SOLUTION BRIEF

Armis Centrix™ Early Warnings and Attack Pathway Mapping: A Powerful, Proactive Combination in OT Environments

Know what attackers target and how they get there

OT assets are fundamental to keeping critical infrastructure operations running in . They power manufacturing, utilities, transportation, and energy worldwide. But as these environments grow more interconnected with IT and IoT systems, their once-isolated networks have become prime targets for modern cyber adversaries.

Today's attackers leverage automation, AI, and threat intelligence of their own to weaponize vulnerabilities faster than ever before. In the past year alone, the industry has seen a surge in OT-focused ransomware and targeted campaigns:

- **Honeywell's 2025 Cyber Threat Report** reported a **46% spike** in ransomware incidents targeting OT systems, often through legacy equipment and weak remote access controls.
- **The BAUXITE campaign (2024–2025)** exploited exposed **Unitronics PLCs** and industrial firewalls across energy and water utilities, deploying a custom OT backdoor known as IOControl.
- **The South African Weather Service** suffered an early-2025 outage that disrupted critical forecasting operations, highlighting the ripple effect OT disruptions can have on safety, supply chains, and economies.

These events share a common theme, Attackers are exploiting visibility gaps, unpatched vulnerabilities, and cross-domain pathways to move laterally from IT networks into OT systems.

For OT teams, the challenge isn't necessarily detecting threats, it's understanding and knowing which vulnerabilities matter most, how attacks could propagate, and acting preemptively to prevent operational impact.

Turning Foresight into Action

Armis delivers the intelligence and context OT security teams need to stay ahead of fast-moving adversaries in an environment where patching is difficult or impossible and mitigations can be time consuming to implement. Here we are honing in on two of Armis Centrix™ powerful capabilities: Early Warning and Attack Pathway Mapping. Let's take a look at how organizations can gain a unified, proactive defense framework by embracing this strategy.

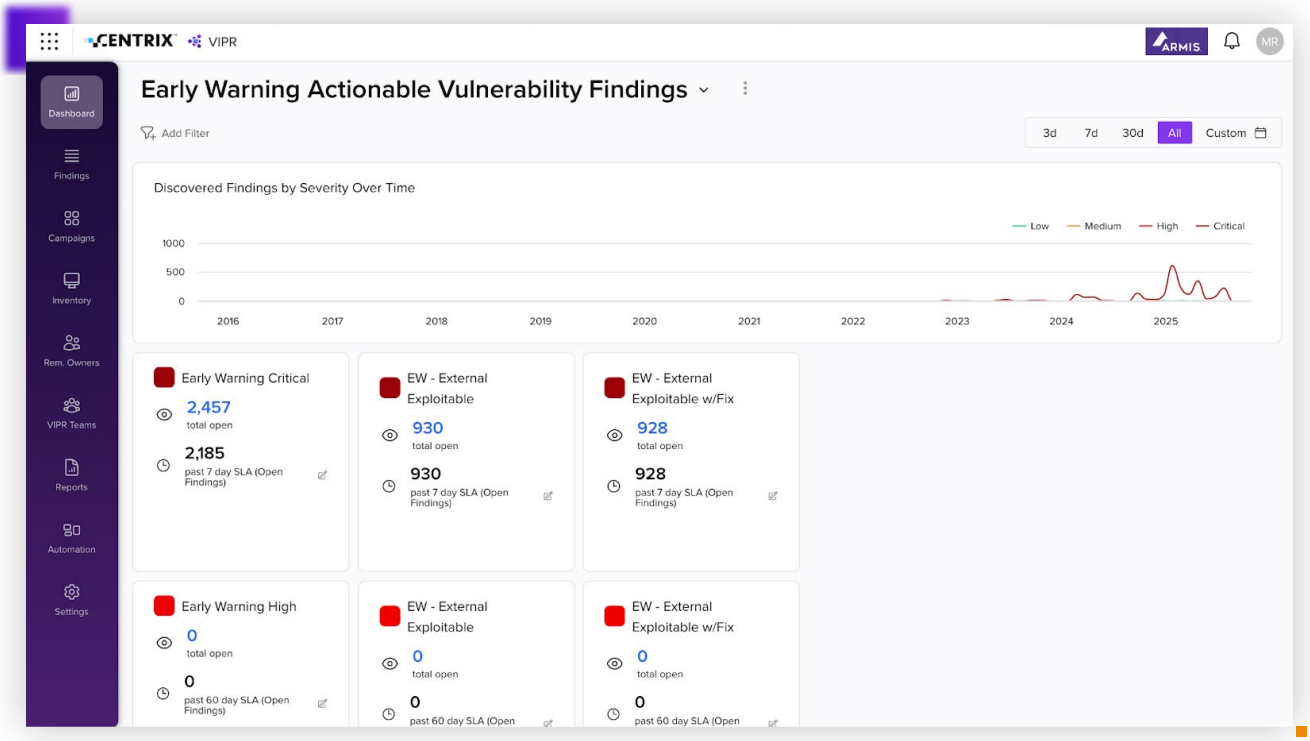
Armis Centrix™ for Early Warning: See the Threats Before They Strike

Armis Centrix™ for Early Warning delivers early, actionable intelligence on vulnerabilities that are being actively exploited or are showing clear signs of imminent weaponization, without relying on predictive modeling. Instead of forecasting risk, Armis draws from a continuously updated intelligence feed of verified, high-risk vulnerabilities and automatically correlates it with your organization's live asset inventory. This makes it easy to see which systems, controllers, or network components are exposed, without requiring advanced security analytics or a highly mature program to benefit from the insights.

For OT operators, that means knowing:

- Which PLC firmware versions are under active exploitation.
- Whether new ransomware families are leveraging known remote-access vulnerabilities in engineering workstations.
- How close your environment is to an attack campaign observed elsewhere in your industry.

This capability allows teams to take preemptive action, hardening or isolating vulnerable assets before attackers can operationalize the exploit. For OT environments, this is especially critical when every maintenance window, downtime, or configuration change carries significant operational cost and risk. By using Early Warning, OT teams can focus their limited resources where it matters most, ensuring they only invest time and disruption to mitigate or remediate the most critical, actively exploited vulnerabilities first.



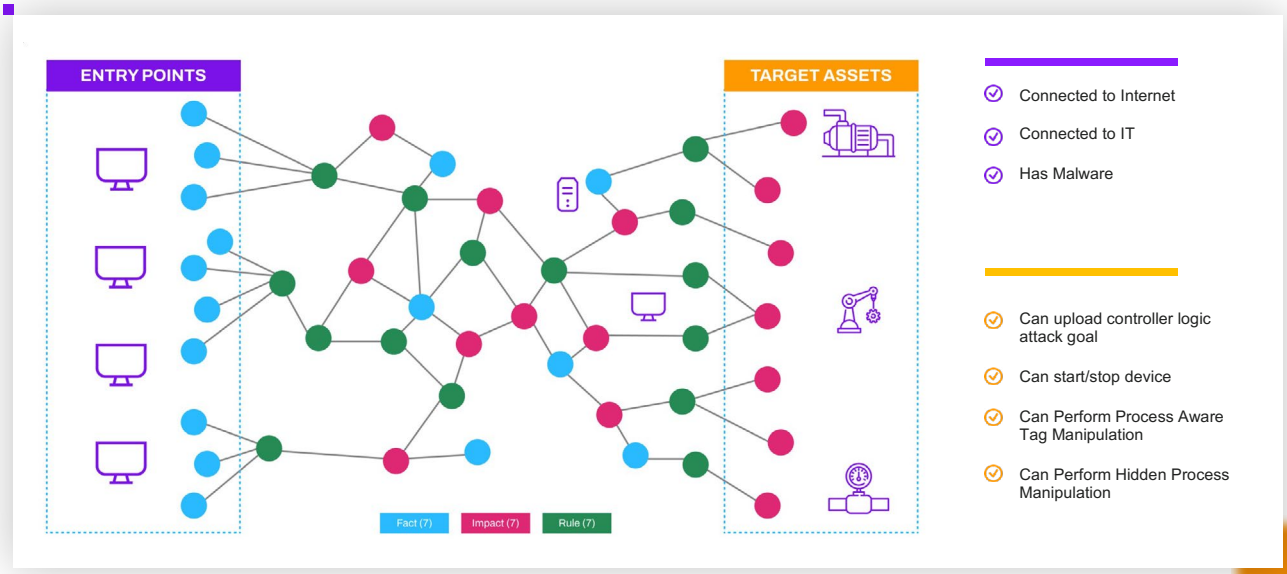
Armis Centrix™ Attack Pathway Mapping: Understand How Threats Move

Early Warning shows what attackers target; Attack Pathway Mapping reveals how they move.

By visualizing lateral movement across interconnected IT, OT, and IoT systems, Armis uncovers the attack paths that real adversaries could exploit. It shows where weak segmentation, shared credentials, or legacy assets create hidden bridges between business and control networks.

Attack Pathway Mapping empowers OT teams to:

- Visualize pathways across entire estate.
- Reachability- how reachable is this asset? If it's an air-gapped asset then even the most severe CVE carries little to no weight in terms of impact.
- Prioritize risks based on operational impact, not isolated CVEs.
- Identify lateral movement routes attackers could take from compromised IT systems into critical control assets.
- Deploy targeted mitigations at key junctions to break the attack chain before escalation occurs.



Why This Matters for OT Teams in Particular

In OT environments, reactive security is not an option. Every minute of downtime can translate into lost productivity, damaged equipment, environmental harm, or even threats to human safety. In sectors like energy, manufacturing, or transportation, an unplanned outage can ripple far beyond a single facility- disrupting supply chains, regional economies, and critical public services.

Traditional cybersecurity tools were designed for IT networks- where patching, downtime, and reboots are part of the normal rhythm. OT doesn't work that way. Industrial systems must run continuously, often on legacy hardware and software, and any change carries operational risk. As a result, defenders are often forced to react to incidents rather than prevent them.

The combined power of Armis Centrix™ for Early Warning and Attack Pathway Mapping changes that equation. Together, they give OT teams what they've never truly had before: the ability to anticipate attacks, understand their potential impact, and act before damage occurs.

Predict and Prevent High-Impact Attacks Before Operational Disruption

Early Warning surfaces the vulnerabilities that adversaries are exploiting, or are about to weaponize, across global threat campaigns. This gives OT teams a forward-looking view of what's coming next, long before attacks reach their environment.

Attack Pathway Mapping turns that foresight into actionable defense by showing how those threats could move within your specific architecture. Instead of chasing alerts, teams can predict where attackers would go next and block them before they ever reach production systems.

This proactive visibility transforms defense from "if" to "when and how", allowing security teams to stop an incident before it starts.

Prioritize Remediation Based on Real-World Threat Intelligence and Propagation Risk

Not every vulnerability is created equal. A theoretical exploit on a disconnected PLC is far less critical than one that sits at a junction between IT and OT systems.

Attack Pathway Mapping gives OT teams that context, revealing which weaknesses could actually lead to an operational impact. When coupled with Early Warning's live intelligence, teams can focus scarce patching and mitigation resources on the few vulnerabilities that truly matter, ensuring maximum risk reduction with minimal disruption.

Enhance Uptime and Resilience by Addressing Vulnerabilities That Truly Matter

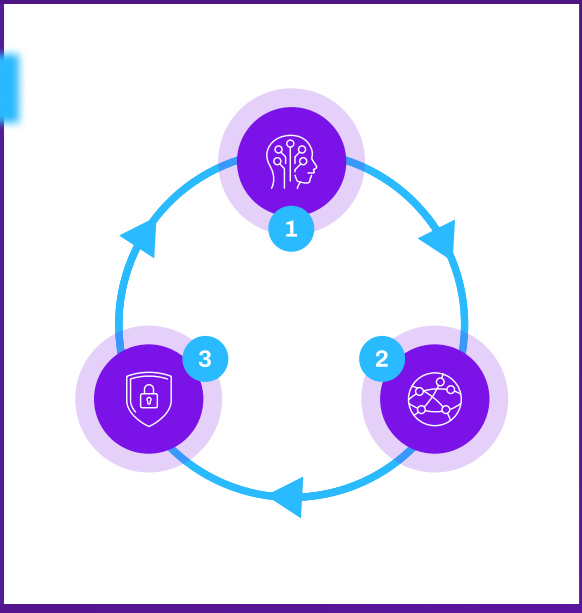
In OT, uptime is everything. The ability to preemptively isolate or secure high-risk assets -before they're exploited -means defenders can maintain operational continuity even in the face of global threat waves. By aligning Early Warning's exploit intelligence with Attack Path Mapping's contextual risk view, OT teams can act with confidence - hardening the right systems, preserving uptime, and building resilience against both known and emerging attack vectors.

Shift from Reactive Firefighting to Proactive Defense

Too often, OT security operates in crisis mode -reacting to incidents after they've already impacted production or safety. Armis flips that paradigm. The integration of Early Warning and Attack Path Mapping creates a continuous feedback loop that keeps security one step ahead of attackers. This enables a strategic shift from reacting to alerts to engineering defenses around foresight and context. The result: fewer surprises, faster decision-making, and a stronger, more resilient OT environment.

Better Together: Predictive Defense in Action

When these two capabilities feed each other, OT teams gain a closed-loop defense system:



1. Early Warning identifies vulnerabilities currently being exploited or likely to be weaponized.

2. Attack Pathway Mapping contextualizes these vulnerabilities within your real asset topology, revealing how an exploit could spread to impact safety or uptime.

3. Vulnerability teams, plant facility teams, and network engineering teams can act proactively-isolating high-risk pathways, applying compensating controls, or patching strategically without disrupting operations.

This fusion turns intelligence into operational insight, ensuring that every mitigation step drives measurable risk reduction.

Let's not forget, this powerful combo also feeds Armis Centrix™ Vulnerability Prioritization and Remediation capabilities to effectively automate, deduplicate, assign ownership and ticketing and remediate risks that are found.

How It Could Have Made a Difference: Recent Scenarios

BAUXITE / IOControl Attacks (2024–2025)

- Early Warning has surfaced emerging exploits similar to those targeting Unitronics controllers weeks before deployment.
- Attack Pathway Mapping could have shown how external connections exposed PLCs directly to the internet or to vulnerable remote gateways, prompting isolation and access control changes.

South African Weather Service Outage (2025)

A cyberattack on critical forecasting infrastructure impacted aviation and agriculture operations.

- Early Warning has identified vulnerabilities in telemetry or SCADA systems being targeted across similar sectors.
- Attack Pathway Mapping would highlight dependencies between data collection systems and operational forecasting servers- enabling targeted defenses to preserve continuity.

Staying Ahead of AI-Driven Adversaries

Modern adversaries are moving at increasing speeds and with impressive complexity. To defend OT environments effectively, security teams need both early insight into emerging threats and deep understanding of how those threats could impact interconnected systems.

Armis Centrix™ for Early Warning and Attack Pathway Mapping together deliver exactly that , turning global intelligence into localized, actionable defense. With this unified approach, OT organizations can outpace evolving threats and safeguard their estate.