Fiducia IT AG Relies on CyberArk to Manage 20,000+ Privileged Accounts in Support of Security & Compliance Requirements

Fiducia IT AG is the leading IT service provider for banks in Germany and offers comprehensive IT services together with its subsidiaries. The company supports the value creation of affiliated banks by providing secure IT solutions that meet the needs of the market and offers one of the leading bank systems in Germany.

The Challenge: Implement Privileged Account Management in a Complex Environment

As an IT service provider to the banking industry, IT security is a top priority for Fiducia. Fiducia continuously strives to enhance the protection it provides its customers and their data, and as such, turned its focus to privileged password and account management.

With a highly complex, heterogeneous data center environment consisting of more than 10,000 UNIX and Windows servers, five IBM mainframes, some 400 databases and 1,500 network components, Fiducia had more than 20,000 privileged accounts that needed to be secured and managed. Previously, Fiducia employees managed all of these privileged accounts and identities manually.

To reduce the time and effort and risk involved in managing privileged accounts, Fiducia decided to introduce an automated password management system. The system needed to be easy to implement and integrate with the existing complex system environment while offering high reliability and absolute data security. Requirements included a secure central password repository, 24/7 application availability, access to stored passwords in a disaster scenario, logical and physical access protection, end-to-end monitoring, full traceability of all activities and rapid recovery in an emergency.

CyberArk’s Privileged Account Security Solution Delivers Rich Functionality

Fiducia briefly considered developing a solution in-house. However, after a thorough research and evaluation phase that included a cost/benefit analysis, Fiducia selected the CyberArk Privileged Account Security Solution. Stephan Zimmermann, responsible for IT services, compliance and security at Fiducia, said, “With the sophisticated security, rich functionality and excellent scalability of the CyberArk Privileged Account Security Solution, it didn’t take long for us to reach a decision in favor of this product.”

CyberArk Enterprise Password Vault (EPV), part of the Privileged Account Security Solution, provides all the functionality required to securely manage shared, generic and privileged accounts across the entire lifecycle. EPV provides secure password storage, automates password management such as scheduled password changes, and policy-driven access control with flexible workflow definition.

At the heart of the solution is the patented Digital Vault, a special hardened server with multiple layers of security offering reliable protection from unauthorized access to the privileged identities it holds. Fiducia runs a highly available disaster recovery solution with a master and a backup vault. The integrated authentication and access control features such as OTP tokens, certificates, RADIUS, password and LDAP make sure that

“Selecting CyberArk was definitely the right decision. By introducing the CyberArk Privileged Account Security Solution, we were able to significantly improve process quality and meet statutory requirements more efficiently.”

Stephan Zimmermann,
Fiducia IT AG
only authorized users can access the system and the passwords, which are encrypted and stored in the Vault. A second person’s authorization can be specified as a requirement for access to particularly sensitive information—a standard procedure at Fiducia.

CyberArk’s solution meets Fiducia’s stringent requirements regarding comprehensive logical and physical access protection. This aspect was extremely important to Fiducia because they wanted to rule out any risks associated with centralized password storage.

Passwords are regularly and automatically changed on the target systems by the CyberArk Central Policy Manager (CPM). The policies which define parameters such as password complexity or the change cycle are centrally managed by the Compliance & Security Department within IT Services. At Fiducia, passwords are verified on a weekly basis and change automatically every month. Depending on the target systems, communication takes place using different protocols. Fiducia uses a total of five Central Policy Managers (CPMs) to enforce the defined policies on the target systems, which are installed in different network segments. This means that protocols do not have to communicate across firewall boundaries, supporting a distributed architecture with a central repository for passwords and single administration interface for managing the multiple network segments.

One of the biggest challenges of the project was connecting the different target systems. For example, Fiducia uses server operating systems from Oracle, SUSE, Red Hat and Microsoft in addition to database solutions from Oracle, IBM and Microsoft. Fiducia used multiple out-of-the-box plug-ins from CyberArk to connect to their target systems. Fiducia also worked with CyberArk to develop additional plug-ins which gave them the flexibility to introduce support to more systems and devices as needed, and today provides secure, privileged account management across their entire data center.

**CyberArk Supports Fiducia’s Security, Compliance and Business Requirements While Improving Efficiency**

Today, the CyberArk Privileged Account Security Solution secures and manages more than 20,000 privileged accounts across Fiducia’s heterogeneous data center—including all of the privileged accounts for all UNIX and Windows systems, the distributed databases and central network components.

The CyberArk solution helps Fiducia meet the risk management regulations of the German banking sector (MaRisk), which include requirements regarding the control of privileged and administrator accounts.

Fiducia was also able to meet their automation requirements without exception due to the CyberArk solution’s ability to automatically create and delete accounts, record logs, forward events to the SIEM solution, and create, dispatch and track audit reports. According to Mr. Zimmermann, “The automation capabilities have led to significant process improvements as well as increased efficiency. We are satisfied with the functionality and reliability of the solution. The high acceptance by our employees speaks for itself.”

Fiducia plans to integrate more systems and applications with the CyberArk Privileged Account Security environment, specifically mainframes, remote Windows systems, LDAP directories and their ticketing system.

“Selecting CyberArk was definitely the right decision. By introducing the CyberArk Privileged Account Security Solution, we were able to significantly improve process quality and meet statutory requirements more efficiently,” Mr. Zimmerman concluded.