BeyondTrust

# Privileged Access Management & SWIFT Customer Security Controls Framework

How a complete PAM program can assist organizations to achieve compliance with the SWIFT Customer Security Controls Framework

TECH BRIEF

## Table of Contents

## Introduction

This guide has been prepared so that IT and security administrators in financial services organizations can quickly understand how the BeyondTrust Privileged Access Management platform addresses the requirements found in the SWIFT Customer Security Controls Framework 1.0, as published on 31 March 2017.

## What is the SWIFT Customer Security Controls Framework?

SWIFT's Customer Security Controls Framework describes a set of mandatory and advisory security controls for SWIFT users grouped into three overall objectives – Secure Your Environment, Know and Limit Access, and Detect and Respond – supported by eight security principles and 27 security controls. For a representation of the framework's objectives and principles, please reference Figure 1 below.

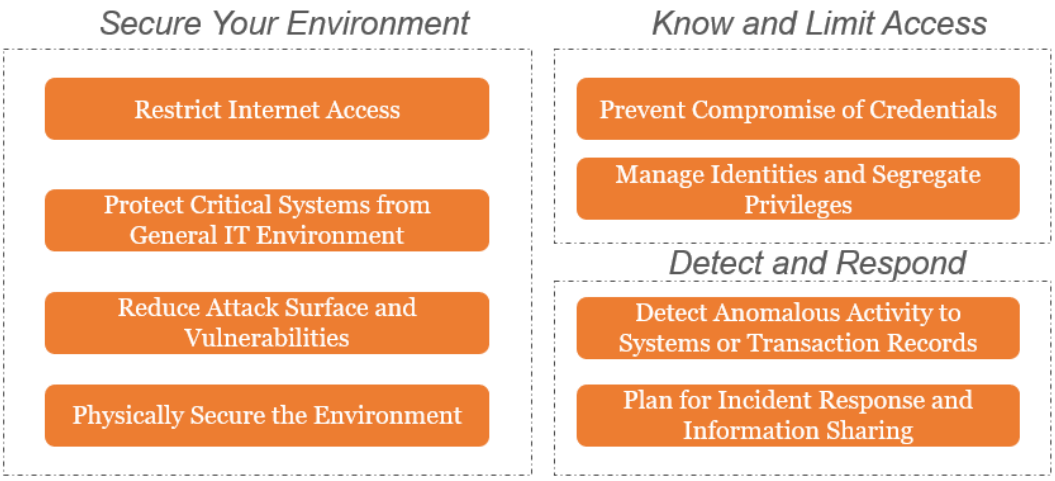



Figure 1: Framework Objectives and Principles
SWIFT Customer Security Controls Framework 1.0
31 March 2017

According to the framework:

*"Mandatory security controls … must be implemented by all users on their local SWIFT infrastructure… Advisory controls are based on good practice that SWIFT recommends users to implement."*

SWIFT requires that users self-attest compliance against the mandatory security controls (it is optional for the advisory controls), with a deadline of January 1, 2018 to submit their self-attestations. This paper includes guidance on both the mandatory security controls and the advisory controls that SWIFT recommends, and how BeyondTrust solutions map into each of them. BeyondTrust solutions therefore address parts of each section using privileged access management (PAM) and vulnerability management (VM) to implement measurable technical controls and manage the requirements. For a summary of these mappings, please see the table in the following section.

## How BeyondTrust Solutions Help with SWIFT Requirements

This section contains summary and detailed tables that demonstrate how BeyondTrust solutions map to SWIFT Security Control requirements.

### TABLE 1: SUMMARY MAPPING OF BEYONDTRUST SOLUTIONS TO SWIFT SECURITY CONTROL FRAMEWORK

*NOTE: Controls marked with an "A" or italicized are advisory controls.*

| Mandatory and Advisory Security Controls | Applicable BeyondTrust Products | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | BeyondTrust Platform | Password Safe | Privilege Management for Windows & MacOS | Privilege Management for Unix & Linux | BeyondTrust AD Bridge | BeyondTrust Auditor | Enterprise Vulnerability Management | Secure Remote Access |
| **1. Restrict Internet Access and Protect Critical Systems from General IT Environment** | | | | | | | | |
| 1.1 SWIFT Environment Protection | | ✓ | | ✓ | | | | ✓ |
| 1.2 Operating System Privileged Account Control | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |
| **2. Reduce Attack Surface and Vulnerabilities** | | | | | | | | |
| 2.1 Internal Data Flow Security | ✓ | ✓ | | ✓ | | | | |
| 2.2 Security Updates | ✓ | | ✓ | | | | ✓ | |
| 2.3 System Hardening | ✓ | | ✓ | ✓ | | | ✓ | |
| *2.4A Back-office Data Flow Security* | | | | | | | | |
| *2.5A External Transmission Data Protection* | | | | | | | | |
| *2.6A Operator Session Confidentiality and Integrity* | ✓ | ✓ | ✓ | ✓ | | | | ✓ |
| *2.7A Vulnerability Scanning* | ✓ | | | | | | ✓ | |
| *2.8A Critical Activity Outsourcing* | ✓ | ✓ | | | | | | ✓ |
| *2.9A Transaction Business Controls* | | | | | | | | |
| **3. Physically Secure the Environment** | | | | | | | | |
| 3.1 Physical Security | | | | | | | | |
| **4. Prevent Compromise of Credentials** | | | | | | | | |
| 4.1 Password Policy | | ✓ | | | | | ✓ | ✓ |
| 4.2 Multi-factor Authentication | ✓ | ✓ | ✓ | | | | | ✓ |
| **5. Manage Identities and Segregate Privileges** | | | | | | | | |
| 5.1 Logical Access Control | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ |
| 5.2 Token Management | | | | | | | | |
| *5.3A Personnel Vetting Process* | | | | | | | | |
| *5.4A Physical and Logical Password Storage* | ✓ | ✓ | | | | | ✓ | ✓ |

| Mandatory and Advisory Security Controls | Applicable BeyondTrust Products | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | BeyondTrust Platform | Password Safe | Privilege Management for Windows & MacOS | Privilege Management for Unix & Linux | BeyondTrust AD Bridge | BeyondTrust Auditor | Enterprise Vulnerability Management | Secure Remote Access |
| **6. Detect Anomalous Activity to Systems or Transaction Records** | | | | | | | | |
| 6.1 Malware Protection | ✓ | | ✓ | | | | ✓ | |
| 6.2 Software Integrity | ✓ | | ✓ | ✓ | | | | |
| 6.3 Database Integrity | | | | | | | | |
| 6.4 Logging and Monitoring | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ |
| *6.5A Intrusion Detection* | ✓ | | | | | | | |
| **7. Plan for Incident Response and Information Sharing** | | | | | | | | |
| 7.1 Cyber Incident Response Planning | ✓ | | | | | | | |
| 7.2 Security Training and Awareness | | | | | | | | |
| *7.3A Penetration Testing* | ✓ | | | | | | ✓ | |
| *7.4A Scenario Risk Assessment* | | | | | | | | |

## TABLE 2: DETAILED MAPPING OF BEYONDTRUST SOLUTIONS TO SWIFT SECURITY CONTROLS

This table provides greater detail on how each BeyondTrust product maps into the SWIFT framework.

| Mandatory and Advisory Security Controls | BeyondTrust Product Details |
|---|---|
| **1. Restrict Internet Access and Protect Critical Systems from General IT Environment** | |
| **1.1 SWIFT Environment Protection**<br><br>**Control Objective:** Ensure the protection of the user's local SWIFT infrastructure from potentially compromised elements of the general IT environment and external environment. | • Password Safe contains proxy technology for secure RDP and SSH access into a secure zone, and the capabilities to replay and alert on privileged session activity into the zone.<br><br>• Privilege Management for Unix & Linux enables separation of the management workstation and the managed server to provide secure access into a zone and can limit activity to specific users and applications that reside remote resources.<br><br>• Secure Remote Access provides a secure session into an environment shielding assets from potentially compromised infrastructure |

| Mandatory and Advisory Security Controls | BeyondTrust Product Details |
|---|---|
| **1.2 Operating System Privileged Account Control**<br><br>**Control Objective:** Restrict and control the allocation and usage of administrator-level operating system accounts. | • The BeyondTrust Platform is designed to manage privileges and control access to administrator level operating accounts with complete reporting, auditing, and session playback of user activity.<br><br>• Password Safe manages privileged passwords and session activity associated with administrator-level access to resources.<br><br>• Privilege Management for Windows Desktops & Privilege Management for Mac Desktops deliver privilege management for servers and endpoints eliminating the need to provide administrator level credentials to users performing administrator-level tasks.<br><br>• Privilege Management for Unix & Linux removes the need for root access through a reliable, granular and flexible least privilege solution.<br><br>• BeyondTrust AD Bridge brings Active Directory (AD) authentication and Group Policy to Unix & Linux systems (including Mac OS X). A single account for access to Windows, Unix and Linux simplifies user management.<br><br>• BeyondTrust Auditor is designed to monitor all changes in Active Directory, Group Policy, File Systems, Exchange, and MS SQL to report on potential privilege abuse.<br><br>• Secure Remote Access can control access to systems and restrict usage of administrator-level operating system accounts via native capabilities and credential injection when integrated with a password safe technology. |
| **2. Reduce Attack Surface and Vulnerabilities** | |
| **2.1 Internal Data Flow Security**<br><br>**Control Objective**: Ensure the confidentiality, integrity, and authenticity of data flows between local SWIFT-related applications and their link to the operator PC. | • The BeyondTrust Platform is designed to provide secure access between applications, operators, and the resulting reports, event management, configuration, and session playback recordings.<br><br>• Password Safe implements a secure connection between operators and applications using proxy technology for SSH and RDP directly in the platform.<br><br>• Privilege Management for Unix & Linux implements a secure connection between operators and applications using a jump host to provide confidentiality and integrity of sessions executed by users on a host. |
| **2.2 Security Updates**<br><br>**Control Objective:** Minimize the occurrence of known technical vulnerabilities within the local SWIFT infrastructure by ensuring vendor support, applying mandatory software updates, and | • The BeyondTrust Platform centralizes information regarding missing security updates and vulnerabilities from all BeyondTrust solutions, including network scanning, agent technologies, and third-party connectors and third-party vulnerability data imports.<br><br>• Privilege Management for Windows contains patented real-time vulnerability assessment technology that can report on missing security |

| Mandatory and Advisory Security Controls | BeyondTrust Product Details |
|---|---|
| applying timely security updates aligned to the assessed risk. | updates through the BeyondTrust platform as users execute applications and operating system tasks.<br><br>• Enterprise Vulnerability Management can identify vulnerabilities and missing security updates across any network connected device using network scanning and agent-based assessment technologies. |
| **2.3 System Hardening**<br><br>**Control Objective**: Reduce the cyber-attack surface of SWIFT-related components by performing system hardening. | • The BeyondTrust Platform provides the aggregation and reporting of system hardening assessments performed by the Enterprise vulnerability management solution family. This identifies configuration anomalies that could be leveraged in a cyber-attack.<br><br>• Privilege Management for Windows Desktops and Privilege Management for Mac Desktops provide system hardening by removing administrative rights, implementing application control, and enforce privilege management to prevent unauthorized hardening changes.<br><br>• Privilege Management for Unix & Linux supplement system hardening by restricting the ability of users to make unauthorized changes that could affect system hardening.<br><br>• Enterprise Vulnerability Management performs system hardening assessments against resources using industry standards from NIST, Microsoft, CIS, DISA, and many others. |
| ***2.4A Back-office Data Flow Security***<br><br>***Control Objective:*** *Ensure the confidentiality, integrity, and mutual authenticity of data flows (…).* | Not Applicable |
| ***2.5A External Transmission Data Protection***<br><br>***Control Objective:*** *Protect the confidentiality of SWIFT-related data (…).* | Not Applicable |
| ***2.6A Operator Session Confidentiality and Integrity***<br><br>***Control Objective:*** *Protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure.* | • The BeyondTrust Platform is designed to protect the confidentiality and integrity between applications, operators and the resulting reports, event management, configuration, and session playback recordings of all operator sessions.<br><br>• Password Safe implements a secure connection between operators and applications using proxy technology for SSH and RDP directly in the platform using secure protocols and storage procedures.<br><br>• Privilege Management for Windows Desktops and Privilege Management for Mac Desktops are privilege management solutions that manage |

| Mandatory and Advisory Security Controls | BeyondTrust Product Details |
|---|---|
| | administrative access to applications and operating system tasks and help ensure that applications running with elevated privileges have high integrity.<br><br>• Privilege Management for Unix & Linux provides a confidential and secure session to resources with high integrity for appropriate access to applications, scripts, and tasks executed during normal operations.<br><br>• Secure Remote Access can protect the confidentiality and integrity of interactive operator sessions connecting to the local SWIFT infrastructure using session monitoring, dedicated jump points, and removing access to traditional remote access protocols like RDP, SSH, and HTTPS via jump clients. |
| ***2.7A Vulnerability Scanning***<br><br>***Control Objective:*** *Identify known vulnerabilities within the local SWIFT environment by implementing a regular vulnerability scanning process.* | • The BeyondTrust Platform aggregates vulnerability assessment information for reporting and patch management from Enterprise's agent based and network scanning solutions. It is also capable of ingesting third party vulnerability data from other solutions to provide a central console regardless of source.<br><br>• Enterprise Vulnerability Management can detect and report on vulnerabilities across the entire enterprise using network scanning and agent-based vulnerability assessment technologies. |
| ***2.8A Critical Activity Outsourcing***<br><br>***Control Objective:*** *Ensure protection of the local SWIFT infrastructure from risks exposed by the outsourcing of critical activities.* | • The BeyondTrust Platform can report of resource changes from ports, services, shares, software, and users that may indicate inappropriate access and exposed risks when resources are shared with external parties.<br><br>• Password Safe can manage contractor and outsourced access to secure zones via context aware policy, segmentation, and reporting on all activity.<br><br>• Secure Remote Access can secure remote vendor or contractor access into an infrastructure and mitigate the risks associated with connectivity when outsourcing critical activity. |
| ***2.9A Transaction Business Controls***<br><br>***Control Objective:*** *Restrict transaction activity (…).* | Not Applicable |

| | |
|---|---|
| **3. Physically Secure the Environment** | |
| **3.1 Physical Security**<br><br>**Control Objective:** Prevent unauthorized physical access (…). | Not Applicable |
| **4. Prevent Compromise of Credentials** | |
| **4.1 Password Policy**<br><br>**Control Objective:** Ensure passwords are sufficiently resistant against common password attacks by implementing and enforcing an effective password policy. | • Password Safe can enforce password complexity through assignments of random passwords at user defined frequency based on policy and usage.<br><br>• Enterprise Vulnerability Management can assess the local password policies assigned to resources, including complexity for Windows and non-Windows assets (based on SCAP hardening assessments).<br><br>• Secure Remote Access can perform credential injection from a password safe enforcing an external password policy. |
| **4.2 Multi-factor Authentication**<br><br>**Control Objective**: Prevent that a compromise of a single authentication factor allows access into SWIFT systems, by implementing multi-factor authentication. | • The BeyondTrust Platform supports multifactor authentication for managing policies, reviewing events and sessions, and generating reports for all privileged access and vulnerability management solutions.<br><br>• Password Safe supports multi-factor authentication for password and session access.<br><br>• Privilege Management for Windows Desktops supports multi-factor authentication for privileged application access.<br><br>• Secure Remote Access supports multi-factor authentication to mitigate the risks of single factor authentication for any remote session activity. |
| **5. Manage Identities and Segregate Privileges** | |
| **5.1 Logical Access Control**<br><br>**Control Objective:** Enforce the security principles of need-to-know access, least privilege, and segregation of duties for operator accounts. | • The BeyondTrust Platform provides complete management capabilities for all of BeyondTrust's privileged management and least privileged solutions.<br><br>• Password Safe enforces logical access to resources based on policies, context aware parameters, and provides separation of duties by restricting privileged password and session access.<br><br>• Privilege Management for Windows Desktops and Privilege Management for Mac Desktops provide least privilege access to applications and operating system tasks on servers and endpoints.<br><br>• Privilege Management for Unix & Linux provides least privilege access and separation of duties based on policies and segregating user access to applications and resources.<br><br>• BeyondTrust AD Bridge allows for segregation of privileged access to Unix and Linux resources based on assignments in Active Directory Groups. |

| | |
|---|---|
| | • BeyondTrust Auditor monitors changes to Active Directory to ensure assignments and revocation of account access is performed appropriately and in a timely manner.<br><br>• Secure Remote Access supports connectivity with the concepts like least privilege and segregation of duties with features like multi user screen sharing to enforce roles and responsibilities associated with multiple operator accounts. |
| **5.2 Token Management**<br><br>**Control Objective:** Ensure the proper management, tracking (…). | Not Applicable |
| ***5.3A Personnel Vetting Process***<br><br>***Control Objective:*** *Ensure the trustworthiness of staff (…).* | Not Applicable |
| ***5.4A Physical and Logical Password Storage***<br><br>***Control Objective:*** *Protect physically and logically recorded passwords.* | • The BeyondTrust Platform provides capabilities for password storage, rotation, and application to application API's for secure password storage.<br><br>• Password Safe is designed to securely store passwords, automatically manage them, and provide complete attestation reporting for their usage and session activity.<br><br>• Enterprise Vulnerability Management can assess targets for poor password storage hygiene as a part of its vulnerability assessment capabilities.<br><br>• Secure Remote Access can protect physical and logical recorded passwords with integration into password safe technologies and native password Vault capabilities. |
| **6. Detect Anomalous Activity to Systems or Transaction Records** | |
| **6.1 Malware Protection**<br><br>**Control Objective**: Ensure that local SWIFT infrastructure is protected against malware. | • The BeyondTrust Platform contains an analytics engine called BeyondInsight Clarity that compares the file, process, and service hash results from various BeyondTrust solutions for potential malware.<br><br>• Privilege Management for Windows Desktops and Privilege Management for Mac Desktops collect hash information from applications that are executed and sends the results to the BeyondTrust Platform for malware analysis.<br><br>• Enterprise Vulnerability Management sends the hash information from processes and services gathered during credentialed scans to the BeyondTrust platform for malware analysis. |

| | |
|---|---|
| **6.2 Software Integrity**<br><br>**Control Objective**: Ensure the software integrity of the SWIFT-related applications. | • The BeyondTrust Platform aggregates all privileged activity occurring on hosts to alert and report on all privilege changes that could affect the software integrity of applications in scope.<br><br>• Privilege Management for Windows Desktops and Privilege Management for Mac Desktops manage privileges required to make changes on a resource and ensure that the software integrity of applications cannot be compromised due to lax privileges or inappropriate file changes.<br><br>• Privilege Management for Unix & Linux manages privileges required to make changes on a resource and ensure that the software integrity of applications cannot be compromised due to inappropriate privileges or inappropriate file changes. |
| **6.3 Database Integrity**<br><br>**Control Objective:** Ensure the integrity of the database records (…). | Not Applicable |
| **6.4 Logging and Monitoring**<br><br>**Control Objective:** Record security events and detect anomalous actions and operations within the local SWIFT environment. | • The BeyondTrust Platform provides logging and monitoring for all privileged access, session recordings, and assessed vulnerabilities.<br><br>• Password Safe provides logging and monitoring for all privileged password access and privileged sessions.<br><br>• Privilege Management for Windows Desktops and Privilege Management for Mac Desktops provide logging and monitoring for all privileged application and operating system access on end points and servers.<br><br>• Privilege Management for Unix & Linux provides logging and monitoring for all privileged application, script, and command access on managed resources.<br><br>• BeyondTrust Auditor provides logging and monitoring of all changes to Active Directory, File Systems, Exchange, and Microsoft SQL within Windows environments.<br><br>• Enterprise Vulnerability Management can assess whether operating system and application logs are configured correctly for the collection of information to meet these requirements. This can be done using native audits and security hardening assessments depending on the platform.<br><br>• Secure Remote Access monitors and logs all remote session activity for anomalous behaviour and can send monitored and logged activity to a security event information manager for additional correlation. |

| | |
|---|---|
| ***6.5A Intrusion Detection***<br>***Control Objective:*** *Detect and prevent anomalous network activity into and within the local SWIFT environment.* | The BeyondTrust Platform can forward all privilege and vulnerability management results to third party solutions to provide advanced correlation and detection of intrusion events. This information includes events from BeyondInsight Clarity – a cluster mapping-based analytics engine – that can identify abnormal user behavior and outlier risks associated with intrusion detection. |
| **7. Plan for Incident Response and Information Sharing** | |
| **7.1 Cyber Incident Response Planning**<br>**Control Objective:** Ensure a consistent and effective approach for the management of cyber incidents. | The BeyondTrust Platform provides a single pane of glass for the collection of privileged activity and vulnerability assessments needed for forensics in a cyber incident response plan. |
| **7.2 Security Training and Awareness**<br>**Control Objective:** Ensure all staff are aware (…). | Not Applicable |
| ***7.3A Penetration Testing***<br>***Control Objective:*** *Validate the operational security configuration and identify security gaps by performing penetration testing.* | • The BeyondTrust Platform aggregates vulnerability assessment results used in penetration testing reconnaissance and integrates with leading commercial penetration testing tools to automate actions.<br>• Enterprise Vulnerability Management performs reconnaissance for penetration testing initiatives and integrates with leading penetration testing tools to automate potential exploitation. |
| ***7.4A Scenario Risk Assessment***<br>***Control Objective:*** *Evaluate the risk and readiness (…).* | Not Applicable |

## Conclusion

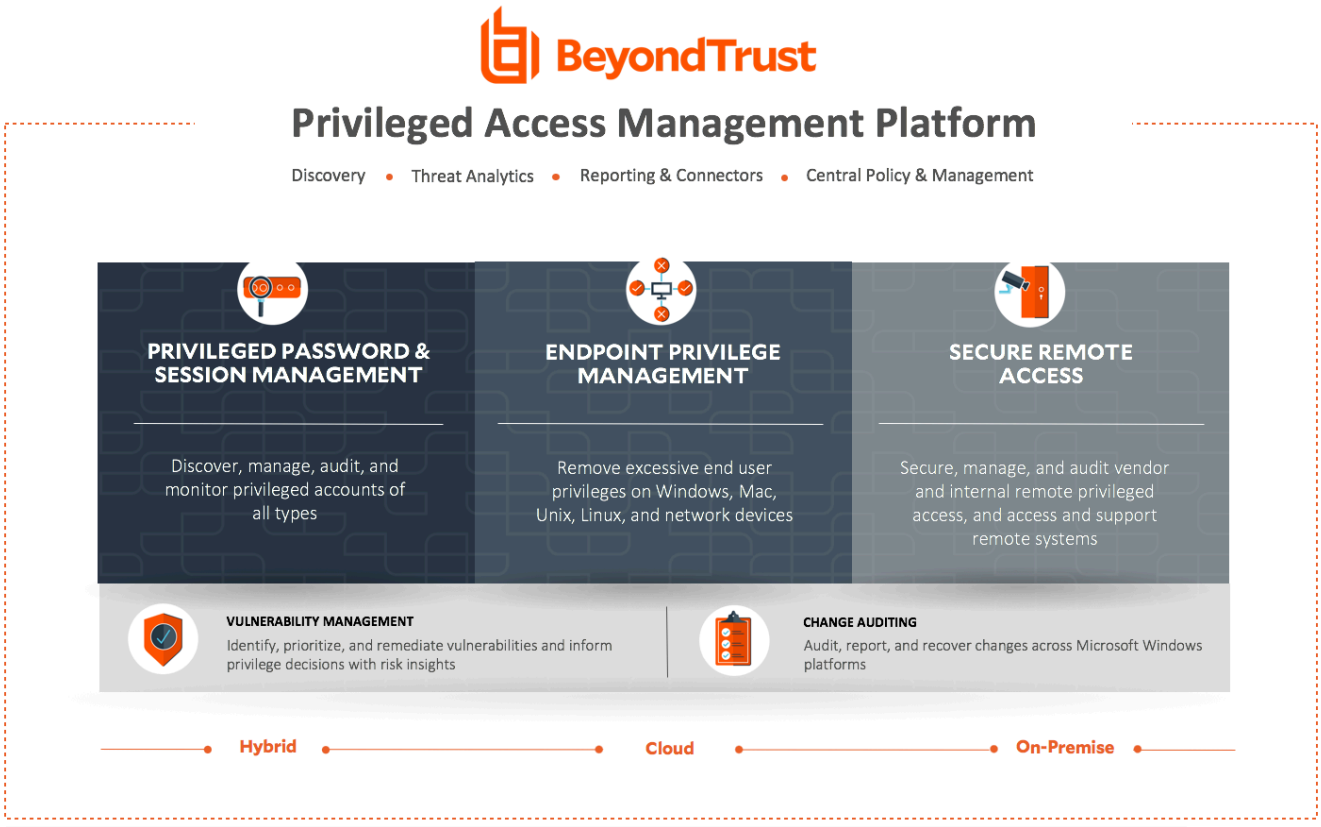
By partnering with BeyondTrust, organizations can address their compliance and security requirements as defined in the SWIFT Customer Security Controls Framework, leaving fewer gaps, better controlling access to customer data, and improving efficiency over their privileged access management and vulnerability management practices.

In addition, if your organization currently adheres to the NIST Cybersecurity Framework, ISO 27002, or PCI DSS, please reference Appendix E in the SWIFT framework guide. This will enable you to expedite the documenting and enforcing of compliance due to overlaps with those regulations. BeyondTrust can provide whitepapers covering these requirements as well to properly cross reference initiatives within your organization and with BeyondTrust solutions.

## Appendix: Privileged Access Management Platform & Solutions

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing data breaches related to stolen credentials, misused privileges, and compromised remote access.

Our extensible platform empowers organisations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. BeyondTrust unifies the industry's broadest set of privileged access capabilities with centralised management, reporting, and analytics, enabling leaders to take decisive and informed actions to defeat attackers. Our holistic platform stands out for its flexible design that simplifies integrations, enhances user productivity, and maximizes IT and security investments.



| | |
|---|---|
| Password Safe | BeyondTrust Password Safe unifies privileged password and privileged session management, providing secure, automated discovery, management, auditing, and monitoring for any privileged credential—including for privileged and administrator accounts, applications, SSH keys, social media accounts, and more). Password Safe enables organizations to achieve complete control and accountability over privileged accounts. |
| Endpoint Privilege Management | BeyondTrust Endpoint Privilege Management enforces least privilege and eliminates admin rights across Windows, Unix, Linux, Mac, network, IoT, ICS, and SCADA devices. Organisations can remove admin rights from desktop users, and also tightly manage privileged access on servers (including eliminating root access), while empowering both IT and non-IT workers to securely do their jobs. The solution monitors and logs all privileged sessions in real-time, providing a thorough compliance trail. Endpoint Privilege Management can also centralise authentication for Unix, Linux, Mac, and Windows by extending AD's Kerberos authentication and single sign-on capabilities across platforms. |
| Vulnerability Management | BeyondTrust Enterprise Vulnerability Management enables IT and security teams to proactively identify security exposures, analyse business impact, and plan and conduct remediation across network, web, cloud, container, and virtual infrastructures—delivering risk analysis in context. The solution also enables organizations to make smarter privileged access decisions—such as denying privileged access or privilege elevation—based on real-time vulnerability information. |
| Secure Remote Access | BeyondTrust Secure Remote Access (compromised of Privileged Remote Access and Remote Support solutions) enables organizations to secure, manage, and audit vendor and helpdesk activity, and all remote privileged access without a VPN. In addition, with Privileged Remote Access, organizations can extend access to important assets, without compromising security. By reducing the number of VPN connections, you reduce the potential footholds cyber-attackers can exploit to access your network. |
| Platform Capabilities | The BeyondTrust Privileged Access Management Platform is an integrated, extensible solution that provides visibility and control over all privileged accounts and users. By uniting the broadest set of privileged security capabilities, the platform simplifies deployments, reduces costs, improves usability, and reduces privilege risks. Common components centralised for all products in BeyondInsight include asset and account discovery, threat analytics, reporting and connectors to third-party systems, and central management and policy. |

For more information, visit beyondtrust.com/solutions.