Securing SWIFT Systems with ARCON|Privileged Access Management

arcon

Is your SWIFT messaging network secure?

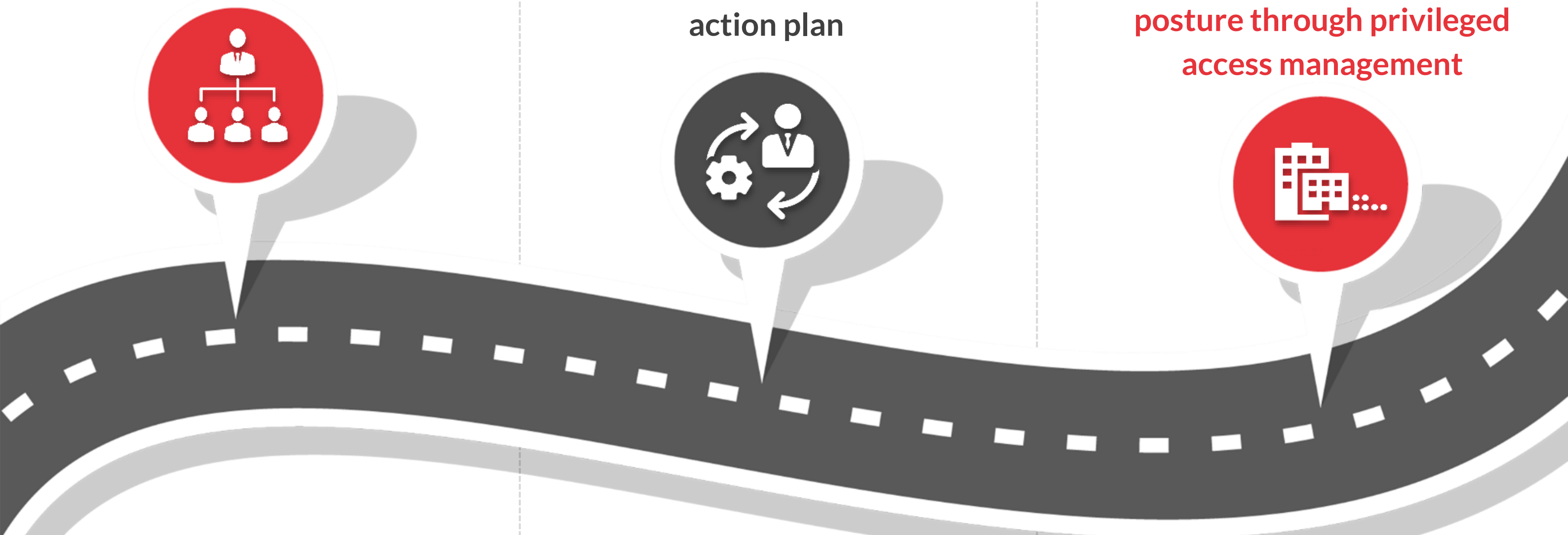
Does your IT security team possesses necessary wherewithal to thwart the insider and third party threats?

Is the IT infrastructure equipped to monitor privileged end user behaviour?

Is your organization SWIFT CSCF compliant?

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) mandates proactive security measures and controls. The SWIFT Customer security and compliance framework (CSCF) essentially provides the foundation for best security practices for an IT ecosystem especially around Privileged Access.

SWIFT CSCF: A road to robust security and controls



CSCF Security Principles

- Know and limit access
- Secure your environment
- Detect and Respond

Self-attestation action plan

- Restrict internet access
- Protect critical systems from general IT environment
- Reduce attack surface and vulnerabilities
- Physically secure the environment
- Prevent compromise of credentials
- Manage identities and segregate privileges
- Detect anomalous activity around SWIFT systems to transaction records
- Plan for incident response

How your organization can ensure enhance security posture through privileged access management

- Reinforce access control
- Enforce Principle of Least Privilege
- Apply Granular level control
- Possess Robust password vaulting and authentication
- Real-time threat alerts and monitoring
- Privileged User Escalation
- Dashboarding and audit trails

SWIFT CSCF: A road to robust security and controls

Predict, Protect, and Prevent the SWIFT messaging network from compromised elements.
Proactively manage and monitor Privileged Accounts to comply with the SWIFT Customer Security Compliance Framework (CSCF)

Rising threats to SWIFT systems: An overview

The IT threat landscape has significantly changed for today's organizations making it more challenging to address the relevant risks.

Critical information is at grave risk from compromised elements both within the organization and from third parties. The Society of Worldwide Interbank Financial Telecommunication (SWIFT) messaging network is no exception. SWIFT gives the ability to exchange confidential information and financial records internationally. The vast network of approximately 11,000 customers across 200+ countries is certainly an attractive target for cyber frauds. This was evidenced by high-profile breach such as the infamous Bangladesh Central Bank heist. By getting access to SWIFT operator credentials, cyber criminals sent fraudulent transfer requests for $81 million from the Central Bank of Bangladesh.

The membership of SWIFT has escalated to 230 banks worldwide in a span of 3 years. Primarily it started as a simple payment tool, though currently it sends wide variety of messages related to security/ treasury transactions. Almost half of the SWIFT traffic is payment based messages. Gradually the robustness of the design format produced huge scalability to provide services to banks, security dealers, trading houses, asset management companies, clearinghouses, corporate business houses, depositories, foreign exchanges etc. As a result, manual entry is never practical. The demand for automating SWIFT message creation, processing and even transferring is growing day by day. Therefore, the SWIFT IT infrastructure has grown and so has the number of privileged users accessing confidential information stored.

The challenge: Cyber frauds target privileged accounts

Most of the sophisticated cyber-attacks exploit privileged accounts, and that's exactly what happened in the Central Bank of Bangladesh heist. The malefactors could successfully capture vital administrative credentials from compromised systems after breaking the perimeter. With the help of those stolen privileged credentials, they ultimately took hostage of the SWIFT-connected systems.

In the case of Central Bank of Bangladesh, fraudsters installed monitoring software on the SWIFT-connected systems with the help of stolen admin rights. This helped them with uninterrupted access to the systems, learned how the secure message platform worked and accessed the digital certificates for authentication of SWIFT network. Thereafter, the attackers used the stolen SWIFT credentials to send financial messages, thus initiating 35 fraudulent transactions. However, this is not an isolated incident involving attack on SWIFT messaging network.

A spate of attacks followed thereafter on the Russian Central Bank, Nepal's NIC Asia Bank and Taiwan's Far Eastern International Bank.

Misuse of privileged credentials, unmonitored and uncontrolled access to target systems, weak authentication mechanism often entice malicious insiders and cyber fraudsters to exploit the security gaps and target confidential information.

These issues have now been acknowledged by several regulators across the world and resulted in various standards clearly highlighting the need of regulating privileged access management. Likewise, the SWIFT has mandated a list of controls (SWIFT Customer Security Control Frameworks (CSCF) that seek to monitor, restrict and control end-users in SWIFT environment.

SWIFT Customer Security Control Frameworks (CSCF)

*S*WIFT CSCF essentially requires users to secure systems through implementing robust granular level access control in an IT environment. It mandates a host of proactive security measures that seek to "know and Limit Access" "Secure (your) Environment" and "Detect and Respond" to thwart data breach threats.

SWIFT CSCF mandates an eight-point action plan to ensure a secure SWIFT infrastructure environment that includes:

- Restrict internet access
- Protect Critical systems from general IT environment
- Reduce attack surface and vulnerabilities
- Physically secure the environment
- Prevent compromise of credentials
- Manage identities and segregate privileges
- Detect anomalous activity around SWIFT system to transaction records
- Plan for incident response

Protecting SWIFT Systems: A strong case for implementing Privileged Access Management

Privileged Access Management solution offers a robust framework and builds a foundation for best practices in identity and access control management. This not only protects an organization from internal but also from advanced cyber threats and essentially against targeted attacks. In a larger context, besides security, the solution offers a single window for all administration activities improving efficiency and productivity.

ARCON | Privileged Access Management - A comprehensive solution

ARCON | Privileged Access Management (PAM) suite enables an organization to overcome identity & access control challenges faced in SWIFT IT environment. Trusted by 250+ enterprise customers across the globe, this highly scalable solution helps in integrating all the IT elements under a single centralized IT policy framework. The solution reinforces an organization's SWIFT systems through real-time monitoring and controlling end user activities around privileged accounts.

Security: Mitigate threats of unauthorized access

- Strong multi factor authentication
- Robust password vaulting with AES-256 bit encryption to manage, secure, and rotate privileged credentials

Efficiency: Centralized administration of all privileged activities through one admin control

- The secure gateway server serves as a centralized policy engine to restrict control and monitor privileges to target devices
- Single-Sign-On (SSO) administrative access to all underlying devices and OSs in SWIFT environment

Access Control: Restriction and elevation of commands to control activities

- The solution enforces deepest levels of granular control over privileged users based on time/day/role/ team based access to SWIFT systems
- Privileged Elevation and Delegation Management (PEDM) enables to control and monitor non-admin users having temporary elevated access rights to systems
- Enforces the principle of least privilege

Threat Alerts: Real-time monitoring, recording, and dashboarding of all privileged activities

- Advanced capabilities such as customized reporting, real-time alerts and analytics enables IT security team to improve upon privilege actions and decision making
- Each and every activity performed by end user is captured in a text and video format

SWIFT CSCF Mapping

Regulation 1.1: SWIFT Environment Protection (Mandatory)

Objective: To ensure protection of users' local SWIFT infrastructure from compromised elements in both IT and external environment.

Solution: ARCON | Privileged Access Management suite comes with robust capabilities to monitor and secure the SWIFT messaging network from compromised elements.

ARCON Secure Gateway Server enforces:

- Centralized control point through which all privileged activities both in premises and cloud are routed for real-time monitoring.
- Granular level control to restrict and control privileged users access to SWIFT systems
- Implement application blacklisting

Regulation 1.2: Operating System Privileged Account Control (Mandatory)

Objective: To restrict and control the allocation and usage of administrator-level OS accounts

Solution: ARCON | PAM provides a security cover that sits on top of all Operating systems and databases. All administrators such as Sys-admins, database admins, application admins are allowed to log on to authorized systems only on "need-to-know" and "need-to-do-basis

- ARCON | Server Manager enforces a centralized policy framework that offers granular control over privileged users and command filtering capabilities
- All privileged activities are logged via Audit Trails
- ARCON | Privileged Elevation and Delegation Management essentially discards unnecessary escalation of privileged accounts and enables controlled privilege escalation

The solution mitigates:

- Abuse of shared privileged credentials
- Misuse of elevated privileges by unauthorized users
- Threat of illegal activity by authorized users

2.3 System Hardening (Mandatory)

Objective: Reduce the cyber-attack surface of SWIFT-related components by performing system hardening

Solution: ARCON | Secure Compliance Management (SCM) is a highly effective system hardening tool.

The solution enables:

- To conduct real-time assessment of baseline security configuration for all critical technology platforms
- The tools ensures desired compliance levels
- ARCON | SCM easily integrates with ARCON | PAM

Regulation 4.1 Password Policy (Mandatory)

Objective: To ensure that passwords are resistant enough against common password hacks by implementing and enforcing an effective password policy.

Solution: ARCON Password Vault is a powerful engine that literally rules out password abuse. This electronic vault, which stores privileged passwords in a highly secure manner uses AES-256 bit encryption. It is further wrapped with a proprietary encryption algorithm. The electronic vault has release request workflow including secured printing to support emergency password retrieval in break-glass scenarios.

ARCON | Robust Password Vaulting enables to:

- Generate and rotate dynamic passwords as mandated by an enterprise IT security policy
- Secure SWIFT infrastructure from privileged password abuse and reinforce overall security and compliance framework

4.2 Multi-factor authentication (Mandatory)

Objective: Prevents any compromise of single authentication factor which allows access into SWIFT systems, by activating multi-factor authentication.

Solution: ARCON | PAM solution provides a fool proof authentication process.

To access securely access SWIFT systems, an admin user has to go through a multi-factor authentication mechanism.

- The solution easily integrates with other authentication devices such as Access Cards, Biometrics, RSA Tokens and Vasco Tokens
- ARCON itself comes with an inbuilt dual-factor authentication system with ARCON One Time Password (OTP). ARCON OTP is a mobile based app which works on all mobile devices

Regulation 5.1 Logical Access Control (Mandatory)

Objective: To enforce the security principles of required access, least privilege and segregation of duties for operator accounts.

Solution: ARCON | PAM solution enforces the principle of least privilege.

Deepest levels of granular level control over privileged users is ensured by:

- Virtual Grouping: enables the SWIFT infrastructure team to segregate privileged users and their access to authorized database and applications based on assigned roles and duties
- Granular control: restricts and elevates privileged user commands for databases to control critical activities on target devices
- Access to target devices are controlled and restricted through day/time/team/department etc.

6.1 Malware Protection (Mandatory)

Objective: Ensure the local SWIFT Infrastructure is protected against Malware

Solution: A malware attack typically originates from an end user device. Unknowingly, workforce often downloads malicious programs that are capable to hijack privileged credentials.

ARCON | PAM comes with capabilities that provides:

- Real-time alerts when any critical command/query is executed by cyber criminals on target systems
- Multi factor authentication mechanism protects target systems from being compromised as it acts a single entry point to privileged accounts

6.3 Database Integrity (Mandatory)

Objective: Ensure the integrity of database records for the SWIFT messaging interface

Solution: End users' access to SWIFT application and database records via ARCON PAM is controlled, restricted, and monitored.

ARCON | PAM enables to:

- Restrict access of non-admins users to shared database administrator accounts
- Robust Password vaulting and authentication process to thwart unauthorized access

6.4 Logging and Monitoring (Mandatory)

Objective: Record security events and detect anomalous actions and operations within the local SWIFT environment.

Solution: ARCON | PAM solution proactively secures the SWIFT environment. It logs each and every activity performed by a privileged end user on target systems in both video and text form.

The robustness of solution reduces the attack vector by:

- Capturing every command or query executed by the privileged end user through Audit Trails
- Dashboarding and session recording of all privileged sessions
- Setting real-time alerts to detect and suspend anomalous privileged activities

Conclusion

- ARCON | PAM safeguards SWIFT environment by seamlessly monitoring every single access to critical systems present in every layer of SWIFT messaging network
- Protects Administrative accounts by enforcing principle of least privilege and granular control
- Isolates anomalies in real time thereby preventing activities that could be fraudulent
- Audit trails, customized reporting, dashboarding and session recording ensure all privileged sessions are logged and monitored in real-time.
- The solution's secure password vaulting, multi factor factor authentication and Privilege Elevation & Delegation management ensures ensure that your confidential information is secure from unauthorized access

About ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us