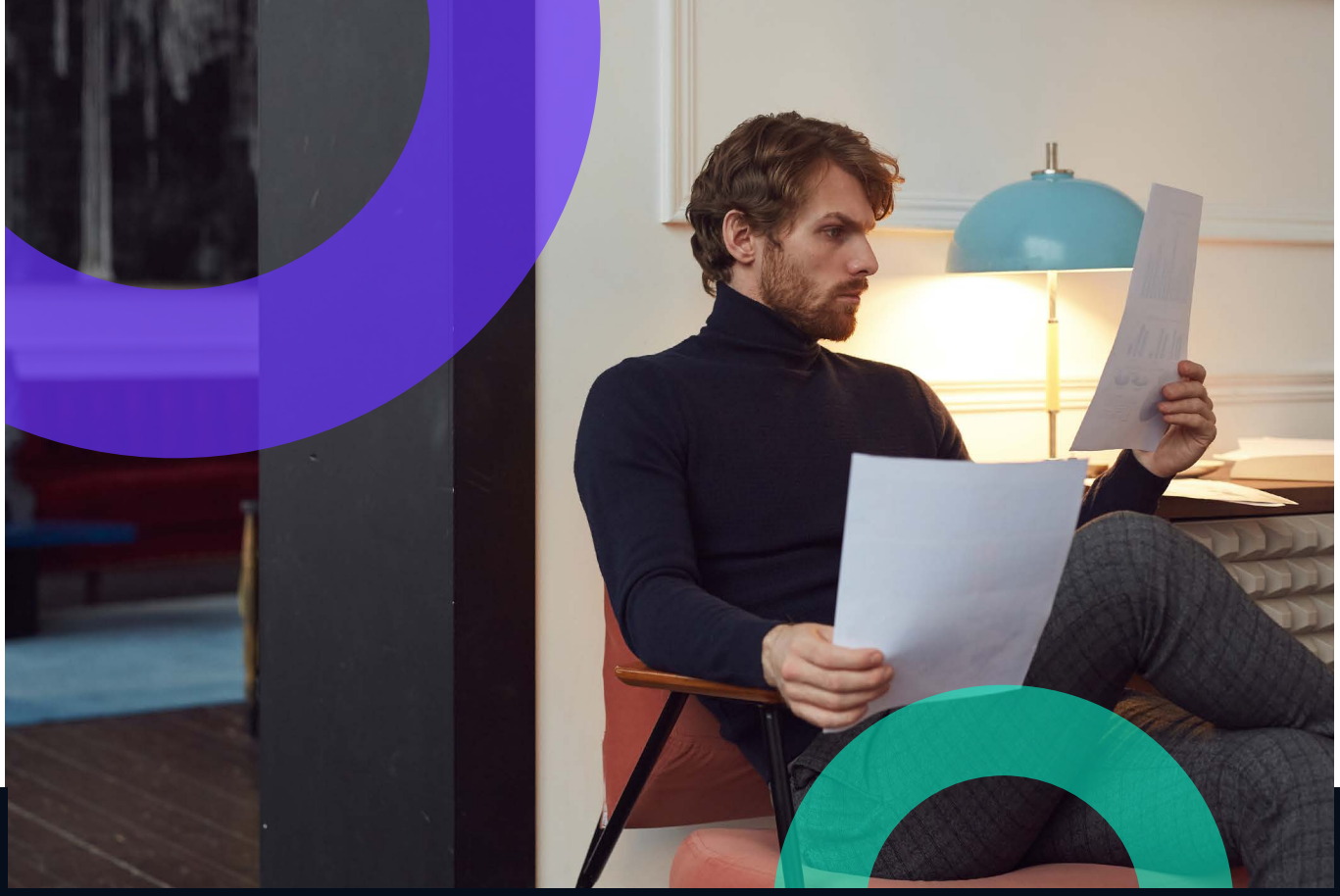

FUD or Fact: Cutting Through the Noise

*To shed some light on a **dimly lit** and **highly inaccurate comparison** that was published about Guardicore, we present you with the **TRUTH**.*

Guardicore

Now part of Akamai

Policy Workflow

THE NOISE
Policy must be designed manually to start – rules are written manually like a traditional firewall. Interactive rule writing from map and flows is complex and difficult to track.

THE TRUTH
Creating rules is quick and intuitive with simple step by step procedures. Manual design is only one way of creating policies -- policies can also be created semi-manually, or fully automated.

THE NOISE
Rules with IP lists program workloads as well, making policy writing difficult.

THE TRUTH
Policy design is very simple and straightforward. The complexity of numerous IPs is simplified by using labels and label intersections, providing a clear view of traffic.

Labeling

THE NOISE
“Infinite” number of labels. However, there is no ability to stack labels (multiple roles).

THE TRUTH
Centra provides label intersections and multiple labels for the same host - also with the same label key. AI Labeling provides labels customized to the customer environment based on traffic analysis.

Dynamic Labeling

THE NOISE
Labels are based on hostname or IP address. Labels will constantly change, so if IPs are changing or the device hostname changes, it will automatically lose or gain labels and, as a result, may lose critical security policy.

THE TRUTH
Besides IP and hostnames, labels are based on container and K8s criteria, as well as host attributes pulled through Guardicore Insight. These attributes are dynamically updated to prevent the labeling scheme from going stale. This enhances critical security policy. If dynamic criteria is not a match for a specific use case, explicit, static labeling is fully supported.

Performance Impact

THE NOISE
Heavyweight agent – if guardrails are not put in place, the agent could overrun the system.

THE TRUTH
The agent is highly optimized to work with Linux, Unix and Windows OS and does not consume substantial resources by design.

Agent

THE NOISE
Heavyweight agent manipulates the kernel and needs safeguards to stop CPU/MEM spikes.

THE TRUTH
Agents are NOT “heavyweight”. Agents are highly optimized to work with Linux, Unix, and Windows OS and do not consume substantial resources. Safeguards manage risk in production environments but are not needed in normal operations.

Automated Rule Writing

THE NOISE
Semi-automated rule writing is operationally hard to use with the custom maps.

THE TRUTH
Semi-automated rule writing is easy to use and facilitated by Guardicore’s Suggestion mode that provides a way to quickly refine policies.

THE NOISE
Ringfencing or micro-segmentation only –no automated tier-to-tier segmentation.

THE TRUTH
Guardicore provides automated tier to tier segmentation, as well as a range of other use case templates and automations.

THE NOISE
No ability to exclude rules during automated policy creation.

THE TRUTH
All policy creation modes allow to exclude, include, and move rules around.

100% Confident Ruleset Creation

THE NOISE
Requires adjusting ruleset to attempt validation.

THE TRUTH
The Reveal map enables precise simulation of policy at any stage.

Rule Limits

THE NOISE
1k rules per endpoint, 12k objects per rule.

THE TRUTH
The real limits: 3.5k rules per endpoint, 40k objects per rule.

Non-disruptive Deployment Modes

THE NOISE
Agents are always enforcing. To validate rules, they need to be moved around the ruleset. This adds increased complexity and risk.

THE TRUTH
Agents are NOT always enforcing. Guardicore also provides Visibility only mode, and Monitor mode that enable efficient rule validation.

THE NOISE
Map data may be delayed or stale at time of generation.

THE TRUTH
The Reveal maps provide near real time, up-to-date flow information.

THE NOISE
Unmanaged workloads require third-party API integration, so if the integration goes down, the workload disappears, which can impact rules and security.

THE TRUTH
Unmanaged assets are updated in an interval fashion and can be continuously expressed in policies using dynamic labels, regardless of whether a managed asset was created.

Architecture

THE NOISE
Centralized control and distributed enforcement. However, all agents must communicate through a proxy to report flows and receive policy.

THE TRUTH
This is an advantage, not a shortcoming! The Centra 3 tier architecture allows scaling the system through optimization and deduplication of flows and logs. In addition, the Aggregator allows long-term caching in case of disconnection from central management.

Policy Revisioning

THE NOISE
No revision details. Versioning is present but contains no details on changes made.

THE TRUTH
Revision information is provided in great detail using special API endpoints and a detailed Audit log.

Enforcement

THE NOISE
Proprietary stateless firewall uses kernel hooks to collect data and enforce rules.

THE TRUTH
Guardicore is a Stateful FW that extends existing Linux and Windows OS capabilities to create a custom firewall with massive advantages: rules go beyond L4 to cover processes, users, FQDNs, etc. with improved performance of large rulesets.

THE NOISE
Agent is inline with traffic, making it a point of failure for security – if it goes down, it will take all the security with it.

THE TRUTH
The Centra agent is not part of the datapath. It only inspects the sessions being created by various applications. If the agent goes down, there is no risk of down time to applications or servers.

Role-based Access Control (RBAC)

THE NOISE
RBAC is present but with limited application owner views as a result of single monolithic ruleset.

THE TRUTH
Centra provides multiple roles that provide different levels of accessibility and control. Owners of a specific application will only be privy to their assets and ruleset.

Ruleset Design

THE NOISE
Monolithic ruleset which is evaluated sequentially in sections.

THE TRUTH
The Guardicore policy is fully modular. Rules are only derived to the respective systems on which the rule\policy should be applied.

THE NOISE
Label-based rules are possible, but operationally it can become difficult to keep track of where rules apply as the rules get longer.

THE TRUTH
Label-based rules are not only possible, they are one of the outstanding features of Guardicore. Flexible labels express the exact applications covered by the policy.

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.