ZERO Networks

SRC CYBER SOLUTIONS LLP
CYBER RISK SOLUTIONS

USE CASES

Defeat Ransomware Attacks in Real Time

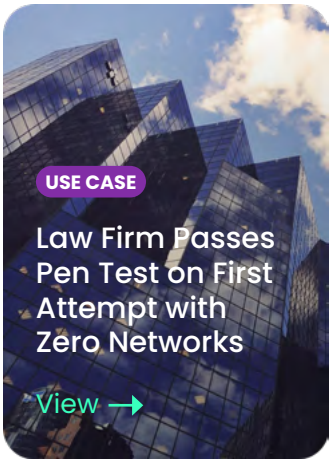
TL;DR

Increasingly sophisticated, ransomware accounts for 70% of malware-related breaches and is the fastest growing cybercrime activity. Microsegmentation, which places a firewall bubble around each asset on the network, is the most effective defense against ransomware. Zero Networks Segment offers an automated, agentless, MFA-enabled microsegmentation solution that can prevent ransomware attacks from scanning the network and propagating to other assets. In incident response cases, Zero Networks stops an attack within less than 24 hours while keeping most of the network operation intact, using a fully hands-free approach.

The Challenge of Ransomware

Ransomware is the fastest growing "hacker trend" according to the 2022 Data Breach Investigations Report (DBIR). It accounts for 70% of malware-related breaches, and 25% of all data breaches. The adversaries behind these attacks have grown more sophisticated. They have developed their own customized tools that are difficult to detect while also deploying advanced techniques like Hypervisor Jackpotting and bypassing EDRs. Ransomware has become a big, profitable business for cybercriminals—and a top concern for security teams.

While the length of a ransomware attack can vary from several hours to several months, the basic plot is almost always the same. The attackers' main goal is to compromise one machine to get a foothold inside the organization, then escalate their privileges, move laterally and quickly compromise and encrypt as many assets as they can, demanding ransom payment in return for the decryption key, and causing their victims severe business disruption and reputational damage. The linchpin for ransomware is lateral movement which enables ransomware to spread far and wide within an organization. It's the reason, according to a report from IBM, that the average cost of a ransomware attack was $4.54 million in 2022. Luckily, lateral movement also relies on a basic assumption: the



compromised machine will have direct network line of sight to other machines that contain profitable data or IP to steal or encrypt.

Microsegmentation to the Rescue- Understanding this assumption makes the solution clear: microsegmentation, i.e., placing a firewall bubble around each asset on the network – every client and server, on prem and in the cloud. Microsegmentation is the most robust defense against lateral movement as it leaves attackers stranded. But it also has a reputation for being costly, labor intensive, and difficult to maintain and scale. This is because legacy solutions involve installing an agent on every asset and then manually creating firewalls rules for each asset, something that is infeasible for most mid-sized and enterprise organizations.

The Fix: Automated, Agentless, MFA-enabled Microsegmentation at Scale
Zero Networks Segment is a military-grade, MFA-enabled microsegmentation solution. It deploys as a virtual appliance that remotely manages the host-OS firewall of every machine in the network to microsegment them without agents . It monitors and learns all network connections over a period of up to 30 days, and then creates corresponding and highly accurate firewall rules and policies . The policies allow legitimate traffic, hence transparent to end users, and apply just-in-time MFA to privileged remote admin protocols like RDP, SSH or WinRM that are also used by attackers to move laterally. At the end of the learning period, Zero Network Segment prevents ransomware attacks from scanning the network (as there are no open ports to scan), finding and exploiting vulnerabilities, and propagating to other assets in the network. Even if credentials are compromised, the just-in-time MFA approach ensures that these credentials cannot be utilized.

Stopping a Ransomware Attack That's Already Underway- What if no segmentation solutions are in place and a ransomware attack is underway? In such a case, manually segmenting each asset in the network is simply too slow. Zero Networks can stop the attack in less than 24 hours while keeping most of network operation intact, using its fully automated, hands-free approach. In such incident response cases, where immediate intervention is required to stop ransomware spread, Zero Networks Segment learns about 80 % of network activities in under 24 hours and applies MFA on all the rest. This approach keeps most legitimate network traffic intact, allowing organizations to resume normal operations while manual firewall rules are created for any network activity not captured by the 24-hour learning.

Glossary

Our Definitive Guide to Ransomware
View →

Developers

Ransomware Open Source Toolkit
View →

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.