PARTNER BRIEF

From Visibility to Control: Securing Cyber-Physical Systems with Armis and Akamai

Overview

From hospitals and factories to transportation hubs and utilities, the connected digital infrastructure depend on a growing network of cyber-physical systems (CPS) such as medical devices, industrial control systems (ICS), IoT sensors, and building automation systems. These assets are essential, yet often invisible to traditional security tools.

The integration of Armis Centrix™ and Akamai Guardicore Segmentation delivers unified visibility, intelligent continuous threat exposure management, and dynamic segmentation across every connected asset whether physical, virtual or a combination of both. Together, Armis and Akamai empower organizations to see, understand, and secure the full scope of their attack surface, reducing risk and operational disruption while simplifying compliance.

The State of the Market

The convergence of IT and OT has expanded the threat landscape beyond traditional endpoints. As attackers exploit these blind spots or grey areas, critical systems are increasingly exposed to ransomware, cyber, and supply chain attacks.

Key challenges include:

- Limited visibility into unmanaged, legacy, or agentless devices that can't be patched or monitored.
- Flat network architectures that enable rapid lateral movement once attackers breach the perimeter.
- Fragmented tools that create data silos and force security teams into "swivel chair" operations.
- Compliance pressures from regulators and insurers are demanding stronger segmentation and access controls.

According to Gartner, by 2027, three out of four CPS-intensive organizations will adopt unified CPS protection platforms that extend beyond visibility to enable active prevention and containment. The time for a converged CTEM platform is now.

The Joint Solution: Actionable CPS Protection

The Armis–Akamai joint solution provides an integrated, risk-based approach to protecting CPS environments. It unifies asset intelligence from Armis Centrix™ with the powerful policy enforcement capabilities of Akamai Guardicore Segmentation.

Together, the platforms enable organizations to:

- **Discover every asset —** Armis provides complete agentless visibility across IT, OT, IoT, and IoMT assets.
- **Understand contextual risk —** Armis applies behavioral analytics, vulnerability context, and real-time threat intelligence so full situational awareness is achieved on every asset and across every path.
- **Segment intelligently —** Akamai enforces fine-grained segmentation and microsegmentation policies based on Armis risk insights and intelligence.
- **Contain threats automatically —** Akamai isolates compromised or high-risk assets to stop lateral movement if an attack has gained a beachhead in the environment.

The result is a truly adaptive protection layer that dynamically discovers, assesses, and defends against threats across complex, converged environments.

How it Works

01

Agentless Discovery & Classification
Armis Centrix™ leverages a multi-detection engine and identifies every device communicating on the network, including unmanaged assets that cannot host agents. Each device is classified with rich metadata such as manufacturer, model, OS, and behavior profile.

02

Contextual Risk Enrichment
Armis continuously analyzes device and attack pathway behaviors and assigns a dynamic risk score based on vulnerabilities, exploits, anomalies, and asset criticality to the business. These insights are shared in real time with Akamai Guardicore Segmentation.

03

Dynamic Segmentation & Policy Enforcement
Akamai automatically maps communications between assets using its Reveal capability. It then applies segmentation rules and policies, defined by Armis context, across IT and OT networks to isolate risky assets and enforce least-privilege, zero trust access.

04

Threat Containment & Continuous Protection
If an early warning, threat, or anomaly is detected, Akamai immediately restricts communication for affected devices, preventing lateral movement and minimizing blast radius while maintaining operational continuity.

Use Cases

This joint solution delivers measurable value across multiple industries. The following use cases illustrate how organizations are applying the joint solution to gain a complete inventory and situational analysis of the entire digital estate, contain threats, and maintain operational continuity.

1. Ransomware Containment in Healthcare

A hospital faces an outbreak targeting vulnerable medical imaging devices.

- Armis identifies exposed, unpatchable MRI machines and infusion pumps.
- Akamai enforces segmentation policies to block unauthorized east-west traffic.
- The ransomware is contained before impacting patient care systems.

2. Manufacturing Resilience

A factory's PLCs and HMIs run legacy firmware with known exploits.

- Armis flags the devices and correlates exposure to attack pathway activity.
- Akamai segments production systems from IT networks, preventing business systems from compromising operational lines.

3. Critical Infrastructure Protection

In an energy utility, remote substations and SCADA devices face constant probing from the internet.

- Armis detects unusual traffic patterns and assigns risk scores.
- Akamai dynamically isolates critical control systems, ensuring uninterrupted power delivery.

4. Zero Trust Network Expansion

Organizations seeking Zero Trust maturity leverage this integration to extend Zero Trust principles across all devices thereby enabling least privilege access control across the entire digital ecosystem.

5. Compliance and Audit Readiness

For regulated sectors such as healthcare, finance, and government, the joint solution simplifies segmentation compliance, helping organizations demonstrate compensating controls and adherence to HIPAA, PCI-DSS, and ISO 27001 through auditable policy enforcement.

Key Differentiators and Benefits

Comprehensive Visibility

See every asset whether managed or unmanaged across IT, OT, IoT, and IoMT environments. No blind spots, no agents required.

Context-Aware Segmentation

Leverage Armis's vast asset intelligence engine and dynamic risk scoring to build targeted segmentation policies within Akamai, aligning controls with real-world, asset specific risk.

Rapid Risk Reduction

Reduce lateral movement and contain ransomware outbreaks before they spread, thus protecting uptime, safety, and brand reputation.

Simplified Compliance

Automatically enforce compensation controls and segmentation policies that satisfy regulatory and insurance requirements.

Operational Continuity

Secure without disruption. Maintain system resilience and uptime even as segmentation and isolation policies are enforced dynamically.

Unified IT-OT Security

Consolidate visibility and control under a single pane of glass, bridging the gap between IT and OT security operations.

Summary

The integration of **Armis Centrix™** and **Akamai Guardicore** marks a major step forward in securing the modern enterprise. Together, they transform siloed security operations into a comprehensive intelligent control plane that protects every connected asset and pathway no matter how complex or distributed the environment.