Machine Translated by Google

Principali vantaggi per l'acquisto di AuthPoint

AuthPoint è un servizio di autenticazione a più fattori (MFA) di facile utilizzo che aiuta le aziende a proteggere le proprie risorse, informazioni e identità degli utenti. Colma una lacuna di sicurezza che lascia le aziende vulnerabili alle violazioni aggiungendo un livello di sicurezza oltre a un semplice nome utente e password, senza creare un'esperienza utente dirompente. L'app mobile di AuthPoint semplifica l'approvazione o il rifiuto dei tentativi di accesso con un solo tocco.

AuthPoint è più sicuro delle soluzioni di autenticazione a due fattori, più sicuro delle soluzioni basate su SMS, più economico (TCO inferiore) e più scalabile rispetto alle soluzioni non basate su cloud, più facile da usare rispetto alle soluzioni che richiedono token. L'interfaccia intuitiva di AuthPoint (dashboard) rende le minacce facili da vedere in tempo reale in modo che chiunque abbia accesso possa facilmente capire esattamente cosa sta succedendo nel proprio sistema. L'autenticazione a più fattori è diventata una necessità nel mondo digitale odierno e AuthPoint consente alle aziende di tutte le dimensioni di beneficiare della sicurezza dell'autenticazione a più fattori. L'AMF è un mercato in forte espansione che sta decollando solo ora. AuthPoint è la soluzione giusta al momento giusto.

Perché AuthPoint?

AuthPoint vince ogni volta quando si tratta di costi e complessità. I partner lo adorano perché è redditizio e facile da implementare e gestire. Gli utenti finali lo adorano perché è conveniente e facile da usare.

1 Elimina la vulnerabilità di sicurezza n. 1 sfruttata dagli hacker

Utente finale:

- L'81% delle violazioni nel 2017 ha sfruttato nomi utente e password rubati; la sicurezza a livello di password non è più sufficiente.
- MFA aggiunge un necessario livello di sicurezza che aiuta a proteggere i dipendenti e le loro organizzazioni dalle minacce che potrebbero portare a una violazione.

Compagno

- Le potenti funzionalità di sicurezza di AuthPoint consentono ai partner di fornire più com servizi completi aiutando i loro clienti a rafforzare la loro posizione di sicurezza.

2 Elimina costi amministrativi e complessità

Utente finale:

- AuthPoint può essere implementato e gestito con le risorse esistenti che non richiedono un esperto di sicurezza interno.
- AuthPoint è progettato per integrarsi con un lungo elenco di applicazioni (con ulteriori aggiunte continue) in modo che possa essere implementato nel sistema dell'utente finale senza un complesso processo di integrazione o lacune nell'assistenza.

Compagno

- Poiché è basato su cloud, non richiede hardware costoso o altre apparecchiature per l'implementazione. WatchGuard Cloud consente ai partner di richiedere e distribuire prove in pochi secondi, creare una nuova istanza in pochi secondi e assegnare gli utenti ai clienti nel modo desiderato.
- Gli utenti finali senza personale di sicurezza possono amministrare le proprie soluzioni o selezionare a fidato WatchGuard MSP per farlo per loro. Ciò consente agli MSP di WatchGuard di aggiungere MFA alla propria offerta di sicurezza senza aumentare il proprio personale o aggiungere oneri ai propri clienti.

3 Un'esperienza cliente sempre fluida

Utente finale:

- Il semplice approccio di autenticazione one-touch di AuthPoint è incredibilmente facile per gli utenti finali e funziona sia online che offline. L'app mobile è facile da usare e significa che i clienti non devono portare con sé token o dispositivi aggiuntivi.

Compagno

- Un'esperienza fluida e semplice significa meno ticket di supporto e meno chiamate di supporto (clienti più soddisfatti, team IT più soddisfatti), indipendentemente dal fatto che il servizio sia gestito dall'IT interno o da un VAR/MSP.

4 Proteggi ciò che conta oggi e oltre

Utente finale:

- Il nostro ecosistema di integrazioni pronte all'uso consente di implementare facilmente la protezione per le applicazioni ei casi d'uso importanti per la tua azienda oggi. Con l'aggiunta di nuove integrazioni ogni giorno, puoi essere certo che, man mano che la tua attività e le tue priorità cresceranno, anche la nostra protezione aumenterà.

Compagno

- L'ecosistema offre ai partner un modo semplice per associare l'AMF alla vendita di altre applicazioni già presenti nel loro listino prezzi; consente anche loro di ridimensionarsi.

5 La giusta protezione al giusto prezzo

Utente finale:

- L'AMF non è più un bene da avere, ma una necessità. Dovrebbe essere accessibile a ogni organizzazione, indipendentemente dal budget o dalle competenze in materia di sicurezza. AuthPoint ha un prezzo accessibile a tutti e scalabile in base alle esigenze.

Compagno

- I partner possono ora aggiungere questa offerta di sicurezza critica al loro portafoglio a una tariffa che i loro clienti possono permettersi, il che significa più adozione, clienti più soddisfatti e, in ultima analisi, maggiori entrate.
- I partner hanno anche accesso a un mercato di spazi verdi vendendo AuthPoint. L'autenticazione non è nuova, ma non è ancora entrata nel mercato delle PMI. AuthPoint elimina i costi e la complessità che in passato impedivano alle organizzazioni di medie dimensioni di acquistare l'autenticazione a più fattori.

6 Facile upsell con applicazioni esistenti o pacchetti di sicurezza

Compagno

- Collegamento ad applicazioni business-critical che già vendi che richiedono due fattori autenticazione.
- Una semplice aggiunta alle suite di servizi di sicurezza esistenti.
- AuthPoint può essere facilmente implementato insieme a WatchGuard Wi-Fi o alla sicurezza di rete.

Machine Translated by Google

Domande a

Comincia a vendere

Profilo Aziendale:

Utilizzi l'accesso remoto? (questo indica un rischio maggiore) Quali tipi di applicazioni Cloud utilizzi? (parla di integrazioni) Che tipo di sicurezza hai attualmente in atto? La tua sicurezza protegge la tua identità oltre il livello della password? Attualmente utilizzi 2FA o MFA? (sottolineare la debolezza di 2FA se pertinente)

Le password sono deboli:

Lo sapevate...?

- Oltre l'80% delle violazioni dei dati in tutto il mondo riguardava password deboli e/o rubate
- Il furto delle credenziali è l'azione principale intrapresa in caso di violazione
- Molte persone usano lo stesso pass parola sugli account aziendali come su quelli personali (es. Netflix)
- Il 6% delle persone utilizza la stessa password su tutti gli account, ma quasi ogni singola persona utilizza la stessa password su più account
- La tua password o quella dei tuoi dipendenti le password dei colleghi sono spesso disponibili, a volte per l'acquisto, sul dark web

Conformità: •

Sapete se il vostro settore o organizzazione richiede standard di conformità e sicurezza più elevati?

Rischio:

- Sapevi che basta una sola credenziale rubata per accedere alla VPN e alla rete della tua azienda?

Gestione delle obiezioni

Duo e Gemalto hanno ampio liste di integrazione	AuthPoint si integra con le principali integrazioni utilizzate dai nostri clienti. Se c'è un'integrazione che vorresti che non fosse nella nostra lista, faccelo sapere. Siamo felici di lavorare con te per aggiungerlo e aggiungiamo continuamente altre integrazioni.
Non basato sul rischio/adattivo autenticazione	WatchGuard aggiungerà questa tecnologia ad AuthPoint nel 2019, ma viene utilizzata principalmente come funzionalità di praticità piuttosto che come funzionalità di sicurezza.
Nessuna interfaccia API per integrare con Portali web	L'esposizione delle API per l'autenticazione degli utenti, chiamate servizi Web, è la chiave per l'integrazione con le applicazioni basate sul Web sviluppate dai clienti. Comprendiamo la sua importanza e forniremo tale funzionalità entro l'inizio del 2019.
Nessun supporto per Connetti ID aperto	OpenID Connect è spesso utilizzato da aziende che vorrebbero utilizzare gli account dei social media (Google, Facebook, Twitter, ecc.) per accedere ai propri portali e quindi non richiederebbero la potenza dell'autenticazione a più fattori. SAML, che supportiamo per Web SSO, è lo standard principale per le applicazioni aziendali.
Nessun deposito password	AuthPoint è un servizio di autenticazione a più fattori, non un gestore di password. Offre Web SSO per applicazioni cloud aziendali. Per le credenziali personali, un utente può scegliere il gestore di password che desidera e utilizzarlo insieme ad AuthPoint.
L'AMF è costoso	La protezione di AuthPoint costa meno del costo di una tazzina di caffè per un utente ogni mese. Il costo medio di una violazione è di 1,3 milioni di dollari per le aziende e di 120.000 dollari per le PMI. Il 60% delle PMI cessa l'attività entro 6 mesi dopo una violazione.

Vendere contro tecnologie concorrenti

Gettoni SMS

Uno dei metodi di autenticazione più deboli; vulnerabili ad essere dirottati/intercettati

- Il NIST ha raccomandato nel 2016 l'uso di metodi MFA alternativi agli SMS, a causa delle sue vulnerabilità
- I token SMS non sono facili da usare, soprattutto se si sta tentando di accedere a un servizio sullo stesso telefono cellulare utilizzato per l'autenticazione o se ci si trova in un luogo con scarsa copertura di rete
- Il protocollo utilizzato dai carrier per inviare SMS – SS7 – è vulnerabile a diversi exploit; può essere intercettato
- I telefoni cellulari con RAT (trojan di accesso remoto) reindirizzano facilmente gli SMS a un telefono malintenzionato, all'insaputa del proprietario
- Gli aggressori possono utilizzare l'ingegneria sociale per fare in modo che gli operatori reindirizzano i messaggi a una scheda SIM diversa

Token hardware

Facilmente perso o rubato; costoso; difficili da distribuire, devono essere trasportati

- Necessità di essere trasportato (in borsa, tasca, borsa, ecc.)
- Più difficile da fornire: è necessario inviare a ciascun individuo, inclusi gli utenti remoti
- Costo più elevato – l'utente potrebbe perderlo, romperlo
- Richiede l'installazione del driver, potrebbe avere problemi di connettività, costi di supporto più elevati

Token hardware OTP

- Soggetto a ingegneria sociale (ad es. qualcuno cerca di convincere l'utente a dare via l'OTP)
- Soggetto ad attacchi man-in-the-middle (ad es. quando l'utente è connesso a un sito Web fasullo che richiede le credenziali dell'utente, inclusa l'OTP corrente)
- Durata della batteria limitata

Token connessi (token USB, smart card con lettori)

- Potrebbero essere necessari adattatori, ad esempio per connettersi a un computer Mac
- Minore portabilità, uso limitato su altri computer o quando si utilizza uno smartphone o un tablet per accedere a un servizio

Token Bluetooth

- A volte richiede l'uso di un dongle Bluetooth separato
- Minore portabilità, uso limitato su altri computer poiché ciò richiederebbe l'associazione Bluetooth
- Durata della batteria limitata

Machine Translated by Google

Vendere contro i principali concorrenti

Sicurezza a due

Costoso, difficile da gestire e utilizzare, ha un canale diretto che fa concorrenza alle vendite dei partner

- Il loro processo per il passaggio degli utenti a un nuovo telefono è molto complesso e di solito richiede un amministratore. La soluzione di AuthPoint è self service.
- Ha un canale di vendita diretto che compete con le vendite dei partner e si traduce in margini inferiori (i margini di AuthPoint possono essere fino a 3 volte più alto)
- Il software gateway di Duo per l'installazione on-premise richiede una grande quantità di configurazioni e script; AuthPoint richiede solo una chiave di registrazione per installare tutto
- Ha vulnerabilità che AuthPoint non ha (ad es. non offre la funzione DNA mobile che aiuta a fermare le minacce di clonazione mobile)
- La loro app è meno user-friendly (ad es. rende difficile aggiungere/personalizzare i token)
- Duo ha una vista Cloud Solution Provider meno potente che rende più difficile la gestione dell'inventario e dell'utente assegnazione ai clienti

Gemalto SAS

Noto per essere difettoso, è difficile da usare e non è progettato per il mercato delle PMI

- Richiede installazioni aggiuntive per la piena funzionalità
- Fornisce un'esperienza utente complicata, non progettata o intuitiva per le PMI; più applicabile per le grandi aziende con configurazioni e requisiti molto complessi
- Non supporta funzionalità e usi chiave: il token mobile non supporta la migrazione del token o l'autenticazione basata su codice QR; l'accesso a Windows non supporta l'autenticazione basata su codice QR o dispone di un bypass MFA per quando gli utenti dimenticano o perdono i propri token

OneSpan (basco) Digipass

Casi d'uso limitati (principalmente eBanking), più una soluzione on-prem che Cloud

- Casi d'uso molto limitati: si concentra sul mercato dell'eBanking • Le soluzioni sono per lo più on-premise senza molta attenzione all'autenticazione basata su cloud
- Di solito vende licenze utente e token separatamente, quindi il costo finale può essere molto più alto

Autenticazione a più fattori di Microsoft Azure

Non progettato per SMBS, richiede licenze e comprensione di Azure

- Molto impegnativo da implementare e mantenere per le PMI poiché non è progettato per quel mercato
- Richiede licenze Azure ed è utilizzato principalmente da negozi Microsoft/Azure con una profonda conoscenza di Azure • È difficile da configurare e implementare (soprattutto con prodotti di terze parti); non intuitivo per semplici implementazioni VPN con firewall; richiede l'installazione e la configurazione dell'estensione Microsoft NPS (Network Policy Server).

Google Authenticator

Vulnerabile come prodotto solo OTP; utilizzato principalmente per i social media e alcune app Web

- Un prodotto solo OTP, non un servizio di autenticazione basato su cloud; OTP è soggetto ad attacchi di ingegneria sociale
- Google Authenticator può essere facilmente clonato dagli hacker, rendendolo molto meno sicuro, se un hacker ruba il codice QR utilizzato per attivare un Google Authenticator, l'aggressore può attivare le stesse credenziali su qualsiasi dispositivo e ottenere così l'accesso agli account utente
- Non fornisce l'integrazione con SAML, VPN o Windows Logon; viene utilizzato principalmente per i social media e alcune applicazioni web

Machine Translated by Google

Principali motivi per acquistare AuthPoint

	Punti di forza	Debolezze	Mobile Autenticatore	Hardware Autenticatore	Gestione	VPN	SAML/Web SSO	finestre Accedere
AuthPoint	Facilità d'uso	Meno integrazioni rispetto ad alcuni concorrenti	Sì	No (tabella di marcia)	Basato su cloud	Supportato	Supportato	Supportato
	Convenienza	Nessun supporto per i servizi Web ancora	★★★★★ Google play					
	App mobile completa, localizzata e di facile utilizzo, generazione di chiavi dinamiche (DSKPP)	Nessuna autenticazione basata sul rischio						
Duo	Giocatore principale che è ben noto e ha un'enorme quota di mercato	Programma partner debole	Sì	Sì, supporta gli autenticatori hardware di terze parti	Basato su cloud, ma con opzioni MSSP limitate	Supportato	Supportato, ma richiede l'installazione locale (Porta doppia)	Sì, ma non supporta l'accesso offline a Windows. Anche il login di Windows ha una configurazione molto complessa
	Forti integrazioni	Molto più costoso	(token basato su eventi, n Autenticazione con codice QR)					
	Forte piattaforma cloud	Può essere complesso da configurare e richiedere script	★★★★★ Google play					
	Interfaccia forte	Usa vecchio, basato sugli eventi OTP (sono molto vulnerabili)						
		Nessuna autenticazione con codice QR offline; richiede invece OTP per l'utilizzo offline (meno sicuro)						
Gemalto SAS	Molte opzioni di autenticazione	È difficile da usare; vecchia interfaccia utente	Sì	Supportato	Basato su cloud o on-premise	Supportato; RADI Server statunitensi nel Cloud, che è meno sicuro (richiede un tunnel dedicato per la sicurezza)	Supportato	Supportato
	Ampio ecosistema di applicazioni supportate	Non è progettato per mercato delle PMI	★★★★★ Google play					
	Flessibilità per la distribuzione on-premise o nel cloud							
OneSpan (Vasco)	Grande varietà di fattori di forma token	Focalizzato su eBanking e grandi imprese	Sì	Supportato	Basato su cloud	Supportato	Supportato	Supportato
		In gran parte in sede	★★★☆☆ Google play					
Microsoft autenticazione a più fattori di Azure	Prezzi aggressivi e flessibili (per utente o per utilizzo)	Non progettato per le PMI	Sì	Supporta terze parti	Basato su cloud	Supportato	Supportato	Non supportato (non è possibile utilizzare Azure MFA per accedere a Windows)
	Stretta integrazione con Prodotti Microsoft	Richiede licenze Azure	★★★★☆ Google play					
		Può essere difficile integrarsi con prodotti di terze parti						
		Nessuna protezione di accesso a Windows						

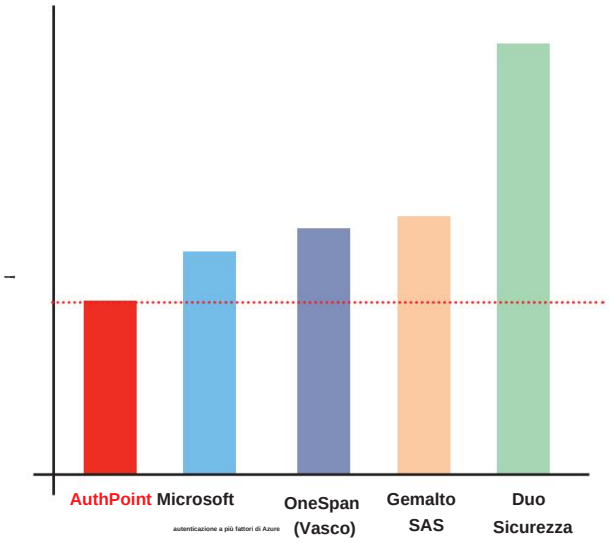
* **Google Authenticator** è stato escluso dal confronto perché non è lo stesso tipo di prodotto degli altri. È destinato più all'uso personale (ad es. sui social) che all'uso aziendale. Google Authenticator fornisce molte API gratuitamente, ma gli utenti devono sviluppare tutto il resto per renderlo paragonabile ad altre soluzioni MFA. È un prodotto solo OTP, il che semplifica la clonazione. Non può essere utilizzato direttamente per VPN o accesso a Windows.

Machine Translated by Google

Confronto dei prezzi

AuthPoint vince sul prezzo!

- $ **AuthPoint:** il prezzo basso include tutte le funzionalità
- $$ **Duo:** 2-3 volte il costo di AuthPoint
- $$ **Gemalto SAS:** non include la tariffa di configurazione iniziale
- $$ **OneSpan (Vasco):** Token non incluso
- $$$ **Azure MFA:** richiede i servizi di Azure, che aumentano il prezzo



*Stime dei prezzi ad agosto 2018

Integrazioni chiave di AuthPoint

Consulta il nostro elenco completo di integrazioni **qui.**

© 2018 WatchGuard Technologies, Inc. Tutti i diritti riservati. N. parte WGCE67121_082018