FICHE TECHNIQUE

AUTHPOINT

L'authentification multifacteur (MFA) : un jeu d'enfant !

LES MOTS DE PASSE NE SUFFISENT PAS

Tous les jours, des cyber-criminels utilisent des identifiants dérobés afin d'infiltrer et d'infecter des systèmes, mais également pour voler des données. Afin de combattre cette situation, il est indispensable de demander des preuves d'identité supplémentaires, et de ne pas se limiter au login et au mot de passe lors de l'authentification.

L'AUTHENTIFICATION MULTIFACTEUR ÉLOIGNE LES IMPOSTEURS

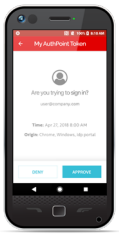
WatchGuard AuthPoint™ permet de corriger cette faille de sécurité à l'aide d'une authentification multifacteur sur une plateforme Cloud simple à utiliser. Avec une simple notification push, l'application mobile AuthPoint signale toute tentative d'identification, ce qui permet à l'utilisateur d'accepter ou de refuser le droit d'accès depuis son smartphone. L'approche unique de WatchGuard se démarque grâce au facteur « ADN de téléphone portable » qui permet de s'assurer que seules les bonnes personnes ont accès aux réseaux et aux applications Cloud sensibles.

GESTION CLOUD INTUITIVE

L'authentification multifacteur était jusqu'alors inaccessible pour bon nombre d'entreprises en raison des intégrations complexes et de la gestion sur site fastidieuse, ainsi qu'un coût élevé. Au contraire, la solution AuthPoint de WatchGuard est un service Cloud. Il ne nécessite pas de déployer du matériel onéreux et il peut être géré depuis n'importe où grâce à l'interface intuitive de WatchGuard Cloud. En outre, notre écosystème offre plusieurs dizaines d'intégrations avec des applications tierces – L'authentification multifacteur est ainsi appliquée pour gérer l'accès à des applications Cloud, des services Web, des VPN et des réseaux sensibles. Les utilisateurs AuthPoint peuvent s'authentifier une fois pour accéder à de multiples applications. Ils ont aussi la possibilité d'ajouter des authentificateurs tiers, comme pour Facebook ou Google Authenticator, sur l'application mobile conviviale.

> *« Les mots de passe non sécurisés sont exploités dans 81 % des cyberattaques dans le monde entier, et dans 61 % de toutes les attaques visant des entreprises de moins de 1 000 salariés. »*
>
> *Verizon, « 2017 Data Breach Investigations Report » (Rapport 2017 sur les atteintes à la sécurité des données)*

TROIS MOYENS DE S'AUTHENTIFIER AVEC L'APPLICATION

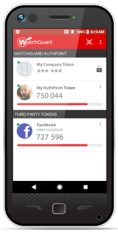


Authentification push

Authentification sécurisée permettant d'approuver d'un simple contact. Vous voyez immédiatement qui tente de s'authentifier et depuis quel endroit ; vous pouvez alors bloquer l'accès non autorisé à vos ressources.

Authentification par QR code

Utilisez l'appareil photo de votre smart-phone pour lire un QR code chiffré unique lorsque vous êtes en mode avion. Il suffit de rentrer le code obtenu afin de finaliser l'authentification.



Mot de passe à usage unique (OTP)

Récupérez votre mot de passe dynamique à usage unique (OTP) comme illustré et saisissez-le lors du login.

FONCTIONNALITÉS ET AVANTAGES

- Authentification en ligne (push) et hors ligne (code QR et OTP)
- Service Cloud avec un faible coût total de possession
- Vérification de l'ADN de l'appareil mobile afin d'établir une étroite correspondance d'identité
- Application mobile complète et légère disponible en 11 langues
- VPN, Cloud et protection du login du PC inclus
- Portail d'authentification unique (SSO)
- Protège facilement vos VPN, les applications Cloud et les services Web à l'aide des guides d'intégration

FICHE TECHNIQUE

Application mobile AuthPoint

FONCTIONS D'AUTHENTIFICATION

- Authentification push (en ligne)
- Authentification par code QR (hors ligne)
- Mot de passe à usage unique (hors ligne)

FONCTIONS DE SÉCURITÉ

- ADN de l'appareil mobile
- Activation en ligne avec génération de clé dynamique
- Accès à l'authentificateur par code PIN, empreinte digitale et reconnaissance faciale (iPhone X)
- Transfert libre et sécurisé de l'authentificateur sur un autre appareil
- Jailbreak et détection du rooting

FONCTIONS DE CONFORT

- Prise en charge de jetons multiples
- Prise en charge de jeton de médias sociaux tiers
- Nom et photo des jetons habituels

PLATEFORMES PRISES EN CHARGE

- Android v4.4 ou plus
- iOS v9.0 ou plus

LANGUES PRISES EN CHARGE

- Anglais, espagnol, portugais, allemand, néerlandais, français, italien, japonais, chinois (simplifié et traditionnel), coréen et thaï

NORMES

- Algorithme de mot de passe à usage unique (TOTP) OATH – RFC 6238
- Algorithmes défi-réponse (OCRA) OATH – RFC 6287
- OATH Dynamic Symmetric Key Provisioning Protocol (DSKPP) – RFC 6063

Services de AuthPoint

LES CAS D'UTILISATION PRIS EN CHARGE

- Authentification basée sur le Cloud avec le Web SSO
- Accès à distance et authentification VPN
- Logon Windows (en ligne/hors ligne)
- Logon MacOS (en ligne/hors ligne)
- Logon Linux

FONCTIONS DE GESTION

- Plateforme Cloud de WatchGuard
- Active Directory, et synchronisation et authentification LDAP de l'utilisateur
- Tableau de bord avec widgets de surveillance et de génération de rapports
- Politique d'accès par groupe d'utilisateurs
- Ressources d'authentification configurables
- Déploiement facile à l'aide de guides d'intégration
- Journaux & rapports

PASSERELLE AUTHPOINT

- Sécuriser la connexion sortante du réseau au Cloud de WatchGuard
- MS-AD et synchronisation LDAP
- Serveur RADIUS

AGENTS AUTHPOINT

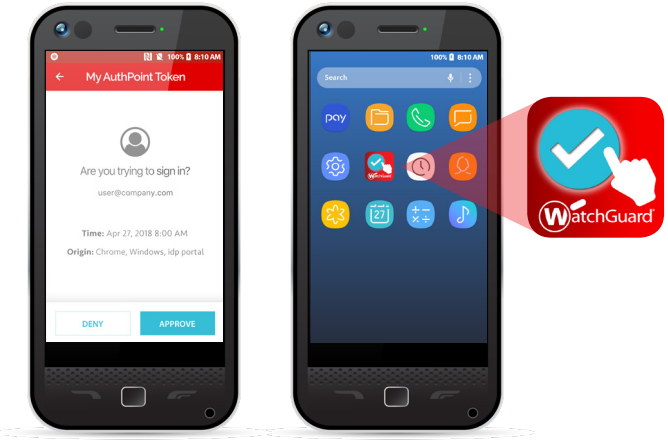
- Connexion Windows
- Connexion MacOS
- ADFS

NORMES

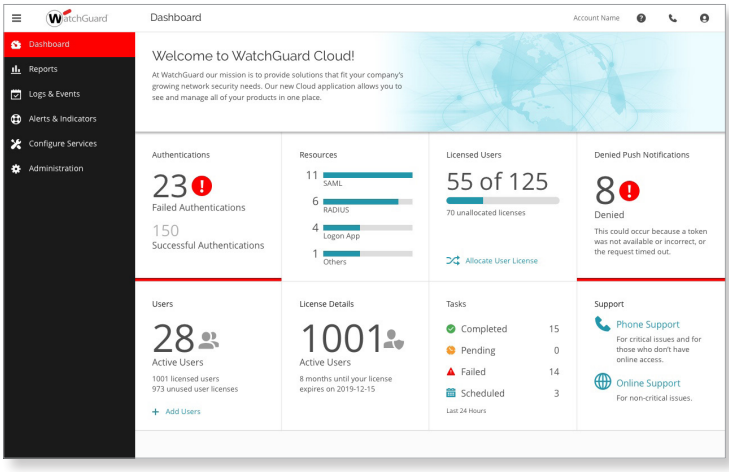
- RADIUS
- SAML 2.0 IdP

INTÉGRATIONS (VEUILLEZ CONSULTER LE SITE WEB DE WATCHGUARD POUR OBTENIR LA LISTE EXHAUSTIVE)

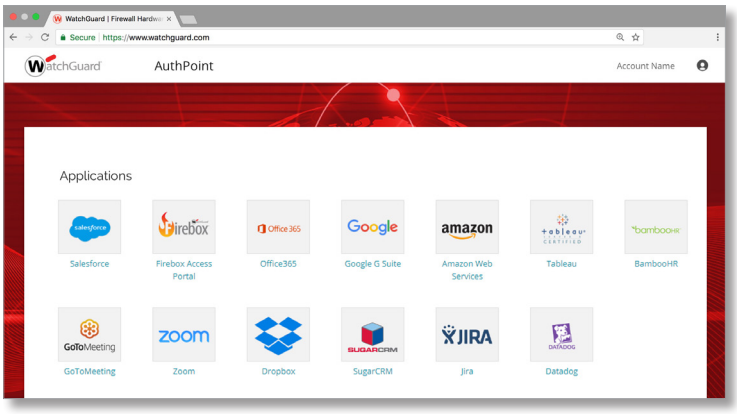
- Microsoft Office 365, G-Suite, WatchGuard Firebox, Dropbox, Go-to-Meeting, Open VPN



Application mobile AuthPoint



Gestion du Cloud de WatchGuard



Intégrations et SSO

LE PORTEFEUILLE DES SOLUTIONS DE SÉCURITÉ WATCHGUARD

Sécurité réseau

WiFi sécurisé

Authentification multifacteur

Pour plus d'informations, veuillez contacter votre intégrateur WatchGuard agréé ou rendez-vous sur **www.watchguard.fr**.

FRANCE 01 40 90 30 35 SERVICE COMMERCIAL INTERNATIONAL +1.206.613.0895

www.watchguard.fr