SPECOPS SECURE SERVICE DESK

Fiche technique

À PROPOS DE SPECOPS Specops Software est le fournisseur leader de solutions de gestion de mots de passe et d'authentification. Specops protège les données de votre entreprise en bloquant les mots de passe faibles et en sécurisant l'authentification des utilisateurs. Chaque jour, des milliers d'organisations utilisent Specops Software pour protéger leurs données. Pour plus d'informations, veuillez visiter specopssoft.com/fr

SPECOPS SECURE SERVICE DESK

Les réinitialisations de mots de passe par les employés continuent de représenter une part importante des tickets adressés au help desk. En plus de mobiliser des ressources informatiques, elles constituent une faille pour la sécurité de votre organisation. Votre support informatique est-il capable de vérifier qu'un utilisateur est bien celui qu'il prétend être, avant de remettre un nouveau mot de passe à un hacker se faisant passer pour lui ?

La vérification des utilisateurs au niveau du support repose souvent sur des questions basées sur des connaissances personnelles, utilisant des informations statiques issues d'Active Directory ou d'Entra ID, ce qui les rend vulnérables à des attaques ciblées, comme l'exploitation des identifiants employés.

Specops Secure Service Desk réduit le risque d'usurpation d'identité de vos utilisateurs. Les options de vérification d'identité vont des codes de vérification envoyés par téléphone mobile ou par e-mail à des fournisseurs d'authentification tiers tels que Duo Security, Okta, Symantec VIP, PingID et YubiKey. Ces solutions d'authentification sont combinées à une application technique stricte de la vérification d'identité : les agents ne peuvent pas donner suite à la demande de l'appelant tant que l'authentification via la plateforme n'a pas été réalisée.

*48 % des organisations n'imposent aucune vérification d'identité des utilisateurs lors des appels au help desk

Source : The Weak Password Report

Fonctionnalités clés

FONCTIONNALITÉ	AUTRES SOLUTIONS	SPECOPS SECURE SERVICE DESK
Service d'identité tiers OOTB (par exemple, Duo Security, Okta, Symantec VIP, PingID)	Un certain support, mais limité	Oui, ainsi que plusieurs autres options d'identification pour aider les utilisateurs qui n'utilisent pas des appareils mobiles
Interface du help desk pour la vérification des utilisateurs	Oui	Oui (plus des connexions sécurisées pour les agents du help desk)
Réinitialisation assistée des mots de passe	Non	Oui (et peut forcer les utilisateurs à changer leur mot de passe lors de leur prochaine connexion)

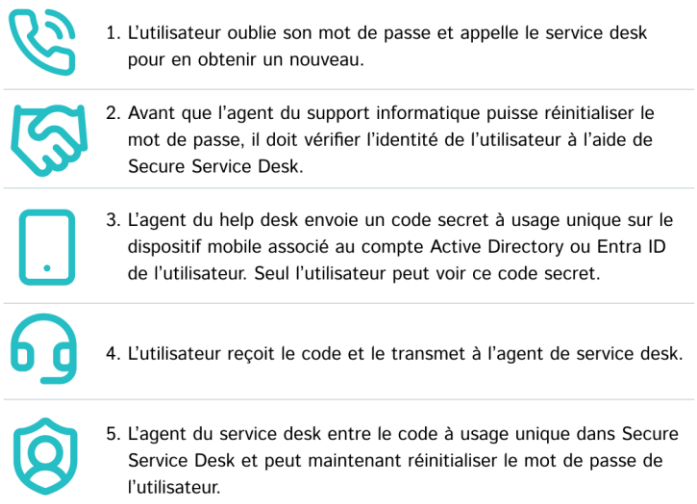
FONCTIONNALITÉ	AUTRES SOLUTIONS	SPECOPS SECURE SERVICE DESK
Obligation de la vérification de l'utilisateur (l'agent ne peut pas procéder sans vérification préalable)	Non (les agents peuvent procéder sans vérifier l'identité du demandeur)	Oui
Suivi de la vérification des utilisateurs	Oui (mais avec des détails limités)	Oui (ils détaillent qui a vérifié, pour quel cas et par qui)
API pour la vérification des utilisteurs	Certains	Oui (permet la vérification des utilisateurs par des systèmes tiers avec plus de 15 services d'identification)

L'attaque par ransomware MGM de 2023, qui a coûté plus de 100 millions de dollars à l'entreprise, a été le résultat d'une absence de vérification d'identité au help desk.

En savoir plus sur l'attaque.

Comment cela fonctionne?

Specops Secure Service Desk est nativement intégré à Active Directory et Entra ID. La configuration du système se fait via une politique de groupe ou de cloud sans ajouter de complexité à votre environnement. La confidentialité est assurée, car l'inscription de vos utilisateurs est chiffrée et n'est pas stockée dans son ensemble à un seul endroit, réduisant ainsi les risques de sécurité tout en garantissant une gestion en temps réel.



À quoi cela ressemble-t-il?

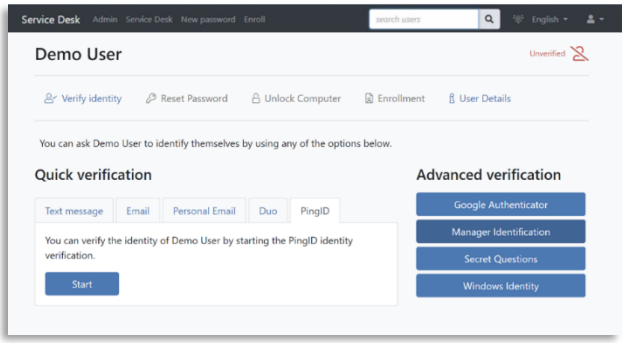
L'interface de la solution permet aux agents du service desk de consulter les informations des utilisateurs et d'effectuer les actions suivantes:

1. Gérer les inscriptions des utilisateurs
2. Réinitialiser les mots de passe Active Directory / Entra ID
3. Récupérer les clés de chiffrement en cas de verrouillage déclenché par BitLocker ou Symantec Endpoint Encryption (non disponible pour Secure Service Desk sur Cloud)

Vue de l'agent du service desk

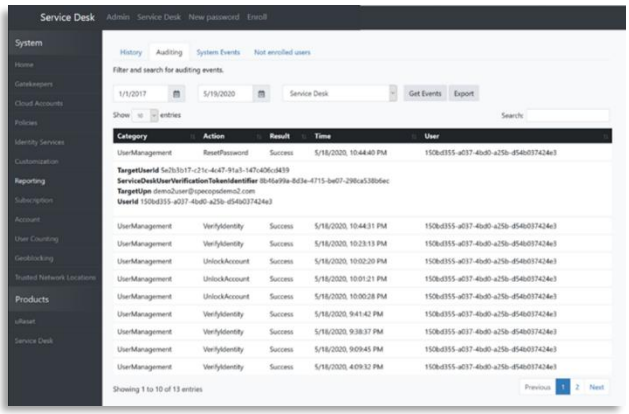
Les actions ci-dessus peuvent être sécurisées en activant l'obligation de vérification de l'identité de l'utilisateur.

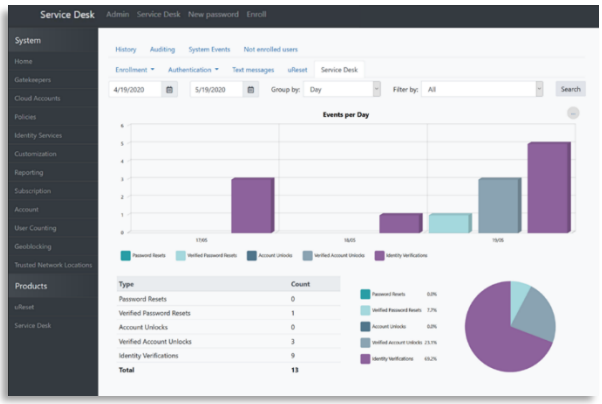
Lorsque cette fonctionnalité est activée, l'agent devra vérifier avec succès l'identité de l'utilisateur avant de pouvoir effectuer l'une de ces opérations critiques.



Interface de rapports pour l'administrateur

La solution permet de suivre la vérification de l'identité des utilisateurs via des journaux d'audit détaillés..





La solution propose également un tableau de bord qui reflète les données de vérification à travers plusieurs cas d'usage. Ces données peuvent également être exportées aux formats JSON ou XLSX pour un traitement ultérieur.

Ce qu'en disent les utilisateurs

Tient ses promesses

" Specops Secure Service Desk tient ses promesses. Il aide les organisations à imposer une vérification sécurisée des utilisateurs grâce à des méthodes d'authentification renforcées."

- Techgenix review par Nuno Mota, Microsoft Exchange, MVP

TechGenix

Exponentiellement plus difficile pour un hacker

"Cela fournit aux techniciens du help desk les moyens de vérifier efficacement l'identité d'un utilisateur supposé lorsqu'il demande une réinitialisation de mot de passe. Cela devrait rendre la tâche exponentiellement plus difficile pour un hacker cherchant à réaliser une attaque par ingénierie sociale ou tout autre type d'attaque visant à voler des identifiants."

- 4sysops review par Brandon Lee, Senior Editor à Virtualizationhowto.com

4sysops

Voir une démo de Specops Secure Service Desk

Souhaitez-vous découvrir comment Specops Secure Service Desk peut être bénéfique pour votre organisation ?

Cliquez ici pour demander une démo ou un essai dès aujourd'hui.

Nos Partenaires Technologiques

Nos partenariats technologiques permettent aux organisations de tirer pleinement parti de leurs investissements et systèmes existants pour renforcer la sécurité des mots de passe — que ce soit en étendant leurs solutions d'authentification multifacteur existantes ou en renforçant les fonctionnalités de Microsoft Active Directory. En savoir plus

Symantec DUO yubico