AuthPoint

MFA potente e facile

L'attuale panorama della sicurezza mostra che l'uso di credenziali rubate per violare risorse di rete è la tattica numero 1 impiegata dagli hacker. Infatti, l'80% delle violazioni dei dati sfrutta principalmente password rubate o deboli.* L'autenticazione a più fattori è l'unica e più importante tutela possibile per la tua azienda.

La soluzione WatchGuard di autenticazione a più fattori (MFA) non solo protegge l'identità dell'utente e riduce le probabilità di intrusioni nella rete e di violazione dei dati causate da credenziali deboli o rubate, ma viene fornita interamente via cloud per la massima semplicità di configurazione e gestione. L'esclusiva tecnologia del DNA del dispositivo mobile di AuthPoint va ben oltre la tradizionale autenticazione a 2 fattori (2FA) perché integra metodi innovativi per identificare e proteggere gli utenti. Grazie a un ampio ecosistema di oltre 130 integrazioni di terze parti, l'efficacia della protezione può essere distribuita in modo coerente sull'intera rete, incluse le VPN e le applicazioni cloud, ovunque sia necessaria. Anche gli utenti non tecnici trovano l'app mobile AuthPoint intuitiva e semplice da usare. Inoltre, WatchGuard AuthPoint è la soluzione giusta al momento giusto per trasformare l'MFA in una realtà per le aziende che necessitano disperatamente di bloccare gli attacchi.

Autenticazione basata sul rischio per l'adozione della strategia Zero Trust

L'adozione della strategia Zero Trust presuppone la protezione dell'identità e, poiché l'autenticazione basata sul rischio è un elemento centrale dell'MFA, AuthPoint diventa un requisito fondamentale per adottare l'approccio "Fidarsi mai, verificare sempre". Se non ha predisposto criteri di rischio, l'azienda è tenuta ad abilitare il metodo di autenticazione più rigido in ogni momento e per tutti gli utenti, causando potenziali rallentamenti nell'adozione in alcuni segmenti. Con AuthPoint puoi accedere senza costi aggiuntivi alle funzioni di rischio, incluse quelle relative alle posizioni della rete, alla pianificazione temporale e alla localizzazione geografica, e all'esclusivo DNA del dispositivo mobile, che previene la clonazione dei token per dispositivi mobili.

Un servizio basato su cloud a basso TCO

La protezione tramite MFA è particolarmente vantaggiosa per quelle aziende con personale IT limitato e poca competenza tecnica, proprio per la sua facilità di implementazione e gestione via cloud. AuthPoint viene eseguito sulla piattaforma WatchGuard Cloud ed è disponibile ovunque. Non occorre installare software, pianificare upgrade né gestire patch. Inoltre, la piattaforma supporta facilmente la vista di un singolo account globale o diversi account indipendenti, in modo che le aziende distribuite e i fornitori di servizi gestiti possano visualizzare solo i dati pertinenti a un determinato ruolo utente.

Ampia copertura con SSO sul web

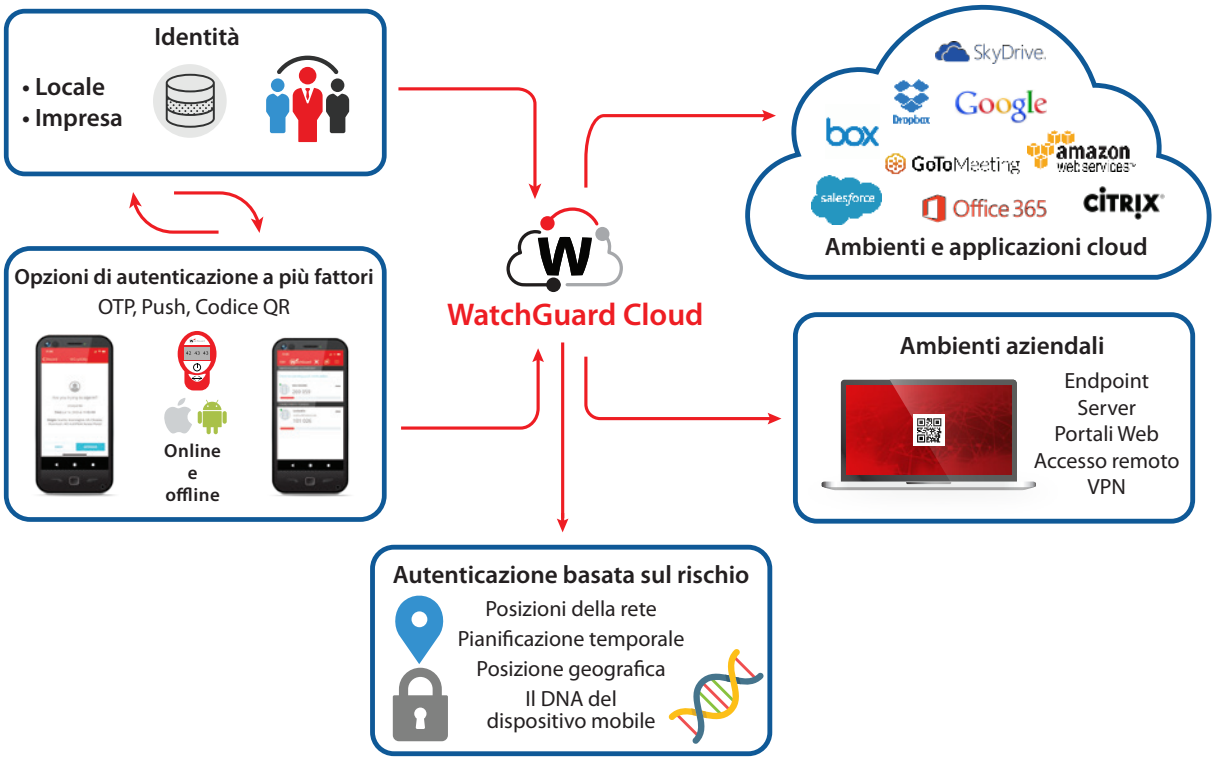
Di' addio a tutte quelle complesse password da ricordare a memoria. Il single sign-on (SSO) sicuro di AuthPoint consente agli utenti di accedere facilmente a più applicazioni cloud, VPN e reti con un solo set di credenziali. Questo risolve il problema dell'impegno eccessivo richiesto dalla gestione delle password e riduce il rischio di vulnerabilità di sicurezza dovute a password deboli, oltre che i costi associati alla reimpostazione delle password. AuthPoint supporta il protocollo standard SAML, che consente agli utenti di accedere una sola volta per avere a disposizione una gamma completa di applicazioni e servizi. La nostra funzionalità di accesso sicuro offre anche l'autenticazione online e offline a computer Windows e Mac tramite l'app o il token hardware AuthPoint.

App mobile intuitiva e ottimizzata

Installa e attiva in pochi secondi l'app AuthPoint di WatchGuard per eseguire l'autenticazione direttamente dal tuo smartphone. L'app non solo abilita l'autenticazione push rapida, ma offre anche la funzione di autenticazione pull per una migliore usabilità e sicurezza. Include inoltre l'autenticazione offline con codici QR tramite la fotocamera del telefono. L'app è disponibile in 13 lingue e il download è gratuito da AppStore e Google Play.

**Report di indagine sulle violazioni di dati, Verizon 2020*

Tenere gli impostori fuori dalle reti, dalle VPN, dalle risorse cloud e non solo!



WatchGuard Cloud Platform

- Gestione basata su cloud al 100% in tre aree geografiche
- Gestione efficace delle policy basata sul rischio
- Registri e report
- Controllo dell'accesso in base ai ruoli
- Interfaccia utente intuitiva e accattivante

App mobile AuthPoint

- Tre metodi di autenticazione in uno:
  1. Messaggi push con distribuzione garantita
  2. Password monouso
  3. Codici QR di autenticazione/risposta
- Autenticatore mobile: senza hardware da portare in giro
- 13 lingue
- Supporto multi-token
- iOS e Android: download gratuito
- Protezione con PIN/biometrica (su alcuni dispositivi)
- DNA del dispositivo mobile, fattore di autenticazione aggiuntivo
- Migrazione del token mobile self-service su nuovi dispositivi
- Supporto di token di terze parti per proteggere gli account personali (Gmail, social media, ecc.)

Gateway AuthPoint

- Gateway rete aziendale
- Sincronizzazione e autenticazione utenti AD e LDAP
- Proxy RADIUS

Agenti AuthPoint

- Integrazione con applicazioni di terze parti senza supporto MFA nativo
- Protezione dell'accesso online, offline e RDP per i computer Windows e macOS
- Agente per Desktop Web remoto e ADFS

Ecosistema AuthPoint

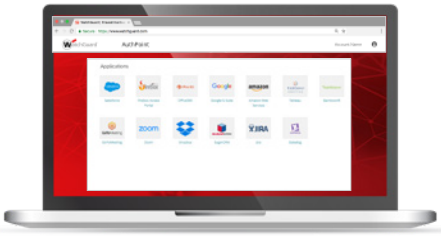
- Aggiunta dell'MFA a risorse cloud, applicazioni, database e risorse web
- Supporto per standard SAML e RADIUS
- Oltre 130 guide alle integrazioni di terze parti, incluse soluzioni CRM e di videoconferenza
- Integrazione diretta di Firebox con AuthPoint per una configurazione rapida della VPN
- Token hardware per AuthPoint senza esposizione dei seed del token e supporto per token hardware di terze parti (OATH TOTP)

Casi d'uso consigliati

Accesso da VPN/remoto

Funziona come l'inserimento di nome utente e password MA è più sicuro e offre la conferma con un clic. Si integra con qualsiasi firewall, in particolare con le appliance Firebox pronte all'uso.

1. Richiedi la connessione con nome utente e password
2. Conferma la connessione VPN con richiesta tramite app AuthPoint



Applicazioni cloud - Web SSO

1. Accedi all'Identity Portal (IdP)
2. Autenticati tramite OTP, push o codice QR
3. Accedi a tutte le app che ti sono state assegnate con una sola password, senza dover eseguire nuovamente l'autenticazione

Accesso al PC o connessione RDP

1. Effettua l'accesso a Windows/Mac con nome utente + password
2. Scegli il tuo metodo di autenticazione preferito (notifica push, codice QR o OTP)
3. Approva l'accesso sul tuo telefono. Accesso effettuato!

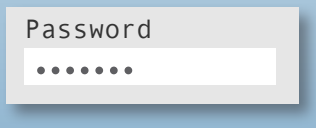
Accesso a PC - Autenticazione offline

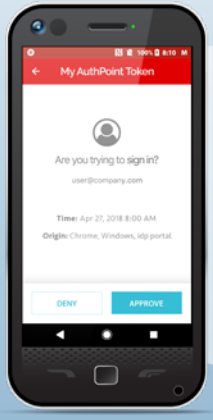
1. Effettua l'accesso a Windows/Mac con nome utente + password
2. Esegui la scansione del codice QR (o OTP) tramite l'app AuthPoint
3. In questo esempio, è necessario scrivere la risposta 717960

Cos'è l'autenticazione a più fattori (MFA)?

Uso di 2 o più fattori di autenticazione:

- **Elementi noti** (password, PIN)
- **Elementi disponibili** (token, cellulare)
- **Elementi personali** (impronta digitale, volto)





Fattori AuthPoint:

1. **Password**
2. **Approvazione su autenticatore mobile**
3. **DNA del dispositivo mobile**
4. **Impronta digitale per l'accesso** (con alcuni modelli di cellulari)

AuthPoint mantiene tutte le promesse dell'MFA limitando i rischi aziendali associati all'uso di password deboli, senza compromettere la semplicità d'uso per i dipendenti e il personale IT.

Tutto in un solo servizio cloud: senza hardware da installare né software da aggiornare, l'MFA è considerata la protezione principale ed è offerta da WatchGuard con estrema semplicità.

Tom Ruffolo
CEO, eSecurity Solutions

Affidati all'autenticazione a più fattori per ridurre i rischi

Le password deboli sono una responsabilità seria per la tua azienda. **L'utente medio dispone di almeno 100 account online** e molti di questi hanno i propri requisiti di password. Gli sforzi legati alle password sono un problema concreto che sta mettendo a rischio la tua azienda. A un criminale informatico basta una password debole o compromessa per accedere a tutti i tuoi dati e account.

Sei davvero sicuro che tutti i tuoi dipendenti si attengano alle best practice per le password?

- Ogni giorno vengono rubate circa 250.000 password[1]
- Solo 1 utente su 5 utilizza una password univoca per tutti gli account[2]
- Il 3% sceglie 1234563 come password[3]

> "Nel 2021 le aziende che ampliano rapidamente l'accesso remoto senza implementare l'MFA subiranno un numero di incidenti con furto di account cinque volte maggiore rispetto a quelle che la utilizzano."
>
> Gartner, Inc., Enhance Remote Access Security With Multifactor Authentication and Access Management
>
> Ant Allan, Rob Smith, Michael Kelley, 6 maggio 2020

Il costo di una violazione può essere tale da far fallire la tua azienda. Il costo medio di una violazione dei dati è pari a 148 dollari per record di dati sensibili... ovvero 1,38 milioni di dollari se si considera la violazione media di 9.350 record. Inoltre, questa stima non include i costi indiretti come i danni alla reputazione dell'azienda, il crollo nella fiducia dei clienti e le ore di lavoro perse.

La buona notizia è che puoi ridurre la tua esposizione ai rischi informatici con facilità e ottenere un ritorno elevato sul tuo investimento per la sicurezza. Fornire a ogni dipendente una protezione mensile tramite autenticazione a più fattori costa meno che una colazione al bar. Scegli AuthPoint ed elimina il rischio numero 1 per la tua azienda.

Vuoi fare una prova? Visita watchguard.com/it/wgrd-products/test-drive-authpoint o contatta uno dei nostri specialisti dedicati per iniziare una prova gratuita di 30 giorni.

1 https://breachalarm.com/
2 https://www.statista.com/statistics/763091/us-use-of-same-online- passwords/
3 https://www.techspot.com/news/77864-worst-passwords-2018-revealed-123456-retains- top-spot.html

WATCHGUARD UNIFIED SECURITY PLATFORM™

Sicurezza di rete

Le soluzioni per la sicurezza di rete di WatchGuard sono progettate da zero per offrire facilità di implementazione, uso e gestione, oltre a fornire la massima sicurezza possibile. Il nostro esclusivo approccio alla sicurezza di rete è incentrato sull'offerta di una sicurezza di livello enterprise e all'avanguardia a qualunque tipo di organizzazione, a prescindere dalle dimensioni o dalle competenze tecniche.

Autenticazione a più fattori

WatchGuard AuthPoint® è la soluzione giusta per gestire le lacune della sicurezza basata su password con l'autenticazione a più fattori tramite una piattaforma cloud facile da usare. L'approccio esclusivo di WatchGuard aggiunge il "DNA del cellulare" come fattore di identificazione, per garantire che solo le persone autorizzate possano accedere a reti sensibili e applicazioni cloud.

Secure Wi-Fi Cloud

La soluzione Secure Wi-Fi di WatchGuard, rivoluzionaria per il mercato di oggi, è progettata per fornire sicurezza e protezione per gli ambienti Wi-Fi, eliminando al contempo le lungaggini amministrative e riducendo notevolmente i costi. Grazie all'ampia gamma di strumenti di coinvolgimento e alla visibilità dell'analisi aziendale, la soluzione offre il vantaggio competitivo di cui le aziende hanno bisogno per avere successo.

Sicurezza degli endpoint

WatchGuard Endpoint Security è un portafoglio di avanzate soluzioni native per il cloud ideato per la sicurezza degli endpoint e che protegge le aziende di qualsiasi tipo di attacco informatico attuale e futuro. WatchGuard EPDR, la sua soluzione principale basata sull'intelligenza artificiale, migliora immediatamente la protezione delle organizzazioni. Combina funzionalità di protezione degli endpoint (EPP) e di rilevamento e risposta degli endpoint (EDR) con un'applicazione Zero Trust e servizi di ricerca delle minacce.

Scopri di più

Per maggiori dettagli, contatta il tuo rivenditore WatchGuard autorizzato o visita **www.watchguard.com**.

Informazioni su WatchGuard

WatchGuard® Technologies, Inc. è un leader globale nella fornitura di servizi relativi a sicurezza di rete, sicurezza degli endpoint, Wi-Fi protetto, autenticazione a più fattori e intelligence di rete. I pluripremiati prodotti e servizi della nostra azienda hanno ottenuto la fiducia di oltre 18.000 rivenditori e fornitori di servizi che provvedono alla sicurezza di più di 250.000 clienti. WatchGuard persegue la missione di rendere la sicurezza accessibile ad aziende di tutti i tipi e dimensioni attraverso la semplicità, diventando in tal la soluzione ideale per le aziende del midmarket e distribuite. La sede centrale di WatchGuard si trova a Seattle (Washington, Stati Uniti); l'azienda dispone di uffici dislocati in Nord America, Europa, Asia e America Latina. Per saperne di più, visita **WatchGuard.com/it**.