

WatchGuard NDR for Firebox

Cloud-Delivered Network Detection and Response

See, Prove, and Protect Everything Crossing Your Perimeter

WatchGuard NDR for Firebox delivers what traditional firewalls and logs can't: real-time, actionable visibility into every inbound and outbound connection across your network. It transforms raw Firebox traffic into actionable intelligence, enabling security teams to validate policy enforcement, detect external threats such as command-and-control (C2) activity, data exfiltration, and misconfigured communications.

Built entirely in the cloud and integrated directly into your WatchGuard Firebox deployment, WatchGuard NDR eliminates the cost and complexity of hardware-based NDR platforms. No sensors. No packet capture infrastructure. Just pure, policy-validating perimeter insight.

Why It Matters

Perimeter blind spots are real. Firewalls enforce rules but don't confirm if they're working as intended, or if unauthorized traffic is slipping through.

WatchGuard NDR closes this gap with:

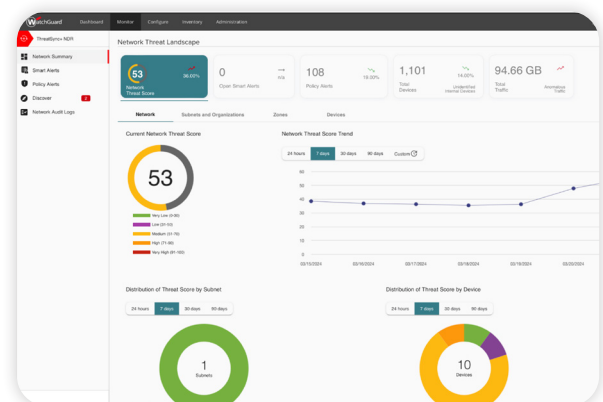
- Complete north-south visibility through Firebox
- Cloud-based analytics powered by WatchGuard's AI Engine
- 24/7 detection of serious external threats
- Verifiable ingress/egress monitoring for compliance
- Automated remediation by blocking IPs and devices

Powerful, Practical Protection

WatchGuard NDR transforms every Firebox into a real-time threat detection engine. It delivers instant visibility into inbound and outbound traffic, validates policies, and detects advanced threats like C2, exfiltration, and brute-force attacks. With cloud-native deployment, there's no new hardware to manage; instead, you get fast setup, smart alerts, and automated reports that support compliance and response.

Key Use Cases

- **Prove Firewall Effectiveness:** Show that policies aren't just in place – they're working.
- **Accelerate Investigations:** Correlated alerts reduce time-to-insight and simplify response.
- **Simplify Compliance:** Generate automated ingress/egress evidence for audits or cyber insurance.
- **Spot Unauthorized Connections:** Detect risky outbound traffic and misconfigurations.



Built for Lean Security Teams

WatchGuard NDR is optimized for the way SMEs and mid-market organizations operate today. It works with the Fireboxes you already have – across HQ, branches, and remote environments – delivering consistent, high-fidelity detection without the complexity of a full SOC. There's nothing extra to tune or maintain. Just turn it on and gain the clarity your team has been missing.

Make Your Firebox Smarter

Your WatchGuard Firebox already defends your perimeter; WatchGuard NDR helps you prove it's working. By turning every Firebox into a real-time detection sensor, you gain the intelligence and evidence to stay ahead of today's threats and tomorrow's audits. From validation to visualization to compliance, WatchGuard NDR delivers clarity at the edge – without complexity at the core.

WatchGuard NDR for Firebox Compatibility

Tabletop Appliances

- Firebox T25
- Firebox T80
- Firebox T115
- Firebox T125
- Firebox T145
- Firebox T185
- Firebox T85-PoE

Rackmount Appliances

- Firebox M290
- Firebox M295
- Firebox M390
- Firebox M395
- Firebox M590
- Firebox M595
- Firebox M690
- Firebox M695

Cloud/Virtual Firewalls

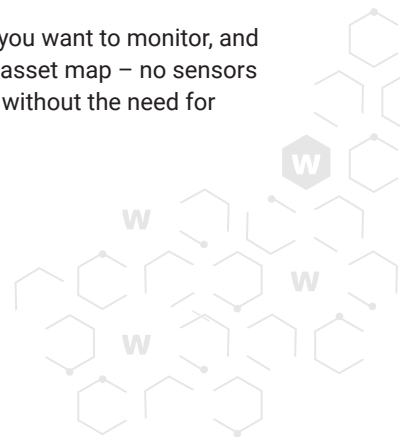
- Firebox Cloud Medium
- Firebox Cloud Small
- FireboxV Micro
- FireboxV Medium
- FireboxV Small

Frictionless Deployment

Deploying WatchGuard NDR takes minutes. Activate the service in WatchGuard Cloud, select the Fireboxes you want to monitor, and start streaming telemetry. The platform immediately begins analyzing traffic logs and building a contextual asset map – no sensors or packet capture required. Default detection policies are active from the start, and alerts begin to populate without the need for manual tuning. It's enterprise-grade protection, without the enterprise overhead.

If you're already a Firebox customer, setup is fast and straightforward:

1. Purchase WatchGuard NDR for Firebox
2. Enable WatchGuard NDR in WatchGuard Cloud.
3. Select Fireboxes for monitoring.
4. Traffic, VPN, and DHCP logs are analyzed automatically.



About WatchGuard

WatchGuard Technologies is a global leader in unified cybersecurity, purpose-built for managed service providers (MSPs). For more than 30 years, WatchGuard has defined how MSPs deliver security at scale, continuously innovating to stay ahead of every major shift in the threat landscape. WatchGuard's AI-powered Unified Security Platform® delivers zero trust-aligned network, endpoint, and identity protection in a single, integrated platform, enabling MSPs to reduce operational complexity, improve security outcomes, and grow their businesses more efficiently. Trusted by more than 25,000 MSPs protecting over 1.5 million customers worldwide, WatchGuard enables partners to deliver strong, measurable security outcomes for customers across the globe. Learn more at [WatchGuard.com](https://www.watchguard.com).