DATENBLATT

PASSPORT™

DAUERHAFTER RUND-UM-DIE-UHR-SCHUTZ, DER DIE ANWENDER ÜBERALLHIN BEGLEITET

Unternehmen müssen die Sicherheitsfunktionen auf Anwender und Geräte – unabhängig von deren Standort – ausweiten. Im Rahmen ihrer Aktivitäten vor Ort und außerhalb nutzen Mitarbeiter, Auftragnehmer, Besucher und ihre Geräte regelmäßig Ihr Netzwerk und verlassen es wieder. Gleichzeitig kann bereits ein einziger infizierter Endpunkt oder ein gestohlenes Passwort einem Angriff auf das Netzwerk Tür und Tor öffnen. Passport von WatchGuard ist ein Bundle aus den anwenderorientierten Sicherheitsdiensten, das die Anwender überallhin begleitet.

Passport bietet Ihnen folgende Möglichkeiten:

1. **Authentifizierung von** Personen und starke Multifaktor-Authentifizierung für VPNs, Cloud-Anwendungen, Endpunkte usw.
2. **Schutz der** Anwender im Internet, Blockieren von Phishing-Versuchen und allgemeine Durchsetzung einer Internetrichtlinie an jedem Ort und zu jeder Zeit ohne VPN.
3. **Vermeiden,** erkennen und reagieren Sie auf bekannte und unbekannte Bedrohungen und dämmen Sie Ransomware, Exploits und andere Angriffstechniken ein.

MANAGEMENT UND BEREITSTELLUNG AUS DER CLOUD

Passport wird zu 100 % in der Cloud verwaltet. Sie müssen also keine Software warten und auch keine Hardware bereitstellen. Die Anzeige von Berichten und Warnmeldungen, die Konfiguration von Diensten, die Bereitstellung von Endpunkt-Clients und das Management von Authentifizierungs-Tokens erfolgen allesamt über die Cloud. Durch die Integration in die führenden Bereitstellungs-Tools von Drittanbietern können Sie Passport zudem schnell und einfach einrichten.

Welche Funktionen sind in Passport enthalten?

Multifaktor-Authentifizierung

Malware, die Anmeldedaten stiehlt, bereitet zunehmend Probleme. Hinzu kommen neue Datensicherheitsverletzungen, die Benutzernamen und Passwörter betreffen. Daher sind strenge Authentifizierungsmaßnahmen wichtiger denn je. WatchGuard AuthPoint entlastet Sie und Ihre Kunden bei diesem Schritt. AuthPoint sorgt mit Push-Nachrichten, QR-Codes oder Einmalpasswörtern einerseits und der Mobilgeräte-DNA des jeweiligen Smartphones andererseits für die Identifizierung und Authentifizierung von Anwendern.

Schutz auf DNS-Ebene

Wenn Anwender außerhalb des Netzwerks unterwegs sind, verlieren Unternehmen leicht den Überblick über ihre Internetaktivitäten. Dadurch können wesentliche Sicherheitsbereiche nicht mehr eingesehen werden, und die Anfälligkeit gegenüber Phishing- und Malware-Angriffen steigt. DNSWatchGO bietet Ihnen eine konsolidierte, transparente Übersicht über geschützte Geräte unabhängig von deren Standort. Dazu überwacht ein Host-Client auch jenseits des internen Netzwerks ausgehende DNS-Anforderungen und gleicht sie mit einer Liste böswilliger Domains ab. Daraufhin werden Versuche, mit derartigen Domains zu kommunizieren, blockiert und der Verkehr für weitere Untersuchungen an DNSWatchGO Cloud weitergeleitet.

Endpoint-Sicherheit

WatchGuard EPDR ist eine innovative Cybersicherheitslösung für Endpoints und Server, die über die Cloud bereitgestellt wird. WatchGuard EDPR kombiniert eine sehr breite Palette an Endpoint-Schutztechnologien (EPP) mit EDR-Funktionen und automatisiert die Prävention, Erkennung und Eindämmung hoch entwickelter Bedrohungen sowie die entsprechende Reaktion. Ermöglicht wird dies durch die zwei Services, die von WatchGuard-Sicherheitsexperten verwaltet werden und in die Lösung eingebunden sind: Zero-Trust Application Service und Threat Hunting Service. Es bietet zudem die folgenden EPP-Funktionen: IDS, verwaltete Firewall, Gerätesteuerung, E-Mail-Schutz, URL- und Content-Filter.

PASSPORT

Mobile AuthPoint-App

AUTHENTIFIZIERUNGSFUNKTIONEN

- Push-basierte Authentifizierung (online)
- QR-Code-basierte Authentifizierung (offline)
- Zeitbasiertes Einmalkennwort (offline)

SICHERHEITSFUNKTIONEN

- DNA-Signatur des Geräts
- Onlineaktivierung mit Erstellung von dynamischen Schlüsseln
- Schutz pro Authentifikator
  - PIN
  - Fingerabdruck (alle Plattformen)
  - Gesichtserkennung (alle Plattformen)
- Self-Service: Sichere Migration des Authentifikators von einem Smartphone zum Nächsten
- Jailbreak und Root-Detection

PRAKTISCHE FUNKTIONEN

- Unterstützung mehrerer Tokens
- Unterstützung für Social-Media-Token von Drittanbietern
- Anpassbare Token-Namen und -Bilder

UNTERSTÜTZTE PLATTFORMEN

- Android v4.4 oder höher
- iOS v9.0 oder höher

STANDARDS

- 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

UNTERSTÜTZTE BETRIEBSSYSTEME

- Chrome OS
- Windows 7, 8 und 10

SICHERHEITSFUNKTIONEN

- Blockieren von Phishing-Angriffen
- Verhindern von C2-Verbindungen
- Inhaltsfilterung
- Sofortige Schulung zum Sicherheitsbewusstsein

VPN-SUPPORT

- Uneingeschränkte Kompatibilität mit folgenden WatchGuard Mobile VPN-Typen:
  - IKEv2
  - SSL/TLS
  - L2TP
  - IPSec

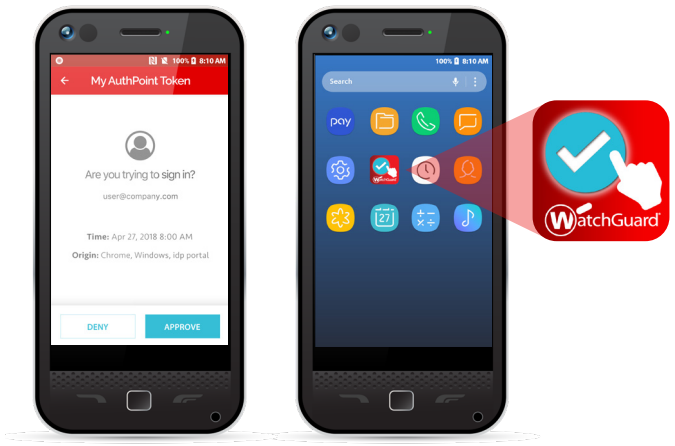
Endpoint Detection and Response

MODERNSTE SICHERHEITSTECHNOLOGIEN

- Ständige Überwachung der Endpunktaktivität
- Klassifizierung von 100 % der Prozesse – es können nur vertrauenswürdige Anwendungen ausgeführt werden
- Sandboxing in realen Umgebungen
- Automatische Erkennung und Abwehr von APTs, Ransomware, Rootkits usw
- Erkennung und Blockierung von Arbeitsspeicher-Exploits
- Threat Hunting Service zur Erkennung von Hackern und Insidern

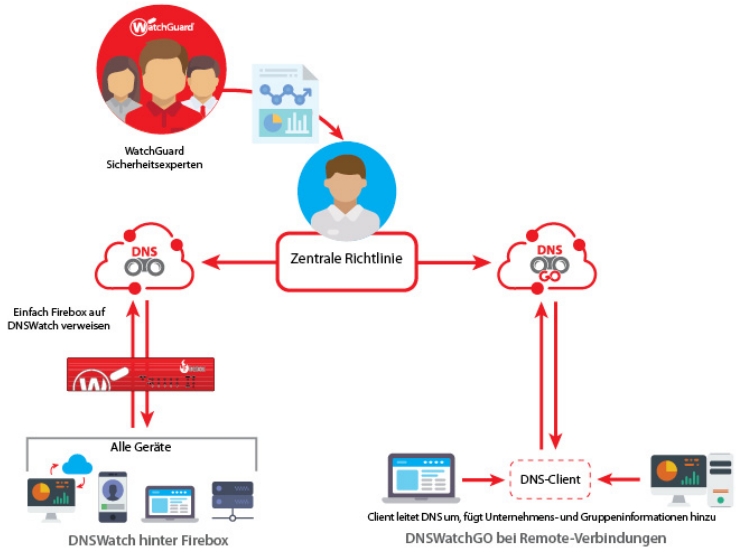
AV-FUNKTIONEN DER NEUESTEN GENERATION

- Persönliche und verwaltete Firewall
- Gerätesteuerung
- URL Filtering
- Anti-Phishing
- Manipulationsabwehr
- Automatisierte Abhilfe
- Möglichkeit für Rollbacks



FUNKTIONSWEISE

WatchGuard DNSWatchGO überwacht ausgehende DNS-Anforderungen und stellt sie einer zusammengestellten Liste böswilliger Sites gegenüber. Als schädlich erkannte Anforderungen werden gesperrt. Die Anwender werden auf eine sichere Site weitergeleitet, auf der sie ihre Kenntnisse zum Thema Phishing auffrischen können.



DIE WATCHGUARD UNIFIED SECURITY PLATFORM™


Netzwerksicherheit


Multifaktor-Authentifizierung


Sicheres, cloud-verwaltetes WLAN


Endpoint-Security

Weitere Informationen erhalten Sie von Ihrem autorisierten WatchGuard-Vertriebspartner oder unter **www.watchguard.de**.

Unterstützte Plattformen und Systemanforderungen für WatchGuard EDPR

Unterstützte Betriebssysteme: Windows (Intel und ARM), macOS (Intel und ARM), Linux und Android.

EDR-Funktionen sind unter Windows, macOS und Linux verfügbar, wobei Windows sämtliche Funktionen uneingeschränkt unterstützt.

Liste kompatibler Browser: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge und Opera.

DEUTSCHLAND, ÖSTERREICH, SCHWEIZ +49 700 92229333 INTERNATIONALER VERTRIEB: +1 206 613 0895 WEB: www.watchguard.de WatchGuard Technologies, Inc.