

Zero Trust Bundle

Security without boundaries

Persistent, always-on protection that follows your user everywhere

Today's workers connect from anywhere – home, office, airports, or public Wi-Fi. Every new connection creates an opportunity for attackers to exploit weak credentials, compromised devices, or exposed applications. WatchGuard Zero Trust Bundle extends protection to every user and device, wherever they work.

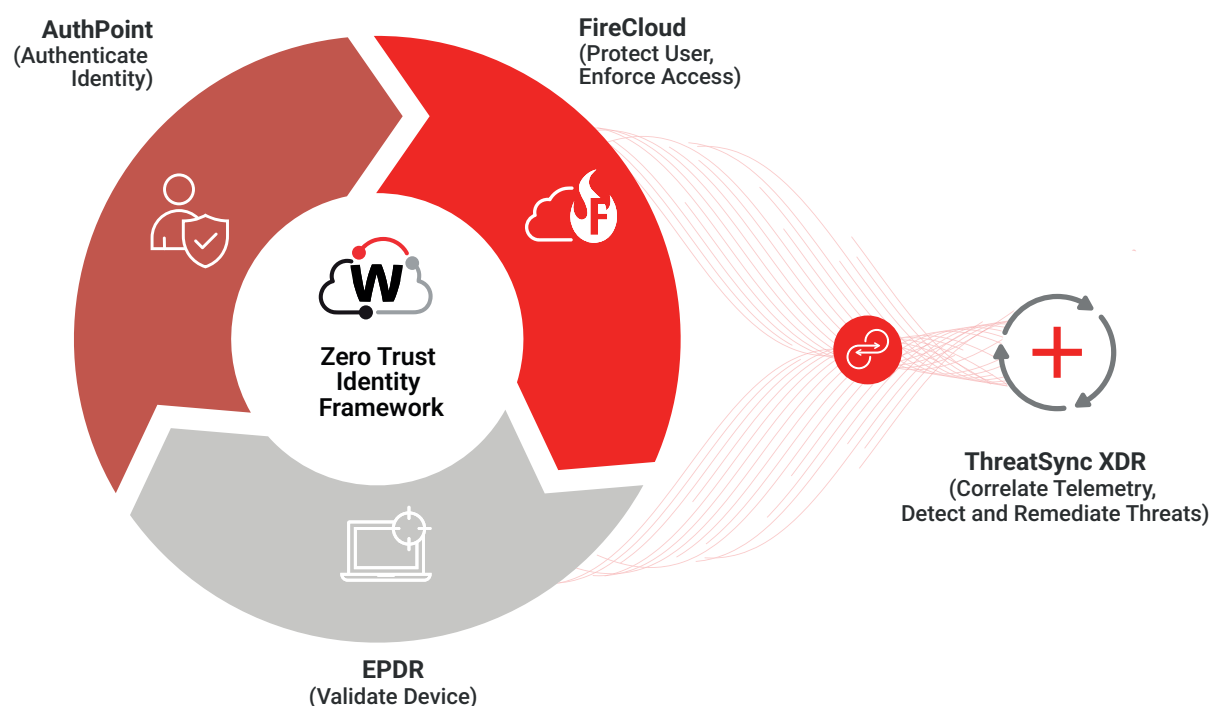
With WatchGuard Zero Trust You Can:

- 1** Create trust by verifying every user and device before granting access with every new session
- 2** Protect against Internet-based threats wherever users connect and gain visibility into user activities and risks
- 3** Prevent attacks and lateral movement across on-premises applications and data with Zero Trust Network Access.

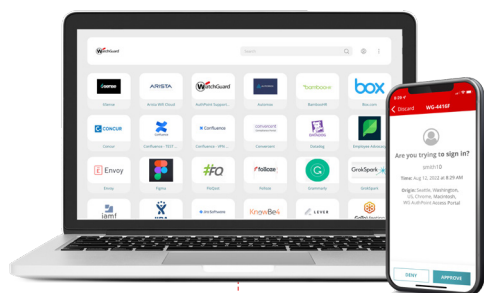
Management and deployment from the cloud

The Zero Trust Bundle is 100% cloud-managed, so there's no software to maintain or hardware to deploy. Administrators define zero trust policies, deploy endpoint agents, and manage authentication tokens all through WatchGuard Cloud, from a unified console. With built-in integration for leading deployment tools and multi-tenant management, organizations and managed service providers can be up and running quickly and scale easily.

> Continuous Verification Across Identity, Device, and Network

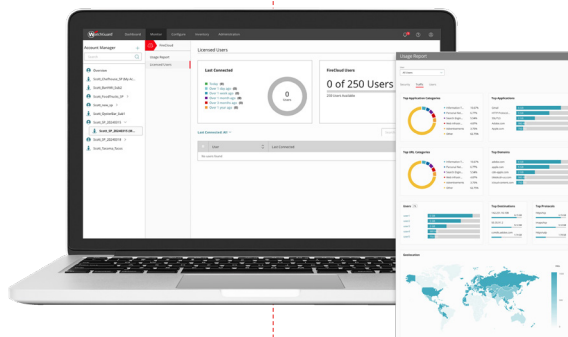


What's included in the Zero Trust Bundle



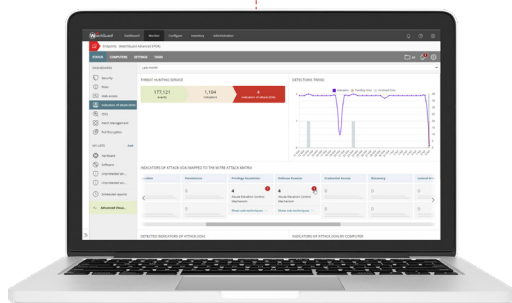
> Multi-Factor Authentication with Dark Web Credential Monitoring

With credential theft and account compromise on the rise, verifying identity is the cornerstone of zero trust. AuthPoint delivers multi-factor authentication, single sign-on, and risk-based policies that verify every user based on context. Integrated Dark Web Credential Monitoring proactively detects exposed credentials before attackers can exploit them. AuthPoint ensures the right person gains access, with the right factors, at the right time.



> Hybrid Network Security and Zero Trust Network Access

FireCloud Total Access merges secure Internet access and Zero Trust Network Access in one cloud service. It replaces VPNs with per-session, identity-based connectivity for SaaS and private apps. Firewall as a Service and Secure Web Gateway block phishing and malware on every network. Zero trust policies verify users and devices before granting access. Global PoPs keep sessions fast, encrypted, and invisible to attackers.



> Advanced Endpoint Security

WatchGuard Endpoint Security's AI engine monitors and classifies every process to block unknown or malicious activity automatically. The Zero-Trust Application Service prevents zero-day exploits and in-memory attacks. Continuous posture checks confirm each device meets security policy before access. Only trusted, compliant endpoints participate in zero trust connections.



AuthPoint Mobile App

AUTHENTICATION FUNCTIONS

Push-Based Authentication (online)

QR Code-Based Authentication (online and offline)

Time-Based One-Time Password (online and 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

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

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: 10.6 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



Want to learn more about the Zero Trust Bundle?

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

Dark Web Credential Monitoring

DETECTION METHODOLOGIES

Continuous credential monitoring

Correlation of compromised credentials by user account

Registers each detected breach event with the context

FireCloud

OS SUPPORT

Windows 7, 8, and 10

Gateway: Hyber-V (Windows Server 2022/2025, VMware ESXi 7.0/8.0, Proxmox 8.4/9.0)

DETECTION METHODOLOGIES

Block phishing attacks

Prevent C2 connections

Content filtering

Deliver immediate security awareness training

AUTHENTICATION SUPPORT

AuthPoint

SAML: Third-party IDP, Entra ID, Okta, FIDO

WatchGuard Cloud Directory: Active Directory, Entra ID, Cloud Directory

Session Level Identity Validation: Unified Zero Trust

MANAGEMENT & DEPLOYMENT

Management: WatchGuard Cloud central console for configuration, policy templates, multi-tenant service provider capabilities

Points of Presence: Global Network Across Five Continents

> How It Works

Authenticate > Validate > Enforce

- **AuthPoint** verifies user identity and assesses risk with each new session.
- **Endpoint security** checks device health and compliance in real time.
- **FireCloud** applies zero trust policies to govern access to web, SaaS, and private apps.
- **The Zero Trust Identity Framework** unites identity, device, and access verification into one continuous process.
- **ThreatSync XDR** correlate all activity for nonstop visibility, detection, and automated response.
- **WatchGuard Cloud** provides unified management for all services, simplifying policy creation, deployment, and reporting through a single, multi-tenant console.

About WatchGuard

WatchGuard® Technologies is a global leader in unified cybersecurity, purpose-built for managed service providers. Unlike others, WatchGuard delivers *Real Security for Real World* environments through its Unified Security Platform®, bringing networks, endpoints, and identities together with AI and zero trust advances for strong protection that scales. Trusted by more than 17,000 security resellers and managed service providers protecting over 250,000 companies, WatchGuard helps partners grow fast, eliminate operational drag, and deliver strong outcomes – without added vendors, consoles, or complexity. WatchGuard is headquartered in Seattle, Washington, with offices worldwide. Learn more at WatchGuard.com

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 WEB www.watchguard.com

WatchGuard Technologies, Inc.

©2025 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, AuthPoint, and ThreatSync 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.WGCE67895_112525