PARTNER BRIEF

Armis Exposure Management & Security on NVIDIA BlueField-3 DPU

Agentless OT Security

Armis has collaborated with NVIDIA to deliver a transformative solution for protecting Cyber-Physical Systems (CPS) by integrating Armis Centrix™ for Cyber Exposure Management & Security on NVIDIA BlueField-3 DPU platforms. This joint solution ensures security from the endpoint-level to the network, as well as operational continuity while providing comprehensive visibility, threat detection, and enforcement capabilities for ICS and OT environments.

The Armis cyber exposure management and security solution, deployed on NVIDIA BlueField-3 DPUs revolutionizes Cyber-Physical System (CPS) protection, delivering in-depth visibility, threat detection, and enforcement capabilities without impacting host performance or operations. This agentless approach ensures seamless deployment across IT and OT environments, enhancing asset visibility, detecting vulnerabilities and threats in real-time, and preventing lateral movement from compromised IT systems into critical OT networks. Leveraging Armis AI-powered exposure management and security capabilities combined with deep packet inspection, and runtime integrity monitoring, the solution provides comprehensive protection, enabling organizations to mitigate sophisticated, targeted attacks while maintaining operational continuity and resilience.

The Challenge

Today, organizations across Energy, Utilities, and Manufacturing face an unprecedented rise in cyberattacks, while lacking effective security solutions that deliver full visibility and control in dynamic environments.

Legacy Systems

Many critical assets in operational environments run on outdated operating systems and firmware, leaving them vulnerable to known CVEs and unpatchable weaknesses. Additionally, proprietary and unsecured protocols further exacerbate risks, as they often cannot be serviced by traditional network security appliances to detect and mitigate threats effectively.

IT/OT Convergence

The growing convergence and integration of IT and OT environments introduces significant security challenges. Limited visibility into network-connected devices makes it difficult to identify vulnerabilities and monitor activity. Moreover, the interconnection of OT systems with cloud services and remote access solutions increases the risk of lateral movement, enabling attackers to transition from compromised IT networks to critical OT systems.

Sophisticated Targeted Attacks

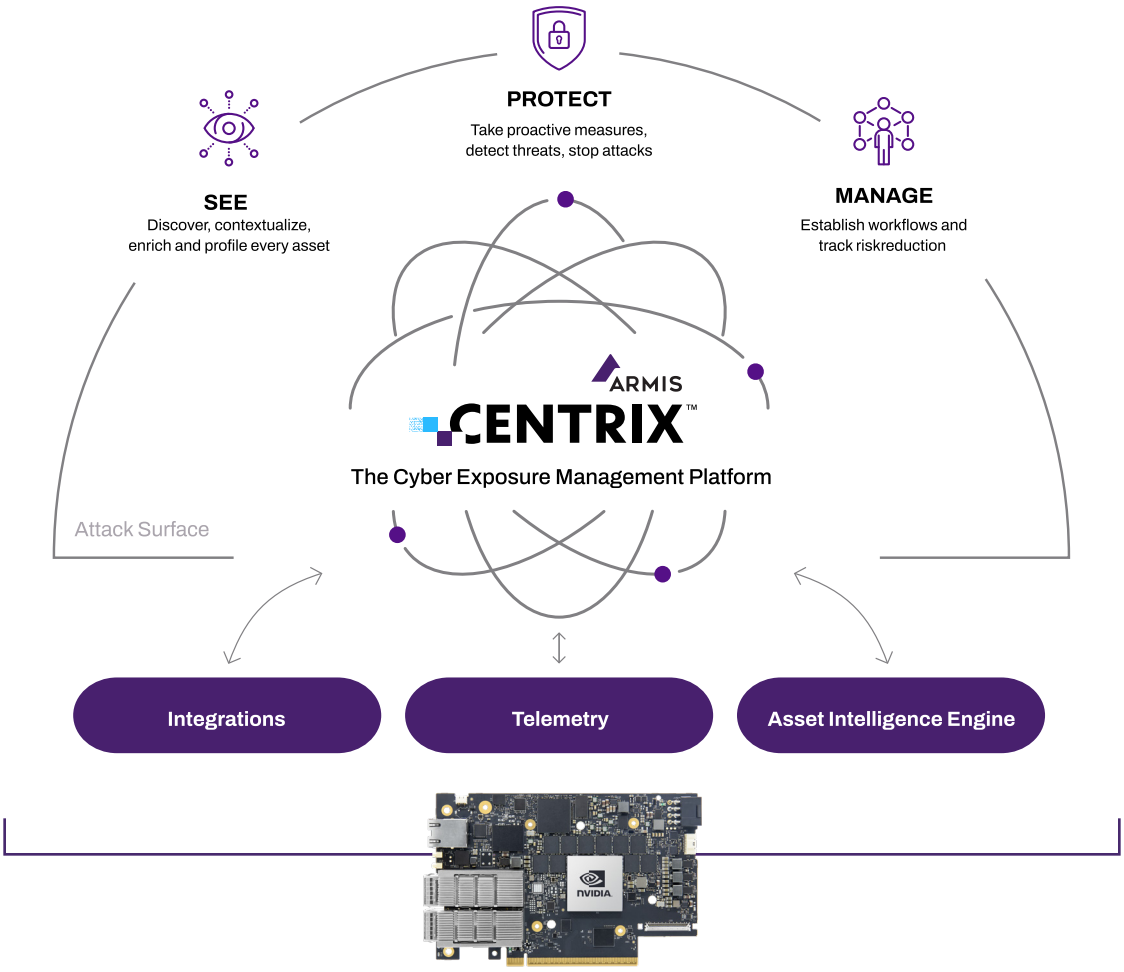
Advanced persistent threats (APTs) and nation-state attacks often mimic legitimate communication patterns or run “low and slow” attacks, making them challenging to detect. Identifying such operational anomalies without disrupting continuity poses a significant challenge, especially in environments where downtime is unacceptable.

Operational Conflicts

A key challenge lies in balancing robust security measures with the need for uninterrupted OT operations. Security best practices, such as segmentation and monitoring, can sometimes conflict with the networking priorities and operational requirements of OT systems, creating friction between security and operational goals.

Why This Solution Is Groundbreaking

This groundbreaking solution technology redefines cybersecurity for critical infrastructure and other OT environments. Unlike traditional solutions that rely on host-based agents or intrusive appliances, this joint solution operates independently of the host system, ensuring zero performance impact and resilience to tampering. By employing non-intrusive data collection techniques, it provides deep asset inventory and insights, real-time threat detection, and AI-powered analytics, offering unmatched visibility and control across IT and OT environments. Its agentless design eliminates deployment complexity while enabling enhanced visibility and isolated protection that is unique in the marketplace, addressing the specific challenges of legacy systems, IT/OT convergence, and sophisticated threats with best-in-class precision and scalability.



Realized Benefits

Enhanced Visibility and Control
Armis, deployed on NVIDIA BlueField-3 DPU platforms, provides unmatched asset visibility by identifying IT, OT and IoT devices as well as non-communicating and dormant devices often overlooked in traditional monitoring. With Deep Packet Inspection (DPI), the solution enables granular traffic analysis directly at the endpoint, ensuring comprehensive oversight of IT and OT environments.

Comprehensive Protection
Armis on BlueField-3 DPUs fortifies security by detecting and preventing lateral movement into and out of critical OT systems. Leveraging real-time monitoring and AI-driven security and analytics, the solution quickly identifies and mitigates threats, delivering robust protection tailored to the needs of modern OT organizations.

Seamless Deployment
The integration of Armis software capabilities with the BlueField-3 DPU architecture ensures an agentless, appliance-free deployment. This minimizes complexity and maximizes the use of existing infrastructure. The platform is agnostic to the host OS and firmware, ensuring compatibility and scalability across a wide range of environments without compromising host performance or resiliency.

Operational Continuity
By isolating security workloads onto the BlueField-3 DPU, Armis prevents the spread of cyberattacks while maintaining uninterrupted operations. Runtime operational integrity monitoring ensures that systems remain functional and secure, preserving business continuity.

How the Solution Works

Platform Integration

Armis' advanced capabilities are deployed directly on NVIDIA BlueField-3 DPUs, providing a secure, isolated environment independent of host systems. These DPUs connect seamlessly as PCIe add-on cards and are broadly available by all major OEM/ODM system vendors.

Multilayered Protection

At the Network Level

Armis, powered by BlueField-3 DPUs, delivers comprehensive visibility and traffic monitoring across IT and OT networks. It enables real-time threat detection, network isolation, and enforcement of approved communication pathways, ensuring secure network operations.

At the Host Level

The solution provides real-time monitoring of hosts and applications, enforcing granular policies for inbound and outbound connections on a per-process basis. This proactive approach dynamically identifies and addresses vulnerabilities and misconfigurations at the host level.

Key Features Include

Asset Discovery

Identifies, classifies, and catalogs devices across the network to provide a comprehensive asset inventory.

Threat Detection

Delivers real-time identification of vulnerabilities, misconfigurations, risk, and active threats to minimize exposure.

Deep Packet Inspection

Monitors all traffic—both inbound and outbound & east / west—for anomalies, violations and potential threats.

Armis AI-Powered Insights

Offers actionable intelligence, findings, cross-device correlations, and advanced vulnerability assessments for informed decision-making.

Optional Features

Includes a multi-detection engine, dynamic network mapping, and enforcement mechanisms to further enhance the security framework.

Armis, the cyber exposure management & security company, protects the entire attack surface and manages an organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world, Armis ensures that organizations continuously see, protect and manage all critical assets - from the ground to the cloud. Armis secures Fortune 100, 200 and 500 companies as well as national governments, state and local entities to help keep critical infrastructure, economies and society stay safe and secure 24/7.

Armis is a privately held company headquartered in California.

1.888.452.4011

Website

Platform
Industries
Solutions
Resources
Blog

Try Armis

Demo
Free Trial