



Smart Security,  
Simply Done.





A Pioneer in  
Cyber Security  
for Over 20 Years





Introduced DNSWatch  
**2018**

Introduced WatchGuard  
Cloud for MSPs  
**2019**

Introduced AuthPoint MFA  
**2018**

Extended DNS filtering to  
clients off-network with  
DNSWatchGO  
**2019**

Added Advanced  
Endpoint Security  
**2020**

 **Founded** in 1996



**Headquarters:** Seattle, WA



**7** operations centers  
and direct presence  
in **21** countries



**1,200** Employees



**250K+** Customers



**100+** Distributors



**16,000+**  
Active  
Resellers

For over 20 years, WatchGuard has been a pioneer in developing cutting-edge cyber security technology and delivering it as an easy-to-deploy and easy-to-manage solution. With industry-leading network security, secure Wi-Fi, multi-factor authentication, advanced endpoint security and network intelligence products and services, WatchGuard enables more than 250,000 customers from around the globe to protect their most important assets in a world where the cyber security landscape is constantly evolving with new threats emerging each day.

# Smart Security, Simply Done.

## MAKING SENSE OF CYBER SECURITY

Cyber security can be complex, and the technology being deployed to keep up with cyber criminals is only going to get more sophisticated. It is about taking all of these technologies and offering them in a package that is easy to consume for small-to-midsize businesses that are without dedicated security teams. It is about providing the tools and resources that make management simple, while still delivering the level of security your organization requires – both for today and tomorrow. WatchGuard is dedicated to this mission. Everything we do starts with how we are going provide the smartest security in the simplest way.

### SIMPLICITY

Easy and straightforward to purchase, configure, deploy, and centrally manage



### INNOVATION

The quickest access to new and improved security services



### PERFORMANCE

Fastest UTM performance at all price points



### VISIBILITY

Translate oceans of data into actionable information via simple reporting and threat correlation.



### SUPPORT

Industry-leading pre and post sales support for maximum customer and partner satisfaction







Today's business ecosystem relies on Internet access across multiple types of IT environments and locations, each presenting their own challenges in cyber security. Whether you are protecting physical or virtual infrastructures, the network, endpoints, or Wi-Fi environments in one location or spanning multiple offices, WatchGuard enables you to effectively manage security across your entire business.

# Enterprise-Grade Security for Today's Business

# A Layered Defense

Stop the attempted discovery and exploitation of vulnerable systems, delivery of advanced malware, and the exfiltration of your personal information. WatchGuard breaks the Cyber Kill Chain® at each level using layered security and intelligent prevention, detection, and response defenses that shut down targeted attacks.



# Best-in-Class Security Services

WatchGuard offers the most comprehensive portfolio of network security services on the market, from traditional IPS, GAV, application control, spam blocking, and web filtering to more advanced services for protecting against advanced malware, ransomware, and the loss of sensitive data. WatchGuard also offers a full suite of network visibility and management services.

## Fundamental Security Services



### Intrusion Prevention Service (IPS)

Uses continually updated signatures to scan traffic on all major protocols to provide real-time protection against network threats.



### Reputation Enabled Defense Service (RED)

Cloud-based reputation lookup service protects users from malicious sites and botnets, while dramatically improving web processing overhead.



### Application Control

Allow, block, or restrict access to apps based on department, job function, time of day – then see in real time what's being accessed and by whom.



### spamBlocker

Real-time spam detection. Our spamBlocker is so fast and effective, it can review up to 4 billion messages per day.



### WebBlocker URL Filtering

Automatically blocks known malicious sites, with granular content filtering tools to block inappropriate content and increase productivity.



### Network Discovery

A subscription-based service that generates a visual map of all nodes on your network so you can easily see where you may be at risk.



### Gateway AntiVirus (GAV)

Continuously updated signatures identify and block known spyware, viruses, trojans, and more – including new variants of known viruses.

## Advanced Security Services



### APT Blocker – Advanced Malware Protection

Relies on an award-winning next-gen sandbox to detect and stop the most sophisticated attacks including ransomware and zero day threats.



### Threat Detection and Response

Correlate network and endpoint security events using threat intelligence to detect, prioritize and enable immediate action to stop attacks.



### Dimension Command

IT pros gain access to a host of network control features including one-click configuration changes, with access to individual appliances through a web UI and VPN management tools.



### IntelligentAV™

IntelligentAV is a signature-less anti-malware solution that relies on artificial intelligence to automate malware discovery. Leveraging deep statistical analysis, it can classify current and future malware in mere seconds.



### DNSWatch™

Reduce malware infections by blocking malicious DNS requests, redirecting users to information to reinforce security best practices.



## ONE EASY-TO-MANAGE AND COST-EFFECTIVE SOLUTION

All of WatchGuard's security services are delivered as an integrated solution within an easy-to-manage and cost-effective Firebox® appliance that is available as both physical and virtual instances. With WatchGuard, you never have to choose between security and performance. Each Firebox appliance is ready to deliver the full portfolio of security services, along with a suite of management and visibility tools to keep you ahead of the rapidly evolving threat landscape. As new technologies are made available, we enable you to easily upgrade software to incorporate the latest offerings.

---

### EASIER TO PURCHASE

One platform, one package, total security. Our security platform delivers a suite of powerful network, Wi-Fi, and endpoint security services along with the intelligence of correlation and industry-leading performance.

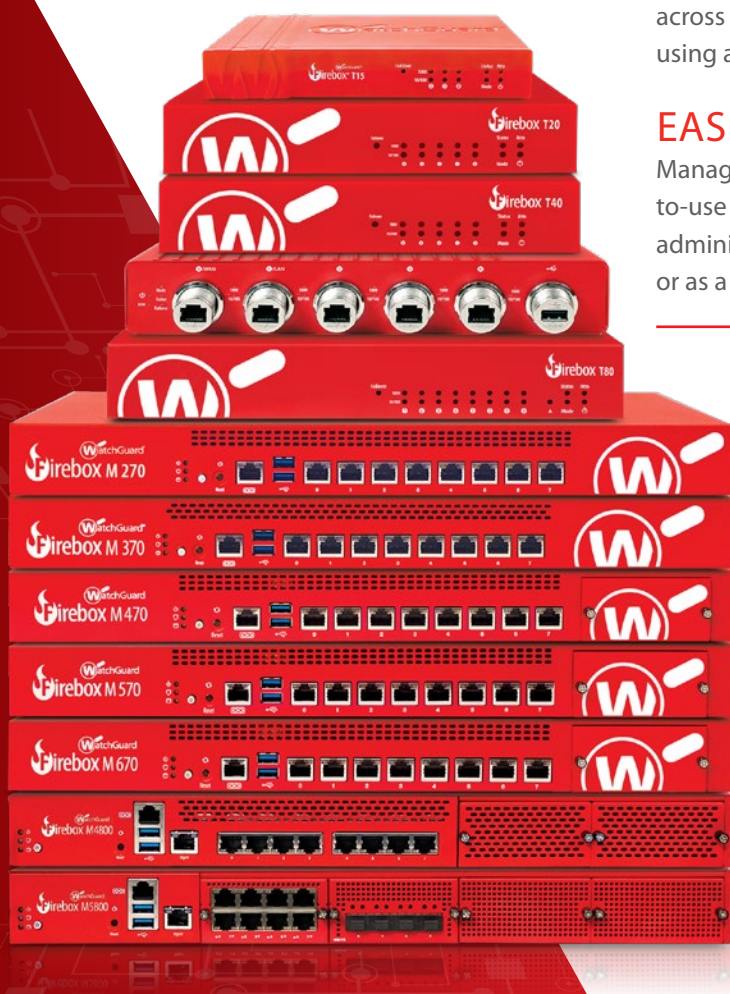
### EASIER TO DEPLOY

Remotely deploy and configure multiple Firebox appliances across a distributed enterprise with minimal on-site assistance using a Cloud-based deployment and configuration tool.

### EASIER TO MANAGE

Manage one Firebox appliance or hundreds from a single, easy-to-use console, maximizing efficiency and streamlining network administration, while applying configuration changes in real time or as a scheduled task.

---



# One Platform, Total Security

# Packaged to Your Needs

Our security service packages allow you to quickly and easily find the right set of features for your business needs today... and tomorrow.

Three packages of security services available on our Firebox T and M Series appliances, as well as our Firebox Cloud and FireboxV virtual models:

In addition to stateful firewalling, the **Support license** includes full VPN capabilities, and built-in SD-WAN.

The **Basic Security Suite** includes all of the traditional network security services typical to a UTM appliance: IPS, antivirus, URL filtering, application control, spam blocking and reputation lookup. It also includes our centralized management and network visibility capabilities, as well as our standard 24x7 support.

The **Total Security Suite** includes all services offered with the Basic Security Suite plus AI-powered malware protection, enhanced network visibility, endpoint protection, Cloud sandboxing, DNS filtering, and the ability to take action against threats right from WatchGuard Cloud, our network visibility platform.

	SUPPORT	BASIC SECURITY	TOTAL SECURITY
Stateful Firewall	✓	✓	✓
VPN	✓	✓	✓
SD-WAN	✓	✓	✓
Access Portal*	✓	✓	✓
Intrusion Prevention Service		✓	✓
Application Control		✓	✓
WebBlocker		✓	✓
spamBlocker		✓	✓
Gateway AntiVirus		✓	✓
Reputation Enabled Defense		✓	✓
Network Discovery		✓	✓
APT Blocker			✓
Threat Detection & Response			✓
DNSWatch			✓
IntelligentAV**			✓
WatchGuard Cloud Visibility Data Retention			30 Days
Support	Standard (24 x 7)	Standard (24 x 7)	Gold (24 x 7)

\*Not available on Firebox T15/T15-W, T20/T20-W, or T35-R. Total Security Suite required for M270, M370, M470, M570, M670

\*\*Not available on Firebox T15/T15-W, T20/T20-W, or T35-R

# Spot Patterns, Make Informed Decisions

## INSTANTLY DISTILL OCEANS OF LOG DATA

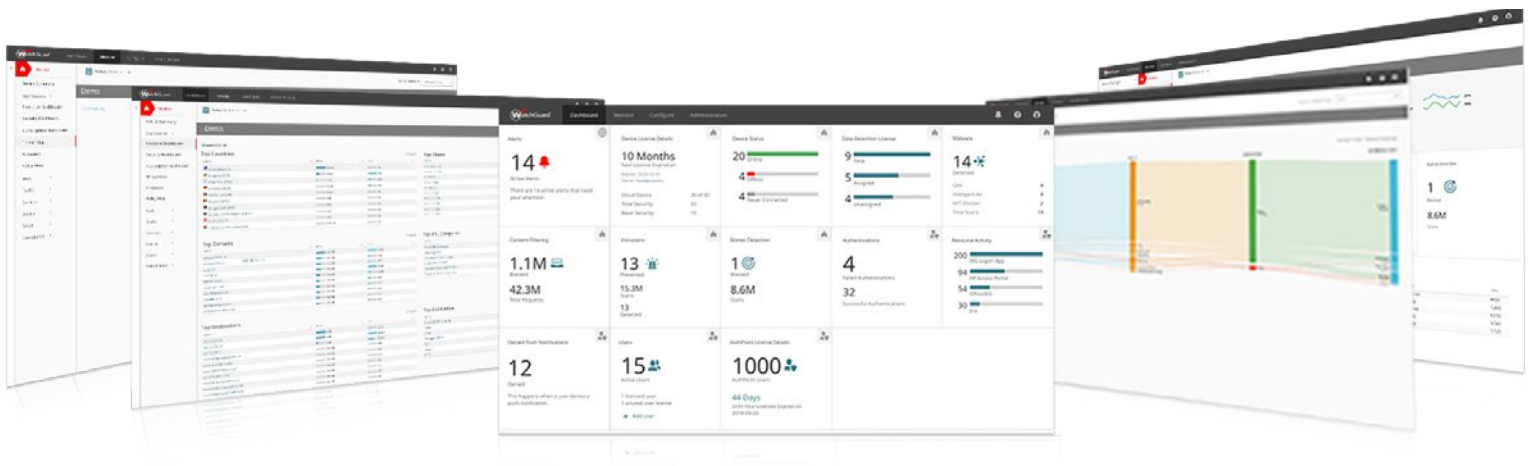
If you can't see what's happening in every corner of your IT infrastructure, you're suffering from blind spots that pose a massive security risk. WatchGuard gives you complete visibility across your network by integrating world-class visualization services into each product, enabling you to see the big picture with over 100 dashboards and reports, as well as the ability drill down for granular details at the log level.

## LEVERAGE REAL-TIME MONITORING

Mitigate risks through proactive monitoring of potential security vulnerabilities and network efficiency issues, while ensuring the effectiveness of security policies. Using a suite of interactive dashboards that deliver real-time data in easy-to-consume visuals, you are able to quickly identify areas of concern with the ability to filter and pivot data to reveal richer details, see how traffic is flowing through your network, which applications and users are consuming the most bandwidth, and much more.

## GENERATE COMPREHENSIVE REPORTS

Get access to a wide range of reports that provide both summary and detailed information on policy usage, compliance demonstration, network and web traffic, security services, engagement and user analytics, and device statistics. Reports can be accessed at any time and scheduled to be auto-delivered for both preventative and corrective actions.



WatchGuard Cloud Visibility



## BRINGING IT ALL TOGETHER

Regardless of the security solutions you have in place, your organization could still be at risk if you're not putting all of your data into context. Correlation takes the mounds of information that these security components produce, and then connects the dots and makes sense of it all. A comprehensive look at both your endpoint and network together provides a better sense of which threats are the most severe.

WatchGuard's ThreatSync is a Cloud-based correlation and threat-scoring engine that improves security awareness and response from across the network to the endpoint. ThreatSync collects network event data from WatchGuard's security

services and correlates it with threat activity from WatchGuard's Host Sensors and enterprise-grade threat intelligence. Through comprehensive analysis of the threat data, you are provided with a threat score and rank of severity.

This proprietary technology not only decreases time to detection by enhancing visibility into threats on both the network and the endpoint, but it ultimately empowers you to quickly and effectively respond. It decreases the time to remediation and provides measurable returns on your investment, while reducing the time and resources required to keep your organization secure.

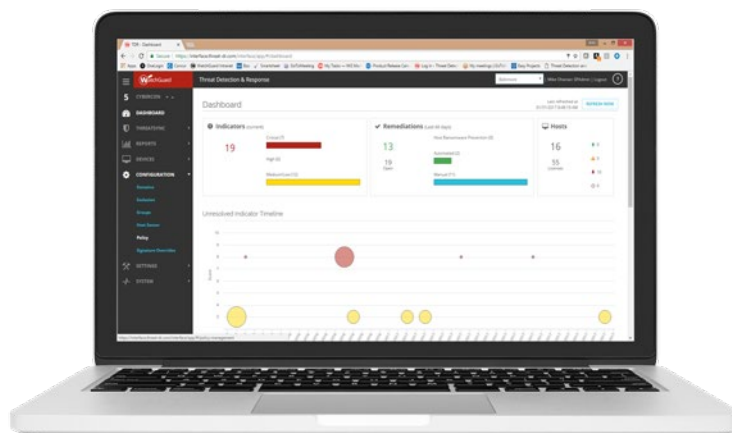
The screenshot displays the WatchGuard Threat Detection and Response interface. It features a sidebar with navigation options like Dashboard, ThreatSync, Reports, and Settings. The main area shows a list of incidents with columns for Source, Host, Score, and Outcomes. A red callout box points to a specific incident, stating: "One comprehensive threat score enables immediate, confident response". Another red callout box points to the "Outcomes" column, stating: "Through policies, incidents can be automatically remediated based on their comprehensive threat score. Any threats not covered via a policy can also be removed through one-click actions." A third red callout box points to the "Indicators" section, stating: "Gain better insight into your overall risk by collecting and analyzing data from both the Firebox and the Host Sensor". A fourth red callout box points to a specific indicator, stating: "Additional information provides greater detail on any signatures or threat feeds leveraged".

WatchGuard Threat Detection and Response

# The Power of Correlation

# Don't Hesitate, Automate

Automation is at the heart of WatchGuard's Unified Security Platform, speeding up processes, killing threats, and empowering IT teams to do more with less. WatchGuard's Automation Core creates a zero-touch security feedback loop and accelerates business-driven security management. The Automation Core makes it possible to seamlessly extend security capabilities to every computing environment where your business operates. It defines an intelligent, autonomous perimeter extending from the LAN, to the Cloud, and ultimately the endpoint to deliver persistent, integrated protection for your business. An Automation Core ensures secure user access to essential resources, blocks advanced threats from entering your network, keeps endpoints free of malware, and optimizes network performance, while requiring minimal interaction from your IT team.



Level 1: Management & Visibility	Signature & Software Updates	Ready-to-Use Reports & Dashboards		Secure Firewall Defaults
Level 2: Operational	Cloud Deployment	License Management	Invoice & Support Ticket Processing	API & Web Service Integration
Level 3: Responsive Security	Behavioral & Statistical Modeling	Remediation	Threat Correlation	Endpoint Isolation
Level 4: Predictive Security	AI-powered Prevention, Detection, Triage, and Remediation			



# The WatchGuard Automation Core delivers:

## SECURITY EFFICACY

- The average Firebox blocked over 2,100 malware variants in 2019, nearly 40% of which were classified as zero day, or completely undetectable by signatures.<sup>1</sup> Each device blocked a further 240 network attacks on average.
- In the NSS Labs testing, WatchGuard was one of just two firewall platforms that had ZERO missed evasions. WatchGuard has achieved the Recommended rating three years running.

## EXTENSIBILITY

- Protect your users from phishing and ransomware, on- and off-network.
- Isolate endpoints and remediate threats anywhere in the world.
- Control access to assets, accounts and information with integrated multi-factor authentication and SSO for centralized access to Cloud-hosted applications, and internal resources via RDP and SSH.
- Seamlessly apply granular policies to users and devices as they transition in and out of the network.

## HIGHER IT STAFF UTILIZATION

- Less time and money spent
- Over 12,000 deployments have used our Cloud deployment service, spending 1/100th the time and cost of a standard device set-up and configuration.
- WatchGuard's powerful visibility tools provide more than 100 dashboards and reports built in, saving hundreds of hours compared with searching through logs for time-sensitive answers on usage and anomalies.
- Using AI, the Firebox platform predicts threats up to 33 months before they appeared in the wild.<sup>2</sup>
- Should attacks find their way to the network, we spot suspicious behaviors early and automatically contain and remediate threats in minutes instead of the months it could exist on your network otherwise.

But we're not done yet! We know that you want a highly automated security experience, where security expertise and up-to-the minute monitoring and security optimizations are built in. Look for more Automation Core advancements to be the hallmark of future product innovation from WatchGuard.

<sup>1</sup> <https://www.watchguard.com/wgrd-resource-center/security-report-q2-2019>

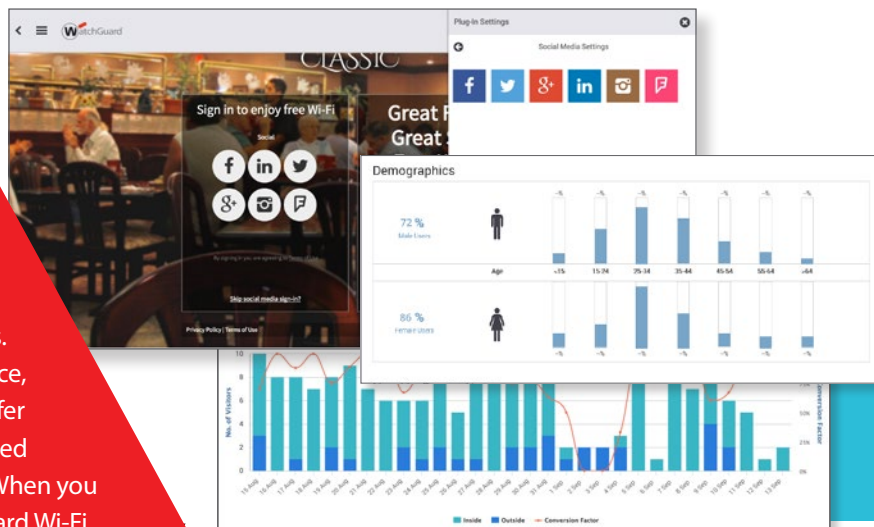
<sup>2</sup> <https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/reports/SELabsPredictiveMalwareResponseTestMarch2018Report.pdf>

# WatchGuard Automation Core



# Secure, Cloud-Managed Wi-Fi

Technology has changed the way everyone does business. Wi-Fi is a necessity that has become all about convenience, security, and performance. WatchGuard doesn't just offer Wi-Fi connectivity, we offer patented security, increased productivity, and improved customer satisfaction. When you deploy a WatchGuard access point with WatchGuard Wi-Fi Cloud enabled, you unlock invaluable tools to take your business to the next level.



## NOT ALL WIPS ARE CREATED EQUAL

WatchGuard's patented Wireless Intrusion Prevention System (WIPS) helps ensure you have the protection you need. WIPS defends your airspace 24/7 from unauthorized devices, man-in-the-middle (MitM) and denial-of-service attacks, rogue APs and more – and with close to zero false positives.

## CAPTIVE PORTALS WITH SOCIAL MEDIA ENGAGEMENT

Get your marketing game on with a suite of easy-to-use, built-in tools that turn a simple wireless connectivity offering into a rich Wi-Fi experience for your customers, guests and employees. Create stunning splash pages without the need for web design skills to engage with visitors using social media authentication, video, polls, and targeted promotions.

## CLOUD MANAGEMENT THAT SCALES

WatchGuard's Wi-Fi Cloud environment can take your business from one to an unlimited number of access points across multiple locations, with no controller infrastructure. Access points can be grouped in many ways including location, building, and floor to maintain consistent policies.

## BUSINESS-DRIVEN ANALYTICS

You can know how, where, and when visitors are using your Wi-Fi so that you can maximize your Wi-Fi investment and optimize the user experience. You will be able to evaluate data around site metrics like footfall, dwell time, and conversion so you can make better business decisions.



Being able to provide fast and secure Wi-Fi to our customers and employees is a must for our business. Plus all the additional capabilities we couldn't live without—engaging with our customers on social media even after they leave our shops and using Wi-Fi Cloud analytics to drive business growth.

~ Jamie Stables, IT Manager, AMT Coffee

# Multi-Factor Authentication with AuthPoint

Using stolen credentials to  
breach network resources is  
the #1 tactic that hackers use\*

\*Verizon Data Breach Investigations Report 2018

“AuthPoint delivers on the promise of MFA by limiting the business risk associated with poor passwords without compromising on ease of use for employees and IT staff alike. Everything in a Cloud service – with no hardware to install and software to maintain... MFA is now considered core protection, and it comes from WatchGuard hassle-free.

*~ Tom Ruffolo, CEO, eSecurity Solutions*

## COMPLETELY CLOUD MANAGED

AuthPoint runs on the WatchGuard Cloud platform and is available from wherever you are. There is no need to install software, schedule upgrades or manage patches. The platform easily accommodates a single global account view or many independent accounts, so that distributed enterprises and managed service providers can display only the data relevant to a person's role.

## EFFECTIVE MFA PROTECTION WITH MOBILE DEVICE DNA

AuthPoint provides a secure MFA product offering 3 ways to authenticate. Furthermore, our mobile device DNA matches the authorized user's phone when granting access to systems and applications. Any attacker attempting to gain access with cloned authentication messages would be blocked when the messages don't originate from the legitimate user's phone.

## EASY-TO-USE AUTHPOINT MOBILE APP

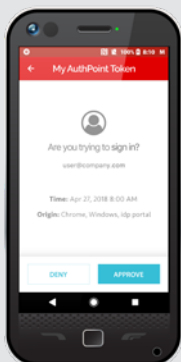
Users can authenticate right from their own phone! No need to carry key fobs or thumb drives; instead install and activate the AuthPoint mobile app in seconds, and it enables speedy push-based authentication as well as offline authentication using QR codes with the phone's camera.

## BROAD COVERAGE WITH WEB SSO

Our ecosystem includes dozens of 3rd party integrations – enabling companies to require users to authenticate before accessing sensitive Cloud applications, web services, VPNs and networks. Moreover, AuthPoint supports the SAML standard, allowing users to log on once to access a full range of applications and services. The secure logon feature provides online and offline authentication to Windows or Mac machines using the AuthPoint app.

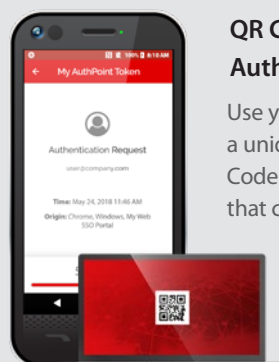


## THREE WAYS TO AUTHENTICATE



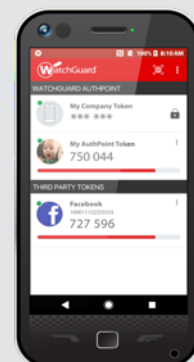
### Push-Based Authentication

Secure authentication with one touch approval. You see who's trying to authenticate, and where, and can block unauthorized access to your resources.



### QR Code-Based Authentication

Use your camera to read a unique, encrypted QR Code with a challenge that can only be read with the app. The response is typed in, to finalize the authentication.



### Time-Based One-Time Password (OTP)

Retrieve your dynamic, time-based, one-time password as displayed, and enter it during login.

# WatchGuard Endpoint Security

Extensible Protection to Prevent, Detect and Respond to Advanced Threats

The endpoint is a favorite target for cyber criminals, with plenty of known vulnerabilities to be exploited, and software versions that are often out of date. These devices are frequently on the Internet without protection from corporate perimeter security, and worse yet, employees can unwittingly enable hackers to make their way onto corporate endpoints and networks. It's past the time when businesses of all sizes need to implement powerful endpoint security that includes endpoint protection (EPP) integrated with advanced endpoint detection and response (EDR) technologies.

WatchGuard's endpoint security platform delivers maximum protection with minimal complexity to take the guesswork out of endpoint security. Our user-centric security products and services offer advanced EPP and EDR approaches with a full suite of security and operations tools for protecting people, devices, and the networks they connect to from malicious websites, malware, spam, and other targeted attacks. Tools to manage patches, remote monitoring encryption and more use the same console to further enhance security. Uniquely powered by automated, AI-driven processes and security analyst-led investigation services, our Panda Adaptive Defense products provide 100% classification, certifying the legitimacy and safety of all running applications – a critical need for any company implementing a zero-trust security model.

## GOOD OR BAD – KNOW WITH 100% CONFIDENCE

Most endpoint security products block what is known to be bad, investigate what is suspicious, and allow what is not known – enabling malware that rapidly morphs to bypass defenses with other unknown traffic. By contrast, the Panda Adaptive Defense products feature a Zero-Trust Application Service that classifies 100% of executables by analyzing all suspicious and unknown processes and applications using special machine-learning algorithms in our Cloud platform, and even verifying with our lab technicians when needed. As a result, all executables are known to be goodware or malware, so that customers receive only confirmed alerts and enjoy the ultimate protection that comes from the default-deny position of a zero-trust model.

# Advanced Endpoint Security

## EXTEND SECURITY, VISIBILITY AND OPERATIONS CAPABILITIES

Panda Adaptive Defense 360 (AD360) is a comprehensive solution, combining next-generation antivirus protection and endpoint detection and response (EDR) as well as the option to add visualization tools, patch management, content filtering, email security, full encryption, and more. Many of these products are also available with other base security offerings, including Panda Endpoint Protection, Endpoint Protection Plus, and Adaptive Defense – allowing customers to create a custom solution that best fits their distinct needs.



WatchGuard acquires Panda Security, June 1, 2020

Both companies have been leading innovators in their respective fields for decades and together deliver a powerful security platform that bridges the network and user perimeter.





## FIND LURKING THREATS WITHOUT ADDING STAFF

Threat hunting usually requires a highly skilled resource and consumes many hours before they detect threats and return the insights that make it clear how to remediate them. Our advanced EDR solutions offer a Threat Hunting service where our security analysts monitor the customer endpoint environment and provide information about potential ongoing attacks including root cause analysis, anomalies detected, relevant IT insights and potential attack surface reduction plans. This is a standard feature that comes with our Adaptive Defense and AD360 products and saves companies from having to allocate IT staff time and energy on investigating infected endpoints themselves.

## ENJOY INTUITIVE, CLOUD-BASED MANAGEMENT

Companies with limited IT staff and security expertise benefit from multi-factor authentication protection that's easy to deploy and manage from the Cloud. AuthPoint runs on the WatchGuard Cloud platform and is available from wherever you are. There is no need to install software, schedule upgrades or manage patches. Moreover, the platform easily accommodates a single global account view or many independent accounts, so that distributed enterprises and managed service providers can display only the data relevant to a person's role.



### A Complete Package with Flexible Options to Meet Every Need

- ✓ Fully Cloud-Native
- ✓ Lightweight Agent

- ✓ Machine Learning Scoring
- ✓ EPP, EDR, Threat Hunting, Zero-Trust Ready



Endpoint Antivirus



Advanced Endpoint Security



Security Operations

Panda Aether Platform and Centralized Security Management



"This multi-tool approach provides increased visibility and holistic reporting, allowing us to identify gaps in our security," says Fourie. Before deploying AD360, BDO had a signature-based solution in place that was unable to detect and block advanced and zero day threats. BDO is now protected against the kind of evasive malware and fileless attacks we see today. "AD360 has allowed us to implement a zero-trust approach, significantly reducing cybersecurity risk,"

~Nico Fourie, BDO National IT director

# What Our Customers Say

“

We chose WatchGuard because it was the only product on the market able to deliver all of the features we required across all of our sites, without breaking the bank to do it.

~ Neil MacGregor, Head of IT, Warren Evans



## Case Studies

“We have improved web security through the use of WatchGuard Reputation Enabled Defense, Application Control and WebBlocker, protecting our users from the growth in potential incoming threats. We also have greater mobility support for laptops and smartphones that is increasingly important....Having been a WatchGuard user for many years I can see no reason to change. Why move to another appliance when the one we have does everything we need and more.”

~ Gary Lovelock, IT Manager, Marshall Amplification



“Our brand is key to our business so ensuring we maintain our prestigious reputation is fundamental. Making sure we have a secure network and protecting our digital assets and databases is paramount... WatchGuard has definitely exceeded our expectations. As well as being great firewalls in terms of what they offer, the improvements continue to arrive with the new releases of firmware. It's very feature-rich and has value-add components – like the System Manager and Dimension – that I'm not aware other vendors bundle with their products. I would definitely recommend WatchGuard to others.”

~ Richard Isted, IT Manager, The Ritz London



“We have found one of the biggest threats to our security is what people bring back on their devices. With a remote workforce in high-risk areas, where cyber attacks are a daily reality, security is a big concern for us. Implementing AD360 and Systems Management has had a significant impact on our business – we now see a more stable and secure environment that is easy to manage through a centralized web console. AD360's capabilities mean we don't have to worry about the devices leaving our network because they are completely protected against zero day attacks.”

- Brandon Kennedy, IT Manager, National Airlines Corporation



## PRODUCT INTEGRATIONS FOR SMARTER SECURITY

WatchGuard partners with industry-leading technology companies to develop tight integrations for stronger security, easier deployments, and better interoperability in your IT environments. From authentication products and service management platforms, to visibility solutions and Cloud services, WatchGuard has you covered, and we continually partner with new companies to offer the most desired and innovative integrations. Each integration is verified and documented with an integration guide for step-by-step configuration.



## A RESELLER FOR YOUR SPECIFIC NEEDS

WatchGuard has the most dedicated and knowledgeable reseller community in the industry. With over 20 years of building the most elite channel base, WatchGuard provides customers with the exact partner they need to ensure success from the start.

Whether you are looking for a general reseller, or you are in need of end-to-end service management on top of your purchase, we will help you find the perfect choice. Our WatchGuardONE program ensures that each partner is trained, certified, and equipped to be your security expert.



A Dedicated  
Channel of  
Certified  
Partners





## PROTECT YOUR BUSINESS • PROTECT YOUR ASSETS • PROTECT YOUR PEOPLE

Cyber security is more relevant than ever before. The number of worldwide cyber attacks are at an all-time high with no signs of slowing down, as small to midsize businesses continue to fall victim with serious impact to their business operations and continuity. WatchGuard is here to provide the layered protection you need against the most advanced types of malware, and deliver it in way that is simple to maintain. You face the same threats as enterprise organizations, shouldn't you have the same level of security?

### **Global Headquarters United States**

Tel: +1.206.613.6600  
Email: [sales@watchguard.com](mailto:sales@watchguard.com)

### **European Headquarters The Netherlands**

Tel: +31(0)70.711.20.85  
Email: [sales-benelux@watchguard.com](mailto:sales-benelux@watchguard.com)

### **APAC & SEA Headquarters Singapore**

Tel: +65.3163.3992  
Email: [inquiry.sea@watchguard.com](mailto:inquiry.sea@watchguard.com)



©2020 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, DNSWatch, IntelligentAV, Firebox, and Dimension are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE67006\_110220