ssh communications security

CASE STUDY

あなたと共感、ハーモニー・バンク
福岡ひびき信用金庫

Fukuoka Hibiki Shinkin Bank Takes Control of Privileged Users

- CryptoAuditor to monitor, control and audit remote administrators in Japan

Fukuoka Hibiki Shinkin Bank was looking for a cost-effective, secure, and extendable privileged ID management system that would bring under control the remote administrative users that access the Windows servers of the distributed organization. They found a perfect solution in CryptoAuditor from SSH Communications Security.

QUICK FACTS ABOUT THE CUSTOMER

- Headquartered in Fukuoka, Japan
- 49 branch offices with about 72,400 employees
- Offers financial services under the Shinkin Bank Act
- Serves SMEs and consumers

あなたと共感、ハーモニー・バンク
福岡ひびき信用金庫
http://www.fukuokahibiki.co.jp/

BRIEF BACKGROUND

The customer was looking for a secure and cost-effective solution that would allow monitoring and controlling of the administrative users that connect remotely to the Windows Servers of the bank. The remote users are internal administrators and trusted 3rd parties whose actions must be monitored and logged for correctness and review.

The remote connections use the Remote Desktop Protocol (RDP) to establish secure connections between remote administrators and the bank's servers. RDP connections are secured with encryption, which makes them invisible to the security team of the bank as they pass through the network perimeter and corporate firewall. The most important customer requirement was to be able to **monitor**, **control**, and **record** the actions that are taken by privileged users, while retaining the connection security offered by RDP.

SOLUTION SELECTION CRITERIA

Fukuoka Hibiki Shinkin Bank took a pragmatic yet proactive approach to selecting the solution for their privileged ID management. The desired solution would give back the capability to trace and record the sessions. They appreciated a cost-effective, high-quality solution to the problem at hand, while acknowledging that the solution would need to provide a realistic growth path to the requirements of the future. Identified future developments included support for encryption beyond the initial RDP, as well as potential integration with data loss prevention (DLP) solutions. They were aware of the migration trend towards cloud services, and valued the cloud readiness of the offered alternatives. Also, while the regulatory requirements in Japan have not yet demanded compliance with specific mandates, they anticipated that the general direction of the financial industry is moving towards more control and compliance requirements, and wanted to be ready well in advance.

The visibility into the encrypted connections was seen as critically important, but the customer also wanted to avoid a solution that would require extensive client installations and expensive user trainings.

あなたと共感、ハーモニー・バンク
福岡ひびき信用金庫
http://www.fukuokahibiki.co.jp/

"After deploying CryptoAuditor, we we able to stop using shared accounts. We also were able to hide passwords of critical systems.

Deploying CryptoAuditor really improved our security level."

Mr. Atsushi Yoshida, Team Manager,
Fukuoka Hibiki Shinkin Bank

SOLUTION

The customer selected CryptoAuditor from SSH Communications Security. The solution was delivered and deployed by a local Japanese partner. The co-operation between the customer and the partner was very successful and detailed specifications from the customer allowed them to plan and execute a smooth and rapid deployment.

CryptoAuditor monitors all of the administrative connections that are taken from outside the bank's internal network, and allows the customer to hide the actual login credentials for the servers from individual users. CryptoAuditor stores the required login credentials in a cryptographically secured vault that allows secure use of shared accounts, and dramatically reduces the risks that are involved in allowing privileged remote access to critical computing resources. With CryptoAuditor, it is always known which individual user accessed a given administrator account at a certain time, and CryptoAuditor records the administrative sessions as search-indexed videos that can be reviewed at a later date.

CryptoAuditor is a fully network-based solution that requires no additional agents or clients to be installed at neither the administrators' workstations nor the bank's servers. This deployment provides significant increase in security level due to:

- Control over third- parties' RDP sessions, with recorded evidence
- No need to share the actual privileged account credentials
- Centralized interception proxy for controlling external privileged access

WHY SSH COMMUNICATIONS SECURITY?

The benefits that tipped the selection to SSH Communications Security were:

- Licensing model that allows a cost-effective gradual deployment. The competitors' models were more rigid and resulted in unbearably expensive deployments.
- To-the-point solution that offered both support for present day requirements (such as the VMware platform) and an attractive growth path towards future requirements (with cloud readiness and support for more encryption protocols).
- Local Japanese partner with excellent support and consultation capability around the SSH Communications Security offering.

Most competing solutions require installation of additional client- and server software. This makes their deployment harder, imposes additional maintenance cost, and typically requires re-training of the end users. All these factors incur costs that translate to non-favorable total cost of ownership of the solution. CryptoAuditor's network-based approach avoids hidden costs and provides a transparent solution that imposes minimal workflow disruption and produces no operational overhead.