

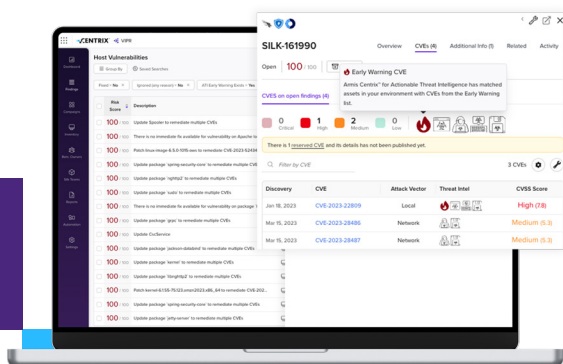


# Armis Centrix™ for Early Warning

Securing an organization from cyberattacks has traditionally been a reactive effort. This approach is fundamentally flawed because it means reacting to events only after an attack is in progress and damage is already done.

## Focus On What Really Matters

Armis Centrix™ for Early Warning is the proactive cybersecurity solution designed to empower organizations with early warning intelligence to anticipate and mitigate cyber risk effectively. By leveraging AI-driven actionable intelligence, Armis Centrix™ provides insights into the vulnerabilities that threat actors are exploiting in the wild or are about to weaponize.



## Shifting from a Reactive to Proactive Response

With human intelligence, smart honeypots and state of the art research, Armis Centrix™ ensures timeliness, unparalleled coverage and accuracy, enabling organizations to stay ahead of evolving tactics from threat actors and protect their critical assets with confidence. Armis Centrix™ for Early Warning allows organizations to:



### See

Potentially weaponized threats before CVEs are ever published and fully visualize your attack surface.



### Protect

Preempt threat actors, address vulnerabilities that are actually being exploited.



### Manage

Ongoing protection against evolving attack methods, establish workflows and track risk reduction.

## Redefining Security By Preempting the Attack

### Operational

#### Early Warning

Early warning intelligence gives you the time to harden your environment before an attack is ever launched. Armis Centrix™ for Early Warning can prove over thousands of instances where the early warning intelligence is ahead (at times, by up to a year) of CISA KEV.

#### SOC/VOC Risk Prioritization

Real-time vulnerability exploit data integrated directly into risk prioritization, empowering the SOC and VOC to focus on what truly matters and what threat actors are actually exploiting.

### Strategic

#### Intelligence-driven Security

Empower organizations to move to an intelligence-driven strategy - determine product configuration, mitigate vulnerabilities and threats, investigate security and product gaps.

### Organizational

#### From Reactive to Proactive

Plan and change, instead of react and break - Improve uptime, staff limitations, site reliability.

See, protect, and manage your attack surface with Armis Centrix™ for Early Warning

Visit [Armis.com](https://armis.com) to find out more



## Key features that make Armis Centrix™ the go-to platform for Total Exposure Management.

A seamless, frictionless, cloud-based cyber exposure management platform, with five AI-driven products, including Armis Centrix™ for Early Warning.

The largest AI-driven Intelligence Engine tracking billions of assets.

A complete, always-on and accurate view of all your assets.

Prioritized vulnerabilities with shorter MTTR.

Accurate threat detection and response.

Dedicated vertical solutions for OT/IoT, governments and medical device security.

“The high fidelity intelligence is critical to us maintaining a secure environment and it’s easy for my team to focus on the most important things, prioritize those vulnerabilities and patch what is required.”

CSO  
Retail

## Why Organizations Trust Armis Centrix™ for Early Warning to Deliver Better Outcomes

- 1 | **Early warnings** to any potential vulnerability before they impact your organization.
- 2 | Proof of over thousands of instances where the **early warning intelligence is ahead** (at times, by up to a year) of CISA KEV.
- 3 | **Attacker Focused Insights** which fills a gap that exists today in intelligence feeds.
- 4 | Focus on the **vulnerabilities that are being exploited** by threats actors before they hit the wild.
- 5 | **98% reduction** in the number of vulnerabilities organizations need to worry about.
- 6 | **AI-driven, automated** contextual risk determination and possible countermeasure actions.
- 7 | **Redefine threat hunting** by proactively identifying CVE gaps and vulnerabilities that are still in the formulation stage.

