ARMIS®

SOLUTION BRIEF

Alignment With The CIS Critical Security Controls

How Armis Centrix™ can help

The Critical Security Controls published by the Center for Internet Security (the "CIS Controls") are considered the defacto cyberdefense guidelines by virtually every security professional.

These guidelines map to popular compliance frameworks, including the NIST Cybersecurity Framework, NIST 800-53, and ISO 27000. They help organizations comply with regulations like PCI DSS, HIPAA, NERC CIP, and FISMA. And they are endorsed by respected authorities, including the U.S. Government and the European Telecommunications Standards Institute (ETSI).

This guide explains how Armis Centrix™ can help your organization align with 12 of the 18 CIS Controls requirements.

CTRL 01 Inventory and Control of Enterprise Assets

CTRL 02 Inventory and Control of Software Assets

CTRL 03 Data Protection

CTRL 04 Secure Configuration of Enterprise Assets and Software

CTRL 05 Account Management

CTRL 06 Access Control Management

CTRL 07 Continuous Vulnerability Management

CTRL 08 Audit Log Management

CTRL 09 Email and Web Browser Protections

CTRL 10 Malware Defenses

CTRL 11 Data Recovery

CTRL 12 Network Infrastructure Management

CTRL 13 Network Monitoring and Defense

CTRL 14 Security Awareness and Skills Training

CTRL 15 Service Provider Management

CTRL 16 Applications Software Security

CTRL 17 Incident Response Management

CTRL 18 Penetration Testing

Armis AI-Driven Asset Intelligence Engine

Core to Armis Centrix™ is our Asset Intelligence Engine. It is a giant, crowd-sourced, cloud-based asset behavior knowledgebase—the largest in the world, tracking over three billion assets—and growing.

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. And, we record and keep a history of everything each asset does.

These asset 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 we have seen in other environments. When an asset operates outside of its baseline, Armis issues an alert or can automatically disconnect or quarantine an asset.

Our Asset Intelligence Engine tracks all managed, unmanaged, and IoT assets Armis has seen across all our customers.

Armis at-a-glance

Asset discovery

- Automatic identification of all devices
- Make, Model, OS, IP, etc.
- Anomalous Behaviour
- Connection and activity history
- Device location
- Integrate with asset inventory systems (CMMS, CMDB)

Risk management

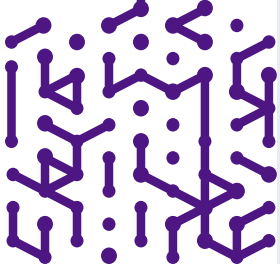
- Passive, real-time, continuous risk assessment
- Risk score with context
- Extensive CVE and compliance intelligence
- Smart adaptive risk scoring
- Risk-based policies

Threat detection

- Device attribution of activities
- Detect changes in device state
- Anomalies based on Anomalous Behaviour
- Automation of response
- Device context into every SOC tool and work flow (Splunk, Ticketing, FW, NAC)

Prevention

- Automatically quarantine devices
- Integrates with firewall, NAC, SIEM
- Reduce malware dwell time
- Improved device incident response



Control 1: Inventory and Control of Enterprise Assets

Armis Centrix™ uses passive listening techniques to discover devices on your network and radio frequency analysis to discover off-network devices in your environment. This agentless discovery covers primarily connected devices (those with an IP address) and peripherally connected devices (those connected to an attached device using protocols like Bluetooth, NRF, Zigbee, etc.). The result is a complete inventory of devices, right down to make, model, MAC address, IP address, and operating system.

Control 2: Inventory and Control of Software Assets

Armis Centrix™ uses passive network monitoring to discover software running on devices in your environment. This discovery includes software running on managed computers, BYOD devices, and the increasingly large number of connected “things” like video cameras, thermostats, interactive voice assistants, medical devices, industrial controls, and more.

Control 3: Data Protection

Armis Centrix™ continuously monitors data transfer between all endpoints and devices, regardless of whether the data traverses the network laterally or exits the network via the Internet. It then compares data movements with expected/normal data movements. Then the platform flags anomalies as either potential privacy violations or exfiltration attempts.

Furthermore, Armis can identify certain data types (such as a social security number) transmitted unencrypted. An example violation that Armis can detect is a medical device transmitting Protected Health Information (PHI) unencrypted, which can be a HIPAA violation.

Control 4: Secure Configurations of Enterprise Assets and Software

Armis Centrix™ can integrate with your existing IT security and management systems to obtain configuration information for managed devices. You can then build policies in the Armis platform based on this information. For example, when the platform identifies outdated software running on a managed computer (relative to the prescribed configuration), or identifies disabled security agents, it can generate an alert or take other remediation action such as blocking the device from the network, or triggering a third-party system to take some other action.

Control 5: Account Management

Armis user data allows tracking of account usage on devices and the network. This tracking quickly identifies lateral usage or overused service accounts.

Control 6: Access Control Management

Armis user and device information, together with integrations into other security and network solutions, enable access control audits. These integrations also allow for the enforcement or quarantine of devices not following company policies.

Control 7: Continuous Vulnerability Management

When a device is first detected, Armis Centrix™ uses information from the Armis Asset Intelligence Engine to identify its known hardware and software vulnerabilities. The platform then performs continuous vulnerability assessments based on a device's activities and behavior.

Device characteristics, vulnerabilities, and behaviors contribute to the risk score Armis Centrix™ maintains for every device. When Armis detects new hardware or software characteristics, vulnerabilities, or abnormal behavior like known attack patterns, it updates the device risk score. Depending on customer-defined risk thresholds and policies, the platform can trigger alerts and actions that mitigate and help manage risk.

Control 8: Audit Log Management

Armis passively monitors the activity of every device on your network and creates logs for each device. Armis stores these logs, analyzes them for signs of attack, and optionally transmits the logs to other storage or analytics systems you may have, such as a SIEM. Enterprises using Splunk and Exabeam can rely on Armis as the primary source of event data about unmanaged devices.

Control 10: Malware Defenses

Traditional anti-malware defenses can not protect IoT devices because they use signature-based detections rather than behavioral analysis. When Armis Centrix™ detects a device, the platform's cloud-based threat detection engine starts identifying abnormal behavior that could indicate unusual software (e.g., malware or ransomware) running on a device.

Control 12: Network Infrastructure Management

Armis Centrix™ provides several capabilities in this area:

Provide a complete inventory of all authorized and unauthorized (rogue) wireless access points in your enterprise airspace.

Monitor all wired and wireless connections in your airspace and detect unintended network bridges and open (unsecured) hotspots frequently found in modern printers.

Monitors Wi-Fi (802.11) and ten other wireless protocols like Bluetooth, NRF, Zigbee, Z-Wave, etc.

Provide traffic analysis to understand traffic load and bandwidth utilization for wired and wireless access points. This analysis helps to identify network issues (e.g., high retransmits) or overloading of a location.

Control 13: Network Monitoring and Defense

Armis Centrix™ continuously monitors data transfer between all endpoints and devices, regardless of whether the data traverses the network laterally or exits the network via the Internet. It then compares data movements with expected/normal data movements. Then Armis flags anomalies as either potential privacy violations or exfiltration attempts.

Furthermore, Armis can identify certain data types (such as a social security number) transmitted unencrypted. An example violation that Armis can detect is a medical device transmitting Protected Health Information (PHI) unencrypted, which can be a HIPAA violation.

Control 17: Incident Response Management

Armis Managed Threat Services streamlines the journey from discovery and identification to effective incident response and risk management capabilities for devices and assets.

The Armis Difference

- Comprehensive: Discovers and classifies all devices in your environment, on or off your network.
- Agentless: Nothing to install on devices, no configuration, no device disruption.
- Passive: No impact on your organization's network. No device scanning.
- Frictionless: Installs in minutes using the infrastructure you already have.

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