CYBERARK®

Securing Privileged Access and the SWIFT Customer Security Controls Framework (CSCF)

A Guide to Leveraging Privileged Account Security to Assist with SWIFT CSCF Compliance

CYBERARK®

Table of Contents

Executive Summary

Establishing a Strong Standard for SWIFT Customers

The Society of Worldwide Interbank Financial Telecommunication (SWIFT) network provides a global community of financial institutions (over 11,000 customers scattered across 200+ countries) the ability to exchange sensitive information relating to international financial transactions. Naturally, this network is highly sought after by attackers as recent history has revealed some of the largest ever cyber heists involving fraudulent payment instructions being sent directly over the SWIFT network. In an effort to establish a consistent secure framework and baseline of accountability, SWIFT has introduced the SWIFT Customer Security Controls Framework (CSCF). This framework has been split into three main objectives, seven core principles that align with the objectives, and 27 controls that alight to each principle. Both mandatory and advisory security controls will need to be implemented across this entire community to mitigate the risk of future attacks.

Each organization will be required to self-attest to prove compliance by January 1st of 2018 and on an annual basis thereafter. Failure to do so can result in being reported to the local supervisory authority as well as the non-compliance status being viewable to all other users and counterparties within the SWIFT network. While attackers have not successfully breached the SWIFT network directly, they have found ways to capture legitimate SWIFT operator credentials through sophisticated hacking techniques to steal funds in the hundreds of millions from banks around the world. Protecting the back offices, PCs and workstations that are connected to the network is paramount for financial institutions that leverage SWIFT to do business.

The Role of Privileged Account Security

Protecting the Privileged Pathway for SWIFT Customers

Securing and managing privileged accounts should be an integral part of any organizations strategy in achieving SWIFT CSCF compliance. Privileged credentials are almost always the initial target after a network perimeter has become compromised. In the wrong hands, privileged accounts enable attackers to disable an organizations security controls, steal confidential information, disrupt business operations, and most importantly, commit financial fraud as we've seen in previous attacks. Organizations using SWIFT need to proactively implement controls to protect against, detect and respond to cyber attacks to not only comply with this regulation, but to also avoid costly breaches. With the necessary privileged account security solution in place, financial institutions can effectively and efficiently secure privileged accounts across all IT systems improving their overall security posture.

CyberArk is the industry leader in securing privileged accounts. Designed from the ground up, CyberArk has developed a powerful, modular technology platform that delivers one of the industry's most comprehensive Privileged Account Security solutions. CyberArk has led the market in securing enterprises against cyber attacks that take cover behind insider privileges and attack critical enterprise assets. Today, only CyberArk is delivering a new category of targeted security solutions that help organizations stop reacting to cyber threats and get ahead of them, preventing attack escalation before irreparable damage is done.

With CyberArk solutions, you can:

- Secure your SWIFT infrastructure and general IT environment
- Limit and control the access of all SWIFT operators
- Detect and respond to high risk activity

Controls Mapping

The table below highlights some of the key mandatory controls where securing privileged accounts plays a critically important role and the key capabilities of CyberArk's solution for implementing those controls.

Key SWIFT CSCF Controls	Key Capabilities of CyberArk's Solutions
1.1 SWIFT Environment Protection **Objective:** Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment. **Control Type:** Mandatory	CyberArk's Privileged Account Security solution suite provides the capability to isolate critical assets and create a secure control point for accessing this sensitive infrastructure. All access is logged, monitored and fully accountable. CyberArk implementation guideline highlights: ▪ Implement session isolation and credential protection ▪ Create a control point for Privileged Access ▪ Mange privileged accounts at all levels – including virtualization and cloud ▪ Implement application whitelisting, blacklisting and greylisting CyberArk Solutions: Endpoint Privilege Manager, Enterprise Password Vault, Privileged Session Manager

1.2 Operating System Privileged Account Control **Objective:** Restrict and control the allocation and usage of administrator-level operating system accounts. **Control Type:** Mandatory	CyberArk not only securely manages all privileged accounts for the operating systems, but also the rest of the IT infrastructure. Protecting the accounts from malicious use and providing full logging of all activities related to these highly critical accounts. Removing local administrative permissions is a key step in preventing credential abuse. CyberArk's least privileged solutions provide SWIFT admins with non-administrative access, with sessions which can then be elevated on-demand based on defined policies. CyberArk implementation guideline highlights: ▪ Credentials for administrative accounts are secured and managed ▪ Removal of local administrative rights and credentials ▪ Enforcement of privileged escalation ▪ Full session monitoring and accountability for privileged users CyberArk Solutions: Endpoint Privilege Manager, Enterprise Password Vault, On-demand Privileges Manager, Privilege Session Manager, SSH Key Manager
5.1 Logical Access Control **Objective:** Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts. **Control Type:** Mandatory	In almost every cyber attack, the attackers are looking for privileged accounts and credentials. This may compromise a privileged user's account or perform exfiltration of a hard coded password in a script or code. CyberArk allows organizations to enforce least privileged for all administrator access; role based access which provides the user with only the permissions they need, specific to their role. This greatly reduces the number of privileged accounts within the SWIFT environment and consequently reduces the attack surface. CyberArk implementation guideline highlights: ▪ Removal of local administrative rights and credentials ▪ Enforcement of privileged escalation ▪ Enforcement of least privilege for both Windows and Unix super users ▪ Implement privileged access control point with approval processes, to validate access requests ▪ Ensure users are given the right access at the right time, for the right reasons CyberArk Solutions: Endpoint Privilege Manager, Enterprise Password Vault, On-demand Privileges Manager, Privileged Session Manager
6.4 Logging and Monitoring **Objective:** Security events and detect anomalous actions and operations within the local SWIFT environment. **Control Type:** Mandatory	Attackers target and compromise legitimate, trusted credentials within the network. This makes detecting their abuse difficult and a serious challenge when attempting to detect and block lateral movement. Additionally it is important to identify if there are attempts to by-pass enforced controls by internal or external threat actors. CyberArk Privileged Threat Analytics implements detection capabilities around the abuse privileged credential compromise and abnormal activity. When combined with Privileged Session Manager, CyberArk can flag high risk activity within a privileged user session to identify suspicious privileged behavior. CyberArk implementation guideline highlights: ▪ Perform behavioral analysis of privileged users and credentials to identify malicious activity ▪ Detect attempts to circumvent Privileged Account Security controls – all privileged activity and logs captured are stored in the tamper-proof vault ▪ Flag high risk session activity for review by approved users CyberArk Solutions: Privileged Session Manager, Privileged Threat Analytics

The table below highlights both mandatory and advisory controls wherein CyberArk provides complementary solutions.

Key SWIFT CSCF Controls	Key Capabilities of CyberArk's Solutions
2.3 System Hardening **Objective:** Reduce the cyber attack surface of SWIFT-related components by performing system hardening. **Control Type:** Mandatory	CyberArk provides an additional layer of proactive protection through the hardening of the server and endpoint by removing local administrator credentials, reducing risk while alleviating pressure on help desk support, and enabling flexible application control, allowing organizations to prevent malicious applications from executing and utilize greylisting to run unknown applications in a restricted mode. CyberArk implementation guideline highlights: ▪ Reduce the vulnerability surface through platform hardening ▪ Removal local admin rights and credentials ▪ Enable flexible application control by placing restrictions on unknown applications CyberArk Solutions: Enterprise Password Vault, Endpoint Privilege Manager, Privileged Session Manager, SSH Key Manager
2.6A Operator Session Confidentiality and Integrity **Objective:** Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure. **Control Type:** Advisory	Through CyberArk's dedicated proxy-based jump server, all privileged sessions are protected by an encrypted RDP session which opens either SSH or https from that server to the targeted endpoint. CyberArk implementation guideline highlights: ▪ Limit potential attacker's ability to move laterally inside SWIFT infrastructure ▪ Prevent the spread of malware from end user devices to target systems ▪ Live monitoring of all privileged operator sessions and terminate any session that poses a high risk CyberArk Solutions: Enterprise Password Vault, Privileged Session Manager, Privileged Threat Analytics
2.7A Vulnerability Scanning **Objective:** Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process. **Control Type:** Advisory	CyberArk provides integrations with many vulnerability scanners – and other security solutions – to secure and manage the privileged identities used during authenticated scans. CyberArk solutions enable organizations to secure, provision, manage, control and monitor all activities associated with all types of privileged identities such as administrator on a Windows server, Root on a UNIX server, as well as embedded passwords found in applications and scripts. Additionally, users can define policies that either allow or block privileged user access to specific applications or systems that shows high-risk vulnerability scores until the vulnerability is eliminated. CyberArk implementation guideline highlights: ▪ Secure and manage privileged credentials used by vulnerability scanners ▪ Allow scanners to securely retrieve credentials when needed ▪ Automatically rotate these credentials ▪ Enhance the vulnerability scan results to reduce the attack surface CyberArk Solutions: Enterprise Password Vault, Application Identity Manager

2.8A Critical Activity Outsourcing **Objective:** Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities. **Control Type:** Advisory	CyberArk solutions provide privileged account security to third party service providers by locking down credentials and keeping a watchful eye on all user activity for both internal contractors and outsourced vendors alike. CyberArk implementation guideline highlights: ▪ Perform behavioral analysis of privileged users and credentials to identify malicious activity ▪ Identify and monitor all third party users, accounts, and associated credentials ▪ Centrally store all credentials in a secure digital vault and implement access controls for remote users requiring access to privileged accounts ▪ Isolate all sessions originating from third parties ▪ Implement live monitoring and session recording ▪ Deploy analytics tools to continuously monitor user and account activity whilst identifying and alerting on suspicious activity CyberArk Solutions: Enterprise Password Vault, Privileged Session Manager, Privileged Threat Analytics
4.1 Password Policy **Objective:** Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy. **Control Type:** Advisory	CyberArk's centralized policy management enables organizations to configure privileged account access, credential and audit policies once and automate the enforcement of those policies throughout on-premises and cloud-based IT environments. This automation helps minimize the on-going efforts and costs associated with managing privileged user and application accounts. CyberArk's password vaulting solution was designed to secure, rotate and control access to privileged account passwords based on organizational policies. The solution is proven to scale in the largest, most complex enterprise IT environments, and it can protect privileged account passwords used to access the vast majority of systems. CyberArk implementation guideline highlights: ▪ Secure, rotate and control access to privileged account passwords for the SWIFT infrastructure ▪ Secure, rotate and control access to passwords used for accessing SWIFT ▪ Apply strong access controls to all secured accounts ▪ Enforce automated credential rotation policies CyberArk Solutions: Enterprise Password Vault, SSH Key Manager
4.2 Multi-Factor Authentication **Objective:** Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication. **Control Type:** Mandatory	CyberArk solutions integrate with a range of authentication solutions to provide an added layer of security. Multi-factor authentication can be enforced for all privileged accounts via the central login to the CyberArk solution. Secured single-sign-on to the CyberArk solution also provides secured and centralized authentication to resources throughout the organization. This can simplify strong authentication implementation while enforcing strong authentication requirements across the business. CyberArk implementation guideline highlights: ▪ Create a single point of entry for all privileged access ▪ Provide an additional layer of security against standard authentication attacks ▪ Prevent laterally movement and privileged escalation CyberArk Solutions: Enterprise Password Vault, Privileged Session Manager

5.4A Physical and Logical Password Storage **Objective:** Protect physically and logically recorded passwords. **Control Type:** Advisory	CyberArk solutions centrally secure and control access to privileged passwords based on privileged account security policies. Automated password rotation reduces the time-consuming and error-prone task of manually tracking and updating privileged passwords to easily meet audit and compliance standards. For non-human users, Cyberark will protect data residing in business systems by eliminating hard-coded credential from application scripts, configuration files and software code. Furthermore, CyberArk detects unauthorized access to privileged accounts in the Windows and Unix/ Linux environments, to identify if stored passwords have been compromised. CyberArk implementation guideline highlights: ▪ Store all privileged credentials for both human and non-human (e.g. applications) users in a tamper resistant, secure digital vault ▪ Eliminate hard-coded credentials in all application scripts ▪ Automatic password rotation eliminates advanced persistent threats ▪ Detect credential theft and compromised accounts CyberArk Solutions: Application Identity Manager, Enterprise Password Vault, SSH Key Manager, Privileged Threat Analytics
6.5A Intrusion Detection **Objective:** Detect and prevent anomalous network activity into and within the local SWIFT environment. **Control Type:** Advisory	As the industry's only targeted privileged threat analytics solution, CyberArk Privileged Threat Analytics identifies previously undetectable malicious privileged user activity. This solution produces accurate, actionable intelligence, allowing incident responders to disrupt and directly respond to attacks within and around the SWIFT infrastructure. CyberArk implementation guideline highlights: ▪ Establish a baseline of normal activity for all SWIFT infrastructure admins ▪ Detect and alert on the most critical attacks ▪ Automated response to security incidents with immediate threat containment ▪ Automatic invalidation of credentials to compromised accounts to accelerate threat response CyberArk Solutions: Privileged Threat Analytics

Support for SWIFT Reference Architectures

Customers of SWIFT will be required to identify with one of four reference architectures: Architecture A1 – Full Stack, Architecture A2 – Partial Stack, Architecture A3 – Connector, or Architecture B – No Local User Footprint. The reference architecture that best resembles their own will then help determine the necessary security controls and components to be applied that are within the scope of the framework to ensure compliance.

From a technical and working model perspective, CyberArk Privileged Account Security solutions can be deployed centrally within the general IT environment, which will then secure and mange access into the SWIFT secure zone (as shown in Figure 1.). Alternatively, a dedicated CyberArk instance could be deployed within the secure zone, specifically for securing and managing access to SWIFT system (as shown in Figure 2.). This latter option provides the highest level of security.

Organizations should work with their SWIFT representative to best understand which deployment option to undertake.

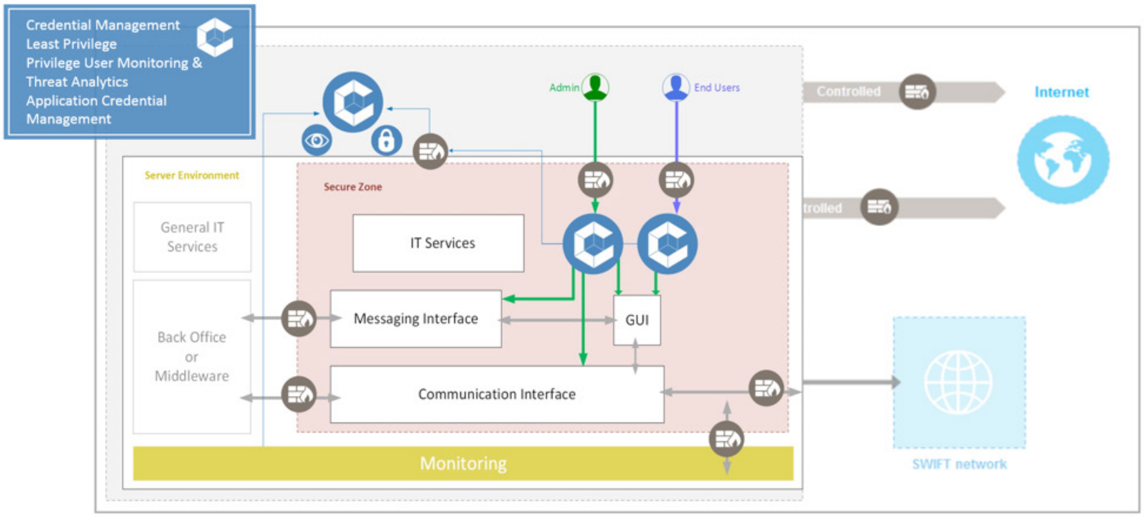


Figure 1. Secure Zone Example for Architecture A with a hybrid model – CyberArk Solutions Inside and Outside

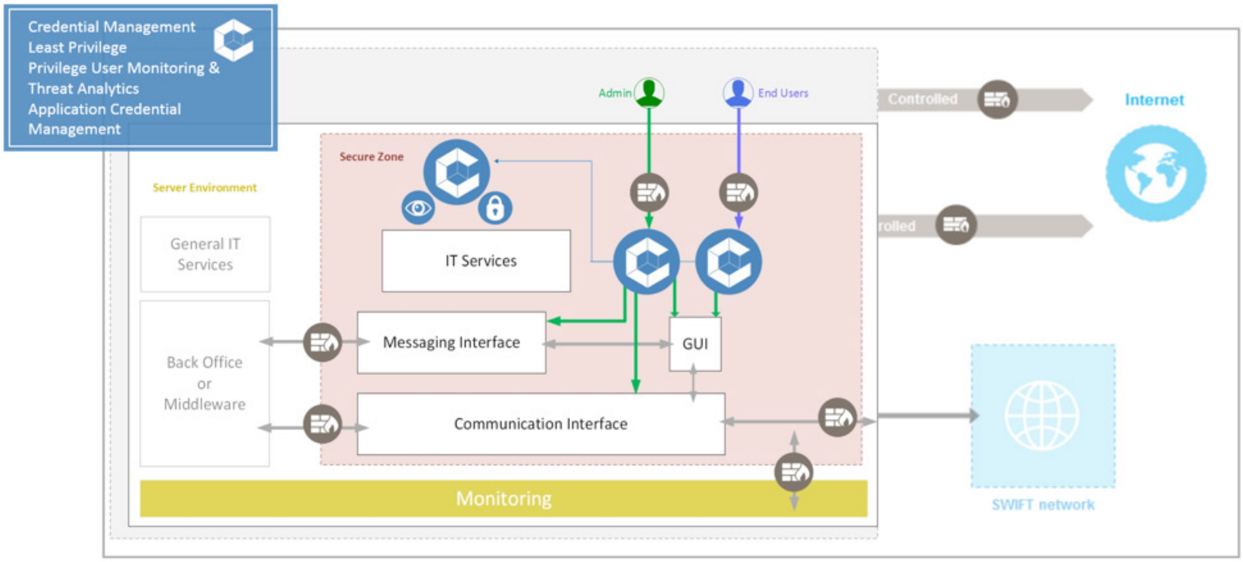
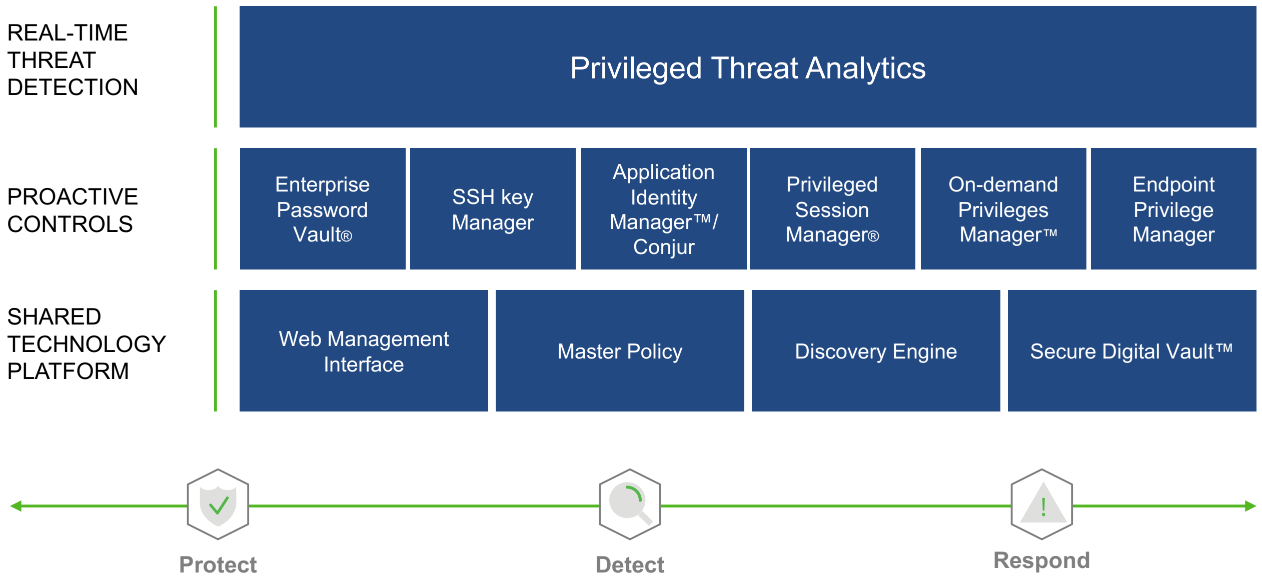


Figure 2. Dedicated Privileged Account Security Instance

CyberArk Solutions Overview

The CyberArk Privileged Account Security solution enables organizations to secure, provision, manage, control and monitor all activities associated with all types of privileged accounts. The solution is built on a common, Shared Technology Platform that delivers a single management interface, centralized policy creation and management, a discovery engine for provisioning new accounts, enterprise-class scalability and reliability, and the secure Digital Vault™. The individual products in the CyberArk Privileged Account Security Solution integrate with the Shared Technology Platform, enabling organizations to centralize and streamline management.



REAL-TIME THREAT DETECTION

Privileged Threat Analytics

PROACTIVE CONTROLS

Enterprise Password Vault® | SSH key Manager | Application Identity Manager™/ Conjur | Privileged Session Manager® | On-demand Privileges Manager™ | Endpoint Privilege Manager

SHARED TECHNOLOGY PLATFORM

Web Management Interface | Master Policy | Discovery Engine | Secure Digital Vault™

Security Solution includes the following products:

Enterprise Password Vault® – protects privileged credentials based on an organizations privileged account security policy and controls for who can access which credentials, and when

SSH Key Manager – secures, rotates and controls access to SSH keys in accordance with an organization's policy to help prevent unauthorized access to privileged accounts

Privileged Session Manager® – isolates, controls, and monitors privileged user access as well as activities for critical UNIX, Linux, and Windows-based systems, databases, and virtual machines

Privileged Threat Analytics™ – analyzes and alerts on previously undetectable anomalous privileged user behavior enabling incident response teams to disrupt and quickly respond to an attack

Application Identity Manager™ – **Conjur** – eliminates hard-coded credentials, including passwords and encryption keys from applications, service accounts and scripts with minimal to no impact on application performance

Endpoint Privilege Manager – controls privileges on the endpoint and contains attacks early in their lifecycle

On-Demand Privileges Manager™ – allows for control and continuous monitoring of the commands super-users run based on their role and task

Conclusion

CyberArk solutions provide the necessary security controls to help support the self-attestation requirements in securing the organizations environment, knowing “who” and “what” has access to critical systems and applications, and detecting and responding to high-risk activity in operator sessions.

CyberArk solutions will help your organization:

- Enforce least privilege principles and the creation of a secure zone for SWIFT related assets
- Enforce privileged account control (passwords and SSH keys) for all operating systems used within the SWIFT secure zone
- Ensure full user accountability and privileged elevation processes
- Create a separation layer within the SWIFT infrastructure isolating critical assets from the end user and the rest of the IT environment
- Enable comprehensive logging and monitoring of privileged operator sessions
- Collect, detect, alert and respond to high-risk, anomalous activity within local SWIFT infrastructure
- Provide a fully detailed and searchable audit trail of all privileged operator activity

By partnering with CyberArk, you can implement comprehensive privileged access protection to the SWIFT environment, support the necessary requirements for self-attestation, and improve the overall security posture of the financial ecosystem.

For more information, visit www.cyberark.com.

CYBERARK®

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.