DATASHEET

# WATCHGUARD 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.

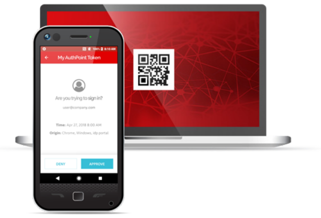
2 **Protect** users on the Internet, block phishing attempts and enforce web policy anywhere, anytime without requiring a VPN.

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.

### Advanced Endpoint Security

Panda Adaptive Defense 360 is an innovative cybersecurity solution for computers, laptops and servers, delivered from the Cloud. It combines the widest range of protection (EPP) technologies with EDR capabilities, providing two services managed by Panda Security experts as a feature of the solution: Zero-Trust Application Service and Threat Hunting Service.

## 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 (Samsung/Apple)
- Face Recognition (Apple)

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 v4.4 or higher

iOS v9.0 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

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
- SSL/TLS
- L2TP
- IPSec

## Endpoint Detection and Response

### OS SUPPORT

**Windows:** Workstations - XP, Vista, 7, 8, 8.1, 10. Servers - 2003 SP2 and later, 2008, 2008 R2, SBS 2011, 2012, 2012 R2, 2016, 2019, Server Core 2008, 2008 R2, 2016, 2019

**Linux**: Red Hat Enterprise 6.0 and later, Debian Squeeze, Ubuntu 12 or later, OpenSuse 12 or later, Suse Enterprise Server 11SP2 or later, CentOS 6.x and later

**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 signatures & heuristics

Cloud-based lookup to the Collective Intelligence

IoAs detection

Firewall, IDS/IPS

Anti-tampering

Device control

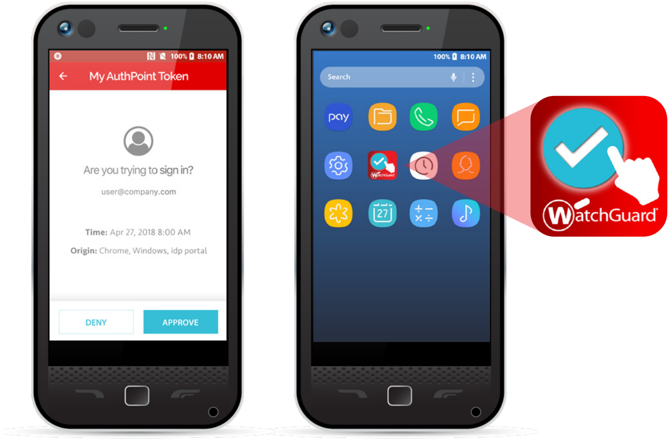
**Endpoint activity monitoring and EDR capabilities such as:**

Contextualized behavior detection

In-memory anti-exploit

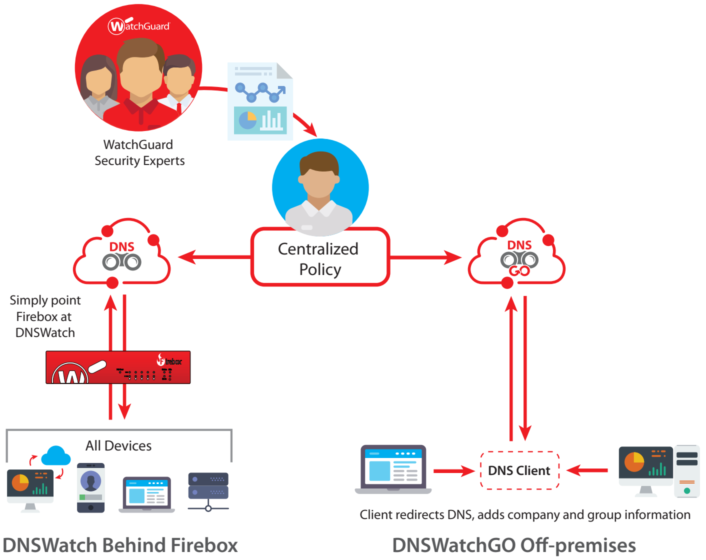
Zero-Trust Application Service

Threat Hunting Service


My AuthPoint Token
Are you trying to sign in?
user@company.com
Time: Apr 27, 2018 8:00 AM
Origin: Chrome, Windows, idp portal
DENY
APPROVE
Search
WatchGuard

## HOW IT WORKS

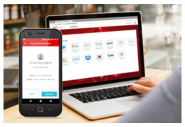
WatchGuard DNSWatchGO monitors outbound DNS requests, correlating them against an aggregated list of malicious sites. Requests that are determined to be malicious are blocked, redirecting the user to a safe site to reinforce their phishing training.


WatchGuard
WatchGuard Security Experts
Centralized Policy
DNS
DNS GO
Simply point Firebox at DNSWatch
Firebox
All Devices
DNS Client
Client redirects DNS, adds company and group information
DNSWatch Behind Firebox
DNSWatchGO Off-premises

## THE WATCHGUARD UNIFIED SECURITY PLATFORM™

Network Security

Secure Wi-Fi



Multi-Factor Authentication

Endpoint Security

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

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