WHITE PAPER

Accelerate Compliance with the NSA Methodology for Adversary Obstruction

Complying with NSA methodology to protect against cybersecurity breaches

What is it?

The Methodology for Adversary Obstruction is a set of security implementation guidelines introduced by the National Security Agency[1] with the ultimate goal of protecting its members from cybersecurity breaches.

This methodology is intended to reduce organizational risk from cyberthreats through compliance with its guidelines.

Key compliance challenges

Diverse infrastructure

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

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

Diverse guidelines

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

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 legacy systems and bare-metal servers to containers on-premises and in the cloud. This approach will save you time and reduce overall costs.

2. Identify solutions that can satisfy multiple guidelines 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 guidelines.

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).

Akamai Guardicore Segmentation accelerates compliance with NSA Methodology for Adversary Obstruction

Akamai Guardicore Segmentation 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.

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

Detailed visibility Our solution 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 Akamai Guardicore Segmentation 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 your entire infrastructure with a single platform. This allows your security policy to follow the workload automatically, however it moves or changes through your environment. We support various use cases for segmentation, such as:

- Environment segregation, such as DEV/PROD/UAT
- Application ringfencing
- User/administrative access controls
- Secure third-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 associated costs.

Breach detection, investigation, and response Akamai Guardicore Segmentation features an integrated set of threat detection and response capabilities such as threat intelligence, malware detection, lateral movement detection, and even an additional managed threat hunting service, as well as tools to allow effective detection of malicious activity in your network. Combined with detailed visibility and policy enforcement capabilities, Akamai Guardicore Segmentation 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.

Our support for NSA guidelines

Akamai Guardicore Segmentation's capabilities map closely to the Adversary Obstruction framework, accelerating compliance and helping teams meet even the most challenging guidelines of this methodology. This table illustrates the relevance of our solution to the 11 guideline groups.

Guideline group	Guideline	Akamai Guardicore Segmentation Support
Protect credentials		
	Implement least privilege	Irrelevant
	Restrict local accounts	Irrelevant
	Limit lateral movement	Fulfills
	Admin access segregation	Fulfills
	Admin access protection	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 communications	Fulfills
	Perimeter filtering	Fulfills
	Use web domain name reputation	Fulfills
	Restrict or prevent admin remote access	Fulfills
Implement HIPS rules		Supports
Centralize logging		Irrelevant
Take advantage of software 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 anti-virus file reputation services		Supports

To speak with an expert, visit akamai.com/guardicore.

1 NSA Methodology for Adversary Obstruction