Zero Trust Deployment Guide

Turning Zero Trust into Action with WatchGuard

Introduction

Zero trust is no longer a theoretical framework, it is a practical, essential security model for modern organizations operating in hybrid environments. With users, devices, and applications distributed across cloud and remote locations, implicit trust has become a critical weakness. Every access request must now earn trust continuously.

This deployment guide provides a clear, practical roadmap to help organizations implement zero trust using WatchGuard's unified Zero Trust Bundle. It outlines the core steps, explains each product in the bundle, and offers guidance on how to license, purchase, and deploy the solution effectively.

The Six Core Steps to Zero Trust

Step 1: Establish Zero Trust Edge Protection

Zero trust begins where exposure is highest, the open Internet. Remote users spend most of their time accessing SaaS platforms and web-based services.

Deploy cloud-delivered security controls that inspect all web traffic, block risky websites, and apply zero trust policies based on identity and device risk. This ensures users are protected regardless of location.

Action: Deploy FireCloud and integrate with your client's strong authentication system.

- ☐ Deploy FireCloud Firewall as a Service (FWaaS) for all users
- ☐ Enable Secure Web Gateway (SWG) to inspect and control outbound web traffic
- ☐ Apply baseline zero trust policies for Internet access (identity + device posture)
- ☐ Configure policy rules for approved SaaS applications and risky website
- ☐ Validate traffic inspection, logging, and threat blocking functionality
- ☐ Test remote user protection from multiple network locations

Outcome: Protection follows users everywhere, blocking malicious sites and compromised connections before damage occurs.

Step 2: Verify Identity Continuously

Zero trust assumes every login attempt is untrusted until proven otherwise.

Deploy adaptive authentication mechanisms that enforce multi-factor authentication (MFA), single sign-on (SSO), and risk-based policies. Integrate credential intelligence to detect exposed credentials and prevent unauthorized access.

Action: Deploy strong authentication to all users. WatchGuard AuthPoint natively integrates with FireCloud through the WatchGuard Zero Trust Identity Framework.

- □ Enroll all users into MFA
- □ WatchGuard supports a Zero Trust Identity Framework that includes AuthPoint MFA as a strong foundation for organizations seeking a more adaptive and resilient zero trust approach.
- □ Enable adaptive MFA and risk-based authentication
- □ Configure single sign-on (SSO) for key applications
- □ Activate Dark Web Credential Monitoring
- □ Apply conditional access policies (location, device DNA, time)
- □ Test step-up authentication and lockout scenarios

Outcome: Only verified, uncompromised identities can initiate access.

Step 3: Validate Device Trust

A trusted user on a compromised device is still a threat.

Use endpoint protection to continuously monitor device posture, ensuring systems are patched, protected, and free of unknown or malicious processes before granting or maintaining access.

Action: Deploy EDR-level protection to all devices. WatchGuard EPDR offers advanced zero trust application and communication controls and integrates into the WatchGuard Zero Trust Identity Framework for superior protection.

- □ Install AI-powered EDR agents on all managed endpoints
- □ WatchGuard supports an endpoint-based zero trust model that incorporates EPDR to help organizations strengthen device trust and reduce risk as part of a broader zero trust strategy.
- □ Verify endpoint posture checks are active (patch level, protection status)
- □ Enable Zero Trust Application Service for real-time classification
- □ Configure device compliance thresholds
- □ Define automatic quarantine rules for non-compliant devices
- □ Validate endpoint telemetry visibility in WatchGuard Cloud

Outcome: Only secure, compliant devices participate in trusted sessions.

Step 4: Enforce Session-Level Access

Replace legacy VPNs with Zero Trust Network Access (ZTNA).

ZTNA ensures users only access the specific applications they are authorized to use for the duration of that session, based on current identity and device health.

Action: Utilize FireCloud ZTNA to create application-level secure access control with session-level verification via the WatchGuard Zero Trust Identity Framework.

- □ Identify applications to replace VPN access
- □ Configure FireCloud Total Access for private applications
- □ Apply session-based access policies per user group
- □ Test identity and device validation flow before session creation
- □ Disable or restrict legacy VPN access
- □ Validate encrypted, application-specific connectivity

Outcome: Granular, secure, VPN-free access that prevents lateral movement.

Step 5: Unify Management and Visibility

Zero trust must simplify operations, not increase complexity.

Implement centralized policy management and visibility to monitor authentication events, device risk, and access patterns from a single control plane.

Action: Utilize the WatchGuard Zero Trust Identity Framework to unify management and visibility by centralizing identity, device, and access controls in a single cloud-based policy engine. Gain insight into user behavior, device health, and authentication events through unified dashboards that eliminate blind spots and fragmented controls.

- ☐ Configure unified zero trust policies in WatchGuard Cloud
- ☐ Validate telemetry integration across identity, endpoint, and network
- ☐ Monitor dashboards for authentication and risk visibility
- ☐ Create alert thresholds based on risk conditions
- ☐ Enable reporting and compliance views

Outcome: One platform, one policy model, complete visibility.

Step 6: Integrate Automated Detection and Response

Security must adapt in real time as risk changes.

Synchronize identity, endpoint, and network telemetry to automatically adjust policies and revoke access when suspicious activity is detected.

Action: Utilize WatchGuard XDR to strengthen the Zero Trust Identity Framework by correlating identity, endpoint, and network telemetry to detect advanced threats and enable automated, coordinated response actions.

- ☐ Enable WatchGuard XDR correlation across AuthPoint, EPDR, and FireCloud
- ☐ Configure automated response playbooks
- ☐ Validate real-time session revocation for high-risk events
- ☐ Test incident response scenarios (compromised device, credential abuse)
- ☐ Monitor response timing and policy enforcement accuracy

Outcome: Threats are contained in seconds, not hours.

The WatchGuard Zero Trust Bundle

WatchGuard packages its zero trust capabilities into a unified solution that eliminates fragmentation and simplifies deployment.

AuthPoint – Identity Security and Credential Monitoring

Provides adaptive MFA, SSO, and risk-based authentication. Integrates Dark Web Credential Monitoring to detect compromised credentials and trigger automated response.

Primary Role: Continuous identity verification and access control.

EPDR – Endpoint Protection, Detection and Response

AI-driven endpoint security that validates device health, prevents ransomware, and blocks zero-day threats through real-time behavior analysis and Zero-Trust Application Service.

Primary Role: Device posture validation and threat prevention.

FireCloud Total Access

Extends network protection to remote users by enforcing cloud-delivered security policies while delivering secure, session-based access to private and cloud applications using Zero Trust Network Access (ZTNA) and cloud-based security controls.

Primary Role: Policy-driven application access and VPN replacement.

Licensing and Purchasing the Zero Trust Bundle

The WatchGuard Zero Trust Bundle is designed to make buying, licensing, and managing zero trust protection as simple and frictionless as possible. Instead of navigating multiple products, SKUs, and licensing terms, customers and partners interact with one clear, unified bundle that removes complexity end-to-end.

From quote to deployment, the entire experience is purpose-built for speed, clarity, and consistency.

Simple by Design: One Bundle, One Order

The Zero Trust Bundle is purchased using a single parent SKU that represents the complete solution. When this SKU is ordered, all required services and underlying licenses are automatically provisioned — no additional product selection, no manual configuration, and no risk of missing components.

This single order automatically enables:

- FireCloud FWaaS and Secure Web Gateway (SWG)
- FireCloud Total Access (ZTNA)
- AuthPoint Identity Services
- Dark Web Credential Monitoring
- EPDR Endpoint Protection

There is no need to:

- Select individual component SKUs
- Coordinate multiple license contracts
- Manage separate activation workflows

Everything is provisioned, aligned, and ready through one simple action.

Automatic Provisioning and Entitlement

Once the Zero Trust Bundle SKU is processed, WatchGuard systems automatically:

- Create all associated licenses
- Align license terms and expiration dates
- Deliver entitlements directly into WatchGuard Cloud
- Make services available for immediate deployment

This automation dramatically reduces administrative effort, eliminates configuration errors, and accelerates time-to-protection.

Unified Licensing and Renewal Experience

All services within the Zero Trust Bundle operate under a co-termed license lifecycle, providing:

- One unified start and end date
- One renewal event
- Predictable billing and budgeting
- Clear, centralized license visibility

Customers renew the bundle once and all underlying services continue without disruption or reconfiguration.

End-User Purchasing Process

For end customers, the process is intuitive and efficient:

- Engage your preferred WatchGuard partner to define requirements
- Select the user count required
- Partner submits the order using the single SKU
- WatchGuard provisions all services automatically
- Security teams can deploy immediately through WatchGuard Cloud

Distribution Ordering for WatchGuard Partners

For partners, the process is equally streamlined:

- Select the Zero Trust Bundle SKU
- Place the order through your authorized distributor
- WatchGuard auto-provisions all licenses
- Services appear in WatchGuard Cloud for customer assignment

License Management Made Simple

All Zero Trust Bundle licenses are managed centrally within WatchGuard Cloud, offering:

- Real-time usage and expiration visibility
- Simple assignment for users and devices
- Easy expansion without service disruption
- Clear renewal alerts and lifecycle tracking

As customer needs evolve, licenses can be adjusted with no architectural changes or redeployment required.

Conclusion and Next Steps

Zero trust is no longer an abstract theory, it is a practical operating framework for securing modern, distributed organizations. By applying continuous verification across identity, device, and access layers, organizations gain stronger protection, clearer visibility, and simplified control without sacrificing performance or user experience. With the WatchGuard Zero Trust Bundle, security becomes unified, scalable, and operationally efficient, enabling teams to move confidently from strategy to execution.

Next Steps

- Evaluate zero trust maturity level
- Define deployment timeline and scope
- Activate a trial license of FireCloud and get started on your journey to zero trust security.

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.