FICHE TECHNIQUE

Defender®

Protégez votre périmètre avec l'authentification à deux facteurs

Avantages

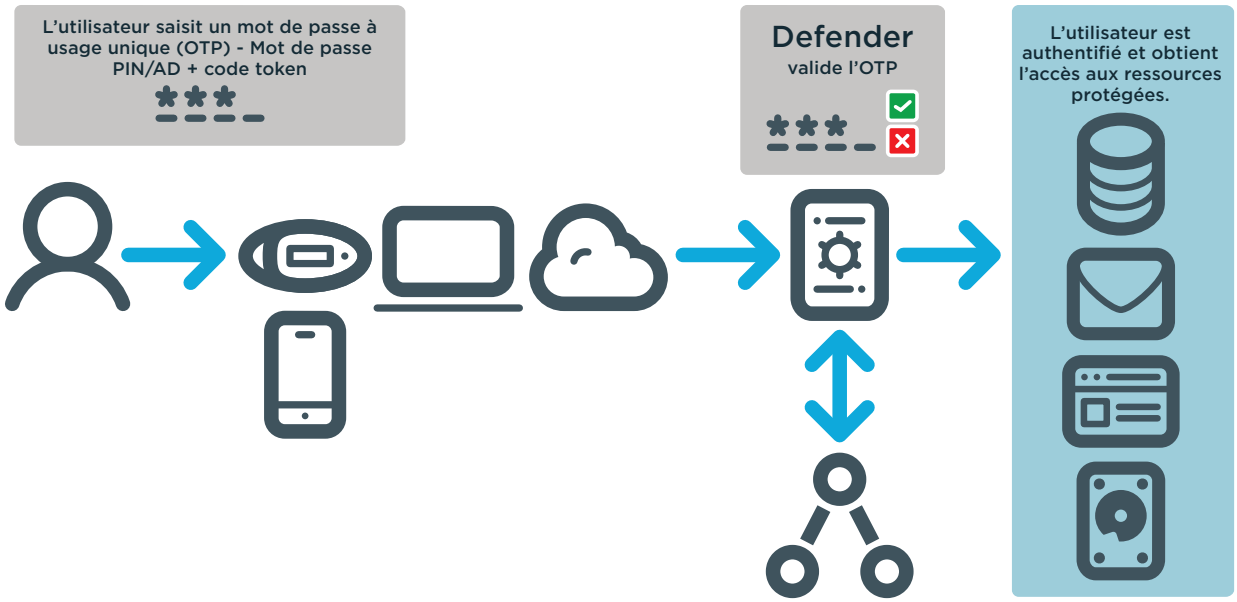
- Sécurité renforcée pour pratiquement tous les systèmes et applications
- S'appuie sur l'extensibilité, la sécurité et la conformité d'Active Directory
- Active l'auto-enregistrement des jetons et le renouvellement par les utilisateurs.
- Accélère la résolution des problèmes d'authentification des utilisateurs par le Helpdesk
- Prend en charge tous les tokens physiques compatibles OATH
- Fournit une piste d'audit complète à des fins de conformité et d'analyses

Configuration système requise

Pour obtenir la liste complète des conditions requises, rendez-vous sur le site oneidentity.com/Defender

Aujourd'hui, les exigences en termes de conformité et de sécurité poussent les organisations à adopter des niveaux de sécurité allant au-delà du nom d'utilisateur et mot de passe classique. L'authentification à deux facteurs (associant un objet possédé, comme un jeton, avec une chose connue, c'est-à-dire un nom d'utilisateur et un mot de passe) est rapidement devenue la méthode la plus courante de sécurité et de conformité des organisations. Auparavant les solutions d'authentification à deux facteurs étaient coûteuses à déployer et elles étaient basées sur des interfaces et des répertoires propriétaires. Cependant, Defender® est une solution entièrement basée sur les standards (OATH, RADIUS, LDAP, PAM etc.) et elle s'appuie sur Active Directory (AD) pour l'administration et la gestion des identités. L'utilisation d'AD améliore la sécurité et l'extensibilité, mais permet également de réaliser des économies en autorisant les collaborateurs actuels à gérer Defender.

ONE IDENTITY



Defender s'appuie sur les infrastructures existantes des organisations afin d'améliorer la sécurité de manière flexible et économique.

En outre, Defender permet aux utilisateurs de faire la demande de tokens physiques et logiciels et de les enregistrer eux-mêmes en toute sécurité, ce qui réduit les coûts et le temps généralement nécessaire pour mettre en place l'authentification à deux facteurs. Defender prend en charge tous les tokens physiques compatibles OATH ainsi que de nombreux tokens logiciels et de navigateurs webs. En s'appuyant sur les infrastructures existantes, en proposant l'auto-enregistrement et en prenant en charge de nombreux types de jetons, Defender offre aux organisations la possibilité de renforcer la sécurité et la conformité de manière flexible et économique.

Fonctionnalités

Concept centré autour d'Active Directory : utilisez l'extensibilité, la sécurité et la conformité d'Active Directory pour fournir une authentification double facteur à tout système, application ou ressource, vous permettant d'exploiter l'annuaire d'entreprise déjà en place sans avoir à en créer un autre qui serait propriétaire. L'attribution des jetons aux utilisateurs se traduit simplement par un attribut supplémentaire de propriété des utilisateurs dans Active Directory.

Administration en ligne : offrez aux administrateurs Defender, aux administrateurs du helpdesk et aux utilisateurs finaux la possibilité de gérer et de déployer des jetons, de consulter des journaux en temps réel, de résoudre les problèmes et de créer des rapports à l'aide du portail de gestion en ligne Defender.

Auto-enregistrement des jetons : offrez aux utilisateurs la possibilité de demander un jeton physique ou logiciel en fonction de la politique définie par les administrateurs, et d'attribuer rapidement et facilement ce jeton à leur compte par le biais d'un mécanisme sécurisé.

Identificateur de problèmes du helpdesk : aidez les administrateurs de Defender et du helpdesk à identifier, diagnostiquer et résoudre les problèmes liés à l'authentification des utilisateurs en quelques clics et à partir de n'importe quel navigateur Internet. Consultez une liste mise à jour des tentatives et itinéraires d'authentification ainsi que les résultats associés, les raisons possibles d'échec et les étapes de résolution en un clic. L'outil montre également les détails des comptes utilisateurs et les jetons attribués, avec la possibilité de tester et de réinitialiser rapidement le code PIN, de fournir une réponse de jeton temporaire, ou encore de réinitialiser ou de déverrouiller le compte.

Flexibilité des jetons : déployez tous les jetons matériels compatibles OATH de votre fournisseur de choix. Defender offre également une large gamme d'authentifications fortes pour

« Après plusieurs années d'utilisation, Defender s'est révélée comme une solution robuste qui n'a jamais connu de défaillance. Elle est tellement simple à utiliser et elle s'est tellement bien intégrée à nos opérations que nous ne la voyons plus comme une solution distincte ».

Gregory Pronovost
Assistant de direction du département informatique
City of Bakersfield

les plateformes mobiles les plus populaires et les plus déployées. Une licence universelle de jeton logiciel permet d'émettre une nouvelle licence adaptée pour l'appareil lorsqu'un utilisateur décide de changer de plateforme mobile.

Accès au webmail sécurisé : mettez en place un accès web sécurisé à votre messagerie d'entreprise quel que soit le navigateur web utilisé, l'heure ou l'endroit avec Webthority, une solution proxy inverse comprise dans Defender. De plus, vous pouvez exiger l'utilisation de jetons Defender afin de garantir une authentification appropriée quel que soit le point d'accès.

Migration ZeroIMPACT : procédez à une migration graduelle vers Defender à partir d'une solution d'authentification héritée avec ZeroIMPACT. Lorsque Defender et votre système hérité fonctionnent côte à côte, toutes les demandes d'authentification des utilisateurs sont redirigées vers Defender. Si l'utilisateur n'est pas encore défini dans Defender, la demande d'authentification est transmise de façon transparente, via la fonction Proxy, à la solution d'authentification héritée. Ainsi, les administrateurs peuvent accomplir la migration des utilisateurs vers Defender à mesure que leurs jetons hérités arrivent à expiration.

Administration centralisée : intégrez Defender à Active Directory et tirez pleinement profit de la gestion centralisée des informations de l'annuaire à travers une interface utilisateur commune et familière. L'attribution de jetons utilisateur consiste simplement à affecter un attribut supplémentaire aux propriétés d'un utilisateur dans l'annuaire, ce qui simplifie grandement l'administration de la sécurité.

Chiffrement : sécurisez les communications en associant un standard de chiffrement des données (DES) avec le serveur de sécurité Defender. Defender prend en charge les algorithmes de chiffrement AES, DES et Triple DES.

Module d'authentification branché (PAM) : précisez que les services et utilisateurs de votre système Unix/Linux seront authentifiés par Defender avec le module Defender pour PAM.

À propos de One Identity

La gamme One Identity de solutions de gestion des accès et des identités (IAM) inclut une offre de solutions IAM concrètes de gouvernance des identités, de gestion des accès, et de gestion des comptes à privilèges axées sur l'entreprise, modulaires, intégrées et tournées vers l'avenir.

Pour en savoir plus, visitez OneIdentity.com

© 2017 Quest Software Inc. TOUS DROITS RÉSERVÉS. Quest et le logo Quest sont des marques et des marques déposées de Quest Software Inc. aux États-Unis et dans d'autres pays. Pour obtenir la liste complète des marques Quest Software, veuillez visiter notre site Web www.quest.com/legal. Toutes les autres marques, marques de service, marques déposées et marques de service déposées appartiennent à leurs propriétaires respectifs.
Datasheet-Defender-US-KJ-FR-WL-25672

ONE IDENTITY