WHITE PAPER

5 ways Armis addresses NIS2

5 ways Armis addresses NIS2

The updated NIS2 directive has been designed to expand the scope of the original , while introducing new requirements to guarantee the availability and uptime of critical services a company or critical national infrastructure operator provides. The directive was passed into law on January 16th, 2023, with a 21-month readiness window and goes live in October 2024.

NIS enshrined cybersecurity responsibility into European law for a much broader group of industry sectors across the market. The original industries defined in NIS were classified as ‘essential’ and included Healthcare, Drinking Water, Finance etc. (See table 1.1)

NIS2 introduces a new and broader category, ‘important’ entities, which includes Postal and Courier Services and Food and Manufacturing, and covers a much broader set of industries. The law is designed to improve the operational and cyber resilience of organizations and reduce the impact of cyber-attacks, especially for services which the public and economy require to function.

Organizations subject to NIS2 will be obligated to *“take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services”.*

NIS2 Organizations that operate in these sectors are deemed “essential”	**NIS2 introduces a second category of “important” entities**
• Energy • Transport • Finance • Healthcare • Drinking Water • Wastewater • Digital Infrastructure • ICT Service Management • Public Administration • Space	• Postal & Courier Services • Waste Management • Chemicals • Food • Manufacturing • Digital Providers • Research Organisations

The difference between “essential” and “important” entities is mainly in the stringency of supervision and sanctions. Essential entities face tighter controls and sanctions than important entities. National authorities may also specifically designate entities as “essential” or “important,” for example, when an entity is the sole service provider in a sector or when a disruption in service provision could have significant consequences for public safety, public security, or public health.

Operational Blind Spots…Continued

Armis research on **Global Attack Surface Management** (ASM) shows there's still much room for improvement in how organizations protect and manage their risk and threat landscape. On an average business day, 55,686 physical and virtual assets are connected to an organizational network.. This rate of growth continues to accelerate each year, reflecting the ongoing expansion of digital connectivity in today's business landscape. Yet global respondents shared that only 60% of these assets are monitored, leaving 40% unmonitored and posing the biggest threat to organizations.

The difficult reality is many organizations still do not have visibility into their total asset base which underpins the critical services they will be measured against under NIS2. To be able to protect assets you need to be able to see where they are and understand the health or risk posture of the assets across your entire attack surface.

Most organizations have focused on building an inventory of asset classes, usually starting with IT assets. However, in many cases, specialized asset classes like Operational Technology (OT) which can be found across all industry sectors, in particular manufacturing and CNI (Critical National Infrastructure) are often not well inventoried, and the cyber risk posture of these assets can be high. They often include solutions which typically do not accept security agents or are traditionally out-of-scope for IT because they live in operational environments. This situation is further compounded by IoT devices which are exploding in scale across clients' environments, are often difficult to track, and are inherently insecure, making them easy targets for bad actors to exploit.

To compound the attack surface resilience challenges across IT, IoT, and OT, the increased regulatory oversight of end-to-end services now includes third-party providers and any cyber or operational risk they may introduce. This new oversight is expanding against a backdrop of sophisticated fraud, supply chain based cyber-attacks e.g. SolarWinds, and hostile nation state sponsored activity which has increased significantly since the start of the war in the Ukraine.

Outsourcing Cyber Services Does Not Outsource the Responsibility

NIS2 also carries more onerous penalties for Enterprises and Critical National Infrastructure providers when service failure occurs. The new penalty matrix also includes critical third-party service providers, should they be deemed responsible for the service or data loss, as defined by NIS2. Fines can reach 2% of global revenue or €10 million euros for 'Essential' entities, whereas "Important" entities in the new category face fines of 1.4% of global revenue or up to €7 million euros. It is estimated that cyber security budgets may need to increase by 22% for the new "important" entity category to put the required controls and protection in place, whereas even the existing "important" entities are looking at an increase of 12% to build in the required visibility and resilience they will require. Some international companies with headquarters outside of the European Union but who have significant European operations will also be subject to NIS2 compliance and penalties, hence the recognition of this new regulation as a global imperative.

Too Many Tools, Too Many Data Points

Many enterprise CMDB (Configuration Management Database) asset data sources are fragmented and rely on 'point in time' scans from different sources to determine a view on IT assets primarily, making it difficult to understand and track all relevant assets associated or linked with a critical service. The concept of an entire IT, IoT, and OT asset inventory being captured within the CMDB is a relatively new idea but it is gaining pace as it is a business imperative to have a single system of record from which remediation and business workflows can be orchestrated, field service operations can be maintained, and third party dependencies can be tracked and monitored.

Consequently, many enterprises are now exploring asset discovery or mapping tools. Unfortunately, in many cases these tools do not detect all the potential assets across their environment, leaving enterprises to resort to manual methods of inventory data collection via spreadsheet applications. Some asset mapping tools also require active scanning which needs to be scheduled within a particular network segment and can be potentially disruptive to 'live' systems and so are often unsuitable for sensitive Healthcare Devices, Operational Technology on a production line, or CNI. Consequently, it is difficult to achieve an 'aggregated view' of underlying asset inventory and any real-time vulnerabilities or attack scenarios that could impact critical services.

In many organizations the internal risk and security, network, and operational or manufacturing teams often don't have access to the same data sources. Sometimes they have disconnected goals. Auditable reporting and root cause analysis of service disruption or health can therefore be constrained by the need to query multiple data sources and pulling in different teams to provide a complete picture of the service composition and where the issues requiring remediation occurred. In simple terms, a security team may detect an issue on the factory floor but not have the processes or know the people to get the issue fixed before it potentially impacts 'uptime' or worse. The more complex the organization and geographic distribution, the more complex this challenge can become. This new challenge is characterized as the IT/OT convergence and solving it requires a complete view across the 'attack surface'. Many organizations are now seeking solutions which enable this next level of visibility.

5 ways Armis addresses NIS2

NIS2 - Article 21	Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems and shall include at least the following: a) policies on risk analysis and information system security b) incident handling

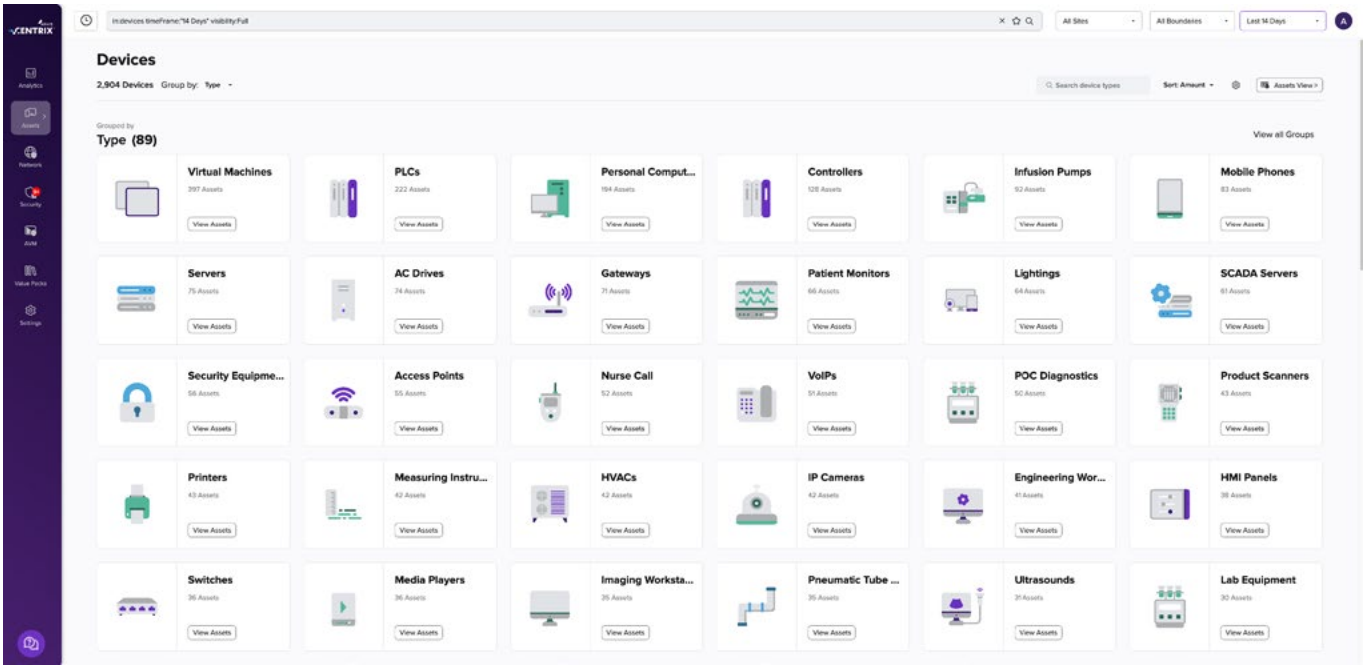
1 Risk Management with Full Asset Visibility

Armis is the first step in enabling a defensible cyber maturity with regards to asset management specified in Article 21.

Armis Centrix™ provides a single source of truth, so you have 100% visibility into every asset in your environment, including hardware, software, operating systems, applications, physical location, users, and more. That's IT, OT, IIOT, IoT, IoMT, virtual, and cloud—managed and unmanaged, and more. With the Armis policy wizard, you can quickly and easily create automated, policy-based actions for virtually any situation. Trigger vulnerability scans on new devices, create CMDB entries for new devices, file trouble tickets, so much more.

2 Incident handling: optimize your organization's incident response management plan.

Armis also cuts through the noise by correlating data from across your IT, network, and security infrastructure, giving you the ability to manage and protect your entire estate and optimize your organization's incident response management plan. It can quickly alert security teams to anomalous device behavior that can indicate an attack. After incident response, security teams can access the platform's logs for review and forensics.

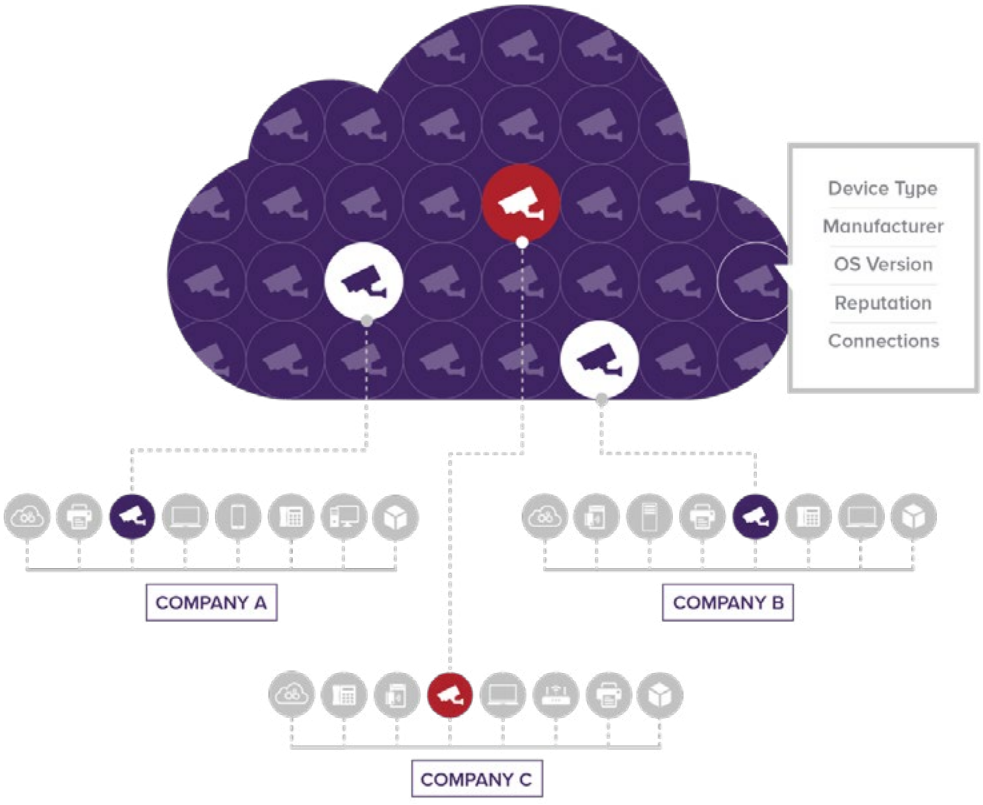


NIS2-Preamble 51	Member States should encourage the use of any innovative technology, including artificial intelligence, the use of which could improve the detection and prevention of cyberattacks, enabling resources to be diverted towards cyberattacks more effectively.

3 Classify assets and detect threats with a high degree of accuracy

At the core of Armis Centrix™ is our AI-powered Asset Intelligence Engine, a giant, crowd-sourced, cloud-based asset behavior knowledgebase—the largest in the world, tracking over 4 billion assets. With our Asset Intelligence Engine, Armis understands not only what the asset is and what it is doing, but what it should be doing. This is because we contextualize each asset in its use in each environment. These asset insights enable Armis to classify assets and detect threats with a high degree of accuracy.

With Armis Centrix™ for Actionable Threat Intelligence, organizations benefit from an early warning system that alerts them proactively - before a vulnerability is announced and before an attack is ever launched. Actionable Threat Intelligence uses AI technology that leverages dark web, dynamic honeypots and human intelligence to stop attacks before they impact your organization.

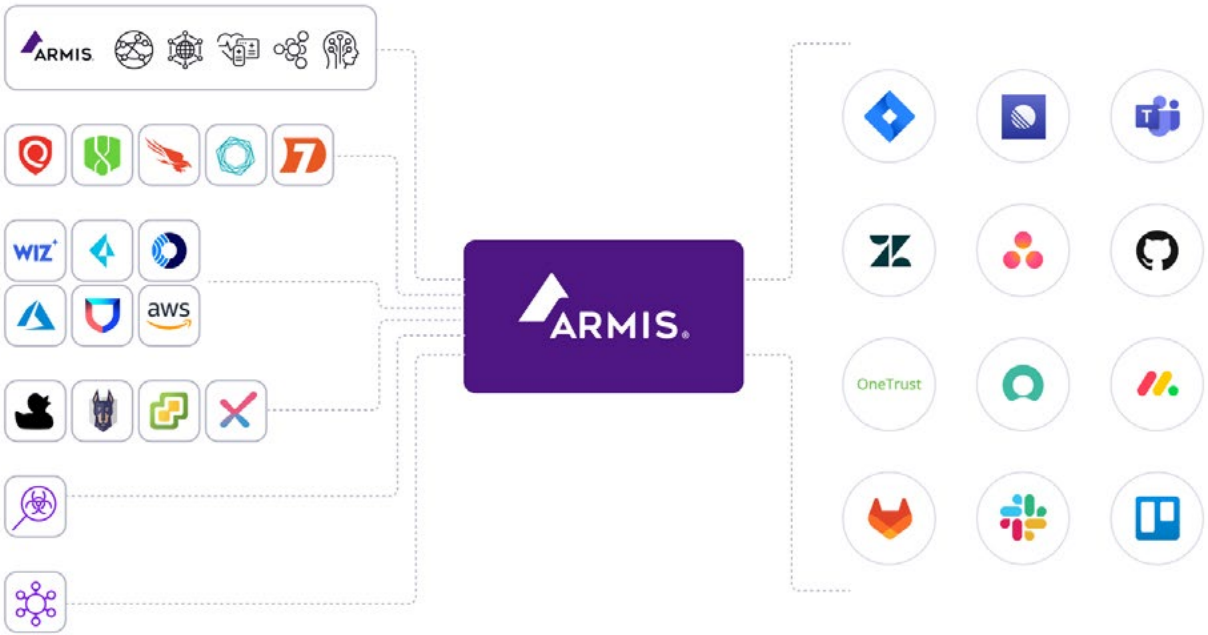


NIS2-Preamble 58	Since the exploitation of vulnerabilities in network and information systems may cause significant disruption and harm, swiftly identifying and remedying such vulnerabilities is an important factor in reducing risk.

4 Focus on high-risk vulnerabilities, prioritizing response, identifying the owner, and operationalizing the remediation lifecycle

Armis Centrix™ for VIPR Pro - Prioritization and Remediation consolidates detection tool findings and deduplicates alerts, extending from on-premise hosts and endpoints to code, cloud services, application security tools, and unconventional assets like medical devices, IoT and OT.

Our technology assigns context to findings, including threat intelligence, likelihood of exploit, and asset attributes like business impact and compliance policies. To facilitate resolution tasks, Armis generates predictive ownership rules through AI to assign fix responsibilities and enables ongoing communication for distributed teams through bidirectional integration with their preferred workflow or ticketing system. Organizations using Armis have seen their mean time to resolution (MTTR) improved by as much as 90%.

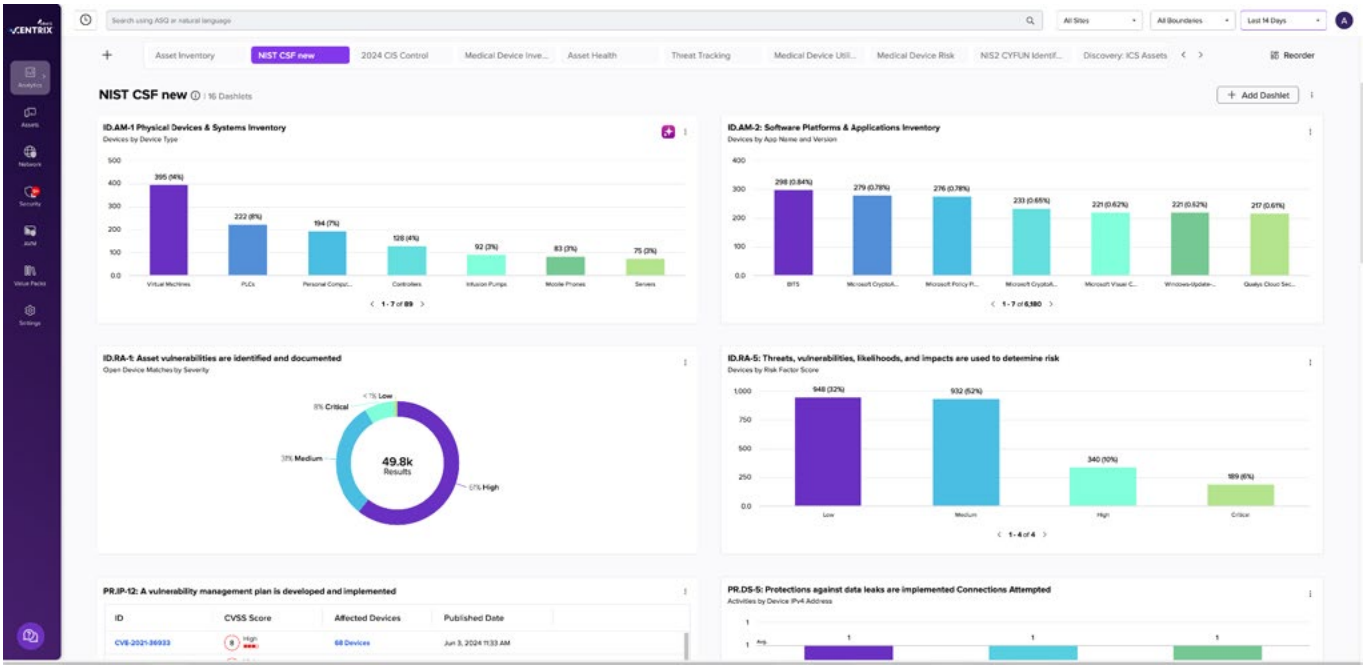


NIS2-Preamble 59	The Commission, ENISA and the Member States should continue to foster alignments with international standards and existing industry best practices in the area of cybersecurity risk management, for example in the areas of supply chain security assessments, information sharing and vulnerability disclosure.

5 Simplified Security Framework And Regulatory Compliance

Frameworks like the CIS Controls and NIST Cyber Security Framework (CSF) are standard security blueprints for most organizations. Armis provides compliance for CIS Controls as well as the NIST CSF controls across the Identify, Protect, Detect, and Respond categories for managed, unmanaged, IoT, ICS, medical devices and more.

Unlike visibility tools that simply tell you a device's IP and MAC addresses, Armis Centrix™ gives you in-depth information about each device. This visibility is important for compliance and reporting cases, such as ensuring that each device is on the most appropriate network segment. It is also useful for asset management situations, such as when trying to determine if your company has any "banned" devices from manufacturers, like Hikvision, Huawei, Dahua, or ZTE—and if so, where.



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