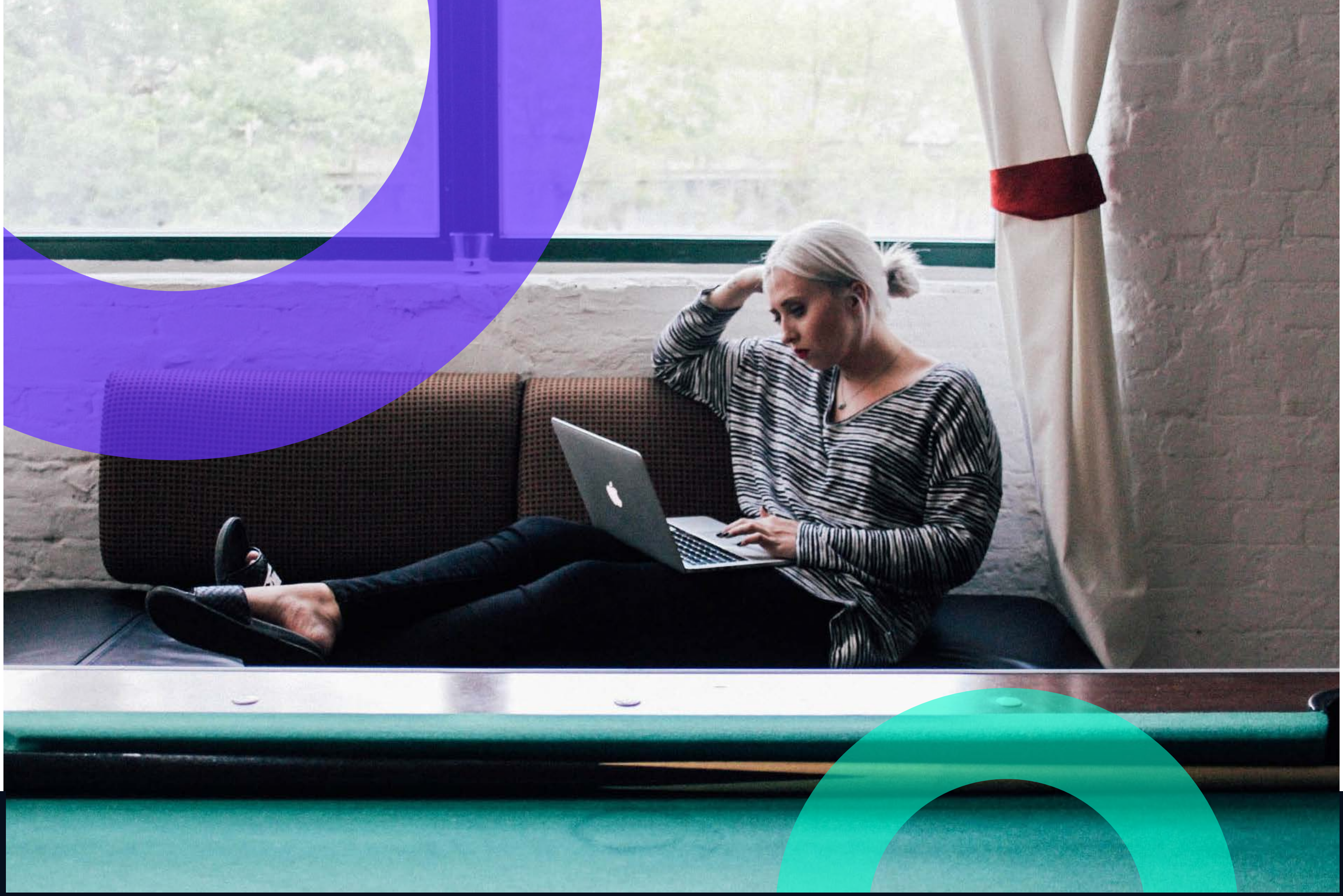

COMPARISON GUIDE:

Guardicore vs. Traditional Microsegmentation Solutions

Guardicore
Now part of Akamai

MARCH 2022
guardicore.com

Unmatched Visibility

To understand your environment it is essential to have visibility into communications between workloads. Truly effective visibility means being able, at any given moment, to know what each workload is doing with full context. In addition, grouping and filtering capabilities are essential to building a policy simply and fast.

GUARDICORE	TRADITIONAL MICROSEGMENTATION
Easily visualize the entire environment Guardicore's agent is a host-based firewall that runs on modern and legacy operating systems, providing full visibility into network flows to the process and service level for both Windows and Linux operating systems.	**Partial visibility for legacy** No optics into Microsoft Windows systems earlier than Windows 2002. This is because the Traditional microsegmentation solutions' agent relies on Windows firewall that was only available with systems later than 2002. . For Linux systems you'll need to settle for L4 visibility only.
Rich, unmatched context When it comes to visibility, context and details are critical to speed and accuracy. Guardicore Reveal collects - in addition to flow data - critical context such as process info, file, patch level and more.	**Minimal context** Collect 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 slow.
No limitation on type or number of labels Guardicore places no restrictions on the number or type of labels you can have, allowing for additional use cases. This will save you the trouble of translating labels from your CMDBs and other data sources.	**Rigid labeling** With a fixed, pre-defined labeling hierarchy, traditional solutions force you into labeling your applications using 4 labels only, regardless of your 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.	**NO CMDB? You're stuck...** With manual labeling and a pre-configured 4 label hierarchy, when an organization doesn't have CMDB to rely on, labeling becomes extremely complicated.

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 and modern, Windows and Linux, on-prem and virtualized, containers and more.

GUARDICORE	TRADITIONAL MICROSEGMENTATION
Complete support for Windows & Linux Guardicore Agents are supported on all ALL Windows and Linux operating systems - new and legacy - completely detached from the underlying infrastructure.	**Limited Windows and Linux support** A Prerequisite for a Windows firewall in Windows environments and one for iptables in Linux ones means no protection for some legacy Windows OSs nor process level rules for Linux environments.
Comprehensive containers support Complete visibility for containerized environments while integrating with native container controls for enforcement.	**Limited support for containers** Reliance on iptables and back and forth policy calculations which don't scale in a container environment, causing latency and down time.

Build Simple Policies. Fast.

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

GUARDICORE	TRADITIONAL MICROSEGMENTATION
Allow & Deny We support Allowlist and Denylist rules and any combination in-between. This allows security and IR teams to respond to any security scenario fast, eliminating the need to first whitelist legit flows.	**Whitelisting with limited Deny rules support** The adherence to the secure yet time-consuming whitelist model doesn’t allow traditional segmentation solutions to automatically respond to known threats that require fast blocking.
Policy templates for a variety of use cases Out-of-the-box templates and policy building workflows for every scenario - ransomware mitigation, ring-fencing, environment segmentation and more. This helps Save time and eliminate human error.	**A limited set of templates** Segmentation templates are mainly supported in Microsoft environments. Templates for common segmentation use cases such as ring fencing and ransomware mitigation and cleanup are not supported.
Rich policy criteria Policy criteria can include source, destination, port, protocol, process, service (e.g. Task Scheduler commonly used by ransomware), user and FQDN.	**Limited criteria** No process-level policies for Linux OSs nor ability to build policies based on Microsoft Windows services**.**

Security First

Combatting complex security threats like ransomware requires a comprehensive approach to security. While segmentation is prescribed by the White House as a fundamental response, it takes an integrated approach to security and breach detection to keep your organization secure.

GUARDICORE	TRADITIONAL MICROSEGMENTATION
Ransomware prevention & mitigation Guardicore provides out-of-the-box templates for all phases of the attack killchain - 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 & 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 malicious activity in the data center.
Deception capabilities Based on a patented technology, The Guardicore 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 as the ability to detect or quarantine machines with Indicators of Compromise (IoCs).
In-house threat hunting team Guardicore provides threat hunting services that extend your security team's capabilities and allow your organization to stay ahead of threats.	**No threat hunting services** Traditional solutions cannot provide threat hunting services, critical in the face of ransomware and malware escalation.
Threat Intelligence Firewall To prevent known malicious behavior, Guardicore Centra 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 out your policy with more rules, labels per assets and other policy objects, all without introducing additional latency.

GUARDICORE

Latency optimized engine

Segmentation engine is built for large-scale scenarios. This is achieved with an optimized filtering mechanism resulting in latency time 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 for enterprise-size east-west traffic. The result is latency increased with policy size.

Guardicore

Now part of Akamai

About Guardicore

Guardicore delivers easy-to-use Zero Trust network segmentation to security practitioners across the globe. Our mission is to minimize the effects of high-impact breaches, like ransomware, while protecting the critical assets at the heart of your network. We shut down adversarial lateral movement, fast. From bare metal to virtual machines and containers, Guardicore has you covered across your endpoints, data centers and the cloud. Our software-based platform helps you become more secure to enable your organization's digital transformation.