“Last Bastion” to protect Business Assets

Profile

Customer	Sony Bank Incorporated
Industry	Personal Internet Banking
Country	Japan
Websites	Sonybank.net

“We take steps in advance against obvious threats before a problem occurs, and must identify the requited security measure.”

Sony Bank is Japan’s online bank that provides financial products and services for individual customers. Upon opening in 2001 and following a corporate philosophy of "fairness", Sony Bank has set a goal of establishing interest rates and prices that are based on market trends and providing easy to understand products and services. Conventionally, advanced financial services require a large workforce and therefore could be provided only to a limited number of customers. Through the utilization of IT, Sony Bank is able to provide such services to a larger number of customers, exceeding one million accounts and achieving 2 trillion yen in assets.

Sony Bank is not only focused on expanding their financial products and services, but also improving their focus on security to guard valuable assets of customers.

“Broadly speaking, there are two basic guidelines we follow regarding security protection. The first is to take steps in advance at the appropriate time against obvious threats before a problem occurs. The second is carefully select and make use of reliable security, or in other words effective security.

For example, careful examination of one-time password systems that use hardware to improve authentication shows that these are truly meaningful security measures that are both easy to understand and actually used by our customers.” Tatsuya Fukushima, System Planning Department Director

Implementation Background

Need for a “Last Bastion” to Protect Business Assets from Sophisticated Cyber Attacks

With the increasing number of threats in cyber security, such as fraudulent money transfers via online banking and an escalation in information leaks due to targeted attacks, Sony Bank felt the need to increase the level of their security now more than ever.

“Due to the recent cyber security incidents, we have decided that it is mandatory for us to strengthen our security measures. This is despite the fact that there have been no actual incidents, information leaks, or fraudulent money transfers” said Tatsuya Fukushima.

Sony Bank was considering the implementation of security improvements to their in-house system with a view toward protection against sophisticated cyber attacks such as targeted attacks. Although there has just been an introduction to a gateway security product that monitors internal networks to discover fraudulent transmissions and uses a sandbox to detect unknown cyber threats, they wanted to strengthen their protection even further.

“Under that situation, endpoint security measures as the last bastion against threats emerged as the area where we wanted to strengthen our system. Although we had already implemented a variety of measures for endpoint security, we decided that it was necessary to add an additional level of protection” said System Planning Department Manager, Shuichiro Sumimoto

Implementation History

Solution to Detect Threats Not Covered by Existing Protection

“As an endpoint security measure, we introduced pattern-matching antivirus and URL filtering, and thin client computers. However, we were also considering solutions to detect threats that could not be covered by that protection alone.
On the network layer, we have already introduced a sandbox to detect threats based on program behavior, we figured we could achieve even more robust security measures by introducing a behavioral detection product with a unique detection logic on a different protection layer (endpoint)” said Shuichiro Sumimoto.

“During the product selection process, we conducted evaluations together with a security consulting firm for a variety of products, including some from overseas security vendors. In the end, we selected FFRI yarai based on its superior balance of functionality and cost. The high level of the domestic support system was also an important factor in our determination. In terms of security in particular, due to important domestic factors such as an increase in cyber attacks targeting Japan, we placed priority on a domestic R&D system and fast domestic response for any problems that occur”, said Tatsuya Fukushima.

Implementation Results

Minimizing Operational Load While Improving the Level of Security

FFRI Yarai has been fully deployed on all computers on OA systems at Sony Bank.

“As we confirmed during the evaluation phase, there have been no issues regarding compatibility with specific system environments or products from other companies, which can often be a concern with security products. FFRI yarai works in tandem with our existing security products, with no additional load on computer performance. Prior to installation, we performed verification and generated a white list, and as a result there have been no issues with false-positives or excessive detection. The low frequency of product updates, about once or twice a year is advantageous for administrators due to the minimal amount of operational work required”, said Shuichiro Sumimoto.

Future Outlook

Importance of the Continuous Review of Security Measures

Sony Bank maintains focus on the trends in IT environment and cyber security that affect its business, for both in-house and client systems, and will continue to make improvements to its’ security measures.

“Due to current circumstances, I do not expect a downward trend in the quality or quantity of cyber attacks in the future. There is no end to security measures. We will conduct assessments at appropriate times to determine where our current level of protection might be sufficient enough in the future, and continue to not only introduce solutions, but continue to make ongoing enhancements to our security program” said Tatsuya Fukushima.

FFRI North America, Inc. 65 Enterprise,Aliso Viejo, CA,92656
Email: Sales@ffri-inc.com