ZERO Networks

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

USE CASES

Apply MFA to Anything in a Click

TL;DR

Multi-factor authentication (MFA) stops nearly all of identity thefts but is typically limited to SaaS applications that live in the cloud. As a result, MFA is underutilized in most enterprise environments.

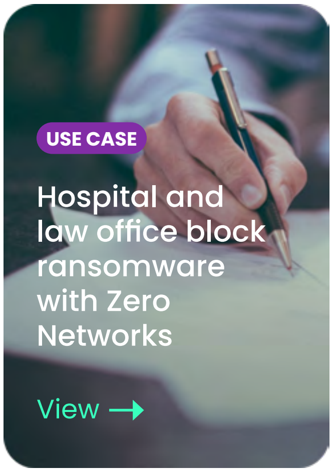
Whether on prem or in the cloud, Zero Networks Segment is the only solution that applies MFA at the port level, enabling just-in-time MFA to clients, servers, and to any asset that could not have been protected by MFA so far, such as legacy applications, databases and OT/IoT devices.

Apply MFA to:

- **Legacy Applications**
- **OT/IoT Devices**
- **Databases**
- **PaaS Solutions**
- **IaaS VMs**
- **On-Prem VMs**
- **Global Clients**
- **Any Protocol**

Almost all organizations use some form of multi-factor authentication (MFA) as an extra layer of security to protect user access to SaaS applications.

With MFA, users are required to provide at least two pieces of evidence to verify their identity, such as a password and a biometric scan, a security token, or a one-time code sent to their mobile device. This added layer of security makes it nearly impossible for attackers to gain unauthorized access to user accounts: Even if an attacker obtains a user’s password, they will unlikely possess the additional factor of authentication.



USE CASE

Hospital and law office block ransomware with Zero Networks

View →

However, applying MFA to non-SaaS assets is difficult. Most organizations struggle to apply MFA on PaaS solutions, legacy applications, databases and OT/IoT devices. Only a few vendors enable MFA on the application layer (specifically, applications that support Kerberos or NLTM). These solutions may cause a false sense of security as attackers often exploit protocol vulnerabilities (especially if not patched on time) to take control of a machine even it is protected by MFA. In fact, all attackers need to overcome MFA is just an open port.

As a result, the stopping power of MFA is underutilized in most enterprise environments.

Glossary

What is multi-factor authentication (MFA)?

View →

The Zero Network way: Tie MFA to the network layer

Zero Networks Segment is a patented and only solution that applies MFA at the port level (network layer): Any protocol, operating system and applications above will be protected with MFA without agents or need to rewrite the application. Tying MFA to the network layer also denies attackers access to vulnerabilities (including zero / one-day) in the organization, preventing them from moving laterally and compromising the organizational network.

Zero Networks Segment enables just-in-time privileged access with self-service MFA to apply security to any abnormal activity, privileged users or anytime extreme security is required.

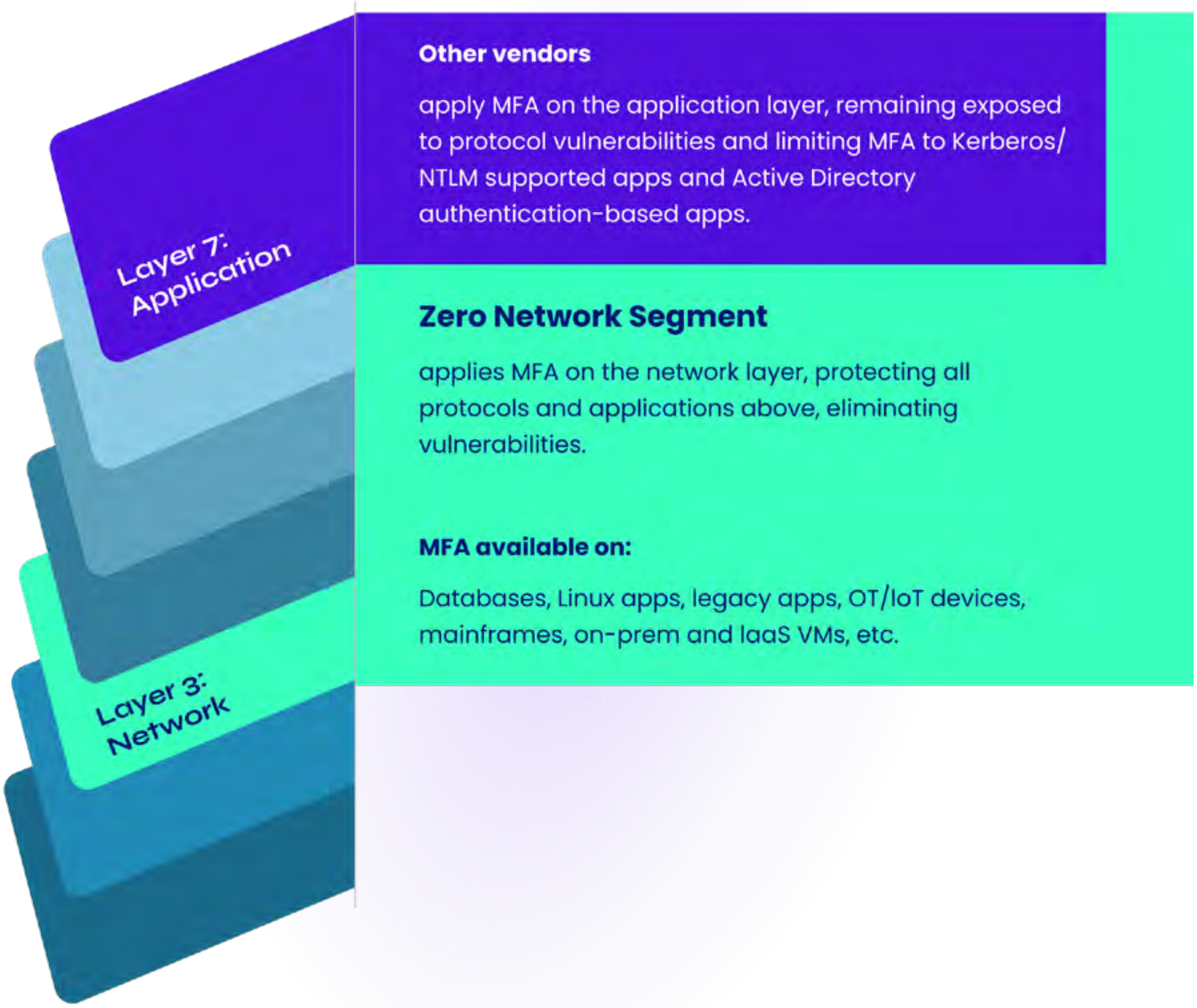
A common scenario: MFA for RDP / SSH

One of the most common use cases is enabling administrators and IT teams to remotely access various servers, on prem and in the cloud, using remote administration protocols like RDP, SSH and WinRM. However, these protocols are also widely used by attackers to move laterally across the network. To ensure server access is allowed to authorized users only, Zero Networks Segment automatically blocks all incoming traffic on administrative ports and prompts users for just-in-time MFA, before temporarily opening the port to the authenticated users for a limited amount of time.

Users can authenticate using the organization's preferred identity provider (for example, Duo, Okta or CyberArk) or can use email or SMS authentication.

By applying MFA at the port level, Zero Networks can protect assets that could not have been protected by MFA so far: legacy applications, databases, OT/IoT devices, mainframes, on-prem VMs, and IaaS VMs.

Zero Networks Vs Other Vendors



Other vendors

apply MFA on the application layer, remaining exposed to protocol vulnerabilities and limiting MFA to Kerberos/NTLM supported apps and Active Directory authentication-based apps.

Zero Network Segment

applies MFA on the network layer, protecting all protocols and applications above, eliminating vulnerabilities.

MFA available on:

Databases, Linux apps, legacy apps, OT/IoT devices, mainframes, on-prem and IaaS VMs, etc.

ABOUT SRC CYBER SOLUTIONS LLP

SRC Cyber Solutions LLP is a renowned name in India for Cybersecurity. We are known for our exclusive distribution of cutting-edge solutions in India, GCC, Africa and APAC. We take pride in offering a comprehensive suite of Cybersecurity solutions which includes Platforms and Technologies for AI-powered Comprehensive Email Security, Automated Patch and Endpoint Management, Asset Visibility and Risk Management, securing the Cloud environments with Hybrid Cloud Workload Protection, enhancing Network Security with Agentless Micro- Segmentation, ensuring Third-Party Data Flow Management and API Management, and Agentless Compliance Management, thereby strengthening our commitment to protecting organizations against evolving known and unknown Cyber Threats. With a focus on embracing innovation, we continuously evolve to meet the dynamic threat landscape, offering a comprehensive range of Nex-Gen technologies with a high degree of automation, reducing the dependency on IT Resources and ensuring a strong value proposition.