DATASHEET

WATCHGUARD PASSPORT

PROTEZIONE PERSISTENTE, SEMPRE ATTIVA, CHE SEGUE I TUOI UTENTI

Le aziende devono poter estendere le funzionalità di sicurezza a utenti e dispositivi, ovunque si trovino. Dipendenti, fornitori, visitatori e i relativi dispositivi entrano ed escono dalla rete mentre svolgono le proprie mansioni, in sede o fuori sede. Allo stesso tempo, anche un solo endpoint infetto o una password rubata potrebbe aprire un varco per gli aggressori. WatchGuard Passport è un pacchetto di servizi di sicurezza incentrati sull'utente che viaggia insieme ai tuoi utenti.

Con Passport puoi:

1. **Autenticare** persone e applicare una solida autenticazione a più fattori in VPN, applicazioni cloud, endpoint e altro ancora.
2. **Proteggere** gli utenti in Internet, bloccare i tentativi di phishing e applicare policy di navigazione Web ovunque, in qualsiasi momento, senza richiedere una VPN.
3. **Previene,** rileva e reagisce a minacce note e sconosciute, contiene il ransomware, gli exploit e qualsiasi altra tecnica di attacco.

GESTIONE E IMPLEMENTAZIONE DAL CLOUD

Passport viene gestito dal cloud al 100%, pertanto non è necessario effettuare alcuna manutenzione di software o implementazione di hardware. La visualizzazione di report e alert, la configurazione di servizi, l'implementazione di sensori host e la gestione di token di autenticazione sono tutte operazioni che è possibile eseguire nel cloud. Inoltre, con l'integrazione con gli strumenti di implementazione di terze parti leader di settore, puoi iniziare a utilizzare Passport in modo semplice e veloce.

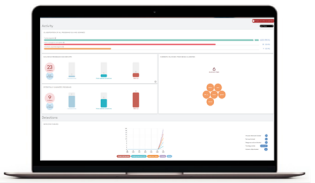
Cosa è incluso in Passport?

Autenticazione a più fattori

Con l'aumento di malware all'origine di furto di credenziali e di nuove violazioni di dati (nomi utente e password utilizzati quotidianamente), l'esigenza di una solida autenticazione non è mai stata maggiore. WatchGuard AuthPoint riduce il carico per te e i tuoi clienti. AuthPoint utilizza notifiche push, codici QR o password temporanee (OTP), unitamente al DNA del dispositivo mobile di ogni utente, per identificare e autenticare le persone.

Protezione DNS

Quando gli utenti si spostano al di fuori della rete, la visibilità della loro attività Internet potrebbe non essere più disponibile e questo crea un punto cieco significativo nella sicurezza, esponendoli agli attacchi di phishing e malware. Con DNSWatchGO puoi ottenere una visibilità consolidata dei dispositivi protetti, ovunque si trovino. Fuori dalla rete, un client host monitora le richieste DNS in uscita e le mette in correlazione con un elenco aggregato di domini dannosi. I tentativi di comunicare con questi domini verrà bloccato, mentre il traffico sarà instradato al cloud DNSWatchGO per ulteriori indagini.



Sicurezza degli endpoint

Panda Adaptive Defense 360 è un'innovativa soluzione per la sicurezza informatica pensata per computer, laptop e server basata su cloud che combina la più ampia gamma di tecnologie di protezione (EPP) con le funzionalità di EDR, grazie a due servizi gestiti dagli esperti di Panda Security forniti come funzionalità della soluzione: servizio Zero Trust per le applicazioni e servizio di ricerca delle minacce.

App mobile AuthPoint

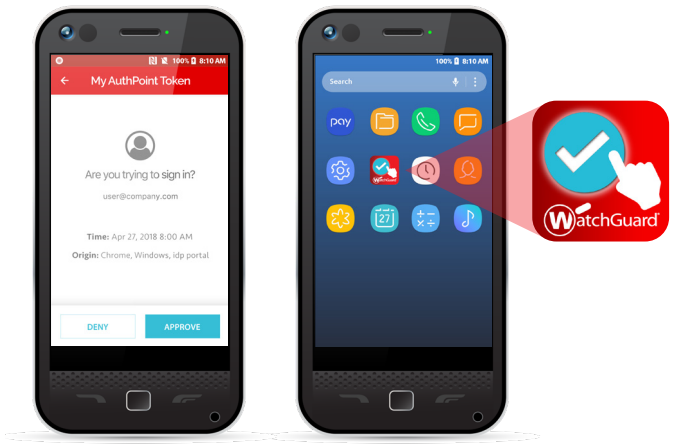
FUNZIONI DI AUTENTICAZIONE
Autenticazione push (online)
Autenticazione con codice QR (offline)
Password univoca a tempo (OTP) (offline)
FUNZIONALITÀ DI SICUREZZA
Firma del DNA del dispositivo
Attivazione online con generazione di chiave dinamica
Protezione per ogni autenticatore • PIN • Impronta digitale (Samsung/Apple) • Riconoscimento facciale (Apple)
Migrazione self-service e sicura dello strumento di autenticazione su un altro dispositivo
Jailbreak e rilevamento della causa principale
FUNZIONALITÀ PRATICHE
Supporto multi-token
Supporto per token di social media di terze parti
Nome e immagine del token personalizzabili
PIATTAFORME SUPPORTATE
Android 4.4 o versione superiore
iOS 9.0 o versione superiore
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

DNSWatchGO

SISTEMI OPERATIVI SUPPORTATI
Windows 7, 8 e 10
FUNZIONI DI SICUREZZA
Blocco degli attacchi di phishing
Prevenzione delle connessioni C2
Filtro dei contenuti
Erogazione del training sulla consapevolezza immediata della sicurezza
SUPPORTO VPN
Completamente compatibile con i seguenti tipi di WatchGuard Mobile VPN: • IKEv2 • SSL/TLS • L2TP • IPSec

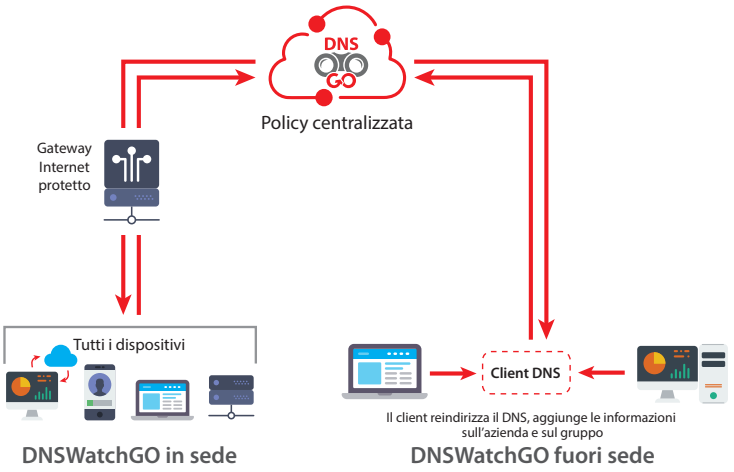
Rilevamento degli endpoint e relativa risposta

SISTEMI OPERATIVI SUPPORTATI
Windows: Workstation - XP, Vista, 7, 8, 8.1, 10. Server - 2003 SP2 e versioni successive, 2008
Linux: Red Hat Enterprise 6.0 e versioni successive, Debian Squeeze, Ubuntu 12 o versioni successive, OpenSuse 12 o versioni successive, Suse Enterprise Server 11 SP2 o versioni successive, CentOS 6.x e versioni successive
MacOS: 106 Snow Leopard, 10.7 Lion, 10.8 Mountain Lion, 10.9 Mavericks, 10.10 Yosemite, 10.11 El Capitan, Sierra
METODOLOGIE DI RILEVAMENTO
Firme generali ed euristica
Ricerca basata sul cloud nell'Intelligenza collettiva
Rilevamento attacchi IoA
Firewall, IDS/IPS
Soluzioni antimanomissione
Controllo dispositivi
Monitoraggio dell'attività degli endpoint e capacità EDR quali:
Rilevamento contestualizzato dei comportamenti
e anti-exploit in memoria
Servizio Zero-Trust Application
Servizio Threat Hunting



COME FUNZIONA

WatchGuard DNSWatchGO monitora le richieste DNS in uscita, mettendole in correlazione con un elenco aggregato di siti dannosi. Le richieste riconosciute come dannose vengono bloccate, mentre gli utenti vengono reindirizzati a siti sicuri per rafforzare il proprio training sul phishing.



WATCHGUARD UNIFIED SECURITY PLATFORM™


Sicurezza di rete


Secure Cloud Wi-Fi


Autenticazione a più fattori


Endpoint Security

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

VENDITE IN ITALIA 800 911 938 E-MAIL italy@watchguard.com WEB www.watchguard.com/it WatchGuard Technologies, Inc.