Cyber Exposure Management

Platform Readiness Model

Introduction

Protect the Entire Attack Surface and Manage Cyber Risk Exposure

Continuously **see**, **protect** and **manage** all critical assets

As organizations continue to adopt and rely on digital technologies, the need for protecting the entire attack surface and managing an organization's cyber risk exposure in real time becomes increasingly critical. However, with the proliferation of devices, applications, and cloud-based services, managing cybersecurity assets has become more complex than ever before. The combination of increasing complexity, fragmentation, and loss of control presents a significant challenge for security teams.

While organizations invest heavily in cybersecurity solutions, they often overlook the security of their own assets, leading to an enterprise security blindspot. Attackers can take advantage of this blindspot to gain unauthorized access to an organization's systems and data, resulting in serious consequences such as data breaches, financial losses, and reputational damage.

To address these challenges, organizations need a comprehensive framework for effective protection of the attack surface and management of cyber risk exposure.

Armis has prepared a **Cyber Exposure Management - Platform Readiness Model** to provide organizations with key criteria, checklists, and questions you can review with your teams to ensure you are ready to protect the entire attack surface through an AI-powered Cyber Exposure Management Platform.

See

Organizations need to be empowered to discover all physical and virtual assets, ensuring that the risk that is associated with them is appropriately identified, prioritized and mitigated.

The entire attack surface must be managed and defended in real time. Unmanaged assets are often the first foothold for attackers. An authoritative and detailed view of every asset in the environment - whether it's OT, IT, IoT, IoMT, virtual, or cloud is imperative to achieve non-stop security coverage and ensure that organizations are extensible and resilient against current and future threats.

Bottom line

The typical organization struggles to have a dynamic and accurate asset inventory database. When choosing a solution to protect the entire attack surface and manage cyber risk exposure, your organization must see all of managed, unmanaged, IoT, industrial and medical devices, applications, cloud and virtual instances.

On an average business day, 55,686 physical and virtual assets are connected to organizational networks. 40% of those are unmonitored.

60% of compromises are from known vulnerabilities

On average, it takes 160 hours per week to monitor and track threats

Attack attempts rose significantly in 2023, with an increase of 104%

Questions to ask

See Every Device and Connection

- How do you discover assets that connect to the network?
- Do you have a complete and up-to-date asset inventory across all asset types including managed and unmanaged assets?
- How much manual work is involved?
- What is your confidence level in the accuracy of the data?
- Can you customize your asset monitoring options with both an agent or agentless?
- Do you want to fix and enrich your configuration management database (CMDB)?
- Can you seamlessly integrate your asset inventory database with your existing IT and security tools, aggregating, deduplicating, and normalizing data for every asset in your environment?

Deep Situational Awareness and Asset Insights- Intelligence requires a combination of data sources

- Do you have a baseline of how typical assets in your deployment scenario should behave.
- Are you learning from others and utilizing an AI-driven asset behavior knowledgebase, tracking billions of assets?
- Can you cut through the noise by correlating data from across your IT, network, and security infrastructure?
- Are you using asset insights to classify assets and detect threats?
- Can you process network traffic and telemetry data from different integrations in real time?
- Do your API-based integrations deliver value in minutes?

Protect

Cyberattacks continue to increase in volume, complexity and sophistication. Concurrently, attack surfaces continue to increase in the form of more devices and assets, both physical and virtual, managed and unmanaged are proliferating across the organization.

Organizations must adopt proactive measures to detect threats and stop attacks.

Bottom line

Organizations need a next-gen approach to cyber exposure management to close the gap between finding and fixing risk. Focus on platforms that utilize early warning detection to prioritize threat actor behaviors and exploitation and can yield significantly improved MTTR. These functionalities are empowered with AI-driven functionality to identify, deduplicate, and prioritize threats. They utilize predictive, automated remediation tactics.

Questions to ask

- Are you in the dark about what vulnerabilities you should prioritize first?
- Are you going beyond vulnerabilities to also identify other security findings such as code errors, misconfigurations etc?
- Do you use a multi-detection engine that can identify anomalies as well as policy violations?
- Are you experiencing an increasing backlog of vulnerabilities and other security findings / alerts that you cannot get to?
- Are you experiencing an increase in MTTR metrics?
- Does CVSS scoring provide little guidance on the criticality of the vulnerability to your business operations?
- Are you able to identify and stop attacks before they hit your environment, while still in the formulation stage?
- Are you able to enrich SOC, SIEM and SOAR?
- Are you able to leverage predictive AI for remediation ownership?
- Are you eager to reduce your backlog with alert consolidation and ML deduplication?
- Are you using AI to deduplicate alarms, predictively assign them and employ advanced mitigation strategies?
- Do you wish to improve your integration into existing tools to establish end-to-end workflows (ticketing and incident response) and enforce security policies?
- Are you able to assess compliance against internal and external policies?
- Can you report on and prove risk education over time?

Manage

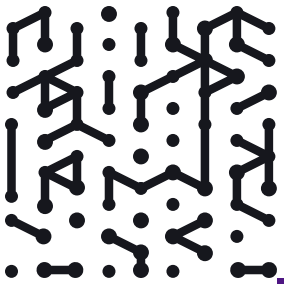
Organizations must demonstrate and report on real-time security, compliance, value and risk mitigation progress with an overall understanding of how teams and tools are performing.

Bottom line

There are hundreds of compliance standards and common security frameworks by organizations such as the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS). Implementing both is a common practice, yet identifying gaps and reporting progress can be difficult. Without clear dashboards and reliable reports on your security gaps and risks, it's like they never happened.

Questions to ask

- Do you know if a company laptop did not have an endpoint security agent installed?
- Do you know if an asset was not being scanned by a vulnerability scanner as scheduled, because it is hidden behind a firewall or in an unknown network segment?
- Can you identify aging operating systems and hardware?
- Can you navigate through different dashboards and reports and contextually drill down into specific data for analysis?
- Can you visualize the environment through interactive network infrastructure maps showing device information, logical connections, and risk levels?
- Can you customize goals, KPIs, policies and progress?
- Can you provide "trend over time" data to your executive teams?
- Do your dashboards support purpose-built natural language input?
- Do you know how your organization is performing in relation to its peers?
- How much time and resources would it take to demonstrate compliance to an auditor?
- How do you ensure that the policies you've enacted have yielded the results you were looking for?



Security Checklist - C-Level

See, Protect and Manage your Assets with a Cyber Exposure Management Platform

	Challenge	Cyber Exposure Platforms can help with
Full Asset Inventory and CMDB Enrichment	The average security organization has 76 security tools to manage and billions of assets to protect.	See, protect and manage all assets - managed, unmanaged, IoT, industrial and medical devices, applications, cloud and virtual instances.
Attack Surface Management and Security Posture	On an average business day, 55,686 physical and virtual assets are connected to organizational networks. 40% of those are unmonitored, completely challenging protection methods.	Quickly uncover and eliminate gaps, optimize your entire network security. Define policies to enforce security controls on your devices and ensure compliance with regulations and industry standards.
Security Hygiene and Gap Analysis	Organizational infrastructures today are very complex and consist of a huge number of assets of all types, networks and subnetworks, local and remote sites, and of a wide variety of security controls.	Enables quick and easy discovery of those security gaps and enables you to take suitable action to close them.
Compliance Reporting	Virtually every business is required to align with an alphabet soup of regulatory compliance and security frameworks and the process is grueling.	By integrating with your existing security and management systems, gain clarity and predictability, simplifying compliance efforts and reducing administrative burdens.
Network Segmentation and Enforcement	The most common approach for performing network segmentation today is via Network Access Control. Unfortunately, NAC systems can be complex to deploy and have poor visibility to all the devices on the network.	Gain a complete picture of all of the devices that are communicating on the network, enabling them to make more informed decisions about security policies for all devices including IT, OT, IoT and IoMT systems.

	Challenge	Cyber Exposure Platforms can help with
Threat Detection and Response	Armis Research Finds One-Third of Global Organizations Experienced Multiple Security Breaches in Last 12 Months. 40% of assets remain unmonitored and pose the biggest threat to organizations globally.	Easily identify and prioritize threats inside the network with deep analysis on 100% of assets of both north-south and east-west traffic.
Vulnerability Detection Coverage Gaps	Traditional scanners, EDRs, and cloud vendors can miss a lot of assets due to licensing, network topology, and device limitations.	Ingest data from existing sources, including asset management, EDR, on premise, cloud services, code, and applications. Leverage non-intrusive, integrations to detection tools, vulnerability scanners, developer tools, developer security platforms and more. Correlate all security findings and reduce the findings volume with ML deduplication.
Vulnerability Data Enrichment	DIY approaches, like manually downloading, correlating, and normalizing data from various platforms into Excel spreadsheets are not practical.	A comprehensive asset intelligence engine adds risk scores, business criticality, and threat intelligence feeds to provide a single pane of glass for organizational assets, their vulnerabilities, and their business impact.
Vulnerability Prioritization with Early Warning Detection	60% of compromises are from known vulnerabilities yet organizations are too burdened with the sheer amount of vulnerabilities to respond to.	98% reduction in the number of vulnerabilities organization's need to worry about.
Vulnerability Remediation	Vulnerability teams struggle with remediation due to manual efforts, limited contextual data shared with existing systems, and automated responses for action.	Focus on high-impact fixes that will resolve the largest number of security issues. Leverage AI-driven predictive capabilities to determine who is most likely responsible for the asset and the remediation. Manage a single, streamlined ticketing process for open findings with a common fix or associated with the same asset type.

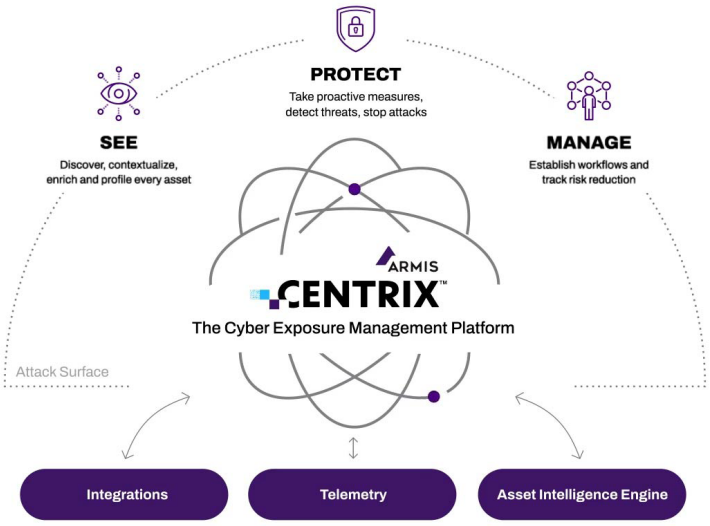
	Challenge	Cyber Exposure Platforms can help with
Track Progress and Process Management	With the sheer volume of vulnerable assets in their environment at any given moment, organizations need to streamline vulnerability management workflows and insights into more efficient processes.	Track and demonstrate progress for both individuals tasks, as for overall risk trends in the organization. Understand how your teams and the tools they are using are performing through a consolidated dashboard, and measure the effectiveness of the remediation process.
Benchmarking	Benchmarking delivers quantifiable metrics to track changes and improvements over time, and compare performance against your peers. Yet, It can be difficult to find relevant, reliable, accurate, timely, and consistent data.	Armis reports and dashboards are used for a wide variety of metrics and to demonstrate progress over time, for example when it comes to monitoring and reporting on obsolete software or hardware. The Benchmarking feature – leverages AI-powered insights from billions of assets tracked around the world in real time.
Assets covered (manual or automatic)	Requires coverage of all assets whether they are IT, OT, IoT or IoMT. Must be real-time and able to function in highly distributed and dynamic environments.	Eliminate blindspots with full coverage of all assets and deep situational awareness down to version #, backplane etc. Coverage included physical and virtual, managed and unmanaged.
Beyond Vulnerabilities	Vulnerability management teams now have responsibility for a much broader range of security issues - not just host vulnerabilities, but also cloud, code and AppSec findings.	Go beyond vulnerabilities: Armis helps obtain a unified and deduplicated view of all security findings.
Secure Remote Access	Attackers are leveraging AI to gain access to a remote user's credentials or devices, they may be able to access sensitive resources and systems.	Allow remote users to easily and securely connect to assets, applications, and services they need.
AI Adoption	80% of data experts agree that AI is making data security more challenging.	Armis Centrix™, the cyber exposure management platform, is powered by the Armis AI-driven Asset Intelligence Engine, to thwart AI-driven attacks.

	Challenge	Cyber Exposure Platforms can help with
Asset Profiling Against Data Lake	Asset inventories are not always updated in real time, causing outdated, unreliable information and the inability to utilize contextual intelligence.	Armis Centrix™ pulls asset-related data from your existing tools and data lake and our AI-driven Asset Intelligence Engine to provide contextual intelligence about each asset in the inventory.
Alignment of Frameworks	Security frameworks can help organizations better meet business outcomes, minimizing the risk of operational downtime. Yet, implementing security frameworks can be a cumbersome process for many.	The Armis Platform shields your operations from cyberattacks – helping you meet security standards and best practices along the way. Armis is integrated with the following security frameworks: NIST Cybersecurity Framework (CSF), Center for Internet Security (CIS) Controls, MITRE ATT&CK® for ICS, Zero Trust Security Model.
Programmatic Maintenance	Assurance that when maintenance windows are scheduled, the right maintenance in being performed in order of severity/priority.	Armis can play a key role in identifying both essential maintenance as well as prioritizing what maintenance is performed during scheduled maintenance windows.
Compensating Controls	Alternative security measures implemented to mitigate risks when primary controls are not feasible or effective. They provide a way to achieve security objectives and compliance requirements by addressing vulnerabilities and other security issues through different, often supplementary, mechanisms.	Armis helps organizations enforce compensating controls by providing comprehensive visibility, continuous monitoring, and risk assessment of all connected devices, including unmanaged and IoT devices. It integrates with existing security infrastructure to enhance policy enforcement, incident response, and regulatory compliance.
Alert Deduplication	Alert fatigue, resource constraints, limited budgets, personnel shortages, and competing priorities: how do you optimize the use of resources while minimizing exposure to the business?	Reduce Security Findings volume by 50-1 with ML deduplication.

	Challenge	Cyber Exposure Platforms can help with
Attack Path Analysis	Ability to track the path by which an attack has progressed across the organization.	Armis performs attack path detection by continuously monitoring the behavior of all connected devices as well as traffic flows; identifying anomalies, vulnerabilities, and potential threats in real time. It uses this data to map potential attack paths and provide actionable insights to prevent and mitigate security incidents.
Ingest/Push of Intel	The ability for the solution to pull in information from other tools as well as push information in the form of alerts, findings or insights to other tools.	Armis can ingest information as well as push intelligence and findings to and from the organization's existing security stack. The yields an "ecosystem of trust" where all investments collaborate to form the most robust and complete solution.
Integrations	With organizations using as many as 100 security tools, getting them to work well together is an ongoing battle.	Armis integrates easily with the tools you already have in your security ecosystem. Eliminate security siloes and blind spots. Leverage existing investments to achieve greater security, value and more automated response.

Introducing Armis Centrix™

Armis Centrix™, the cyber exposure management platform, is powered by the Armis AI-driven Asset Intelligence Engine, which sees, secures, protects and manages billions of assets around the world in real time. Our seamless, frictionless, cloud-based platform proactively mitigates all cyber asset risks, remediates vulnerabilities, blocks threats and protects your entire attack surface.



40 Fortune 100 companies trust our real-time, and continuous protection

+100,000

deployments worldwide in 165 countries

+500 Billion

security events handled daily by Armis Centrix™

ARMIS

Armis, the asset intelligence cybersecurity company, protects the entire attack surface and manages the organization's cyber risk exposure in real time.

In a rapidly evolving, perimeter-less world Armis ensures that organizations continuously see, secure, protect and manage all critical assets.

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 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