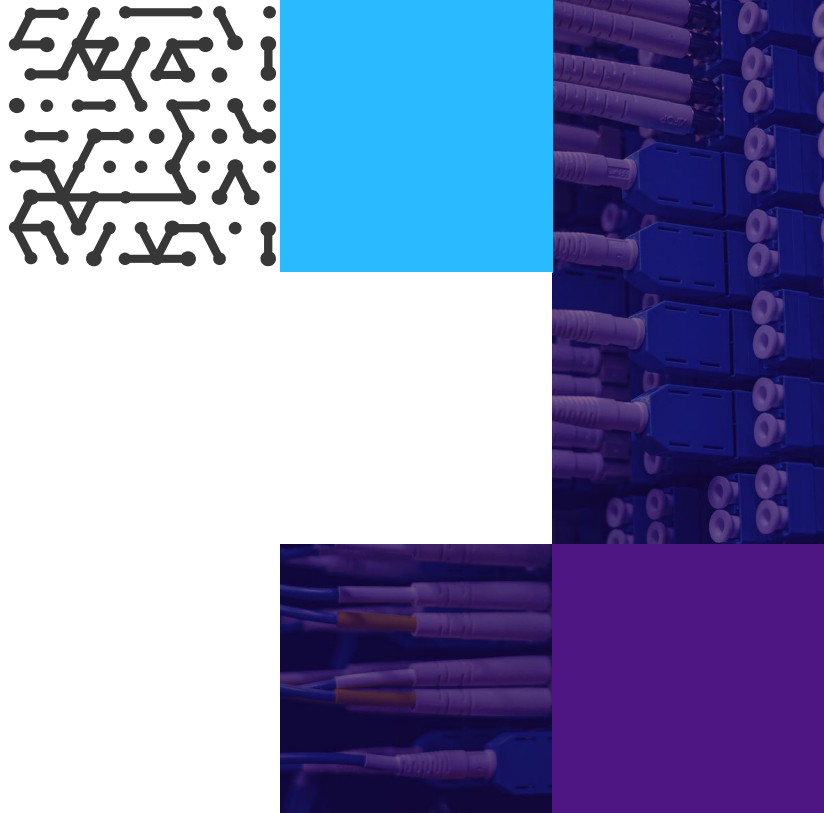


SOLUTION BRIEF

Alignment to NIST Cyber Security Framework

For Unmanaged and IoT Devices



Identify, Protect, Detect, Respond, and Recover.

The National Institute of Standards and Technology (NIST) publishes a set of security guidelines called the “Cybersecurity Framework”, or CSF for short. It consists of five major functions: Identify, Protect, Detect, Respond, and Recover. These functions are divided into a total of 22 categories, which in turn are divided into a total of 98 subcategories, each defining an increasingly granular set of desired outcomes.

Many of the CSF functions can be implemented with fairly common asset discovery, management and security tools that have been developed and marketed over the past ten or fifteen years. However, in most cases, these tools assume that you can place an agent on the endpoint that you are trying to discover, manage and secure.

How can you implement all of the NIST CSF functions when you can't put an agent on the endpoint?

This is a very serious question because as the number of unmanaged things on enterprise networks increases, enterprise security managers need to ensure that their security controls encompass those devices just as much as traditional computers.

Many security products fail to do this, giving rise to the ‘shadow IT’ phenomenon. Although IT departments are aware of the security risks of Shadow IT to their organizations, most employees are not. [More than one-third](#) (37 percent) of the IT employees say their organization does not have clearly outlined internal consequences for when employees bring on new technologies without IT approval.

Armis is an agentless solution that has been specifically designed to help you implement many of the security controls listed in the NIST CSF framework for both managed and unmanaged devices, including OT, IoT, IoMT, virtual and cloud assets.

The information below explains how Armis helps you implement cyber security controls as outlined in the NIST Cybersecurity Framework for all of your endpoints—managed, unmanaged, and IoT.

Identify

Category	Subcategory	Armis
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization’s risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried.	Through passive listening techniques, Armis discovers all devices on your enterprise network as well as devices that are in proximity to your network. A passive listening approach has several benefits compared to agent-based or network scanning approaches: 1) It is more comprehensive; 2) it is more real-time; 3) it does not require configuration or maintenance; 4) it can not disrupt endpoint devices. The information that Armis generates includes device type, manufacturer, model, MAC address, IP address, operating system, applications, connections, and risk score.
	ID.AM-2: Software platforms and applications within the organization are inventoried.	Without using agents, Armis discovers software that is running on all devices in your enterprise. The fact that Armis does not use agents allows Armis to discover software running not just on managed computers but also BYOD devices and the increasingly large number of connected “things” that are on enterprise networks—video cameras, thermostats, medical devices, industrial devices, etc.
	ID.AM-3: Organizational communication and data flows are mapped.	Armis automatically maps communication and data flows between all of the devices in the organization’s network. Armis baseline deviation capabilities will also alert on changes in these data flows.
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	ID.RA-1: Asset vulnerabilities are identified and documented.	Armis Centrix™ constantly monitors all devices on the enterprise network and identifies the vulnerabilities that are present in each device. Armis does this without any need for an agent on the endpoint; this allows Armis to detect software vulnerabilities on just about everything—managed computers, BYOD devices, and the increasingly large number of connected “things” on enterprise networks.
	ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.	Armis receives various sources of threat intelligence. This is used by the Armis cloud-based risk analysis engine to produce a unique risk score for every device in our customer environments, and to detect live threats and attacks.

Category	Subcategory	Armis
	ID.RA-3: Threats, both internal and external, are identified and documented.	Armis Centrix™ continuously monitors the behavior of every device in the enterprise environment and compares that behavior to various baselines. When a behavioral anomaly is detected, this is almost always an indication that the device has been compromised by a threat actor.
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	The Armis cloud-based risk analysis engine generates a unique risk score for every device in every customer environment. The score is based on multiple risk factors including historical risks associated with the device, current behavior of the device as compared with known “good” behavioral baselines, and known software vulnerabilities.
	ID.RA-6: Risk responses are identified and prioritized.	This risk score that Armis generates for each device helps enterprise security teams prioritize their actions to reduce the enterprise attack surface.

Protect

Category	Subcategory	Armis
Data Security (PR.DS): Information and records (data) are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.	PR.DS-5: Protections against data leaks are implemented.	Armis continuously monitors all connections in your environment and will alert you if a device’s connections are consistent with a data leak. For example: connections to unauthorized networks; connections to known malicious domains; anomalous quantities of data; anomalous times of data transmission.

Category	Subcategory	Armis
<p>Information Protection Processes and Procedures (PR.IP): Security policies that address purpose, scope, roles, responsibilities, processes, and procedures are maintained and used to manage the protection of information systems and assets.</p>	<p>PR.IP-12: A vulnerability management plan is developed and implemented.</p>	<p>Armis recognizes and alerts on vulnerabilities to managed and unmanaged endpoints based on known vulnerabilities issued in the CVE list.</p> <p>Armis Centrix™ for Vulnerability Prioritization and Remediation adds rich capabilities to consolidate, prioritize and remediate all vulnerabilities based on potential risk to the business.</p>
<p>Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.</p>	<p>PR.PT-4: Communications and control networks are protected.</p>	<p>Armis passively monitors device communications and associates active ports, services, and protocols to the hardware assets in the asset inventory. The Armis policy engine can be configured to alert or remediate (e.g. quarantine) whenever Armis observes a device utilizing unauthorized ports, protocols or services.</p>

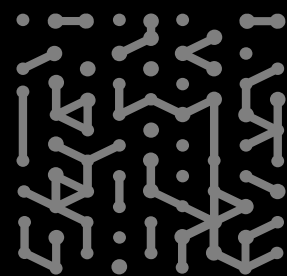
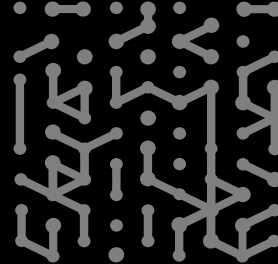
Detect

Category	Subcategory	Armis
<p>Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.</p>	<p>DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed.</p>	<p>Armis AI-driven Asset Intelligence Engine contains 3 billion distinct device baselines of normal device behavior. These baselines are gleaned from multiple sources including Armis research, device manufacturers, and Armis enterprise customer environments.</p>
	<p>DE.AE-3: Event data are collected and correlated from multiple sources and sensors.</p>	<p>The Armis virtual appliance passively and continuously monitors the behavior of every device on our customers' networks. Armis compares every device's real-time activity to the established and "known-good" activity baseline for the specific device which is stored in our Asset Intelligence Engine. When abnormal behavior in your network is detected, Armis updates the risk score and generates a security alert.</p>

Category	Subcategory	Armis
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	DE.CM-1: The network is monitored to detect potential cybersecurity events.	Armis passively monitors network communications and alerts whenever Armis observes a device utilizing unauthorized ports, protocols or services or whenever anomalous traffic is observed.
	DE.CM-8: Vulnerability scans are performed.	Armis uses passive monitoring, not active network scans, to detect vulnerabilities. Passive monitoring is easier and more comprehensive than active scans, and passive monitoring is less disruptive to devices that are on the network.
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	DE.DP-4: Event detection information is communicated.	When Armis detects abnormal behavior, it alerts your security team, and depending on your policies, can initiate an automated response. Armis also communicates event detection to existing SIEM systems and other management systems.

Respond

Category	Subcategory	Armis
Mitigation (RS.MI): Activities are performed to prevent the expansion of an event, mitigate its effects, and resolve the incident.	RS.MI-1: Incidents are contained	Through integration with your switches and wireless LAN controllers, as well as your existing security enforcement points like Cisco and Palo Alto Networks firewalls and/or network access control (NAC) products, Armis can restrict access of malicious devices immediately when they attack your network.



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