PARTNER BRIEF

Armis + NVIDIA: Supercharging AI and Data Center Security

Summary

Armis and NVIDIA are joining forces to redefine cybersecurity for the age of AI and high-performance computing. Through the integration of the Armis Centrix™ cyber exposure management platform with NVIDIA BlueField-3 Data Processing Units (DPUs), this joint solution delivers complete visibility, real-time threat detection, and automated enforcement—without sacrificing performance. By shifting security processing off the host and onto the DPU, organizations can now protect their most critical AI and data center infrastructure with zero performance trade-offs, ensuring both speed and security at scale.

The Challenge

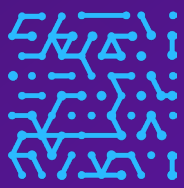
AI and Data Center Growth = Explosive Cyber Risk

As enterprises accelerate AI adoption and scale data center operations, their environments grow increasingly complex. Virtualization, distributed workloads, and hybrid architectures create massive, opaque attack surfaces that traditional tools cannot adequately protect.

Expanding & Invisible Attack Surface: Physical servers, hypervisors, and thousands of VMs create blind spots where assets go unmanaged and vulnerabilities persist.

Fragmented Security Controls: Legacy tools operate in silos, providing partial views and inconsistent data. This lack of unified visibility prevents teams from prioritizing real risks or coordinating rapid response.

The Performance Dilemma: Host-based agents consume valuable CPU cycles, forcing security teams to choose between visibility and performance which is an unacceptable trade-off for AI-intensive environments.



The Breakthrough: Security, Offloaded to the DPU

The Armis on NVIDIA BlueField-3 solution breaks the decades-old compromise between protection and performance. By embedding Armis Centrix™ directly onto the DPU, security operations are fully offloaded from the host, creating an independent, tamper-proof, and high-speed security control plane.

Core Advantages

- Zero Performance Impact - Security workloads run on the DPU, not the host thus freeing CPU cycles for critical AI and compute operations.
- Tamper-Proof Security Plane - Running independently from the host OS, the DPU remains invisible and inaccessible to attackers, even in a compromised environment.
- Total Visibility - The combined solution delivers deep host and hypervisor introspection with complete internal and external network visibility thereby closing the final blind spot in data center security.
- Future-Ready Architecture - Validated on NVIDIA RTX PRO Server and built for BlueField-4, the joint solution is ready to evolve with the next generation of AI and hardware acceleration technologies.

How It Works: A Closed-Loop, Hardware-Accelerated Security Pipeline

01

See & Classify
Armis on the DPU continuously discovers and classifies every connected asset by monitoring all east-west and north-south traffic for anomalies and potential threats.

02

Analyze & Detect
NVIDIA DOCA Argus provides hardware-level introspection into hosts and VMs, detecting malicious processes, kernel tampering, or unknown vulnerabilities.

03

Protect & Enforce
Armis continuously monitors and manages asset posture, enforcing policies directly from the DPU to minimize exposure and maintain resilience. When misconfigurations, vulnerabilities, or threats are detected, Armis Centrix™ automatically isolates affected systems and enacts compensating controls to blocks malicious traffic, and prevents lateral movement across the data center.

Key Benefits

Unleash AI & Compute Performance - Eliminate the need for a host and leverage the DPU to eliminate the visibility-performance trade-off and maximize return on compute investments.

Comprehensive Host Exposure Management - Achieve hardware-level insight into the host, hypervisor, and virtual machines for real-time identification of vulnerabilities, misconfigurations, and active threats.

Automated Orchestration & Enforcement - Armis Centrix™ integrates with your existing firewalls, NAC, and other enforcement points to automatically contain threats thereby quarantining compromised assets and blocking malicious traffic before it spreads.

Agentless, Seamless Deployment - Delivered as an application directly on BlueField-3, the solution eliminates host-based agents entirely by simplifying deployment and ensuring compatibility across operating systems, hypervisors, and firmware.

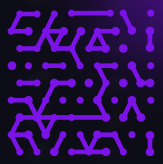
Use Cases

- **Securing High-Performance AI/ML Workloads -** Protect GPU-accelerated servers during model training and inference without consuming critical CPU/GPU cycles. Ensure that high-value AI infrastructure is secured without slowing down innovation.
- **Zero-Trust Segmentation for Virtualized Environments -** Enforce granular microsegmentation policies between virtual machines and containers on the same host. By monitoring all east-west traffic, the solution can detect and prevent the lateral movement of threats inside the data center, a critical tenet of modern security.
- **Continuous Host Integrity and Vulnerability Management -** Leverage hardware-level introspection to continuously monitor host systems for vulnerabilities, misconfigurations, and malicious processes. Identify risks in real-time without deploying performance-impacting agents.
- **Accelerated Threat Detection for Encrypted Traffic -** Offload and accelerate the inspection of encrypted traffic at line rate on the DPU, uncovering threats that would otherwise remain hidden without impacting host performance.

The Future of AI and Data Center Security

Together, Armis and NVIDIA are building the foundation for secure, intelligent, and autonomous data centers where performance, visibility, and protection coexist seamlessly.

This collaboration eliminates the trade-offs that have long defined cybersecurity, empowering organizations to accelerate innovation safely while maintaining the highest levels of operational integrity and resilience.



ARMIS®

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