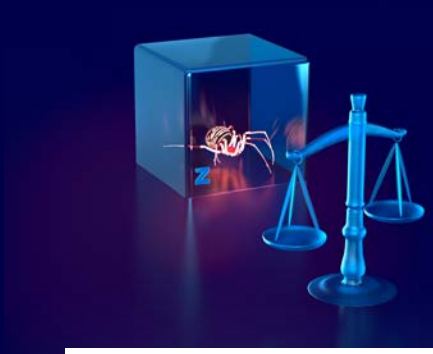

A leading law firm implements Zero Networks to overcome legacy segmentation techniques

The past few years have been a **nightmare for security executives**. The normalization of remote work and unprecedented employee turnover resulted in many organizations **struggling to adapt and protect their network**.

As a result, networks began to convolute with countless potential points of entry. **Developing an impenetrable exterior became impossible**. And with access permissions exponentially increasing as a result of remote work, one successful penetration could compromise the entire organization[1]. **Organizations had to reduce the excessive network access privilege within their networks** to quarantine compromised machines. That has proven to be easier said than done.

The challenge

The shortcomings of legacy segmentation techniques

Segmentation presents problems for organizations of all sizes. Its manual approach presents barriers to entry every step of the way.

01

Documenting all traffic flows and application functionality

The process of mapping an organization's network is tedious, requiring enormous amounts of employees, while prone to error.

02

Implementing access controls

Establishing access controls effective enough to stop lateral movement requires sophisticated policies and experts that not readily available for most organizations.

03

Deploying firewalls to enforce access controls

Deploying firewalls is expensive and difficult to implement, requiring hair pinning that causes unnecessary latency. Even after overcoming those initial barriers to entry, agents cause additional administrative burden.

04

Performing maintenance and management

While segmentation cuts down on excessive network access, it doesn't provide visibility into the identity of users. Attackers illicitly perusing through networks can easily seem like normal traffic, meaning administrators can easily overlook hidden attacks.

To solve these issues, **organizations must automate each step** to reduce implementation and maintenance costs. However, building a security platform with all those capabilities would require further expertise and time investment. **So how did a law firm achieve micro segmentation with a single dedicated IT employee**?

[1] https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/

The solution

Implementing Zero Networks' adaptive MFA segmentation

A leading securities class action and derivative law firm in the United States needed their SOC 2 certification, a compliance prerequisite to demonstrate their network is secure enough to store sensitive information. This included passing a penetration test, and in this case, one of the most advanced automated testing platform on the market – **Pentera**.

Pentera, that recently raised $150M at a $1B evaluation, simulates a cyberattack by continuously scanning networks for vulnerabilities and credentials, using them to spread to additional machines. This simulates an adversary propagating inside a network, without causing any real harm.

Passing this test was highly challenging for the law firm. The firm only had one dedicated IT person, who had no security background. Thus, despite having a relatively small network, manual segmentation was not an option.

Working with a tight budget and timeline, the firm needed a single solution that was simple and automated while requiring minimal oversight and maintenance. Enter Zero Networks.

Segmenting the network in a few hours

The firm first used Zero Networks to discover the managed and unmanaged assets in their network, giving their IT team details of the overall exposure level of each asset while providing detailed insights into network topology.

Unlike traditional segmentation techniques where teams would assess the entire map of connections before creating policies and trust zones, the firm **automated the entire segmentation processes** as well as placed MFA policies for all admin access, effectively locking down the entire network.

Within a few hours, the firm passed the pen test with flying colors.

Passing a world-class penetration test

Phase 1

Scanning the network attack surface

In the first phase of the simulated attack, Pentera's reconnaissance efforts were stale as critical vulnerabilities were not seen. With Zero Networks protecting the network, the test did not have the required access to detect, let alone exploit, such vulnerabilities. In fact, Pentera found that only 3% of protocols were accessible – domain controllers, file share, printers, and other machines that had to be accessible to all devices in the network.

Phase 2

Harvesting credentials and elevating privileges

The second phase of the test included various attempts at harvesting credentials from the network or utilizing vulnerable protocols for MITM and relay attacks. Here, the test was again only successful in collecting credentials of lower privileged accounts, and performing relay attacks against one file service, which by nature had to be open to the entire network.

Phase 3

Simulating an attack with a breached account

The last phase of the pen test used gained credentials, provided by the law firm, to spread to additional resources inside the network. Even with the initial entry, every following attempt to peruse through the network was blocked by automatic MFA policies, protecting the harvested credentials from being misused for gaining access to additional resources.

Key Takeways

Beyond completing their SOC2 certification, the firm was able to implement a proven segmentation strategy – a feat that traditionally takes organizations years to build in-house – in just a few hours.

Using Zero Networks, the firm was able to:

Automatically generate a report of their entire network attack surface (try it out yourself with our free tool!), eliminating tedious work while futureproofing against a fast-changing environment.

Lock down all access points by extending MFA everywhere with a single click, removing the need to develop access policies and manually deploy firewalls.

Provide an identity-based access controller to prevent attacks, even with stolen credentials, from moving laterally inside the network.