Solution Brief

Addressing the SWIFT CSP

Ensure SWIFT Customer Security Controls Framework compliance with CounterACT®

Address compliance in accordance with the SWIFT Customer Security Programme (CSP) without disruption, significant cost or risk that can result from breach of SWIFT infrastructure.

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 payment ecosystem.
- Enforce appropriate access for compliant and non-compliant servers and endpoints.

Solution

- ForeScout CounterACT unifies security management and supports a wide range of SWIFT CSP controls.
- CounterACT enables a broad range of host controls and network access, allowing SWIFT customers to restrict access and quarantine.

Benefits

ForeScout helps organizations address SWIFT CSP compliance by:

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

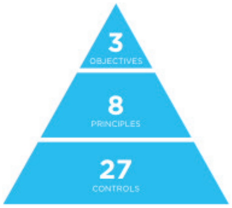
The Society for Worldwide Interbank Financial Telecommunication (SWIFT) launched the Customer Security Programme (CSP) to provide a customer security control framework, improve information sharing throughout the community and enhance SWIFT-related tools. SWIFT customers are responsible for the security 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, and randomly selects customers to provide additional assurance as required either from internal or external auditors. 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.

Customers, in addition, are able to choose to disclose their compliance with a further 11 advisory controls that supplement the 16 mandatory controls.

SWIFT Customer Security Programme

The SWIFT CSP consists of 3 objectives, 8 principles and 27 controls. ForeScout CounterACT can be leveraged across the 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®

CounterACT plays a crucial role in helping ensure SWIFT CSP compliance in all four SWIFT deployment architectures A1, A2, A3 and B. For example, CounterACT 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.

Companies are not completely immune to compromise of SWIFT infrastructure and payment systems, and new threats can target their businesses at any time. The financial services industry is increasingly targeted by cybercriminals, as recently confirmed by several reported SWIFT breaches reported below.

- SWIFT hacking 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 as a result.

The ForeScout CounterACT 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. CounterACT 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. CounterACT automatically identifies policy violations, remediates security deficiencies and measures adherence to regulatory mandates.

CounterACT 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 CounterACT provides organizations an efficient way to drive compliance toward the SWIFT CSP.

ForeScout CounterACT in the SWIFT Customer Security Controls Framework

CounterACT 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

Type: Mandatory

Objective: Ensure the protection of the user’s local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.

Statement: A segregated secure zone safeguards the user’s SWIFT infrastructure from compromises and attacks on the broader enterprise and external environments.

Context: Segmentation between the user’s local SWIFT infrastructure and its larger enterprise network reduces the attack surface and has shown to be an effective way to defend against cyber attacks which commonly involve compromise of the general enterprise IT environment. Effective segmentation will include network-level separation, access restrictions, and connectivity restrictions.

ForeScout Solution PRIMARY

ForeScout CounterACT 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.

CounterACT 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

Type: Mandatory

Objective: Restrict and control the allocation and usage of administrator-level operating system accounts.

Statement: Access to administrator-level operating system accounts is restricted to the maximum extent possible. Usage is controlled, monitored, and only permitted for relevant activities such as software installation and configuration, maintenance, and emergency activities. At all other times, an account with least privilege access is used.

Context: Tightly protecting administrator-level accounts within the operating system reduces the opportunity for an attacker to use the privileges of the account as part of an attack (for example, executing commands, deleting evidence).

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.

- CounterACT 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.
- CounterACT 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

Type:	Mandatory
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.
Statement:	All hardware and software inside the secure zone and on operator PCs are within the support lifecycle of the vendor, have been upgraded with mandatory software updates, and have had security updates promptly applied.
Context:	The closure of known security vulnerabilities is effective in reducing the various pathways that an attacker may use during an attack. A security update process which is effective, repeatable and timely implemented, is necessary to continuously close these known vulnerabilities when security patches are available.

ForeScout Solution SECONDARY

ForeScout CounterACT 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

Type:	Mandatory
Objective:	Reduce the cyber attack surface of SWIFT-related components by performing system hardening.
Statement:	Security hardening is conducted on all in-scope components.
Context:	System hardening applies the security concept of "least privilege" to a system by disabling features and services that are not required for normal system operations. This process reduces the system capabilities, features, and protocols that a malicious person may use during an attack.

ForeScout Solution PRIMARY

ForeScout CounterACT provides means to harden the SWIFT environment, covering 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 2 – Reduce Attack Surface & Vulnerabilities (continued)

Control #	Title	Architecture	A	B
2.7A	Vulnerability Scanning		●	●

Control Definitions

Type:	Advisory
Objective:	Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process.
Statement:	Secure zone and operator PC systems are scanned for vulnerabilities using an up-to-date, reputable scanning tool.
Context:	The detection of known vulnerabilities allows vulnerabilities to be analysed, treated, and mitigated. The mitigation of vulnerabilities reduces the number of pathways that a malicious actor can use during an attack. A vulnerability scanning process which is effective, repeatable and implemented in a timely manner, is necessary to continuously detect known vulnerabilities and to allow for further action.

ForeScout Solution

PRIMARY & SECONDARY

Comprehensive integration with Vulnerability Assessment (VA) systems provide the means to initiate scanning of devices and automate policy-based enforcement actions as needed.

- ForeScout Extended Modules for VA systems such as Qualys®, Rapid7®, and Tenable® deliver sharing of data to trigger real-time scanning.
- CounterACT isolates the device in an inspection VLAN while the VA system performs a scan.
- Scans are triggered on devices that meet certain policy conditions, such as endpoints with SWIFT applications, or when endpoint configuration changes are detected.
- Real-time and continuous scanning ensures both endpoint and network remediation actions can be taken against non-compliant devices operating with SWIFT infrastructure.

CSP Control 4 – Prevent Compromise of Credentials

Control #	Title	Architecture	A	B
4.1	Password Policy		●	●

Control Definitions

Type:	Mandatory
Objective:	Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.
Statement:	All application and operating system accounts enforce passwords with appropriate parameters such as length, complexity, validity, and the number of failed log-in attempts.
Context:	Implementing a password policy that protects against common password attacks (for example, guessing, brute force) is effective for protecting against account compromise. Attackers often use the privileges of a compromised account to move laterally within an environment and progress the attack. Another risk is the compromise of local authentication keys to tamper with the integrity of transactions. It is however important to recognise that passwords alone are generally not sufficient in the current cyber threat landscape. Users should consider this control in close relationship with the multifactor authentication requirement.

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

Type: Mandatory

Objective: Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts.

Statement: Accounts are defined according to the security principles of need-to-know access, least privilege, and segregation of duties.

Context: Applying the security principles of (1) need-to-know, (2) least privilege, and (3) segregation of duties is essential to restricting access to the local SWIFT infrastructure. Effective management of operator accounts reduces the opportunities for a malicious person to use accounts as part of an attack.

ForeScout Solution PRIMARY

ForeScout CounterACT 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.

CounterACT 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

Type: Mandatory

Objective: Ensure that local SWIFT infrastructure is protected against malware.

Statement: Anti-malware software from a reputable vendor is installed and kept up-to-date on all systems.

Context: Malware is a general term that includes many types of intrusive and unwanted software, including viruses. Anti-malware technology (a broader term for anti-virus) is effective in protecting against malicious code that has a known digital or behaviour profile.

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

Type:	Mandatory
Objective:	Record security events and detect anomalous actions and operations within the local SWIFT environment.
Statement:	Capabilities to detect anomalous activity are implemented, and a process or tool is in place to frequently store and review logs.
Context:	Developing a logging and monitoring plan is the basis of effectively detecting abnormal behaviour and potential attacks. As the operational environment becomes more complex, so will the logging and monitoring capability needed to perform adequate detection. Simplifying the operational environment will enable more straightforward logging and monitoring.

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.

- CounterACT discovers infected endpoints, then sends the information to the SIEM.
- CounterACT 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.

Control #	Title	Architecture	A	B
6.5A	Intrusion Detection		●	○

Control Definitions

Type:	Advisory
Objective:	Detect and prevent anomalous network activity into and within the local SWIFT environment.
Statement:	Intrusion detection is implemented to detect unauthorised network access and anomalous activity.
Context:	Intrusion detection systems are most commonly implemented on a network – establishing a baseline for normal operations and sending notifications when abnormal activity on the network is detected. As an operational network becomes more complex (for example, systems communicating to many destinations, Internet access), so will the intrusion detection capability needed to perform adequate detection. Therefore, simplifying network behaviour is a helpful enabler for more straightforward and effective intrusion detection solutions. Intrusion detection systems often combine signature- and anomaly-based detection methods. Some systems have the ability to respond to any detected intrusion (for example, terminating the connection).

ForeScout Solution SECONDARY

ForeScout extends the reach of existing IDS and IPS systems through the ForeScout Extended Modules.

- The IDS/IPS system detects an intrusion and notifies CounterACT.
- CounterAct takes network or endpoint remediation actions, such as quarantining or performing an endpoint antivirus scan.

CSP Control 7 – Plan for Incident Response and Information Sharing

Control #	Title	Architecture A	B
7.1	Cyber Incident Response Planning	●	●

Control Definitions

Type:	Mandatory
Objective:	Ensure a consistent and effective approach for the management of cyber incidents.
Statement:	The organisation has a defined and tested cyber incident response plan.
Context:	Availability and adequate resilience is of key importance in the field of information security. In this respect, defining and testing an incident response plan is a highly effective way of reducing the impact and duration of a real cyber incident. As lessons are learnt either by testing this plan, or through real incidents, it is essential to apply these learnings and improve the plan. Additionally, planning for the sharing of threat and incident information is critical to assisting the broader financial community in implementing effective protections against cyber attacks.

ForeScout Solution PRIMARY

CounterACT 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®.

- CounterACT 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 Technologies, Inc.
190 West Tasman Drive
San Jose, CA 95134 USA

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

* As of June 30, 2017

[1] Bloomberg News, 26 May 2016, 14:36 BST.