Sepio Applicability to SWIFT Customer Security Controls Framework v2026

Compliance Mapping and Implementation Support Guide

Executive Summary

- The SWIFT Customer Security Controls Framework (CSCF) v2026 establishes mandatory and advisory security controls designed to protect the SWIFT user environment, reduce cyber risk, and support industry-wide resilience against fraud and compromise. Its three overarching objectives are to secure the environment, know and limit access, and detect and respond.
- Sepio is applicable to the CSCF because the framework repeatedly emphasizes the need to protect SWIFT-related infrastructure, customer connectors, operator PCs, network devices, secure zones, bridging servers, and other in-scope components from compromise. Sepio strengthens this posture by providing hardware-level visibility, device identity validation, rogue device detection, asset location intelligence, and continuous hardware risk monitoring across the environments that support SWIFT operations.
- Sepio is especially relevant where the CSCF requires organizations to identify and protect in-scope infrastructure components, reduce the attack surface created by unmanaged or unauthorized devices, secure customer connectors and operator environments, detect anomalous activity, and maintain accurate monitoring of the environment.
- The strongest areas of Sepio applicability are CSCF controls related to environment protection, system hardening, vulnerability scanning, physical security, malware protection, logging and monitoring, intrusion detection, and cyber incident response planning. Sepio does not replace controls such as MFA, password policy, business transaction controls, or staff screening; instead, it provides important supporting evidence and compensating visibility by validating what hardware is actually connected, where it is located, and whether it should be trusted.
- In practical terms, Sepio helps financial institutions extend the CSCF from traditional software, credential, and network controls down to the hardware layer. This is important because SWIFT environments depend not only on secure applications and credentials, but also on trusted infrastructure, trusted operator devices, trusted connectors, and trusted network paths.

Intended Audience

This compliance mapping document is intended for financial institutions and SWIFT users that need to understand how Sepio can support their SWIFT CSCF v2026 security and compliance posture.

- CISOs and security leadership: to understand how hardware-level visibility and Zero Trust Hardware Access can strengthen SWIFT environment protection, reduce blind spots, and support cyber-risk governance.
- Compliance, risk, and audit teams: to map Sepio capabilities against relevant SWIFT CSCF controls and support evidence collection, attestation preparation, and internal or external audit discussions.
- SWIFT security officers and SWIFT operations teams: to identify where Sepio can help protect SWIFT-related infrastructure, customer connectors, operator PCs, network devices, secure zones, and supporting components that fall within CSCF scope.
- IT infrastructure and network security teams: to understand how Sepio can provide continuous visibility into connected assets, detect rogue or unauthorized devices, validate hardware identity, and support secure-zone segmentation and monitoring.
- Incident response and SOC teams: to use Sepio hardware-level asset intelligence, device location, and anomaly detection as part of detection, investigation, and response workflows aligned with CSCF detect-and-respond expectations.
- Executive stakeholders in financial services: to understand the business value of extending SWIFT security controls down to the hardware layer, reducing operational, regulatory, reputational, and financial risk.

Document Objective

The objective of this document is to map Sepio hardware-level security capabilities to the relevant controls and security objectives of the SWIFT Customer Security Controls Framework v2026, helping SWIFT users understand where Sepio can support, strengthen, or provide evidence for their CSCF compliance posture.

Specifically, the document is designed to identify relevant CSCF controls where Sepio provides direct or supporting value; explain Sepio applicability to SWIFT environments; show how hardware-level visibility and Zero Trust Hardware Access reduce risks related to rogue devices, unmanaged assets, spoofed hardware, shadow IT, unauthorized peripherals, and infrastructure blind spots; support compliance, audit, and attestation discussions; and position Sepio as a complementary control layer that extends traditional cybersecurity protections beyond software, credentials, and network traffic into the physical hardware layer.

In short, the document demonstrates how Sepio helps financial institutions answer a key CSCF-related question: Can we continuously verify that the hardware assets supporting our SWIFT environment are known, authorized, trusted, and properly monitored?

How to use this guide

This guide is intended to help SWIFT users, security teams, compliance stakeholders, and auditors understand where Sepio can support the SWIFT CSCF v2026 framework. It should be used as a practical mapping tool, not as a replacement for the official SWIFT CSCF document, the organization's own risk assessment, or the formal SWIFT attestation process.

Start by identifying the organization's applicable SWIFT architecture type, such as A1, A2, A3, A4, or B. The SWIFT CSCF v2026 defines control applicability based on architecture type and in-scope components, including SWIFT infrastructure, customer connectors, operator PCs, secure zones, network devices, bridging servers, middleware, and file-transfer systems.

Next, review the Sepio applicability mapping by control. For each relevant CSCF control, the guide explains whether Sepio provides primary support, supporting evidence, limited applicability, or no direct applicability. This distinction is important because Sepio strengthens specific areas of the control environment, but it does not replace all required administrative, procedural, application, identity, or transaction-level controls.

Use the guide to support internal discussions between security, compliance, SWIFT operations, infrastructure, and audit teams. For compliance and audit preparation, use it to identify the types of evidence Sepio can provide, such as inventories of connected assets, hardware identity validation, unauthorized device alerts, device location data, policy violations, and historical asset activity.

Finally, use this guide as a starting point for a broader security conversation. SWIFT CSCF focuses on protecting the operating environment of SWIFT users, but hardware risk often extends beyond traditional software, credential, and network controls. Sepio helps organizations validate that the physical devices supporting SWIFT operations are known, authorized, trusted, and continuously monitored.

1. Purpose and Scope

This document maps Sepio's Zero Trust Hardware Access capabilities to the SWIFT Customer Security Controls Framework (CSCF) v2026. It is intended for customer-facing compliance, partner enablement, and security architecture discussions with financial institutions using SWIFT infrastructure or customer connectors.

The mapping is not a legal attestation, audit opinion, or substitute for the customer's own SWIFT CSP assessment. It identifies where Sepio can support implementation, validation, evidence gathering, and continuous monitoring for selected CSCF controls.

2. CSCF Context Relevant to Sepio

SWIFT CSCF v2026 is organized around three objectives: secure the environment, know and limit access, and detect and respond. The framework contains 32 controls: 26 mandatory controls and 6 advisory controls. SWIFT also expects users to attest compliance against mandatory controls and optionally against advisory controls.

The framework scope includes SWIFT secure zones, customer secure zones, SWIFT and customer connectors, operator PCs, network devices, HSMs, bridging servers, data exchange layers, and virtual/cloud platforms. This is where Sepio's hardware-level visibility and device validation are most relevant.

A notable v2026 change is the expanded treatment of customer client connectors. Customer client connectors are now considered mandatory in-scope components for several basic cyber hygiene controls, including 1.2, 1.3, 1.4, 2.2, 2.3, 2.6, 2.7, 3.1, 4.1, 4.2, 5.1, 5.4, 6.1, and 6.4. Sepio can help customers discover, validate, monitor, and evidence the hardware identity and physical location of these endpoints and their surrounding infrastructure.

3. Sepio Value Proposition for SWIFT CSCF

- Hardware-level inventory and asset validation: Sepio identifies and classifies devices based on physical-layer and device-level attributes rather than relying only on declared MAC, IP, hostname, firmware, or agent status.
- Continuous trust verification: Sepio supports a Zero Trust Hardware Access model by validating what is physically connected before it is trusted.
- Rogue and masquerading device detection: Sepio helps identify unauthorized, spoofed, rogue, or unmanaged hardware connected to secure zones, operator environments, bridging layers, or customer connector infrastructure.
- Precise location context: Sepio can help identify where a device is connected, such as switch/AP context, edge port, USB port, or endpoint attachment context, supporting investigation and remediation.
- Trafficless operation: Sepio does not inspect payloads and does not require taps or passive probes, making it complementary to network monitoring, SIEM, SOAR, NAC, EDR, and vulnerability management tools.
- Evidence for audits and incident response: Sepio can provide asset history, policy alerts, hardware change events, and integration-ready event records that support CSCF logging, monitoring, physical security, and incident response activities.

4. High-Level Applicability Summary

Applicability Level	Meaning	Relevant Controls
Primary applicability	Controls where Sepio directly supports the control objective or major implementation expectations.	1.1, 1.5, 2.3, 2.4, 3.1, 6.4, 6.5A, 7.1, 7.3A, 7.4A
Supporting applicability	Controls where Sepio provides evidence, context, device validation, or integrations that strengthen an existing control.	1.2, 1.3, 1.4, 2.1, 2.2, 2.6, 2.7, 2.8, 5.1, 5.2, 5.4, 6.1, 6.2, 7.2
Limited / indirect applicability	Controls where Sepio can provide context but does not implement the core requirement.	2.5A, 2.10, 4.1, 4.2
Not primary	Controls Sepio should not be positioned as satisfying.	2.9, 2.11A, 5.3A, 6.3

5. Detailed Control Mapping

Use the table below as a customer-facing mapping. “Sepio applicability” indicates how Sepio may help satisfy, evidence, or strengthen the control. Customers remain responsible for assessing applicability based on their architecture type and in-scope components.

Control	CSCF control title	Sepio applicability	How Sepio supports the control	Typical evidence / artifacts
1.1	SWIFT Environment Protection	Primary	Validates that only authorized hardware is present in or around the SWIFT secure zone; detects rogue, masquerading, or unmanaged devices that could bypass segmentation assumptions.	Asset inventory, AssetDNA/ device validation, secure-zone hardware baseline, alerts for new/unknown devices, switch/ port/AP/USB context.
1.2	Operating System Privileged Account Control	Supporting	Does not manage OS privileged accounts, but provides context on the systems and hardware where privileged actions may occur and supports monitoring of unauthorized hardware introduced near privileged administration paths.	Hardware inventory of systems, operator PCs, jump servers and network devices; alerts for unexpected devices; event records to SIEM/SOAR.

Control	CSCF control title	Sepio applicability	How Sepio supports the control	Typical evidence / artifacts
1.3	Virtualisation or Cloud Platform Protection	Supporting	Does not replace hypervisor or cloud security controls. Supports visibility into physical hosts, network devices, and on-premises infrastructure supporting virtualization or virtual VPN components.	Physical/virtualization host asset context, network device validation, change history, integration with CMDB.
1.4	Restriction of Internet Access	Supporting	Does not enforce web filtering or proxy policy. Helps detect unauthorized connectivity paths, unmanaged network devices, rogue gateways, or hardware that may introduce internet exposure.	Detection of unmanaged switches, rogue network devices, unauthorized hardware changes, location-based policy evidence.
1.5	Customer Environment Protection	Primary	Highly relevant for Architecture A4 customer connector environments. Helps protect customer connectors by validating the hardware and network devices that host or surround the connector.	Customer connector hardware inventory, trusted device baseline, detection of rogue/ unknown devices, physical location and topology context.

Control	CSCF control title	Sepio applicability	How Sepio supports the control	Typical evidence / artifacts
2.1	Internal Data Flow Security	Supporting	Does not provide encryption or application-flow authentication. Supports assurance that the endpoints, servers, and network devices participating in internal SWIFT-related flows are known and validated.	Verified asset inventory for SWIFT-related components and data-flow infrastructure; rogue device alerts.
2.2	Security Updates	Supporting	Does not patch systems. Supports accurate asset inventory and hardware/ software context that can improve patch scoping, prioritization, and evidence completeness.	Inventory completeness, device classification, vulnerability intelligence correlation where available, CMDB enrichment.
2.3	System Hardening	Primary	Helps validate that hardening assumptions are not undermined by unauthorized peripherals, rogue network devices, unmanaged switches, spoofed devices, or hidden hardware.	Policy rules for allowed/ unauthorized devices, hardware identity validation, USB/network peripheral detection, hardware change alerts.

Control	CSCF control title	Sepio applicability	How Sepio supports the control	Typical evidence / artifacts
2.4	Back Office Data Flow Security	Primary	Supports identification and monitoring of bridging servers, first-hop connectivity, and devices participating in back-office-to-SWIFT flows. Does not replace cryptographic protections.	Topology and asset context for bridging servers, middleware/ file-transfer infrastructure, ports and network paths, anomaly alerts.
2.5A	External Transmission Data Protection	Limited / indirect	Sepio does not implement encryption for external transmissions. It can help validate that endpoints and devices used for transmission are trusted and unchanged.	Device identity and asset validation at external connector endpoints.
2.6	Operator Session Confidentiality and Integrity	Supporting	Does not encrypt sessions. Can detect suspicious hardware used to compromise operator sessions, such as unauthorized USB peripherals, IP-KVM, rogue input devices, or unexpected endpoint hardware.	Host peripheral visibility, USB/ device policy enforcement support, alerting for rogue operator devices.

Control	CSCF control title	Sepio applicability	How Sepio supports the control	Typical evidence / artifacts
2.7	Vulnerability Scanning	Supporting	Sepio is not a traditional vulnerability scanner. It complements scanning by improving inventory accuracy and identifying hardware assets that scanners may miss or misclassify.	Hardware asset inventory, device classification, vulnerability/risk context, known-to-vulnerable asset reporting where available.
2.8	Outsourced Critical Activity Protection	Supporting	Can provide evidence and monitoring for customer-owned or provider-hosted hardware components where Sepio has visibility, helping validate outsourced infrastructure assumptions.	Asset inventory for outsourced/hosted components, connector validation, reporting for third-party assurance discussions.
2.9	Transaction Business Controls	Not primary	Sepio does not validate payment transaction logic, reconciliation, confirmation, RMA, or transaction business rules.	No primary Sepio control claim. May provide infrastructure trust context only.

Control	CSCF control title	Sepio applicability	How Sepio supports the control	Typical evidence / artifacts
2.10	Application Hardening	Limited / indirect	Sepio does not harden SWIFT applications. It supports the surrounding infrastructure by detecting unauthorized hardware changes that could compromise hardened applications.	Hardware-level monitoring around application hosts and operator PCs.
2.11A	RMA Business Controls	Not primary	Sepio does not manage RMA authorizations or counterparty business controls.	No primary Sepio control claim.
3.1	Physical Security	Primary	One of the strongest Sepio alignments. Sepio helps validate physical asset presence, device identity, location, and unauthorized hardware attachment across sensitive environments.	Physical-layer asset discovery, location context, unauthorized hardware alerts, USB/ removable/connected device visibility, evidence reports.
4.1	Password Policy	Limited / indirect	Sepio does not enforce password policy. It may help identify unmanaged systems or devices that should be subject to password controls.	Asset inventory and unmanaged device detection.

Control	CSCF control title	Sepio applicability	How Sepio supports the control	Typical evidence / artifacts
4.2	Multi-Factor Authentication	Limited / indirect	Sepio does not provide MFA. It can strengthen the trust posture of devices used for privileged access or administration.	Trusted device validation for operator/admin environments; detection of rogue endpoints.
5.1	Logical Access Control	Supporting	Does not replace IAM. Extends access governance by adding device-level trust: whether the hardware participating in access is known, authorized, and physically where expected.	Device identity, location-based context, unauthorized device detection, integration into NAC/SIEM/SOAR workflows.
5.2	Token Management	Supporting	Does not manage token lifecycle. Can detect hardware tokens/removable devices or unauthorized USB attachments when visible through Sepio Host capabilities.	USB/removable device visibility, operator PC device monitoring, event logs.
5.3A	Staff Screening Process	Not primary	Sepio has no role in HR screening or background checks.	No Sepio applicability.

Control	CSCF control title	Sepio applicability	How Sepio supports the control	Typical evidence / artifacts
5.4	Password Repository Protection	Supporting	Does not manage password repositories. Can monitor hardware around systems or operator PCs used to access password repositories and detect unauthorized removable devices.	Endpoint peripheral monitoring, unauthorized hardware alerts, asset evidence.
6.1	Malware Protection	Supporting	Sepio is not antivirus/EDR. It complements malware controls by detecting malicious or unauthorized hardware implants and peripherals that can enable compromise without malware on the host.	Rogue hardware alerts, USB/ network peripheral detection, host/network asset validation.
6.2	Software Integrity	Supporting	Does not verify software binaries. Helps detect hardware changes that may indicate tampering, unauthorized platforms, or unexpected systems hosting SWIFT-related software.	Hardware baseline, host asset validation, change history.

Control	CSCF control title	Sepio applicability	How Sepio supports the control	Typical evidence / artifacts
6.3	Database Integrity	Not primary	Sepio does not perform database integrity validation or database control monitoring.	No primary Sepio control claim.
6.4	Logging and Monitoring	Primary	Strong alignment. Sepio generates security events related to asset changes, unknown devices, location changes, policy violations, and hardware anomalies. These can feed SIEM/ SOAR and support response workflows.	Audit trail, alerts, asset history, policy violations, integration with SIEM/SOAR/CMDB, forensic timelines.
6.5A	Intrusion Detection	Primary	Sepio complements NIDS/ HIDS by detecting hardware-level intrusions and rogue/ masquerading devices without packet inspection. It is especially useful where declared identity or traffic analysis is insufficient.	Trafficless device discovery, rogue device detection, spoofing/masquerade detection, integration alerts.

Control	CSCF control title	Sepio applicability	How Sepio supports the control	Typical evidence / artifacts
7.1	Cyber Incident Response Planning	Primary	Supports IR with rapid identification of unauthorized hardware, connection location, timeline of changes, and affected assets. HWDR can strengthen response when customers lack hardware security expertise.	Incident evidence, device timeline, port/location, policy history, HWDR service support.
7.2	Security Training and Awareness	Supporting	Can support awareness around hardware attack techniques, rogue devices, supply-chain risks, and operator environment threats.	Hardware security workshops, attack scenario demonstrations, internal awareness material.

Control	CSCF control title	Sepio applicability	How Sepio supports the control	Typical evidence / artifacts
7.3A	Penetration Testing	Primary	Supports hardware-focused test scenarios, including rogue device insertion, spoofed peripherals, unmanaged switches, IP-KVM, and physical-layer bypass attempts.	Detection validation scenarios, evidence from alerts, red-team/purple-team test reports.
7.4A	Scenario-based Risk Assessment	Primary	Highly relevant for scenario-based assessments involving hardware supply chain compromise, insider device insertion, rogue customer connectors, unauthorized bridging devices, and secure-zone bypass.	Scenario mapping, risk evidence, attack path validation, asset and location reports.

6. Compliance Positioning by Control Cluster

Secure the environment - segmentation, secure zones, customer connectors

Deploy Sepio as a continuous hardware validation layer for SWIFT secure zones and customer secure zones. The strongest messaging is that segmentation and secure zones are only as trustworthy as the physical devices connected to them. Sepio helps verify that devices are genuine, authorized, and located where expected.

Know and limit access

Deploy Sepio as device-level trust that complements IAM, PAM, MFA, and logical access control. The key message: user identity is not enough if the device used for access is unknown, spoofed, or compromised.

Reduce attack surface - hardening, data flows, vulnerabilities

Deploy Sepio as an inventory accuracy, hardware trust, and anomaly detection control that complements patching, hardening, encryption, and vulnerability scanning. Sepio is not replacing cryptographic controls or vulnerability scanners.

Detect and respond

Deploy Sepio as a monitoring and detection source for hardware anomalies. Sepio events can enrich SIEM/SOAR, improve incident triage, and support forensic reconstruction of unauthorized hardware activity.

Physically secure the environment

Deploy Sepio as directly applicable. The ability to validate hardware identity, detect rogue devices, and locate assets strengthens the customer's physical security evidence beyond badge access, CCTV, and facility controls.

Incident response and risk exercises

Deploy Sepio as enabling hardware-based incident response and realistic scenario testing: rogue customer connector, unauthorized USB device, unmanaged switch, physical bypass, or supply-chain device masquerading as a legitimate asset.

7. Evidence Package Sepio Can Provide for CSCF Discussions

- Current inventory of discovered hardware assets in SWIFT-related zones, customer connector environments, operator PC environments, and relevant network segments.
- Validated device identity records, including hardware-level classification and trusted/unknown status.
- Change history showing first seen, last seen, location change, and policy violation events.
- Rogue, unknown, spoofed, or non-compliant device alerts.
- Physical location evidence such as switch, port, access point, USB port, endpoint, or infrastructure tag where supported.
- Integration logs or event forwarding evidence to SIEM, SOAR, CMDB, NAC, ticketing, or case-management systems.
- Reports supporting incident response, forensic analysis, or scenario-based risk assessment.
- Policy configuration showing allowed and unauthorized hardware profiles for secure zones and operator environments.

8. Customer-Facing Compliance Wording

For Control 3.1 Physical Security

Sepio supports physical security controls by continuously validating the identity, location, and status of hardware assets connected to SWIFT-related environments, customer connector infrastructure, operator endpoints, and associated network devices. Sepio helps detect unauthorized or masquerading devices that may not be visible through conventional logical access or traffic-monitoring controls.

For Control 2.7 Vulnerability Scanning

Sepio does not replace vulnerability scanning. It improves the quality and completeness of vulnerability management by providing an independent hardware asset inventory and risk context for assets that may be missed, misclassified, or hidden from conventional scanners.

For Control 6.4 Logging and Monitoring

Sepio contributes hardware-level security events and asset-change telemetry to the monitoring program, including unknown device detection, hardware identity changes, physical location changes, and policy violations. These events can be integrated into SIEM/SOAR workflows to improve investigation, escalation, and response.

For Control 7.4A Scenario-based Risk Assessment

Sepio enables realistic scenario assessments for hardware supply-chain compromise, unauthorized customer connectors, rogue devices, malicious peripherals, and secure-zone bypass attempts. Sepio evidence can be used to validate detection and response readiness for these scenarios.

For Control 6.5A Intrusion Detection

Sepio complements traditional NIDS/HIDS by detecting hardware-level intrusions and rogue or spoofed devices without relying on traffic inspection. This strengthens detection coverage for attacks that manipulate declared identity or operate below the visibility of software agents.

9. Important Boundaries and Non-Claims

- Sepio is not a SWIFT attestation tool and does not certify compliance by itself.
- Sepio does not replace network segmentation, firewall policy, encryption, MFA, password policy, PAM, IAM, transaction reconciliation, database integrity controls, or formal incident response governance.
- Sepio is a hardware trust, visibility, detection, and evidence layer that complements existing security controls and helps close blind spots in hardware identity and physical connectivity.
- Customer architecture type and final control applicability must be determined by the customer based on SWIFT CSCF guidance and the customer's actual environment.

10. High-Level Applicability Summary

Control	Control Title	Sepio Coverage
1.1	SWIFT Environment Protection	Primary
1.2	Operating System Privileged Account Control	Supporting
1.3	Virtualisation or Cloud Platform Protection	Supporting
1.4	Restriction of Internet Access	Supporting
1.5	Customer Environment Protection	Primary
2.1	Internal Data Flow Security	Supporting
2.2	Security Updates	Supporting
2.3	System Hardening	Primary
2.4	Back Office Data Flow Security	Primary
2.5A	External Transmission Data Protection	Limited / indirect

Control	Control Title	Sepio Coverage
2.6	Operator Session Confidentiality and Integrity	Supporting
2.7	Vulnerability Scanning	Supporting
2.8	Outsourced Critical Activity Protection	Supporting
2.9	Transaction Business Controls	Not primary
2.10	Application Hardening	Limited / indirect
2.11A	RMA Business Controls	Not primary
3.1	Physical Security	Primary
4.1	Password Policy	Limited / indirect
4.2	Multi-Factor Authentication	Limited / indirect
5.1	Logical Access Control	Supporting
5.2	Token Management	Supporting

Control	Control Title	Sepio Coverage
5.3A	Staff Screening Process	Not primary
5.4	Password Repository Protection	Supporting
6.1	Malware Protection	Supporting
6.2	Software Integrity	Supporting
6.3	Database Integrity	Not primary
6.4	Logging and Monitoring	Primary
6.5A	Intrusion Detection	Primary
7.1	Cyber Incident Response Planning	Primary
7.2	Security Training and Awareness	Supporting
7.3A	Penetration Testing	Primary
7.4A	Scenario-based Risk Assessment	Primary

11. Source Document Notes

This mapping is based on SWIFT Customer Security Controls Framework v2026, Detailed Description, dated 01 July 2025. Key source areas reviewed include: Executive Summary, Framework Objectives and Principles, Scope of Security Controls, Architecture Types, Security Controls Compliance, Security Controls Summary Table, and Detailed Control Descriptions.

Relevant source pages include pages 4-6 for CSP/CSCF purpose and 2026 changes; pages 8-13 for objectives, principles, and in-scope components; pages 25-29 for control structure, compliance approach, and control summary; and pages 30-97 for detailed control objectives and implementation guidance.

Summary

This guide explains how Sepio can support financial institutions and SWIFT users in strengthening their security posture against the SWIFT CSCF v2026. Sepio is applicable because it extends security and compliance visibility to the hardware layer, helping organizations identify, validate, monitor, and control the physical devices connected to or supporting SWIFT-related environments.

The guide maps Sepio capabilities to relevant CSCF controls and shows where Sepio provides direct or supporting value. Its strongest relevance is in areas such as environment protection, asset visibility, secure-zone monitoring, system hardening support, physical security, vulnerability and exposure management, logging and monitoring, anomaly detection, and incident response.

Sepio does not replace CSCF controls related to identity management, MFA, password policies, staff screening, transaction validation, or application-specific hardening. Instead, it complements those controls by providing a trusted view of the hardware assets that form the foundation of the SWIFT operating environment.

In short, the guide positions Sepio as a practical compliance and security layer that helps SWIFT users answer a critical question: Are the hardware assets supporting our SWIFT environment known, authorized, trusted, properly located, and continuously monitored?.