storing data on dangerous clouds. Particularly in the work from home environment, many staff will make use of a variety of clouds.

2) Secure Settings Management for the Cloud

In some cases, it can be challenging for businesses to manage clouds when providing enterprise cloud services to staff. For example, there are endless cases where mistakes in settings have led to customer data accidentally being exposed to people outside of the company. Thus it is necessary for companies to visualize and correctly apply settings based on company policy.

## 3. Security Solutions Required in the New Normal Era

This section describes the solutions provided by Fujitsu to meet the new security needs in the new normal era.

### 3.1 Device Security Solutions

This section describes the device security solutions for working from home provided by Fujitsu.

1) Counter-Cyber Attack Solution

As described above, businesses need what are termed EDR measures to trace cyber attacks even from afar in the work from home environment. To meet this need, Fujitsu offers its "FUJITSU Security Solution Cybereason EDR Service." **Figure 3** shows an outline of the Cybereason EDR Service. Using this solution, it is possible to monitor the signs of an attack in real time while using AI to analyze the data on devices, and respond immediately by remotely disconnecting devices where necessary.

2) Insider Data Leak Countermeasure

As described above, companies need a structure that lets them detect the signs of internal corruption and so protect against it, in order to act as a measure to prevent data leaks by insiders.

To realize this, Fujitsu offers "FUJITSU Security Solution Dtex Internal Risk Visualization (UEBA) Operation Support Service." This service offers companies a solution that lets them use machine learning to understand the daily activity of their users, detect and analyze anomalies, and so prevent the risk of data leaks.

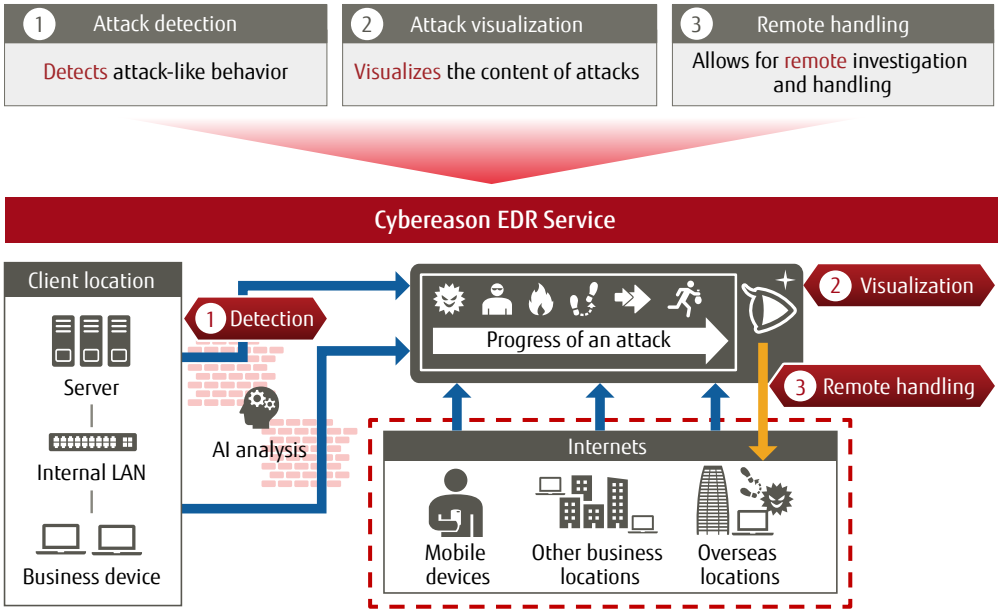



**Figure 3**
**Overview of the Cybereason EDR Service.**

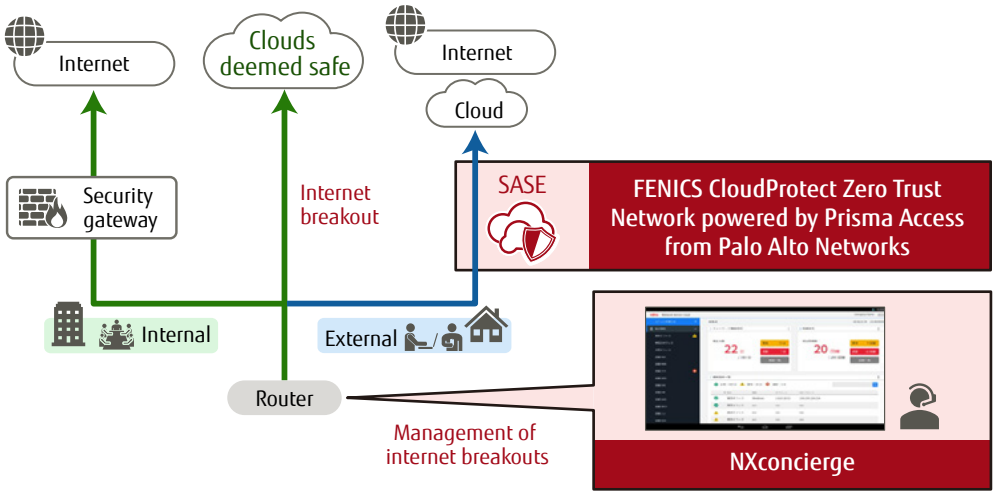



**Figure 4**
**Overview of network security solutions.**

## 3.2 Network Security Solutions

This section describes Fujitsu's network security solutions. **Figure 4** provides an overview of the system.

1) Solution for Implementing Internet Breakouts

We have already described the necessity of internet breakouts that allow for secure direct access to the web without passing through security gateways.

To implement this, Fujitsu offers "FUJITSU Network Nxconcierge" (Figure 4). This solution achieves secure access to the web while reducing the burden on security gateways by centrally managing and controlling access to the SaaS needed by clients.

2) Solution for Implementing SASE

Fujitsu offers "FUJITSU Managed Infrastructure Service FENICS CloudProtect Zero Trust Network powered by Prisma Access from Palo Alto Networks" as a solution for implementing the SASE approach that makes it possible to freely achieve secure access, by putting the security functions concentrated in data centers onto the cloud (Figure 4). By doing this, the functionality that SASE requires is provided, making it possible to achieve SASE for clients.

## 3.3 Security Solutions for Using the Cloud

This section describes security solutions for using the cloud.

1) Visualizing the Status of Cloud Utilization

Fujitsu has partnered with McAfee to provide "McAfee MVISION Cloud (CASB)," which allows businesses to implement control over the usage of the various clouds that exist. Through this solution, businesses are not only able to visualize the particular risks and staff usages of all the various clouds in the system, but also to link this up with the company's existing firewall and other security measures, and so respond through actions such as suspending services.

2) Managing Secure Settings for the Cloud

As described above, there is a risk of data leaks occurring through mistakes in configuring settings even in the clouds provided to staff by businesses.

In order to resolve this issue, Fujitsu offers "Prisma Cloud." This solution automatically finds mistakes in settings and sounds an alarm, prompting administrators to make appropriate changes.

# 4. Conclusion

Working from home has spread rapidly throughout the business world due to the spread of COVID-19. In this article, we have presented the challenges that demand improvement from businesses in terms of security in the new normal era, as well as the approaches and problem-solving solutions offered by Fujitsu.

However, challenges still exist. Cyber attacks are expected to continue advancing, while closing all the security holes that could lead to data leaks by insiders is not so easy. Going forward, these are the types of challenges for which solutions will have to be found.

Computer technology began as a means for bringing about a more prosperous world for humanity. Put another way, IT security can be thought of as the technology that ensures this dream is achieved correctly. We believe it is thus Fujitsu's responsibility to push open the doors of history to that bright future.



## References and Notes

[1] International Labour Organization: A practical Guide: Teleworking during the COVID-19 pandemic and beyond (2020).
*https://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---travail/documents/instructionalmaterial/wcms_751232.pdf*



**Ken Saito**
Fujitsu Limited, Strategic Planning and Promotion Office
Mr. Saito is engaged in educating businesses about the prevention of cyber attacks and in the promotion and marketing of security products.

**Takeshi Tagawa**
Fujitsu Limited, Strategic Planning and Promotion Office
Mr. Tagawa works on business development for cyber security products.