DATASHEET

AUTHPOINT

ZMNIEJSZ RYZYKO DZIĘKI WYDAJNEMU, PRZYJAZNEMU DLA UŻYTKOWNIKA UWIERZYTELNIANIU WIELOSKŁADNIKOWEMU

HASŁA SĄ NIEWYSTARCZAJĄCE

Każdego dnia cyberprzestępcy wykorzystują skradzione dane uwierzytelniające, aby uzyskać dostęp do systemów i infekować je lub wykraść dane. Najbardziej potrzebne do odwrócenia tego trendu jest to, aby uwierzytelnianie wymagało dodatkowego dowodu tożsamości poza prostą nazwą użytkownika i hasłem i było szeroko wdrażane przez wszystkie firmy – bez względu na ich wielkość.

MFA TRZYMA OSZUSTÓW Z DALA

WatchGuard AuthPoint® to właściwe rozwiązanie we właściwym czasie, aby rozwiązać tę lukę w zabezpieczeniach dzięki uwierzytelnianiu wieloskładnikowemu (MFA) na łatwej w użyciu platformie w chmurze. Dzięki prostemu powiadomieniu push aplikacja mobilna AuthPoint uwidacznia każdą próbę logowania, umożliwiając użytkownikowi zaakceptowanie lub zablokowanie dostępu bezpośrednio ze smartfona. Unikalne podejście WatchGuard dodaje „DNA telefonów komórkowych" jako czynnik identyfikujący, aby dodatkowo zapewnić, że tylko właściwa osoba ma dostęp do wrażliwych sieci i aplikacji w chmurze

INTUICYJNE ZARZĄDZANIE W CHMURZE

MFA było poza zasięgiem niektórych organizacji ze względu na złożone integracje i uciążliwe zarządzanie lokalnie, co uniemożliwia wdrożenie bez dużego personelu IT i znacznych kosztów początkowych. Natomiast rozwiązanie AuthPoint WatchGuard jest usługą w chmurze, więc nie ma drogiego sprzętu do wdrożenia, i można nim zarządzać z dowolnego miejsca za pomocą intuicyjnego interfejsu WatchGuard Cloud. Ponadto nasz ekosystem oferuje dziesiątki integracji z aplikacjami innych firm – zapewniając, że ochrona MFA jest szeroko stosowana w przypadku dostępu do wrażliwych aplikacji w chmurze, usług internetowych, sieci VPN i sieci.
Użytkownicy AuthPoint mogą zalogować się raz, aby uzyskać dostęp do wielu aplikacji, i doceniają możliwość dodania zewnętrznych uwierzytelniaczy, takich jak Facebook lub Google Authenticator, do przyjaznej aplikacji mobilnej.

> "MFA is now considered core protection, and it comes from WatchGuard hassle-free."
>
> *~Tom Ruffolo, CEO, eSecurity Solutions*

TRZY SPOSOBY UWIERZYTELNIANIA APLIKACJI

Uwierzytelnianie oparte na wypychaniu
Bezpieczne uwierzytelnianie z zatwierdzaniem jednym dotknięciem. Widzisz, kto i gdzie próbuje się uwierzytelnić, a także możesz zablokować nieautoryzowany dostęp do Twoich zasobów

Uwierzytelnianie oparte na kodzie QR
Użyj aparatu, aby odczytać unikalny, zaszyfrowany kod QR z wyzwaniem, które można odczytać tylko za pomocą aplikacji. Odpowiedź jest wpisywana, aby sfinalizować uwierzytelnianie.

Hasło jednorazowe oparte na znaczniku czasowym (OTP)
Odzyskaj swoje dynamiczne, czasowe, jednorazowe hasło w takiej postaci, w jakiej się wyświetla, i wprowadź je podczas logowania.

CECHY I ZALETY

- Uwierzytelnianie online (push) i offline (kod QR i OTP)
- Usługa chmury o niskim całkowitym koszcie posiadania
- Sprawdzanie DNA urządzenia mobilnego pod kątem silnego dopasowania tożsamości
- Lekka, w pełni funkcjonalna aplikacja mobilna w 13 językach
- Ochrona logowania VPN, Cloud i PC w zestawie
- Portal internetowego jednokrotnego logowania (SSO)
- Łatwa ochrona VPN, Aplikacje i usługi internetowe w chmurze korzystające z przewodników integracji
- Konfiguruj zasady ryzyka i twórz niestandardowe reguły, które są zgodne z Twoimi potrzebami w zakresie bezpieczeństwa

DATASHEET

AuthPoint Mobile App

FUNKCJE UWIERZYTELNIANIA
- Uwierzytelnianie typu Push (online)
- Uwierzytelnianie na podstawie kodu QR (offline)
- Hasło jednorazowe oparte znaczniku czasowym (offline)

FUNKCJONALNOŚĆ ZWIĄZANA Z BEZPIECZEŃSTWEM
- Mobile Device DNA
- Aktywacja online za pomocą dynamicznego generowania klucza
- Dostęp do uwierzytelnienia za pomocą kodu PIN, odcisków palców i rozpoznawania twarzy (iPhone)
- Samoobsługowa, bezpieczna migracja uwierzytelniania na inne urządzenie
- Jailbreak i wykrywanie rootów

WYGODNE FUNKCJE
- Obsługa wielu tokenów
- Obsługa tokenów sprzętowych innych firm
- Obsługa tokenów mediów społecznościowych innych firm
- Niestandardowa nazwa tokena i zdjęcie

OBSŁUGIWANE PLATFORMY
- Android v4.4 lub nowszy
- iOS v9.0 lub nowszy

OBSŁUGIWANE JĘZYKI
Angielski, hiszpański, portugalski (brazylijski i portugalski), niemiecki, holenderski, francuski, włoski, japoński, chiński (uproszczony i tradycyjny), koreański, tajski

STANDARDY
- 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

AuthPoint Service

WSPIERANE ZASTOSOWANIA
- Uwierzytelnianie w chmurze z jednokrotnym logowaniem w sieci
- Dostęp zdalny i uwierzytelnianie VPN
- Ochrona logowania do systemu Windows (online/offline)
- Ochrona logowania macOS (online/offline)
- Zdalny dostęp, zdalny pulpit i uwierzytelnianie VPN
- Ochrona logowania do systemu Linux

FUNKCJE ZARZĄDZANIA
- Platforma chmurowa WatchGuard
- Synchronizacja i uwierzytelnianie użytkowników Active Directory i LDAP
- Pulpit nawigacyjny z widżetami monitorowania i raportowania
- Dostosowane zasady uwierzytelniania
- Konfigurowalne zasoby uwierzytelniania
- Łatwe wdrażanie dzięki przewodniku integracji
- Dzienniki i raporty
- Konfiguracja bezpiecznej lokalizacji

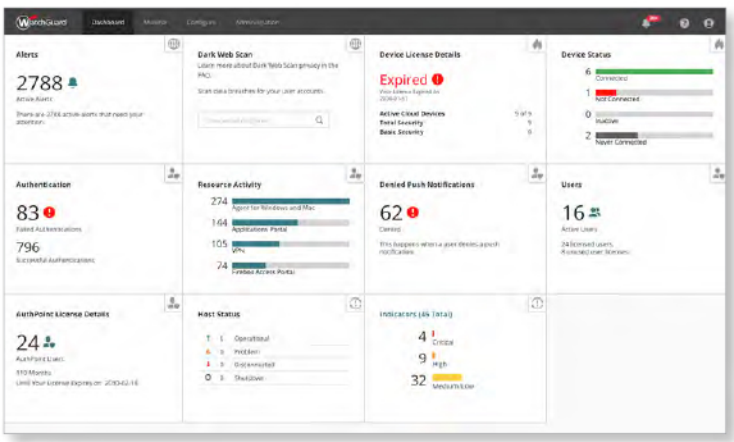
AUTHPOINT GATEWAY
- Bezpieczne połączenie wychodzące z sieci do chmury WatchGuard
- Synchronizacja MS-AD i LDAP
- Serwer RADIUS
- Zapewnia wsparcie HA (wysoka dostępność)

AUTHPOINT AGENTS
- Windows Logon
- macOS Logon
- ADFS
- RD Web

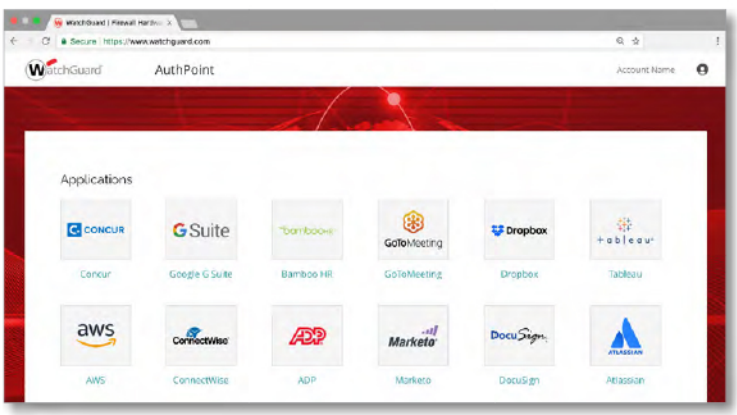
STANDARDY
- RADIUS
- SAML 2.0 IdP

INTEGRACJE (DOSTĘPNE PONAD 100 INTEGRACJI)
Microsoft Office 365, G-Suite, WatchGuard Firebox, Dropbox, Go-to-Meeting, Open VPN

AuthPoint Mobile App



AuthPoint WatchGuard Cloud Dashboard



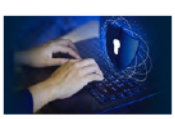
Integrations and SSO

WATCHGUARD UNIFIED SECURITY PLATFORM™


Bezpieczeństwo sieci


Bezpieczne Wi-Fi


Multi-Factor Authentication


Bezpieczeństwo punktów końcowych

Skontaktuj się z autoryzowanym sprzedawcą WatchGuard lub odwiedź
netcomplex.com, firebox.com.pl
aby dowiedzieć się więcej

Net Complex Sp. z o.o. ul. Wita Stwosza 5, 43-300 Bielsko-Biała biuro@netcomplex.pl 501 196 890