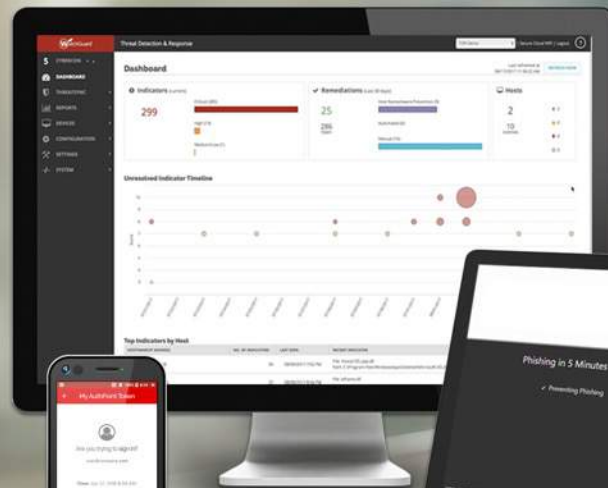
A white commercial airplane is shown in flight, viewed from a low angle. The sky is a mix of orange, yellow, and blue, suggesting a sunset or sunrise. The airplane is moving from left to right across the frame.

Passport – Mit Sicherheit unterwegs



Michael Haas
Area Sales Director Central Europe

It's time for Off-Network Security



Work Locations Are Dramatically Different



Home office



Car



Coffee shop or library



On-site, using guest network



Hotel or restaurant



Customer sites

More and more often, users are not taking advantage of the strong perimeter in the office/site...rather, they perform their jobs from wherever they are.

Recent Survey Results Confirm This Trend



92% of
organizations
allow remote
workers



The average
employee works
remotely more than
2x per week



80% expect
the remote
workforce to grow
over the next
three years.

But...Work Flexibility Comes at a Cost

Despite using common off-network defenses...

90 %

report using some sort of endpoint security solution

88 %

are confident that remote employees use a VPN

85 %

believe that their employees are well-trained enough that they can identify and avoid phishing emails

survey respondents are still concerned.

91 %

state they're concerned that an endpoint could introduce an infection on their network

89 %

are worried that remote employee devices could be accessed by unauthorized parties while off network

64 %

claim a remote worker has been the victim of a cyber attack

Off-network security is a fast-growing market!

Endpoint Security = USD 7B by 2024, 7% CAGR (Gartner Market Insights)

MFA = \$20.4B by 2025, 24% CAGR (Adroit Market Research)

Off-Network Security – Midmarket Businesses



Support safe connections via public networks

Protect from risky clicks

Protect endpoint access

Block endpoint attacks

Prevent network attack from endpoint

Confirm ID to corporate resources

Promote employee productivity

AV, endpoint firewall, VPN

Education

RMM, "Find Device" services

Policy

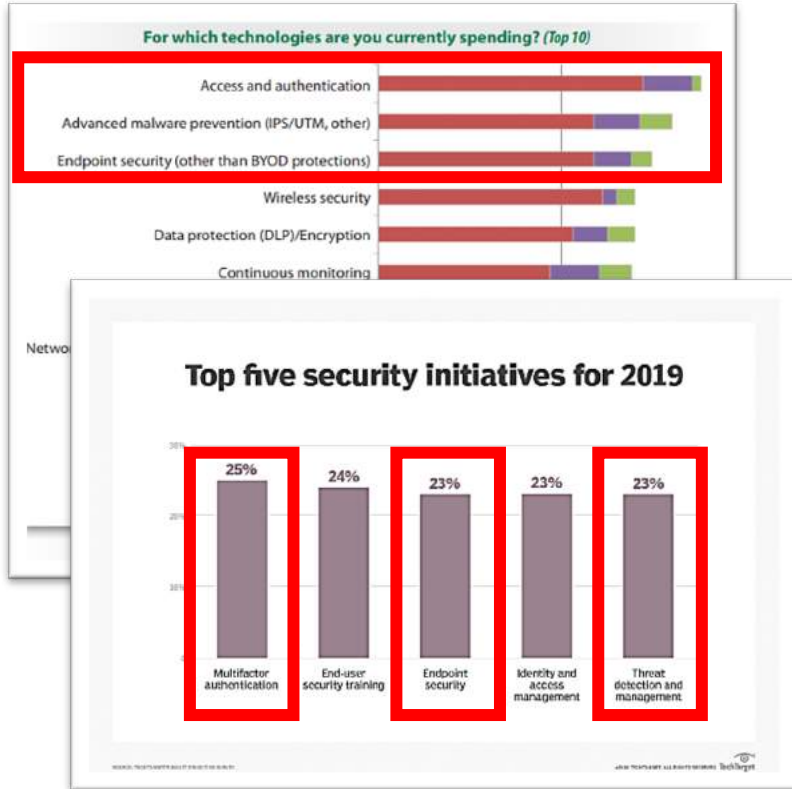
No specific approaches

Education

Not applicable

Current Approach

Customers Are Looking for Solutions



MFA

is THE priority cyber security purchase in 2019/2020

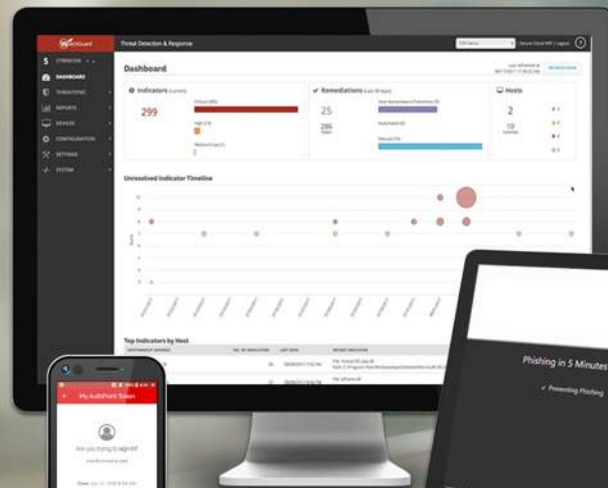
Endpoint

is viewed as the new battleground

Advanced malware

requires advanced protection

Succeeding with WatchGuard





Departures



Arrivals

Terminal

Terminal D
Terminal B
Terminal A
Terminal D
Terminal D
Terminal Z
Terminal B
Terminal D
Terminal A
Terminal A

AF7651AT
DL8611CO
AZ 300AF
51007DL

Rome
Newcastle
Dusseldorf
Berlin
Glasgow

07:40
07:45
07:50
07:55
08:00

24
25
46
47

DELAYED
ON TIME
ON TIME
DELAYED
ON TIME

Terminal A
Terminal A
Terminal A
Terminal B
Terminal D

EK 807
AF1265
CX 605
BA 125
CC9078
33358

Destination	Time	Gate	Remarks
Basel	06:40	11a	ARRIVED
Manchester	06:40	22a	LANDING
Tel Aviv	06:45	31a	LANDING
Brussels	07:00	32a	EXPECTED
Kyiv	07:05	12a	EXPECTED
Vancouver	07:05	41a	EXPECTED
Munich	07:10	14a	EXPECTED
Charlotte	07:15	42a	EXPECTED
Beijing	07:15	33a	EXPECTED
Shanghai	07:15	15a	EXPECTED
Beijing	07:20	23a	DELAYED
Shanghai	07:25	34a	EXPECTED
Beijing	07:40	16a	EXPECTED
Beijing	07:50	24a	EXPECTED
Beijing	07:50	43a	EXPECTED
Beijing	07:55	17a	EXPECTED
Singapore	08:10	18a	EXPECTED
Frankfurt	08:15	19a	EXPECTED
Frankfurt	08:20	11a	EXPECTED
New York	08:20	25a	EXPECTED
New York	08:20	44a	DELAYED
Los Angeles	08:20	44a	EXPECTED
Hong Kong	08:25	26a	EXPECTED
Zurich	08:35	12a	EXPECTED
Sydney	08:45	35a	EXPECTED
Seoul	08:55		
Geneve			
London			

WatchGuard Passport

Passport is an easy-to-buy bundle of user-focused security services.

Each service provides persistent, always-on protection that travels with your user.





Security with a User-Focus



Authenticate people



Protect them on the internet



Keep their endpoints free of malware

Addresses Top Security Concerns...



- ⇒ Phishing
- ⇒ Ransomware
- ⇒ Malware
- ⇒ Weak/Stolen Passwords
- ⇒ Risky-clicks

Top 5 attacks experienced in the past 24 months

Attack	Percent respondents
1. A careless employee fell for a phishing scam that resulted in credential theft	67%
2. A significant disruption to business processes caused by malware	48%
3. A third party misused or shared confidential information with other third parties	41%
4. A cyber attack that caused significant downtime	35%
5. A data breach involving 10,000 or more customer or employee records	41%

Source: *Measuring & Managing the Cyber Risks to Business Operations*, Ponemon Institute & Tenable, December 2018.

Anywhere in the world...



- ⇒ Delivered from the cloud
- ⇒ Lightweight GO client and mobile app
- ⇒ Works on and off-network

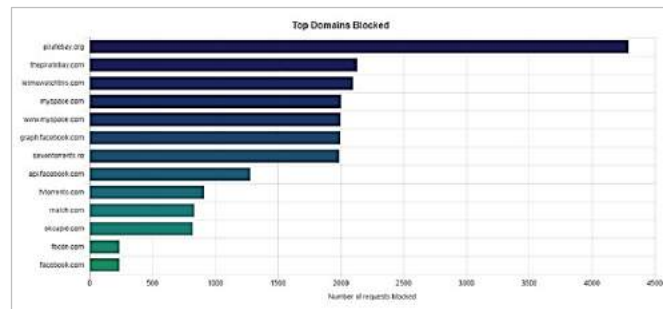


DNSWatchGO



Content Filtering

- ✈️ Keep users safe on the web and block phishing attempts
- ✈️ Gain visibility and enforcement, anywhere
- ✈️ No VPN required



How DNSWatchGO Works...



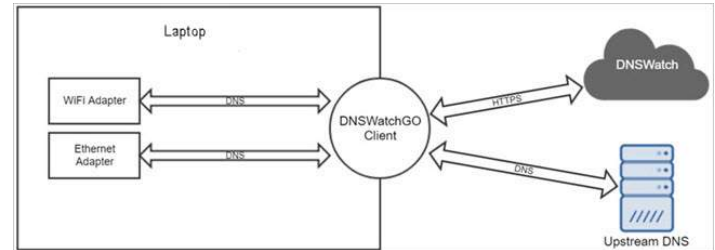
DNSWatchGO listens on localhost port 53 (both TCP and UDP) and intercepts DNS requests.

When it receives a request, DNSWatchGO:

- Sends a query to DNSWatch to determine if the domain is blocked.
- Sends a request for the IP address of the domain to the upstream DNS servers.




After DNSWatch sends the response:

- If the response is block or filter, DNSWatchGO returns the block page.
- If the response is Allow or Whitelist, DNSWatchGO returns the requested content provided by the upstream DNS server.





Establishing Policies



-  Use policies to block domains on protected networks and devices.
-  Use Safe Search option to filter out explicit content in search results.
-  Create multiple policies to meet the needs of different networks.

Create and apply these types of policies:

-  **Protected network or Firebox policy** — This policy is assigned to a protected network to filter requests for content in the specified categories. Fireboxes with DNSWatch enabled are considered to be the same as a protected network for content filter policies.
-  **Client policy** — This policy is used by DNSWatchGO when users are not connected to a protected network. You can allow domains categorized as social media and streaming media for users who are traveling and not on the network but block those domains for users who are on the protected network. You can designate only one policy as the Client Policy.

Default Policy: Austin

Client Policy: Marketing and Sales

UPDATE POLICIES

Manage Policies

Create and manage policies for protected networks and devices.

- Austin** (Default Policy) - Used by 2 networks [EDIT POLICY]
- Boston** - Used by 5 networks [EDIT POLICY]
- Marketing and Sales** (Client Policy) - Used by 0 networks [EDIT POLICY]
- Seattle** - Used by 3 networks [EDIT POLICY]

NETWORK	DESCRIPTION
	SoMa
	Southie
	Fenway
	Back Bay
	Dorchester Heights

No Fireboxes use this policy.

CREATE NEW POLICY



DNSWatchGO Setup: Easy as 1-2-3

Step 1 — Download and install DNSWatchGO Client on a portable device

Step 2 — Create a content filter policy

The content filter policy blocks domains based on content categories.

Step 3 — Test DNSWatchGO protection

With DNSWatchGO installed on a portable device, such as a laptop, users cannot view domains in blocked categories or that appear in the malicious domains feed.

“Does DNSWatchGO work with my VPN?”





DNSWatchGO is compatible with most split tunnel VPNs, and fully compatible with these WatchGuard Mobile VPN types:

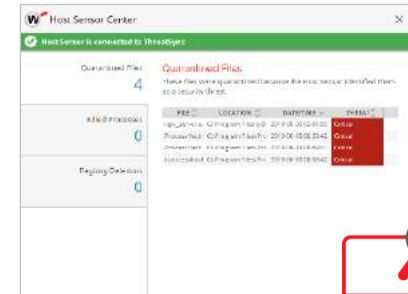
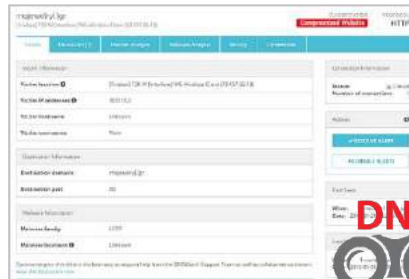
- IKEv2
- SSL/TLS
- L2TP
- IPSec

Endpoint Detection and Response



Endpoint Security

-  Block C&C connections
-  Prevent ransomware file encryption
-  Detect and kill malware
-  Isolate infected hosts



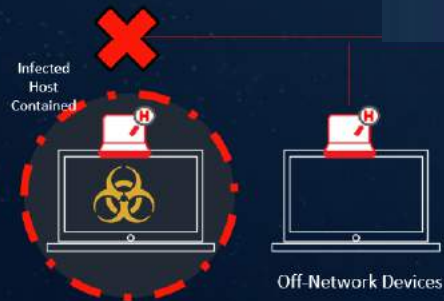
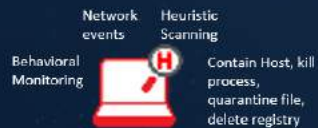
Anywhere in the world...



- ⇒ Delivered from the cloud
- ⇒ Lightweight GO client and mobile app
- ⇒ Works on and off-network






Endpoint Detection and Response



AuthPoint



Multi-Factor Authentication

-  Control access to assets, accounts, and information
-  Authenticate straight from your mobile phone
-  Eliminate the risk of weak or stolen passwords



MFA: How it Works



Passport





How Passport Works...

Passport consist of the lightweight GO client installed on managed endpoints, and the AuthPoint mobile app. All services are managed and deployed from the cloud.



Easy to Buy...



Each License Includes:

- ⇒ Content Filtering
- ⇒ MFA
- ⇒ Endpoint Security*

Bundled = Savings

Cost without Passport for 1 user, 1 year.

€28 AuthPoint

+ €37 DNSWatchGO

+ €51 EDR* (single user TDR host sensor)

= ~€116 - save nearly 33%!

Users	Term	MSRP
5 to 250	1 Year	€78
251 to 1000	1 Year	€62
1001+	1 Year	€49
5 to 250	3 Year	€187
251 to 1000	3 Year	€150
1001+	3 Year	€120

* Coming Soon!

Passport Introductory Promotional Pricing!

- ✈️ All purchasers get a discount on initial purchase of Passport
- ✈️ Promo purchases receive latest product component **no charge** when available
- ✈️ Promotion runs through Q1 of 2020

Users	Term	MSRP	Promo
5 to 250	1 Year	€78	-20%
251 to 1000	1 Year	€62	-20%
1001+	1 Year	€49	-20%
5 to 250	3 Year	€187	-20%
251 to 1000	3 Year	€150	-20%
1001+	3 Year	€120	-20%

Danke

und bleiben Sie gesund!