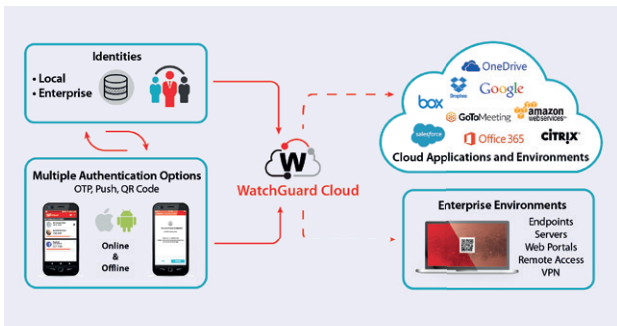


Authentification multi-facteurs – enfin abordable pour les PME

Une authentification efficace sur une plate-forme Cloud sécurisée: avec la solution ouverte et évolutive AuthPoint de WatchGuard, c'est une réalité. Avec une application mobile, la plate-forme offre une sécurité de connexion de haut niveau et conviviale pour les PME de toutes tailles.



AuthPoint de WatchGuard fournit une authentification multi-facteurs sécurisée (MFA) aux PME d'une manière simple et économique.

Un mot de passe seul ne répond plus aux exigences de sécurité d'aujourd'hui. Ce qu'il faut, c'est une authentification multi-facteurs sécurisée (MFA) - une procédure qui était auparavant trop compliquée et trop coûteuse pour les PME. Ce qui est mis en évidence dans une étude de CITE Research: 61% des entreprises interrogées qui comptent moins de 1000 employés ont déclaré que le MFA était réservé aux grandes entreprises.

Avec AuthPoint de WatchGuard, cela change radicalement. Avec sa solution basée sur le Cloud, le célèbre fabricant de produits de sécurité définit de nouvelles règles d'authentification sécurisée - que ce soit pour l'accès aux services web ou Cloud, la connexion au réseau de l'entreprise via VPN ou la connexion au PC.

Le cœur d'AuthPoint est une plate-forme Cloud en charge de la gestion des processus d'authentification, couplée à une application pour les appareils mobiles Android et iOS. L'utilisateur n'a pas besoin d'installer quoi que ce soit

d'autre que l'application mobile - aucun serveur d'authentification sur site n'est nécessaire et aucun logiciel client ne doit être installé sur les terminaux. La distribution complexe et l'utilisation peu conviviale des tokens matériels sont également éliminés: l'application prend entièrement en charge leurs fonctions sur la base de tokens logiciels.

Authentification flexible

L'application AuthPoint prend en charge trois méthodes d'authentification différentes. Avec l'authentification push, AuthPoint génère un message push à chaque fois que vous essayez de vous connecter. L'utilisateur peut vérifier si le login est légitime et approuver ou bloquer l'accès du bout du doigt. L'authentification basée sur un QR Code est différente: Ici, l'utilisateur lit un QR Code avec l'application, qui est affiché sur l'écran du PC. L'application émet alors un code de réponse avec lequel l'utilisateur peut activer l'accès. Cette méthode peut également être utilisée hors ligne, par exemple

pour se connecter à un ordinateur portable s'il n'y a pas de connexion de données. La troisième méthode est connue de divers services en ligne: L'accès est accordé avec un mot de passe unique limité dans le temps (OTP) qui s'affiche dans l'application pendant le processus de connexion.

Particulièrement sûr et bien intégré

La technologie AuthPoint va bien au-delà de la simple authentification: AuthPoint capture diverses caractéristiques de l'appareil mobile utilisé et exploite cet «ADN mobile» comme facteur de sécurité supplémentaire. Ceci garantit que seuls les utilisateurs réellement autorisés ont accès à leurs appareils enregistrés.

AuthPoint utilise les normes SAML 2.0 IdP et RADIUS pour se connecter aux services Cloud et autres applications tierces. De nombreuses intégrations fonctionnent en standard, par exemple avec Office 365, Salesforce, AWS ou Dropbox. Les services d'annuaire tels que l'AD sont intégrés via un logiciel qui fait office de passerelle et qui est gratuit. AuthPoint n'est pas limité aux entreprises disposant d'une infrastructure WatchGuard: La solution est ouverte et peut être utilisée avec tous les firewalls.

Licence attractive à prix fixe

Le modèle de licence AuthPoint répond aux besoins des utilisateurs et des revendeurs. AuthPoint est licencié par utilisateur et est disponible à partir de cinq utilisateurs à des prix attractifs. Il n'y a pas de coûts supplémentaires

pour le service Cloud. La solution est entièrement multi-clients et convient donc parfaitement aux intégrateurs et aux fournisseurs de services de sécurité gérés (MSSP). Cela permet aux partenaires MSSP d'obtenir des licences d'utilisation sous forme de pool et de les attribuer librement à leurs clients, ils n'ont pas à se soucier de la mise en place et de l'exploitation d'une plate-forme de gestion - tout cela est couvert par la plate-forme Cloud.

WatchGuard AuthPoint: les points forts

- Authentification push, QR Code ou mot de passe unique
- Basé sur le Cloud et accessible
- Déploiement facile
- Sécurité supplémentaire grâce à «l'ADN mobile»
- Sécurise l'accès aux services Cloud, VPN et login PC (Windows, macOS, Linux)
- Portail SSO pour les applications web
- A partir de seulement cinq utilisateurs
- Entièrement multi-clients pour les MSSP et les intégrateurs
- Convient à tous les environnements quel que soit le firewall en place

BOLL
IT Security Distribution

BOLL Engineering SA

En Budron H15
1052 Le Mont-sur-Lausanne
T: 021 533 01 60
vente@boll.ch | www.boll.ch