# The 1% of Ports Causing 90% of Breaches

**Closing the privileged port gap that gives attackers free reign in your network**


Administrative ports like SSH, RDP, RPC, WMI, SMB and more are the main attack vectors in most ransomware campaigns and attack tool kits. **In fact, Remote Desktop Protocol (RDP) alone was involved in 90% of ransomware incidents investigated in 2024.**

While legacy microsegmentation solutions may block most of the 65,535 available network ports, they typically leave these privileged administrative ports permanently open, enabling lateral movement and essentially leaving the network highly vulnerable.

Security and Operations teams find themselves conflicted over the question of privileged ports, presenting network admins with an impossible dilemma:

- **IT teams** request to leave these ports open to enable administrative access.
- **Security teams** request to close these ports as they pose a serious risk.

**To solve this,**
Zero Networks developed a solution for dynamically securing administrative ports. This patented technology enables Just-In-Time access to privileged ports:

**1 MFA required**

*Any attempt to access a privileged port on a protected machine is blocked at the network level.*

**2 MFA verification**


*The admin requesting access is authenticated via MFA.*

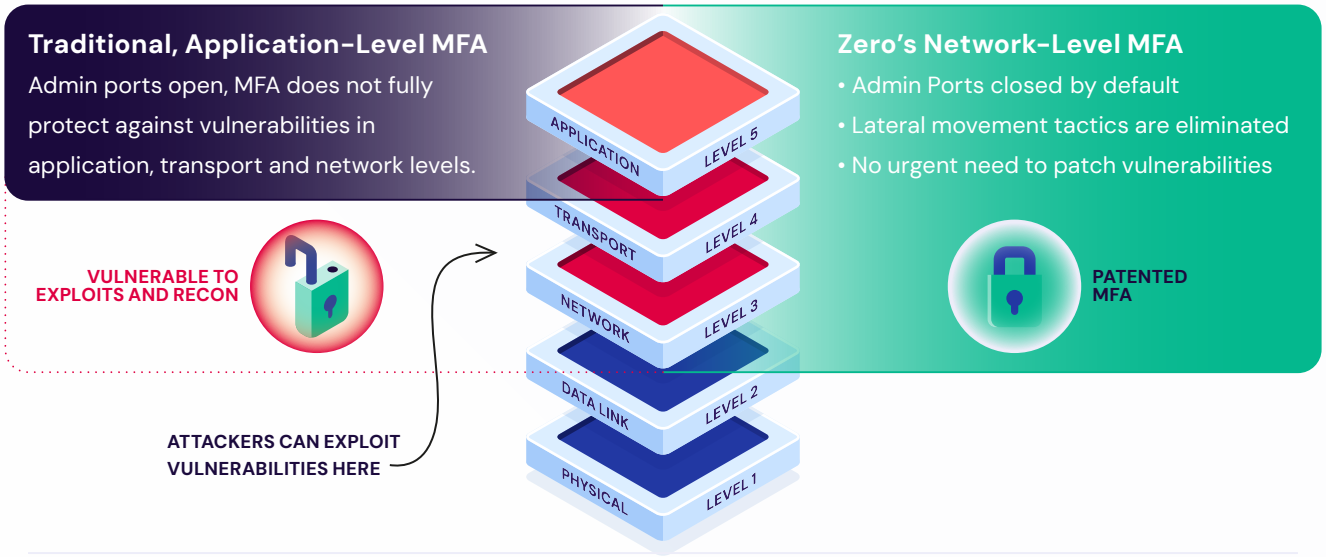
**3 Access granted**

*The port is opened only to connection from this device and only for a limited duration.*

**How is this different** from traditional, identity-based, application-level MFA?

Identity MFA solutions run on application level protocols such as NTLM or Kerberos, whereas threat actors use vulnerabilities that can be exploited before the authentication layer. An anonymous, unauthenticated packet with a malicious payload can exploit these vulnerabilities and is therefore unaffected by this level of protection.

Zero Networks' MFA on the other hand happens at the Network level, effectively preventing RDP-based exploits. Blocking connections to devices at the network level makes them invisible to the attackers, making even recon impossible and significantly reducing the risk of an effective ransomeware attack.




Zero Networks uses this technology and more to deliver **the most secure microsegmentation** solution on earth:

- Non-intrusive, agentless deployment
- Automatically create and apply least-privileged policies to network devices identities
- Dynamically enforce access to privileged ports using network-level MFA
- Provide proxyless, high-performance Zero Trust Network Access

Visit our website to learn more: **zeronetworks.com**

**"Zero's Networks redefines least privilege architecture, providing a level of protection that the market has never seen before."**

*Chris Turek, CIO of Evercore*

ZERO. Networks