DATASHEET

PASSPORT™

PERSISTENT, ALWAYS-ON PROTECTION THAT FOLLOWS YOUR USER

Businesses need to be able to extend the security capabilities to users and devices, no matter where they may be. Employees, contractors, visitors, and their devices regularly enter and leave your network as they perform their duties on- and off-premises. At the same time, a single infected endpoint or stolen password could open the floodgates for an attacker. WatchGuard's Passport is a bundle of user-focused security services that travels with your users.

With Passport you can:

1. **Authenticate** people and enforce strong, multi-factor authentication into VPNs, Cloud applications, endpoints and more.
2. **Protect** users on the Internet, block phishing attempts and enforce web policy anywhere, anytime without requiring a VPN.
3. **Prevent**, detect and respond to known and unknown threats, contain ransomware, exploits and any other attack techniques.

MANAGEMENT AND DEPLOYMENT FROM THE CLOUD

Passport is 100% Cloud managed, so there's no software to maintain or hardware to deploy. Viewing reports, alerts, configuring services, deploying endpoint clients, and managing authentication tokens are all done in the Cloud. And, with integration with the leading 3rd party deployment tools, you can be up and running with Passport quickly and easily.

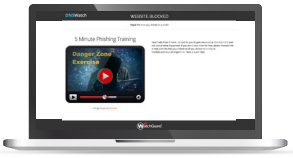
What's included in Passport?

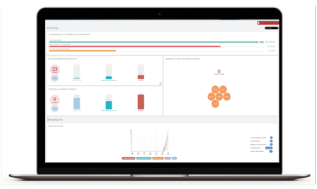
Multi-Factor Authentication

With credential-stealing malware on the rise and new data breaches of usernames and passwords exposed every day, the need for strong authentication has never been greater. WatchGuard AuthPoint lightens the load for you and your customers. AuthPoint uses push messages, QR codes, or one-time passwords (OTPs), in combination with the mobile device DNA of each user's phone to identify and authenticate users.

DNS Protection

As users travel outside the network, visibility into their Internet activity may be lost, creating a significant blind spot in security and leaving them vulnerable to phishing and malware attacks. With DNSWatchGO you gain consolidated visibility into protected devices, no matter their location. When off-network, a host client monitors and correlates outbound DNS requests against an aggregated list of malicious domains. Attempts to communicate with any of these domains will be blocked while the traffic is routed to DNSWatchGO Cloud for further investigation.





Endpoint Security

WatchGuard EPDR is an innovative cybersecurity solution for endpoints and servers, delivered from the Cloud. WatchGuard EPDR combines the widest range of endpoint protection (EPP) technologies with EDR capabilities, automating the prevention, detection, containment, and response to any advanced threat thanks to its two services, managed by WatchGuard security experts and delivered as a feature of the solution: Zero-Trust Application Service and Threat Hunting Service. It also provides the following EPP capabilities: IDS, managed firewall, device control, email protection, URL & content filtering.

PASSPORT

AuthPoint Mobile App

AUTHENTICATION FUNCTIONS

- Push-Based Authentication (online)
- QR Code-Based Authentication (offline)
- Time-Based One-Time Password (offline)

SECURITY FEATURES

- Device DNA signature
- Online Activation with Dynamic Key Generation
- Per authenticator protection
  - PIN
  - Fingerprint (all platforms)
  - Face Recognition (all platforms)
- Self-service, secure authenticator migration to another device
- Jailbreak and root detection

CONVENIENCE FEATURES

- Multi-token support
- 3rd Party Social Media token support
- Customizable Token Name and Picture

SUPPORTED PLATFORMS

- Android v6.0 or higher
- iOS v11.0 or higher

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

OS SUPPORT

- ChromeOS
- Windows 7, 8 and 10

SECURITY FUNCTIONS

- Block phishing attacks
- Prevent C2 connections
- Content filtering
- Deliver immediate security awareness training

VPN SUPPORT

Fully compatible with these WatchGuard Mobile VPN types:

- IKEv2
- L2TP
- SSL/TLS
- IPSec

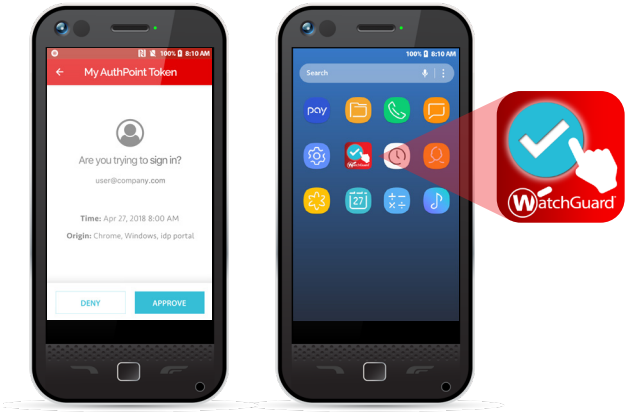
Endpoint Detection and Response

ADVANCED SECURITY TECHNOLOGIES

- Continuous Endpoint monitoring
- Classification of 100% of processes - only trusted applications are allowed to run
- Sandboxing in real environments
- Automatic detection and response for APTs, ransomware, rootkits, etc
- Detection and blockage of in-memory exploits
- Threat Hunting service to detect hackers and insiders

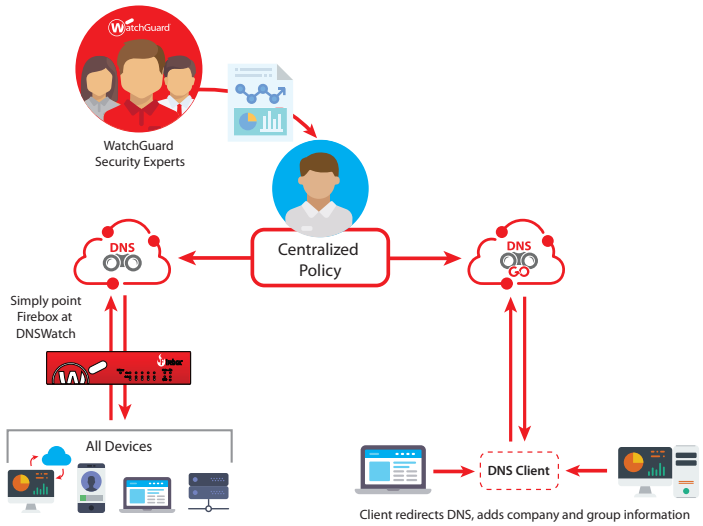
NEXT-GEN AV FEATURES

- Personal or managed firewall
- Device control
- URL filtering
- Anti-phishing
- Anti-tampering
- Automated remediation
- Ability to rollback



HOW IT WORKS

WatchGuard DNSWatchGO monitors outbound DNS requests, correlating them against an aggregated list of malicious sites. Requests that are determined to be malicious are blocked, redirecting the user to a safe site to reinforce their phishing training.



THE WATCHGUARD UNIFIED SECURITY PLATFORM™

Network Security | Multi-Factor Authentication | Secure Cloud Wi-Fi | Endpoint Security

Contact your authorized WatchGuard reseller or visit **www.watchguard.com** to learn more.

Supported platforms and systems requirements of Watchguard EPDR

Supported operating systems: Windows (Intel & ARM), macOS (Intel & ARM), Linux and Android.

EDR capabilities are available on Windows, macOS, and Linux, with Windows being the platform that provides all the capabilities in their entirety.

List of compatible browsers: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge and Opera.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com WatchGuard Technologies, Inc.