Meeting SWIFT's Customer Security Program (CSP)

Mitigating risks of cyberattacks on financial networks and facilitating automatic compliance to established global interbank security controls with Entrust

Overview

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is a Belgian cooperative society providing services related to the execution of financial transactions and payments between banks. As a global financial network processing millions of sensitive transactions, SWIFT has been and continues to be the target of cyberattacks.

SWIFT's Customer Security Program (CSP) was introduced to respond to the growing sophistication of cyberattacks on member banks. The initiative raised the level of cybersecurity hygiene across the banking industry, reducing risks while minimizing the monetary impact of fraudulent transactions.

SWIFT's Customer Security Controls Framework (CSCF) was introduced to help member banks secure local environments and foster a secure financial ecosystem.

The Challenge

Member banks are required to participate in KYC-SA (know your customer security attestation) to carry out an annual program to ensure compliance with mandatory and optional security advisory controls. For banking members with large estates of virtual machines and customer data in these virtual machines KYC-SA can be a challenge to carefully design the security aspects and attack vectors of their environment to harden and make it resilient to attack.

Meeting SWIFT's Security Attestation With Entrust CloudControl

The Solution

Entrust, in partnership with VMware, offers extended control and environmental hardening for achieving a higher level of security and compliance. Developed based on SWIFT's analysis of cyber-threat intelligence, industry expert advice, and user feedback, the control definitions align with existing information security industry standards and best practices. Leveraging comprehensive access controls and monitoring within the SWIFT environment, the solution empowers member banks to provide favorable attestation to the CSP program while protecting the virtual infrastructure and data.

Entrust CloudControl adheres to industry best practices and compliance frameworks such as NIST (National Institute of Standards and Technology) 800-53, CIS Benchmark, Payment Card Industry Data Security Standard (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), and customized requirements. CloudControl also provides frequent and ongoing testing, automated remediation, and reporting of IT systems. These capabilities make it easy to view the overall compliance posture of a bank's environment.

Benefits

Comprehensive security controls help meet compliance requirements across virtualization, public cloud, and containers.

- Provide automation with real-time compliance and security features
- Deliver unified policy, visibility, and administrative guardrails, establishing baseline to constantly monitor deployments
- Support built-in compliance templates for hardening virtual machine and containerized environments
- Secure separation of workloads across environments
- Offer seamless integration and support for VMware Cloud Foundation (VCF)
- Generate granular, user-specific logs in human-readable format for all privileged user activity including root access

Automated Compliance and Assessment Protects Against Threats

Leveraging Entrust automated compliance assessment and remediation, enterprises can be assured that their infrastructure is always in a compliant state and aligned with the SWIFT standards – thereby protecting against internal threats.

Learn more about CloudControl at entrust.com

Meeting SWIFT's Security Attestation With Entrust CloudControl

The Entrust Difference

Entrust solutions provide centralized and consistent security policy management to reduce the risk of cyberattacks on financial networks and meet security controls defined by the SWIFT Customer Security Program.

Entrust offers a range of products that are independently validated and certified. Knowledgeable and responsive technical support, as well as proven integrations with leading technology providers, enable customers to automate attestation to banking regulations to ensure continued compliance.

Features

A list of security controls defined by SWIFT CSP is provided below. The table outlines how Entrust CloudControl addresses the prescribed requirements and facilitates compliance.

SWIFT CSP Reference	SWIFT Security Control	Entrust CloudControl and related product features
1.1 SWIFT Environment Protection	Requires member banks to isolate SWIFT environment from the rest of the business.	Provides granular role, object, and attribute-based access controls with multi-factor authentication.
1.2 Operating System Privileged Account Control	Ensures administrator-level access is limited to required personnel.	Protects and controls hypervisor-level and workload-level access via unified role-based access control (RBAC) policy executed through a SWIFT secure zone group membership and permission-level mapping.
1.3 Virtualization Platform Protection	Secure virtualization platform and virtual machines (VMs) for SWIFT-related components to the same level of physical systems.	Mitigates damage that may result from a breach or escalation of privilege with RBAC and object-based access control (OBAC). Provides strong protection of the virtualization platform and VMs by monitoring and requiring secondary approval of actions that may impact environment.
2.1 Internal Data Flow Security	Ensure the confidentiality, integrity, and authenticity of SWIFT-related data.	Protects SWIFT-related data via Entrust DataControl. DataControl offers strong and granular encryption with a built-in Enterprise Key Manager (KMS) for (operating system) OS boot drive and data partition encryption.
2.2 Security Updates	Minimize occurrence of known technical vulnerabilities within local SWIFT infrastructure.	Mitigates damage that may result from a breach or escalation of privilege with RBAC & OBAC. Limit user access to objects within the virtualization platform by hiding unauthorized objects and making them invisible.

Learn more about CloudControl at entrust.com

Meeting SWIFT's Security Attestation With Entrust CloudControl

SWIFT CSP Reference	SWIFT Security Control	Entrust CloudControl and related product features
2.3 System Hardening	Reduce cyberattack surface on SWIFT-related components by performing system hardening.	Identifies, remediates, and reports on configuration and security management drift increasing visibility and decreasing risk of misconfigurations that can lead to unintended downtime or security exposure. Automates Configuration Hardening to remove human error from accidental or malicious activity.
2.5a External Transmission Data Protection	Protect confidentiality and integrity of interactive operator sessions connecting to local SWIFT infrastructure.	Protects SWIFT-related data via Entrust DataControl. DataControl offers strong and granular encryption with a built-in Enterprise Key Manager (KMS) for (OS) boot drive and data partition encryption.
2.6 Operator Session Confidentiality and Integrity	Protect confidentiality and integrity of interactive operator sessions connecting to local SWIFT infrastructure.	Enforces multi-factor authentication (MFA) to mitigate exploitation of virtual infrastructure and Active Directory to protect against ransomware attacks. Add secondary approval for critical administrative access to the virtualization platform and virtual administration layers.
2.7 Vulnerability Scanning	Identify known vulnerabilities within the local SWIFT environment by implementing regular vulnerability scanning and acting on results.	Scans container registries for known vulnerabilities and enforces an image deployment policy to allow/deny which images can be deployed in the environment.
2.8 Critical Activity Outsourcing	Ensure protection of local SWIFT infrastructure from risks exposed by outsourcing critical activities.	Protects and controls usage of hypervisor-, workload-level, and network (via NSX) access via a unified RBAC policy controlled by a SWIFT secure zone group membership and permission-level mapping. Separates policy from virtualization platform and workloads to ensure principle of least privilege access is maintained.
4.1 Password Policy	Ensure passwords are sufficiently resistant against common password attacks.	Mitigates exploitation of virtual infrastructure and Active Directory by leveraging CloudControl to enforce authentication into virtual environments.
4.2 Multi-factor Authentication	Prevent that a compromise of a single authentication factor allows access into SWIFT-related systems.	Manages and deploys identities for tokens and mobile devices with Entrust PKI (Public Key Infrastructure) and Certificate Hub. Issues keys and certificates backed by PKI by securely storing private keys in an Entrust nShield Hardware Security Module (HSM).
5.1 Logical Access Control	Enforce security principles of need-to-know access, least privilege, and isolation of duties for operator accounts.	Extends VMware's RBAC, increasing granularity to support separation of duties in multi-departmental or multi-tenant SWIFT environments.

Learn more about CloudControl at entrust.com

Meeting SWIFT's Security Attestation With Entrust CloudControl

SWIFT CSP Reference	SWIFT Security Control	Entrust CloudControl and related product features
5.2 Token Management	Ensure proper management, tracking, and use of connected hardware authentication tokens (when tokens are used).	Add Entrust PKI and Certificate Hub to manage and deploy identities for tokens and mobile devices, issuing keys and certificates backed by PKI and securely storing private keys in an Entrust nShield HSM.
6.1 Malware Protection	Ensure local SWIFT infrastructure is protected against malware.	Protects against security threats resulting from malware.
6.4 Logging and Monitoring	Record security events and detect anomalous actions and operations within local SWIFT environment.	Enhances native logging capabilities of the VMware platform to provide granular, system-level logging of all administrative privileged account actions (allowed and denied), and events that have taken place in the virtual infrastructure. Ensures systems supporting virtual platform maintain their integrity in the SWIFT secure zone.
7.1 Cyber Incident Response Planning	Ensure a consistent and effective approach for the management of cyber incidents.	Enforces the use of the CloudControl proxy and MFA to authenticate and control access to the virtualization platform. Applies Trust Manifests (security as code) to enforce policies to the virtual infrastructure and record all (allow/denied) actions.
7.2 Security Training and Awareness	Ensure personnel are knowledgeable and up to date on threats, risks, and vulnerabilities.	Provides training and enablement for SWIFT compliance.

Entrust CloudControl provides SWIFT member banks with a comprehensive solution by providing a unified framework for security and compliance addressing the CSP program requirements – reducing both risk and operational overhead. entrust.com/digital-security/cloud-security-posture-management

CloudControl is part of a suite of data encryption, multi-cloud key management, virtual machine, and containerized workload security policy compliance products. Use Entrust DataControl for fine-grained, agent-based control and encryption key management of virtual machine encryption in multi-cloud environments. Choose Entrust KeyControl for enterprise encryption key management for KMIP (Key Management Interoperability Protocol) enabled workloads. Entrust nShield hardware security modules provide a hardened, tamper-resistant environment for secure cryptographic processing, key generation and protection, encryption, key management, and more.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223