A CISO's Guide to Micro-Segmentation

Today's data-driven, multicloud environment is an increasing target for hackers and micro-segmentation is increasingly regarded as a key defense mechanism against stealthy attacks and data breaches. It is the software-based extension of network segmentation but in a micro-segmented network, perimeters are fine-grained and applied at the workload level. Micro-segmentation is also based on the *Principle of Least Privilege*, which establishes that every module in the environment (such as a process, a user, or a program, depending on the subject) should only be able to access the information and resources necessary for legitimate purposes. It is the fine-grained control and the *Principle of Least Privilege* which make micro-segmentation far more effective as compared to traditional network segmentation. In a multicloud environment, this translates into each workload only being permitted to make connections necessary to accomplish its tasks and is typically implemented through basic ACLs (access control lists).

However, ACL-based controls alone are not enough to secure all layers in the protocol stack. Virtualization and cloud coupled with workloads moving around continually have created a visibility challenge for security teams, making it very necessary to complement micro-segmentation with a full spectrum of strong policy enforcement controls. Security teams need to be able to not only detect and block attackers but also to learn the identity and techniques being employed by attackers to be better prepared for future attacks.

While micro-segmentation is increasingly viewed as an ideal approach, there are a few factors that have hindered the adoption of micro-segmentation technologies to date:

- Many solutions do not work uniformly across a multicloud environment that then requires leveraging different approaches and toolsets to cater to each cloud environment.
- Many of the solutions are not scalable.
- And many may require upfront large investments and expert knowledge requirements.

CHECKLIST: HOW TO TAKE THE PAIN OUT OF MICRO-SEGMENTATION

Here are some tips to make the micro-segmentation process go smoother.

☐ **Leverage a consistent approach.**

- ☐ Look for a solution that offers multi-vendor support: This is a fundamental requirement for visibility and consistent policy across your cloud-extended enterprise.

☐ **Automate and orchestrate policy at scale.**

- ☐ Leverage an automated approach to discovering workloads and applications across multiple clouds: Agentless approaches that leverage machine learning can identify connection patterns, protocols and ports that are being used in a non-intrusive manner. The results of this discovery process form the foundation of the *Principle of Least Privilege*, which is key to the creation of micro-segmentation policy. In addition to enabling scale and agility, automation is essential to achieving the *Principle of Least Privilege*.
- ☐ Group workloads according to behavior, configuration and function: Machine learning automates the process of workload grouping and generating and assigning policy through clustering. In today's large-scale and dynamic cloud environments, it is impossible to accomplish this manually.

- ☐ Validate automated groupings and recommended policy: Fine tune as necessary.

☐ **Apply the full spectrum of security controls.**

Employ security controls that span through Layer 7 to ensure that sensitive workloads and data are optimally protected.

- ☐ Access Control at Layer 4 to secure against unauthorized access.
- ☐ Threat Prevention and Data Loss Prevention (DLP) at Layer 7 to protect against data infiltration and exfiltration.
- ☐ Deep Packet Inspection (DPI) at Layers 4 through 7 to uniquely detect and prevent the lateral spread of threats.
- ☐ Sandboxing technologies can complement DPI to further disrupt threats at their origin.

When employed with strong policy controls has strong advantages for enabling secure multicloud environments. However, orchestration and automation are essential for achieving a uniform approach to micro-segmentation and also ensuring the *Principle of Least Privilege*. In today's cloud environments, automation is also essential to securely enabling the velocity and scale that business and engineering require.

SHIELDX MAKES SECURITY THE EASIEST THING ENTERPRISES DO IN THE CLOUD.

Our cloud-native, network security platform elastically delivers a full stack of agentless security controls—IPS, firewall, malware prevention, microsegmentation, and more—to protect data centers, cloud infrastructure, applications, and data. Our driving philosophy is to bring cloud speed, scale, and orchestration into the hands of security professionals worldwide. Based on cloud agnostic microservices technology, ShieldX ensures that security teams understand and maintain vigilance over cloud operations and workflows by continuously translating a security's intention into controls as cloud infrastructure rapidly evolves. Today, customers including Alaska Airlines and IDT have saved millions of dollars by eliminating control sprawl and consolidating security processes to dramatically reduce tactical systems management.

SHIELDX

ShieldX Networks, Inc.
2025 Gateway Place, Suite 400
San Jose, CA 95110 USA

+1 408.758.9400
info@shieldx.com
www.shieldx.com

October 2018