
Sei disposto a basare tutto il tuo business sull'efficacia delle password dei tuoi dipendenti?
WatchGuard
Dimostra chi sei, Blocca gli intrusi
Be Authentic
with AuthPoint MFA
WatchGuard Technologies

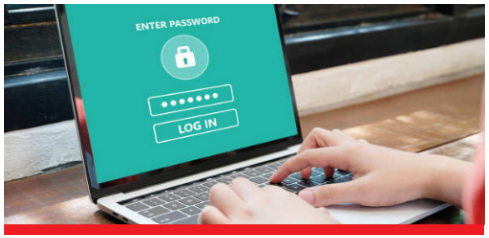
Sommario

Tra te e un hacker c'è solo una password debole a difenderti...
.... E anche le password più "complicate" che riuscirai a inventarti possono essere violate.

Ormai le password non sono più sufficienti per proteggere le tue risorse, gli account e le informazioni.
Ecco spiegati alcuni dei motivi principali:

l'80% degli utenti **UTILIZZA la stessa password per più di un account**[2]

Il 6% degli utenti Internet utilizza la **STESSA password per tutti i suoi account online**[2]



Circa il 46% dei dipendenti utilizza **password personali** per gli account aziendali[3]

Le persone scelgono password deboli

La lista delle 25 password più deboli del 2017[1]

1 123456
2. Password
3 12345678
4. qwerty
5 12345
6 123456789
7. letmein
8. 1234567
9. football
10. iloveyou
11. admin
12. welcome
13. monkey
14. login
15. abc123
16. starwars
17 123123
18. dragon
19. passw0rd
20. maste
21. hello
22. freedom
23. whatever
24. qazwsx
25. trustno1

1. https://www.teamsid.com/worst-passwords-2017-full-list/2. https://www.csoonline.com/article/3244137/password-security/password-managers-grow-up-target-business-users.html3. http://www.statista.com/statistics/763091/us-use-of-same-online-passwords4. https://www.fastcompany.com/40469838/dashlane-reused-password-hygiene

Pensi che le tue password siano abbastanza complesse? Questo non fermerà gli hacker.

Gli hacker comprano le credenziali nel dark web con la stessa facilità con cui tu fai un acquisto su Amazon.

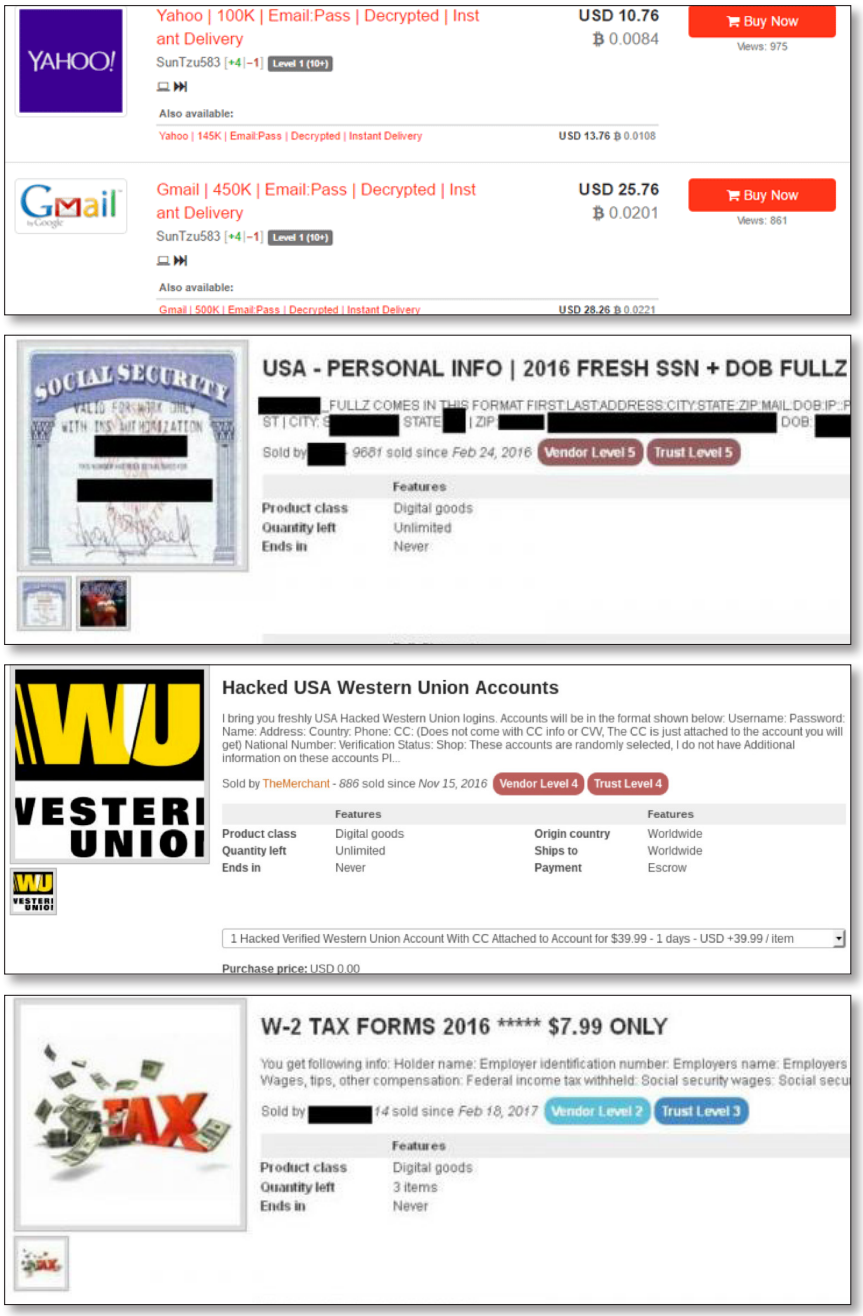
Il costo medio di una password nel dark web[5]: **$160,15**
Il costo medio di un'identità utente (le credenziali usate per tutti gli account) per un hacker: **$1.200.**

Se il tuo IP, le informazioni sui clienti e sui dipendenti o qualsiasi altra risorsa nella tua rete valgono più di $1.200, allora non è difficile comprendere perché sia economicamente vantaggioso per un hacker acquistare la chiave di accesso (cioè le tue credenziali) per quelle informazioni.

Pensi che una cosa del genere non possa succedere alle tue credenziali?
O alle credenziali del tuo collega?

Ci sono miliardi di credenziali in vendita nel dark web, e molte di queste sono di utenti amministratore. Solo alla fine del 2017 è stato scoperto un singolo file che conteneva 1,4 miliardi di password non crittografate.[6] Le stime parlano chiaro, le tue informazioni di login potrebbero essere comprate in pochi secondi.

Nel dark web si comprano password con la stessa facilità con cui faresti un acquisto su Amazon. A destra puoi vedere alcuni esempi di pagine del dark web che vendono credenziali.



5. https://www.nbcnews.com/tech/security/your-identity-sale-dark-web-less-1-200-n855366 6. https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14
7. http://www.cyberinject.com/gmail-yahoo-passwords-on-dark-web/ 8. https://www.theteneogroup.com/2017/06/08/understanding-deep-web-dark-web-guard-network/ 9. https://zerohedge.whotrades.com/blog/43790836676 10. https://zerohedge.whotrades.com/blog/43790836676

Se un hacker dovesse decidere di violare la tua password invece di comprarla, **anche in quel caso non ci metterebbe molto tempo.**

In effetti per violare la maggior parte delle password ad un hacker serve meno del tempo che impiegherai a leggere questa

Tipologia	Password	Tempo (HSIMP) How Secure Is My Password?	Tempo (PA) Analizzatore Passfault	Livello di sicurezza
parola comune con 8 caratteri	required	52 secondi	<1 giorno	Inutile
8 caratteri casuali	qkcrmztd	52 secondi	<1 giorno	Inutile
8 caratteri casuali con numeri	kqwbv832	11 minuti	<1 giorno	Inutile
8 caratteri casuali con maiuscole e minuscole, simboli e numeri	J5bZ>9p!	20 giorni	<1 giorno	A rischio

Tipologia	Password	Tempo (HSIMP)	Tempo (PA)	Livello di sicurezza
Password con 2 parole comuni	orange tea	98 giorni	<1 giorno	A rischio
Password con 3 parole comuni	this is cool	546 anni	<1 giorno	A rischio
Password con 5 parole non comuni	du-bi-du-bi-doo	12 milioni di anni	<1 giorno	A rischio

Le password vengono violate con facilità e offrono una sola linea di difesa. Se un hacker riesce a rubare anche solo una password dei tuoi dipendenti, di solito è poi in grado di accedere all'intera rete. Una volta entrato, sarà libero di fare ciò che vuole. Normalmente un hacker diffonde malware, ruba, modifica o cancella le informazioni importanti.

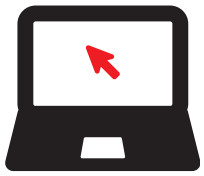
11. https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity/

Di seguito troverai una panoramica semplificata dei passaggi con cui un hacker ruba una password.

La ricostruzione è basata sul libro “Hacking the Hacker” dell’esperto di sicurezza informatica e hacker etico Roger Grimes:

Raccoglie le informazioni
(Fingerprinting e/o social engineering)

Accede al tuo account
usando verosimilmente delle credenziali perse o rubate.



Si muove per il sistema
fino alle vulnerabilità di identità

Ottiene l’accesso admin
(Aumento dei privilegi)

Concretizza l’attacco

Grimes afferma:

“Se l’hacker ha fatto bene il suo lavoro nella fase di fingerprinting, tutto il resto viene da sé.”

Vuole dire che a quel punto per gli hacker è un gioco da ragazzi accedere ai tuoi account. Alcuni coprono anche le loro tracce o si creano un punto di accesso per poter ritornare in futuro, anche se non succede sempre.

Rubare le tue password è un gioco da ragazzi

Il furto delle password è diventato incredibilmente facile (e redditizio) per gli hacker. Gli strumenti e le tecnologie per l'individuazione delle password sono diventati più sofisticati e automatizzati, tanto che spesso non richiedono neanche il "password-guessing" manuale. Anche nel caso fosse ancora richiesto, gli algoritmi avanzati, la social engineering (ad es. attacchi di phishing e trojan horse), i keylogger e gli altri metodi consentono loro di ipotizzare e testare in maniera efficace le password più plausibili e spesso permettono loro di portare a termine il loro intento criminale.

Le tecniche di hacking più frequenti includono:

Attacco a dizionario

Gli hacker cercano di individuare la password inserendo una lista di parole comuni prese da un "dizionario" di password. I dizionari di password più avanzati comprendono una lista delle password più comuni. Questa tecnica è relativamente semplice ed è particolarmente efficace quando si tratta di riconoscere le password meno complicate. Se hai scelto parole realmente esistenti come password, allora sappi che sei a rischio.

Attacco di forza bruta

Anche se non è un metodo efficiente come l'attacco a dizionario, l'attacco di forza bruta risulta più efficace nell'indovinare una password. Questa tecnica prevede che un hacker, attraverso l'uso di appositi strumenti, inserisca ripetutamente ogni combinazione possibile di lettere, numeri e simboli finché non riesce a violare la password. Un approccio simile è l'attacco di forza bruta inverso, in cui un hacker prova una sola password per più nomi utente.

Attacco tabella arcobaleno

Questa tecnica sfrutta una risorsa chiamata tabella arcobaleno per violare gli hash di password (in sostanza le password criptate memorizzate nei database di sistema) ed è molto più efficace ed efficiente degli attacchi di forza bruta o a dizionario.

Attacco con riempimento di credenziali

Dato che molte persone utilizzano le stesse password o una leggera variante per tutti gli account, gli hacker hanno trovato il modo di inserire in maniera automatica elenchi di database con combinazioni nome utente/password violate per forzare la sezione login dei siti web. Secondo Shape Security il 90% dei tentativi di login negli e-commerce sono dovuti a questo genere di attacco. Questa tecnica ha successo nel 3% dei casi.

Social Engineering

Questo tipo di attacco può assumere forme diverse, tutte accomunate dall'idea di ingannare e manipolare una persona per spingerla a rivelare delle informazioni o ad agire in un certo modo. Le tecniche più comuni di social engineering usate per il furto di password includono gli attacchi di phishing e trojan. Una tecnica meno usata è il shoulder surfing, in cui l'hacker scopre una password semplicemente stando alle spalle di chi la sta digitando.

Con le tecnologie e gli strumenti di hacking sempre più sofisticati, per i criminali impossessarsi della password è diventato il passaggio più semplice di tutta la trafila. In verità è così facile che molto spesso non richiede nemmeno di dover perdere tempo a indovinare la password. La cosa che fa più paura è che non importa quanto sia inattaccabile la tua password, ne basta una sola poco sicura, magari di un tuo collega, per mettere a rischio l'intero sistema dell'azienda.

La protezione tramite autenticazione:
Cambiare l'atteggiamento dei dipendenti verso le password è un tattica che non funziona.

Un metodo per ridurre il rischio di furto di password è educare i propri dipendenti a creare password più sicure e invitarli a cambiarle di frequente. Cercare di modificare il comportamento di tutti i dipendenti richiede un grande dispendio di tempo ed energie, e in fin dei conti non apporta grandi benefici in termini di sicurezza.

Storicamente questo approccio si è dimostrato fallimentare
Lo testimoniamo i database di milioni di aziende che sono stati violati e le decine di milioni di password trafugate che si possono trovare online (considera che si possono acquistare molte di queste credenziali nel dark web).

Si crea un'esperienza utente eccessivamente complessa
Usare per ogni account una password casuale, unica e con 16 caratteri è complicato. Le persone optano per password semplici perché altrimenti sono difficili da ricordare. Molte persone creano password leggermente più complicate, ma si danno la zappa sui piedi riutilizzando la stessa password (o delle varianti simili a quella) per tutti gli account.

Se le password non sono sufficienti, qual è il prossimo passo?

L'autenticazione a più fattori (MFA) è un metodo di verifica che aggiunge un livello di sicurezza agli accessi, andando oltre la semplice combinazione nome utente/password. Ti garantisce che gli hacker non avranno accesso al tuo sistema anche se le password di uno dei tuoi dipendenti fossero compromesse.

WatchGuard offre una soluzione di autenticazione a più fattori (MFA) facile da usare che aiuta le aziende a mantenere al sicuro le loro risorse, le informazioni e le identità degli utenti. AuthPoint.

AuthPoint è facile da implementare e da gestire. Può essere tuo pagando al mese (per utente) meno del costo di un caffè. È anche più sicuro dell'autenticazione a due fattori (2FA) e delle soluzioni basate su SMS; più economico (TCO ridotto) delle opzioni non basate sul cloud; e più immediato per l'utente finale delle soluzioni che richiedono un token.

Nota bene:
Non tutti gli MFA sono uguali

L'autenticazione a più fattori basata su SMS non è più un metodo sicuro. Gli utenti che si affidano all'autenticazione basata su SMS dovrebbero optare per altre soluzioni quanto prima. Nella sua guida 2016 "Digital Identity Guidelines", il National Institute of Standard Technology (NIST) invitava gli utenti a lasciar perdere l'autenticazione basata su SMS:

"Dato il rischio che gli SMS vengano intercettati o reindirizzati, gli implementatori di nuovi sistemi dovrebbero valutare attentamente degli strumenti alternativi per l'autenticazione. L'autenticazione fuori banda che utilizza [SMS o chiamate vocali] è fortemente sconsigliata. Attualmente stiamo valutando se eliminarla nelle edizioni future di questa guida."

L'Harvard Business Review si è spinto addirittura oltre, affermando: "Si potrebbe quasi dire che l'autenticazione con SMS è diventata più un vettore di attacco che una vera misura di sicurezza."

Il motivo per cui l'autenticazione basata su SMS è rischiosa è il livello di vulnerabilità dei messaggi e la facilità con cui possono essere intercettati. Reddit, vittima di un attacco informatico nel 2018, è un caso abbastanza emblematico. Reddit ha commentato l'attacco al sito attribuendo la responsabilità alla debolezza del suo sistema di autenticazione basata su SMS: "Abbiamo appreso che l'autenticazione basata su SMS non è sicura come necessiteremmo e l'attacco principale si è verificato tramite intercettazione SMS. Lo sottolineiamo per incoraggiare tutti a passare a 2FA basato su token."

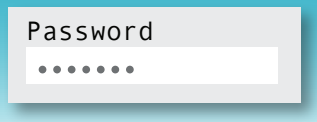
Di certo un MFA basato su SMS è preferibile al solo metodo password e nome utente, ma conserva comunque un alto grado di vulnerabilità. Per ridurre il rischio di violazioni le aziende dovrebbero affidarsi ad una soluzione MFA che utilizzi metodi di autenticazione più affidabili.

Come funziona AuthPoint?

AuthPoint è un servizio di autenticazione a più fattori (MFA) che aiuta le aziende a mantenere al sicuro le loro risorse, le informazioni e le identità degli utenti. Richiede agli utenti di utilizzare due o più fattori di autenticazione per accedere, invece di basarsi solamente sulle password.

Questi fattori sono una combinazione di:

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

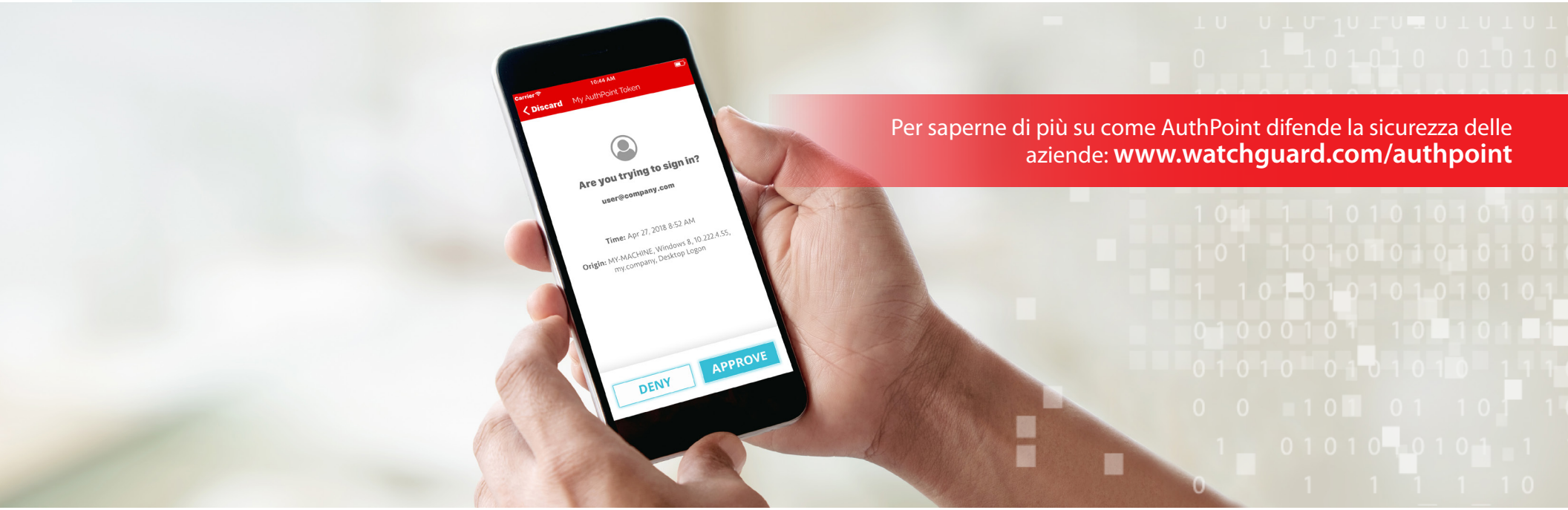


Grazie all'uso di **più livelli di autenticazione** le aziende possono ridurre in maniera significativa il rischio che i loro account vengano violati. Se un hacker dovesse entrare in possesso di una password, si troverà la strada sbarrata da uno degli altri livelli di protezione.

Con AuthPoint proteggersi diventa facilissimo. Con l'app mobile AuthPoint gli utenti concedono o negano l'accesso con un tocco. Una volta effettuato l'accesso, gli utenti si possono godere il Single Sign-On (SSO) su tutti gli account per cui sono abilitati.

Dato che gli accessi vengono approvati tutti tramite l'app mobile dell'utente, non servono token da portarsi in giro. È facilissimo! AuthPoint è interamente basato sul cloud. Significa che non richiede hardware da distribuire o software da aggiornare. Può essere gestito da qualsiasi luogo e, visto che è così facile da distribuire e gestire, non sarà necessario avere un esperto di sicurezza in-house per iniziare a usarlo.

Viaggi per lavoro? AuthPoint funziona sia online che offline, perciò gli utenti potranno accedere in completa sicurezza anche in aereo. Usando l'autenticazione con codici QR, gli utenti possono accedere sempre e ovunque si trovino.



Per saperne di più su come AuthPoint difende la sicurezza delle aziende: **www.watchguard.com/authpoint**

AuthPoint è la soluzione giusta per te?

Dato che le password possono essere rubate o violate con estrema facilità, molte aziende hanno scelto di adottare un sistema di autenticazione a più fattori per proteggere le identità degli utenti e le risorse. WatchGuard vuole che questa modalità di protezione sia a disposizione di aziende di ogni tipo e dimensioni, per questo motivo ha creato l'autenticazione a più fattori AuthPoint. L'autenticazione a più fattori è una delle forme di difesa principali per le piccole e medie imprese moderne. È disponibile presso il tuo rivenditore WatchGuard.

Puoi avere una protezione affidabile e costa meno di un cappuccino.

Allora, sei ancora disposto a basare tutto il tuo business sull'efficacia delle password dei tuoi dipendenti? Con AuthPoint non dovrai più farlo. È economico, potente e facile da usare.

Contatta il tuo rivenditore WatchGuard e inizia subito la prova gratuita di un mese. Per maggiori informazioni su AuthPoint, visita il sito www.watchguard.com/authpoint.

LA GAMMA DI PRODOTTI PER LA SICUREZZA WATCHGUARD

Sicurezza di rete

Oltre a fornire una sicurezza di livello enterprise, la nostra piattaforma è progettata per assicurare facilità di implementazione, di utilizzo e di gestione continua. È questo che rende WatchGuard la soluzione ideale per le PMI e le aziende distribuite in tutto il mondo.

Wi-Fi protetto

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 a strumenti completi di coinvolgimento e alla visibilità dell'analisi aziendale, la soluzione offre il vantaggio competitivo che serve alle aziende per avere successo.

Autenticazione a più fattori

WatchGuard AuthPoint™ è la soluzione ideale per risolvere le lacune di sicurezza legate alle password che rendono le aziende vulnerabili a violazioni. Offre l'autenticazione a più fattori su una piattaforma cloud intuitiva. Il nostro approccio unico aggiunge il "DNA del dispositivo mobile" come fattore di identificazione, per assicurare che solo le persone autorizzate accedano alle reti sensibili e alle applicazioni cloud.

Scopri di più

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

Informazioni su WatchGuard

WatchGuard® Technologies, Inc. è un leader globale nella fornitura di servizi relativi a sicurezza di rete, Wi-Fi sicuri, autenticazione a più fattori e intelligence di rete. I pluripremiati prodotti e servizi della nostra azienda hanno ottenuto la fiducia di circa 10.000 rivenditori in tutto il mondo, che provvedono alla sicurezza di circa 80.000 clienti. La missione di WatchGuard è di rendere la sicurezza accessibile ad aziende di tutti i tipi e dimensioni attraverso la semplicità, rendendo la soluzione di WatchGuard ideale per le aziende distribuite e le piccole e medie imprese. 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.

Vendite Nord America: 1.800.734.9905 • Vendite internazionali: 1.206.613.0895 • Web: www.watchguard.com/authpoint