Protéger vos ressources réseau avec de l'Authentification Multi-Facteurs

Sommaire

L'ÉVOLUTION DE L'AUTHENTIFICATION – COMMENT Y SOMMES-NOUS PARVENUS ?

Le problème de l'authentification

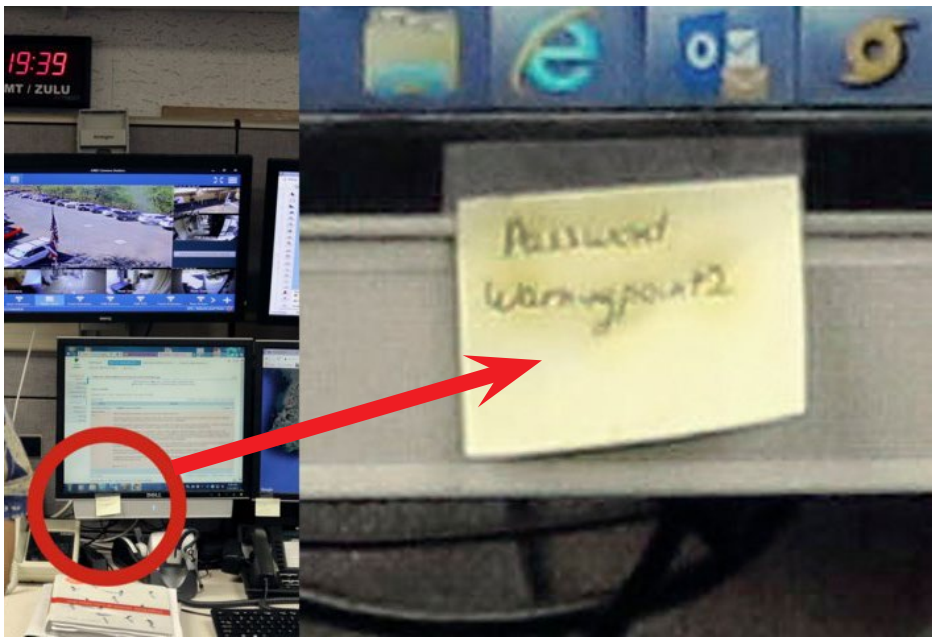
Internet a modifié notre façon de travailler. L'accès à l'Internet rapide, que ce soit à la maison ou grâce aux millions de bornes WiFi dans les espaces publics, permet aux employés de travailler n'importe où – chez eux, dans les hôtels, dans les cafés. Les informations d'entreprise ne sont plus concentrées dans des salles de serveurs ou des centres de données sur site ; elles sont distribuées dans le Cloud par le biais des CRM, des serveurs de messagerie et des portails Web.

Chaque jour, au moins un employé s'authentifie sur plusieurs de ces services. Il commence par allumer son ordinateur. Ensuite, il se connecte à un serveur de messagerie et peut-être à une application Cloud. S'il ne peut se rendre physiquement à son bureau, il se connecte probablement au réseau via un VPN. Et où se trouvent les identifiants de l'utilisateur ? Le trafic de données transporte les identifiants de l'utilisateur sur les connexions WiFi et les réseaux publics.

Si, à un moment donné, ces identifiants sont exposés, quelle est la chance que le même mot de passe soit utilisé sur la plupart des autres services ? Il y a de fortes chances que ce soit le cas. Sachant que nous utilisons des dizaines de mots de passe chaque jour – pour l'entreprise, la banque, les cartes de crédit, les sites de commerce en ligne, les médias sociaux, les points de vente mobiles, etc. – qui choisirait volontairement un mot de passe différent pour chacun de ces services ?

Le mot de passe qui est saisi lorsque vous accédez au site Web de votre supermarché est probablement identique à celui que vous utilisez pour vous connecter à votre ordinateur, voire pire, au VPN qui vous connecte au réseau de l'entreprise. Comme nous pouvons le voir, le problème du mot de passe ne se limite pas au réseau de l'entreprise. Il est impossible de dire à l'avance si un employé utilisera le même mot de passe pour chaque type de service personnel ou s'il partagera un jour son mot de passe avec quelqu'un d'autre.

Une chose est sûre, c'est que nous ne pouvons pas faire confiance aux mots de passe. Ils peuvent être partagés. Écrits. Usurpés. Devinés. Crackés. Volés.



81 %

des fuites survenues en 2016 sont la conséquence de mots de passe volés et/ou vulnérables

Verizon sur les atteintes à la sécurité des données

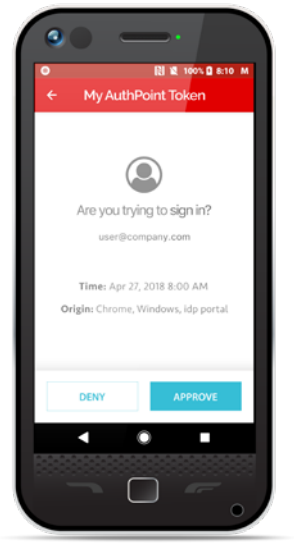
L'authentification multifacteur

L'expression « authentification à deux facteurs » ou « authentification robuste » n'est pas nouvelle. Son utilisation s'est répandue dans les années 1990 pour désigner un jeton physique générant des mots de passe à usage unique (OTP) associés à un mot de passe fixe. En réalité, l'authentification à deux facteurs consiste à utiliser les deux facteurs suivants :

- Quelque chose que vous connaissez : mot de passe, code PIN
- Quelque chose que vous possédez : jeton, appareil physique, clé
- Un attribut physique : empreinte digitale, reconnaissance faciale

L'évolution de la technologie, en particulier concernant l'utilisation des smartphones et la croissance des applications, a permis d'accroître le nombre de facteurs simultanés sans compromettre la facilité d'utilisation. Lorsque que deux facteurs ou plus sont utilisés, on parle d'authentification multifacteur (MFA). La solution AuthPoint de WatchGuard constitue un bon exemple de MFA puisqu'elle utilise quatre facteurs d'authentification.

POURQUOI CHOISIR L'AUTHENTIFICATION MULTIFACTEUR (MFA) ?



Voici les facteurs d'authentification standard qui peuvent être utilisés par les solutions de MFA :

1. **Quelque chose que vous connaissez**
   (votre mot de passe)
2. **Quelque chose que vous possédez**
   (un jeton sur votre téléphone)
3. **Quelque chose que vous possédez**
   (un ADN de téléphone)
4. **Un attribut physique**
   (une empreinte digitale pour bénéficier de l'accès)

L'utilisation de facteurs multiples améliore la sécurité globale de la solution et offre une protection supplémentaire contre plusieurs types d'attaques telles que l'ingénierie sociale et les RAT (les chevaux de Troie à distance) destinées à cloner des applications.

Sécurité vs. Expérience utilisateur

Les premiers authentificateurs, ou jetons de mots de passe à usage unique (OTP), étaient fournis comme équipements matériels dont la forme et la taille étaient légèrement supérieures à un porte-clés. Les OTP changeaient toutes les 60 secondes et pour s'authentifier sur un système, l'utilisateur devait saisir le mot de passe suivi de l'OTP figurant sur l'écran. Par exemple, le mot de passe pouvait être « monmotdepasse » et le jeton affichait « 122134 ». L'utilisateur devait donc taper :

```
monidentifiant
monmotdepasse122134
```

Sans parler du fait que l'utilisateur devait en permanence être muni de son porte-clés. En outre, le fait qu'il s'agisse d'un porte-clés physique n'arrangeait pas vraiment les choses. Si vous avez déjà utilisé un jeton de porte-clés par le passé, il est très probable que vous l'ayez oublié un jour à la maison et qu'il ait fallu appeler quelqu'un pour qu'il vous communique l'OTP par téléphone . Vous êtes peut-être également parti en voyage en attachant le jeton sur votre trousseau de clés de voiture, lequel est resté à la maison.

Les professionnels de la sécurité ont souvent clamé haut et fort que la facilité d'utilisation était inversement proportionnelle à la sécurité. C'était un fait et la situation allait empirer. Les utilisateurs possédant des jetons connectés ou des cartes à puces avec lecteur devaient installer un logiciel et un middleware en plus de gérer des certificats numériques – le tout pour un énorme coût total de possession. Et s'ils devaient les utiliser pour s'authentifier sur des applications mobiles, bonne chance pour se connecter !

Lorsque les téléphones portables sont finalement devenus populaires, ce fut également le cas des SMS, lesquels pouvaient désormais être utilisés pour recevoir l'OTP à condition d'être au bon endroit pour bénéficier d'un service efficace. Il n'était pas rare, lorsque l'on était en déplacement à l'étranger, de ne pas recevoir du tout les SMS ou de les recevoir avec plusieurs heures de retard. En outre, si vous souhaitiez vous authentifier à l'aide de votre navigateur de téléphone, il fallait sans cesse switcher entre les applications. En 2016, après avoir exploré différentes façons de contourner l'authentification basée sur les SMS, le NIST (National Institute of Standards and Technology) a fini par désapprouver le SMS comme méthode d'authentification à deux facteurs.

À la fin des années 2000, les téléphones portables ont connu des améliorations même s'il existait plusieurs systèmes d'exploitation et distributeurs. Symbian, BlackBerry OS, Windows Mobile, BREW... La liste est longue. Le développement d'une application pour téléphone n'était pas une mince affaire. Il était nécessaire d'avoir les SDK du distributeur ainsi qu'une série de modèles de téléphones variés. Pour faire fonctionner une application Java, il fallait installer le logiciel J2ME et les résultats visuels n'étaient absolument pas attrayants jusqu'à ce que le marché des smartphones connaisse un essor important, impulsé et polarisé par Android et iOS. Cela a permis aux entreprises de développer des applications professionnelles en suivant les directives en matière de facilité d'utilisation et en privilégiant le même format pour les menus, les boutons, etc. C'est à ce moment que les jetons mobiles ont connu une popularité croissante.

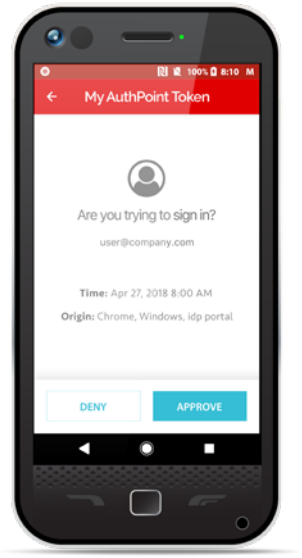
Le smartphone est devenu un objet de notre vie quotidienne, comme les vêtements. Si l'on est toujours avec notre smartphone, quel est l'intérêt d'être muni de jetons physiques ?

En fin de compte, la technologie push a modifié le paradigme opposant la facilité d'utilisation et la sécurité. En effet, elle a permis d'améliorer à la fois la sécurité et l'expérience utilisateur.

> En raison du risque que les messages par **SMS** ou les **appels téléphoniques** soient **interceptés ou redirigés,** les agents d'exécution de nouveaux systèmes doivent sérieusement envisager des authentificateurs alternatifs.
>
> *National Institute of Standards and Technology, 2016*

Technologie push

BlackBerry a présenté le « push » comme une technologie capable d'améliorer la productivité. Le BlackBerry offrait un avantage majeur, celui de pouvoir voir quasiment instantanément quand un nouveau courriel arrivait sur notre téléphone. La lumière rouge clignotante du BlackBerry est devenue partie intégrante de notre vie.



L'évolution des iPhone et des appareils Android a permis d'utiliser les services push sur différentes applications. La messagerie, l'actualité, les courriels. Il n'était plus nécessaire d'ouvrir son téléphone et de se connecter à un service, car les notifications arrivaient par le biais de ce nouveau canal.

Cette situation a ouvert la voie à de nouvelles possibilités pour la MFA. Au lieu d'ouvrir l'application mobile du jeton, de lire l'OPT et de le saisir, il était désormais possible de recevoir la demande d'authentification sur son téléphone avec des informations plus détaillées, notamment sur la personne tentant de s'authentifier et sur son emplacement. La seule action requise était d'approuver ou de rejeter en appuyant sur un simple bouton. La connexion s'établissait de nouveau avec le service demandant l'accès et, si tout était correct, l'OTP unique était renvoyé de manière sécurisée sans même que l'utilisateur le sache.

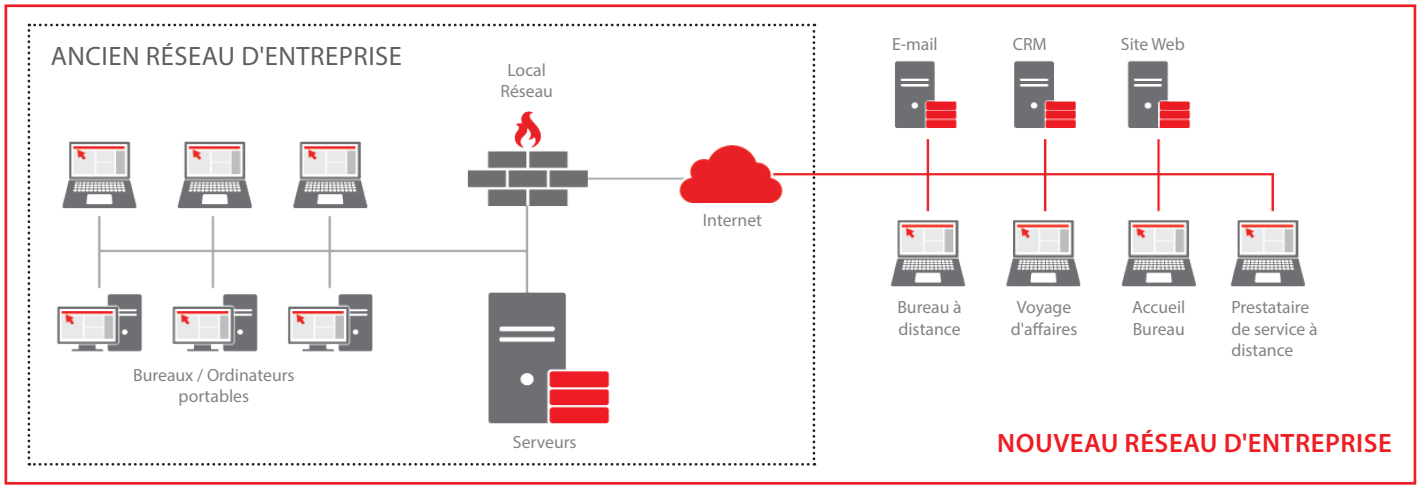
À présent, il existe une solution capable d'offrir une plus grande facilité d'utilisation consistant à appuyer sur un bouton afin de savoir à quoi vous vous authentifiez, le tout en toute sécurité : l'Authentification Multi-Facteurs (MFA).

PROTÉGER VOS RESSOURCES RÉSEAU AVEC DE L'AUTHENTIFICATION MULTI-FACTEURS

Le nouveau réseau d'entreprise

Le réseau ne se résume pas à des bureaux et des serveurs connectés et protégés derrière un pare-feu. Les ressources réseau de l'entreprise sont distribuées sur des applications Cloud, des serveurs de réseau et des ordinateurs à distance. Chacune d'entre elles connait des utilisateurs et des mots de passe différents, et des prestataires de service tiers y accèdent parfois de manière temporaire. Cette situation engendre des risques pouvant mener à toutes sortes d'attaques, dont la plupart commencent par la capture, le crackage ou le partage d'un identifiant ou d'un mot de passe par le biais de l'ingénierie sociale.

Nous allons vous expliquer comment utiliser la solution AuthPoint de WatchGuard afin de protéger vos applications avec de l'Authentification Multi-Facteurs.



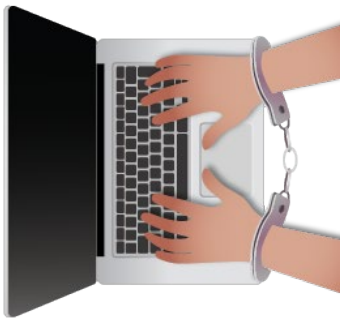
VPN / Accès à distance

L'accès à distance au réseau de l'entreprise est essentiel pour permettre aux utilisateurs éloignés ou en déplacement d'accéder aux serveurs et aux informations internes. Il suffit :

- d'un utilisateur dont le mot de passe vulnérable a été cracké
- d'un utilisateur dont l'ordinateur est infecté par un enregistreur de frappes sous la forme d'un cheval de Troie
- d'un utilisateur qui partage son mot de passe ou son OTP

Le pirate informatique, quel que soit son emplacement, jouit désormais d'un accès au réseau et, la plupart du temps, des mêmes privilèges que toute personne physiquement présente dans les locaux de l'entreprise et connectée au réseau.

Il est donc indispensable d'instaurer un contrôle d'identité supplémentaire, au-delà du simple mot de passe, avant d'autoriser les utilisateurs à accéder aux VPN. Par ailleurs, l'Authentification Multi-Facteurs offre une intégration rapide et facile avec les pare-feux et les passerelles d'accès à distance grâce au protocole RADIUS. Par exemple, avec le service MFA AuthPoint de WatchGuard, la configuration peut s'effectuer en quelques minutes et de deux façons différentes :



1. **Utilisation d'un mot de passe + OTP**

   Cette solution ne se limite pas à saisir l'identifiant et le mot de passe sur un VPN client ou un VPN sans client basé sur le navigateur ; l'utilisateur doit en effet ajouter l'OTP – composé de 6 chiffres généralement – à la fin du mot de passe. Le pare-feu reçoit alors la demande et la transmet à AuthPoint, qui validera à la fois le mot de passe et l'OTP.

2. **Utilisation d'un mot de passe + push**

   Cette méthode offre une expérience utilisateur idéale, car elle ne varie pas tellement de la méthode actuelle. L'utilisateur continuera en effet de saisir son identifiant et son mot de passe, comme avant. La seule différence, c'est qu'AuthPoint enverra une demande d'authentification à l'aide du push. L'utilisateur recevra un message sur son application lui indiquant précisément la personne qui tente de s'authentifier et son emplacement. Si l'utilisateur est la personne identifiée, il ne lui reste plus qu'à approuver en cliquant sur un bouton.

Méthode d'authentification	Avantages	Inconvénients
OTP classique	• Méthode classique et connue de tous, utilisée depuis plus de 20 ans.	• Soumise à l'ingénierie sociale • L'utilisateur doit saisir l'OTP à chaque fois • Cette méthode peut être déroutante pour certains utilisateurs (mot de passe + OTP ou OTP + mot de passe ?)
Push	• Meilleure expérience utilisateur ; l'utilisateur n'a plus qu'à approuver ou rejeter • Meilleure visibilité ; le message push affiche le contexte de l'authentification et réduit les risques d'ingénierie sociale • Plus grande sécurité ; l'OTP envoyé dans le push ne peut être copié ou volé	• Nécessite une connexion de données depuis le téléphone portable (authentification en ligne)

Face à l'émergence des applications et des solutions Cloud, les services basiques mais essentiels, tels que la messagerie électronique et les serveurs Web, ont commencé à migrer sur le Cloud. À l'heure actuelle, le fait d'installer et de maintenir ces serveurs sur le réseau est impensable. Les services du Cloud offrent pratiquement tout ce qu'on peut imaginer comme les CRM, les ERP, les plateformes de développement, etc.

Toutefois, tous ces nouveaux services font naître de nouveaux défis :

- Comment les utilisateurs seront-ils capables de garder en mémoire les différents mots de passe de ces services ?
- Les utilisateurs doivent ajouter les URL à leurs favoris et tenter d'organiser tous les services auxquels ils ont accès
- Comment s'assurer que les informations d'identification usurpées ne donneront pas accès à d'autres services qui sont facilement accessibles de partout dans le monde ?

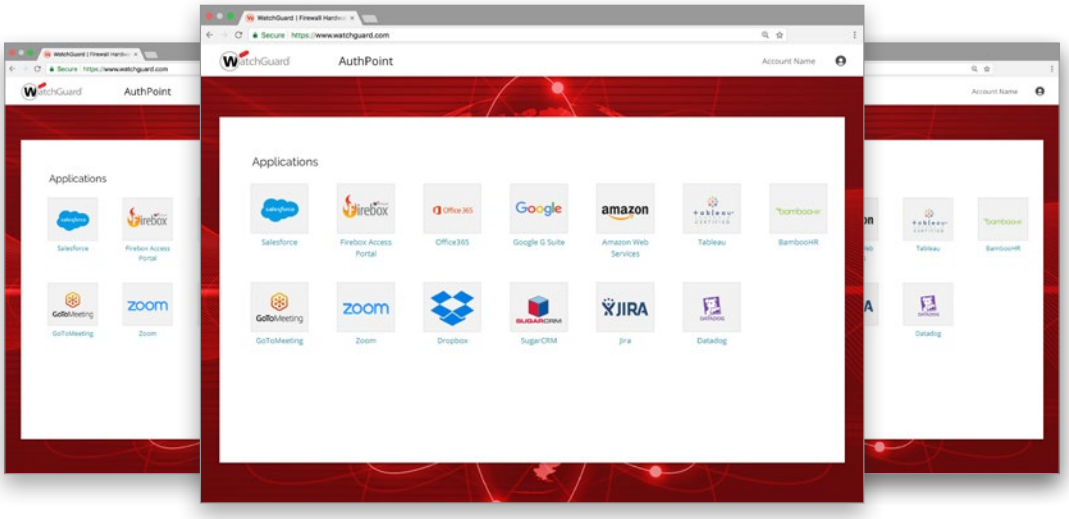
Le protocole SAML (Security Assertion Markup Language) a vu le jour pour résoudre la plupart de ces problèmes. Son implémentation est fondée sur deux entités principales :

- Le fournisseur d'identité (IdP) : toute entité chargée d'authentifier et d'identifier correctement les utilisateurs
- Le fournisseur de service (SP) : toute entité qui entretient une relation de confiance avec un idP et qui l'utilise pour vérifier l'identité

Expliquons les choses très simplement : un SP entretient une relation de confiance avec l'IdP, ce qui signifie que si l'IdP authentifie et identifie un utilisateur, le SP se basera sur cette information pour procéder à l'authentification unique de l'utilisateur sur le service – même si l'utilisateur possède un mot de passe différent pour le service. Parmi les SP figurent Firebox® Access Portal, Salesforce, Google Apps, BambooHR, Jira, Office365, entre autres.

Partant de ce constat, il va sans dire que l'IdP est l'élément essentiel. Une fois que l'IdP a authentifié l'utilisateur, ce dernier bénéficie d'un accès d'authentification unique à l'ensemble des applications Cloud qui lui sont autorisées. Il est par conséquent capital de choisir le bon IdP.

Les solutions de MFA basées sur le Cloud ont la possibilité de fournir un service IdP. Par exemple, en choisissant notre solution AuthPoint, un abonné pourra bénéficier d'un portail exclusif afin d'authentifier les utilisateurs. Une fois authentifié, l'utilisateur aura accès aux applications Cloud liées à son groupe.



Cette solution offre des avantages considérables en termes de sécurité et d'expérience utilisateur.

- L'utilisateur a simplement besoin de mettre la page de portail de l'IdP dans ses favoris
- La méthode d'authentification principale peut être configurée afin d'accroître la sécurité – par exemple, l'authentification push au lieu de l'OTP classique
- L'utilisateur n'a pas besoin de garder en mémoire tous les mots de passe de l'application Cloud. Une fois que le portail IdP d'AuthPoint authentifie l'utilisateur, une relation de confiance s'établit avec les applications Cloud.
- Les stratégies de groupe autorisent les administrateurs à définir précisément quelles applications sont accessibles par chaque utilisateur
- Si des informations d'identification ont été usurpées, la MFA aura bien lieu, mais elle bloquera l'accès aux pirates informatiques qui n'ont pas pu s'authentifier

Ordinateurs portables / Logon ordinateurs

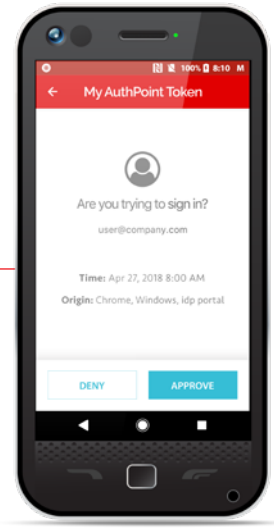
Encore une fois, les données d'identification de l'utilisateur peuvent être volées, crackées ou devinées. Un ordinateur laissé sans surveillance peut être du pain béni pour une personne qui est en possession de ces données d'identification. Un tel cas de figure peut se produire dans les locaux de l'entreprise, mais également avec des employés qui travaillent à distance ou sont en déplacement.

L'utilisation de la MFA pour l'identification sur un ordinateur non seulement protège le processus d'identification, mais offre également une meilleure expérience utilisateur.

AuthPoint Logon Agent est un composant qui peut être installé sur les ordinateurs Windows et macOS afin d'intégrer la MFA au processus d'identification. Après avoir saisi l'identifiant et le mot de passe, l'utilisateur reçoit un message push dans l'application AuthPoint lui demandant s'il approuve l'identification sur son ordinateur.

ÉTAPE 1

Cliquez sur « Envoyer une push »



ÉTAPE 2

Confirmez la demande d'identification du PC avec l'application AuthPoint

ÉTAPE 3

Vous êtes authentifié !

L'expérience utilisateur est également meilleure lorsque l'utilisateur verrouille l'ordinateur. En effet, il n'est pas nécessaire de saisir à nouveau l'identifiant et le mot de passe. La seule action requise est d'approuver l'identification lorsque vous recevez le message push.

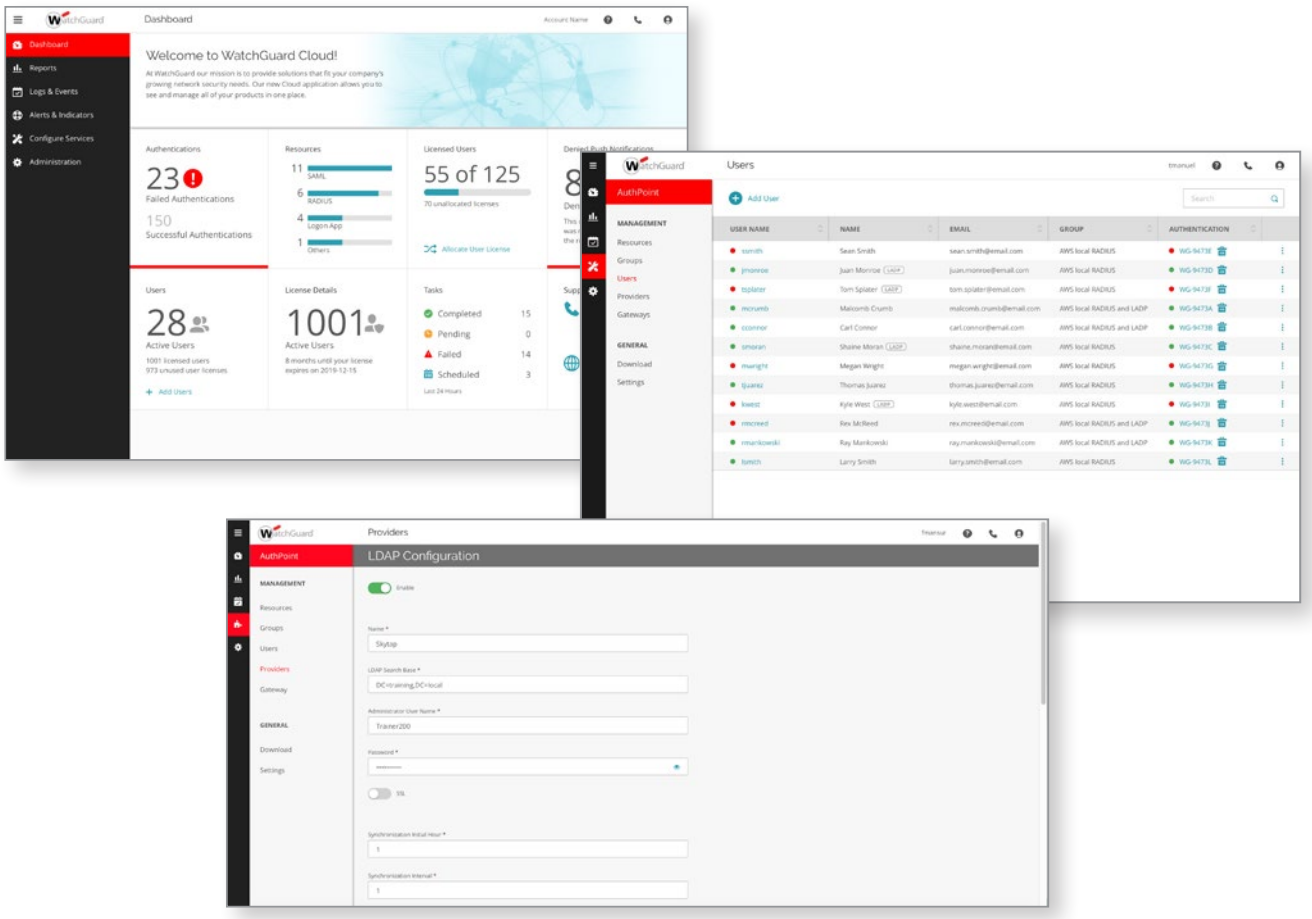
Grâce à sa polyvalence, cette solution permet de s'identifier sur l'ordinateur même lorsqu'aucune connexion Internet n'est accessible – en mode hors ligne. Cette option peut se révéler très pratique lorsque vous utilisez votre ordinateur dans l'avion, par exemple. Le cas échéant, une authentification défi-réponse peut être utilisée avec un code QR contenant des données chiffrées ; seul l'authentificateur AuthPoint de l'utilisateur est capable de les lire, de les déchiffrer et de générer une réponse.

Gestion dans le Cloud

La MFA basée dans le Cloud offre de nombreux avantages par rapport aux solutions de MFA sur site.

- Aucune installation requise
- Déploiement rapide
- Inutile d'investir dans du matériel ou des systèmes d'exploitation
- Inutile de se soucier des correctifs, de la disponibilité, des performances ou de la haute disponibilité
- Tout le monde est capable de gérer cette solution, où que ce soit dans le monde

La configuration, l'installation et la mise en fonctionnement d'une solution d'authentification sur site peuvent prendre plus d'une journée. La MFA basée dans le Cloud crée un tout nouvel environnement en moins d'une minute et peut être immédiatement configurée. Son implémentation peut prendre moins d'une heure.



Les piliers de la solution AuthPoint de WatchGuard

La technologie de l'authentification a évolué vers les services basés dans le Cloud qui garantissent un déploiement rapide, une intégration facile et une gestion sans tracas. Lorsqu'ils sont combinés à une application mobile, la sécurité est largement à la portée de l'utilisateur. D'une simple pression, l'utilisateur peut vérifier et approuver une demande d'authentification ou rejeter la tentative d'accès d'un intrus non autorisé et ainsi tuer dans l'œuf toute cyberattaque.

WatchGuard AuthPoint entend proposer la solution de sécurité MFA idéale en mettant l'accent sur ce qui importe le plus à chaque entreprise – la protection de l'accès aux ordinateurs, aux réseaux et aux applications Cloud dans les meilleures conditions et la garantie d'une expérience utilisateur inégalée.
Afin d'y parvenir, nous avons bâti AuthPoint sur six piliers essentiels :

- La sécurité
- La simplicité
- L'expérience utilisateur
- Déploiement rapide
- L'intégration facile
- La rentabilité

Pour en savoir plus sur le service AuthPoint de WatchGuard, rendez-vous sur le site www.watchguard.com/authpoint.

À propos de WatchGuard

WatchGuard® Technologies, Inc. est un leader mondial de la sécurité réseau, des connexions Wi-Fi sécurisées et des produits et services de supervision réseau, et sert plus de 80 000 clients dans le monde. La société a pour mission de rendre la sécurité de pointe accessible aux entreprises de tous types et de toutes tailles, ce qui fait de WatchGuard la solution idéale pour les entreprises multisites et pour les TPE, PME, ETI et administrations. WatchGuard a établi son siège social à Seattle, aux États-Unis, et possède des bureaux dans toute l'Amérique du Nord, en Europe, en Asie-Pacifique et en Amérique latine. Pour en savoir plus, rendez-vous sur le site WatchGuard.com.

Pour obtenir des informations supplémentaires, des promotions et des mises à jour, suivez WatchGuard sur Twitter @WatchGuard, sur Facebook ou sur la page LinkedIn de l'entreprise. N'hésitez pas à consulter notre blog InfoSec, Secplicity, pour des informations en temps réel sur les toutes dernières menaces et sur la manière d'y faire face : www.secplicity.org.

FRANCE 01 40 90 30 35 SERVICE COMMERCIAL INTERNATIONAL +1.206.613.0895 www.watchguard.fr