SEVEN & I HOLDINGS CO., LTD.

CASE STUDY

CYBERARK®

Company: Seven & i Holdings Co., Ltd.

Business: Seven & i Holdings Co. is a Japan-based holding company that operates approximately 22,500 stores. The organization's business operations include convenience stores, general supermarkets, food supermarkets, department stores, specialty stores, food services, financial services and IT services.

Headquarters: 8-8 Nibancho, Chiyoda-ku, Tokyo, Japan

Established: September 2005

Seven & i Holdings Achieves a High-Level of Security Across its Global Infrastructure with CyberArk® Privileged Access Management Solutions

From convenience stores and supermarkets to department stores and financial services, Seven & i Holdings' business portfolio is vast and diverse. Through digital transformation (DX) initiatives, the company is establishing a common infrastructure for the group's entities, which will integrate supply chains, store networks, and information and logistics platform across its more than twenty-thousand-store footprint. Seven & i Holdings selected CyberArk Privilege On-Premises to be an essential protection measure for this expansive infrastructure.

THE CHALLENGE

Implementing Control over Common Infrastructure

Through a thriving global network that includes Japan and 18 other countries, Seven & i Holdings delivers value and high-quality service to 25 million store visitors every day. The holding company for the whole group is Seven & i Holdings. The business of its member companies is represented by the group's main convenience store business, 7-Eleven; supermarkets such as Ito-Yokado and York-Benimaru; department stores such as Sogo and Seibu; financial service providers like Seven Bank; and specialty stores such as Akachan Honpo and Loft. The group reported sales of about 12 trillion yen (USD 108 billion) for its fiscal year ending February 2020 created by approximately 138,000 employees.

In April 2020, the company rebranded its Group IT Strategy Promotion Headquarters to Group DX Strategy Headquarters. Seven & i Holdings' embrace of digital transformation initiatives is aimed at optimizing value across the company's services and products through the adoption of new technology and creation of a cohesive, interconnected technological environment. "One of the pillars of our growth strategy is to promote DX as a means to bring convenience and ease to the lives of people we serve; a mission that has become increasingly important when we think about the impact COVID-19 has had on society and daily life. We are currently working on our digital transformation with the implementation of a common infrastructure for the whole group," shared Kawamura Seigo, senior officer of Group DX Strategy Headquarters, IT infrastructure department.

Kawamura Seigo,
Senior Officer, Group DX Strategy Headquarters, IT infrastructure department.

Given the growing sophistication and prevalence of targeted attacks, Seven & i Holdings recognized the importance of enhancing security over across the company's global environment.

"While there is an increase in security threats, there also is a shortage of experts with in-depth security knowledge and it can be challenging for each of the group's member companies to staff a dedicated engineer with the appropriate level of experience. Also, when each member company implements its own security measures, there is always the chance that they're duplicating the efforts of another member company in the environment. Centralizing and optimizing the skill sets of experts from across the group into a common infrastructure has been important and invaluable to our digital transformation," said Kawamura.

Among the many indispensable security measures in Seven & i Holdings' common infrastructure, Kawamura set up a centralized privileged ID mechanism for each system in the environment, and a process for controlling access for these elevated credentials. "Our defenses not only have to prevent an attack from the outside, but there also is a need to implement strict security measures to protect against possible illegal internal activities. Either scenario could occur with the unauthorized use of privileged credentials. For example, an external attacker can use a privileged ID to steal sensitive information, or an internal member could exploit access to a privileged ID to do something against company policy. A strong privileged access management (PAM) program is effective at addressing the root of the issue for both internal and external incidents and contributes to strengthening our overall security posture," said Kawamura.

SOLUTION

Flexibility to Operate in Any Environment

Prior to the project be launched, there were no rigorous PAM guidelines for the whole group, so every member company implemented privileged access security measures independently. In contrast, a comprehensive PAM implementation is foundational to the company's creation of a common infrastructure. The IT infrastructure department that Kawamura belongs to is well-positioned for developing this strategy. Established in February 2020, the department was formed by hiring experts from various member companies whose internal knowledge and experience could help inform implementation of the common infrastructure and its security controls.

The department team determined that Seven & i Holdings' internal IT infrastructure required an environment where authentication information is concealed from users, and where neither users nor applications have direct access to sensitive information. The team also wanted to create an environment in which the strength of passwords is maintained with regular, automated updates to help eliminate operational workload.

CyberArk Product and Services:

- CyberArk Privilege On-Premises
- CyberArk Secrets Manager

Key Benefits:

- Flexibility to operate in a multi-cloud environment enables PAM program to scale and include all member companies
- Automated password generation and credential rotation reduces the operational workload of the PAM program
- User and application direct access to confidential information is replaced with secure session isolation
- Authentication information is concealed from the user with centralized management
- Ability to implement secrets management in a DevOps environment using the same PAM solution
- Availability of a wide range of plugin solutions for applications, API and SSL key management delivers a comprehensive, integrated approach to PAM security

Solution:

- Implementation of integrated PAM program complete with automated password rotation and privileged session isolation
- Centralization of member companies' individually operated privileged access management solutions
- Enhanced security of common infrastructure and improvement of operational efficiency of cybersecurity programs

"We assessed a number of solutions that fulfilled those requirements and the Privilege On-Premises solution really caught our attention," said Kawamura. "There were individual tools from other vendors that could be implemented for the different types of privileged access management but there were not many that offered a comprehensive, integrated approach for managing various credentials and identities. Of these, CyberArk really stood out as being the best fit for us."

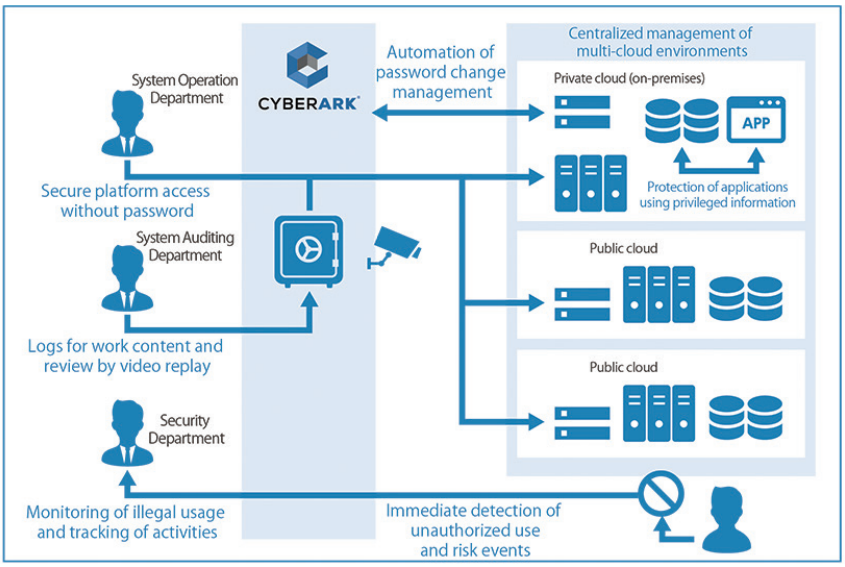
He continued, "Also, with the current common infrastructure, we've planned for each of the group's member companies to continue to operate their existing multi-cloud environments. Every company has its own unique combination of on-premises, AWS, GCP and other types of infrastructure, and CyberArk gave us a PAM solution that had the flexibility to operate in all these environments. As our PAM program has matured, we now also use CyberArk for secrets management in our DevOps environment."

In the area of functionality, Seven & i Holdings will use the wide range of applications and plugins offered by CyberArk for API and SSL key management.

IMPLEMENTATION

Implementing a Critical PAM Program

The first targets for implementation of the PAM program are member companies that were already underway with revising their administration and production environments. Every new infrastructure revision project will be assimilated into the company's common infrastructure as part of the group's overall digital transformation efforts. Seven & i Holdings anticipates that within two years, it will have supported deployment to more than 1,000 virtual machines running on approximately 500 physical servers. Over the course of the company's five-year migration plan, the number of privileged IDs running on systems in multi-cloud environments is expected to jump from a few thousand to tens of thousands.



Once the implementation is live and in full operation, all privileged access requests will be processed through an administration platform built into the common infrastructure. “To enable as many employees as possible to use the platform, including the executives of member companies, we created a unified UX that employees use to both request privileged access and receive communication about their assigned credentials. When a user requests privileged access from the platform, the decision for approval or denial will be based on the user’s rights. If approved, the user will be able to access the protected environment in an isolated session,” said Kawamura.

With automated password rotation, Seven & i Holdings has been able to easily and efficiently strengthen its security without unnecessary effort. The company also integrated CyberArk Secrets Manager into the framework for its common infrastructure. Secrets Manager uses a master key to decrypt sensitive personal information from memory so that privileged account data does not need to be embedded in application scripts and left vulnerable to exploitation.

“The management of privileged credentials can be a significant administrative burden. In addition to achieving a high level of security, the centrally managed privileged access solution we implemented from CyberArk has made a huge impact on reducing the operational workload on our security teams,” emphasized Kawamura.

Also, especially in terms of functionality, the ability to centralize management of SSH and to collect detailed audit logs and video recordings of user activity with Privilege On-Premises has been a large benefit for Seven & i Holdings.

“There are many tools for key management that break up the functions of storing, rotating, monitoring and controlling access to SSH keys but there are hardly any integrated solutions available like CyberArk. For example, remote desktop logging often requires a different system to be set up to capture the recordings, but in the case of CyberArk, these functions are all provided in a single platform and this is very helpful,” said Kawamura.

Also, centralizing the privileged access management of all its member companies increases the effectiveness of Seven & i Holdings’ security and eliminates the need to create individual secure environments, which results in a significant reduction in cost for the organization.

“In terms of the current situation of a shortage of security experts, working with CyberArk is like having a ‘guard rail’ that helps keep employees on track and protected, no matter their experience level. The ability to create this type of environment that we can use without concern is a big advantage,” explained Kawamura.

Regarding the CyberArk deployment, Kawamura has reported that the project is progressing smoothly. “Partway through, we were able to coordinate a discussion on whether the latest version of the VMware environment could also be managed by the Privilege On-Premises solution. Together with support from

CyberArk professional services consultants, we installed a customized plugin. We are grateful that they were flexible and worked with our requirements," said Kawamura.

THE FUTURE

The Future of the PAM Program

"In the future, we plan to expand access to Privilege On-Premises and make it a common service platform for the group. This will enable us to maintain centralized management of privileged access as we scale out of the current architecture to increase security standards and efficiency of operations," said Kawamura. "As we continue to collaborate closely with CyberArk, if we discover additional features and functionality that are beneficial for us, we will definitely consider adding them to our deployment. An indispensable factor of our digital transformation initiative is actively introducing and optimizing our technology footprint." CyberArk is one of the leading options for a PAM solution for the company's integrated OA environment network.

Seven & i Holdings also is interested in the perimeter security capabilities offered by CyberArk Endpoint Privileged Manager. Endpoint Privileged Manager is a solution that can prevent lateral movement of an attack by managing the local administrator authority and is an effective security measure against targeted ransomware attacks, which are a big threat. "We are attracted to Endpoint Privileged Manager as a means to enhance the level of security around computer endpoints," said Kawamura.

For the creation of its common infrastructure, Seven & i Holdings will continue to onboard additional member companies as they embark on their own infrastructure renewal projects. The full, company-wide migration will take a few years to develop, but Kawamura knows it is important to take the time to help each member company understand the aim and significance of setting up the environment; Especially when optimizing PAM for a member company will require securing operational areas that used to be outsourced to an external partner, including integrators.

Discussing Seven & i Holdings' future plans, Kawamura concluded, "One key takeaway from the creation of the current common infrastructure is the value in understanding and communicating the needs of the organization. It requires one to really understand the company's future direction and to ensure the security of that business while also ensuring that there are no damages to the current business. For any member company that may worry about challenges in daily operations stemming from our privileged access management approach, clearly explaining the significance of the initiative and expanding coverage to them within the common infrastructure eases any concerns."