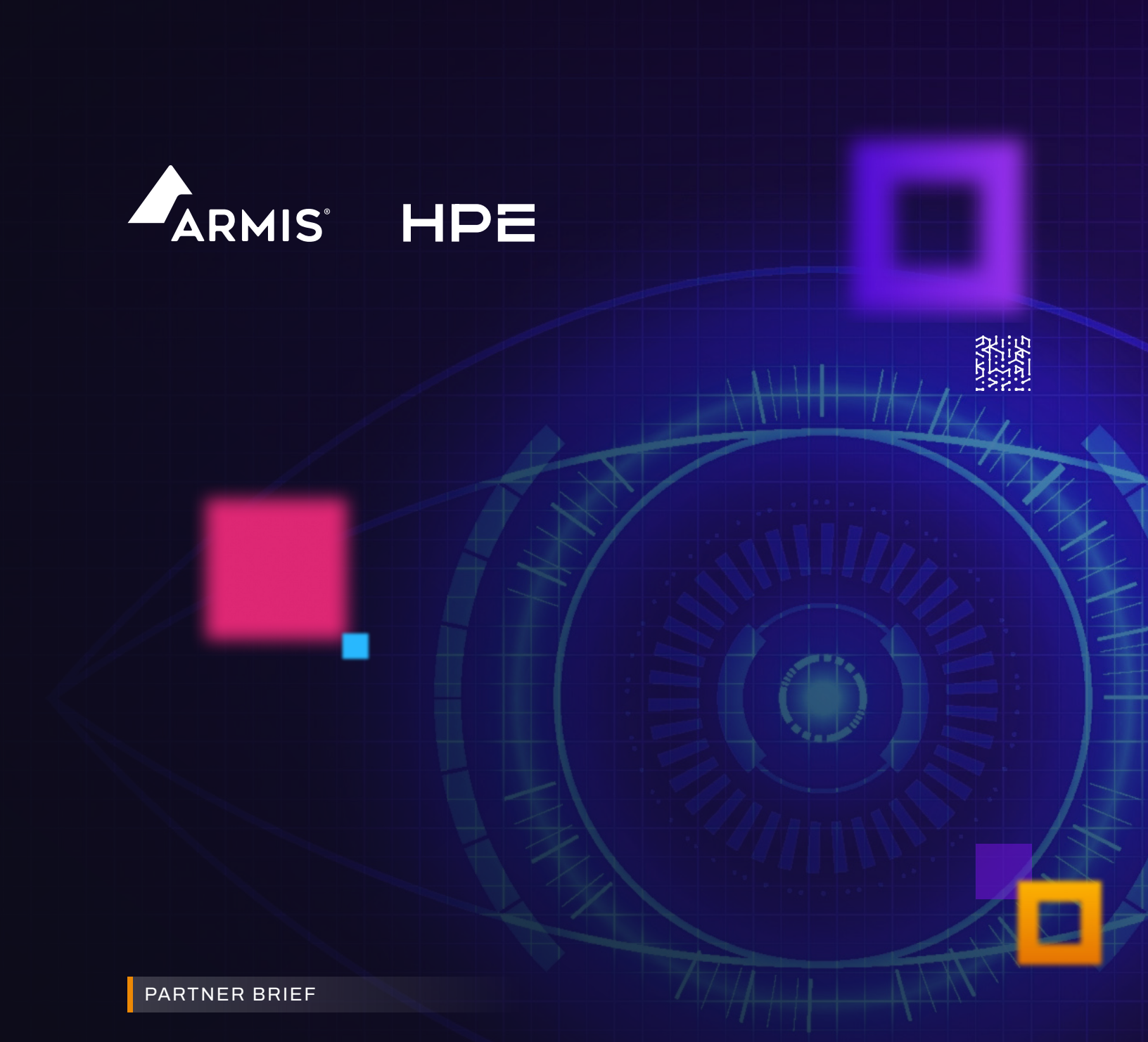

PARTNER BRIEF

Armis + HPE Neworking: Complete Asset Visibility and Security

Overview

As networks evolve, traditional boundaries are disappearing, and organizations face an explosion of connected devices which include IT, OT, IoT, and IoMT that are physical, virtual and a combination of both. Every new connection and every new asset increases the attack surface, creating blind spots that conventional security tools cannot address. The joint Armis and HPE Networking solution delivers a closed-loop, automated security system that combines best-in-class network infrastructure with comprehensive Cyber Exposure Management (CEM) across the digital footprint.

State of the Market

Modern enterprises are experiencing unprecedented device proliferation. IoT, OT, BYOD, and cloud-managed devices now coexist with traditional corporate endpoints, creating highly dynamic and complex networks. Organizations struggle to answer fundamental security questions that include:

- What devices are on the network?
- Are they secure and compliant?
- How can risky devices be identified, appropriately triaged and mitigated before they become a threat?

This lack of visibility, contextual intelligence, and applied security that align with business requirements leaves businesses vulnerable to breaches, operational disruptions, and compliance violations.

The Challenge

Traditional security solutions are inadequate for today's diverse networks due to:

Blind Spots - Unmanaged devices, ephemeral assets and dormant devices largely remain invisible and thus are unable to be secured.

Point Solutions - Lack of centralized device intelligence is a fertile environment for stealthy and sophisticated threats to be missed due to fragmented information that is never correlated.

Manual Enforcement - Risk mitigation has traditionally relied on human intervention, slowing response, increasing the change for human error and thus increasing exposure.

Organizations need a solution that delivers comprehensive visibility, contextual intelligence, prioritization and automated compensating control across all connected assets and their pathways.

The Joint Solution

The Armis and HPE Networking solution provides a unified approach to network security by delivering:

Complete Visibility - Armis Centrix™ discovers, identifies, and classifies every asset, including those managed by HPE Aruba Networking WLC, Mobility Conductor, Central, and HPE Juniper Networking Mist.

Contextual Intelligence - Armis Centrix™ enriches device data with extensive context including, OS, serial numbers, version number, deployed patches, historical connections, user details, and much more, thus creating a detailed asset profile for accurate risk assessment.

Automated Enforcement - Armis Centrix™ continuously evaluates device behavior and pushes intelligence to HPE Aruba Networking ClearPass, triggering compensating controls like quarantines or session disconnects, transforming the network into a self-defending ecosystem.

How It Works

STEP	DESCRIPTION
See Everything	Armis Centrix™ utilizes a multi-detection engine to discover and classify all assets in real-time.
Add Rich Context	The Armis Asset Intelligence Engine integrates with HPE Aruba Networking WLC, Mobility Conductor, Central, and HPE Juniper Mist to enrich device data and map network topology and potential attack paths.
Analyze & Detect	Armis Centrix™ correlates traffic behavior with contextual insights to detect misconfigurations, vulnerabilities, and threats. It then builds a prioritized list of actions to take based on business operations and provides a path for quick and efficient mitigation.
Automate Response	Detected risks trigger immediate automated actions via HPE Aruba Networking ClearPass, such as blocking, quarantining or disconnecting high-risk devices.

This creates a virtuous cycle: visibility fuels intelligence, intelligence drives detection, and detection triggers automated enforcement and business resilience.

Use Cases

Across industries, organizations are using the combined power of Armis and HPE Networking to transform their security posture. From hospitals protecting connected medical devices to manufacturers securing production lines and enterprises enforcing zero trust at scale, these case studies showcase how complete visibility and automated enforcement drive measurable results in resilience, compliance, and operational efficiency. Typical use cases include:

- **Enterprise Security -** Detect and secure unmanaged or misbehaving assets before they cause damage.
- **OT and IoT Environments -** Ensure operational technology assets that have been traditionally ignored are visible, monitored, and protected from threats.
- **Compliance and Audit -** Maintain an accurate, up-to-date inventory and proof of compliance for regulatory reporting and internal audits.
- **Remote and Hybrid Work -** Securely enforce access policies for laptops, BYOD, and cloud-managed endpoints whether they are across the campus or across the globe.

Key Business Outcomes and Benefits

The Armis and HPE Networking solution delivers more than visibility, it drives measurable business value. By unifying asset intelligence with automated network enforcement and compensating controls, organizations gain stronger security, simplified operations, and greater confidence in their ability to protect the organization. The result is a smarter, self-defending network that ensures secured business operations, streamlines compliance, and supports digital transformation.

- **Complete Asset Visibility -** Gain a real-time, comprehensive inventory of all network-connected devices.
- **Eliminate Unacceptable Cyber Exposure -** Ensure operational technology assets that have been traditionally ignored are visible, monitored, and protected from threats.
- **Operational Efficiency -** Eliminate costly and error prone manual asset tracking and incident response processes.
- **Improved Compliance -** Maintain audit-ready records and security posture reports.
- **Future-Proof Security -** Scale security effortlessly as the network and its devices grow in complexity and as cyber risk evolves.

Conclusion

HPE Networking provides the secure, high-performance foundation, and Armis delivers the intelligence and automation to secure every device on the network. Together, the Armis and HPE Networking solution delivers unmatched visibility, contextual awareness, and automated threat enforcement, enabling organizations to safely scale and embrace innovation.

Contact your local HPE or Armis representative to learn how to secure your entire network ecosystem with this industry-leading solution.

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

armis.com

Learn how Armis empowers our partners and joint customers with unmatched visibility and control.

Book A Free Demo