Leap into a Unified Future

Cut complexity.
Evolve your security practice.
Fuel your business.

Agenda

Welcome

Unified Security Platform

Clarity and Control

BREAK

Comprehensive Security

Shared Knowledge

Operational Alignment

Automation

Q & A

Lack of a unified cybersecurity strategy is the #1 reason organizations fall victim to a ransomware attack.

-Powered by Pulse

Complex and Disconnected Security Leads to Breaches

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
June 4, 2021, 12:58 PM PDT

Colonial Pipeline paid a ransom of nearly $5 million.

"In the case of this particular ***legacy VPN****, it* ***only had single-factor authentication****,"*
Joseph Blount, Chief Executive, Colonial Pipeline

Florida water hack highlights risks of remote access work without proper security

By Eric Levenson, CNN
Updated 4:08 AM ET, Sat February 13, 2021

Remote access exploited to increase the level of lye in the water supply 11x.

11 credential pairs linked *to the Oldsmar water plant* ***found in a 2017 compilation of stolen breach credentials.***

The 6th-largest school district in the US was hacked, and the hackers threatened to post student and teacher data online if a $40 million ransom wasn't paid

AP Terry Spencer , Associated Press Apr 1, 2021, 1:28 PM

Hackers demanded $40 million to return stolen school district data.

After not receiving payment, ***hackers published 25,971 district files*** *dating all the way back to 2012.*

62% of midmarket organizations report that their
IT environments are more complex now than two years ago.

What Do MSPs Think It Takes to Unify Security?

We collaborated with Pulse to find out.

Pulse is a social research platform trusted by technology leaders around the world. These executives rely on the community to make connections, share knowledge, get advice, and stay on top of current trends in the technology space.

95%

of MSPs believe their team loses productivity and efficiency switching between different product interfaces to manage their client’s security

91% of MSPs believe Cloud-based solutions and single pane of glass are required to productize services.

-Powered by Pulse

96% of MSPs are currently in the process of consolidating vendors or planning to start the process in 2021/2022.

-Powered by Pulse

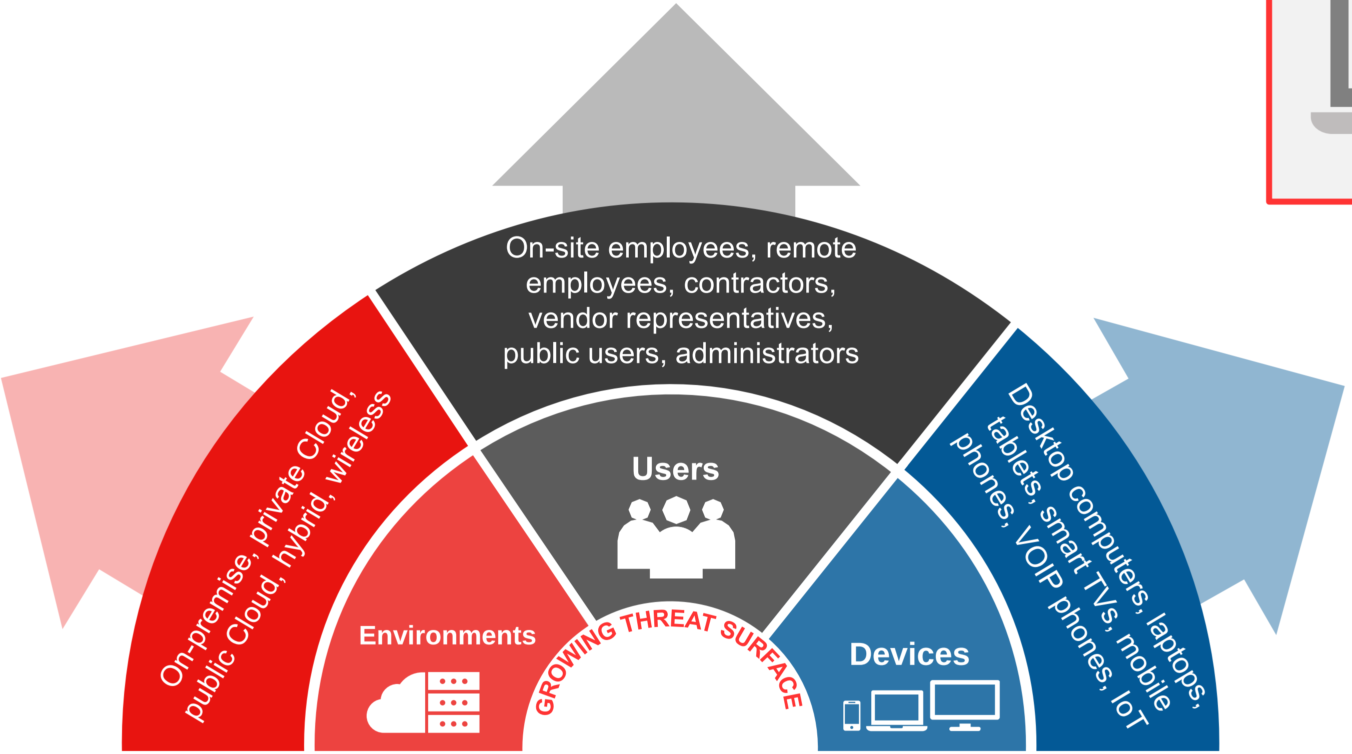
81% of MSPs consider management and configuration from a single-pane-of-glass a unified security platform

Only 19% also include sharing security insights across products and automated response to incidents

True Unified Security Is More Than Just Vendor Consolidation and Centralized Management

It’s Not Security Unless It’s Effective At Scale

The number of network environments, users, devices, and connections is exploding


On-site employees, remote employees, contractors, vendor representatives, public users, administrators
Users
On-premise, private Cloud, public Cloud, hybrid, wireless
Environments
GROWING THREAT SURFACE
Desktop computers, laptops, tablets, smart TVs, mobile phones, VOIP phones, IoT
Devices

Yesterday’s security platforms cannot provide the seamless oversight, comprehensive security, shared knowledge, automation and operational alignment necessary for effective security delivery today.

- ✗ Oversight is fragmented by multiple management solutions and/or missing SIEM feeds
- ✗ Specialized solutions from multiple vendors limit insights and compromise security efficacy across all environments
- ✗ Restrictive business terms and manual processes introduce friction with subscription-based service delivery models, placing security, reputation, CSAT and company profits at risk

You’ve been trying to force security technology to fit into your business practices for far too long. You deserve better.

A Scalable Platform for Elevating the Practice of Modern Security Delivery

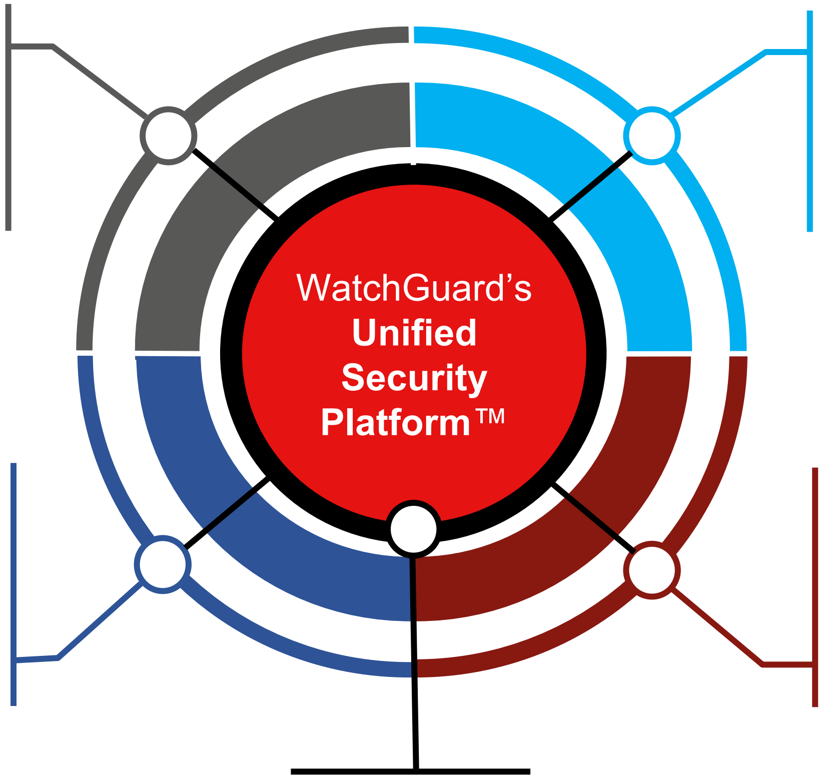
WatchGuard’s Unified Security Platform

COMPREHENSIVE SECURITY

A complete portfolio of security products and services for protecting environments, users, and devices.

CLARITY & CONTROL

Centralized security policy management, threat remediation, visibility, and reporting to streamline security administration.



OPERATIONAL ALIGNMENT

Direct API access, hundreds of out-of-the-box integrations, and support for all payment and consumption models for streamlined business operations.

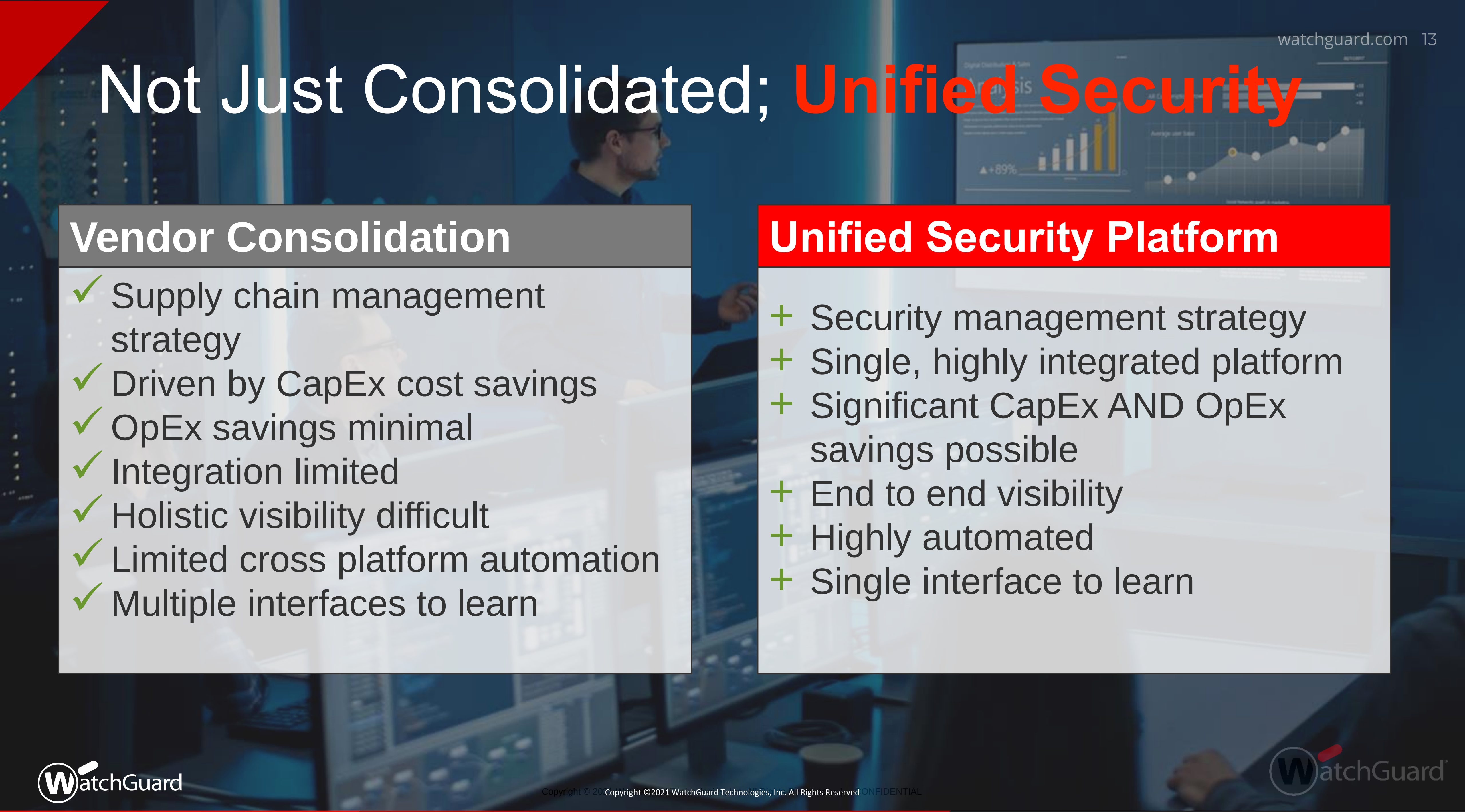
SHARED KNOWLEDGE

A fully integrated platform for adopting a zero-trust, identity-based security posture and deploying a true XDR-based approach to threat detection and remediation.

AUTOMATION

Business and security automation built into each layer of the platform to simplify every aspect of security consumption, delivery, and management.

Not Just Consolidated; Unified Security



Vendor Consolidation

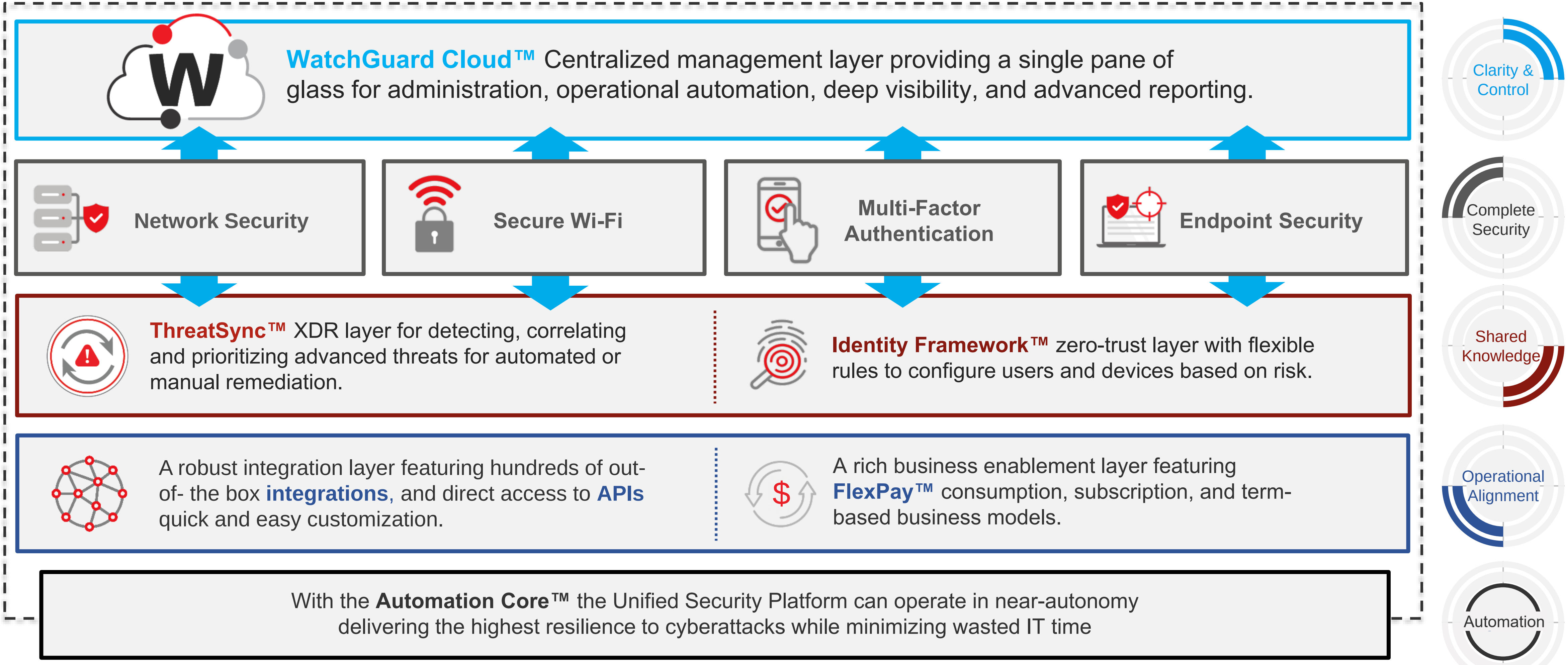
- ✓ Supply chain management strategy
- ✓ Driven by CapEx cost savings
- ✓ OpEx savings minimal
- ✓ Integration limited
- ✓ Holistic visibility difficult
- ✓ Limited cross platform automation
- ✓ Multiple interfaces to learn

Unified Security Platform

- + Security management strategy
- + Single, highly integrated platform
- + Significant CapEx AND OpEx savings possible
- + End to end visibility
- + Highly automated
- + Single interface to learn

Empowers MSPs to Leap to Advanced, User-Centric Security

WatchGuard’s Unified Security Platform



WatchGuard Cloud™ Centralized management layer providing a single pane of glass for administration, operational automation, deep visibility, and advanced reporting.

Network Security

Secure Wi-Fi

Multi-Factor Authentication

Endpoint Security

ThreatSync™ XDR layer for detecting, correlating and prioritizing advanced threats for automated or manual remediation.

Identity Framework™ zero-trust layer with flexible rules to configure users and devices based on risk.

A robust integration layer featuring hundreds of out-of- the box **integrations**, and direct access to **APIs** quick and easy customization.

A rich business enablement layer featuring **FlexPay™** consumption, subscription, and term-based business models.

With the **Automation Core™** the Unified Security Platform can operate in near-autonomy delivering the highest resilience to cyberattacks while minimizing wasted IT time

Clarity & Control

Complete Security

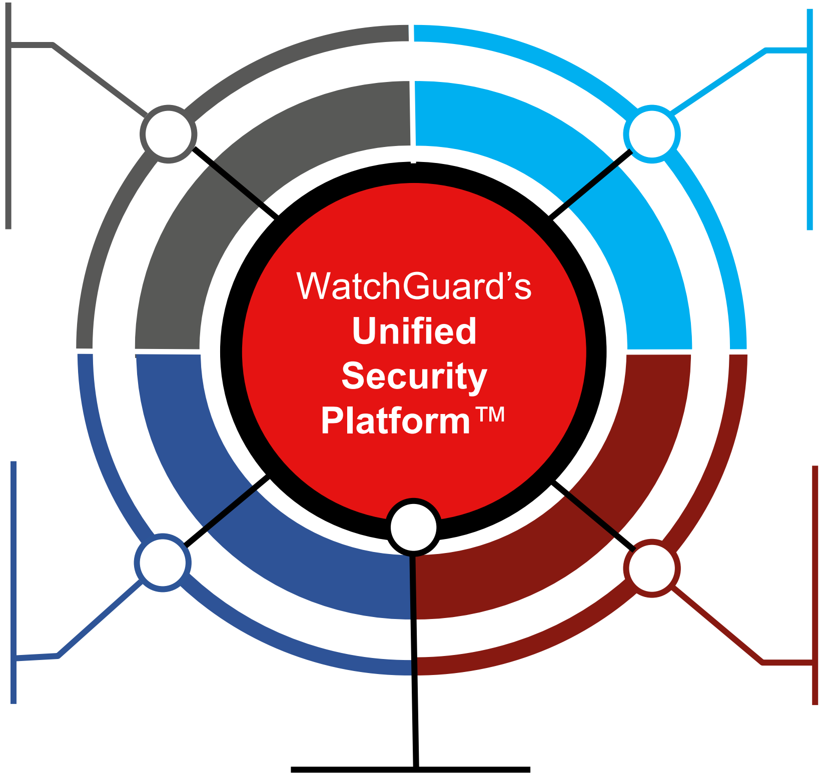
Shared Knowledge

Operational Alignment

Automation

WatchGuard’s Unified Security Platform

A scalable platform for elevating the practice of modern security delivery.



COMPREHENSIVE SECURITY

A complete portfolio of endpoint, multi-factor authentication, and network security products and services for protecting environments, users, and devices.

CLARITY & CONTROL

Centralized security administration, visibility, and advanced reporting via WatchGuard Cloud™.

OPERATIONAL ALIGNMENT

Simplified business operations with direct API access, a rich ecosystem of out-of-the-box integrations, and support for all payment and consumption models via FlexPay™.

SHARED KNOWLEDGE

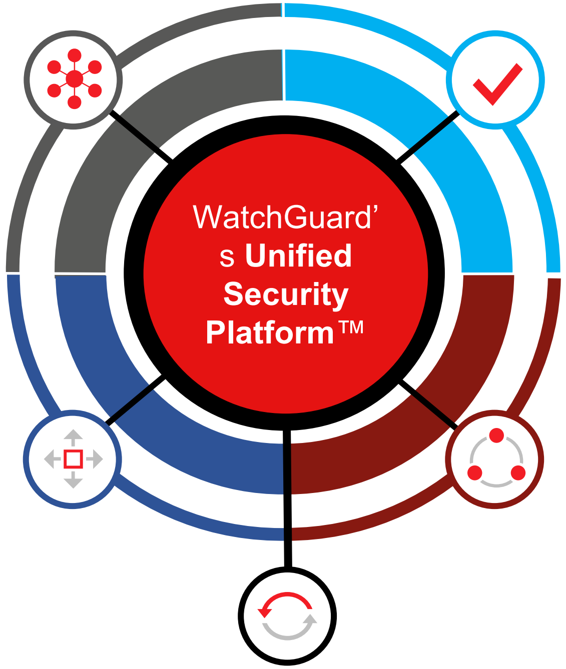
A fully integrated platform for adopting a zero-trust security posture via WatchGuard’s Identity Framework™ and deploying a true XDR-based approach to threat detection and remediation via ThreatSync®.

AUTOMATION

WatchGuard’s Automation Core™ brings simplification and scale to every aspect of security consumption, delivery, and management.

A Purpose-Built Platform for MSPs

MSP PRIORITY	WATCHGUARD DIFFERENTIATION
BREADTH & RELEVANCE OF PORTOFLIO	A complete portfolio of endpoint, multi-factor authentication, and network security products and services for protecting environments, users, and devices.
EASE OF ADMINISTRATION	WatchGuard Cloud is a centralized security administration, visibility, and advanced reporting hub acting as a single pane of glass for MSP partners
ENABLE THE S in MSSP	A fully integrated platform for adopting a zero-trust security posture via WatchGuard’s Identity Framework and deploying a true XDR-based approach to threat detection and remediation via ThreatSync.
PROCESS AUTOMATION	WatchGuard’s Automation Core brings simplification and scale to every aspect of security consumption, delivery, and management.
BUSINESS MODEL FLEXIBILITY	Simplified business operations with direct API access, a rich ecosystem of out-of-the-box integrations, and support for all payment and consumption models via FlexPay.



Throughout 2021, We’ve Advanced Our Unified Security Platform

In the next sessions, we’ll outline how our most recent product and platform enhancements have put the Unified Security Platform into motion.

Our future releases will continue elevate this platform built to enable and differentiate our MSPs services and capabilities.

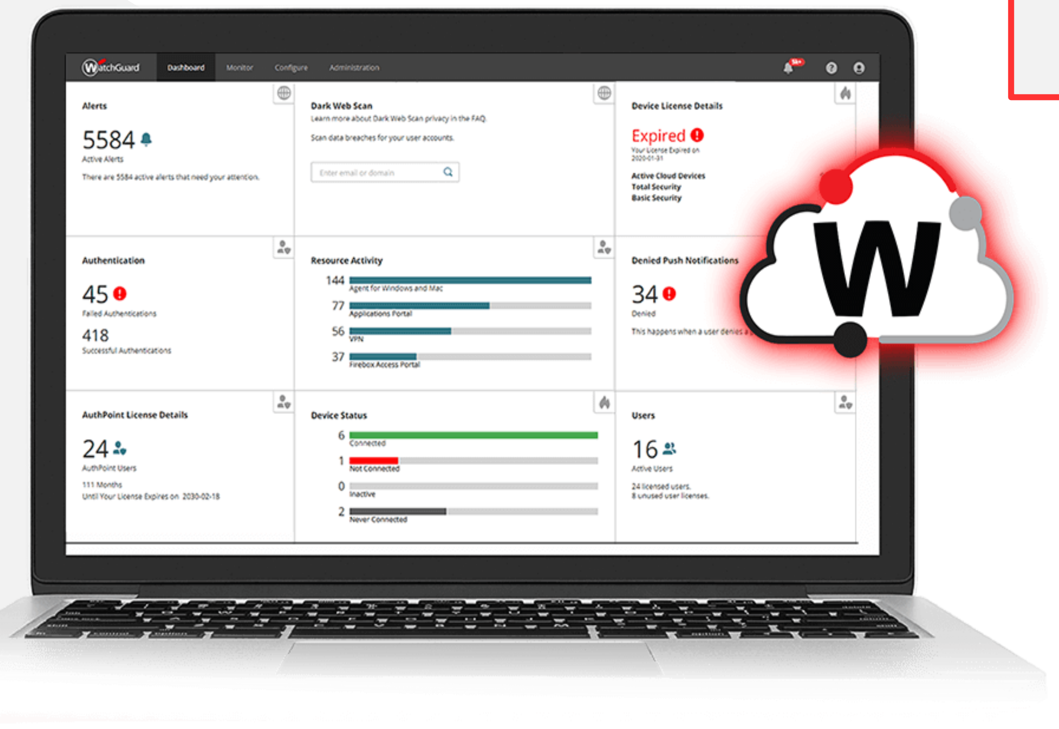
Clarity and Control

Clarity &
Control

Centralized Control with WatchGuard Cloud™

Clarity & Control

WatchGuard Cloud is the centralized management interface for the entire Unified Security Platform and is the central authority for security policy management, dissemination, and enforcement.



Alerts

5584

Active Alerts

There are 5584 active alerts that need your attention.

Dark Web Scan

Learn more about Dark Web Scan privacy in the FAQ.

Scan data breaches for your user accounts.

Enter email or domain

Device License Details

Expired

Your License Expired on 2020-01-31

Active Cloud Devices

Total Security

Basic Security

Authentication

45

Failed Authentications

418

Successful Authentications

Resource Activity

144 Agent for Windows and Mac

77 Applications Portal

56 VPN

37 Firebox Access Portal

Denied Push Notifications

34

Denied

This happens when a user denies a

AuthPoint License Details

24

AuthPoint Users

111 Months

Until Your License Expires on 2030-02-18

Device Status

6 Connected

1 Not Connected

0 Inactive

2 Never Connected

Users

16

Active Users

24 licensed users.

8 unused user licenses.

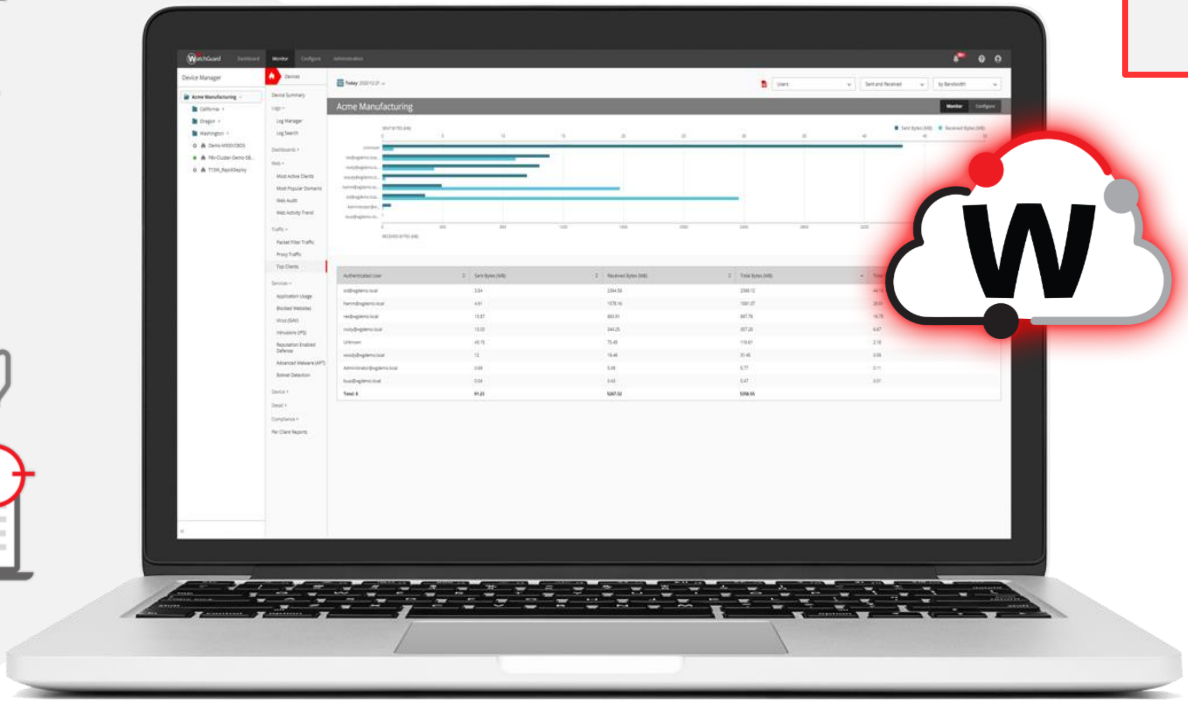
Management for the MSP:

- Multi-tier, multi-tenant architecture
- Quickly enable or disable security services for clients
- Zero-touch deployment of network security, MFA and endpoint security
- Minimize alert fatigue and stay ahead of threats with automation
- Integration with leading RMM and PSA tools

Superior Clarity with WatchGuard Cloud™

Clarity & Control

Easily identify actionable security trends, monitor security service efficacy, and generate business, compliance, and security reports with stunning visualization tools right from WatchGuard Cloud. Choose from over 100 comprehensive reports and dashboards.



Actionable Visibility:

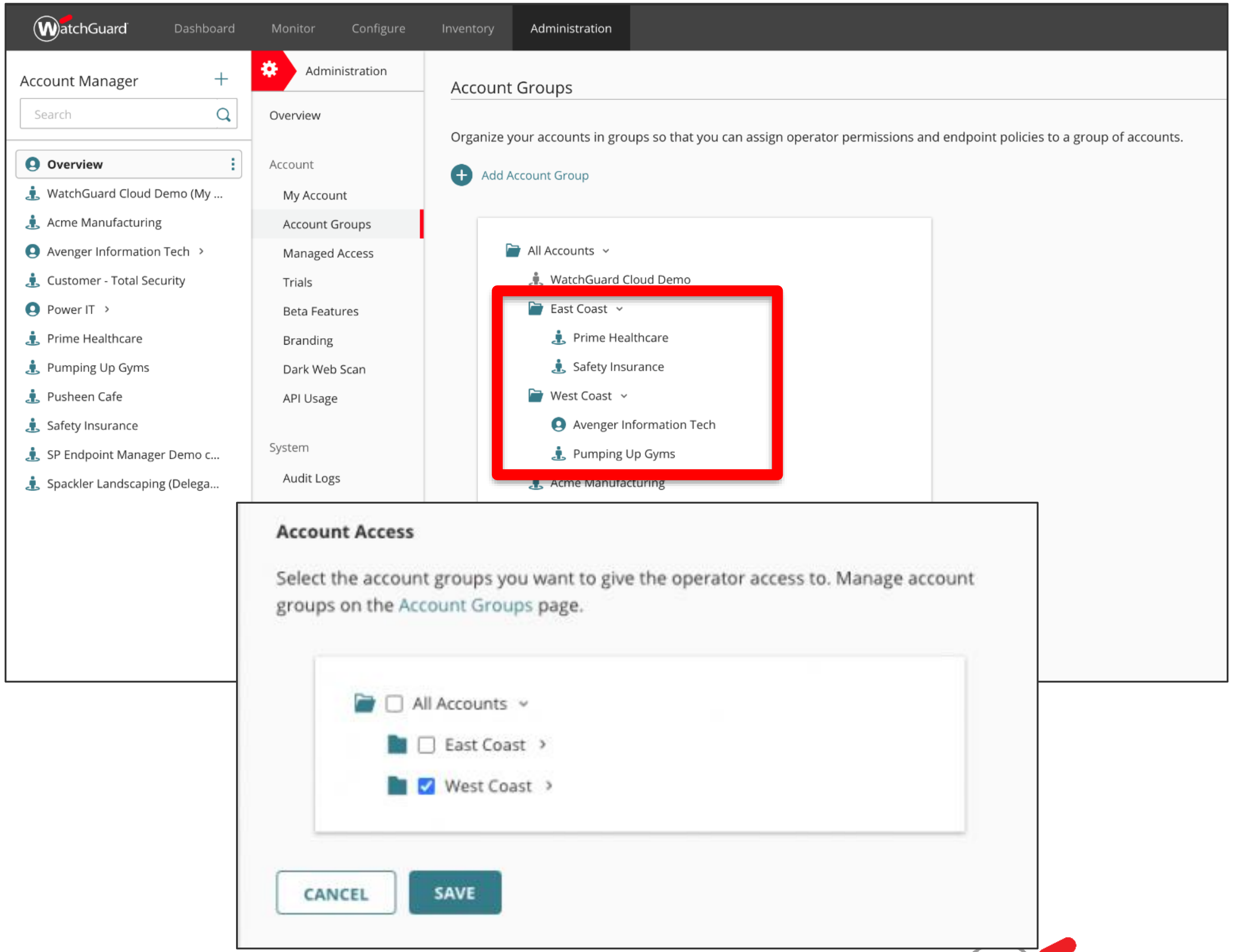
- Summary views of each security layer via the Dashboard
- Quickly identify issues and drill down to services
- Instant access to key findings across terabytes of data
- Make your value visible with custom, automated reports

Organize and Secure Accounts with Account Groups

Clarity & Control

- Quickly organize accounts into folders based on customer characteristics
    - Enforce segregation of duties.
    - Create groups with existing managed accounts
    - Quickly apply policies to groups of accounts

- Account groups can be used to assign operator permissions.
    - Restrict access for operators with Helpdesk and Auditor roles to specific groups of managed accounts.

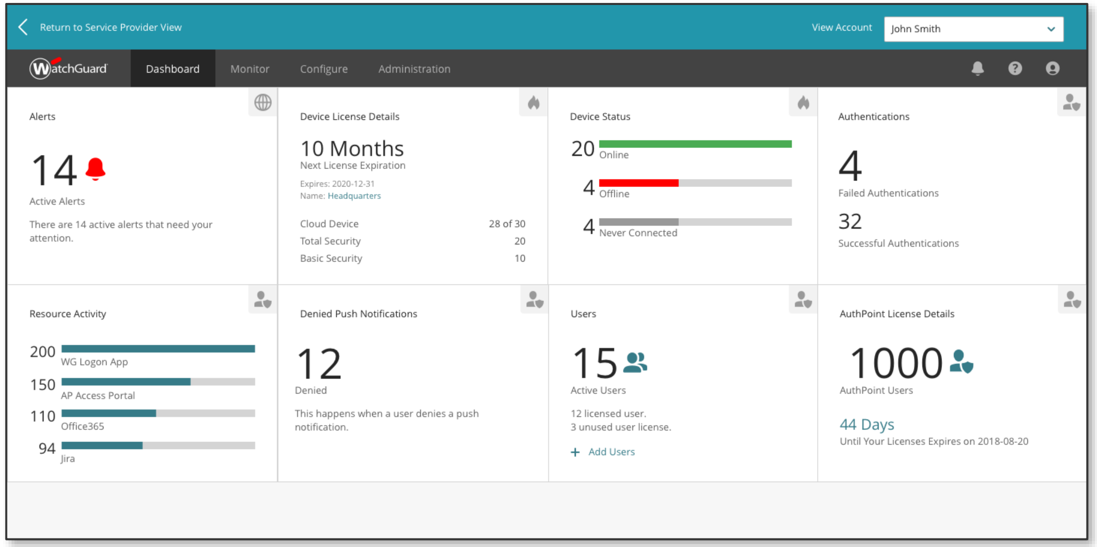


Organize your accounts in groups so that you can assign operator permissions and endpoint policies to a group of accounts.

Select the account groups you want to give the operator access to. Manage account groups on the Account Groups page.

Demonstrate your value to your customers – Easily!

Clarity & Control



Alerts

14

Active Alerts

There are 14 active alerts that need your attention.

Device License Details

10 Months

Next License Expiration

Expires: 2020-12-31

Name: Headquarters

Cloud Device	28 of 30
Total Security	20
Basic Security	10

Device Status

20 Online

4 Offline

4 Never Connected

Authentications

4

Failed Authentications

32

Successful Authentications

Resource Activity

200	WG Logon App
150	AP Access Portal
110	Office365
94	Jira

Denied Push Notifications

12

Denied

This happens when a user denies a push notification.

Users

15

Active Users

12 licensed user.
3 unused user license.

+ Add Users

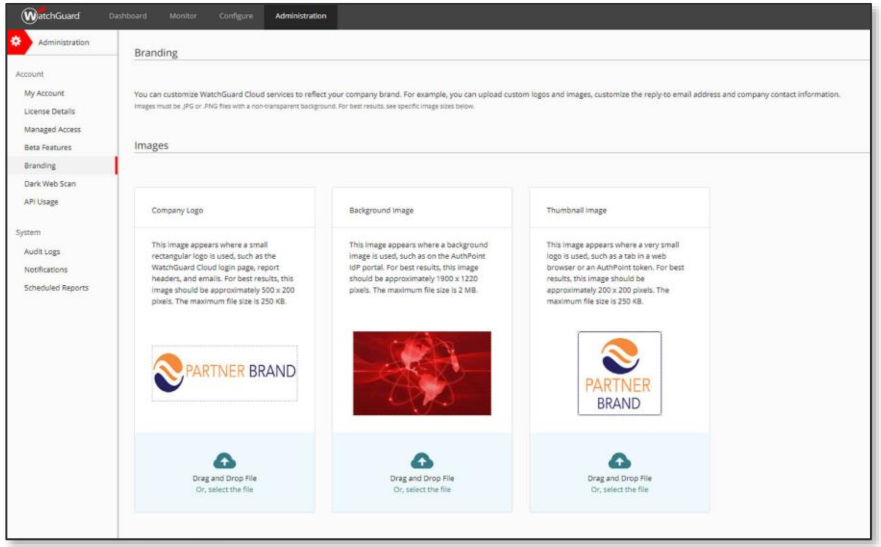
AuthPoint License Details

1000

AuthPoint Users

44 Days

Until Your Licenses Expires on 2018-08-20



Branding

You can customize WatchGuard Cloud services to reflect your company brand. For example, you can upload custom logos and images, customize the reply-to email address and company contact information.

Images must be .JPG or .PNG files with a non-transparent background. For best results, see specific image sizes below.

Images

Company Logo

This image appears where a small rectangular logo is used, such as the WatchGuard Cloud login page, report headers, and emails. For best results, this image should be approximately 500 x 200 pixels. The maximum file size is 250 KB.

Background Image

This image appears where a background image is used, such as on the AuthPoint IdP portal. For best results, this image should be approximately 1900 x 1220 pixels. The maximum file size is 2 MB.

Thumbnail Image

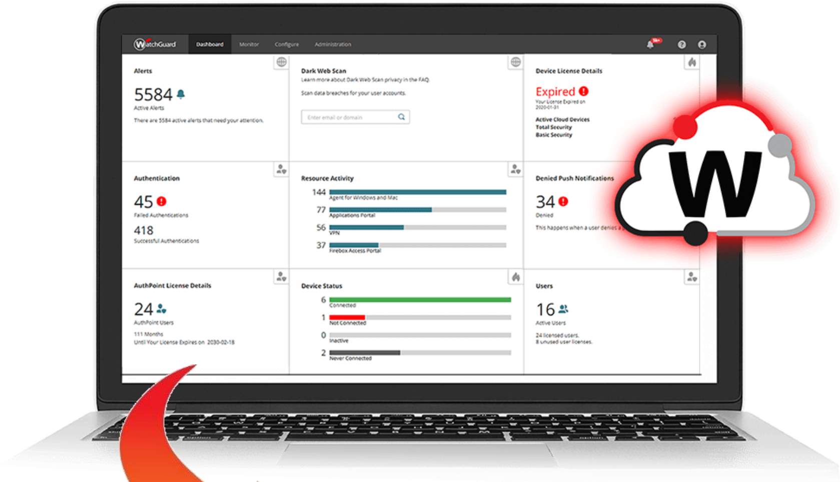
This image appears where a very small logo is used, such as a tab in a web browser or an AuthPoint token. For best results, this image should be approximately 200 x 200 pixels. The maximum file size is 250 KB.

- Aggregated reports and logs
- Simultaneous account access for both partners and customers
- Clear, easy-to-download reports
- Easy way to differentiate yourself

- Easily add your company logo, images, and contact information to emails and reports, and identity portals to reinforce your brand
- Build trust by pointing customers to your support team.

Centralized Firebox Management in WatchGuard Cloud

Clarity & Control



Alerts
5584
Active Alerts
There are 5584 active alerts that need your attention.

Dark Web Scan
Learn more about Dark Web Scan privacy in the FAQ.
Scan data breaches for your user accounts.
Enter email or domain

Device License Details
Expired
Your License Expired on 2020-01-31
Active Cloud Devices
Total Security
Basic Security

Authentication
45
Failed Authentications
418
Successful Authentications

Resource Activity
144 Agent for Windows and Mac
77 Applications Portal
56 VPN
37 Firebox Access Portal

Denied Push Notifications
34
Denied
This happens when a user denies a

AuthPoint License Details
24
AuthPoint Users
111 Months
Until Your License Expires on 2030-02-18

Device Status
6 Connected
1 Not Connected
0 Inactive
2 Never Connected

Users
16
Active Users
24 licensed users.
8 unused user licenses.

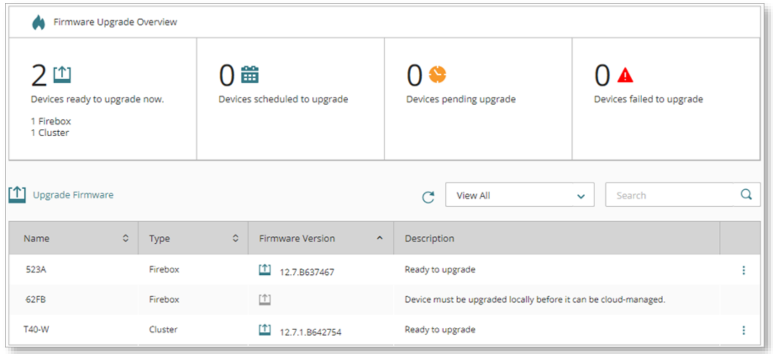
Firebox®

- ✓ Centralize policy enforcement
- ✓ Configure the entire network
- ✓ Deploy firewalls remotely
- ✓ Automate reporting to stakeholders
- ✓ Schedule firmware upgrades
- ✓ Lead with your brand

WatchGuard®

New Fireware Management

Clarity & Control



Firmware Upgrade Overview

2 Devices ready to upgrade now.
1 Firebox
1 Cluster

0 Devices scheduled to upgrade

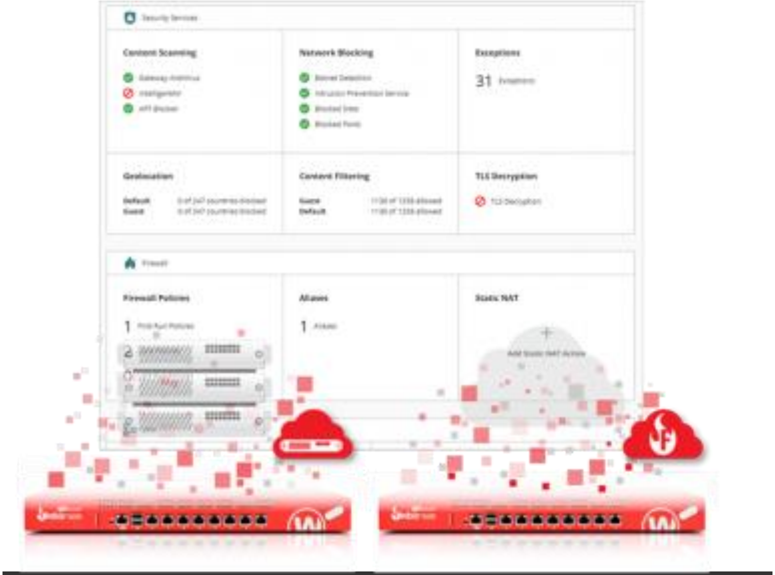
0 Devices pending upgrade

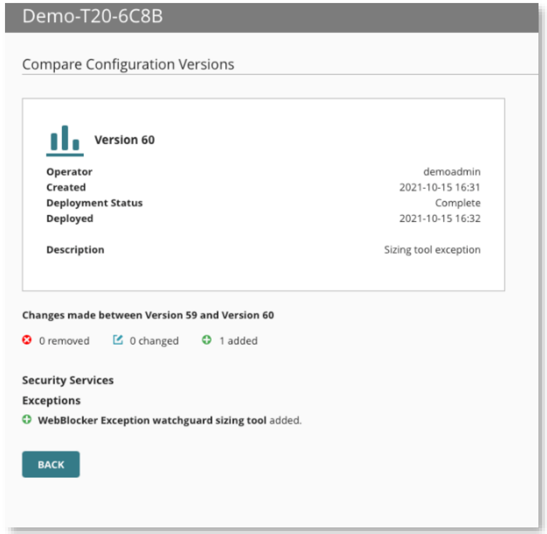
0 Devices failed to upgrade

Upgrade Firmware

View All | Search

Name	Type	Firmware Version	Description
523A	Firebox	12.7.B637467	Ready to upgrade
62FB	Firebox		Device must be upgraded locally before it can be cloud-managed.
T40-W	Cluster	12.7.1.B642754	Ready to upgrade





Demo-T20-6C8B

Compare Configuration Versions

Version 60

Operator	demoadmin
Created	2021-10-15 16:31
Deployment Status	Complete
Deployed	2021-10-15 16:32
Description	Sizing tool exception

Changes made between Version 59 and Version 60

0 removed 0 changed 1 added

Security Services

Exceptions

WebBlocker Exception watchguard sizing tool added.

BACK

System Actions for Firecluster

- Upgrade firmware
- Reboot
- Backup

FireboxV and Firebox Cloud

- Policy management in WatchGuard Cloud

Configuration Differences

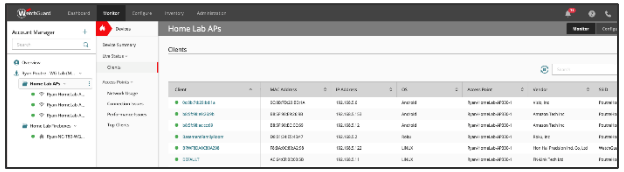
Compare two Firebox configuration versions to see what has changed between them:

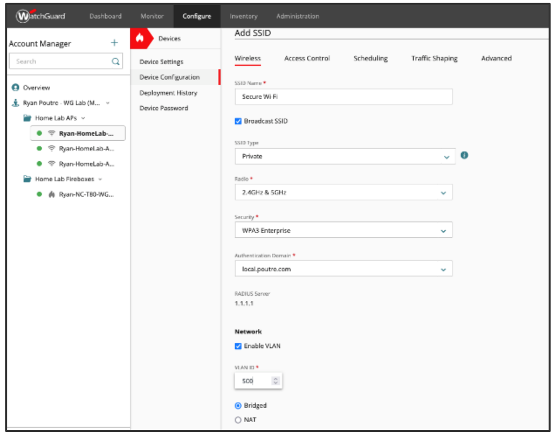
- Deployment history and versioning
- Clear view of what has changed
- Added, deleted, updated
- User/operator change owner

WatchGuard

Wi-Fi in WatchGuard Cloud Features

Clarity & Control





Add SSID

SSID Name * Secure Wi-Fi

☑ Broadcast SSID

SSID Type Private

Radio * 2.4GHz & 5GHz

Security * WPA3 Enterprise

Authentication Domain * local.poutre.com

RADIUS Server 1.1.1.1

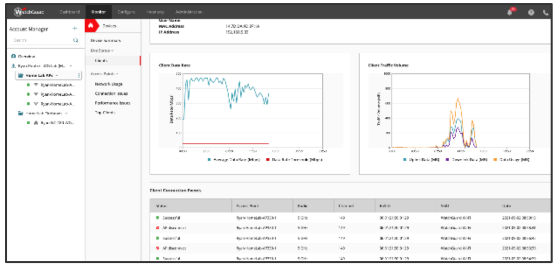
Network

☑ Enable VLAN

VLAN ID * 500

● Bridged

○ NAT



Joe's Café

Enjoy Free Wi-Fi

Welcome to Joe's Cafe

CONNECT

□ I agree to the Terms of Use and have reviewed the Privacy Policy

Copyright © 1996-2021 WatchGuard Technologies, Inc. All Rights Reserved.

Management & Deployment

- Accelerated Customer/Site Onboarding
- Site configuration (Templates) for easy deployment
- True 0-Touch deployments
- Authentication Domains shared configuration across WG Portfolio
- Radio and SSID Management

Reporting & Visibility

- Service Provider Level Alerting and Device Status
- Track Connected Clients
- Live Client List
- Device Health and Status
- Firmware versions
- Bandwidth Usage
- Channel and Signal reporting

Network & Troubleshooting

- Diagnose Connectivity Issues
- Easy visualization of signal strength for clients
- Detection of failures and anomalies from client devices
- Detailed reports for Network Usage, Connectivity Issues, Performance Issues, and Top Clients

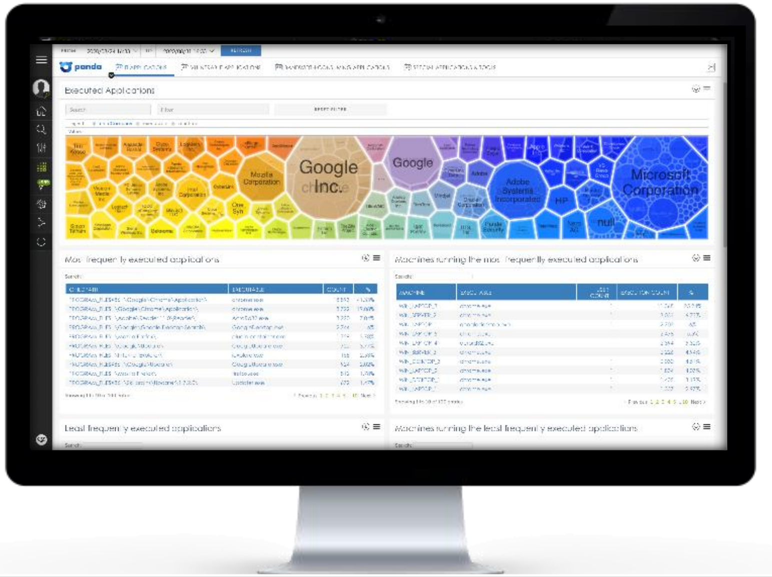
Captive Portal

- Standard click through splash pages
- Customizable splash pages tied to branding in WatchGuard Cloud

Endpoint Modules

Clarity & Control

Block malicious behaviors, deploy patches and updates, and much more from a single pane of glass.


panda
Executed Applications
Google Inc.
Google
Mozilla Corporation
Adobe Systems Incorporated
HP
Microsoft Corporation
null
Most frequently executed applications
Machines running the most frequently executed applications
Least frequently executed applications
Machines running the least frequently executed applications

WatchGuard Advanced Reporting Tool

WatchGuard EPDR and WatchGuard EDR only

Generate security intelligence and IT insights to pinpoint attacks, unusual behavior, and internal misuse

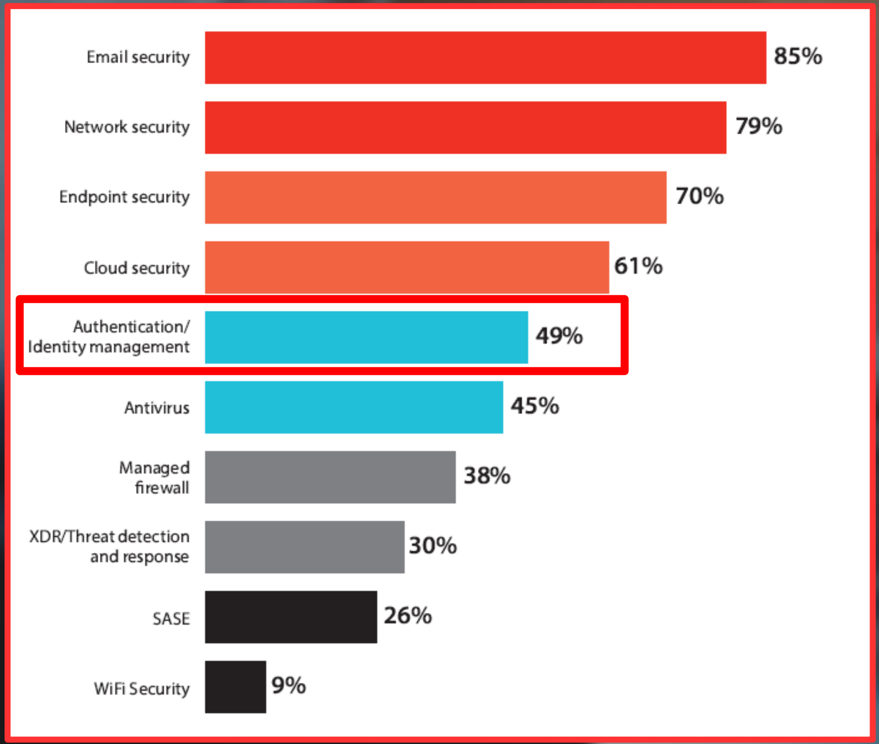
- Delivers real-time, deep insight into the day-to-day behavior of your applications, your network, and your users

Comprehensive Security

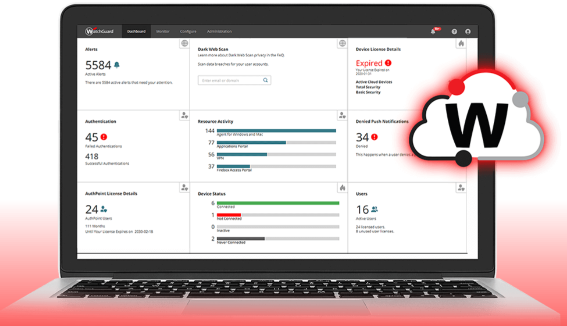
Complete Security

Less than 50% of MSPs offer Authentication and Identity Management

-Powered by Pulse



A Portfolio Built for Differentiation



Network

Total network protection:

- Intrusion prevention
- URL filtering
- Application control
- Spam blocking
- AI-powered anti-malware
- Cloud sandboxing
- DNS-filtering
- And more!

Wi-Fi

Unified Wi-Fi:

- Wi-Fi 6
- OWE & WPA3 encryption
- Diagnose, monitor and report
- PSA integration
- IKEv2 VPN (RAP)
- And more!

Endpoint

A Full endpoint suite:

- Signatures and heuristics
- Contextual detection
- Anti-exploit
- Automated response
- DNS-filtering
- Zero-trust application service
- Threat Hunting
- Patch Management
- And more!

User

Unique approach to MFA:

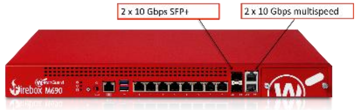
- Mobile Device DNA
- Push message
- QR code,
- One-time password (OTP)
- Authenticate right from your phone
- Fast VPN and Remote Access
- Hardware token available

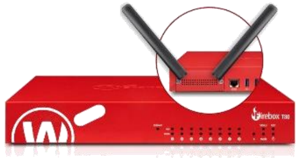
Remote Access

Extending protection:

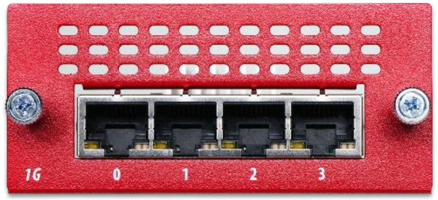
- Risk-based policies
- Integrated clientless VPN
- SAML support
- 3rd party integrations
- Full user synchronization
- 140 third-party integrations

New Boxes and Modules





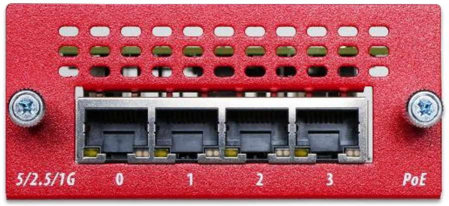
Firebox M290	Firebox M390	Firebox M590	Firebox M690	Firebox T80 LTE Module
Up to 75 users *700 Mbps (HTTPS + IPS)* **Expansion Bay:** • 4 x 1 Gb Copper • 4 x SFP • 2 x SFP+ • 4 x Multispeed	*Up to 250 users* *1.33 Gbps (HTTPS + IPS)* **Expansion Bay:** • 4 x 1 Gb Copper • 4 x SFP • 2 x SFP+ • 4 x Multispeed	*Up to 500 users* *2.0 Gbps (HTTPS + IPS)* **Expansion Bay:** • 4 x 1 Gb Copper • 4 x SFP • 2 x SFP+ • **4 x Multispeed PoE+**	*Up to 850 users* *2.9 Gbps (HTTPS + IPS)* **Expansion Bay:** • 4 x 1 Gb Copper • 4 x SFP • 2 x SFP+ • **4 x Multispeed PoE+**	*Up to 50 users* *356 Mbps (HTTPS + IPS)* **Expansion Bay:** • *NEW* LTE Interface • 1 Port 10 GB SFP+ Fiber



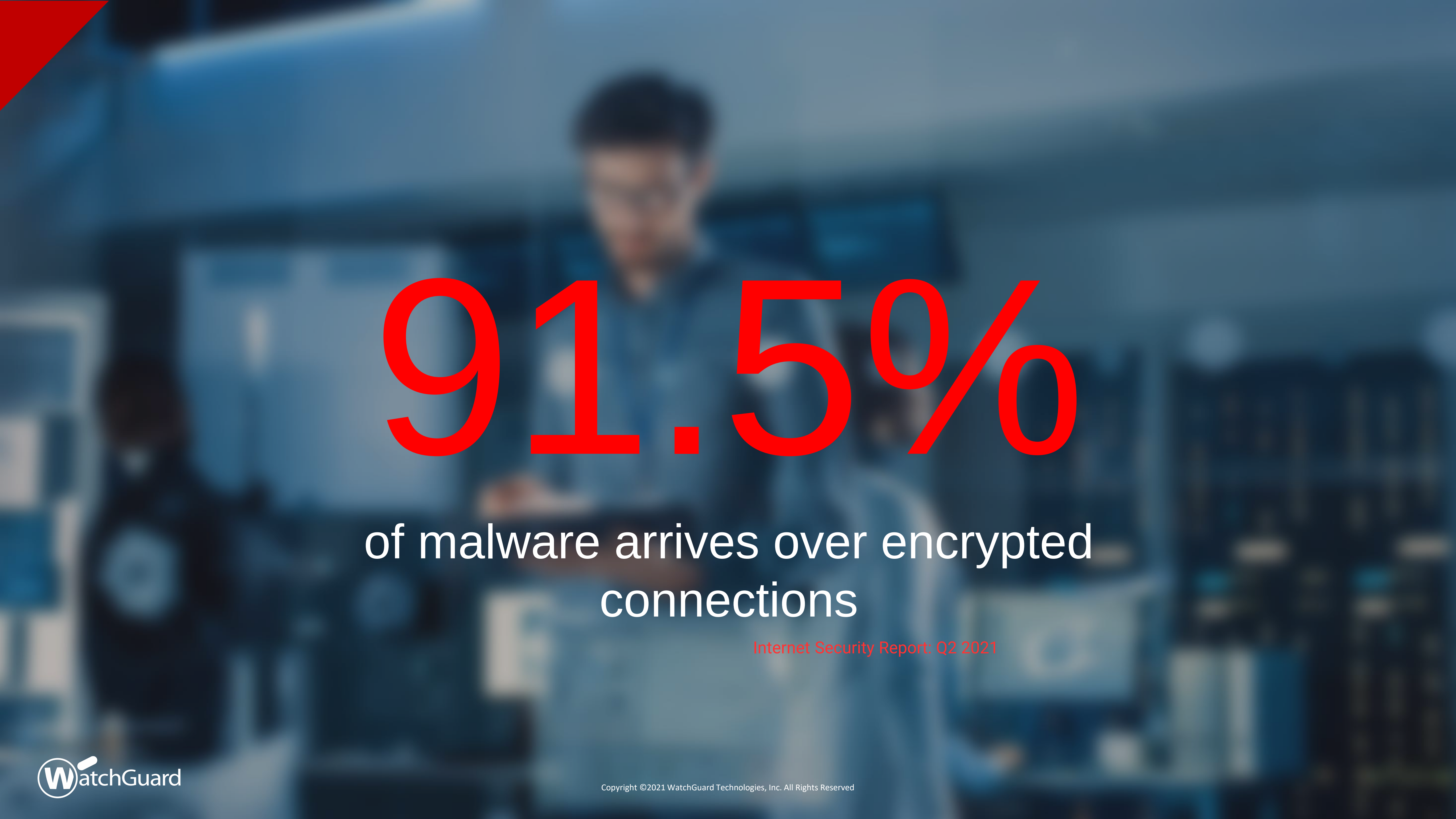
4 x 1 Gb Copper

4 x SFP

2 x SFP+



4 x Multispeed



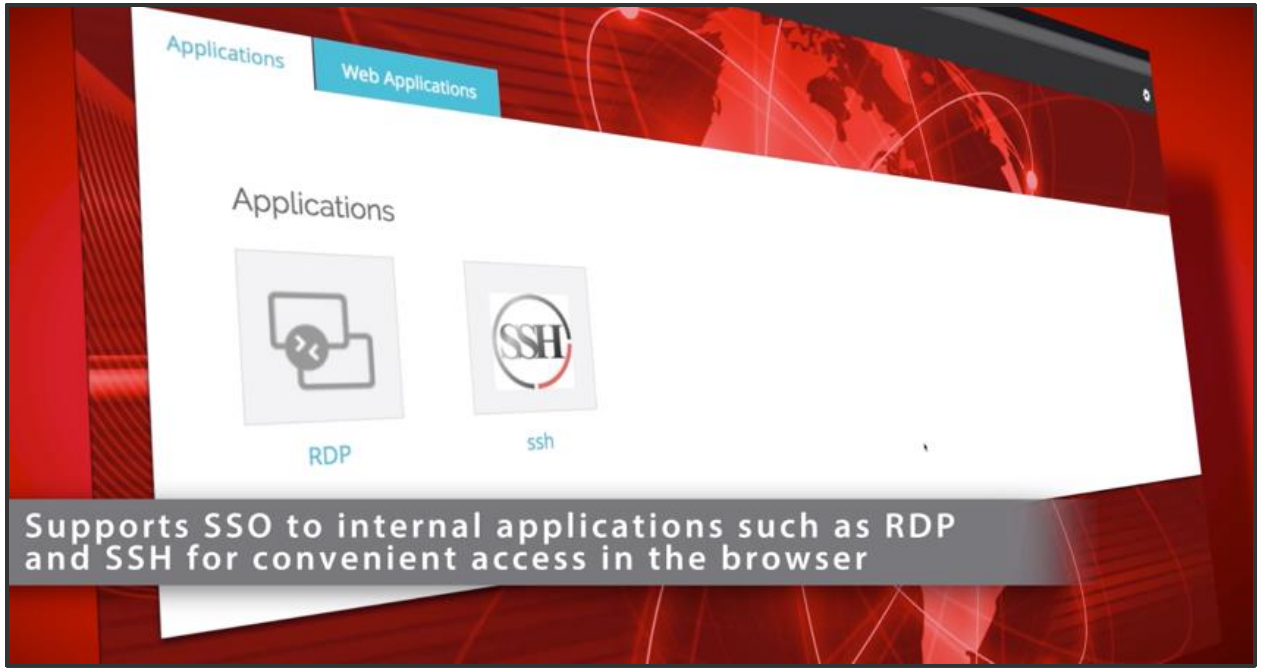
91.5%

of malware arrives over encrypted connections

Internet Security Report: Q2 2021

More Access Portal Sessions

Complete Security



Supports SSO to internal applications such as RDP and SSH for convenient access in the browser

- RDP (Remote desktop protocol)
- TLS Encrypted sessions
- No client required

Model	Max RD Sessions
T40	65
T80	65
M290	65
M390	175
M590	175
M690	380
M4800	380
M5800	800
FireboxV Small	65
FireboxV Medium	65
FireboxV Large	175
FireboxV Extra Large	380

WatchGuard

New WatchGuard Wi-Fi 6 Hardware

Complete Security

↑ Connectivity

↑ Speed

↑ Security

↓ Complexity

	AP130	AP330	AP430CR
Recommended Use Cases	Low-density	Mid-range	High-density for Rugged or Outdoor Environments
Radios and Streams	Wi-Fi 6 2x2 Scanning	Wi-Fi 6 2x2 w/ 2x2 Dedicated Scanning Security Radio	Wi-Fi 6 4x4 w/ 2x2 Dedicated Scanning Security Radio
Deployment	Indoor	Indoor	Rugged/Outdoor
Number of Antennas	4 Internal omnidirectional	7 Internal omnidirectional	6 External N-Type Connectors (Antennas Not Included)
BLE + Zigbee	No	Yes	Yes
Outdoor Rating	N/A	N/A	IP67 Rated Enclosure
PoE Power	12v/2A DC In, 802.3at (PoE+)	12V/2A DC In, 802.3at (PoE+)	802.3at (PoE+)
Maximum TX Power	22 dBm + 3 dBi Antenna Gain	22 dBm + 2 dBi Antenna Gain	23 dBm
Max. Data Rate (5/2.4GHz)	1201 Mbps / 574 Mbps*	1201 Mbps / 574 Mbps*	2402 Mbps (4x4) / 574 Mbps (2x2)*
Ethernet Ports Power over Ethernet (PoE)	1 x 1Gbps (PoE+)	1 x 2.5 Gbps (PoE+)	1 x 5 Gbps (PoE+) 1 x 1 Gbps

WatchGuard Remote Access Point Feature

Complete Security

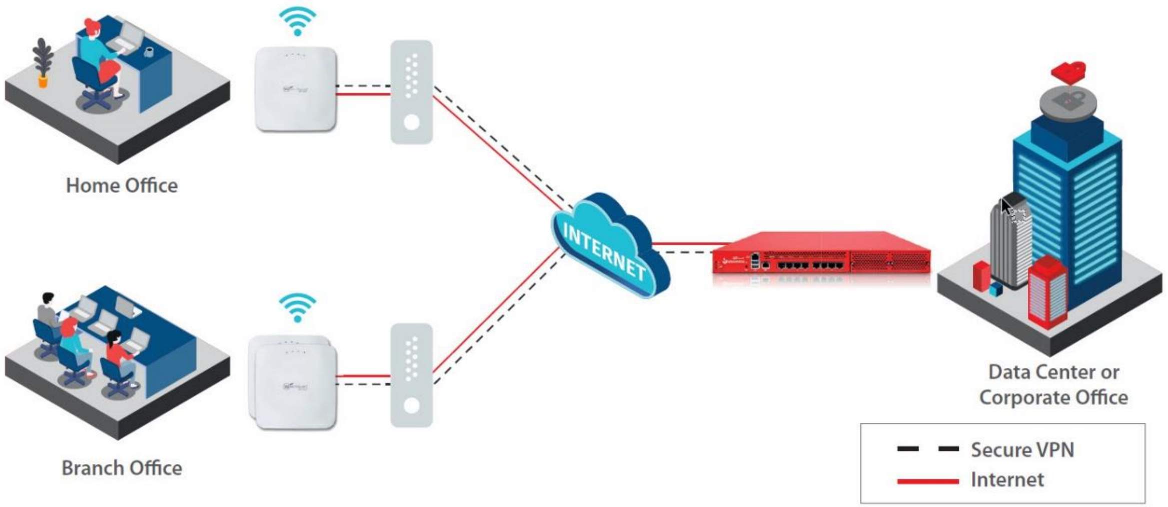
WatchGuard's Cloud-managed access points can tunnel traffic back to corporate resources based on the SSID an end-user is using from home.

Use Cases:

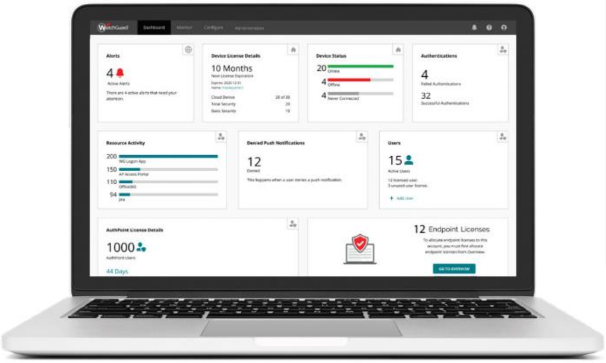
- Remote employees
- Remote student and faculty
- Corporate office
- Small branch office

RAP Specifications:

- Supported on WatchGuard AP225W and AP327X
- IPsec VPN between AP and WatchGuard Firewall.
- Centralized Cloud-management for easy deployment and visibility.



Endpoint Security in WatchGuard Cloud



Endpoint Security Offering

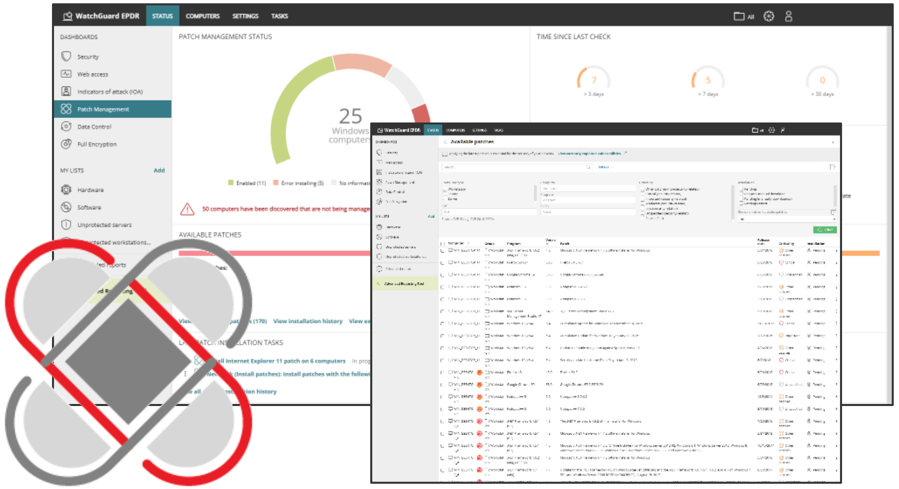
EPP	WatchGuard EPP	**EPP** **Windows, macOS, Linux and Android**
EDR	WatchGuard EDR	**EDR** **Services: Zero-Trust Application & Threat Hunting**
EPDR	WatchGuard EPDR	**EPP + EDR** **Services: Zero-Trust Application & Threat Hunting**

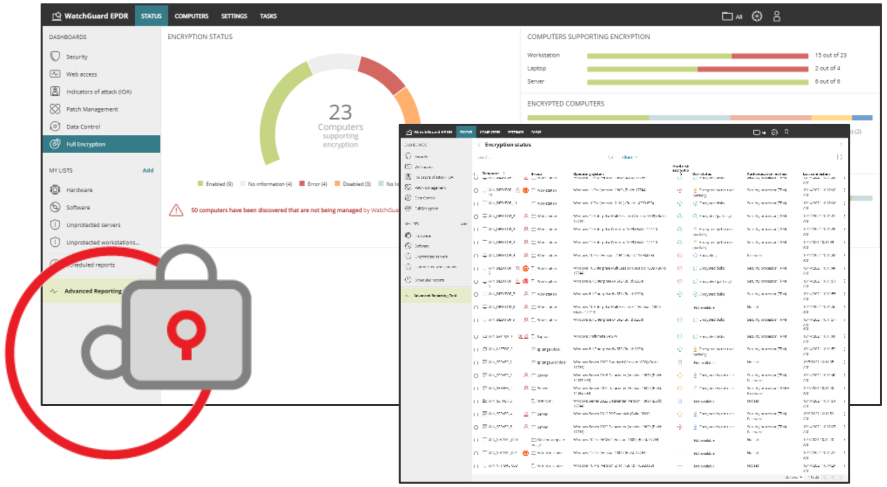
Additional Products

DNS GO	DNSWatchGO	**Cloud-based, domain-level protection, content filtering, keep users safe outside the network**

Endpoint Modules

Complete Security





WatchGuard Patch Management

WatchGuard EPDR, WatchGuard EDR, and WatchGuard EPP

Manage operating system and third-party application vulnerabilities on your workstations and servers

- Assess, monitor and prioritize operating systems and application vulnerabilities and Updates
- Prevent incidents, systematically reducing the attack surface created by software vulnerabilities
- Contain and mitigate vulnerability exploitation attacks with immediate updates

WatchGuard Full Encryption

WatchGuard EPDR, WatchGuard EDR, and WatchGuard EPP

Encrypt and decrypt disks and USB drives centrally without impact to end users

- leverages BitLocker, a proven and stable Microsoft technology, to encrypt and decrypt disks without impacting end users
- Prevent loss, theft and unauthorized access. Recovery keys are stored and recovered securely from the cloud.
- No need to deploy or install additional agents. No servers or additional costs for additional servers.

WatchGuard®

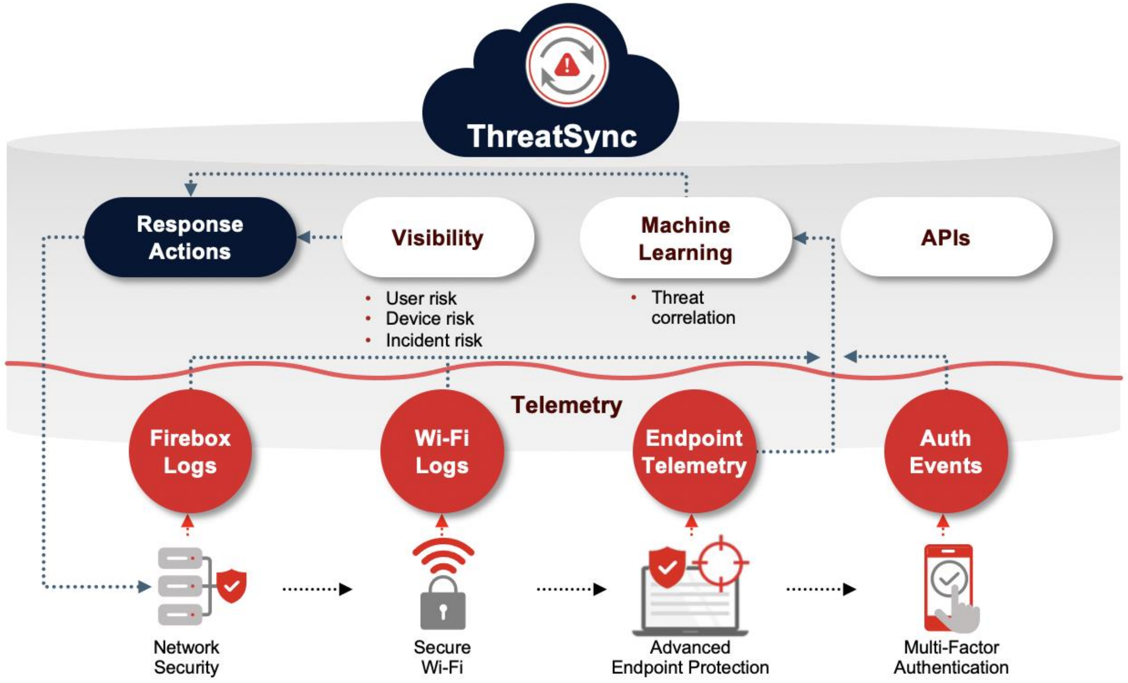
Shared Knowledge

Shared Knowledge

Correlation with ThreatSync™

Shared Knowledge

ThreatSync saves security team cycles, speeds detection, and increases their accuracy by automatically correlating relevant threat data from the entire WatchGuard Unified Security Platform.



ThreatSync:

- An integrated platform for delivering extended detection and response (XDR) across environments, users and devices
- Collects, correlates, analyzes and responds to threats across security layers
- Delivers an easy-to-understand threat score for indicators and incidents
- Provides a detailed, contextualized, and actionable picture of your threat surface

100s of billions of events analyzed

2.1 billion binaries classified

Millions adversary movements tracked

Thousands of zero-day malware blocked

WatchGuard

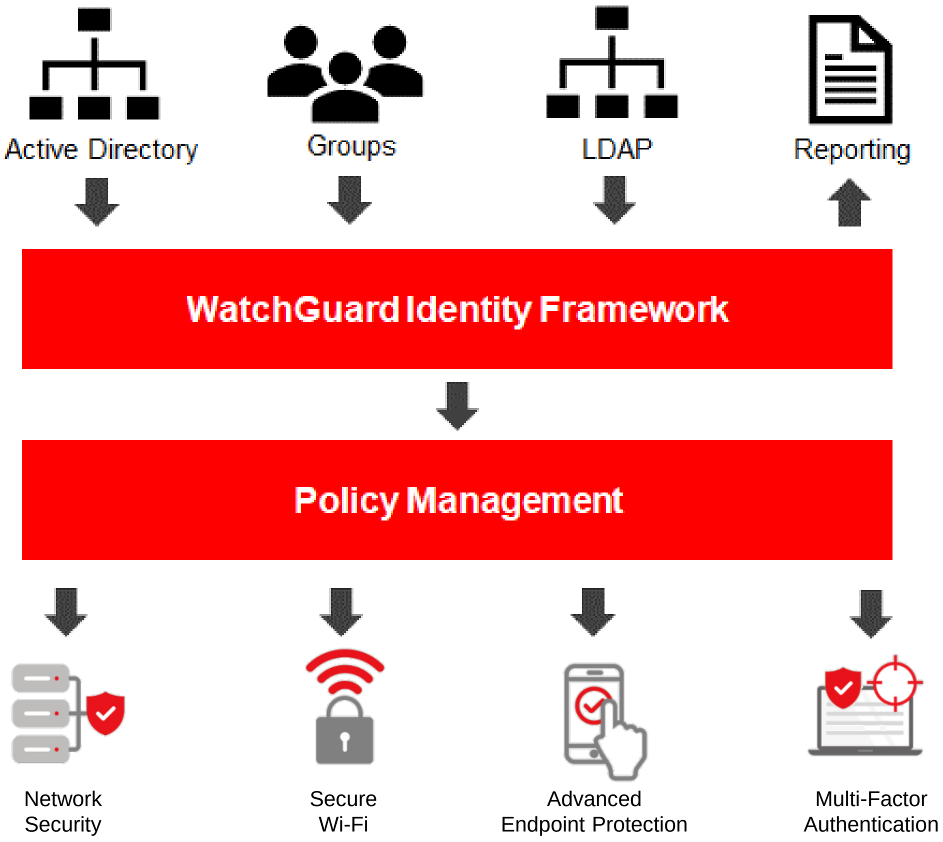
WatchGuard Identity Framework™ for User-Centric Security

Shared Knowledge

The Unified Security Platform introduces verified identity as a factor in every security analysis and improves identity management with flexible rules to configure users and devices based on risk.

WatchGuard Identity Framework:

- Unlocks risk-based user management and authentication across security layers
- Synchronizes Active Directory for all WatchGuard applications
- Simplifies reporting with group definitions and user groups
- Facilitates secure remote access via the Firebox without requiring RADIUS hardware


Active Directory
Groups
LDAP
Reporting
WatchGuard Identity Framework
Policy Management
Network Security
Secure Wi-Fi
Advanced Endpoint Protection
Multi-Factor Authentication

WatchGuard

AuthPoint and Firebox Integration

Shared Knowledge

Use AuthPoint as an authentication server on your Firebox.

This makes it easier to configure AuthPoint for:

- Mobile VPN with SSL
- Mobile VPN with IKEv2
- Firebox authentication portal

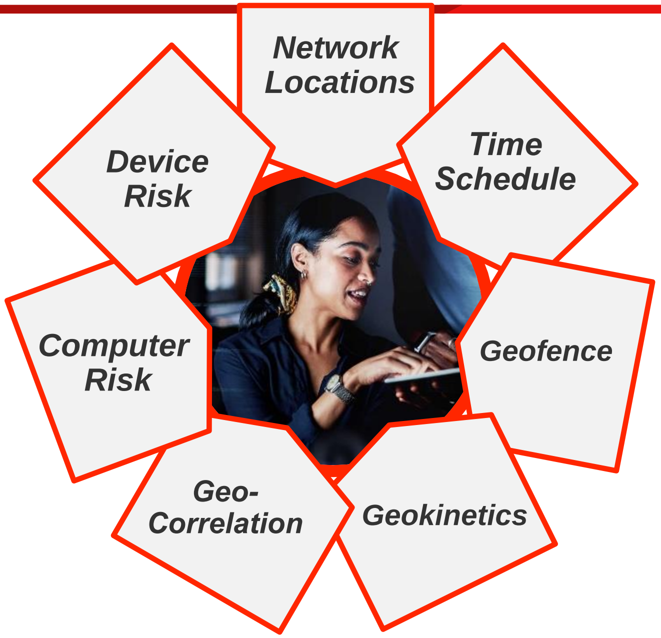
No need for additional RADIUS hardware!

AuthPoint Gateway is ONLY required to sync users from an LDAP database.

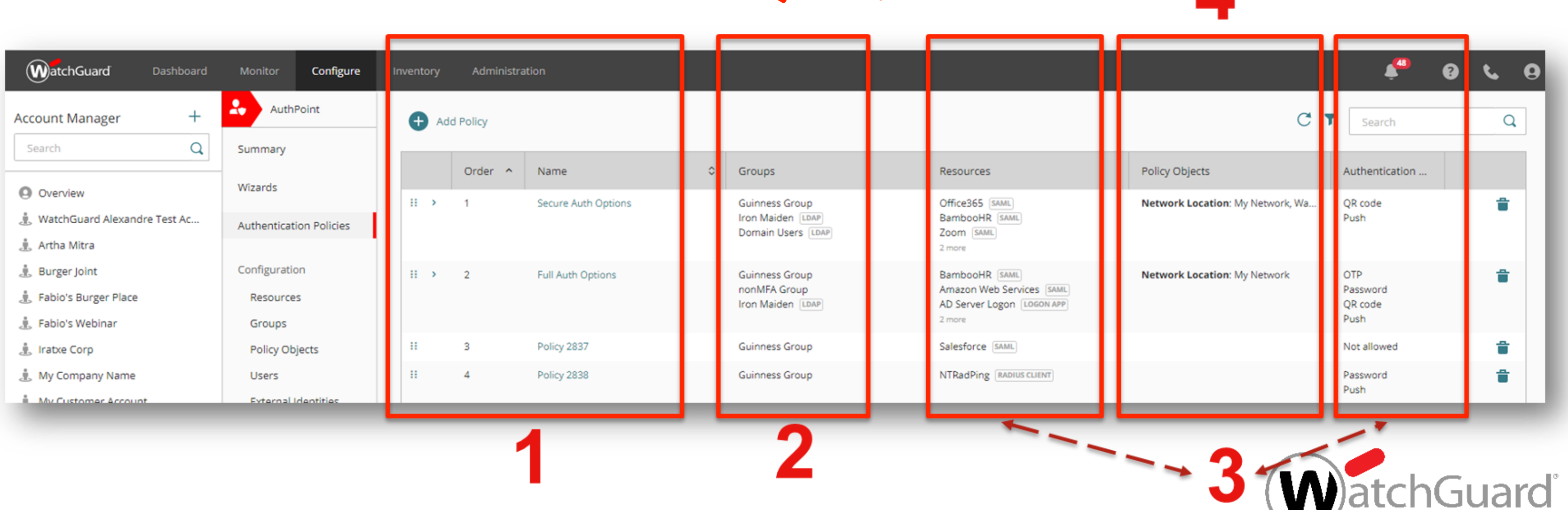
Shared Knowledge

AuthPoint Risk Framework

Improve identity management capabilities by providing customizable and flexible rules based on level of risk.



1. Powerful method to configure authentication policies
2. AD Groups sync – Use the AD groups within AuthPoint
3. Resources per policy, with specific authentication requirements
4. Risk Policies: Network Location, Time/Schedule and Geolocation, more



Order	Name	Groups	Resources	Policy Objects	Authentication ...
1	Secure Auth Options	Guinness Group Iron Maiden LDAP Domain Users LDAP	Office365 SAML BambooHR SAML Zoom SAML 2 more	**Network Location**: My Network, Wa...	QR code Push
2	Full Auth Options	Guinness Group nonMFA Group Iron Maiden LDAP	BambooHR SAML Amazon Web Services SAML AD Server Logon LOGON APP 2 more	**Network Location**: My Network	OTP Password QR code Push
3	Policy 2837	Guinness Group	Salesforce SAML		Not allowed
4	Policy 2838	Guinness Group	NTRadPing RADIUS CLIENT		Password Push

WatchGuard

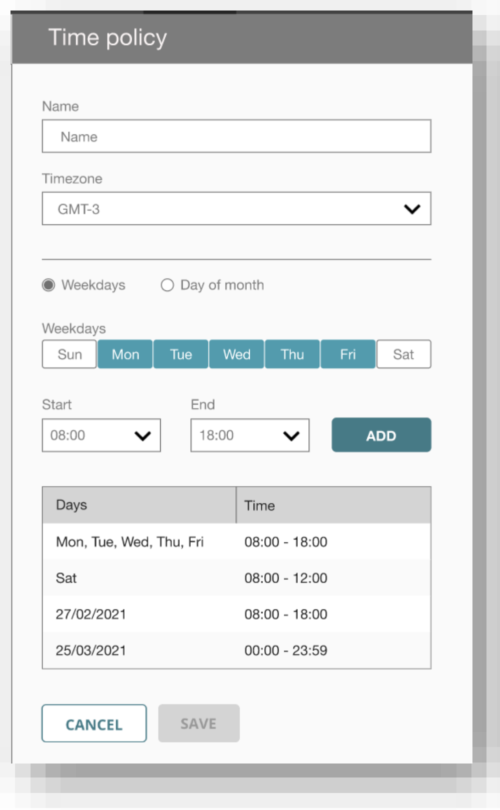
AuthPoint Risk Framework: Time Schedule

Shared Knowledge

Specify the dates and times when authentication policies apply to user authentications.

You can configure a time schedule policy object if you want to:

1. Allow authentication only during specified times, such as work hours.
2. Restrict authentication during specific times, such as non-work hours and holidays.
3. Enforce different authentication requirements at different times.
4. Use a safe network location to allow users to bypass MFA when they authenticate from the office, but only during specified times, such as work hours.



Time policy

Name: Name

Timezone: GMT-3

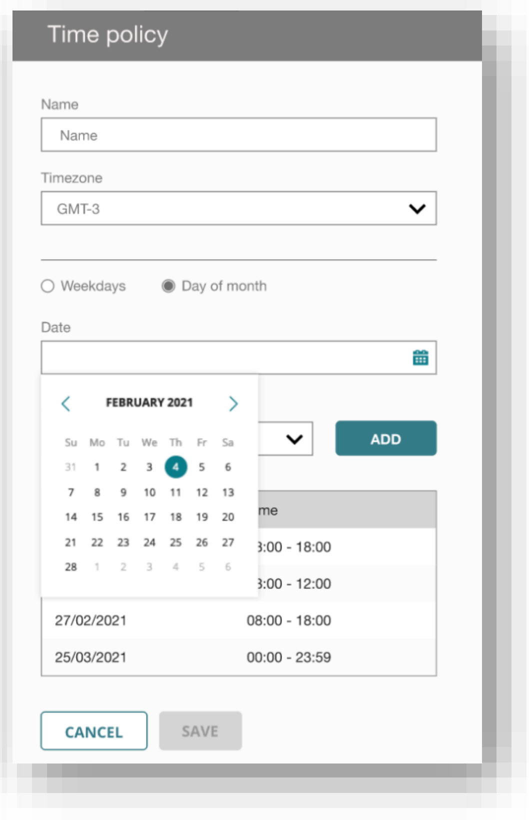
● Weekdays ○ Day of month

Weekdays: Sun [✓ Mon] [✓ Tue] [✓ Wed] [✓ Thu] [✓ Fri] Sat

Start: 08:00 End: 18:00 ADD

Days	Time
Mon, Tue, Wed, Thu, Fri	08:00 - 18:00
Sat	08:00 - 12:00
27/02/2021	08:00 - 18:00
25/03/2021	00:00 - 23:59

CANCEL SAVE



Time policy

Name: Name

Timezone: GMT-3

○ Weekdays ● Day of month

Date:

FEBRUARY 2021

Su	Mo	Tu	We	Th	Fr	Sa
31	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	1	2	3	4	5	6

ADD

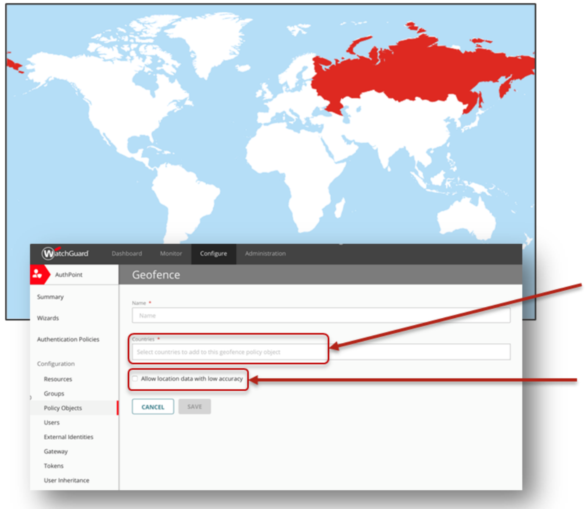
	me
	3:00 - 18:00
	3:00 - 12:00
27/02/2021	08:00 - 18:00
25/03/2021	00:00 - 23:59

CANCEL SAVE

WatchGuard

AuthPoint Risk Framework: Geographic Policy Controls

Shared Knowledge



Geofence

Name * Name

Countries * Select countries to add to this geofence policy object

☐ Allow location data with low accuracy

CANCEL SAVE

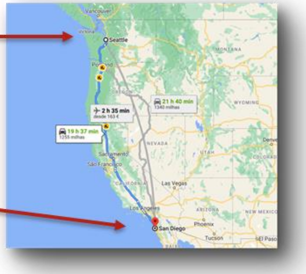
Add the countries that will be part of the policy

Determine if GPS location will be required

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

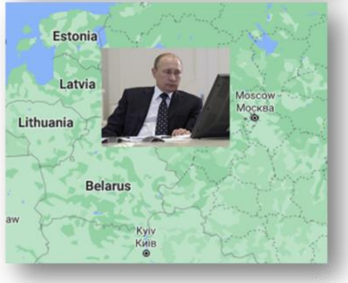
User: Roadrunner
Location: Seattle
1st Authentication: 9:05am

User: Roadrunner
Location: San Diego
2nd Authentication: 9:30am(?)



Alex Mobile phone: Portugal

Computer Location: Russia?



Geofence – Q4 2021

- Policies based on countries protect you from risky places you don't do business
- Geolocation based only on IP address can be circumvented with VPNs
- Requiring the GPS location of the login device gives better precision for the policy

Geokinetics – Q1 2022

- Prevents access from "impossible" locations
- Considers initial login location and time/distance between 2nd login location
- Travel 1000 miles in 30 minutes? Blocked.

Geocorrelation – Q2 2022

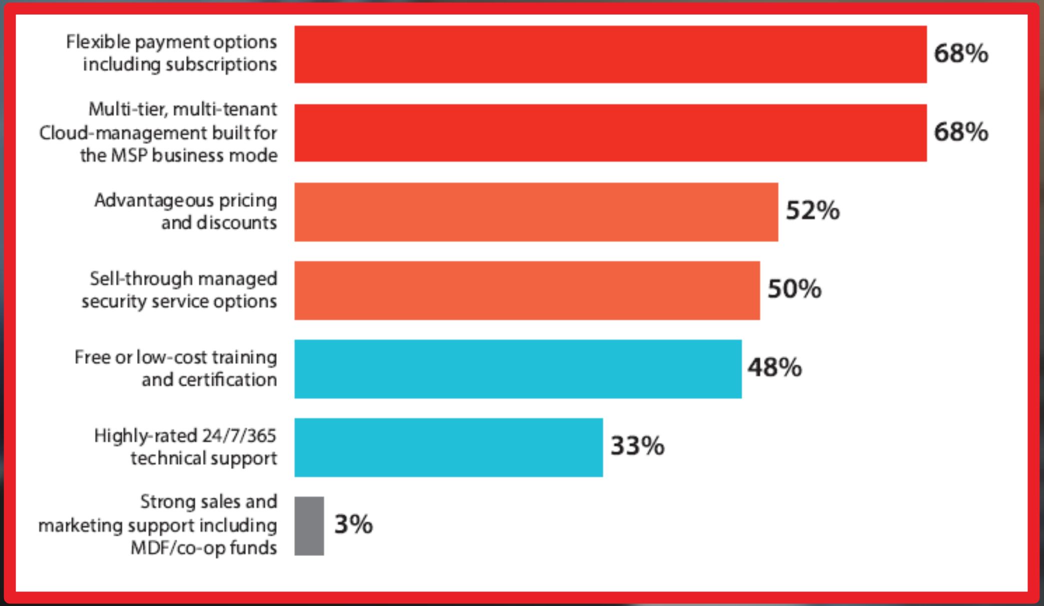
- Defense against social engineering/phishing
- Mobile phone used for Authentication MUST be in the same location as PC they are logging in to.

Operational Alignment

Operational Alignment

Flexible Payment Options, and Multi-tier, multi-tenant-cloud management are must haves.

-Powered by Pulse



Integrations for Robust Business Automation

Operational Alignment

Firebox

Microsoft
portnox
DUO
splunk>
Tigerpaw
ManageEngine
liongard
Cyberoam
Centrify
ArcSight An HP Company
ConnectWise
CITRIX
Azure Sentinel
auvik
Autotask
solarwinds
Google Cloud
bigleaf networks
amazon webservices
gemalto security to be free

AuthPoint

6sense
freshservice
box
G Suite
GitLab
bambooHR
ITGlue
bmc
Adobe
EGNYTE
CYBERARK
BlueJeans
Apache Guacamole
Akamai
LogMeIn
Parallels Remote Application Server
pfsense
onelogin

Wi-Fi

TAOGLAS CROWD Insights™
GuestAir
secure W2 next-gen wired & wireless security
skyfii IO
octopus
eduroam
NETSCOUT
purple intelligent spaces

Endpoint

Microsoft Windows Virtual Desktop
mac OS
citrix
Windows Server
vmware

With a robust set of APIs available at multiple layers of the Unified Security Platform, MSPs can enjoy the operational benefits of integration at scale.

Scaling your business through integration:

- More than 140 3rd party integrations to support your unique environment
- Superior interoperability with leading solutions MSP tools and marketplaces
- Easier deployments with greater confidence
- Publicly available RESTful APIs

Business Model Agility With FlexPay™

Operational Alignment

Fixed-term Pre-Pay

Fixed-term Pay-as-you-go

Zero commitment Pay-as-you-go

With WatchGuard, MSPs to choose how they want to transact with us and with their customers, offering support for a wide variety of subscription, consumption, and term-based business models

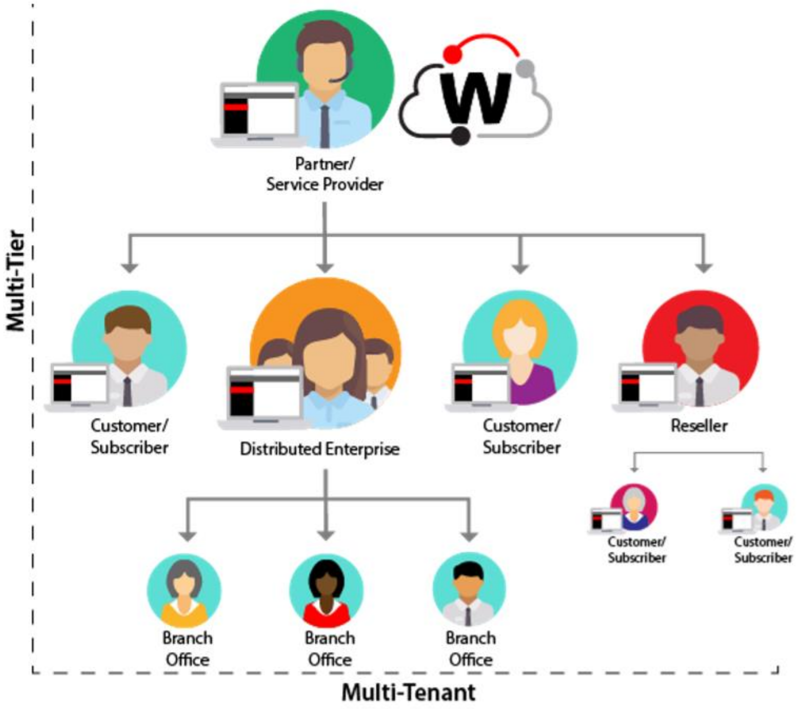
FlexPay:

- Traditional up-front purchases
- Monthly, 1-, and 3- year payment terms
- Pay-as-you-go models
- Subscriptions
- Usage-based invoicing
- Automated renewal

WatchGuard

Manage the Way You Want

Operational Alignment

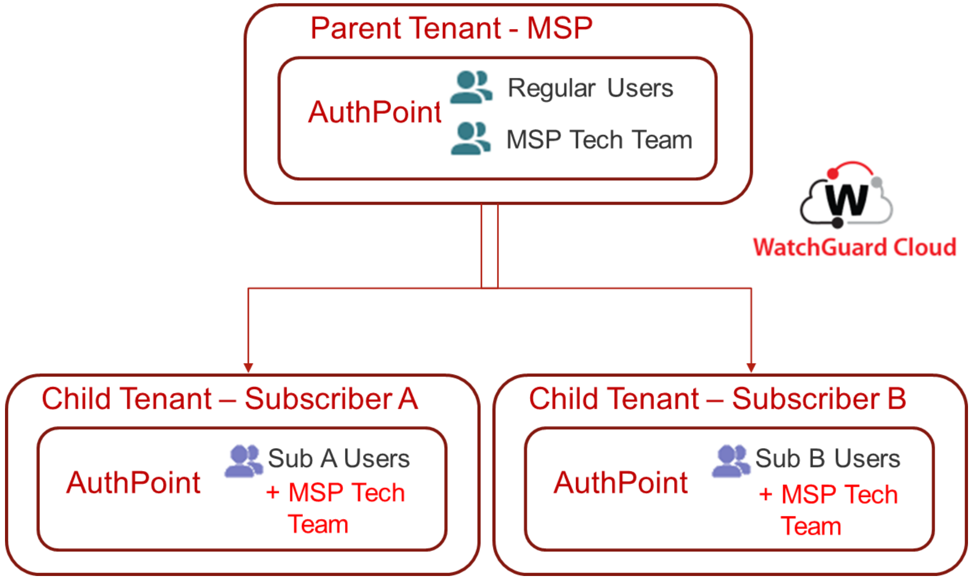


Key Features:

- Create unlimited tenants
- Scale to unlimited tiers
- Service Provider or Subscriber accounts
- Logically separated tenants
- Regional selection per account
- Built-in tenant types
- Parent-Child tenant relationship
- Built-in security and compliance
- Account Delegation for additional support

The AuthPoint MSP Management Dilemma: Solved

Operational Alignment



Parent Tenant - MSP

AuthPoint

Regular Users

MSP Tech Team

WatchGuard Cloud

Child Tenant – Subscriber A

AuthPoint

Sub A Users

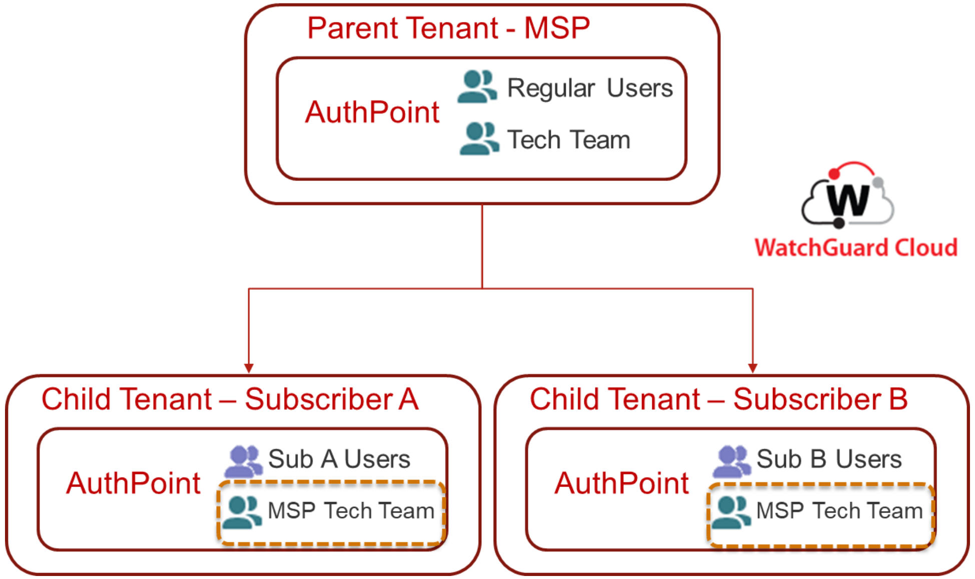
+ MSP Tech Team

Child Tenant – Subscriber B

AuthPoint

Sub B Users

+ MSP Tech Team



Parent Tenant - MSP

AuthPoint

Regular Users

Tech Team

WatchGuard Cloud

Child Tenant – Subscriber A

AuthPoint

Sub A Users

MSP Tech Team

Child Tenant – Subscriber B

AuthPoint

Sub B Users

MSP Tech Team

Before: Additional Licenses required for Tech Teams

- MSP Tech users need to be **created on every Subscriber Tenant**
- Tech users will need to have 1 additional token **per Subscriber**
- MSP or subscribers **must pay for additional licenses**

Now: AuthPoint User Inheritance

- MSP Technical Team **get visibility into their managed accounts**
- **Child tenants can inherit** Tech Team users:
  - **No additional licenses**
  - MSP Tech users will **use their own token**
  - MSP users **can be used on Subscribers' policies**, as any other user from the tenant

AuthPoint Integrations – What’s New

Operational Alignment

6sense
freshservice
box
G Suite
GitLab
bambooHR
ITGlue
Adobe
bmc
EGNYTE
CYBERARK
BlueJeans
Apache Guacamole
Akamai
LogMeIn
Parallels Remote Application Server
pfsense
onelogin

EGNYTE
6sense KNOW EVERYTHING. DO ANYTHING.
sugarcrm SUGARIDENTITY
moodle
pagertree
QualityKick
Apache Guacamole

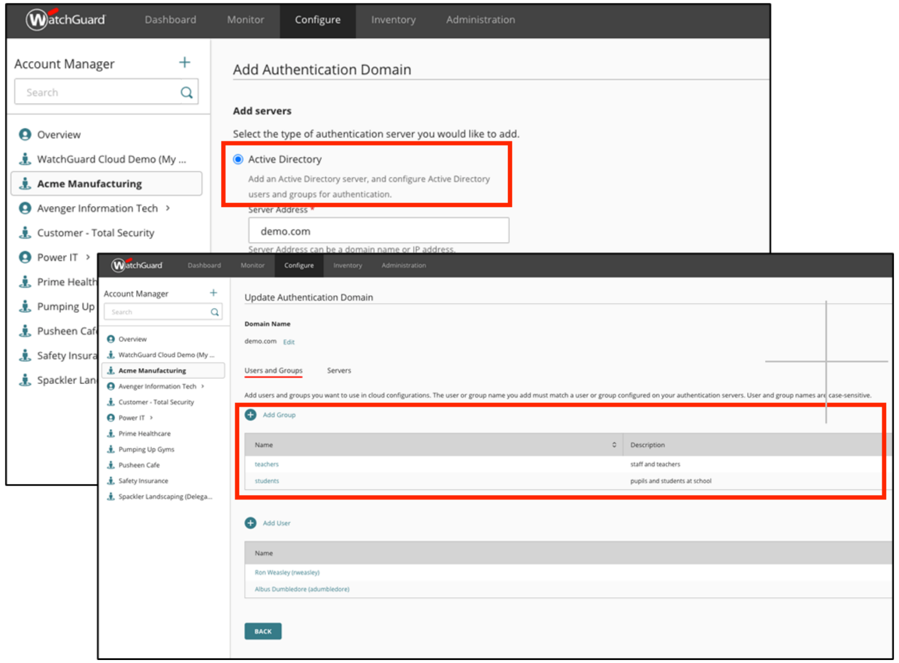
- Internally, we separate into 5 categories:
  - **Remote Access & VPN:** Firewalls, remote access applications, mostly RADIUS
  - **Cloud Applications:** SAML, for Web SSO
  - **Operating Systems:** User login using agents or integrations
  - **IAM:** IAM and Privileged access applications
  - **Other Integrations:** Agents with direct integration, 3rd party hardware tokens, APIs, etc.
- Updated Integration Guides:
  - Firebox Direct Integration
  - Splunk
  - FilesAnywhere
  - ConnectWise Control
  - NetDocuments
  - Fortinet SSL VPN

More than 140 documented integrations!

WatchGuard

Firebox: Active Directory and Azure AD

Operational Alignment



Add Authentication Domain

Add servers

Select the type of authentication server you would like to add.

● Active Directory

Add an Active Directory server, and configure Active Directory users and groups for authentication.

Server Address *: demo.com

Server Address can be a domain name or IP address.

Update Authentication Domain

Domain Name

demo.com Edit

Users and Groups | Servers

Add users and groups you want to use in cloud configurations. The user or group name you add must match a user or group configured on your authentication servers. User and group names are case-sensitive.

Add Group

Name	Description
teachers	staff and teachers
students	pupils and students at school

Add User

Name
Ron Weasley (rweasley)
Albus Dumbledore (adumbledore)

BACK

Azure
Active Directory

Active Directory Authentication Domain

- Alternative to Radius and the internal Firebox DB
- With Auth Domains you can setup users and groups for use in Firewall policies

Support for Azure Active Directory

Supports Azure Active Directory users for:

- Mobile VPN with SSL
- Mobile VPN with IKEv2
- Firebox Authentication Portal

WatchGuard

Firebox Policy in WatchGuard Cloud: Policy Templates

Operational Alignment

Global Configuration Template

Service Provider creates and deploys the global template once.

When the Service Provider updates and deploys the template, any changes deploy to all subscribed devices automatically.

Multiple Templates

The Service Provider creates each template once.

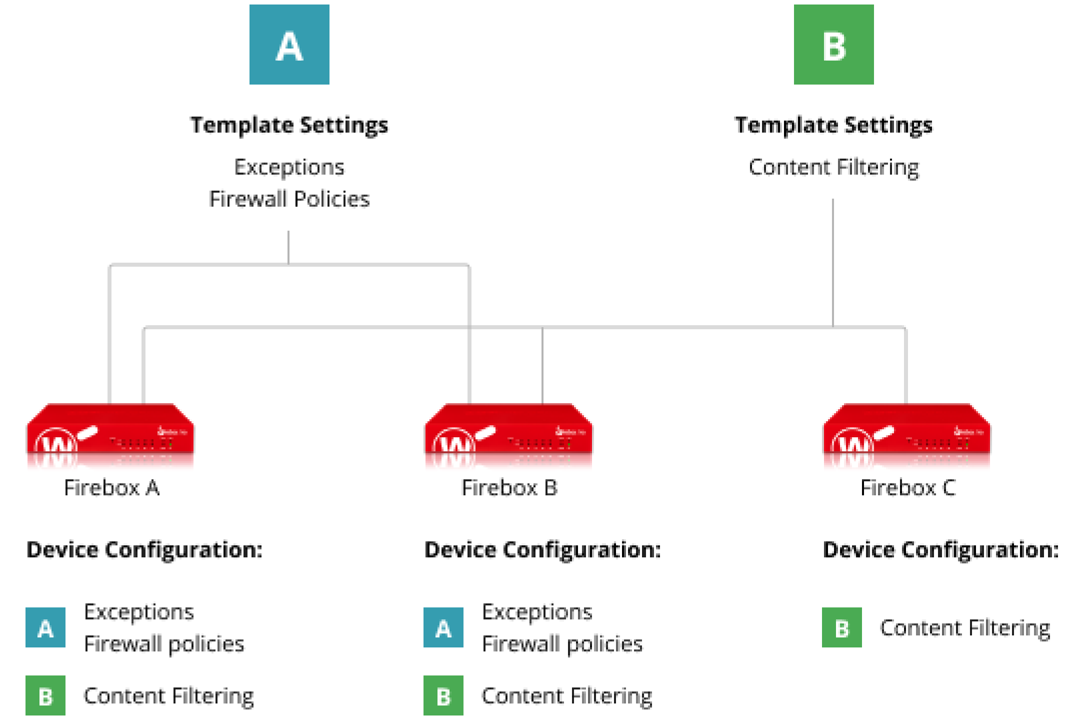
When the Service Provider deploys an update to a template, any changes deploy to all subscribed devices automatically.

Standard Configuration Template

Service Provider creates and deploys the standard configuration template once.

The copied template in each account starts with standard settings.

Example of Firebox template settings on subscribed devices.



A

Template Settings

Exceptions
Firewall Policies

B

Template Settings

Content Filtering

Firebox A

Device Configuration:

A Exceptions
Firewall policies

B Content Filtering

Firebox B

Device Configuration:

A Exceptions
Firewall policies

B Content Filtering

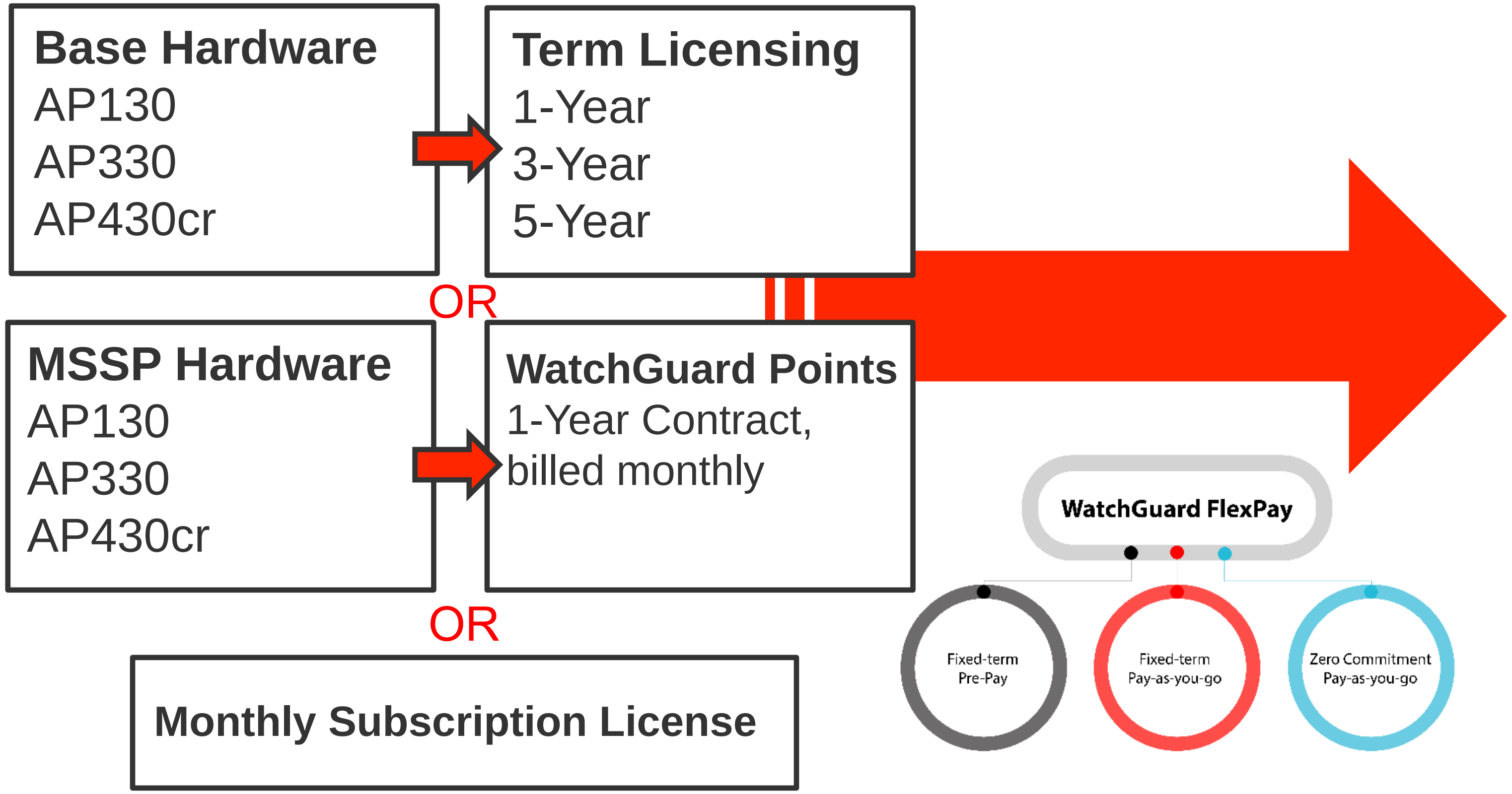
Firebox C

Device Configuration:

B Content Filtering

FlexPay and Wi-Fi Licensing

Operational Alignment



Base Hardware
AP130
AP330
AP430cr

Term Licensing
1-Year
3-Year
5-Year

OR

MSSP Hardware
AP130
AP330
AP430cr

WatchGuard Points
1-Year Contract, billed monthly

OR

Monthly Subscription License

Management License

Feature Description	Standard Wi-Fi	USP Wi-Fi
Native WG Cloud Management Features	x	x
24/7 Support and Hardware Warranty	x	x
Inventory Management	x	x
SSH/CLI Access	x	x
Configuration of Radio Settings	x	x
Configuration of SSID	x	x
Configuration of Device Settings	x	x
Firmware Updated	x	x
24-Hour Reporting/Visibility	x	x
Live Status Visibility	x	x
WatchGuard Cloud API Integration for PSA	x	x
AP Site Templating	x	x
Syslog Server Output		x
IKEV2 VPN Features (RAP)		x
Captive Portal		x
30-Day Reporting/Visibility		x
Future WatchGuard Portfolio Integrations		x
Future Security and Wi-Fi Features *		x

* Features included in USP license will be determined by WatchGuard some features may require additional products from WatchGuard to work.

WatchGuard®

Automation

Automation

Nearly a third (28%) of breaches in 2020 involved a small to midsize business

Before the pandemic, it took an average of 800 days for a midsize business to detect a breach

99% of businesses recognize that they will require managed cybersecurity services to keep up with remote work

Don’t Hesitate, Automate with the Automation Core

Automation

Accelerated Detection and Response

Significant Savings in Staff Hours and Cost

Increased Visibility and Actionable Insight

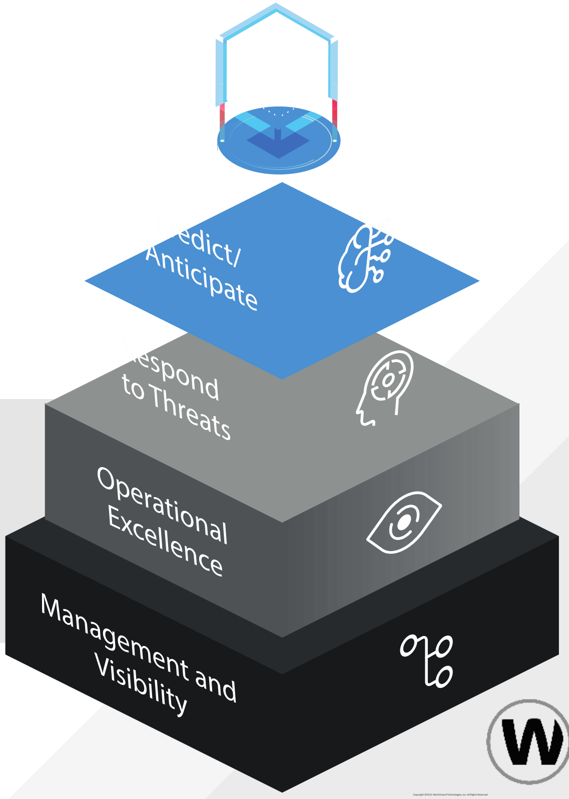
Not all network automation is created equal. The WatchGuard Automation Core accelerates processes, kills more threats, improves accuracy, and empowers your team to do more in less time, with less headache!

Security Automation

Programmatically detect, investigate and remediate

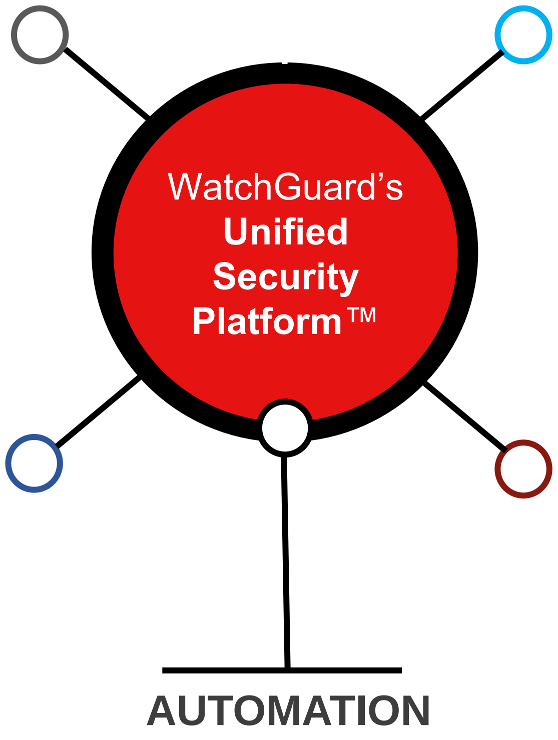
Operational Automation

Provisioning and management



The WatchGuard Automation Core

Operational Alignment



Clarity & Control

Use artificial intelligence in threat triage.
Even with the guidance a threat score provides, you can be left dealing with a host of threats labeled as suspicious. AI trained to identify patterns humans may miss can provide tremendous value and allow you to automate the process of triaging suspicious threats.

Complete Security

Block more threats at the gateway with artificial intelligence.
With defensive solutions that leverage artificial intelligence (AI) and automation, you can block cyberattacks with greater efficiency, and even predict and prevent unknown threats without manual intervention.

Shared Knowledge

Reduce time to detection with automate telemetry correlation and scoring.
Correlating telemetry across endpoints, environments, and users exposes stealthy threats and eliminates alert confusion. And, with correlated threat scoring, you can take the guesswork out of the process.

Operational Alignment

Automate Security Management
With tight integrations with leading professional services automation (PSA) and remote monitoring and management (RMM) platforms, you can better manage your customers' networks while providing streamlined end-to-end service management, including ticketing, automated reporting, and auto-synchronizing asset information.

WatchGuard's Unified Security Platform

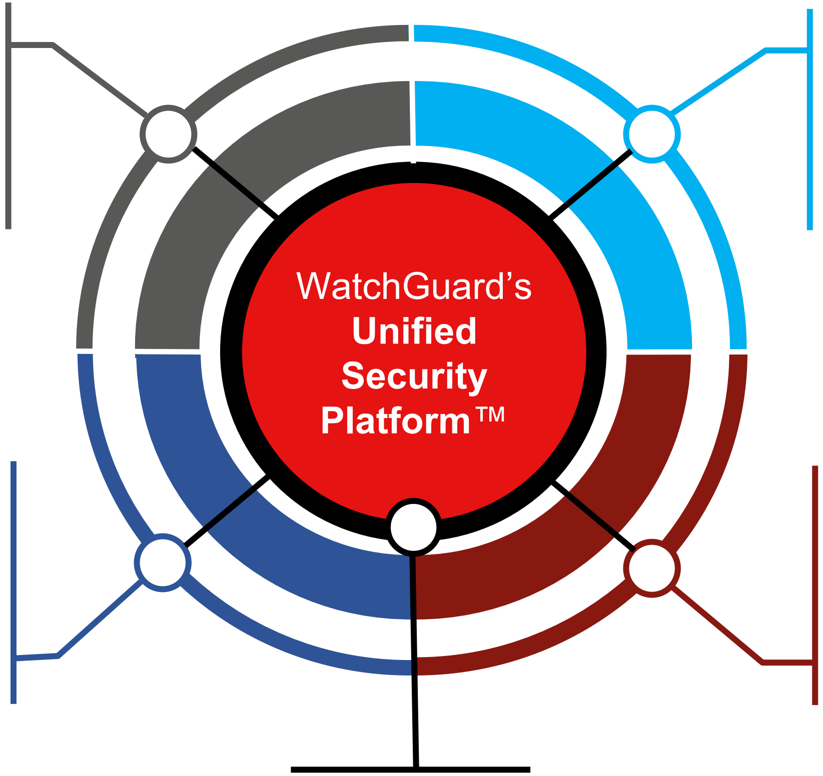
A scalable platform for elevating the practice of modern security delivery.

COMPREHENSIVE SECURITY

A complete portfolio of endpoint, multi-factor authentication, and network security products and services for protecting environments, users, and devices.

CLARITY & CONTROL

Centralized security administration, visibility, and advanced reporting via WatchGuard Cloud™.



OPERATIONAL ALIGNMENT

Simplified business operations with direct API access, a rich ecosystem of out-of-the-box integrations, and support for all payment and consumption models via FlexPay™.

SHARED KNOWLEDGE

A fully integrated platform for adopting a zero-trust security posture via WatchGuard's Identity Framework™ and deploying a true XDR-based approach to threat detection and remediation via ThreatSync®.

AUTOMATION

WatchGuard's Automation Core™ brings simplification and scale to every aspect of security consumption, delivery, and management.

WatchGuard

Questions?

WatchGuard®

Thank You