



Accelerating AODG Compliance with Visibility and Segmentation

WHITE PAPER

Complying with AODG to Protect Against Cybersecurity Breaches

What is AODG?

The Adversarial Obstruction Defense Guidelines (AODG) are a set of security implementation guidelines based on the methodology introduced by the National Security Agency¹ with the ultimate goal of protecting its members from cybersecurity breaches.

AODG reduces organizational risk from cyber threats through compliance with its requirements.

Key AODG Compliance Challenges

1 Diverse Infrastructure

One key theme of the AODG requirements is the need to create and enforce segregation and access controls. This can be especially challenging as both require infrastructure-wide change, including the reconfiguration of networks and the need to implement changes across multiple infrastructure types and the cloud.

Combined with the implied downtime, these application changes require significant teamwork to plan and execute, introducing a high toll to teams already maxing out their existing resources.

2 Diverse Requirements

On par with a layered approach to security, the AODG's requirements cover a broad range of disciplines, ranging from network to endpoint security capabilities. Addressing such a diverse set of requirements usually requires multiple tools. However, implementing, configuring and maintaining these with limited team resources and headcount can be a significant challenge.

1. <https://www.cdse.edu/documents/cdse/nsa-methodology-for-adversary-obstruction.pdf>

Guidance for Effective Compliance

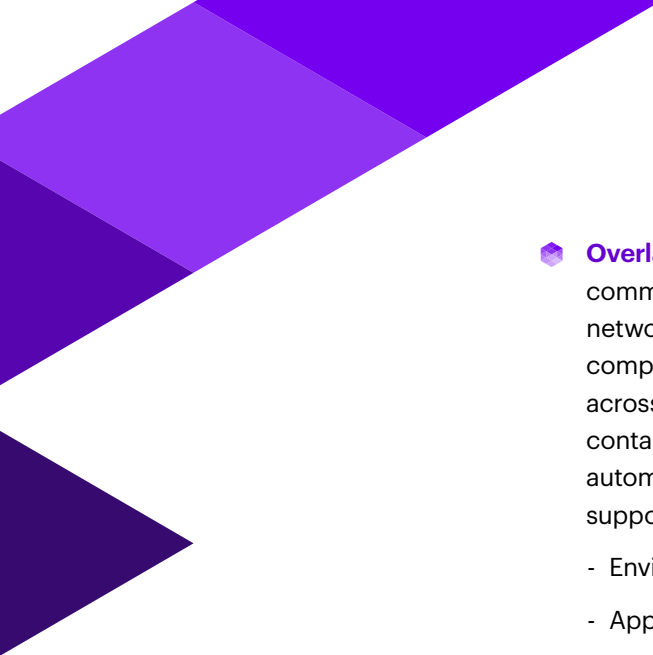
- 1** Look for solutions that enforce segmentation without requiring changes to your current infrastructure or network. Solutions exist today that allow you to implement segregation without the need to reconfigure networks, create VLANs or make application changes. The only solution that can account for infrastructure differences will use an Overlay model and support anything from bare metal to containers in the cloud. This approach will save time and reduce overall costs.
- 2** Identify solutions that can fulfill multiple requirements with a single tool. Fewer tools means less time and resources spent on installation, training, maintenance and configuration. Often, this is the only way a small team can effectively manage a diverse set of requirements.
- 3** Consider solutions that provide detailed visibility into your entire environment, including data centers, legacy applications and east-west traffic (a common blind spot for many organizations). Effectively managing risk, applying controls, investigating incidents and passing audits requires consistent, 'always-on' visibility with rich context. You need to be able to answer any questions about what is happening in your data center to evaluate the effectiveness of specific controls and take real-time action on your findings.
- 4** Ensure future-readiness - compliance is not a one-time project, but something to enforce at all times. Select solutions that are infrastructure agnostic and DevOps ready so everything can be automated and integrated into your operational cycle, even when your environment evolves (e.g., adoption of cloud/containers).

Guardicore Accelerates AODG Compliance

Guardicore was designed to provide comprehensive controls to business-critical applications. We understand that modern infrastructure complexity and detailed regulations require very high operational efficiency from security teams to efficiently deploy and operate security controls.

Guardicore Centra helps security teams comply with the most demanding standards and regulations across any infrastructure and with limited resources through:

- Detailed Visibility** -Centra collects detailed information and generates a dynamic visual map of your entire IT infrastructure down to the individual process level. This allows security teams to understand internal traffic patterns, identify applications and their dependencies, review their environments with various view groupings and drill down to a specific inquiry with powerful filtering. Access to this rich real-time and historical data speeds up numerous operational processes and reduces the risk of introducing new controls.



📦 **Overlay Software-Defined Segmentation** - Guardicore Centra simplifies communication policy development and enforcement without requiring network changes, application changes or downtime. Centralized management is completely decoupled from the infrastructure and means a one-policy approach across everything, from bare-metals to virtualized environments and clouds to containers with a single platform. This allows the policy to follow the workload automatically however it moves or changes through your environment. Centra supports various use-cases of segmentation, such as:

- Environment segregation - such as DEV/PROD/UAT
- Application ring-fencing
- User/administrative access controls
- Secure 3rd party access control
- East-west traffic restriction
- North-south traffic restriction

With this approach, there is no need to involve multiple teams to create a separation between two environments or applications. This results in an acceleration of the compliance process and reduces costs.

📦 **Breach Detection, Investigation and Response** - Centra features an integrated set of threat detection and response capabilities such as threat intelligence, malware detection, lateral movement detection and file integrity monitoring, as well as deception tools to allow effective detection of malicious activity inside the data-center. Combined with detailed visibility and policy enforcement capabilities - Centra gives IT security teams the ability to rapidly investigate a potential breach or unusual activity and apply restriction controls in real time to minimize the impact.

Guardicore Support for AODG Requirements

Guardicore Centra's capabilities map closely to the AODG framework, accelerating compliance and helping teams meet even the most challenging requirements of this regulation. The table below illustrates the relevance of Centra to the 11 requirements of AODG.

Requirement Group	Requirement	Guardicore Support
Protect credentials		
	Implement least privilege	Irrelevant
	Restrict local accounts	Irrelevant
	Limit lateral movement	Fulfills
	Admin access segregation	Fulfills
	Admin access	Fulfills
	Admin accounts do not have emails or internet	Fulfills
	Utilize strong authentication	Irrelevant
	Log and monitor privileged accounts	Supports
	Log and monitor admin tools usage	Fulfills
Segregate networks and functions		
	Know your network	Fulfills
	DMZ isolation	Fulfills
	Network function segregation	Fulfills
	Limit workstation to workstation	Fulfills
	Perimeter filtering	Fulfills
	Web domain name reputation	Fulfills
	Restrict admin remote access	Fulfills
Implement HIPS rules		Supports
Centralize logging		Irrelevant
Take advantage of SW improvements		Supports
Implement application whitelisting		Fulfills
Install and correctly use EMET		Irrelevant
Public services utilization		Fulfills
Use a standard baseline		Irrelevant
Data at rest and in transit encryption		Irrelevant
Use file reputation services		Fulfills



About Guardicore

Guardicore is an innovator in data center and cloud security that protects your organization's core assets using flexible, quickly deployed, and easy to understand micro-segmentation controls. Our solutions provide a simpler, faster way to guarantee persistent and consistent security - for any application, in any IT environment.

www.guardicore.com