ARMIS®

CATO NETWORKS

PARTNER BRIEF

Armis + Cato Networks: Unified Visibility, Security and Control Across The Digital Landscape

Overview

The Armis and Cato Networks joint solution brings together two industry leaders to deliver an end-to-end Zero Trust approach to enterprise security. By combining Armis Centrix™ with Cato's cloud-native Secure Access Service Edge (SASE) platform, organizations gain unified visibility, contextual insight, and consistent cyber exposure management (CEM) across all connected assets and their associated pathways, whether physical, virtual or hybrid.

State of the Market

Modern enterprises often operate in a more distributed and dynamic environment than ever before. Cloud adoption, hybrid work, the convergence of IT and OT, and the web of interconnected networks have created complex environments filled with managed, unmanaged, devices & assets that are essential for organizational operations. These environments offer new opportunities for agility and efficiency, but they also dramatically expand the attack surface.

Traditional network and endpoint security tools were designed for static, perimeter-based models and not for the attack surfaces of today. As the number of connected assets explodes, organizations struggle to maintain visibility and enforce consistent security controls. Meanwhile, attackers increasingly target unsurveilled devices and assets as entry points, exploiting blind spots that conventional tools can't see or manage.

The Challenge

As digital transformation accelerates, enterprises face a growing disconnect between their expanding digital ecosystem and the security tools meant to protect it. The proliferation of unmanaged assets, from smart sensors and cameras to industrial controllers and medical devices, introduces countless new entry points that often go unmonitored.

Organizations need to know what's connected to their networks, where those connections originate, what threats may be lurking, and what level of risk they pose. Traditional solutions lack the visibility and context needed to identify these assets or understand their behavior and variations that may pose a risk. Enforcing consistent policies and effective compensating controls across hybrid networks, remote sites, and cloud environments remains difficult. These gaps lead to inconsistent protection, regulatory non-compliance, and increased exposure to attacks. Enterprises require an integrated, automated solution that can bridge the divide between asset intelligence and compensating controls, in order to ensure that every asset and pathway is visible, secured and controlled.

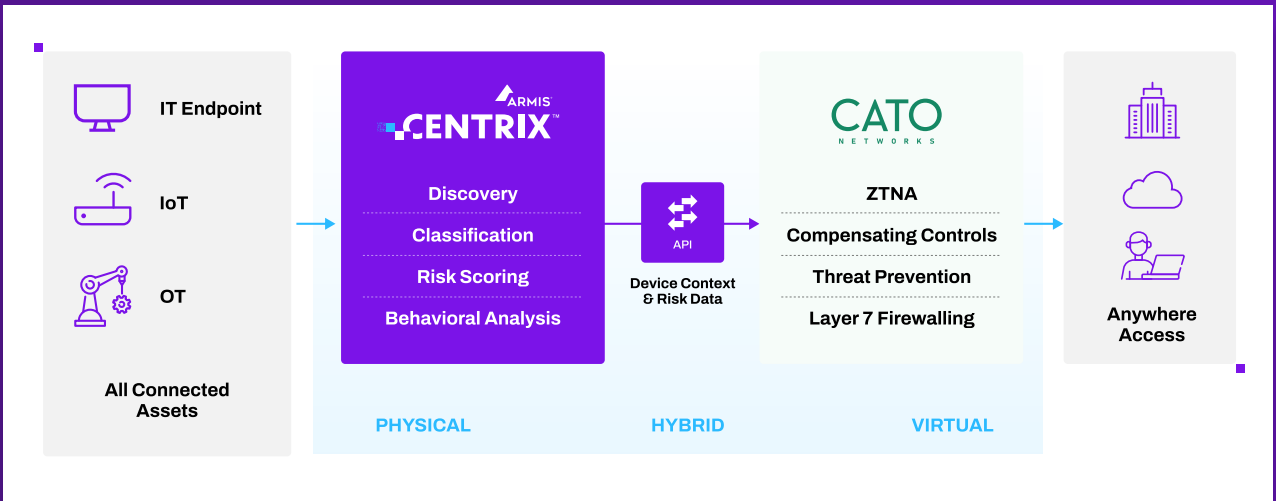
The Solution

The joint Armis and Cato Networks solution provides that bridge. Armis Centrix™ offers unmatched visibility into every asset connected to the enterprise network whether it is managed or unmanaged, or whether it is physical, virtual or a combination of the two. It discovers and delivers detailed insights into every asset and associated pathway, operating system, behavior, and risk posture. This continuous intelligence is then fed into Cato's cloud-native SASE platform, which provides centralized firewalling, Zero Trust Network Access (ZTNA), threat prevention, and secure SD-WAN capabilities.

Armis enriches Cato's enforcement engine with device context and risk scoring based on business criticality. This allows Cato to apply risk-based access policies and dynamic segmentation and compensating controls automatically, isolating vulnerable or compromised devices before they can threaten critical systems. Together, Armis and Cato create a unified, intelligent security fabric that spans every asset, user, and connection, enabling a true Zero Trust posture across both IT and OT domains.

How It Works

The integration between Armis and Cato Networks connects **Armis Centrix™** with **Cato's SASE cloud platform** through a secure API framework. Armis continuously identifies every asset and pathway and evaluates each security posture based on observed behavior, known vulnerabilities, and threat intelligence.



This real-time data, including asset attributes, operating system, and risk score, is automatically shared. Cato then uses this information to inform and refine its network access decisions, enforce segmentation policies, and correlate security events across user traffic and asset activity.

For example, if Armis detects that a device's behavior deviates from its baseline or its risk score increases, Cato can dynamically restrict that device's network privileges or isolate it entirely. The integration is agentless, cloud-native, and deploys quickly without requiring new infrastructure. The result is immediate, automated visibility, security and control across the entire connected environment.

Use Cases

Securing IoT and OT Assets Across Global Operations

A global manufacturing enterprise uses Armis to discover and classify every connected asset across its factories and remote facilities, including industrial controllers and IoT sensors. This intelligence is fed into Cato's SASE platform, which applies access and segmentation policies based on device risk. High-risk or vulnerable devices are automatically isolated from critical systems, ensuring both operational safety and business continuity.

Zero Trust Access for Distributed Workforces

A multinational organization retains a large remote workforce. When users attempt to connect, Cato leverages Armis' risk scoring to determine whether their assets meet security requirements. Assets exhibiting suspicious behavior or outdated security configurations can be denied access or placed in restricted network zones, strengthening Zero Trust compliance across the enterprise.

Unified Compliance Across IT and OT Environments

In regulated industries such as healthcare and energy, compliance demands end-to-end visibility and control over every connected device. By combining Armis' continuous asset discovery and risk analysis with Cato's centralized security enforcement, organizations can demonstrate full compliance with frameworks like NIST, ISO 27001, and IEC 62443, while simplifying and delivering full audit preparation and reporting.

Key Business Outcomes and Benefits

The Armis and Cato Networks integration transforms enterprise security by bridging the visibility and security gap that threatens resilience and operation. It empowers organizations to identify and automate risk-based policy decisions with precision and confidence.

The joint solution delivers continuous risk assessment, improved detection of unmanaged or shadow IoT/OT devices, and real-time policy enforcement that scales globally. Operationally, it unifies visibility and control within a single, cloud-native architecture, thereby reducing management overhead and accelerating incident response. Financially, enterprises benefit from reduced cyber exposure, increased operational resilience, while eliminating the need for multiple point solutions that never fully solve the challenges that impact the bottom line. Armis and Cato enable organizations to operate securely and efficiently in a connected, perimeterless world with complete confidence that every asset, user, and connection is continuously monitored and protected.

Summary

Armis and **Cato Networks** redefine what it means to have unified visibility, security and control in modern enterprise CEM. The partnership delivers the clarity, context, and control that today's enterprises need to manage risk, meet compliance requirements, and secure innovation at scale. By combining Armis' asset discovery, deep asset intelligence and risk scoring with Cato's global, cloud-native network protection, organizations gain a powerful, adaptive security framework that extends Zero Trust and compensating controls across all environments to ensure that the organization can deliver on its mission with a security and business aligned network.