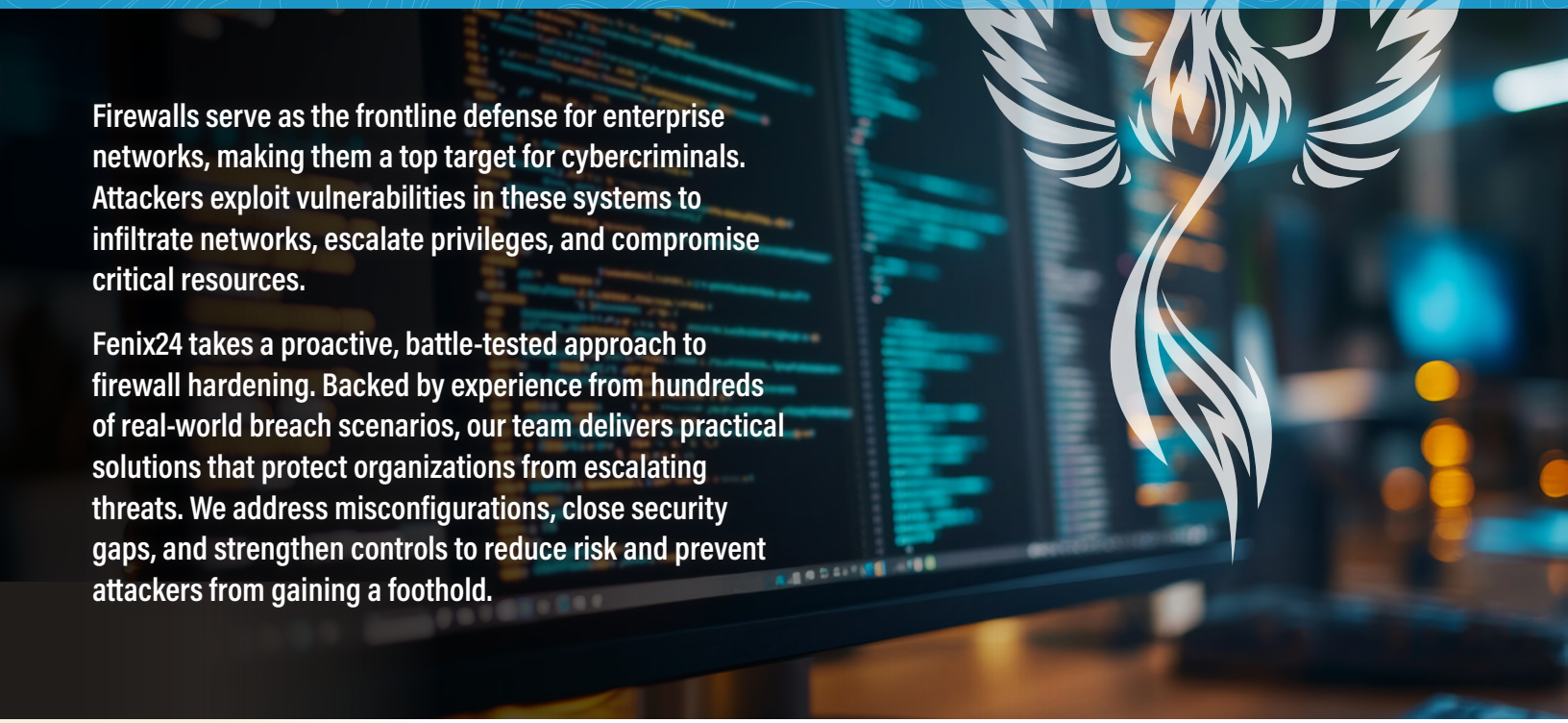
Securing Your Perimeter



Firewalls serve as the frontline defense for enterprise networks, making them a top target for cybercriminals. Attackers exploit vulnerabilities in these systems to infiltrate networks, escalate privileges, and compromise critical resources.

Fenix24 takes a proactive, battle-tested approach to firewall hardening. Backed by experience from hundreds of real-world breach scenarios, our team delivers practical solutions that protect organizations from escalating threats. We address misconfigurations, close security gaps, and strengthen controls to reduce risk and prevent attackers from gaining a foothold.

Why It Matters

A COMMON ENTRY POINT FOR THREAT ACTORS

Firewalls are one of the most frequently exploited entry points for cyberattacks. Threat Actors (TAs) leverage outdated firmware, improper access management, and VPNs without multi-factor authentication (MFA) to bypass defenses. Without proper security measures and access controls, organizations remain vulnerable.

KEY FIREWALL SECURITY CHALLENGES

Misconfigurations: Excessive privileges, dormant accounts, inadequate access controls, outdated firmware, and vague rules allowing unauthorized traffic into the network create openings for TAs.

Outdated Protocols and Practices: Legacy authentication methods, poorly created and managed rule sets, and VPN access without MFA increase risk.

Lack of Visibility: Many organizations struggle to monitor and audit firewall changes and traffic coming across the network, leading to blind spots that attackers can exploit.

Outdated Firmware: Older firmware with known vulnerabilities is one of the most common points of entry for TAs.

FENIX24

Fenix24's Approach to Firewall Hardening

We deliver a systematic and proactive strategy for securing firewalls that leverages industry best practices and advanced tools to detect, mitigate, and prevent vulnerabilities. Our methodology includes:

Comprehensive Review

- Evaluate the current firewall configurations, access policies, and firmware.
- Identify vulnerabilities and misconfigurations.

Firmware Updates

- Ensure firewalls are running the latest, most secure firmware.

Access Management

- Implement local accounts for management access.
- Restrict management access to specific IP addresses.
- Remove WAN management access.
- Remove Active Directory (AD) auth for management access.

Inbound and Outbound Traffic Control

- Restrict traffic to only essential ports to minimize risk exposure.

Additional Security Enhancements

- Enforce mandatory MFA for VPN access.
- Implement dedicated logging servers to ensure all network traffic is properly captured for security analysis.

Defense in Depth

Defense in depth is a layered security strategy that uses multiple defensive measures to protect an organization's network. Firewalls play a critical role in this approach by providing different layers of traffic filtering and access control. This strategy also includes SIEM and EDR technology that can help detect anomalies and provide alerting for fast response times to limit data exfiltration.

Why Choose Fenix24?

Fenix24 combines deep cybersecurity expertise, innovative tools, and a commitment to strengthening network defenses. Our team partners with organizations to:

- Proactively reduce attack surfaces.
- Strengthen detection and response capabilities.
- Align security strategies with business goals.

Let's Get Started

For more information or to schedule a consultation, call 423.305.7890 (press option 2) or email us at rapidresponse@fenix24.com.