The bridge to possible

Hitachi, Ltd.

Hitachi to adopt SASE to implement a Zero Trust Model

Hitachi is working to restructure its security infrastructure, because users, devices, systems, and data are scattered widely inside and outside the company's network due to diversified work styles and advancement of digital technologies. Hitachi then partners with Cisco to enhance its infrastructure to ensure strict authentication of users and devices using Zero Trust architecture.

Hitachi, Ltd.

Address
1-6-6 Marunouchi,
Chiyoda-ku, Tokyo

Founded
1910

Capital
460,790 million yen
(as of March 31, 2021)

Number of employees
350,864 people (consolidated,
as of March 31, 2021)

The bridge to possible

Since its founding, Hitachi, Ltd. (“Hitachi”) has been operating its business under the corporate mission of “Contribute to society through the development of superior, original technology and products.” As this mission expresses, Hitachi emphasizes promoting its social innovation business to respond to social challenges. The corporate slogan “Hitachi Social Innovation is POWERING GOOD” reflects the company’s mission. Hitachi is committed to taking a leadership role in promoting social innovation business on a global scale.

Challenges

- Cyberattacks targeting corporations have become more sophisticated and malicious.
- Diversified work styles and cloud shifting expanded the scope of protection (including users, objects, systems, devices, information), making the solutions more complicated.
- Careful adjustments are needed to apply a new group-wide security policy for Hitachi Group comprising subsidiaries engaged in a wide spectrum of business.

Solutions

- Cisco Umbrella® is a cloud-based integrated solution that offers multiple security functions.
- Cisco Secure Access by Duo is a secure and convenient solution that provides multifactor authentication and single sign-on.
- Cisco Umbrella and Duo solutions working together enable SASE as a basis for a zero-trust strategy with Cisco Umbrella ensuring security with Internet access and Duo delivers multi-factor authentication for zero-trust security.
- Cisco has been a trusted partner to tackle these difficult challenges together.

Results

- Cisco’s SASE deployment enabled Hitachi to take a huge leap forward in security restructuring.
- Hitachi built an environment where unauthorized data transmission can be detected by authenticating users and monitoring sensors and production equipment.
- Integrated licensing provides flexible options in purchasing only the necessary software licenses.

The Future

- Hitachi aims to help their clients by sharing the accumulated know-how as a Cisco solution user.

“Cisco is a dependable partner who can share the same vision and help us tackle difficult challenges. We can do this together!”

Hitoshi Tanaka
General Manager of Global Solution 2nd Office
IT Strategy & Digital integration Division
Hitachi, Ltd.

Challenges

The limitations of closed network and perimeter-based defense

Develop a new service by combining products and technologies to improve the convenience of people's lives. Gain experience in achieving carbon neutrality and sharing the know-how to the public. Propose best use cases of adopting new technologies including drones and biometric authentication in the social infrastructure. Hitachi is engaged in such numerous varied activities as part of its commitment to promoting social innovation business.

Concurrently with these efforts, Hitachi is working to rebuild its security system because security risks surrounding corporations are becoming increasingly complex today.

A good example is the diversification of work styles. The coronavirus pandemic has spurred reforms in the way people work. Remote work, including work-at-home arrangements, became widespread, giving people more options besides commuting to their office daily.

Another example is the expanded scope of Internet use. As corporations started using cloud services and transitioned to smart factories leveraging the power of IoT, digitization of logistics, and other operations, more employees, devices, and objects are connected to the Internet. All these must be protected appropriately.

It is also important to note that cyberattacks are becoming increasingly highly developed. Attackers use a variety of highly developed techniques for targeted exploitation, from spoofed business email attempting to steal money, to ransomware demanding payment of a ransom by taking control of a corporation's information systems and confidential information.

"We need to protect more users, objects, systems, and devices from sophisticated exploitation, including targeted attacks that cannot be prevented by conventional security measures. Plus, what we need to protect is scattered all over the place. Formerly, the closed network and perimeter-based defense worked well to prevent threats to a certain degree for an environment where everything was located inside the premises. But such defense is not good enough to combat threats these days," says Tanaka.

Robust security solutions leveraged by a synergy of IT vendors

Solutions

How to authenticate users and devices

Hitachi defined overall specifications of restructuring its security infrastructure.

One of them is to enable behavior detection on computers, smartphones, and factory devices, as well as networks—paths for attackers to gain access.

"Signature-type measures are not effective enough to combat the current form of intrusions, where attackers investigate the target before attempting to gain access in a method uniquely designed for the attack. As a common practice, any unusual behavior or abnormal activity is screened for unauthorized access even though the signature-type defense did not detect it. Think of a case where a user accessed from Tokyo, but an hour later, there was access from the U.S. We had to include such behavior detection in order to ensure the security of devices and networks," says Tanaka.

Another specification is the authentication of every access per user and device, based on the Zero Trust security model.

Zero Trust is a new decentralized approach to security where the policy follows the user and verification is required for everything because anything that accesses the systems or data cannot be trusted. As the limitations of perimeter-based defense are becoming apparent, this approach is gaining popularity as a future form of security architecture. "Safety must be verified against both the users and objects, because now factory sensors and production equipment are autonomously transmitting data and accessing systems and services," says Toshihiko Ono (Hitachi).

Hitachi chose Cisco as a partner for the group-wide deployment project.

As a framework for realizing the Zero Trust security model, Hitachi looked into implementing Cisco's Secure Access Service Edge (SASE), which unifies security and network functions into a cloud-delivered service. Upon comparing several solutions, Hitachi ultimately chose Cisco's solution.

Cisco SASE mainly consists of the four solutions: Network, Cloud Security, ID/Access Management, and Monitoring. Hitachi decided to implement Cisco Umbrella for cloud security and install Cisco Secure Access by Duo ("Duo") for ID/access management.

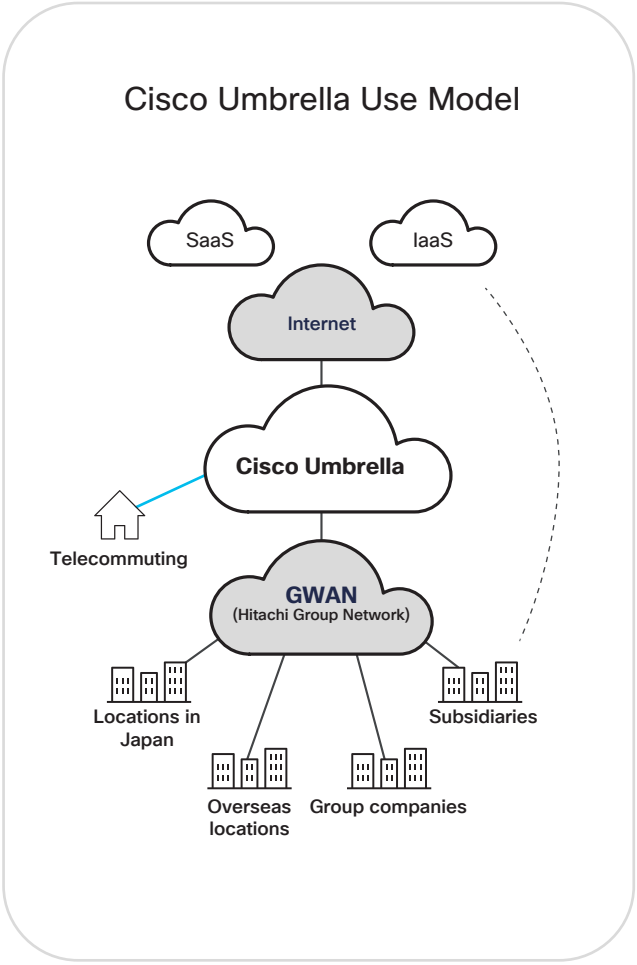
Cisco Umbrella was initially provided as Domain Name System (DNS) security solutions, enabling users outside the company to access a cloud service directly. After more functions were added, such as URL filtering, antivirus, firewall, and cloud security features, it turned into a comprehensive security suite. Duo is an authentication platform supporting multifactor authentication including biometrics. While ensuring the credibility, a basis of the Zero-Trust model, it offers the convenience through single sign-on.

"Since SASE is becoming more prevalent as an approach to realize the Zero-Trust model, many vendors are working on its development. Among the many vendors available, we chose Cisco because we wanted a good and trusted partner with inherent flexibility to our specific needs. We had to consider how the system first installed at Hitachi offices in Japan would be deployed to the rest of the Hitachi Group companies, where approximately 350,000 people work worldwide. Hitachi Group is composed of companies engaged in diverse business operations. Considering that each of the companies has circumstances unique to their nature of business, for instance, some have highly specialized machines running, the group-wide deployment is an intricate process. Cisco is a global corporation and well-versed in IT and information security, and we believe Cisco will share a same vision and work with us to tackle even the toughest challenges. That's why we chose Cisco," emphasizes Tanaka.

Results and the future

Flexible licensing enables a wide range of protection on users and devices

Hitachi initially issued approximately 50,000 licenses to its employees in Japan. This is a huge step forward in restructuring its security infrastructure.



"Multifactor authentication is required for accessing the systems and services after starting a PC at home, inside the office or from a remote location outside the office. Duo allows us to choose any combination of multifactor authentication. It enables us to design an authentication environment tailored to the work style and job type," says Ono.

For Cisco Umbrella, Hitachi issued 155,000 user licenses for its employees in Japan as the first step. Since Umbrella provides many security functions as a unified system, Hitachi is looking into assigning the licenses to devices as well.

"One of the key features of Cisco Umbrella is the secure internet gateway that prevents access to potentially dangerous or prohibited sites. This function can be enabled per user, and for devices, per production equipment or sensor. As part of IoT and data utilization amid the transition toward smart factories, we also have production equipment and sensors transmitting operating status data to other systems and services via the Internet. Using Cisco Umbrella, we can monitor the devices to see if they are transmitting data to correct destinations and check for unauthorized activities to minimize the risk of information leakage from the devices," according to Ono.

Given this view, Hitachi has entered into the EA (Enterprise Agreement) with Cisco to allow flexible and prompt application of Cisco solutions to as many users and devices as possible. This is one of the procurement options available with Cisco software products. During a valid contract term, customers can purchase and use eligible software licenses without going through the standard procurement process, enabling efficient management of the licenses. "We appreciate this service because it provides necessary scalability to rebuild the entire security infrastructure of the Hitachi Group," says Tanaka.

In line with their objectives, Hitachi believes Cisco is an essential partner of its security restructuring project, but the word "partner" has another meaning for Hitachi. It refers to a business alliance that delivers superior IT solutions to customers.

"Security is agenda top priority for all corporations. It is not something to compete with others or differentiate ourselves from them, so all of us should work together to improve the security. Anything we learned from using Cisco solutions, we'd like to share the know-how with our customers. Through a robust business alliance with Cisco, we, as IT vendors, hope to make this happen together," says Tanaka. As digitization continues to advance in society, security is becoming increasingly important. Cisco and Hitachi are the global corporations aiming to bring benefits to society, and we will work together to tackle challenges in information security.

Hitoshi Tanaka
General Manager
Global Solution 2nd Office
IT Strategy & Digital integration Division
Hitachi, Ltd.

Toshihiko Ono
Manager
Next Generation Security & Solutions Department
Global Solution 2nd Office
IT Strategy & Digital integration Division
Hitachi, Ltd.

The bridge to possible

HITACHI
Inspire the Next

In the medium-term management plan 2024, Hitachi defined targets under the slogan “Support people’s quality of life with data and technology that fosters a sustainable society.” Their targets are expressed as “Planetary Boundaries” where they protect the earth while maintaining social infrastructure by promoting social innovation business with a focus on digital, green, and innovation, as well as “well-being” that refers to a society where every individual is comfortable and active.

URL https://www.hitachi.co.jp/

Products and services

- Cisco Umbrella
- Cisco Secure Access by Duo
- Cisco Enterprise Agreement