TRUEFORT

ARTICLE

How To Stop Lateral Attacks With Workload Microsegmentation

Forbes Technology Council

Sameer Malhotra
FORBES COUNCILS MEMBER

Sameer Malhotra is co-founder and CEO of TrueFort, a former Wall Street tech exec and an expert in IT infrastructure and cyber security.

Network segmentation is a widely accepted tool for improving performance and boosting security. By splitting a network into multiple parts or segments, it's possible to establish more granular controls, manage policies more effectively, boost compliance and isolate certain attacks or activities.

No one would argue that the concept isn't valid — and useful. Yet implementing network segmentation — particularly microsegmentation — can be difficult, error-prone and expensive to manage and maintain. Moreover, microsegmenting the network only addresses part of the threat challenge, leaving gaps that attackers can exploit. For organizations looking to build a robust zero trust security framework, a complementary security capability that incorporates applications and their workloads is more effective at responding to today's growing lateral movement threats.

As a result, a growing number of organizations are turning to more advanced intelligent, behavior-driven, workload segmentation. Using this approach, it's possible to detect and prevent attacks that evade conventional network segmentation and implement zero trust security at the application layer.

Gain Speed And Accuracy With Dynamic, Behavior-Based Analysis

Within a conventional framework, network segmentation relies on a north-south traffic perimeter to slow or halt threat actors. This zoning model inspects data packets using a combination of methods — including VLANS, ACLS and VFRs — and a set of rules about what to let in or out based on IP addresses. While this is necessary, it's not sufficient to detect and respond to unwanted activity at a granular level where lateral movement takes place.

At the heart of the problem, much of today's data arrives as a result of workload communications originating in microservices architectures. As it passes through systems, it can carry and spread threats. Unfortunately, conventional methods of network segmentation and microsegmentation do not deliver insights into this east-west traffic flow. In fact, the sheer volume and amount of change inherent in workload data overwhelms traditional network segmentation and results in out-of-date and erroneous policies.

Intelligent application workload segmentation takes aim at this challenge by creating a unique runtime behavioral trust profile (think of it as an identity) for each application and workload. This identity is baselined for trusted behaviors, regardless of where those workloads are running (on-prem, in a container or in the cloud). Intelligent automation generates a real-time trusted activity graph for all applications in the environment and auto-generates accurate and effective security policies based on known trusted behaviors. It then automatically maintains these policies based on the behavior of each workload.

In the end, there's no need for a complex and often ineffective rules-based approach — and the manual oversight and intervention that typically comes with it. Intelligent workload segmentation auto-generates policies based on trusted behaviors. These policies are as granular as an organization requires — and it's easily and continuously updated as needed.

Speed Up Zero Trust

As networks and security become more complex, organizations require sophisticated tools to better manage threats. Microsegmentation of workloads is a major step forward in implementing a zero trust strategy. With an intelligent behavior-based workload segmentation framework in place, organizations gain an array of advanced capabilities. These include improved business uptime with fewer segmentation policy errors, faster time to value through auto-generated segmentation policies, lower total cost of ownership as a result of reduced application security overhead, and zero trust integration.

Intelligent workload segmentation helps organizations stay agile and respond quickly to specific signals and events while eliminating blind spots that occur using conventional tools and technologies. It also enables better network oversight and zero trust policy enforcement at the application layer.

FIVE ELEMENTS OF INTELLIGENT WORKLOAD SEGMENTATION

Consider these five best practices for implementing intelligent workload segmentation:

1. **Comprehensive application and workload visibility.** Collect telemetry from applications, identities and network devices to gain unified, real-time discovery, visualization and traffic flow mapping of discrete application workloads across cloud, hybrid, virtual, container-based and traditional server environments. Among other things, this translates into a view of inter-application relationships and dependencies, including trusted and untrusted relationships.
2. **Create context-based policies.** Use the visibility mentioned above to create segmentation policies based on a contextual behavioral understanding (not a set of rules or frameworks) of workload activity. These policies are easily adapted and, therefore, more secure.
3. **Apply fine-grained controls.** Using workload behavioral attributes and runtime context rather than IP addresses, enforce highly granular policies based on network, identity and process attributes that span specific workload runtime contexts across bare metal servers, VMs and containers.
4. **Enforce zero trust.** By applying zero trust principles inside the network perimeter, even if threat actors breach segmentation barriers, their activity will be detected when they attempt to move laterally. As a result, an organization can mitigate problems early to reduce or eliminate damage.
5. **Centralize administration.** Unify the management of segmentation policies across physical servers, VMs, containers and clusters and cloud workloads as well as a range of operating system configurations to improve your security posture and reduce exposed attack surfaces.

ABOUT TRUEFORT

TrueFort reduces business risk for security-focused enterprises striving for zero or lean trust application environments. Our innovative and uniquely application-centric Fortress platform delivers comprehensive realtime cloud-to-the-ground insight, protection and automated response with patented machine intelligence and a single or bring-your-own agent. Fortress overcomes the application security blindspots inherent in legacy infrastructure-centric tools, providing unparalleled visibility and protection for applications in on-prem, hybrid and cloud environments and for security teams across the enterprise. Fortress speeds response times, minimizes the blast radius of compromises, prioritizes resources, and enhances application risk posture.

TRUEFORT

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM