MINI MFA GUIDE:

Extend MFA Beyond Login. Close the Privileged Pathways Attackers Rely On.

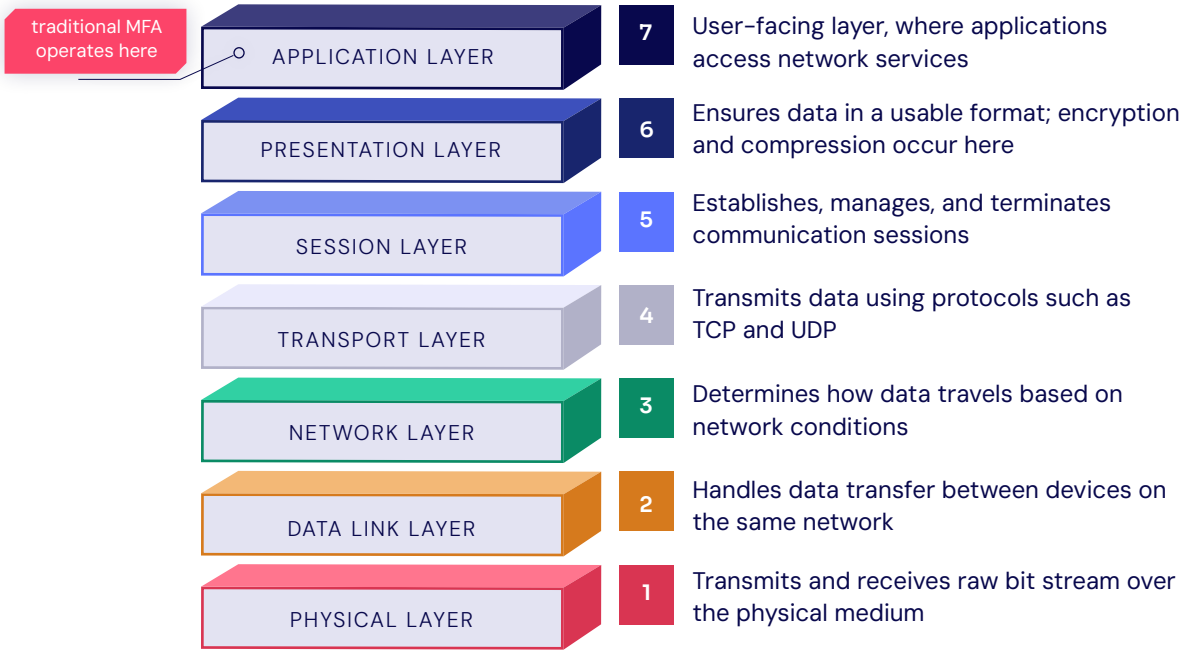
A 4-step playbook for enforcing just-in-time authentication on admin ports and sensitive systems, so lateral movement highways stay closed by default

Most enterprise risk today isn't driven by sophisticated exploits or novel zero-days that enable initial access. Instead, threat actors rely on valid logins and normal, trusted access paths that traditional MFA wasn't built to protect.

To stop identity-based threats from escalating into full-blown business crises, security teams need network-layer MFA that reinforces granular segmentation without adding operational complexity.

Where (Conventional) MFA Operates: Layer 7 of the OSI Model

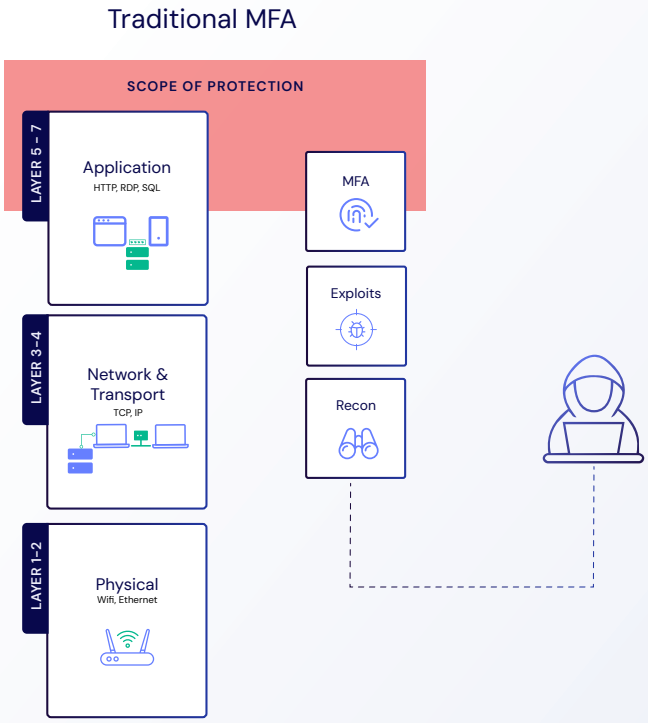
Conventional MFA operates at Layer 7 of the OSI model – the application layer. While this strategy effectively protects SaaS applications and web portals, it leaves privileged ports and protocols, legacy systems, and other non-SaaS assets operating below Layer 7 unprotected.



The result?
Most MFA protects login portals, cloud apps, VPN gateways, and email platforms – governing authentication at the entry point into an application without determining what happens inside the network, after initial access.

But identity isn't just how attackers gain an initial foothold – it's also how adversaries escalate minor incidents into high-impact breaches.

> There's a structural gap between where MFA enforcement stops and attackers' movement begins.



Security Gaps Left by Traditional MFA

Breaches escalate due to unchecked lateral movement – not advanced tactics for gaining initial access. Traditional Layer 7 MFA leaves organizations vulnerable to threats that use identity as a vehicle to expand blast radius and drive business disruption.

Credential abuse remains a top initial access vector[1]

» Today, most attackers don't break in – they log in. When attackers exploit valid credentials, traditional MFA only blocks 1.5% of adversary attempts.[2]

71% of threat activity flows through four admin protocols

» SMB, RDP, WinRM, and RPC are high-trust highways for IT operations – they're also lateral movement thoroughfares.[3]

A single compromised system gives attackers access to 85% of the environment in one hop[4]

» Overly permissive internal access makes it easy for attackers to expand reach and escalate privileges; 99% of cloud users, roles, and services held excessive permissions – often unused for 60 days or more.[5]

Machine identity and service account sprawl

» Overprivileged, under-monitored machine identities (like service accounts and API tokens) make up over 70% of networked identities.[6] And AI agents inheriting excessive privileges are only compounding the problem.

Legacy apps and non-SaaS assets create an orphaned attack surface

» From databases and OT infrastructure to custom internal tools and beyond, legacy systems typically can't be onboarded to an identity provider and don't support modern authentication protocols.

[1] Verizon Data Breach Investigations Report, 2026
[2] Microsoft Digital Defense Report, 2025
[3] Zero Networks Threat Analysis: "One Compromised System and BOOM, Meet Your Blast Radius"
[4] Zero Networks Threat Analysis: "One Compromised System and BOOM, Meet Your Blast Radius"
[5] Unit 42 Global Incident Response Report, 2026
[6] SC Media, "Fast networks, fast hackers: Microsegmentation gets a security comeback"

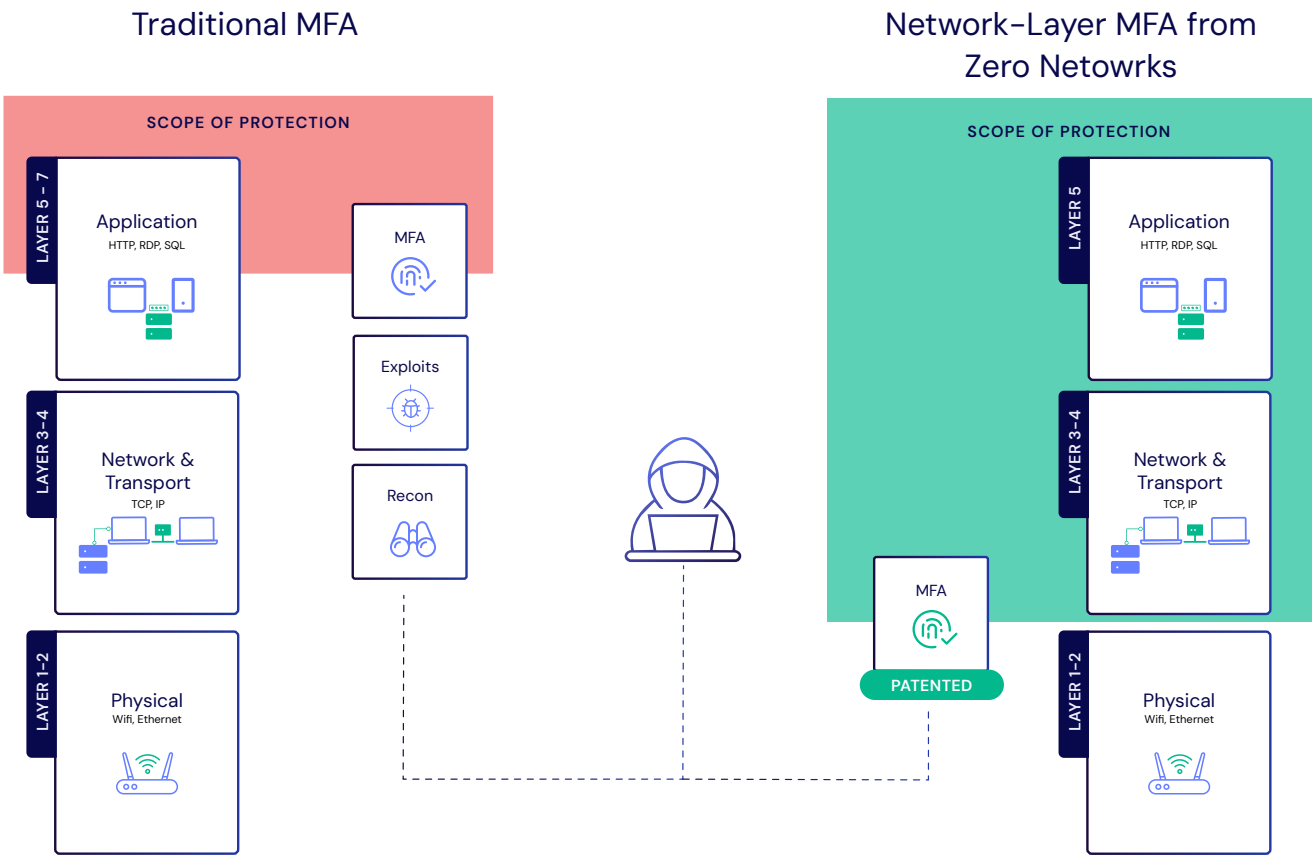
The Solution

Network-Layer MFA: Enforce Just-in-Time Authentication Anywhere

Unlike conventional MFA, which operates at the application level and requires users to verify their identity through SMS codes, authentication apps, or hardware tokens, Zero Networks' patented network-layer MFA is seamlessly integrated into the network infrastructure at Layer 3 of the OSI Model.

Rather than only prompting authentication when a user opens an application, network-layer MFA triggers verification long before a session reaches the application layer – directly at the point of access.

With just-in-time (JIT) MFA enforcement, ports open dynamically for a limited amount of time – privileged users can only access pre-approved assets after authenticating, and only temporarily.



> The combination of Zero's network and identity segmentation capabilities redefines least privilege architecture, providing a level of protection that the market has never seen before. It allows security teams to control network device segmentation down to the port and protocol level and then layer complete control of user logon access by logon type – network, local, service, etc. As if that wasn't enough, you can also add multi-factor authentication to any of those controls! You simply can't do this using any other platform on the market today. Security teams need to take note and get ahead of the game.
>
> **- Chris Turek, Former CIO, Evercore**

Stop Identity-Based Attacks with Multi-Factor Segmentation:

A 4-Step Playbook

Security teams looking to do more than apply another login challenge can build a comprehensive defense against identity threats in four steps.

Step 1:

Apply Microsegmentation to Enforce Least Privilege at Scale

Minimizing blast radius and limiting the scope of breaches requires a closed-by-default architecture that restricts what assets every identity can reach once inside the network, and not just where they can enter. Microsegmentation is key to operationalizing that architecture, protecting every asset (including legacy systems) inside its own secure zone so lateral movement pathways must be explicitly defined.

Because microsegmentation creates networks where lateral movement is constrained structurally, an attacker who compromises one system can't freely pivot to the next.



Step 2:

Extend Granular, Identity-Based Access Controls Across the Network

Using the same fine-grain approach used to microsegment every asset, security teams must apply granular, least-privilege logic to who – or what – is connecting. The goal is to restrict access to operational need only, eliminate implicit trust, and ensure that no identity (human or machine) carries more reach than is strictly necessary.

By enforcing identity-based access controls internally on the network layer, organizations can de-escalate identity as an attack vehicle – even when adversaries are armed with legitimate credentials. The combination of network and identity segmentation creates the framework for a resilient, self-defending architecture.



Step 3:

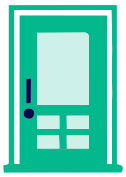
Eliminate Standing Privileges with Just-in-Time Access



With the right architecture in place, the next lever is tightening the privilege model itself. Persistent, always-on access to privileged systems and activities is one of the most consequential structural conditions enabling modern attacks. Still, when administrative users need to perform privileged functions, a closed-by-default strategy can create operational friction without a contingency plan in place.

JIT access with network-layer MFA eliminates standing privilege by replacing persistent permissions with time-bound, purpose-bound access that expires automatically. Users and systems request elevated access when they need it, verify their identity, receive a scoped grant for a defined window, and lose access when that window closes.

FRONT DOOR
Login or VPN



Traditional at Layer 7

INSIDE THE PERIMETER

Zero Networks puts MFA on every door on the inside

✓MFA **LEGACY APP** RDP *Port-level, just-in-time*	✓MFA **DATABASE** 1433 / 5432 *Port-level, just-in-time*	✓MFA **OT / IOT** Modbus / S7 *Port-level, just-in-time*
✓MFA **CLOUD VM** SSH *Port-level, just-in-time*	✓MFA **ADMIN PORT** WinRM / SMB *Port-level, just-in-time*	✓MFA **FILE SHARE** SMB / NFS *Port-level, just-in-time*

Step 4:

Enforce Network-Layer MFA on Admin Protocols



Network-layer MFA extends protection to the protocol level itself. With microsegmentation defining internal pathways, identity-aware controls determining who or what can traverse those pathways, and JIT verification policies eliminating standing privileges to control when certain actions or assets are accessed, network-layer MFA makes dynamic enforcement across high-traffic, high-risk areas possible.

Redefine least privilege architecture with Zero Networks –
implement identity-based microsegmentation reinforced by network-layer MFA.

Request a Demo→

©2026 Zero Networks. All rights reserved.

ZERO Networks