DATASHEET

AUTHPOINT

Autenticazione a più fattori (MFA): efficace e semplice da usare

LE PASSWORD NON BASTANO

Ogni giorno, i criminali informatici usano credenziali rubate per accedere ai sistemi e infettarli o per rubare dati. Quello che serve per invertire questa tendenza è un meccanismo di autenticazione con un ulteriore livello di accertamento dell'identità, oltre alla semplice combinazione di nome utente e password, adottato da tutte le aziende, a prescindere dalle dimensioni.

L'MFA TIENE FUORI INTRUSI E IMPOSTORI

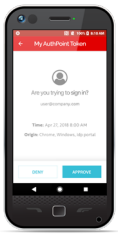
WatchGuard AuthPoint™ è la soluzione giusta al momento giusto per affrontare questa lacuna nella sicurezza con l'autenticazione a più fattori su una piattaforma cloud facile da usare. Con una semplice notifica push, l'app mobile AuthPoint rende visibile ogni tentativo di accesso, permettendo all'utente di accettarlo o bloccarlo direttamente dallo smartphone. L'approccio unico di WatchGuard aggiunge il DNA del cellulare come fattore di identificazione, per assicurare che solo le persone autorizzate accedano a reti sensibili e applicazioni cloud.

GESTIONE CLOUD INTUITIVA

A causa delle complesse integrazioni e della dispendiosa gestione interna, l'MFA era in passato una soluzione fuori portata per alcune aziende, che non potevano permettersi una tale implementazione senza personale IT a sufficienza e senza un investimento iniziale considerevole. Al contrario, la soluzione WatchGuard AuthPoint è un servizio cloud che non necessita di hardware costoso e può essere gestita ovunque con l'interfaccia intuitiva WatchGuard Cloud. Inoltre, il nostro ecosistema offre decine di integrazioni con applicazioni di terze parti, garantendo un'applicazione estesa della protezione MFA per l'accesso ad applicazioni cloud sensibili, servizi web, VPN e reti. Gli utenti di AuthPoint possono accedere una sola volta per utilizzare più applicazioni e possono aggiungere strumenti di autenticazione di terze parti, ad esempio per Facebook o Google Authenticator, all'intuitiva app mobile.

> *"L'81% degli attacchi informatici nel mondo sfrutta le cattive abitudini degli utenti rispetto alla sicurezza delle password, mentre il 61% di tutti gli attacchi è rivolto ad aziende con meno di 1000 dipendenti."*
>
> *Report di indagine sulle violazioni di dati, Verizon 2017*

TRE MODI PER AUTENTICARSI CON L'APP

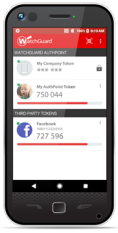


Autenticazione push

Autenticazione sicura con approvazione one-touch. Visualizza chi sta tentando di autenticarsi e dove, e blocca gli accessi non autorizzati alle tue risorse.

Autenticazione con codice QR

Usa la fotocamera per leggere un codice QR univoco e crittografato con una domanda visualizzabile solo nell'app. Per completare l'autenticazione, occorre digitare la risposta.



Password univoca a tempo (OTP)

Recupera la password dinamica, univoca e a tempo quando viene mostrata e inseriscila durante l'accesso.

CARATTERISTICHE E VANTAGGI

- Autenticazione online (push) e offline (codice QR e OTP)
- Servizio cloud a basso TCO
- Controllo del DNA del dispositivo mobile per la verifica efficace dell'identità
- App mobile snella e ricca di funzioni in 11 lingue
- Protezione dell'accesso a VPN, cloud e PC tutto incluso
- Portale Web Single Sign-On (SSO)
- Protezione facile di VPN, app cloud e servizi Web con le guide per l'integrazione

DATASHEET

App mobile AuthPoint

FUNZIONI DI AUTENTICAZIONE

- Autenticazione push (online)
- Autenticazione con codice QR (offline)
- Password univoca a tempo (OTP) (offline)

FUNZIONI DI SICUREZZA

- DNA del dispositivo mobile
- Attivazione online con generazione di chiave dinamica
- Accesso allo strumento di autenticazione con PIN, impronta digitale e riconoscimento facciale (iPhone X)
- Migrazione self-service e sicura dello strumento di autenticazione su un altro dispositivo
- Jailbreak e rilevamento root

FUNZIONI DI PRATICITÀ

- Supporto multi-token
- Supporto per token di social media di terze parti
- Nome e immagine token personalizzato

PIATTAFORME SUPPORTATE

- Android v4.4 o superiore
- iOS v9.0 o superiore

LINGUE SUPPORTATE

- Inglese, spagnolo, portoghese, tedesco, olandese, francese, italiano, giapponese, cinese (semplificato e tradizionale), coreano, tailandese

STANDARD

- OATH Time-Based One-Time Password Algorithm (TOTP) – RFC 6238
- OATH Challenge-Response Algorithms (OCRA) – RFC 6287
- OATH Dynamic Symmetric Key Provisioning Protocol (DSKPP) – RFC 6063

Servizio AuthPoint

CASI D'USO SUPPORTATI

- Autenticazione basata su cloud con Web SSO
- Accesso remoto e autenticazione VPN
- Protezione dell'accesso Windows (online/offline)
- Protezione dell'accesso MacOS (online/offline)
- Protezione dell'accesso Linux

FUNZIONI DI GESTIONE

- WatchGuard Cloud Platform
- Autenticazione e sincronizzazione utenti Active Directory e LDAP
- Dashboard con widget di monitoraggio e reporting
- Criteri di accesso per gruppi di utenti
- Risorse di autenticazione configurabili
- Implementazione facile con le guide per l'integrazione
- Registri e report

GATEWAY AUTHPOINT

- Connessione in uscita sicura dalla rete a WatchGuard Cloud
- Sincronizzazione MS-AD e LDAP
- Server RADIUS

AGENTI AUTHPOINT

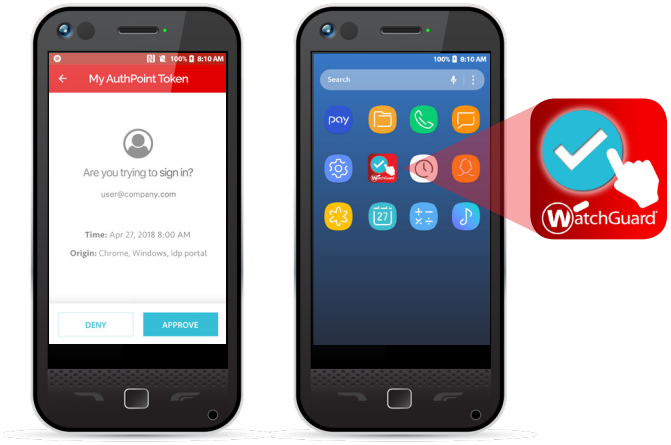
- Accesso Windows
- Accesso MacOS
- ADFS

STANDARD

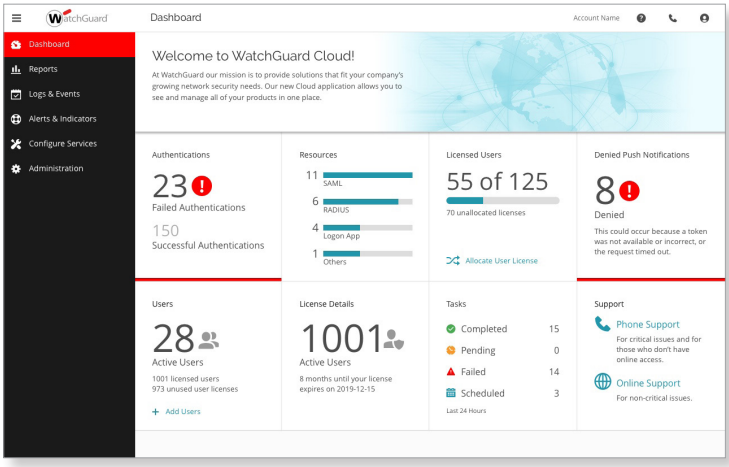
- RADIUS
- SAML 2.0 IdP

INTEGRAZIONI (CONSULTA IL SITO WATCHGUARD PER L'ELENCO COMPLETO)

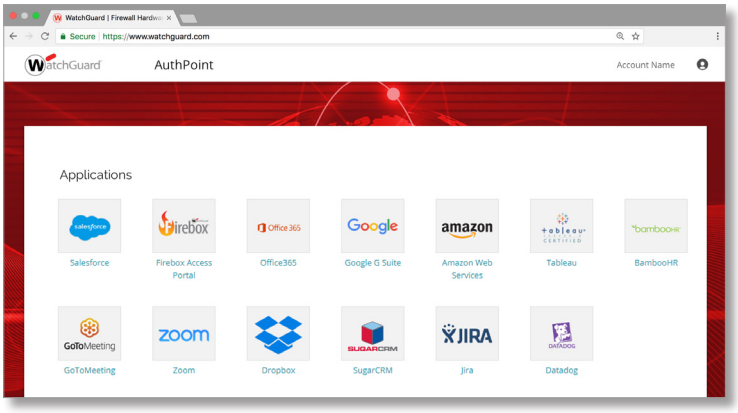
- Microsoft Office 365, G-Suite, WatchGuard Firebox, Dropbox, Go-to-Meeting, Open VPN



App mobile AuthPoint



WatchGuard Cloud Management



Integrazioni e SSO

LA GAMMA DI PRODOTTI PER LA SICUREZZA WATCHGUARD

Sicurezza di rete

Wi-Fi protetto

Autenticazione a più fattori

Per saperne di più, contatta il tuo rivenditore WatchGuard autorizzato o visita il sito **www.watchguard.it**

Numero Verde Italia: 800-911.938 VENDITE INTERNAZIONALI: +1.206.613.0895 www.watchguard.it