ERSTE DIGITAL

CASE STUDY

CYBERARK®

Company: Erste Digital

Erste Digital is the IT service provider for Erste Group Bank, one of the largest financial services companies in Central and Eastern Europe. Headquartered in Vienna, Austria, Erste Digital is responsible for the operation of data centers, point-of-sale terminals, servers, PC networks, and banking software for Erste Group entities.

Industry: Financial Services

Employees: 2,000

CyberArk Product & Services:

- CyberArk Privilege On-Premises

"When I first saw CyberArk Privilege On-Premises in action, I thought, 'Now nobody needs to waste any more time on passwords!'"

Solutions Manager
Erste Digital

Erste Digital Enhances Protection Without Compromising Convenience with CyberArk Privilege On-Premises

"Whenever there is change in a company, especially when that change involves IT security, there's always the fear that daily tasks will become more complicated. However, our business users have come to thoroughly appreciate how easy managing passwords and accessing critical systems is with CyberArk Privilege On-Premises," reported a solution manager for Erste Digital.

The IT services unit oversees the critical business systems and banking software for nearly 2,200 users in multiple Erste Group locations in over 10 countries.

One of the team's responsibilities entails supporting the bank's SWIFT infrastructure. The SWIFT system enables entities to exchange information securely and efficiently with other financial institutions around the world.

Adhering to SWIFT's Customer Security Controls Framework (CSCF)

The SWIFT payment network provides important web applications that facilitate electronic transfers, such as platforms for determining exchange rates between different currencies. To secure access to these web applications, Erste Digital must monitor the activity and credential usage of hundreds of users, many of whom manage multiple passwords across many systems.

To further add to the challenge, some of the applications require SWIFT certificate passwords with extraordinary length. "Managing all of these passwords with their varying requirements was very cumbersome. No IT team wants to waste precious resources by dedicating an engineer to manually administer passwords," shared the solutions manager.

While Erste Digital has implemented single sign-on (SSO) protocols for most of its systems, elements of the SWIFT infrastructure aren't compatible with SSO. SWIFT – the Society for Worldwide Interbank Financial Telecommunications – also has launched its own customer security program to help members protect against new and emerging cybersecurity threats.

KEY BENEFITS

- Automated password rotation is more secure and frees internal resources to focus on more strategic tasks
- Session isolation and recording, and searchable audit trails ensure compliance with key requirements of SWIFT Customer Security Controls Framework (CSCF)
- Secrets management reduces risks associated with deploying new applications
- Real-time analysis of privileged user activity enables immediate detection and prevention of suspected attacks
- Seamless integration with existing technology stack maximizes value from current security tools and systems

The framework for this program emphasizes the importance of separating critical systems from less sensitive IT environments. It also requires that member institutions track and limit access to protected systems by securing privileged credentials and enhance their ability to detect and respond to suspicious privileged user activity.

CyberArk Leads in Secrets Management and Threat Analytics

To build a rigorous layer of defense around the SWIFT infrastructure, Erste Digital searched for a solution that would help simplify the management of privileged credentials and compliance with the framework.

The solutions manager recounted, "We were drawn to CyberArk Privilege On-Premises because of the platform's ability to extract and securely store secrets embedded in applications.

"We also liked the threat analytics capabilities included in the CyberArk platform. The other products we were considering had jump servers and some level of secret storage, but nothing compared to CyberArk's ability to evaluate commands as they're executed and detect in real-time when an attack may be underway."

Working in partnership with its managed service provider Bacher Systems, Erste Digital deployed CyberArk Privilege On-Premises to secure access to the bank's SWIFT environment.

Operational Efficiencies and Strengthened Defenses

"When I first saw CyberArk Privilege On-Premises in action, I thought, 'Now nobody needs to waste any more time on passwords!'" remarked the solutions manager.

CyberArk automates password rotation for access to the bank's SWIFT infrastructure, which removes the manual task of distributing new credentials and the need for individual oversight of password security.

The solutions manager highlighted, "With the automation we have with CyberArk, we can rotate privileged credentials much more often and use more complex strings to further strengthen defenses. When we had to manually update passwords, we'd maintain some of the more complicated passwords for up to two years; the longest they were valid according to SWIFT standards. Now, we're able to refresh all our credentials as often as we want with minimal effort."

To help customize access and rotation policies for an expansive directory of users, Erste Digital wrote middleware for its proprietary identity access management solution to integrate CyberArk Privilege On-Premises into the platform. CyberArk's REST APIs enabled seamless integration with the bank's existing technology stack.

"Now, we can implement the added layer of protection of having users log-in to CyberArk with multi-factor authentication, which is a requirement of SWIFT's security framework. After this initial sign-in, business users can request access to any application with just a click of a button," appreciated the solutions manager.

When Erste Digital underwent its first annual external audit for adherence to SWIFT's security framework, the IT services unit used CyberArk's searchable audit trail logs to efficiently demonstrate compliance. The solutions manager explained, "We hadn't yet finished configuring the CyberArk report engine, but we were still able to easily gather a user list and associated documentation from Privilege On Premises that verified our credentials were all centrally secured, stored, and encrypted."

Reflecting on the successful implementation of CyberArk Privilege On-Premises, the solutions manager concluded, "Our bank needs SWIFT; It's a given for us, just like using electricity, and CyberArk is now an integral part of this process."