PARTNER BRIEF

Armis + CyberArk: Unified Asset Intelligence and Identity Security

Overview

Enterprises today rely on an enormous range of connected devices to run their businesses and deliver critical services. Yet these devices often operate outside the reach of traditional security tools, leaving organizations with significant cyber exposure risk from blind spots and unmanaged access pathways. Armis and CyberArk have partnered to close this gap. Together, they combine full-spectrum device intelligence with a trusted identity security platform, extending privileged access protection to every device in the enterprise.

State of the Market

The modern enterprise has evolved into a sprawling landscape of interconnected technologies. Digital transformation, automation, and smart systems have accelerated the adoption of new device categories far beyond laptops and servers. Industrial control systems, building management sensors, medical devices, cameras, badge readers, and thousands of other embedded systems now form the backbone of daily operations. Most of these devices were never designed with security in mind, and many lack agents, standard authentication mechanisms, or proper credential management.

At the same time, attackers have increasingly shifted their tactics toward identity-based compromise. Default passwords, hardcoded credentials, and unmanaged service accounts have become easy entry points that allow adversaries to quietly gain a foothold in the environment and then move laterally across networks. Regulatory pressure is also intensifying, with industries such as healthcare, manufacturing, and critical infrastructure now being required to prove they can identify and control both devices and their associated privileges.

These trends have forced organizations to rethink how they secure their environments. Visibility is no longer enough. Identity control is no longer enough. The market now requires a unified approach where device intelligence and privileged access security work hand in hand to reduce risk across every layer of the enterprise.

The Challenge

Most organizations simply do not know the full scope of devices operating in their environment. Unmanaged OT controllers, IoT sensors, clinical equipment, and other agentless technologies quietly connect to corporate and industrial networks every day. Many of them use embedded or default credentials that have never been changed, and security teams often have no way to discover these identities, let alone bring them under the protection of a privileged access program.

This lack of visibility, security and control creates ideal conditions for attackers. A compromised camera, PLC, or badge reader becomes a launch pad for lateral movement, allowing adversaries to access high-value systems that were otherwise well secured. Without an authoritative, real-time inventory of devices and full knowledge of acceptable and questionable behaviors, organizations are left with hidden pathways that bypass even the strongest PAM deployments.

The Solution

Armis and CyberArk have partnered to close unaddressed cyber exposure threats by unifying asset intelligence with identity security.

Armis provides agentless discovery and classification of every device and their pathways along with continuous risk assessment and behavioral monitoring.

CyberArk delivers the industry's leading privileged access security, managing and rotating credentials, enforcing least privilege (zero trust), and monitoring all authenticated sessions.

By feeding Armis's deep, contextual device intelligence into CyberArk, organizations can automatically secure the privileged accounts and embedded credentials associated with every connected device, without agents, manual intervention, or disruption to operations.

How It Works

The integration between Armis and CyberArk is designed to operate seamlessly in the background, enhancing security without adding operational friction. Armis begins by discovering every device on the network. It builds a real-time picture of what each device is, how it behaves, what it connects to and what risks it may pose. This includes details like manufacturer, model, operating system, communication patterns, and indicators of vulnerable or unsafe behavior.

Once Armis has developed this full device profile, it shares the relevant context with the CyberArk Identity Security Platform through an API-based connector. CyberArk uses this information to apply the appropriate policies automatically, vaulting and rotating device credentials, onboarding accounts, and enforcing access controls based on the device's purpose, sensitivity, and risk level. If a new device appears or an existing one starts behaving abnormally, both platforms respond in real time, ensuring the proper identity protections are always in place.

This creates a dynamic, closed-loop system where devices are continually monitored, identities are continuously secured, and privileged access governance extends across the entire environment.

Use Cases

Securing Privileged Access in OT Environments

A manufacturing plant needs to secure its industrial control systems without interrupting critical production. Armis discovers every PLC, HMI, and engineering workstation and identifies a PLC using default credentials with a known vulnerability. Armis sends this intelligence and context to CyberArk, which automatically vaults and rotates the PLC's credentials and ensures any technician access flows through a monitored CyberArk session. The PLC is secured instantly, without agents or downtime.

Additional Use Cases

- Controlling access to clinical IoMT devices (infusion pumps, imaging systems) with default passwords
- Securing IoT devices like cameras, sensors, and access control systems
- Automatically onboarding new devices into PAM as they appear
- Enforcing Zero Trust access across IT and OT operations

Key Business Outcomes and Benefits

Security Benefits

- Eliminates misbehaving or at risk devices and potential attack pathways
- Blocks lateral movement by securing default and embedded credentials
- Extends Zero Trust controls to every device
- Enforcing Zero Trust access across IT and OT operations

Operational Benefits

- Automates the onboarding of device identities into PAM
- Reduces manual credential updates and routine identity tasks
- Provides a unified view of device and identity risk across the entire digital footprint

Financial Benefits

- Automates resource heavy operations such as asset inventory and vulnerability management
- Reduces the likelihood and impact of breaches originating from unmanaged devices
- Lowers operational overhead by automating cyber exposure and credential management
- Supports regulatory compliance without additional headcount

In Summary

Together, Armis and CyberArk bring visibility, identity control, and automation to every connected device across IT, OT, IoT, and IoMT environments. This joint solution eliminates blind spots, closes unmanaged access pathways, and provides organizations with a more scalable and resilient approach to Zero Trust. By unifying asset intelligence with identity security, Armis and CyberArk help enterprises reduce risk, strengthen defenses, and protect the systems that power their operations.