

CUSTOMER SUCCESS STORY:
ORIENT CORPORATION

Orient Corporation and Fujitsu Credit Solutions Secure Sensitive Personal Information to Meet Government Privacy Laws



Customer Profile

Industry: Financial
Company: Orient Corporation
Revenue: \$2.8 Billion
Employees: 3,700

Business Impact Summary:

Business:

Orient Corporation (Orico) is an established company in the Japanese credit industry, providing a variety of financial services for the consumer market. Fujitsu Credit Solutions is a more recent entrant to the financial industry, and a joint venture between Orico and Fujitsu, to capitalize on the demand for outsourced IT services in areas including compliance, security and reliability.

Challenge:

As companies in the credit industry, both Orico and Fujitsu Credit Solutions understand the value of protecting the sensitive personal information of their customers. This sense of responsibility is reinforced by government regulations, specifically the Personal Information Protection Act and the planned Japanese version of the Sarbanes-Oxley Act. A fundamental element to protecting sensitive information is limiting and auditing access to this data.

Solution:

Orico followed the lead of Fujitsu Credit Solutions in selecting CA Access Control, a component of CA's Identity and Access Management solution, to enforce secure password policies and limit the risk of privileged administrative access. This solution is supplemented with a defined application process for those requesting privileged access. The combination improves the accountability of all parties involved in maintaining critical servers.

Result:

Orico and Fujitsu Credit Solutions have been able to protect business confidence and reliability while responding to the immediate requirement of personal information protection for their credit business. In doing so they have also built a sustainable foundation to help meet future compliance needs by mitigating the technical threat of unauthorized access.

Business

Two Related Organizations with Complementary Businesses

Established in 1954, Orico is one of the largest consumer finance companies in Japan. They provide consumer credit, credit cards, guarantee and loan agent services and direct cash loans through a network of 195 domestic branches. These financial services are also available nationwide through more than 668,000 member merchants. Orico also performs debt collection and servicing, operates a temporary employment service and offers a wide variety of other services to meet customers' needs.

Fujitsu Credit Solutions was established in 1999 through capitalization from Fujitsu and Orico. Fujitsu Credit Solutions entered a diverse credit industry where demand is increasing to provide high quality, low cost outsourcing services. In addition to their high regard in the area of compliance, the company has also established technical expertise in security, stability and reliability. By training employees to respond to new business environments, Fujitsu Credit Solutions aims to become a trusted IT advisor for its customers.

Challenge

Urgent Need to Meet Government Privacy Requirements

As a credit provider, Orico is impacted by the Japanese Personal Information Protection Act of 2005. This act requires an especially high level of protection for personal information in the medical, communication, financial and credit industries. It states that, "Credit companies must take organizational, personnel, physical, technical and safety control measures to prevent leakage, loss or damage of personal data that they handle as well as safe control of other personal data."

In response to the Personal Information Protection Act, Orico began a company wide review regarding the handling of personal information, centered on the personal information department. Specifically, Orico generated an assessment of the current state of information security and an improvement implementation plan based on guidelines from the Ministry of Economy, Trade and Industry.

Compliance requirements are expected to evolve, including the impending Japanese Sarbanes-Oxley Act. Katsumi Takahashi, System Planning Manager for Orico states, "Based on a previous incident, if personal information is disclosed externally, a penalty of approximately 15,000 yen (-\$125) per occurrence is generated. If several million items of personal information hosted on a server are leaked, damages would be in the hundreds of millions of yen."

Learning from Prior Experiences

Fujitsu Credit Solutions provides IT consulting services to Orico and was familiar with these challenges, having previously dealt with them on multiple occasions. A fundamental step in securing sensitive information is achieving strict control of access rights to the servers hosting that data. In particular, administrative accounts with unlimited access privileges such as the superuser account pose potential security risks.

"If several million items of personal information hosted on a server are leaked, damages would be in the hundreds of millions of yen."

Katsumi Takahashi
System Planning Manager,
Orient Corporation

Katsumasa Kawamura, Operating Officer at Fujitsu Credit Solutions explains, “In addition to files in which personal information is recorded, we must control important files related to business based on our relationship of performing system operations. We realized that there was a problem with an environment where an administrator who had obtained a special rights ID could easily inspect and edit files.”

“There are other security products that are also compatible with satisfying individual functional requirements. However, the only product that can cover all of the functional requirements that we require using a single product is CA Access Control.”

Katsumasa Kawamura
Operating Officer,
Fujitsu Credit Solutions

Solution

Selecting a Solution for Comprehensive Security Management

Reliably protecting their business requires a complete host access management solution that protects all of the server varieties Orico has deployed. While evaluating potential solutions, Orico performed a detailed analysis of CA's Identity and Access Management solution to test its capabilities. Takahashi describes, “For example, we checked password policy definition, automatic generation and lapse as well as history control. Furthermore, we evaluated the ability to restrict use of commands for privileged account users and the ability to protect critical files.”

CA Access Control was found to meet Orico's standards regarding the protection of personal information, while enabling efficient security administration and monitoring. “There are other security products that are also compatible with satisfying individual functional requirements. However, the only product that can cover all of the functional requirements that we require using a single product is CA Access Control,” says Kawamura.

Orico also stressed the need for their host access management solution to function in the context of their overall Identity and Access Management security strategy. In their selection of CA Access Control, Orico was pleased to find a solution that is compatible and interchangeable with other types of security software.

Restricting Terminals and Placing Server Usage on a Request Basis

Orico targeted servers that store or process personal customer information and defined access policies with a focus on secure password practices and strict tracking of user IDs. Terminals that can be used to connect to a server were also restricted, further enhancing the company's ability to regulate access. A detailed history of “who did what, when and from what terminal” is captured in audit logs, increasing accountability for server administrators.

The company auditor emphasized that Orico should develop an understanding of the usage conditions of privileged administrative IDs such as the superuser account. In particular, Orico's business presents the need to supervise subcontractors that might require privileged access. CA Access Control limits access rights for such users to the minimum set necessary to perform their job function. Orico also implemented an application process for privileged rights IDs. Application for a server login ID is performed beforehand and with the approval of the company, the process to lend a valid account with the appropriate permissions is enacted.

“The introduction of CA Access Control has produced significant results regarding not only privileged users accessing servers, but also an increase in the morals of server administrators regarding security.”

Katsumi Takahashi
System Planning Manager,
Orient Corporation

Result

Phased Deployment Enables Manageable and Scalable Solution

Given the scale of the operation, Orico opted for a phased deployment of CA Access Control. “Of the approximate 700 corporate servers, the system was introduced to 200 prioritized servers that handle personal information,” says Makoto Kurosawa, Chief Engineer at Fujitsu Credit Solutions. “These servers are not only located at the IT center, but also dispersed throughout the country.”

The application request process has also been well received — only legitimate users who have completed an application for a privileged account ID beforehand are granted appropriate access to servers. This has helped enable a 100% legitimate access rate. “The introduction of CA Access Control has produced significant results regarding not only privileged users accessing servers, but also an increase in the awareness of server administrators regarding security,” says Takahashi.

As an added benefit, securing their critical servers using CA Access Control has enabled Orico to meet the immediate requirements of the Personal Information Protection Act as well as position themselves for future compliance. “From the perspective of the Japanese Sarbanes-Oxley Act, access control and monitoring logs will become necessary for financial servers as well. These are issues regarding the entire company and we have developed a plan to have the financial planning department integrate projects.”

To learn more and see how CA software solutions enable other organizations to unify and simplify IT management for better business results, visit ca.com/customers.