

Make Unpatched Vulnerabilities Unreachable with Zero Networks

Identity-based microsegmentation automatically contains exploits, buying enterprises time to patch safely without costing business continuity.

Frontier AI models are collapsing the window between vulnerability discovery and exploitation, leaving security teams buried under an avalanche of patches while AI-driven attacks move at machine speed.

You can't out-patch AI. Instead, enterprises need a proactive containment layer that leaves attackers with nowhere to go – regardless of how they gain initial access or how fast they move.

#1

Initial Access Vector

Vulnerability exploitation is the most common way attackers get in.

Verizon Data Breach Investigations Report, 2026

-7 Days

Mean Time to Exploit

On average, vulnerabilities are exploited before a patch is available.

Mandiant M-Trends Report, 2026

↑56%

AI-Driven Attacks

Attackers are weaponizing AI while defenders are stuck chasing them.

IBM Cost of a Data Breach Report, 2026

Preemptive Cyber Resilience for the AI Era

Rushing an unvalidated fix into production trades one business risk for another. Zero Networks' identity-based microsegmentation buys security teams time to patch safely by closing unnecessary access paths by default, enforcing MFA for privileged access, and scaling protection across the entire network.

Build a Closed-by-Default Architecture with Identity-Based Microsegmentation

Vulnerabilities give attackers a foothold. Open internal access is what turns that initial compromise into a business crisis. Granular network segmentation combined with identity-based access controls proactively limit how far any breach can spread – even if an unpatched vulnerability gives attackers a way in.

“

Having microsegmentation in place has really given us a precautionary protection layer so we can delay applying some of these patches. This gives us plenty of time to test, make sure everything's working, and then apply it, but still have that protection layer in place.

”

— Aaron Goodwin, CISO, B. Riley Financial

Enforce MFA on Privileged Internal Pathways

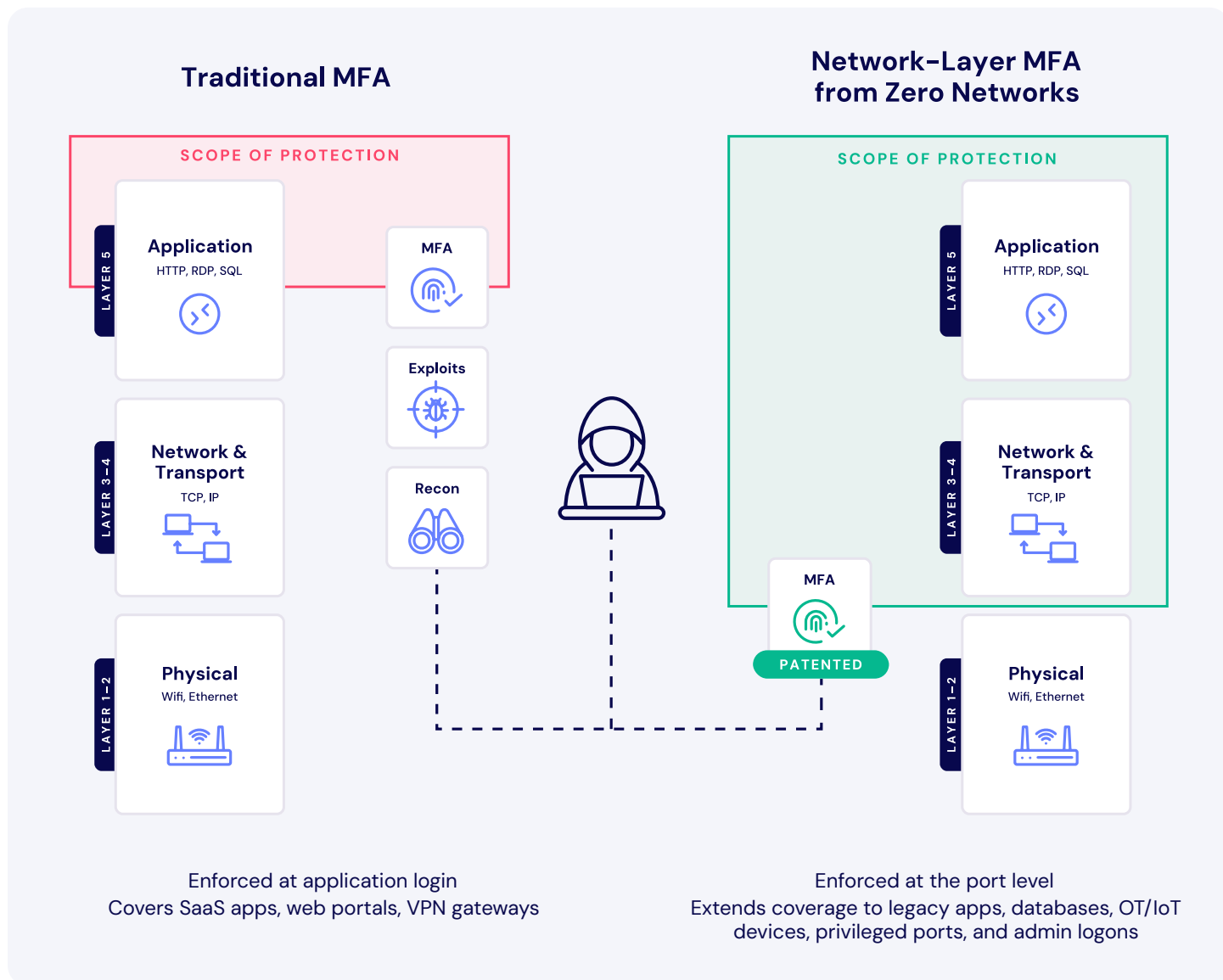
Over 70% of enterprise threat activity flows through admin ports and protocols – they're the highways attackers use to leverage initial access into operational disruption. With Zero Networks' Layer 3 MFA, admin ports, sensitive systems, and critical services stay closed by default, then open after just-in-time verification – only for pre-approved identities, and only for a limited window.

Even if attackers exploit a vulnerability to gain a foothold, they can't use admin pathways to expand it, giving teams time to test patches before deploying them without leaving the business exposed.

Traditional MFA vs. Zero's Network-Layer MFA

Traditional MFA keeps attackers from coming through the front door – leaving internal systems exposed. Legacy MFA can't reach legacy applications, databases, OT and IoT devices, PaaS solutions, and the admin protocols that IT teams rely on every day to keep the business running.

Zero's patented network-layer MFA protects internal systems that legacy MFA doesn't.



Protect Legacy, OT, and Other Hard-to-Patch Systems

Legacy applications, OT and IoT devices, and end-of-life infrastructure can't be patched on short notice – or at all. Zero Networks enables security teams to contain what can't be patched, governing access to every system with identity-based policies.

An attacker can't exploit an unpatched legacy system to move laterally if there's nowhere to go. Zero's agentless approach seamlessly integrates with existing infrastructure and uses native OS components to deliver comprehensive, non-disruptive microsegmentation.

**Build a containment architecture
with Zero Networks to protect
uptime while patching safely.**

[Request a Demo](#)

