FORESCOUT

Addressing the SWIFT CSP

Ensure SWIFT Customer Security Controls Framework compliance with CounterACT®

Reduce risk and address compliance in accordance with the SWIFT Customer Security Programme (CSP) without disruption.

Challenges

- Protect and monitor SWIFT infrastructure as mandated by the SWIFT Customer Security Programme (CSP).
- Require tools that provide visibility, control and information sharing across the SWIFT ecosystem.
- Orchestrate appropriate network access, authorization and segmentation controls from campus to datacenter to cloud.

Solution

- ForeScout unifies security management and supports a wide range of SWIFT CSP controls.
- ForeScout enables a broad range of host and network controls, allowing SWIFT customers to ensure control posture from client to server.

Benefits

ForeScout helps organizations address SWIFT CSP compliance by:

- Protecting SWIFT infrastructure as mandated by the Customer Security Controls Framework.
- Automating control and policy enforcement on endpoints and network.

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) launched the Customer Security Programme (CSP) to provide a customer security control framework, improve information sharing throughout the community and enhance SWIFT-related tools. SWIFT customers are responsible for the security of their own environments and must be compliant in accordance with the CSP.

SWIFT reports the status of any non-compliant customers to their regulators. those who haven't attested their level of current compliance will be reported to the relevant financial regulator, and from the end of 2018, those not compliant with the mandatory controls will similarly be reported. The quality assurance process does not preclude customers from independently requesting additional assurance from counterparts, thus ensuring interbank exchange is secure with all parties of the transaction.

SWIFT Customer Security Programme

The SWIFT CSP consists of 3 objectives, 8 principles and 27 controls. ForeScout can be leveraged across all applicable objectives, principles and controls, including both mandatory and advisory.

Secure Your Environment	1. Restrict Internet Access 2. Protect critical systems from general IT environment 3. Reduce attack surface and vulnerabilities 4. Physically secure the environment
Know and Limit Access	5. Prevent compromise of credentials 6. Manage identities and segregate privileges
Detect and Respond	7. Detect anomalous activity to system or transaction records 8. Plan for incident response and information sharing

Improving SWIFT Compliance with ForeScout CounterACT®

ForeScout plays a crucial role in helping ensure your SWIFT CSP compliance in all four SWIFT deployment architectures A1, A2, A3 and B. For example, ForeScout helps SWIFT customers build and maintain secure networks, drive their vulnerability management programmes, implement strong access control measures, monitor and test networks and maintain information security policies.

The financial services industry is increasingly targeted by cybercriminals, as recently confirmed by several reported incidents.

- Financial services probe exposed[1] up to a dozen banks compromised
- Notable recent SWIFT breaches:
  - Bangladesh Bank – $81M
  - Ecuadorian Bank – $12M
  - Taiwanese Bank – $60M

SWIFT created the Customer Security Programme to help ensure their customers meet the required levels of security and compliance, with a framework as part of the programme that covers 16 mandatory controls and 11 additional advisory controls. It is up to each organization to implement the controls in ways best suited to their businesses. Compliance with these requirements significantly reduces the chance of data compromise and fraudulent transactions.

The ForeScout platform delivers a set of unique technologies that work with your devices—managed and unmanaged, known and unknown, server, desktop and mobile, IoT, embedded and virtual. ForeScout helps ensure that servers and endpoints on your network are compliant with your antivirus policy, properly patched and provisioned with the proper policy-sanctioned software. The platform then orchestrates the associated network access, authorization and segmentation controls from campus devices through to datacentre and cloud servers. ForeScout automatically identifies policy violations, remediates security deficiencies and measures adherence to regulatory mandates.

ForeScout physically installs out of band, avoiding latency or issues related to the potential for network failure, and works across heterogeneous environments. It can be centrally administered to dynamically manage more than one million endpoints from a single console. ForeScout provides organizations an efficient way to drive compliance toward the SWIFT CSP.

ForeScout in the SWIFT Customer Security Controls Framework

ForeScout is uniquely positioned to cover all three CSP objectives as well as the majority of principles and controls by primary and secondary means.

Objective	CSP #	Principle	CounterACT
Secure Your Environment	1.x	Restrict internet access	●
		Protect critical systems from general IT environment	●
	2.x	Reduce attack surface and vulnerabilities	●
	3.x	Physically secure the environment	○
Know and Limit Access	4.x	Prevent compromise of credentials	●
	5.x	Manage identities and segregate privileges	●
Detect and Respond	6.x	Detect anomalous activity to system or transaction records	●
	7.x	Plan for incident response and information sharing	●

CSP Controls Addressed by CounterACT

CSP Control 1 – Restrict Internet Access & Protect Critical Systems				
Control #	Title	Architecture	A	B
1.1	SWIFT Environment Protection		●	○
Control Definitions				
Objective:	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.			
ForeScout Solution		PRIMARY		

ForeScout lets you see and control devices on your SWIFT network—regardless of whether or not they have security agents installed.

- Discover unknown devices on the network that are not company-owned (and not outfitted with agent software).
- See ports, protocols and applications specific to your SWIFT environment.
- Perform deep endpoint inspection without an agent.
- Measure effectiveness of security controls and support your efforts to demonstrate compliance with regulations.

ForeScout automatically initiates one or more of your policy-based enforcement and remediation actions, ranging from an email notification of non-compliance to mandatory remediation to outright quarantine or access prevention.

- Segment SWIFT assets leveraging existing infrastructure, with integration to switches, wireless, Next-Generation Firewall (NGFW)s and Software-Defined Networking (SDN)s.
- Control access to confidential data based on device and user profiles.
- Prevent infected or non-compliant devices from spreading malware.
- Automatically enforce actions for identified situations without human involvement.

Control #	Title	Architecture	A	B
1.2	Operating System Privileged Account Control		●	○
Control Definitions				
Objective:	Restrict and control the allocation and usage of administrator-level operating system accounts.			
ForeScout Solution		SECONDARY		

Integration with Privileged Account Management (PAM) systems provides real-time agentless visibility into undiscovered local privileged accounts and automated response to threats based on holistic visibility into user activity, device security posture, incident severity and overall threat exposure.

- ForeScout discovers devices and undetected local privileged accounts in the SWIFT infrastructure.
- The ForeScout Extended Module for PAM shares this information and device context with a PAM system, like CyberArk®.
- The PAM system identifies and alerts CounterACT.
- ForeScout isolates devices on the network and limits SWIFT network access.

CSP Control 2 – Reduce Attack Surface & Vulnerabilities				
Control #	Title	Architecture	A	B
2.2	Security Updates		●	●
Control Definitions				
Objective:	Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and applying timely security updates aligned to the assessed risk.			
ForeScout Solution		SECONDARY		

ForeScout lets you identify missing patches on your endpoints and servers using a combination of native support and module configuration:

- Detect missing patches and software.
- Orchestrate resolution through SCCM, IBM® BigFix® and other means.
- Custom integration through ForeScout Open Integration Module.

Control #	Title	Architecture	A	B
2.3	System Hardening		●	○
Control Definitions				
Objective:	Reduce the cyber attack surface of SWIFT-related components by performing system hardening.			
ForeScout Solution		PRIMARY		
ForeScout supplements VM scanning tools ensuring they have not missed scanning the systems on the network. ForeScout provides the means to harden the SWIFT environment, covering both operating systems and networks: • Windows – registry keys, drive encryption, agent-based solutions. • Linux – Code execution in accordance to CMDB, hardening guidelines. • VMware® – VMware plugin to enact published hardening guidelines. • Networks – default password detection, insecure protocol use; telnet/FTP, etc.				

CSP Control 4 – Prevent Compromise of Credentials				
Control #	**Title**	**Architecture**	**A**	**B**
4.1	Password Policy		●	●
Control Definitions				
Objective:	Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.			
ForeScout Solution		PRIMARY & SECONDARY		
ForeScout integrates with existing directory systems to assist with password policy enforcement and management. For example: • Enforce network-based remediation for devices with users violating password policies. • Pop up a browser message or send an email when password is close to expiration to aid usability. • Integrate with PAM solutions; refer to previous Control #1.2 detail.				

CSP Control 5 – Manage Identities and Segregate Privileges				
Control #	**Title**	**Architecture**	**A**	**B**
5.1	Logical Access Control		●	●
Control Definitions				
Objective:	Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts.			
ForeScout Solution		PRIMARY		
ForeScout gathers rich contextual insights regarding the endpoint, its location, who owns it and what's on it. It can help to ensure: • Unauthorized devices and unsanctioned applications are not on your SWIFT network. • Authorized devices are configured with the latest operating systems, up-to-date antivirus software is installed and running and vulnerabilities are properly patched. • Encryption and data loss prevention agents are working across the SWIFT infrastructure. • Users are prevented from running unauthorized applications or peripheral devices on the network. • Access is granted or denied based on device compliance and user authorization. ForeScout integrates with more than 70 network, security, mobility and IT management products via ForeScout Base and Extended Modules*.				

CSP Control 6 – Reduce Attack Surface & Vulnerabilities				
Control #	Title	Architecture	A	B
6.1	Malware Protection		●	●
Control Definitions				
Objective:	Ensure that local SWIFT infrastructure is protected against malware.			
ForeScout Solution		PRIMARY		

ForeScout Extended Modules provide true security orchestration between CounterACT and various protection systems. The combined solution can automatically detect indicators of compromise (IOCs) on your SWIFT network(s) and quarantine infected devices, thereby limiting malware propagation and breaking the cyber kill chain.

- Ensure malware protection agent is installed, functional, and up-to-date.
- Perform endpoint and/or network-based remediation should an infection be detected.
- Endpoint modules for Symantec®, McAfee®, CrowdStrike®, Bromium®, and Invincea®.
- Network modules for Palo Alto Networks® WildFire™, CheckPoint®, FireEYE® and McAfee®.

CSP Control 6 – Reduce Attack Surface & Vulnerabilities (continued)				
Control #	Title	Architecture	A	B
6.4	Logging and Monitoring		●	●
Control Definitions				
Objective:	Record security events and detect anomalous actions and operations within the local SWIFT environment.			
ForeScout Solution		SECONDARY		

ForeScout Extended Modules for Security Information and Event Management (SIEM) facilitate information sharing and policy management via CounterACT and leading SIEM systems to improve situational awareness and mitigate risks using advanced analytics.

- ForeScout discovers infected endpoints, then sends the information to the SIEM.
- ForeScout receives instructions from the SIEM and automatically takes policy-based mitigation actions to contain and respond to the threat.
- Various actions can be performed depending on the severity or priority of the threat: quarantine endpoints, initiate direct remediation, share real-time context with other incident-response systems, initiate a scan by third-party products, notify end users via email or SMS, etc.

CSP Control 7 – Plan for Incident Response and Information Sharing				
Control #	Title	Architecture	A	B
7.1	Cyber Incident Response Planning		●	●
Control Definitions				
Objective:	Ensure a consistent and effective approach for the management of cyber incidents.			
ForeScout Solution		PRIMARY		

ForeScout plays a key role in incident response through visibility and control of devices on the network and integration with various solutions from Splunk® and ServiceNOW®.

- ForeScout discovers compromised endpoints and can send information to Splunk Enterprise and other solutions for faster incident response times.
- Enables incident response teams to rapidly locate and contain compromised endpoints.
- Automatically contain compromised endpoints at the network level.
- Jointly detect indicators of compromise (IOCs) and share with SIEM systems.
- Bidirectional sharing of data for CMDB systems from ServiceNOW and others.

Learn more at
www.ForeScout.com

FORESCOUT

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591