USE CASES

Comply with Cyber Insurance

TL;DR

As cyber-attacks become more frequent and sophisticated, cyber insurance is becoming mandatory for businesses of all sizes. Insurers and government regulators have put network security requirements in place, with MFA, network segmentation and secure work-from-home access taking centerstage. Zero Networks offers a single, simple platform for MFA-enabled microsegmentation and Zero Trust remote access, streamlining insurance and regulatory compliance and lowering the recently skyrocketing insurance premiums.

Cyber Insurance Requirements

Cyber-attacks are becoming increasingly common and sophisticated. As more and more sensitive information is stored and transmitted online, businesses are at risk of operations disruption, financial loss, reputational damage, and legal liabilities in the event of a breach. That's why cyber insurance is quickly becoming mandatory for businesses of all sizes.

Some industries already require cyber insurance as part of their contractual obligations or as a condition for doing business with certain clients or partners. The state of New York's Department of Financial Services, for example, has issued a cybersecurity regulation that requires financial institutions to maintain cybersecurity programs that include the evaluation of insurance coverage for cyber risks. Similarly, some federal contractors are required to carry cyber insurance as part of their contract requirements.

Insurers have put strict network security requirements for policyholders: multi-factor authentication (MFA), network segmentation and secure work-from-home access are the main pillars. Implementing these requirements not only helps comply with the insurer's policy but also helps

lower the recently skyrocketing premiums and comply with government regulations, such as PCI DSS for credit card transactions, HIPAA for the healthcare industry and even the EU's GDPR.

One Platform, Total Compliance

Zero Networks Segment™

MFA **Network Segmentation**

Extending just-in-time MFA well beyond SaaS:

Apply MFA to any port, protocol, and application, even those that could not have been protected by MFA

Microsegmentation of every asset:

Segment any client, server, OT, on-prem and in the cloud – automatically and without any agents

Zero Networks Segment™

Secure Remote Access

Connecting employees and vendors using Zero Trust:

Leveraging the speed of VPN and the security of ZTNA – without their flaws

Just-In-Time MFA for Everything

Nearly all cyber insurance companies require policyholders to implement multi-factor authentication (MFA) for accessing critical systems and applications.

Zero Networks' patented MFA solution is the industry's most comprehensive way to secure client-to-server and client-to-client sensitive traffic. Zero Networks Segment applies MFA at the network layer, 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.

Privileged traffic, such as RDP, WinRM and SSH, can only be accessed after a multi-factor authentication prompt is approved. This MFA prompt can be configured using third-party identity providers (e.g. Duo, Okta, CyberArk), or by using standard methods such as SMS, email, or a browser pop-up. The JIT (just-in-time) access provided by the MFA prompt ensures a

Glossary

What is multifactor authentication (MFA)?
View →

What is Microsegmentation?
View →

What is Network Segmentation?
View →

What is Zero Trust Network Access (ZTNA)?
View →

frictionless yet secure connection for a limited time. This prompt can be limited to a specific group of admins or made available to any user.

Microsegmenting Every Asset - Nowadays, a simple firewall on the perimeter is no longer enough to secure a network. According to Ponemon Institute's 2022 Cost of Insider Threats report, insider threats account for 82 % of all cyber incidents, which cannot be prevented by traditional firewall solutions. Microsegmentation, which is the technique of breaking down the network into smaller, firewall-protected segments, is widely accepted as the ultimate network segmentation solution. Zero Networks Segment makes implementing it easier than ever before. Zero Networks Segment places a firewall "bubble" around every asset which completely blocks lateral movement. It leverages the host-based firewall built into each asset , protecting servers, clients, and even OT/ IoT devices, both on-prem and in the cloud. Zero Networks Segment is agentless and fully automated, as opposed to legacy solutions that require agents and manual rule creation. This saves significant time and cost on deployment and maintenance and makes the solution highly scalable for any organization size.

Zero Trust Remote Access - Zero Networks Connect, which combines the speed of VPN and the security of ZTNA (while eliminating their flaws), is the optimal answer for secure work-from-home connectivity. Although a VPN provides great network speeds, its open port to the internet is vulnerable to brute-force attacks. On the other hand, while ZTNA provides a secure, zero-trust connection, routing all traffic through the cloud introduces latency and incurs high costs. Zero Networks Connect offers the best of both worlds by providing true Zero Trust connectivity without compromising on speed and performance. Plus, as soon as an employee connects, all of Zero Networks Segment's rules and MFA policies apply to them.

Insured and Secured - Zero Networks' agentless, automated solutions make cyber insurance and regulatory compliance simple. JIT MFA policies for privileged applications, true and total microsegmentation and Zero Trust remote access are the ultimate combo for maximum security and compliance for organizations of all sizes.

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.