

WatchGuard Passport, la sicurezza che “segue” l’utente



Con un panorama di minacce che prende sempre più di mira applicazioni cloud e dispositivi endpoint per fare breccia nelle reti aziendali, le aziende devono estendere la tradizionale sicurezza incentrata sulla rete oltre il perimetro, concentrandosi sull’utente, per proteggere utenti e dispositivi, sempre, ovunque si trovino.

Dipendenti, fornitori, visitatori e i relativi dispositivi entrano ed escono dalla rete mentre svolgono le loro mansioni, in sede o fuori sede. Allo stesso tempo, anche un solo endpoint infetto o una password rubata potrebbe aprire un varco per gli attaccanti.

La sicurezza deve quindi “viaggiare” insieme all’utente. **WatchGuard Passport** è un pacchetto di servizi di sicurezza che è stato pensato proprio con questo scopo. È stato ideato per fornire rilevamento e risposta agli endpoint, bloccare i tentativi di phishing, proteggere le informazioni riservate e autenticare le persone ovunque nel mondo.

Con Passport è possibile autenticare le persone e applicare una solida autenticazione a più fattori a VPN, applicazioni cloud, endpoint e altro ancora. Inoltre, Passport protegge gli utenti in Internet, blocca i tentativi di phishing e permette di applicare policy di navigazione Web ovunque, in qualsiasi momento, senza richiedere una VPN. Previene, rileva e reagisce a minacce note e sconosciute, e aiuta a contenere ransomware, exploit e qualsiasi altra tecnica di attacco.

Il bundle Passport include:

- Autenticazione a più fattori con **WatchGuard AuthPoint**: questa soluzione 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 con **DNSWatchGO**, per 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 verranno bloccati, mentre il traffico sarà instradato al cloud DNSWatchGO per ulteriori indagini.
- Sicurezza degli endpoint con **Adaptive Defense 360**, 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.

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, è possibile iniziare a utilizzare Passport in modo semplice e veloce.

Per maggiori informazioni sulla sicurezza per i lavoratori da remoto di WatchGuard:

<https://www.watchguard.com/it/wgrd-solutions/remote-worker-sec>

urity

<https://www.ictsecuritymagazine.com/notizie/watchguard-passport-la-sicurezza-che-segue-lutente/>