BeyondTrust

Gestion des accès privilégiés & SWIFT Customer Security Controls Framework

Comment une stratégie PAM efficace peut aider les entreprises à se mettre en conformité avec le SWIFT Customer Security Controls Framework

TECH BRIEF

Sommaire

Introduction

Ce guide s'adresse aux administrateurs IT et aux équipes sécurité des sociétés de services financiers. Il a pour but de les aider à comprendre comment la plateforme BeyondTrust Privileged Access Management permet de répondre aux préconisations du SWIFT Customer Security Controls Framework 1.0 daté du 31 mars 2017.

Qu'est-ce que le SWIFT Customer Security Controls Framework ?

Le SWIFT Customer Security Controls Framework établit la liste des contrôles de sécurité obligatoires et recommandés aux utilisateurs SWIFT. Il vise 3 objectifs principaux : sécuriser votre environnement, connaitre et limiter les accès, détecter et réagir. Ces objectifs sont soutenus par 8 principes de sécurité et 27 contrôles de sécurité. Le schéma 1 (ci-dessous) représente les objectifs et principes de ce cadre réglementaire.

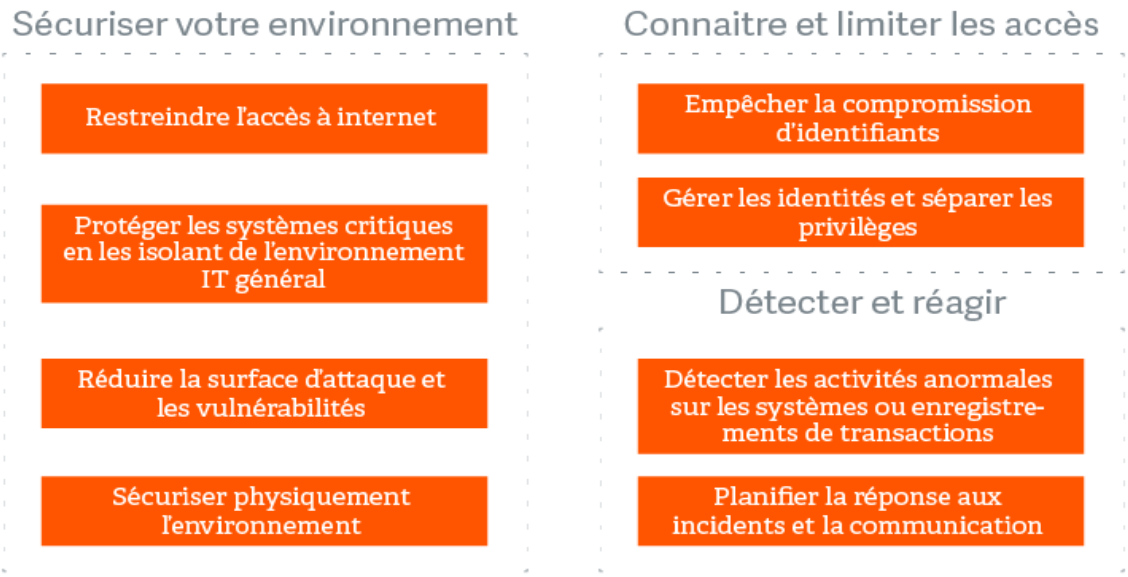


Schéma 1 : Objectifs et principes du SWIFT Customer Security Controls Framework 1.0, 31/03/2017

Aussi, selon le cadre : *« Les contrôles de sécurité obligatoires [...] doivent être mis en œuvre par tous les utilisateurs sur leur infrastructure SWIFT locale [...]. Les contrôles recommandés s'appuient sur les bonnes pratiques que SWIFT préconise aux utilisateurs. »*

SWIFT exigeait que les utilisateurs attestent eux-mêmes de leur conformité aux contrôles de sécurité obligatoires (optionnels pour les contrôles recommandés), le délai de soumission de ces auto-attestations ayant étant fixé au 1er janvier 2018. Vous trouverez ici des conseils concernant les contrôles de sécurité obligatoires et recommandés de SWIFT et vous découvrirez quelles réponses peuvent apporter les solutions BeyondTrust. Celles-ci adressent différents aspects de chaque principe en

termes de gestion des accès privilégiés (PAM : Privileged Access Management) et de gestion des vulnérabilités pour mettre en œuvre des contrôles techniques mesurables et se conformer aux préconisations. Le résumé de ces correspondances principes / solutions figure dans le tableau ci-dessous.

Comment les solutions BeyondTrust aident à respecter les préconisations SWIFT

Cette section comporte deux tableaux : l'un offre une vision synthétique des correspondances entre les solutions BeyondTrust et les préconisations SWIFT Customer Security Control Framework et le second détaille la façon dont les solutions adressent ces points spécifiques.

TABLEAU 1 : RESUME DES REPONSES BEYONDTRUST AU SWIFT CUSTOMER SECURITY CONTROLS FRAMEWORK

Remarque : les contrôles notés A ou en italique sont des contrôles recommandés mais non obligatoires.

Contrôles de sécurité obligatoires / recommandés	**Solutions BeyondTrust**							
	Plateforme BeyondTrust	Password Safe	Privilege Management for Windows & MacOS	Privilege Management for Unix & Linux	BeyondTrust AD Bridge	BeyondTrust Auditor	Enterprise Vulnerability Management	Secure Remote Access
1. Restreindre l'accès à internet et protéger les systèmes critiques en les isolant de l'environnement IT général								
1.1 Protection de l'environnement SWIFT		✓		✓				✓
1.2 Contrôle des comptes privilégiés sur les systèmes d'exploitation	✓	✓	✓	✓	✓	✓		✓
2. Réduire la surface d'attaque et les vulnérabilités								
2.1 Sécurité des flux de données internes	✓	✓		✓				
2.2 Mises à jour de sécurité	✓		✓				✓	
2.3 Renforcement du système	✓		✓	✓			✓	
2.4A Sécurité des flux de données de back-office								
2.5A Protection des données transmises à l'extérieur								
2.6A Confidentialité et intégrité des sessions des opérateurs	✓	✓	✓	✓				✓
2.7A Analyse des vulnérabilités	✓						✓	
2.8A Externalisation d'activités critiques	✓	✓						✓
2.9A Contrôles des transactions commerciales								

Contrôles de sécurité obligatoires / recommandés	Solutions BeyondTrust							
	Plateforme BeyondTrust	Password Safe	Privilege Management for Windows & MacOS	Privilege Management for Unix & Linux	BeyondTrust AD Bridge	BeyondTrust Auditor	Enterprise Vulnerability Management	Secure Remote Access
3. Sécuriser physiquement l'environnement								
3.1 Sécurité physique								
4. Empêcher la compromission d'identifiants								
4.1 Politique de gestion des mots de passe		✓					✓	✓
4.2 Authentification multifactorielle	✓	✓	✓					✓
5. Gérer les identités et séparer les privilèges								
5.1 Contrôle d'accès	✓	✓	✓	✓	✓	✓		✓
5.2 Gestion des tokens								
5.3A Processus de vérification du personnel								
5.4A Stockage des mots de passe réseaux et locaux	✓	✓					✓	✓

Contrôles de sécurité obligatoires / recommandés	Solutions BeyondTrust							
	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. Détecter les activités anormales sur les systèmes ou enregistrements de transactions								
6.1 Protection contre les malwares	✓		✓				✓	
6.2 Intégrité logicielle	✓		✓	✓				
6.3 Intégrité de la base de données								
6.4 Enregistrement et contrôle	✓	✓	✓	✓		✓	✓	✓
6.5A Détection d'intrusion	✓							
7. Planifier la réponse aux incidents et la communication								
7.1 Planification des réponses aux cyber-incidents	✓							
7.2 Formation et sensibilisation à la sécurité								
7.3A Test de pénétration	✓						✓	
7.4A Evaluation des scénarios à risque								

TABLEAU 2 : DETAIL DES REPONSES BEYONDTRUST AU SWIFT CUSTOMER SECURITY CONTROLS FRAMEWORK

Le tableau ci-dessous détaille la façon dont les solutions BeyondTrust aident à respecter le cadre SWIFT.

Contrôles de sécurité obligatoires / recommandés	Solutions BeyondTrust
1. Restreindre l'accès à internet et protéger les systèmes critiques en les isolant de l'environnement IT général	
1.1 Protection de l'environnement SWIFT **Objectif du contrôle :** Assurer la protection de l'infrastructure SWIFT locale de l'utilisateur vis-à-vis d'éléments potentiellement compromis sur le reste de l'environnement IT et l'environnement externe.	• Password Safe intègre une technologie proxy pour l'accès sécurisé RDP et SSH à une zone de sécurité, ainsi que la possibilité de rejouer l'activité des sessions privilégiées dans la zone et de déclencher des alertes. • Privilege Management for Unix & Linux permet d'isoler la console d'administration et le serveur géré pour permettre un accès sécurisé à une zone et permet de limiter l'activité à certains utilisateurs et applications résidant sur des ressources distantes. • Secure Remote Access permet d'ouvrir une session sécurisée au sein d'un environnement, et isole les actifs de l'infrastructure possiblement compromise
1.2 Contrôle des comptes privilégiés sur les systèmes d'exploitation **Objectif du contrôle :** Restreindre et contrôler l'attribution et l'utilisation des comptes de système d'exploitation de type administrateur.	• La plateforme BeyondTrust permet de gérer les privilèges et de contrôler l'accès aux comptes d'exploitation admin en offrant des fonctions complètes de reporting, d'audit et de visionnage des sessions et activités des utilisateurs. • Password Safe gère les mots de passe privilégiés et l'activité des sessions associées aux accès admin aux ressources. • Privilege Management for Windows Desktops & Privilege Management for Mac Desktops assurent la gestion des privilèges pour les serveurs et les endpoints, ce qui permet de supprimer les identifiants admin des utilisateurs. • Privilege Management for Unix & Linux élimine la nécessité d'un accès root via une solution fiable, granulaire et flexible fondée sur le principe du moindre privilège. • BeyondTrust AD Bridge permet d'appliquer l'authentification Active Directory (AD) et les fonctionnalités Group Policy aux systèmes Unix & Linux (y compris Mac OS X). L'utilisation d'un seul compte pour accéder à Windows, Unix et Linux simplifie la gestion utilisateur. • BeyondTrust Auditor contrôle tous les changements dans Active Directory, Group Policy, les systèmes de fichiers, Exchange et MS SQL et rend compte d'éventuels usages abusifs de privilèges.

Contrôles de sécurité obligatoires / recommandés	Solutions BeyondTrust
	• Secure Remote Access contrôle l'accès aux systèmes et restreint l'usage des comptes de système d'exploitation de type admin via des fonctionnalités natives et l'injection d'identifiants quand on l'intègre avec une solution de gestion des mots de passe.
2. Réduire la surface d'attaque et les vulnérabilités	
2.1 Sécurité des flux de données internes **Objectif du contrôle** : Assurer la confidentialité, l'intégrité et l'authenticité des flux de données entre les applications locales liées à SWIFT et le poste de l'opérateur.	• La plateforme BeyondTrust sécurise les accès entre les applications, les utilisateurs, les rapports, la gestion des événements, la configuration et les enregistrements de session. • Password Safe établit une connexion sécurisée entre les opérateurs et les applications via une technologie proxy pour SSH et RDP intégrée à la plateforme. • Privilege Management for Unix & Linux établit une connexion sécurisée entre les opérateurs et les applications via un hôte jump assurant ainsi la confidentialité et l'intégrité des sessions exécutées sur l'hôte par des utilisateurs.
2.2 Mises à jour de sécurité **Objectif du contrôle :** Limiter les vulnérabilités techniques connues au sein de l'infrastructure SWIFT locale en garantissant l'installation des mises à jour logicielles obligatoires et l'application rapide des mises à jour de sécurité selon le niveau de risque estimé.	• La plateforme BeyondTrust centralise les informations identifiées sur l'ensemble des solutions BeyondTrust concernant les mises à jour de sécurité manquantes et les vulnérabilités détectées, y compris l'analyse réseau, les agents installés, les connecteurs tiers et l'import des données de vulnérabilités tierces. • Privilege Management for Windows intègre une technologie brevetée d'évaluation de vulnérabilités en temps réel qui rend compte des mises à jour de sécurité manquantes via la plateforme BeyondTrust lorsque les utilisateurs exécutent des applications et des tâches du système d'exploitation. • Enterprise Vulnerability Management permet d'identifier les vulnérabilités et les mises à jour de sécurité manquantes de tout dispositif connecté au réseau grâce à des agents installés ou scan de réseau.
2.3 Renforcement du système **Objectif du contrôle** : Réduire la surface de cyberattaque des composants SWIFT en procédant au renforcement des systèmes.	• La plateforme BeyondTrust centralise et génère des rapports portant sur les opérations de renforcement système réalisées par ses solutions de gestion des vulnérabilités. Elle révèle ainsi les anomalies de configuration pouvant être utilisées pour une cyber-attaque. • Privilege Management for Windows Desktops et Privilege Management for Mac Desktops assurent le renforcement du système en supprimant les droits admin, en instaurant le contrôle des applications et en appliquant la gestion des privilèges pour éviter tout changement non autorisé qui pourrait affecter la robustesse du système.

Contrôles de sécurité obligatoires / recommandés	Solutions BeyondTrust
	• Privilege Management for Unix & Linux contribue à renforcer davantage le système en limitant la capacité des utilisateurs à apporter des changements non autorisés pouvant affecter la robustesse du système. • Enterprise Vulnerability Management évalue le renforcement système de ressources sur la base des standards NIST, Microsoft, CIS, DISA et bien d'autres.
2.4A Sécurité des flux de données de back-office ***Objectif du contrôle :*** *Assurer la confidentialité, l'intégrité et l'authenticité réciproque des flux de données [...].*	Non applicable
2.5A Protection des données transmises à l'extérieur ***Objectif du contrôle :*** *Maintenir la confidentialité des données liées au SWIFT [...].*	Non applicable
2.6A Confidentialité et intégrité des sessions des opérateurs ***Objectif du contrôle :*** *Protéger la confidentialité et l'intégrité des sessions des opérateurs se connectant à l'infrastructure SWIFT locale.*	• La plateforme BeyondTrust protège la confidentialité et l'intégrité entre les applications, les utilisateurs, les rapports, la gestion des événements, la configuration et les enregistrements de session de tous les opérateurs. • Password Safe établit une connexion sécurisée entre les opérateurs et les applications via une technologie proxy pour SSH et RDP intégrée à la plateforme, via des protocoles et des procédures de stockage sécurisés. • Privilege Management for Windows Desktops et Privilege Management for Mac Desktops sont des solutions de gestion des privilèges qui gèrent l'accès admin aux applications et tâches du système d'exploitation et garantissent une intégrité optimale des applications tournant avec des privilèges élevés. • Privilege Management for Unix & Linux établit une session confidentielle et sécurisée d'accès aux ressources avec un niveau de sécurité supérieur pour l'accès aux applications, scripts et tâches exécutés au cours d'opérations habituelles. • Secure Remote Access peut protéger la confidentialité et l'intégrité des sessions des techniciens se connectant à l'infrastructure SWIFT locale via la surveillance de session, des points jump dédiés et la suppression de l'accès aux protocoles traditionnels d'accès à distance comme RDP, SSH et HTTPS via des clients jump.

Contrôles de sécurité obligatoires / recommandés	Solutions BeyondTrust
2.7A Analyse des vulnérabilités ***Objectif du contrôle :*** *Identifier les vulnérabilités connues dans l'environnement SWIFT local en mettant en place un processus régulier d'analyse des vulnérabilités.*	• La plateforme BeyondTrust regroupe les informations de vulnérabilités remontées par des agents installés ou via un scan réseau à des fins de reporting et de gestion des patchs. Elle peut aussi ingérer les données de vulnérabilités de solutions tierces afin de centraliser toutes ces informations dans une seule et même console. • Enterprise Vulnerability Management peut détecter les vulnérabilités sur l'ensemble de l'infrastructure et générer des rapports grâce à des agents installés ou via un scan réseau.
2.8A Externalisation d'activités critiques ***Objectif du contrôle :*** *Protéger l'infrastructure SWIFT locale des risques liés à l'externalisation d'activités critiques.*	• La plateforme BeyondTrust peut indiquer des changements de ressources de ports, services, partitions, logiciels et utilisateurs pouvant signaler un accès inapproprié et l'exposition à des risques quand les ressources sont partagées avec des parties extérieures. • Password Safe peut gérer l'accès des tiers et sous-traitants à des zones sécurisées via des règles contextuelles et la segmentation, et générer des rapports complets de toutes les activités réalisées. • Secure Remote Access peut sécuriser l'accès de fournisseurs ou sous-traitants à distance à une infrastructure et ainsi limiter les risques lorsqu'ils se connectent et / ou accèdent à des ressources sensibles.
2.9A Contrôle des transactions commerciales ***Objectif du contrôle :*** *Contrôler et restreindre les risques lors de transactions commerciales […].*	Non applicable

3. Sécuriser physiquement l'environnement	
3.1 Sécurité physique **Objectif du contrôle :** Empêcher l'accès physique non autorisé aux installations […].	Non applicable
4. Empêcher la compromission d'identifiants	
4.1 Politique de gestion des mots de passe **Objectif du contrôle :** S'assurer que les mots de passe sont suffisamment forts pour résister aux attaques en instaurant et en faisant appliquer des politiques efficaces de gestion des mots de passe.	• Password Safe renforce la complexité des mots de passe en attribuant des mots de passe aléatoires à une fréquence définie selon les règles en place, l'usage etc. • Enterprise Vulnerability Management évalue les politiques locales de mots de passe attribués aux ressources, y compris leur complexité pour les actifs Windows et non-Windows (d'après les évaluations de renforcement SCAP).

	• Secure Remote Access peut injecter des identifiants depuis une solution de gestion des mots de passe et permettre d'appliquer une règle de mot de passe externe.
4.2 Authentification multifactorielle **Objectif du contrôle** : Eviter qu'un facteur d'authentification unique compromis donne accès aux systèmes SWIFT, en mettant en œuvre l'authentification multifactorielle.	• La plateforme BeyondTrust supporte l'authentification multifactorielle pour la gestion des règles, le visionnage d'événements et de sessions, et la production de rapports pour l'ensemble des solutions de gestion des vulnérabilités et des accès privilégiés. • Password Safe intègre l'authentification multifactorielle pour l'accès par mot de passe et aux sessions. • Privilege Management for Windows Desktops intègre l'authentification multifactorielle pour l'accès aux applications à privilèges. • Secure Remote Access intègre l'authentification multifactorielle pour atténuer les risques inhérents à l'authentification à facteur unique dans le cadre de sessions de prise en main à distance.
5. Gérer les identités et séparer les privilèges	
5.1 Contrôle d'accès **Objectif du contrôle :** Instaurer les principes de sécurité tels que la granularité des accès, le moindre privilège et la séparation des tâches.	• La plateforme BeyondTrust et ses solutions propose des fonctionnalités complètes de gestion des droits et du moindre privilège. • Password Safe permet l'accès aux ressources sur la base de règles et de paramètres contextuels et assure la séparation des tâches en restreignant l'accès aux sessions et mots de passe privilégiés. • Privilege Management for Windows Desktops et Privilege Management for Mac Desktops permettent l'accès selon le principe du moindre privilège aux applications et tâches du système d'exploitation sur les serveurs et endpoints. • Privilege Management for Unix & Linux permet l'accès selon le principe du moindre privilège et la séparation des tâches sur la base de règles et via la ségrégation entre les accès utilisateur et les applications et ressources. • BeyondTrust AD Bridge permet la ségrégation de l'accès privilégié aux ressources Unix et Linux d'après les attributions définies dans les groupes Active Directory. • BeyondTrust Auditor contrôle les changements apportés à Active Directory pour vérifier que les attributions et les révocations d'accès aux comptes se font dans les règles et dans les délais. • Secure Remote Access conjugue connectivité, moindre privilège et séparation des tâches avec des fonctionnalités telles que le partage d'écran multi-utilisateurs pour renforcer les rôles et les responsabilités associés à plusieurs comptes de techniciens.
5.2 Gestion des tokens	Non applicable

Objectif du contrôle : Assurer la bonne gestion et le suivi des tokens [...].	
5.3A Processus de vérification du personnel ***Objectif du contrôle :*** *Vérifier la fiabilité du personnel [...].*	Non applicable
5.4A Stockage des mots de passe réseaux et locaux ***Objectif du contrôle :*** *Protéger les mots de passe présents sur le réseau et en local.*	• La plateforme BeyondTrust propose des fonctionnalités de stockage et de rotation des mots de passe, et des API inter-applications pour le stockage sécurisé des mots de passe. • Password Safe assure le stockage sécurisé des mots de passe, les gère automatiquement et produit des rapports d'attestation d'usage et de l'activité des sessions. • Enterprise Vulnerability Management peut définir des cibles pour l'évaluation des bonnes pratiques de stockage de mots de passe dans le cadre de ses fonctionnalités d'évaluation des vulnérabilités. • Secure Remote Access peut protéger les mots de passe réseaux et locaux grâce à l'intégration avec des solutions de coffre-fort et des fonctionnalités vault natives.
6. Détecter les anomalies dans les enregistrements système ou des transactions	
6.1 Protection contre les malwares **Objectif du contrôle** : S'assurer que l'infrastructure SWIFT locale est protégée contre les malwares.	• La plateforme BeyondTrust Platform contient un moteur analytique appelé BeyondInsight Clarity qui compare les résultats hash de fichiers, processus et services de différentes solutions BeyondTrust à la recherche de malwares. • Privilege Management for Windows Desktops et Privilege Management for Mac Desktops collectent les informations hash d'applications en cours d'exécution et envoient les résultats à la plateforme BeyondTrust en vue d'une recherche de malwares. • Enterprise Vulnerability Management envoie les informations hash de processus et services collectées lors d'analyses d'identifiants à la plateforme BeyondTrust en vue d'une recherche de malwares.
6.2 Intégrité logicielle **Objectif du contrôle** : S'assurer de l'intégrité logicielle des applications SWIFT.	• La plateforme BeyondTrust compile toute l'activité privilégiée se produisant sur les hôtes pour alerter et rendre compte de tous les changements de privilèges pouvant affecter l'intégrité logicielle des applications visées. • Privilege Management for Windows Desktops et Privilege Management for Mac Desktops gèrent les privilèges nécessaires pour apporter des changements à une ressource et veillent à ce que l'intégrité logicielle des applications ne puisse être compromise du fait de privilèges trop souples ou de changements de fichiers inappropriés. • Privilege Management for Unix & Linux gère les privilèges nécessaires pour apporter des changements à une ressource et veillent à ce que

	l'intégrité logicielle des applications ne puisse être compromise du fait de privilèges ou de changements de fichiers inappropriés.
6.3 Intégrité de la base de données **Objectif du contrôle :** S'assurer de l'intégrité des enregistrements sur la base de données [...].	Non applicable
6.4 Enregistrement et contrôle **Objectif du contrôle :** Enregistrer les événements de sécurité et détecter les actions et opérations anormales au sein de l'environnement SWIFT local.	• La plateforme BeyondTrust permet de lister et de contrôler tous les accès à privilèges, d'enregistrer les sessions et d'identifier les vulnérabilités. • Password Safe permet de lister et de contrôler tous les accès et sessions à privilèges. • Privilege Management for Windows Desktops et Privilege Management for Mac Desktops permettent l'enregistrement et le contrôle de tous les accès privilégiés aux applications et tâches du système d'exploitation sur les serveurs et endpoints. • Privilege Management for Unix & Linux permet l'enregistrement et le contrôle de tous les accès privilégiés aux applications, scripts et commandes sur les ressources gérées. • BeyondTrust Auditor permet l'enregistrement et le contrôle de tous les changements apportés à Active Directory, aux systèmes de fichiers, à Exchange et Microsoft SQL au sein des environnements Windows. • Enterprise Vulnerability Management évalue si les fichiers journaux des applications et systèmes d'exploitation sont correctement configurés pour la collecte d'information conforme. Ceci peut se faire via des audits natifs et des évaluations du renforcement de la sécurité selon la plateforme. • Secure Remote Access permet l'enregistrement et le contrôle de l'activité de toutes les sessions distantes à la recherche de comportements anormaux et peut envoyer l'activité ainsi consignée et surveillée à un gestionnaire d'information sur les événements de sécurité pour affiner la corrélation.
6.5A Détection d'intrusion **Objectif du contrôle :** Détecter et éviter toute activité anomale sur le réseau et l'environnement SWIFT local.	La plateforme BeyondTrust peut communiquer les informations relatives à la gestion des privilèges et des vulnérabilités à des solutions tierces pour affiner la corrélation et mieux détecter les intrusions. C'est le cas des événements en provenance de BeyondInsight Clarity, un moteur analytique de mise en correspondance de clusters, capable d'identifier les comportements utilisateur anormaux et les risques liés à la détection d'intrusion.

7. Planifier la réponse aux incidents et la communication	
7.1 Planification des réponses aux cyber-incidents **Objectif du contrôle :** Garantir une approche cohérente et efficace pour la gestion des cyber incidents.	La plateforme BeyondTrust centralise les informations liées aux activités à privilèges et aux évaluations de vulnérabilités dans le cadre d'investigations légales prévues dans le plan de réponse aux cyber incidents.
7.2 Formation et sensibilisation à la sécurité **Objectif du contrôle :** Veiller à ce que tous les membres du personnel soient sensibilisés [...].	Non applicable
7.3A Test de pénétration **Objectif du contrôle :** Valider que les configurations de sécurité soient opérationnelles et identifier les failles de sécurité en réalisant des tests de pénétration.	• La plateforme BeyondTrust compile les résultats des évaluations de vulnérabilité réalisées lors de tests de pénétration et les intègre à des solutions de tests de pénétration permettant d'automatiser ces opérations. • Enterprise Vulnerability Management effectue une reconnaissance en amont de tests de pénétration et intègre les résultats à des solutions de test de pénétration pour automatiser leur exploitation.
7.4A Evaluation des scénarios à risque **Objectif du contrôle :** Evaluer le niveau de risque et de préparation [...].	Non applicable

Conclusion

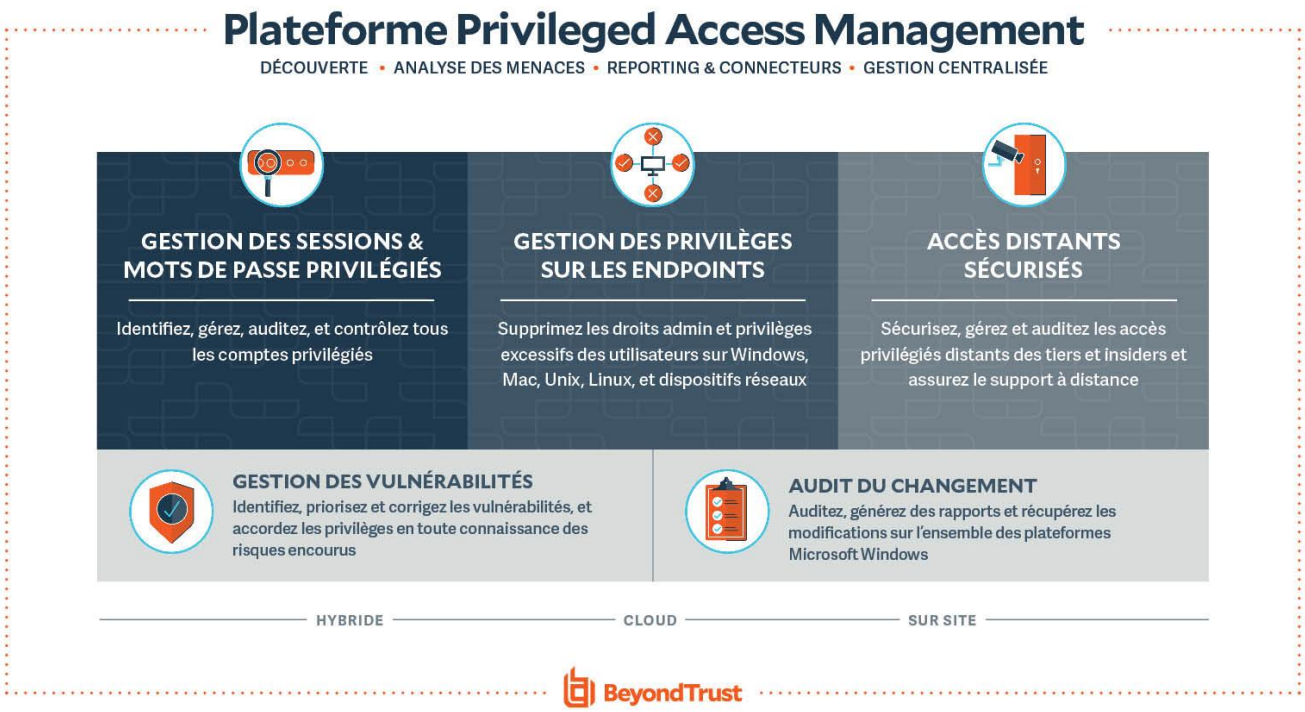
En choisissant BeyondTrust, les entreprises peuvent adresser les obligations de conformité et de sécurité prévues par le SWIFT Customer Security Controls Framework. Cela leur permet de combler davantage de failles, en contrôlant mieux l'accès aux données clients et en renforçant l'efficacité de leurs pratiques de gestion des accès privilégiés et des vulnérabilités.

Si votre entreprise est soumise au NIST Cybersecurity Framework, ISO 27002 ou PCI DSS, référez-vous à l'Annexe E du guide du cadre SWIFT. Vous éviterez ainsi les doublons liés aux efforts de documentation et de mise en conformité du fait de chevauchements entre réglementations. BeyondTrust peut vous fournir des livres blancs à ce sujet et vous aider à identifier les correspondances entre les initiatives mises en place et les solutions BeyondTrust.

Annexe : Plateforme et solutions de gestion des accès privilégiés

BeyondTrust est le leader mondial du Privileged Access Management (gestion des accès privilégiés). Nous proposons une approche intégrée permettant de réduire les menaces liées aux vols d'identifiants, aux compromissions de privilèges et aux accès distants indésirables.

Notre plateforme modulaire et flexible permet aux organisations de sécuriser les privilèges sur les *endpoints*, serveurs, réseaux et environnements cloud, DevOps etc. de façon évolutive pour faire face aux menaces en constante mutation et évolution. BeyondTrust offre ainsi les fonctionnalités les plus compètes du marché, une gestion centralisée et des capacités de reporting et d'analytics uniques. Cela permet aux décisionnaires de prendre les mesures nécessaires et d'agir sur la base d'informations solides pour écarter les cybercriminels toujours plus efficacement. Notre plateforme se distingue par sa flexibilité, laquelle facilite les intégrations, augmente la productivité des utilisateurs et optimise les investissements IT et sécurité réalisés.



Password Safe

BeyondTrust Password Safe unifie la gestion des mots de passe et des sessions privilégiés, permettant la découverte, la gestion, l'audit et le contrôle de tous les identifiants privilégiés, y compris pour les comptes privilégiés et admin, les applications, les clés SSH, les comptes de réseaux sociaux etc. Password Safe permet un contrôle complet des comptes privilégiés et des activités réalisées par utilisateur.

Endpoint Privilege Management

BeyondTrust Endpoint Privilege Management permet d'appliquer le principe du moindre privilège et de supprimer les droits admin sur les postes Windows, Unix, Linux, Mac, sur les appareils IoT, les systèmes en réseau ICS et SCADA, les dispositifs réseaux etc. Les entreprises peuvent supprimer les droits admin des utilisateurs de PC et mieux gérer l'accès privilégié sur les serveurs (en éliminant l'accès root), tout en permettant aux salariés, IT et non-IT, de faire leur travail en toute sécurité. La solution assure l'enregistrement et le contrôle de toutes les sessions privilégiées en temps réel, garantissant une mise en conformité et une préparation aux audits optimales. Endpoint Privilege Management peut aussi centraliser l'authentification auprès des systèmes Unix, Linux, Mac et Windows en étendant l'authentification Kerberos AD et l'authentification unique SSO aux plateformes.

Vulnerability Management	Vulnerability Management permet d'identifier de manière proactive les risques et vulnérabilités, d'analyser l'impact sur les opérations et d'effectuer des actions correctives sur les infrastructures réseau, Web, cloud, en fournissant une analyse des risques en contexte. La solution permet également de prendre de meilleures décisions concernant les accès privilégiés, comme de refuser un accès privilégié ou une élévation de privilège, sur la base d'informations de vulnérabilités en temps réel.
Secure Remote Access	BeyondTrust Secure Remote Access (conjuguant les solutions Privileged Remote Access et Remote Support) permet de sécuriser, gérer et auditer l'activité des fournisseurs et du support technique, ainsi que l'ensemble des accès à distance privilégiés, sans VPN. Avec Privileged Remote Access, il est en plus possible d'étendre l'accès à des actifs importants, sans compromettre la sécurité. En réduisant le nombre de connexions VPN, vous limitez les points d'infiltration de cybercriminels sur votre réseau.
Platforme	La plateforme PAM de BeyondTrust est une solution intégrée et modulaire offrant contrôle et visibilité sur tous les comptes et utilisateurs à privilèges. En réunissant le plus large éventail de fonctionnalités applicables à la sécurité des privilèges, la plateforme se déploie et s'utilise facilement, permet de maitriser les coûts et réduit les risques liés aux privilèges. Parmi les composants disponibles et centralisés sur la plateforme BeyondInsight pour l'ensemble des solutions BeyondTrust, se trouvent la découverte d'actifs et de comptes, l'analyse des menaces, le reporting et les connecteurs aux systèmes de tiers, ainsi que l'administration centrale et la gestion centralisée des règles.

Plus d'information sur beyondtrust.com/fr/solutions.