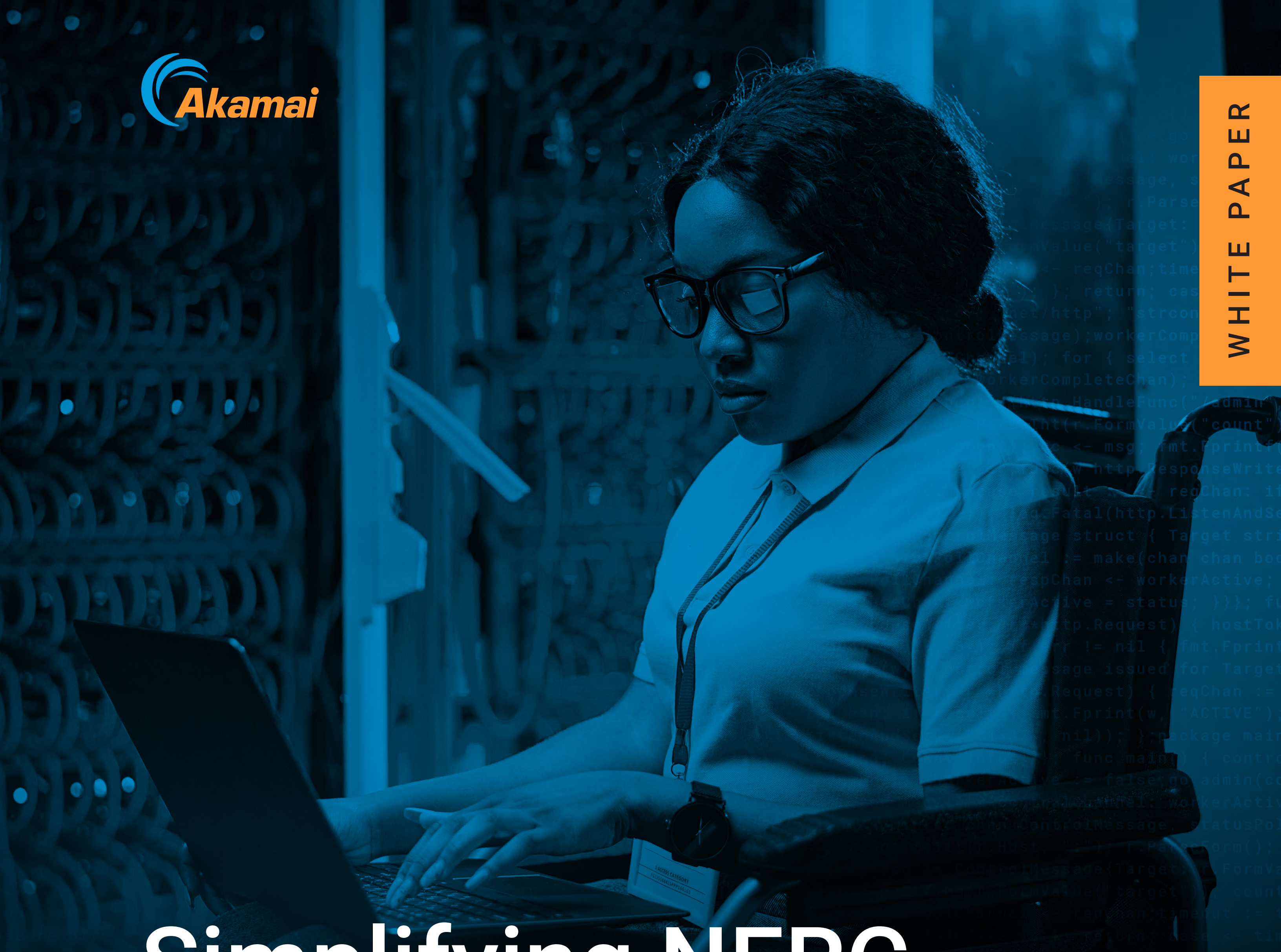


WHITE PAPER

Simplifying NERC CIP Compliance with Akamai Guardicore Segmentation

Introduction

The North American Electric Reliability Corporation (NERC) is charged with ensuring the reliability of North American bulk power systems. Cybersecurity is a key risk area that power system operators must address, and NERC's Critical Infrastructure Protection (CIP) standards are a collection of specific security requirements that North American operators must comply with.

Akamai Guardicore Segmentation can help organizations that are already compliant with NERC CIP by simplifying and enhancing their compliance posture as follows:

- Reducing the cost and complexity of audit preparation through visualization tools that present the power system and its assets' communications patterns in a clearly visible and searchable manner
- Making it easier to remain compliant by combining visibility with a set of software-based firewall controls that can be changed in minutes without physical network changes or complex firewall rule modifications
- Providing a simple way to perform granular segmentation within an Electronic Security Perimeter (ESP) to significantly reduce risk to critical assets
- Enabling faster infrastructure and data center changes through an overlay segmentation approach
- Reducing dependence on network appliances that introduce complexity and operational inefficiencies
- Replacing legacy breach detection tools with an integrated solution

Akamai Guardicore Segmentation can also help power system operators that are developing a NERC CIP compliance strategy for the first time by:

- Implementing ESPs (requirement CIP-005-6) orders of magnitude faster by replacing complex firewall and VLAN approaches with a software-based approach that avoids network changes, application changes, and downtime
- Providing full visibility into the network to aid in security decision-making, audit evidence presentation, ESP border detection, and asset classification
- Simplifying intra-ESP segmentation to significantly reduce the risk to critical assets
- Enabling faster infrastructure and data center changes and integrations through an overlay segmentation approach
- Simplifying compliance with breach detection requirements such as CIP-008-5

Microsegmentation and breach detection with Akamai Guardicore Segmentation

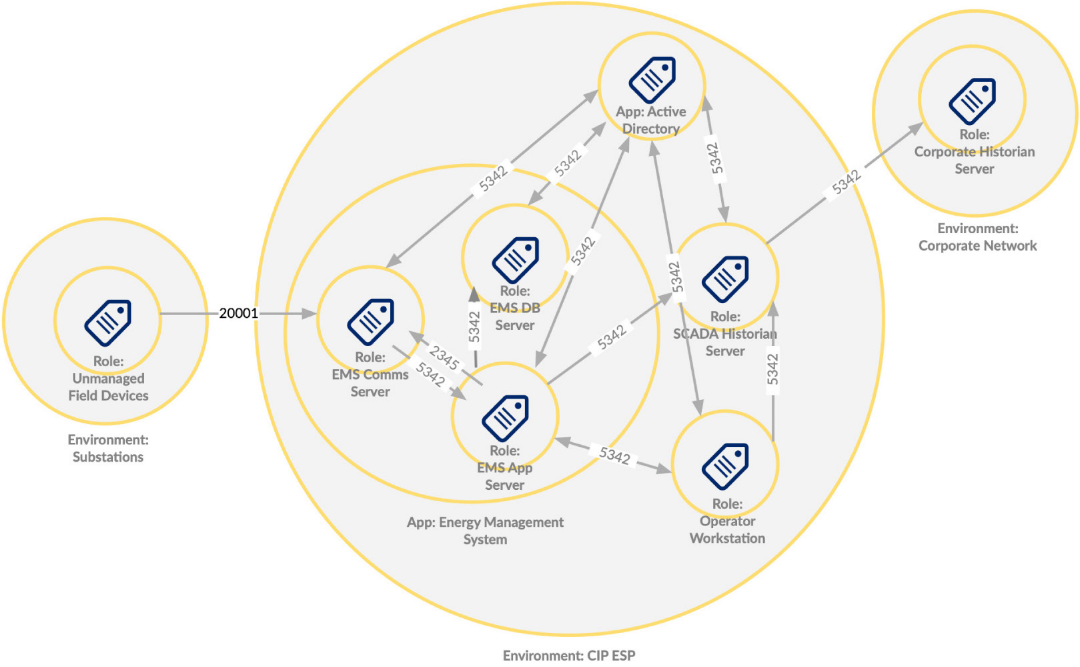
Akamai Guardicore Segmentation makes visualizing and securing the network and data center infrastructure for power systems much simpler, by replacing or augmenting infrastructure-based security controls with a software-based segmentation overlay that provides:

- Real-time and historical visibility
- Easy-to-implement policy controls with process- and user-level granularity
- Integrated breach detection and response capabilities

How it works

Our solution utilizes a distributed collection of software agents, installed on servers and virtual machines, to collect detailed information about activity in the environment and enforce security policies. Optionally, our agents can be supplemented by dedicated network data collectors to enrich the application and network data available for analysis. While our solution is compatible with a wide range of modern and legacy operating systems, we also offer agentless configuration options to address any scenarios where installation of agents on legacy systems or certain devices is impractical or impossible.

In addition to collecting detailed activity information, Akamai Guardicore Segmentation has a highly flexible asset labeling model that can interface with existing data sources such as configuration management databases and orchestration tools. This allows our solution to generate maps of the environment that provide the context required to create effective security policies.


App: Active Directory
Role: Corporate Historian Server
Environment: Corporate Network
Role: EMS DB Server
Role: SCADA Historian Server
Role: Unmanaged Field Devices
Environment: Substations
20001
Role: EMS Comms Server
Role: EMS App Server
Role: Operator Workstation
App: Energy Management System
Environment: CIP ESP
5342
2345

Our visualization interface is very flexible and gives power system operators the ability to assess their operations and security posture on both a real-time and historical basis. This helps operators demonstrate to NERC CIP auditors that they have effective controls in place and makes it easy to assess the impact of security incidents.

Security policies are created from the same visual interface, enabling granular control without complexity or changes to the underlying network infrastructure. Security policies can extend beyond traditional network layer controls to enforce policies at the individual process or service level. Policies can also be based on user identity, allowing access to protected environments using terminal servers or other types of jump boxes to be tightly controlled based on business need.

Akamai Guardicore Segmentation also includes built-in breach detection and response capabilities. Security teams can be alerted when known malware is detected or when activity originates from sources with a known bad reputation. In addition, with our managed threat hunting service, we can collect and correlate data from your environment and Akamai's global platform to surface suspicious activity that other tools miss, and provide you with dedicated security experts to investigate that activity and assist you with incident response.

Simplifying NERC CIP compliance with Akamai Guardicore Segmentation

Akamai's solution for software-based segmentation and breach detection builds on power system operators' existing firewall implementations by increasing visibility, enabling more granular control, and decoupling security policies from the underlying network infrastructure.

The following examples illustrate some of the ways that our solution can be applied to simplify and enhance NERC CIP compliance.

CIP-003-7 — Cyber Security — Security Management Controls	
Requirement 2	Our microsegmentation policy capabilities can be used to implement and enforce the Electronic Access Controls described in Attachment 1, Section 3, of the CIP-003-7 requirements documentation. This includes enforcement of process-level controls between systems, as well as the ability to create identity-based policies to govern remote access.
CIP-005-5 — Cyber Security — Electronic Security Perimeter(s)	
Requirement 1.1	Akamai Guardicore Segmentation's policy capabilities can be used to establish software-defined ESPs or apply more granular policy control within an ESP that is implemented using a traditional network firewall. In either case, the solution's visualization capabilities can be used to provide evidence of compliance.
Requirement 1.2	Policies can be used to establish a software-defined Electronic Access Point (EAP) or apply more granular policy control within an EAP that is implemented using a traditional network firewall. In either case, the solution's visualization capabilities can be used to provide evidence of compliance.
Requirement 1.3	Akamai Guardicore Segmentation can be used to visualize and apply policies to inbound and outbound connections to and from high-impact and medium-impact systems. Customizable labeling and mapping capabilities can be used to demonstrate the rationale for specific policies and support compliance activities.
Requirement 1.4	When users connect remotely, Akamai Guardicore Segmentation can apply user-level policies to tightly manage access to specific systems based on need. The solution's visualization capabilities can be used to demonstrate historical enforcement of remote access policies.
Requirement 1.5	Akamai Guardicore Segmentation employs multiple methods of detecting and blocking suspected malicious communication. These include: • Allowlisting known good processes and detecting communication attempts by processes that are not explicitly allowed • Detecting known malware or activity from suspicious sources attempting to communicate with systems in the environment
Requirement 2.1	Akamai Guardicore Segmentation's user-based policies can be used to apply more granular controls to remote access through Intermediate Systems.

CIP-007-6 — Cyber Security — Systems Security Management	
Requirement 1.1	Akamai Guardicore Segmentation's visualization capabilities can be used to identify the specific network ports that are needed for authorized communication flows. Policies can then be created to restrict communications based on need. These policies can be applied both at the network/port level and at the individual process level. This ensures that even when a specific port is open, only authorized processes will be able to communicate over it.
Requirement 3.1	Akamai Guardicore Segmentation's breach detection capabilities can detect the presence of known malware and alert or proactively block its communication based on policy. The solution can also detect communication from known sources of malicious activity and take policy actions in these scenarios.
Requirement 3.2	In addition to blocking malware, Akamai Guardicore Segmentation provides detailed reporting of detected malware, responses taken, and resulting outcomes. This information can be used to enhance security policies to mitigate future threats and provide documentation to support compliance activities.
Requirement 4.1	Akamai Guardicore Segmentation generates events for a wide range of activities in the environment, including failed or blocked communication attempts, detected malicious code, and many other types of security events. This information is presented in a user-friendly manner with supporting details and context. Events can also be transmitted to external security information and event management systems if desired.
Requirement 4.2	Akamai Guardicore Segmentation offers a highly flexible set of alerting options that can be defined to address the specific needs of the Responsible Entity through the creation of custom alerting policies.
Requirement 4.3	Akamai Guardicore Segmentation's event reporting can be viewed in real time and on a historical basis, including the ability to meet or exceed the 90-day minimum retention requirement.
Requirement 4.4	The Responsible Entity can view events through an easy-to-use web console, simplifying the required incident review process.
CIP-008-5 — Cyber Security — Incident Reporting and Response Planning	
Requirement 1	Akamai Guardicore Segmentation's breach detection and response capabilities can play a central role in an effective Cyber Security Incident response plan. This includes information-rich alerting at the time of a breach, and historical forensic information that can be used to recover from incidents and comply with Reportable Cyber Security Incident reporting requirements.
CIP-009-6 — Cyber Security — Recovery Plans for BES Cyber Systems	
Requirement 1.5	The historical activity data captured by Akamai Guardicore Segmentation can be used to determine the cause of Cyber Security Incidents that trigger a recovery plan. This information can be used to determine which Cyber Assets were affected and how to best enhance security policies based on lessons learned.

Summary

Our solution's software-based segmentation and breach detection capabilities enable organizations to comply with NERC CIP by:

- Visualizing their environment, so they can understand in detail how systems are communicating
- Creating granular policies down to the individual process level and user level to enhance control instead of added network hardware or complex configurations
- Detecting and blocking malicious activity
- Fully capturing events and generating detailed alerts to support incident response and compliance efforts

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