Microsegmentation in a Click

A SANS First Look

Written by **Matt Bromiley** | October 2023

Introduction

Recently, security teams have focused on the concept of zero trust architecture, which, for an organization to achieve fully, requires both microsegmentation and ZTNA (zero trust network access). Theoretically, when combining these two solutions, an organization can mitigate or prevent attacks, especially those requiring lateral movement for success. However, these projects often raise concerns that stem from technical feasibility and the delicate balance between security and user needs. This is especially true for microsegmentation, which is often considered the harder of the two to implement but also the most beneficial.

In this SANS First Look, we consider a product that challenges the notion that microsegmentation is too difficult to realistically implement: Zero Networks Segment™, part of the Zero Networks platform. A microsegmentation solution that centrally manages host-based firewalls and automates policy implementation in *real time*, Segment provides an agentless solution to effective zero trust. Segment installs easily into any active environment, with minimal overhead, and offers granular MFA enforcement across IT and OT networks.

In our initial exploration, we found that Segment's microsegmentation capabilities empower organizations to help secure all forms of access to systems and resources, including remote access. Effective, host-based zero trust, however, offers more capabilities. It can implement strong lateral movement blocks, stopping adversaries in their tracks or ensuring that privileged and non-privileged accounts only access the *correct* resources respectively.

A Look at Zero Networks Segment

We began our First Look at Segment with its rapid, agentless deployment throughout an organization. Zero Networks allows you to manage deployment (and subsequently access policies and controls) all through a centralized platform. As it works seamlessly within any Windows Active Directory, Linux data center, both on-premises or in the cloud, an organization can get up and running *in hours* with Segment. Furthermore, deployment is fully automated—configure it and Segment does the rest.

Figure 1 provides a screenshot of the initial dashboard.

As mentioned earlier, Segment offers a completely agentless approach to host-based zero trust via microsegmentation. Rapid deployment means a return on value is quick. The other inherent benefit teams can find with Segment is limited user impact. After all, effective microsegmentation allows users to access only the resources they need, which should, in theory, provide zero disruption.

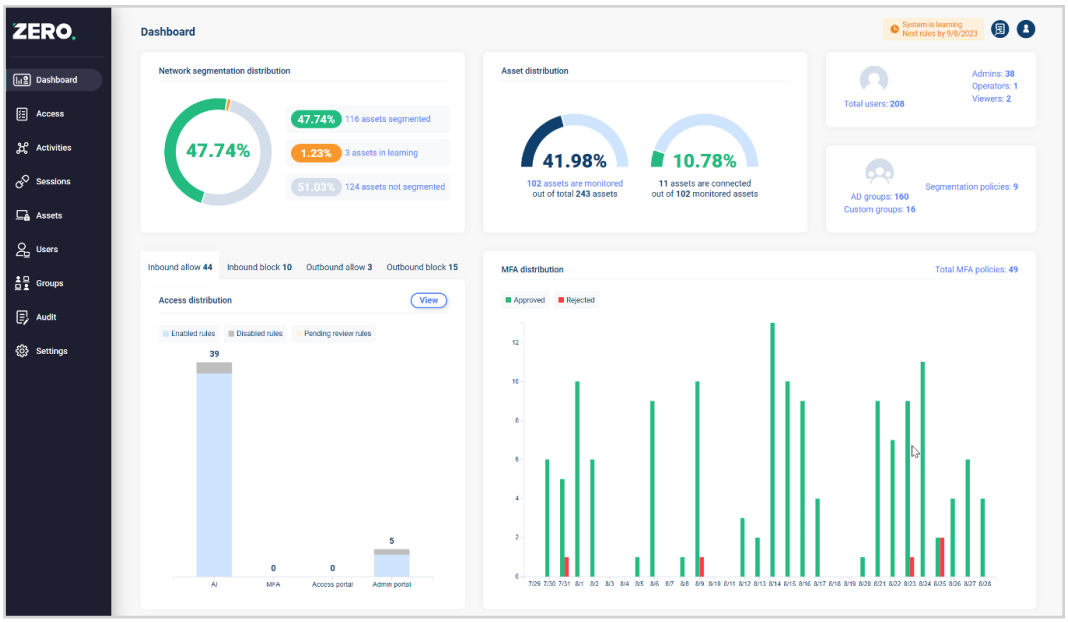

Figure 1. Screenshot of Segment's Dashboard

This capability enables organizations to incorporate Segment into their playbooks and use cases almost immediately, a benefit in contrast to tools that often take weeks or months to deploy. Some of the immediate use cases we see from Segment include:

- Enabling MFA on *any* activity, including privileged activities or access to any resource
- Limiting or stopping adversary lateral movement, putting a dent in ransomware success
- Simplifying network security operations with accurate and automated policy design and enforcement
- Restricting red team or penetration testing activities or, conversely, aiding organizations in passing a penetration test
- Complying with cybersecurity insurance requirements

Once in place, Segment provides an easy-to-use interface for uncomplicated policy creation, management, and enforcement. This ease of use further lowers the barrier to entry because security teams can implement policies immediately, helping achieve microsegmentation goals quickly and locking down their networks. Figure 2 provides a screenshot of a sample access policy within Segment.

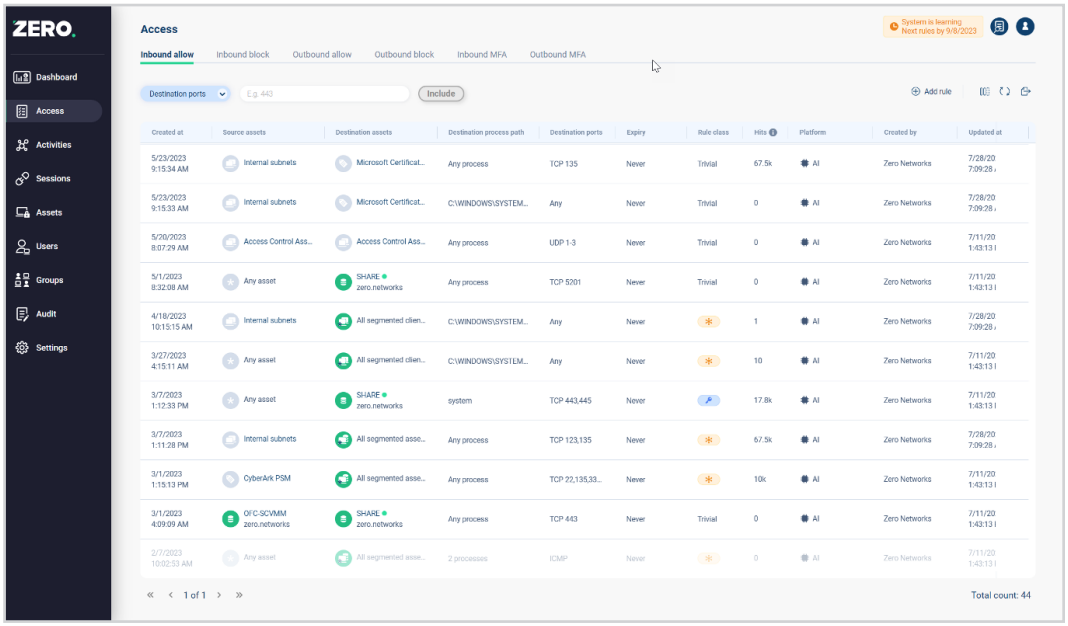

Figure 2. Sample of Access Policy Within Segment

Segment also allows you to issue blanket policies to protect the environment against attacks. For example, teams may want to implement an outbound block to the untrusted internet from various systems, subnets, or system types. In these cases, Active Directory integration allows for easy system classification and segmentation. It also can automatically block malicious IPs and domains, relying on threat intelligence sources to increase the confidence and assessment of network traffic.

One of Segment's most significant benefits is the enabling of multi-factor authentication (MFA) policies around any concept within the organization. We observed that Segment can wrap MFA around any protocol, application, or asset across the entire organization. This capability is unique to Zero Networks and is one of the inherent benefits of enterprise-wide deployment with granular controls. The security team can lock down any object anytime, restricting access to only the necessary users—a key concept of zero trust.

Granular MFA also can reshape the security landscape for many organizations by allowing them to safely deploy applications or use remote access protocols without fear of potential compromise. Although MFA is imperfect, it reduces risk significantly compared to single-factor or unprotected protocol exposure. For example, consider remote access such as Remote Desktop Protocol (RDP). RDP is necessary for remote system administration but can pose significant security risks. Segment lowers those risks, as shown in Figure 3 on the next page, with a tightly controlled MFA policy and access revocation at any time.

Our assessment walked through the various other features of Segment, including detailed entity analysis and an access map, providing yet another viewpoint into *who* can access *what* across the organization. Segment also has an incredibly robust and automated tagging capability, allowing for quick internal- and external-facing asset classification.

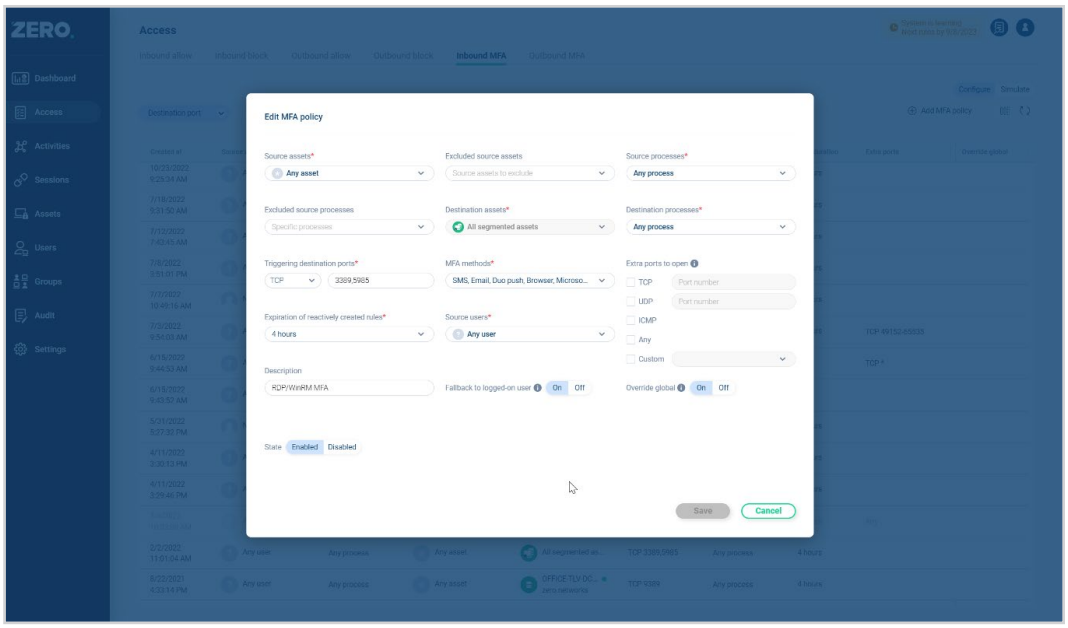

Figure 3. Screenshot of Segment's RDP MFA Policy

Closing Thoughts

Overall, we found Zero Networks Segment to be an easy-to-use tool that can safely introduce the idea of microsegmentation to any applicable network. For organizations on a path toward a better zero trust strategy, Segment can help them find alignment and help implement zero trust concepts with little friction. Deployment is rapid and automated, meaning teams can get to work soon.

Furthermore, many organizations may need to realize how powerful microsegmentation concepts can be. As we explored Segment, we found many attacks and access violations that are minimized or prevented with microsegmentation and enterprise-wide MFA enforcement. Ransomware and other attacks that rely on lateral movement cannot compete. These blocks can bolster a security team's confidence, allowing them to focus on keeping the organization secure rather than constantly chasing attacks.

Sponsor

SANS would like to thank this paper's sponsor:

ZERO. Networks