Securing Education with Armis Centrix™

Armis empowers higher and further education institutions with the foundations to align with the five technical controls set out in the Cyber Essentials and Cyber Essentials Plus framework by delivering complete Asset Exposure Management.

Quickly Protect and Manage Explosive Growth of Connected Campus Assets

FEIs and HEIs nationwide are working overtime to manage the explosive growth of connected campus assets. With continued migration to the cloud, the move to BYOD, attacks like Log4j and regulatory compliance requirements, assets increasingly need interconnectivity to remain functional. Using Armis Centrix™, IT leaders and administrators can establish and maintain authoritative, accurate and real-time information about all their interconnected assets.

Passive, Agentless Platform Designed To Address Expanding Attack Surface

Powered by our AI-driven Asset Intelligence Engine, Armis helps you prioritise your attack surface. Through telemetry data and deep packet inspection, smart active querying, integrations with your existing solutions and collective intelligence gathered from our extensive multi billion asset engine, you can now:

See
Discover, contextualise, enrich and profile every asset

Protect
Take measures and prioritise efforts against all exposures

Manage
Establish workflows and track risk reduction

Supercharge your Education Infrastructure with Armis:

Complete Asset Visibility in Education Environments

Armis Centrix™ uses a holistic asset discovery approach to gather deep knowledge and context of all assets without risk to uptime. Creating complete visibility with insights to reduce risk exposure and empower intelligent actions to mitigate risk is absolutely essential in Education environments.

Asset Management and Security

Utilising a whole-of-state approach with an agentless, cost effective platform gives education institutions of all sizes shared insights, leading to reduced tech debt and more efficient services for their students, staff, and researchers.

Vulnerability Prioritisation and Remediation, Leverage Early Warning Detection

For education, focus on finding risk, prioritising response, identifying the owner, and operationalising the remediation lifecycle. Empower the prioritisation step - leveraging early warning detection and threat intelligence to address the vulnerabilities that are actually being exploited by threat actors.

OT/IoT/BMS on Campus

IoT technologies have changed how we teach and consume information, and many college and university IT environments are no longer separate from their OT environments such as identity access cards and building controls. Reducing visibility gaps prevents compromised assets from acting as launching-off points for hackers to infiltrate portions of the network that house sensitive student, facility, and research data.

Medical Device Security

Whether your university focuses on health sciences research, education, patient care or all the above, the need to see, protect, and manage medical and research devices along with laboratory, patient, and financial data is essential.

See, protect, and manage your attack surface with Armis for Education

Visit **Armis.com** to find out more

Empowering FEIs and HEIs to Align to the Cyber Essentials Framework

NCSC has stated that "Asset management and Cyber Essentials Asset management isn't a specific Cyber Essentials control, but effective asset management can help meet all five controls, so it should be considered as a core security function".

Control One - Firewall

Armis tracks asset network connectivity and displays traffic information, making it easier to identify open firewall ports allowing internet communication into your environment.

Control Two - Secure Configuration

Armis helps discover installed applications and flags risky or vulnerable applications, calculating a risk score for each asset.

Control Three - Security Update Management

Armis identifies components, including applications and operating systems, that have reached or are nearing End of Life (EOL) or End of Support (EOS), highlighting those that cannot be patched and may need replacement or isolation.

Control Four - User Access Control

Armis fetches user account information from connected data sources, providing a unified view of user accounts and tracking users across devices to identify potential compromises or unusual behaviour.

Control Five - Malware Protection

Armis uses AI-based behavioural analytics and rule-based matching to detect network-based threats, identifying both known and unknown threats, including signature-based attacks and behavioural patterns like brute force attempts and port scans.

> *"When it comes to whether somebody gets into our network or not, we have to be right 100% of the time, and the intruder only has to be right once. Armis has helped us tremendously with identifying devices that may be out of date for software or patches."*

Jamie Pownall CIO, Henry County

Key features that make Armis the go-to platform for total exposure management

Achieve cyber resilience with an agentless, cost effective platform.

Full asset inventory and CMDB enrichment, providing complete asset visibility across all asset types, including IT, IoT, OT, IoMT, and cloud, whether managed or unmanaged.

Create an up-to-date inventory of which applications are deployed on which assets.

Create policies and queries that highlight boundary violations, then automate your segmentation processes with intelligent recommendations.

Adhere to regulatory compliance guidelines, including Cyber Essentials, Cyber Essentials Plus and NIS

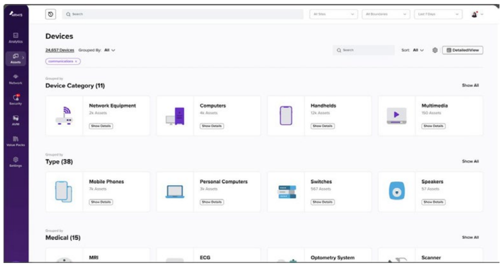
Identify any abnormal or risky activity with network baseline rules.

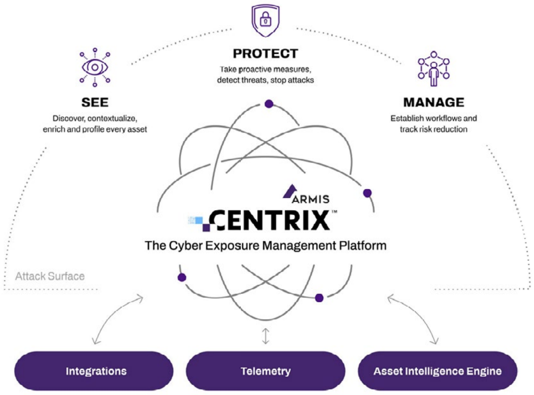
Minimise the Risk posed by unmanageable student devices connected to the network.

Monitor connectivity and track asset behaviour. Create a real-time network baseline.

Smart Active Querying to safely deep dive into asset visibility through smart querying.

Actionable Threat Intelligence including early warning detection to act on a vulnerability before it is published.




PROTECT
Take proactive measures, detect threats, stop attacks
SEE
Discover, contextualize, enrich and profile every asset
MANAGE
Establish workflows and track risk reduction
ARMIS
CENTRIX™
The Cyber Exposure Management Platform
Attack Surface
Integrations
Telemetry
Asset Intelligence Engine

See, protect, and manage your attack surface with Armis for Education

Visit **Armis.com** to find out more