DATENBLATT

WATCHGUARD 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.

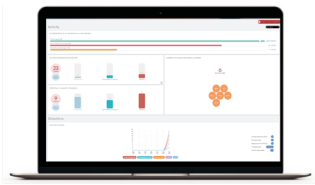
Welche Funktionen sind in Passport enthalten?

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

Panda Adaptive Defense 360 ist eine innovative Cybersicherheitslösung für Desktop-PCs, Laptops und Server, die über die Cloud bereitgestellt wird. Sie kombiniert eine sehr breite Palette an Schutztechnologien (EPP) mit EDR-Funktionen und bietet zwei, in die Lösung eingebundene Services, die von Panda Security-Experten verwaltet werden: Zero-Trust Application Service und Threat Hunting Service.

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 (Samsung/Apple)
  - Gesichtserkennung (Apple)
- 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

- 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

OS SUPPORT

Windows: Workstations – XP, Vista, 7, 8, 8.1, 10 Server – 2003 SP2 und höher, 2008

Linux: Red Hat Enterprise 6.0 und höher, Debian Squeeze, Ubuntu 12 oder höher, Open-Suse 12 oder höher, Suse Enterprise Server 11SP2 oder höher, CentOS 6.x und höher

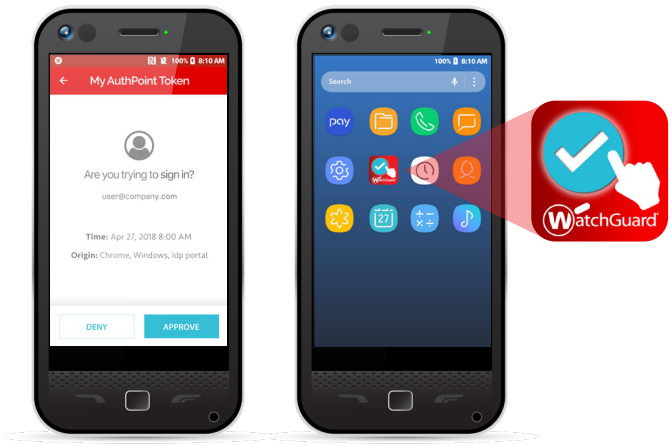
MacOS: 106 Snow Leopard, 10.7 Lion, 10.8 Mountain Lion, 10.9 Mavericks, 10.10 Yosemite, 10.11 El Capitan, Sierra

DETECTION METHODOLOGIES

- Generalist-Signaturen und -Heuristiken
- Cloudbasierter Abgleich mit der Schwarmintelligenz
- IoAs-Erkennung
- Firewall, IDS/IPS
- Manipulationsabwehr
- Gerätesteuerung

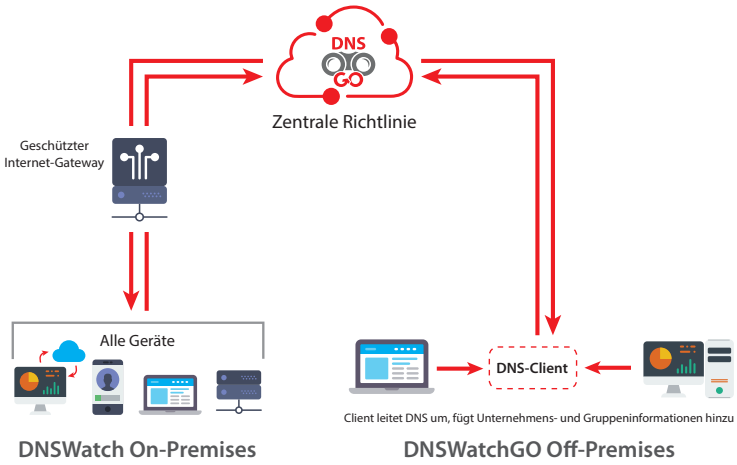
Endpoint-Aktivitätsüberwachung und EDR-Funktionen wie:

- Kontextuelle Verhaltenserkennung
- Anti-Exploit-Technologie für den Arbeitsspeicher
- Zero-Trust Application Service
- Threat Hunting Service



FUNKTIONSWEISE

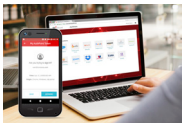
WatchGuard DNSWatchGO überwacht ausgehende DNS-Anforderungen und stellt sie einer zusammengestellten Liste böswilliger Sites gegenüber. Als schädlich erkannte Anforderungen werden gesperrt. Die Anwender werden auf eine sichere Site weitergeleitet, auf der sie ihre Kenntnisse zum Thema Phishing auffrischen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



WATCHGUARD UNIFIED SECURITY PLATFORM™


Netzwerksicherheit


Sicheres WLAN


Multifaktor-Authentifizierung


Endpoint Security

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

Deutschland, Österreich, Schweiz +49 700 92229333 E-MAIL: germanysales@watchguard.com WEB: www.watchguard.de WatchGuard Technologies, Inc.