GuardiCore

Micro-Segmentation Architecture Choices: Agent vs. Agentless

There's a great debate among different schools of solution architects about the adequate type of server solution deployment options: an agent-based approach that requires installation on every workload or an agentless approach that relies on third-party APIs or network-level access.

Overview

Due to the complex and dynamic nature of modern data centers and clouds, along with very high traffic rates, data center security architecture requires us to control the workloads themselves within the perimeter. As has been demonstrated many times, once attackers make their way into the data center they are able to move laterally to any workload within and thus, micro-segmentation has become one of the strongest security controls and the preferred project when talking data center security.

To implement effective and secure micro-segmentation controls, it is not enough to place single or multiple choke points at the egress or ingress of the network/VPC. There's a great debate among different schools of solution architects about the adequate type of server solution deployment options: an agent-based approach that requires installation on every workload or an agentless approach that relies on third-party APIs or network-level access.

Agentless Segmentation

The agentless approach usually relies on third-party controls in order to collect and control traffic.

Some of the possible ways to collect network flow in agentless environments are to use span port, ingest netflow from existing infra equipment or leverage cloud APIs.

The approach to actual traffic control in an agentless solution either relies on implementing network choke points or pushing rules to existing network enforcement control on the different workloads.

Agent-Based Segmentation

An agent-based approach assumes that genuine real-time protection requires control of the workload itself. In order to use this method, software is deployed on the workload.

The software would usually either use existing user space mechanisms and only push policy to an existing control on the workload. Another method is for the software to employ its own mechanism that leverages the different OS APIs in order to implement the network-layer enforcement.

Agentless Solutions are not Enough to Secure the Data Center and Cloud

Agentless solutions are not sufficient to truly secure the hybrid data center in today's era. Some of the restrictions of these solutions include:

- Requires hairpinning of traffic through a single network point, resulting in a constrained and unscalable solution
- No real L2 network visibility or control. Any traffic on that same VLAN remains invisible and uncontrolled
- No real-time L7 process-level visibility into the session
- Lack of real-time context and the ability to correlate between processes and flows
- Limited visibility due to encryption and proprietary applications
- Decryption and key management for session termination may become an attack vector
- Does not provide a consistent solution across different infrastructures (bare metal, virtual, cloud)
- Gateway solutions can't control the container layer within the data center
- NAT/network architecture design limitations. Requires topology changes

To Secure the Data Center and Clouds, Agents are the Way to Go

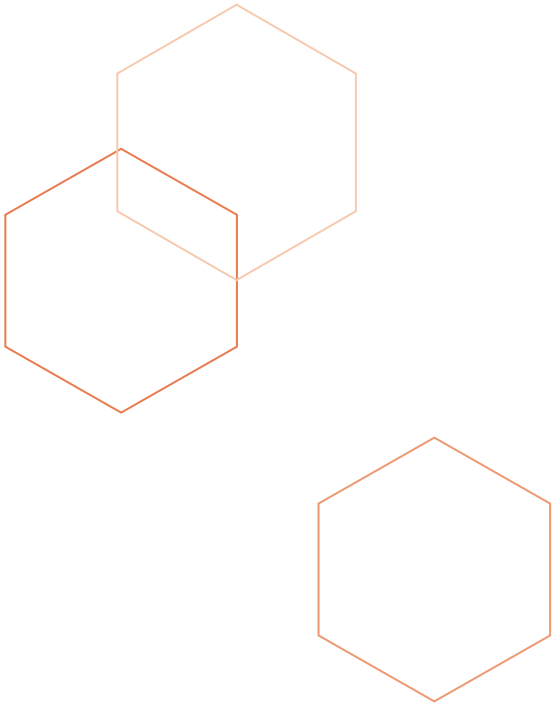
In contrast to the limitations of agentless solutions, by using agents you get a more robust, deep, and flexible solution. Advantages of using an agent approach include:

- The only way to achieve real-time process-level visibility and blocking all the way to the process level in Windows, Linux and Unix
- Independent of infrastructure/operational environments. Support for bare-metal, virtual, containers and any cloud (AWS, Azure, GCP, IBM, etc.)
- Provides visibility and control into the container layer independent of the container orchestration
- Facilitate change—workloads can be moved between operational environments with security policy following workload and automatically adjusting

- Agents provide visibility and enforcement for microservices/ containers, giving you a consistent cohesive solution across technologies
- Policy is infinitely scalable—no choke points
- Agents provide additional capabilities such as account, user, or hash-based enforcement, all within the same agent
- Agents can be easily pushed with any deployment management tools (Ansible, Chef, Puppet, SCCM, etc.), or built into cloud workload templates

GuardiCore offers agents that are lightweight, use a minimal amount of resources and have built-in protection against high memory or CPU consumption. All flow and policy processing is done onto GuardiCore infrastructure and doesn't consume any workload resources, thus presenting no risk to the asset, and the network continues to perform at line speed.

In summary, there are two main approaches to implementing segmentation. It's up to you to define the right criteria for your organization. Choosing an agent-based approach grants solutions extensibility and the ability to provide an advanced and deep approach to workload protection.



About GuardiCore

GuardiCore is an innovator in data center and cloud security focused on delivering more accurate and effective ways to stop advanced threats through real-time breach detection and response. Developed by the top cyber security experts in their field, GuardiCore is changing the way organizations are fighting cyber attacks in their data centers and clouds.

More information is available at **www.guardicore.com**