ARMIS®

SOLUTION BRIEF

Armis Risk Factors

A Holistic Approach to Risk Management
Powered by Armis Centrix™

At a glance

Holistic approach including a Risk Register and precise remediation recommendations

Unique combination of network - and integrations-based risk discovery

Seamless integration into existing risk management workflows

Cybersecurity risk management is challenging due to the complexity of modern IT and OT environments, the constant evolution of cyber threats, and the need for continuous adaptation. Balancing security with business needs, addressing the skills shortage, and managing costs add layers of difficulty to this critical task.

Complexity and Fragmentation

Today's organizations operate within intricate and interconnected ecosystems. With cloud computing, Internet of Things (IoT) devices, and remote work setups, the attack surface has expanded significantly. This complexity makes it challenging to maintain a secure environment, as weak points can exist at multiple layers and points within the network.

Fragmentation also hinders efficient threat response. When a security incident occurs, having multiple disconnected systems can delay the identification and mitigation of the threat. Inconsistent data formats and lack of real-time information sharing can slow down response times, increasing the risk of damage.

Evolving Nature of Cyber Threats

Cyber threats are continuously changing, with cybercriminals developing new methods to exploit vulnerabilities. This constant evolution demands that organizations remain vigilant and adapt their security measures regularly to protect against the latest threats. Keeping up with this threat intelligence requires substantial resources, making it difficult to always stay one step ahead.

Shortage of Skilled Cybersecurity Professionals

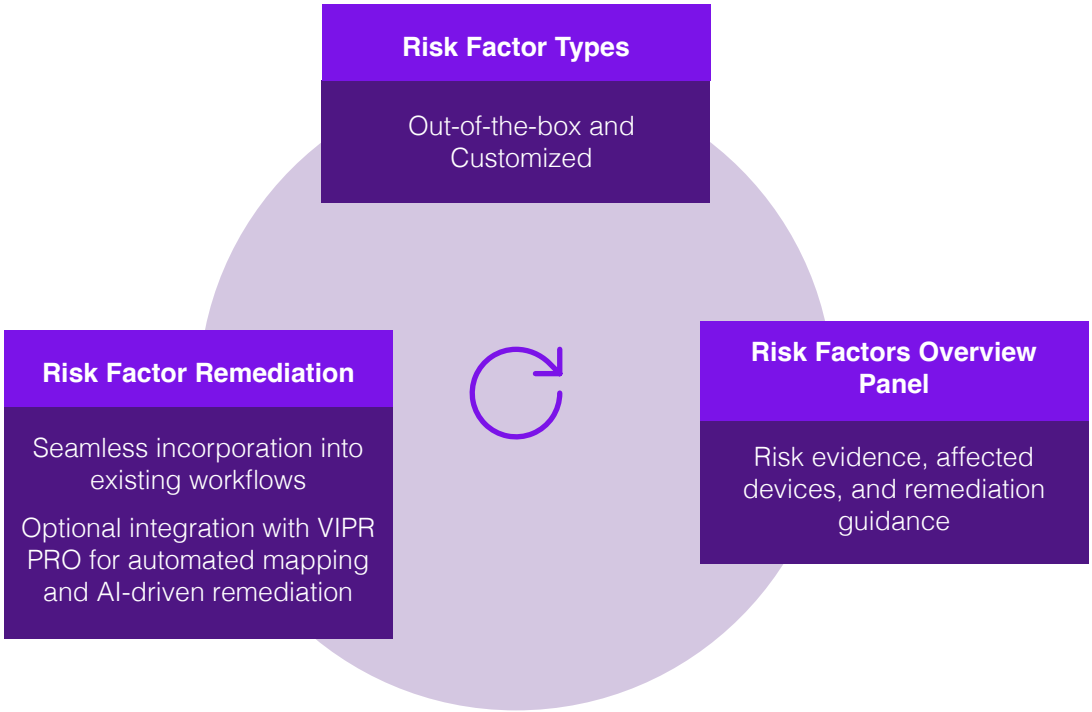
There is a significant gap between the demand for and the supply of skilled cybersecurity experts. This shortage makes it challenging for organizations to build effective cybersecurity teams and accelerates the need for automation.

Traditional risk management fails to capture these dynamics, requiring organizations to adopt more **agile**, **automated** and **adaptive strategies**.

Armis' Unique Approach

Armis Risk Factors offer a pragmatic and holistic approach to risk management based on a combination of integrations-based discovery for known assets, and telemetry data for non-traditional assets. As a result, Armis' native risk identification engine covers both traditional integrations-based risks like Common Vulnerabilities and Exposures (CVEs), but also captures risks identified from the network traffic such as NTLMv1 usage, plaintext credentials or unencrypted network traffic.

With an updated, accurate, and comprehensive view of all assets and risks, the Armis Asset Intelligence Engine acts as the brains behind the platform and feeds Armis Centrix ™ with unique, actionable intelligence to discover, prioritize and address risks across the entire attack surface. With Armis, organizations have the ability to obtain a holistic view of their security posture at any point in time, and gain the means to investigate these risks via the provided root cause analysis and evidence. To close the loop, Armis Centrix™ delivers tailored, actionable remediation recommendations.



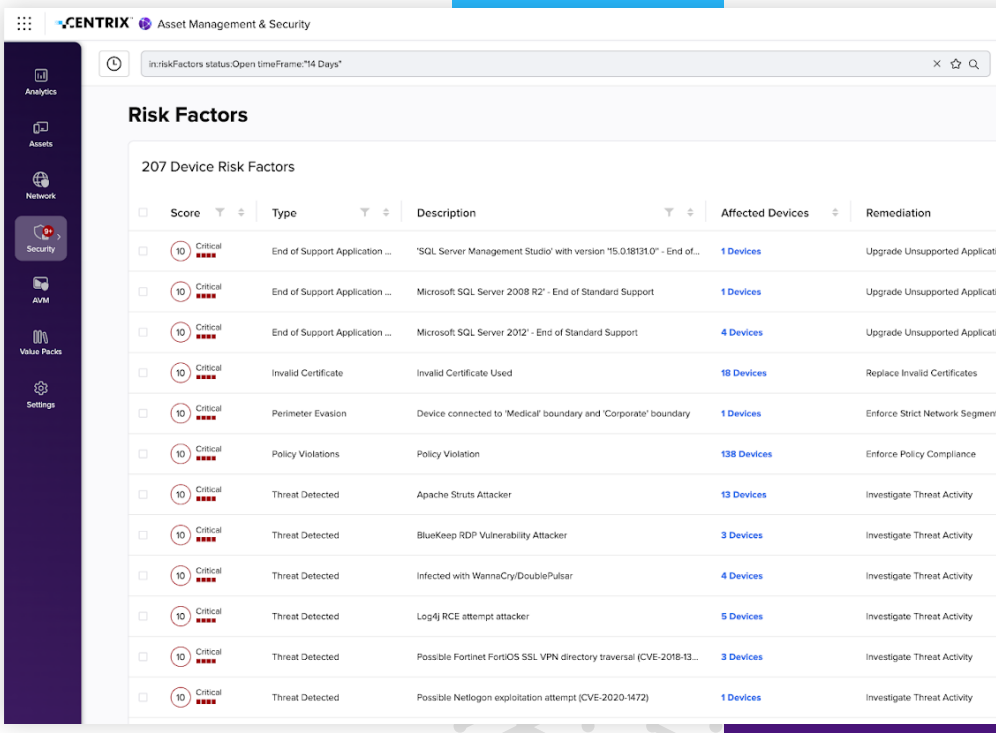
Collective AI-powered Asset Intelligence Engine

The Armis Asset Intelligence Engine tracks all managed, unmanaged, and IoT assets Armis has seen across all our customers. It is a giant, crowd-sourced, cloud-based asset security datalake—the largest in the world, tracking billions of assets. Each profile includes unique device information such as how often each asset communicates with other devices, over what protocols, how much data is typically transmitted, whether the asset is usually stationary, what software runs on each asset, etc. These insights enable Armis to classify assets and detect threats with a high degree of accuracy. Armis compares real-time asset state and behavior to “known-good” baselines for similar assets observed in other environments. When an asset operates outside of its baseline, Armis issues an alert or can automatically disconnect or quarantine an asset through segmentation. Our Asset Intelligence Engine tracks all managed, unmanaged, and IoT assets

Risk Register

Maintaining a risk register is an essential component of effective risk management, enabling organizations to handle risks systematically and efficiently.

The Armis Risk Factors page offers a unified risk register of all identified risks, built on the breadth, depth, and accuracy of the Armis asset inventory. Finally, there’s a single place to manage, prioritize and remediate risks

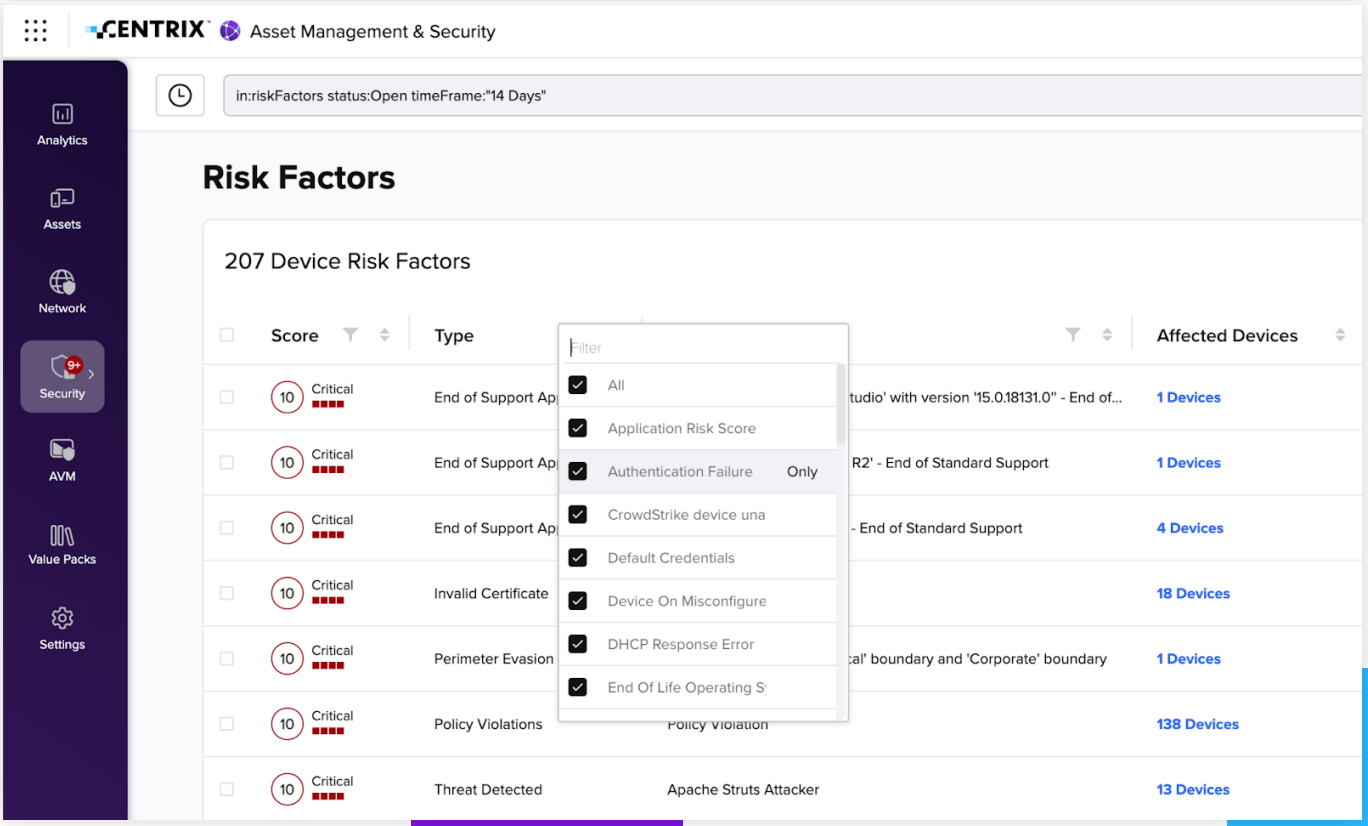


Risk Factor Types

The lack of transparency and interpretability of many (AI) algorithms often makes it difficult to understand how a solution arrives at its risk score calculation. Our combination of adaptable out-of-box Risk Factor types and custom Risk Factors types, offers the flexibility and transparency needed to ensure that we seamlessly align with your specific needs and security posture.

Armis lets you benefit from pre-loaded Risk Factor types including End Of Service (EOS), invalid certificates, unencrypted traffic, and many more - allowing for first assessment to identify and minimize potential risks. Out-of-the-box Risk Factor Types can be enabled, disabled or tailored to your needs using a Risk Score weighting algorithm.

Armis Centrix™ also lets you configure and manage custom Risk Factor types using a policy to refine the risk factors that are most relevant to your industry and individual environment.

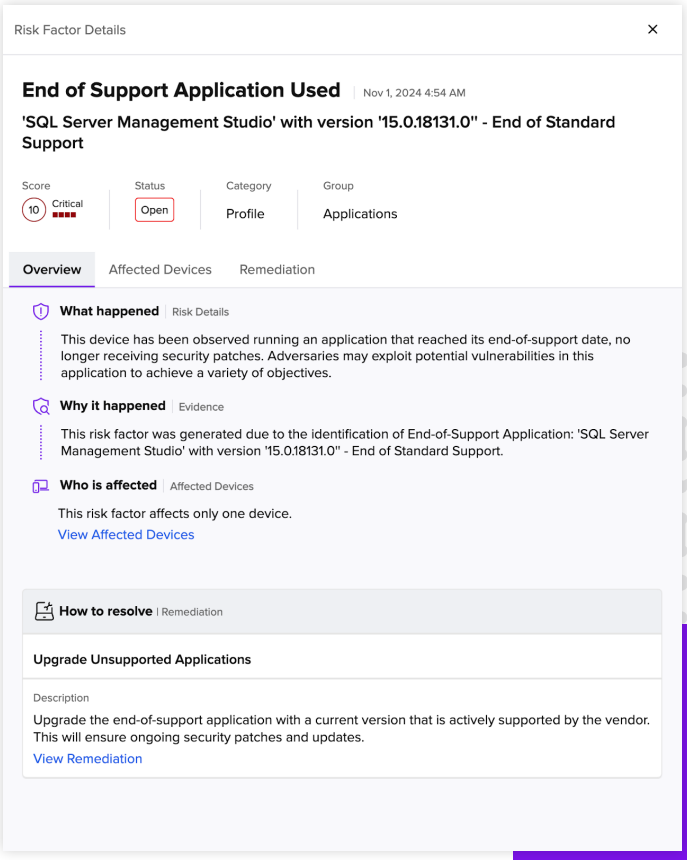


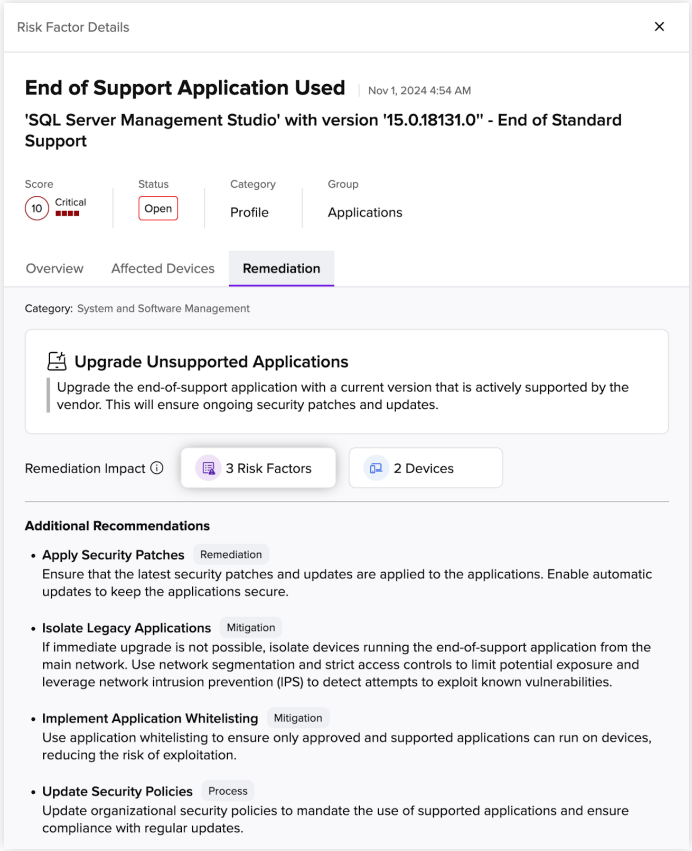
Risk Factor Overview Panel

A single pane of glass provides a unified view of an organization's data and operations, which is crucial for effective monitoring and decision-making.

By consolidating data from various sources into a single Risk Factor Overview Panel, Armis empowers you to make informed decisions quickly, which is vital in managing risks effectively. Quickly assess risk evidence, track affected devices and obtain remediation guidance.

With all relevant information in one place, teams can respond to incidents faster and more efficiently, reducing potential damage and downtime.





Risk Factor Remediation

Remediation and mitigation serve complementary roles in managing and reducing risks associated with cyber threats.

By combining both approaches, Armis lets you manage immediate risks effectively while working towards eliminating the underlying causes of threats and vulnerabilities. This dual strategy helps ensure both short-term protection and long-term and effective security.

Our remediation and mitigation recommendations let you make the most of tailored, actionable insights for each risk-factor type.

Accessible directly through the Armis console or via an external API, we ensure seamless integration into existing workflows.

With Armis Risk Factors you get

- Reduced risk of data breaches and other incidents
- Enhanced resilience and continuity of business operations
- Operational efficiency with a streamlined and approach to risk management
- Prevention of reputational damage

The Armis Difference

Non-Stop Coverage Across Every Industry

Both known and unknown assets represent a growing attack surface yet most cyber tools and programs lack the depth of knowledge to understand and manage them. Armis eliminates the information and security silos and security blindspots that exist within organizations so you can have an authoritative and detailed view of every asset and risk in your environment - from the ground to the cloud. The breadth, depth, and accuracy of the Armis asset inventory exceeds that of any other product on the market today.

Minutes to Visibility, Security and Control

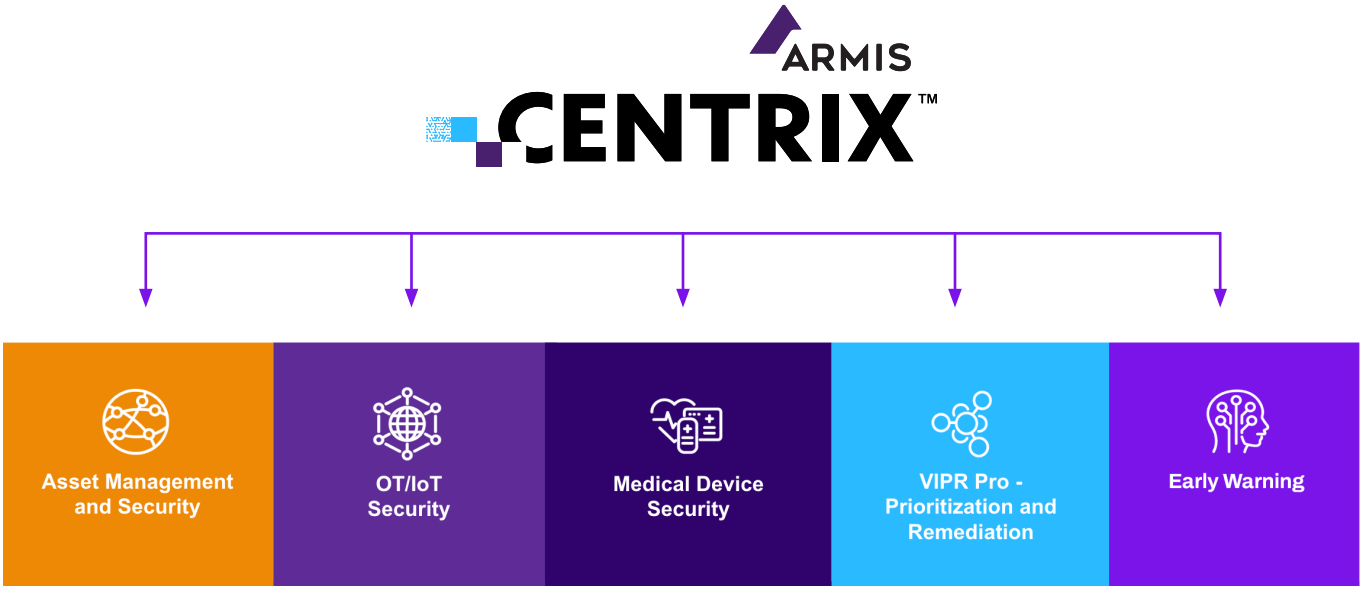
As soon as your data is ingested into Armis Centrix™ the time to useful insights is measured in minutes, not days or weeks. And in the fast-paced battle of cybersecurity, minutes matter. Intelligent risk management insights reduce Mean Time To Resolution (MTTR) significantly.

AI-driven Asset Intelligence Engine

Being the industry's first, Armis monitors billions of global assets. We define what's "normal" and instantly pinpoint anomalies. This vast data pool aids in enhancing data, and continually updates customers with fresh intelligence. Through integration with Armis Centrix™ we don't leave any asset behind, identifying risks even on unconventional assets like medical devices, IoT and OT.

Integration with Armis Centrix™ for VIPR Pro – Prioritization and Remediation

Leverage optional AI-driven predictive capabilities to determine who is most likely responsible for the asset and the remediation. Assign ownership for prioritized fixes based on automated mapping, with ongoing AI-based refinement based on operations feedback.



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
Free Trial