COMPARISON GUIDE

Akamai Guardicore Segmentation vs. Traditional Microsegmentation Solutions

Unmatched visibility

To understand what's going on in your environment, it is essential to have visibility into the communications among workloads. Truly effective visibility means being able to know, at any given moment, what each workload is doing with full context. In addition, grouping and filtering capabilities for both assets and rules are essential components to building policy quickly and effectively.

Akamai	Traditional microsegmentation
Easily visualize the entire environment The Akamai Guardicore Segmentation agent is a host-based firewall that runs on both modern and legacy operating systems, providing full visibility into network flows down to the individual process and service levels for both Windows and Linux operating systems, along with coverage for MacOS endpoints.	**Partial visibility for legacy** No optics into Microsoft Windows systems earlier than Windows Server 2003. This is because the traditional microsegmentation solutions' agent relies on a Windows firewall, which was only available with systems later than 2002. For Linux systems, their agents support L4 visibility only.
Rich, unmatched context When it comes to visibility, having proper context and details are critical. Our solution collects — in addition to flow data — critical context such as process info, file, patch level, and more.	**Minimal context** Collects information about flows and machines only, missing critical context details such as process and file. This makes the process of understanding application dependencies more laborious and time-consuming.
No limitation on type or number of labels We place no restrictions on the type or number of labels you can have, allowing for flexibility and supporting additional use cases. This will save you the effort of having to translate your existing labels from configuration management databases (CMDBs) and other data sources.	**Rigid labeling** With a fixed, predefined labeling hierarchy, traditional solutions force you into labeling your applications using a set amount determined only by them, regardless of your own environment requirements and business needs.
AI-driven labeling AI-powered application detection and labeling will help you identify applications when there is no reliable CMDB, and automatically assign them the correct label.	**No CMDB? You're stuck ...** With manual labeling and a preconfigured label hierarchy, if your organization doesn't have a CMDB to rely on, the labeling process becomes extremely complicated.

Akamai

Industry-leading coverage

One of the core elements of a good microsegmentation solution is the ability to protect critical assets no matter where they are deployed or accessed — legacy or modern, Windows or Linux, on-premises, or virtualized, containers, and much more.

Akamai

Complete support for Windows and Linux

Akamai Guardicore Segmentation agents are supported on all Windows and Linux operating systems — new and legacy — as our solution is not dependent on the underlying infrastructure.

Comprehensive containers support

Complete visibility for containerized environments while leveraging Container Network Interface (CNI) controls for enforcement.

Traditional microsegmentation

Limited Windows and Linux support

Policy enforcement depends on the Windows firewall for Windows environments, and iptables for Linux environments. This inevitably means limited or no protection for some legacy Windows OSs, and no L7 process-level rules for Linux environments.

Limited support for containers

Enforcement relies on iptables and back-and-forth policy calculations, which don't scale in a container environment, and cause both latency and downtime.

Build simple policies. Fast.

A good policy engine allows you to express your intent using the smallest number of rules possible, without forcing policy language restrictions. It will also help minimize the work of managing policy by providing automation and wizards.

Akamai

Allow and deny

We support allowlist and denylist rules — and any combination in between. This allows security and IR teams to respond to any security scenario quickly, eliminating the need to first allowlist every single legitimate flow.

Policy templates for a variety of use cases

Out-of-the-box templates and policy-building workflows for common scenarios — ransomware mitigation, application ringfencing, environment segmentation, and more. Templates help save time and reduce human error.

Rich policy criteria

Policy criteria can include source, destination, port, protocol, process, service (e.g., Task Scheduler commonly used by ransomware), user, and fully qualified domain name (FQDN).

Traditional microsegmentation

Allowlisting with limited deny rules support

The adherence to the secure yet time-consuming allowlist model doesn't allow traditional segmentation solutions to automatically respond to known threats that require fast blocking.

A limited set of templates

Segmentation templates are mainly supported in Microsoft environments. Templates for common segmentation use cases, such as ringfencing and ransomware mitigation and remediation, are not supported.

Limited criteria

No L7 process-level policies for Linux OSs nor any ability to build policies based on individual Microsoft Windows services.

Security first

Combating complex security threats like ransomware requires a comprehensive approach to security. While segmentation is prescribed by both National Institute of Standards and Technology (NIST) and the White House as a fundamental response, it takes an integrated approach to security and breach detection to keep your organization secure.

Akamai	Traditional microsegmentation
Ransomware prevention and mitigation Akamai Guardicore Segmentation provides out-of-the-box templates for all phases of the attack kill chain — from prevention through containment and mitigation.	**No ransomware templates** Traditional solutions are limited in their ability to block ransomware attacks with out-of-the-box templates.
Query endpoints for threat detection and compliance Our osquery-based tool, Insight, allows you to query servers and endpoints in real time for compliance and malware detection.	**No real-time detection** Traditional solutions can't detect real-time malicious activity in the data center.
Deception capabilities Based on a patented technology, the Akamai Guardicore Segmentation agent redirects blocked and failed sessions to a dynamic deception engine for further analysis and quarantine.	**No ability to quarantine** Traditional solutions lack deception capabilities, as well as the ability to detect or quarantine machines using known indicators of compromise (IOCs).
Managed threat hunting team Akamai provides managed threat hunting services that extend your security team's capabilities and allow your organization to stay ahead of the latest threats.	**No threat hunting services** Traditional vendors cannot provide threat hunting services built on top of their solution, which can be a critical differentiator in the face of ransomware and malware escalation.
Threat intelligence firewall To prevent known malicious behavior, Akamai Guardicore Segmentation blocks malicious IPs, files, and hashes using automatic firewall rules.	**No threat feeds** Lacking a similar capability, traditional solutions can't stop access to and from known bad IPs and URLs.

Operations or performance and latency

Low latency is critical to a successful segmentation project. This means you should be able to scale your policy with more rules, labels per assets, and other policy objects — all without introducing additional latency.

Akamai

Latency-optimized engine

Our segmentation engine is built for large-scale scenarios. This is achieved with an optimized filtering mechanism, resulting in a latency time that is relatively insensitive to the policy size.

Traditional microsegmentation

More rules lead to increased latency

Agents introduce more latency as the amount and size of rules grow. Linux iptables were simply not built to scale for enterprise-size east-west traffic. The result is significant latency that directly increases with policy size.

For more information about Akamai Guardicore Segmentation, or to request a personalized product demo, visit akamai.com/guardicore.