FICHE TECHNIQUE

Starling Two-Factor Authentication

Une vérification simple et sécurisée de l'identité

Avantages

- Renforce la sécurité pour pratiquement tous les systèmes et applications
- Simplifie la gestion continue sans les coûts des infrastructures et les difficultés des solutions sur site
- Facilite l'adoption par les utilisateurs avec des options d'authentification simples à utiliser, telles que la technologie « push-to-authenticate », les messages SMS et les appels téléphoniques
- Permet au centre d'assistance de répondre rapidement aux problèmes d'authentification à partir de tous les navigateurs Internet
- Réduit les risques de violations de sécurité utilisant des informations d'identification perdues ou volées
- Fournit un suivi d'audit complet pour assurer la conformité

Présentation

Quelle que soit la manière dont les mots de passe sont compromis : à cause du comportement contestable de l'utilisateur, de l'utilisation d'un mot de passe faible ou du vol d'un mot de passe, cela affectera la réputation de votre entreprise et votre chiffre d'affaires. L'authentification à deux facteurs constitue un moyen simple de renforcer la sécurité pour l'accès à vos ressources réseau et d'empêcher la fuite de données.

Grâce à Starling Two-Factor Authentication, une solution SaaS, vous pouvez sécuriser votre entreprise, améliorer la productivité des utilisateurs et réduire considérablement le nombre de demandes de réinitialisation de mot de passe auprès de votre centre d'assistance.

Facilitez et sécurisez l'accès des utilisateurs

La façon la plus simple et la plus sécurisée de remédier à ce problème est l'authentification à deux facteurs (TFA). Cependant, toutes les solutions d'authentification à deux facteurs ne se valent pas. Vous devez tenir compte du fonctionnement de votre entreprise, chercher un moyen de rendre vos processus d'authentification plus efficaces, savoir quels facteurs de forme des jetons sont nécessaires, et connaître la compatibilité de votre infrastructure et de vos piles d'applications existantes.

La solution Starling Two-Factor Authentication résout le problème des mots de passe sans nécessiter de dépenses d'investissement comme cela peut être le cas avec les solutions locales classiques. Son tableau de bord administrateur simple à utiliser et ses options d'authentification flexibles pour les utilisateurs permettent aux entreprises de vérifier facilement et rapidement l'identité d'un utilisateur.

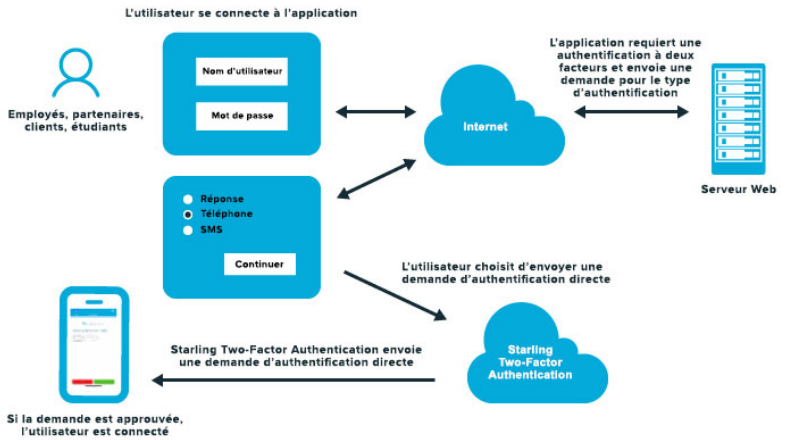

Figure 1. Architecture et modules Starling Two-Factor Authentication.

Fonctionnalités

Tableau de bord administrateur simple à utiliser

Le tableau de bord destiné aux administrateurs est basé sur des rôles et applique un flux d'approbation qui garantit que les administrateurs et les agents du Helpdesk reçoivent les tâches et les droits appropriés. Parallèlement, ce tableau de bord leur simplifie la gestion des comptes utilisateurs, la génération de codes de réponse temporaires et l'exécution de tests d'intégrité pour vérifier que l'application mobile fonctionne correctement.

Méthodes d'authentification multiples

Les utilisateurs peuvent générer des mots de passe à usage unique avec les applications mobiles Starling 2FA pour iOS, Android et Chrome ou bien recevoir un mot de passe à usage unique par SMS ou par téléphone.

Push-to-Authenticate

Simplifiez encore davantage l'authentification à deux facteurs pour vos utilisateurs : ils peuvent contourner le mot de passe à usage unique en choisissant l'option « push-to-authenticate », après avoir saisi leur nom d'utilisateur et leur mot de passe dans l'application. Ceci enverra un SMS de vérification sur leur application mobile leur demandant s'ils approuvent ou refusent la demande de connexion à l'application. Après approbation, ils seront automatiquement connectés à l'application.

Jetons

La solution d'authentification à deux facteurs Starling offre plusieurs options, notamment les applications mobiles pour iOS, Android et Chrome, les messages SMS, et les appels téléphoniques.

Personnalisation des jetons

À l'aide du tableau de bord Starling, les administrateurs peuvent facilement personnaliser l'apparence du jeton sur l'application mobile afin de lui appliquer la marque de leur entreprise.

Adaptateur ADFS

Ceci permet aux entreprises de mettre en place l'authentification à deux facteurs pour les applications qui utilisent le protocole Microsoft WS-Federation, comme Office 365. Par ailleurs, cette fonction est compatible avec d'autres protocoles de fédération, y compris SAML 2.0, afin de prendre en charge les connexions aux applications Cloud comme Google Apps et salesforce.com.

Agent Radius

Cette fonction permet aux entreprises de prendre en charge l'authentification à deux facteurs sur tout appareil qui utilise le protocole radius comme moyen d'authentification.

Agent HTTP

Ceci met en place l'authentification à deux facteurs pour les sites Web IIS.

Connexion sur les postes de travail

Ceci permet d'améliorer votre environnement et ajoute une authentification à deux facteurs aux ordinateurs et aux serveurs des utilisateurs en unifiant les connexions et en renforçant l'authentification.

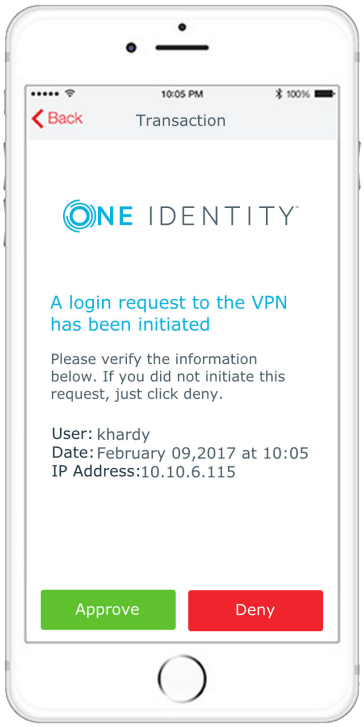

Figure 2. La technologie « push-to-authenticate » simplifie et sécurise le processus de connexion des utilisateurs.

À propos de One Identity

One Identity aide les entreprises à assurer une gestion réussie des accès et des identités. Grâce à notre combinaison unique d'offres, notamment une gamme de gestion des identités, de gestion des accès, de gestion des accès à privilèges, et des solutions d'identité « as a service » les entreprises peuvent réaliser leur potentiel sans être entravées par la sécurité et tout en étant protégées contre les menaces. En savoir plus sur le site OneIdentity.com