GLOBAL FINANCIAL COMPANY

CASE STUDY

Company: Global Financial Company

Global Financial Services Firm Overcomes Operational Complexity to Improve Emergency Access to Privileged Accounts

Industry: Financial Services
Employees: 2,400+
CyberArk Product & Services:
CyberArk Privileged Access Manager Solution
CyberArk Secrets Manager

"Overall, our team has benefited a great deal from the ease of- use and related efficiencies afforded by the CyberArk Privileged Account Security Solution."

Security Manager, Global Finanical Services Firm

With nearly 12,000 users and 85,000 break-glass accounts worldwide that enable emergency access to dozens of systems across multiple lines of business, the CyberArk Privileged Access Manager Solution automates key processes and improves productivity and accountability.

THE CHALLENGE

This global financial services firm is one of the oldest in the United States, with $2 trillion in assets. The company operates in more than 60 countries with 200,000 employees and is a leader in investment banking, financial services for consumers, small business and commercial banking, financial transaction processing, asset management and private equity.

The firm's Security and Risk Management Group was under tremendous pressure from a resource and workflow perspective. This group has wide responsibilities including on-boarding and off-boarding users, enforcing policies for break-glass and emergency privileged accounts, managing Enterprise Single Sign-On (ESSO) accounts and user authentication for more than 10,000 internal and external users.

This group needed to overcome the manual, burdensome processes required to manage nearly 50,000 emergency or break-glass accounts that enabled emergency user access to more than 20 target platforms across seven lines of business. Emergency accounts are special generic accounts used by the enterprise when elevated privileges are required to fix urgent problems, such as business continuity or disaster recovery. The accounts are often referred to as fire-call IDs or break-glass accounts and frequently require managerial approval. In this case, access to the firm's break-glass accounts is often required by users such as production support people, developers and those responsible for managing data center infrastructure.

Additionally, break-glass accounts, group- defined user rights and password generation were traditionally managed in three large, regional Lotus Notes databases for Asia, EMEA and the U.S. The complexity and resource- intense management of those databases was a significant contributor to extended password request and fulfillment times.

Primary goals for investing in a privileged identity management solution were to drive down costs to lines of business through better use of automation and decreased resources, migration from its slow, complex Notes technology, and centralization of its databases.

THE SOLUTION

After considering other solutions, the firm chose the CyberArk Privileged Access Manager Solution, which is a full life-cycle solution for securing, managing, automatically changing and monitoring all activities associated with privileged accounts.

"Given the firm's global presence and operational complexity, we required an automated solution for securing privileged accounts and managing passwords that was highly-scalable and enterprise-

ready in terms of its ability to adapt to current business practices including workflows and existing compliance requirements," commented the firm's security manager for Emergency Access, Midrange, and Mainframe within the Security and Risk Management Group.

The initial phase of the project entailed the global rollout of the Digital Vault®, a component of the CyberArk solution. The Digital Vault enables organizations to enforce an enterprise policy that protects their most critical systems, minimizes business loss, ensures accountability and approval for every access to sensitive data, and improves workforce productivity with a simple web-based access control interface and automated password replacement engine. Today, the system supports 12,000 users who need to access privileged accounts on a routine basis.

Results & Key Benefits:

- Rapid time-to-value
- Improved workforce efficiencies
- Application passwords are generated for all new projects
- Developers manage Dev-QA (self-service)
- Regular password changes
- "Firefighter accounts" auditable production access
- Successful audit related to privileged and production account management

THE RESULTS

With the CyberArk Privileged Access Manager Solution and successful integration with the firm's existing enterprise environment, including ESSO technology, three helpdesk ticketing systems and all target platforms, the firm has significantly streamlined the processes necessary for managing and granting emergency user access and automating password resets.

For example, today, if there is unusual activity detected on one of the firm's systems, an alert is automatically sent to an administrator who logs into the Digital Vault with his SSO credential, and, once approved, is granted a password to log into the system in question and observe any irregular activity. Within 24 hours, the owner of the system for which the alert was issued receives a report that the password had been accessed; the password is automatically changed so that user cannot access the system anymore. With the ESSO integration, users benefit from one shared account to all the systems they have access to based on predetermined policies and access rights.

"CyberArk's automated, enterprise-ready privileged identity management solution and dedicated team were instrumental in the success of our complex, worldwide roll-out. They were able to tackle the sheer size and complexity of the project while delivering on our requirements for greater productivity and accountability," commented the security manager.

Additional benefits included the implementation of out-of-the box and custom APIs to Oracle, SQL, Sybase and LDAP databases and the ability to easily develop custom reports. The firm will also be able to decrease the number of dedicated resources necessary for managing break-glass accounts and reassign them to other roles.

"Overall, our team has benefited a great deal from the ease-of-use and related efficiencies afforded by the CyberArk Privileged Access Manager Solution. Being able to quickly check out accounts and automate many of the related processes, we've been able to eliminate the manual steps that would traditionally bog down productivity," added the security manager.

LESSONS LEARNED

Some of the most significant challenges associated with the complexity of this global rollout was not only gaining buy-in for the technology investment, but also navigating and integrating with the specific workflows and policies of each of the firm's lines of business. For example, some groups require password resets within two days; others do not require it for up to five days. Additionally, each geography has different compliance requirements that must be taken into consideration. With the flexibility of the CyberArk solution, the Risk and Security Management Group can define different policies and workflows for multiple lines of business, which contributed to make the implementation smoother.

To encourage adoption and use of the Digital Vault, the group was diligent in "advertising" the upcoming implementation of the new system. For example, the group created web banners on its employee portal with an implementation count down, initiated the roll out of global Centers of Excellence for training and to create a level of comfort and familiarity with the new technology.

GOING FORWARD

The firm has also rolled out the CyberArk Secrets Manager in one of its lines of business. Future CyberArk implementations will provide privileged session control and isolation, session monitoring and recording, secure remote access, and privileged single sign-on capabilities.