EXECUTIVE BRIEF
MAY 2018

SWIFT Security Controls

How CA Technologies can help you comply

The financial and insurance sector continues to be a primary target for external attackers. The finance sector reported 998 incidents (over half with reported data disclosure) and accounted for 24 percent of the breaches.[1] The sad fact is that exploited privileged accounts are a common thread in many of these data breaches (71 percent), regardless of whether those accounts were compromised by external actors (94 percent) or abused by insiders (6 percent).

Background

Since hackers stole US$81 million from the Bangladesh central bank earlier this year through rogue SWIFT transfers, additional investigations have been launched as more banks look into possible security breaches. As a result, SWIFT has issued a security controls framework that outlines a series of mandatory and advisory security controls for its customers. This framework is based on analysis of cyber threat intelligence, user feedback and consultation with industry experts. The controls are also intended to align with existing security and industry standards. The following section describes each control and how CA security solutions can help address them.

SWIFT Security Control Framework

Mandatory Security Controls

The following security controls are mandatory and must be implemented by SWIFT customers in order to establish a security baseline for the entire SWIFT community.

Control	Control Objective	How CA addresses
1. Restrict Internet Access and Protect Critical Systems From General IT Environment		
1.1 SWIFT Environment Protection	Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment.	Privileged access management solutions from CA provide comprehensive protection for a bank's mission-critical servers with powerful, fine-grained controls over operating system-level access and privileged user actions.
1.2 Operating System Privileged Account Control	Restrict and control the allocation and usage of administrator-level operating system accounts.	Privileged access management solutions from CA are capable of enforcing access controls on powerful native Superuser accounts like the UNIX® and Linux® root and Microsoft® Windows® administrator. This system-level, host-based privileged access management solution controls, monitors and audits privileged user activity, improving security and simplifying audit and compliance.

Control	Control Objective	How CA addresses
2. Reduce Attack Surface and Vulnerabilities		
2.1 Internal Data Flow Security	Ensure the confidentiality, integrity and authenticity of data flows between local SWIFT-related applications and their link to the operator PC.	Application-to-application communications are generally not within the scope of the CA solutions; however, the CA API Gateway can secure Web services communications between applications. CA Privileged Access Manager also supports application-to-application security by allowing applications to call out to retrieve a password necessary to perform activities (versus hard-coding this password within the application or a script).
2.2 Security Updates	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.	The CA solutions are routinely patched to address any known or discovered security vulnerabilities, and are updated to support the latest infrastructure versions (e.g., OS, database, etc.).
2.3 System Hardening	Reduce the cyber-attack surface of SWIFT-related components by performing system hardening.	CA Privileged Access Manager Server Control can help with system hardening by providing in-depth protection of critical servers to enforce host-based, fine-grained access controls to resources, segregated duties of superusers, management of system resources and secure task delegation (sudo).
3. Physically Secure the Environment		
3.1 Physical Security	Prevent unauthorized physical access to sensitive equipment, workplace environments, hosting sites and storage.	Although CA does not provide a physical access control system (PACS), we can manage physical access via our identity management solution, CA Identity Suite, which can provision and de-provision users to a PACS and allow for periodic reviews or certifications of the physical access that has been granted to users.
4. Prevent Compromise of Credentials		
4.1 Password Policy	Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy.	CA provides a variety of solutions that can enforce password policies; however, the primary solution is to leverage CA Privileged Access Manager to vault passwords that are used to access privileged or shared accounts. Users and applications request these passwords through a checkout process. In addition, CA Privileged Access Manager can also automatically change these passwords.
4.2 Multi-factor Authentication	Prevent a compromise of a single authentication factor from allowing access into SWIFT systems by implementing multi-factor authentication.	CA Advanced Authentication provides a variety of software-based, two-factor credentials to make logins more secure. It also allows organizations to silently and transparently collect data and assess risk based on device identification, geolocation and user behavior, among other factors. Combining risk assessment and multi-factor credentials enables an intelligent, layered security approach to prevent inappropriate access and online identity fraud without impacting the user experience.

Control	Control Objective	How CA addresses
5. Prevent Compromise of Credentials		
5.1 Logical Access Control	Enforce the security principles of need-to-know access, least privilege and segregation of duties for operator accounts.	CA provides a variety of solutions that can help enforce logical access controls. CA Identity Suite can help establish least-privileged access and enforce segregation-of-duties rules across all apps and accounts. CA Privileged Access Manager can enforce access controls and segregation of duties across privileged accounts. And CA Single Sign-On can enforce access controls across all online applications.
5.2 Token Management	Ensure the proper management, tracking and use of connected hardware authentication tokens (if tokens are used).	Although CA does not provide hardware tokens, we can track and monitor their usage through our two primary access management products, which would authenticate the user based on the hardware token for Web access (CA Single Sign-On) and privileged accounts (CA Privileged Access Manager).
6. Detect Anomalous Activity to Systems or Transaction Records		
6.1 Malware Protection	Ensure that local SWIFT infrastructure is protected against malware.	Although CA does not provide typical malware solutions, CA Privileged Access Manager Server Control can prevent software, such as malware being loaded onto a machine via a privileged account.
6.2 Software Integrity	Ensure the software integrity of the SWIFT-related applications.	The CA Veracode platform can scan all of the applications and components you build or buy, covering all major languages, frameworks and application types. It gives you a central repository for your applications and components, so you have full visibility into your risk posture.
6.3 Database Integrity	Ensure the integrity of the database records for the SWIFT messaging interface.	CA Privileged Access Manager can audit and record all activities performed in a database by a privileged user.
6.4 Logging and Monitoring	Record security events and detect anomalous actions and operations within the local SWIFT environment.	The misuse or takeover of privileged accounts constitutes the most common source of breaches today. CA Threat Analytics for PAM provides a continuous, intelligent monitoring capability that helps enterprises detect and stop hackers and malicious insiders before they cause damage. The software integrates a powerful set of user behavior analytics and machine learning algorithms with the trusted controls provided by CA Privileged Access Manager. The result is a solution that continuously analyzes the activity of individual users, accurately detects malicious and high-risk activities and automatically triggers mitigating controls to limit damage to the enterprise.

Control	Control Objective	How CA addresses
7. Plan for Incident Response and Information Sharing		
7.1 Cyber Incident Response Planning	Ensure a consistent and effective approach for the management of cyber incidents.	CA Threat Analytics for PAM enables organizations to deploy user behavior analytics that detect and stop both external hackers and insider threats. The solution's advanced algorithms continuously assess the behavior of privileged users and compare their actions to historical observations and the behavior of other users. In this way, the solution accurately identifies attacks and high-risk activities, such as users observed surveying an environment in search of high-value assets or those who try to exfiltrate data off sensitive servers. In addition, unlike solutions that simply require alerts, CA Threat Analytics for PAM mitigates detected risks by automatically triggering controls to stop attacks and limit damage. For example, the system can generate additional authentication or automatically record suspicious user sessions.
7.2 Security Training and Awareness	Ensure all staff are aware of and fulfil their security responsibilities by performing regular security training and awareness activities.	Security training would be handled outside of our products; however, we have had customers leverage the session recording for training purposes. New admins can watch recordings of how to perform specific tasks, or watch recordings of how specific mistakes were made so they can learn not to repeat them in the future.

Advisory Security Controls

The following security controls are based on best practices, and SWIFT recommends that these be implemented by all customers. In addition, SWIFT also notes that as new threats emerge, some of these may become mandatory in the future.

Control	Control Objective	How CA addresses
2. Reduce Attack Surface and Vulnerabilities		
2.4 Back Office Data Flow Security	Ensure the confidentiality, integrity and mutual authenticity of data flows between back office (or middleware) applications and connecting SWIFT infrastructure components.	Application-to-application communications are generally not within the scope of the CA solutions; however, the CA API Gateway can secure Web services communications between applications. CA Privileged Access Manager also supports application-to-application security by allowing applications to call out to retrieve a password necessary to perform activities (versus hard-coding this password within the application or a script).

Control	Control Objective	How CA addresses
2.5 External Transmission Data Protection	Protect the confidentiality of SWIFT-related data transmitted and residing outside of the secure zone.	CA Privileged Access Manager protects privileged identities in physical, virtual and cloud environments. In addition, CA Privileged Access Manager Server Control can monitor inbound and outbound TCP/IP connections to ensure that malicious programs cannot connect to rogue servers outside the network.
2.6 Operator Session Confidentiality	Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure.	CA Single Sign-On provides enhanced session assurance, which prevents unauthorized users from hijacking legitimate sessions by stealing session cookies using a patent-pending device fingerprinting approach. CA Threat Analytics for PAM can also monitor privileged user sessions for anomalous behavior (please see response to 7.1 above for additional details).
2.7 Vulnerability Scanning	Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process.	The CA Veracode platform can scan all the applications and components you build or buy, covering all major languages, frameworks and application types. It gives you a central repository for your applications and components so you have full visibility into your risk posture.
2.8 A Critical Activity Outsourcing	Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.	CA Privileged Access Manager protects against third-party risk by enhancing security for the privileged identities/accounts these outsourced users may be accessing. By protecting sensitive administrative credentials such as root and administrator passwords, controlling privileged user access, proactively enforcing policies and monitoring and recording privileged user activity across all IT resources, CA Privileged Access Manager can significantly reduce third-party risk.

Control	Control Objective	How CA addresses
5. Prevent Compromise of Credentials		
5.3 A Personnel Vetting	Ensure the trustworthiness of staff operating the local SWIFT environment by performing personnel vetting.	This would occur outside our software solutions.
5.4 A Physical and Logical Password Storage	Protect physically and logically recorded passwords.	CA Privileged Access Manager protects and manages credentials used to access privileged accounts. These credentials are stored within a secure vault and are only checked out to a user or application after they have authenticated to the solution.

Summary

To guard against costly data breaches, smart financial institutions are protecting and automating access to privileged accounts across both physical and virtual systems. Whether your company's data is on premises, in the cloud or within a hybrid infrastructure, it's critical to protect, monitor and audit privileged access everywhere. Employing a zero-trust model with a defense-in-depth approach to security that includes privileged access management offers your organization the best chance of protection against ever-evolving threats.

To learn more about Privileged Access Management from CA, please visit **ca.com/pam**

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate—across mobile, private and public cloud, distributed and mainframe environments. Learn more at **ca.com**.

1 Verizon, "**2017 Data Breach Investigations Report**," April 2017

Connect with CA Technologies

CS200-360302_0518