

SOLUTION BRIEF

Maintaining Compliance with Cyber Insurance Requirements Using Armis Centrix™

Introduction

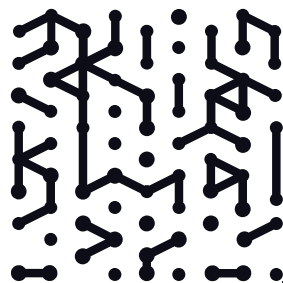
In cybersecurity, the only constant is change. As cyber threats grow in sophistication and frequency, organizations must adopt robust security measures to protect their assets and maintain compliance with industry standards and regulatory requirements. One critical aspect of this compliance is meeting the stringent requirements of cyber insurance policies, which have become increasingly complex and demanding.

The Role of Cyber Insurance in Enterprise Security

Cyber insurance serves as a risk transference strategy for enterprises, protecting them against financial losses resulting from cyber incidents. However, the rising threat of ransomware and other cyber attacks has made obtaining and maintaining cyber insurance coverage more challenging. According to a 2023 study by S&P Global Market Intelligence, 53% of cyber insurance policyholders report that it is more difficult to meet policy requirements than it was 12 months ago.

As premiums rise and coverage requirements become more stringent, enterprises must invest in effective security technologies to meet these demands and control premium costs.

This is where Armis Centrix™ comes into play.



Key Benefits of Using Armis Centrix™ for Cyber Insurance Compliance

1. Reduction in Cyber Insurance Costs

Armis Centrix™ helps organizations implement insurer-recommended security technologies, which can significantly reduce cyber insurance premiums. By providing more comprehensive answers to insurance questionnaires and leveraging security telemetry directly from the Armis Centrix™ platform, organizations can demonstrate a robust security posture, reducing the risk perceived by insurers.

2. Staying in Compliance with Cyber Insurance Requirements

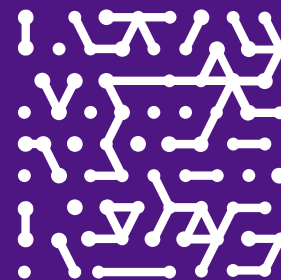
Armis Centrix™ ensures continuous compliance with cyber insurance requirements by automating critical security functions and providing real-time visibility into the security posture of the enterprise. The platform supports the Center for Internet Security (CIS) Critical Security Controls, helping organizations identify and mitigate vulnerabilities before they can be exploited.

3. Peace of Mind and Asset Protection

Armis Centrix™ provides IT professionals with peace of mind by continuously monitoring network traffic and device behavior for unusual activity. Automated alerts and regular monthly implementation calls with the Armis Centrix™ team ensure that potential threats are addressed promptly, safeguarding the organization's intellectual property and sensitive data.

4. Dashboards and Reporting

Armis Centrix™ lets you quickly configure and report on company-specific policies and external security frameworks, including cyber insurance requirements, CIS Critical Security Controls, DORA, MITRE ATT&CK for ICS, NIS2, NIST, SOCI, and Zero Trust. Ready-to-run value packs contain out-of-the-box policies, dashboards, and reports to streamline your business workflows and benefit from deployment best practices specific to your industry or requirement.



Case Study: Armis Centrix™ in Action

A food manufacturer experienced significant benefits from implementing Armis Centrix™, including cost savings, peace of mind, and enhanced data protection. The Director of IT at the company highlighted several key advantages:

Automated Alerts:

Ability to automate alerts across the IT team reduced the need to chase “noise” and allowed the team to focus on strategic initiatives.

Peace of Mind:

Regular monthly implementation calls with the Armis team provided assurance that malware and other threats were being effectively managed.

Reduction in Cyber Insurance Costs:

The Director of IT was able to check “yes” for many items on the cyber insurance questionnaire that were previously unchecked, leading to premium reductions.

Data Protection:

Armis Centrix™ flagged unusual data movement on the network and created alerts for unencrypted critical data, ensuring the protection of the company’s intellectual property.

Compliance Reporting:

Complete asset visibility and contextual intelligence, value packs for dashboards and reporting, natural language processing and the ability to implement security frameworks, quickly and easily transforms data into actionable insights required for cyber insurance audits.



Strategies for Maintaining Cyber Insurance Compliance with Armis Centrix™

1. Implementing Insurer-Recommended Security Technologies

Armis Centrix™ supports the implementation of specific security tools required by cyber insurance policies. By leveraging the platform's advanced capabilities, organizations can meet these requirements and demonstrate a proactive approach to cybersecurity.

2. Leveraging Security Telemetry

Armis Centrix™ provides direct security telemetry, which can be shared with insurance providers to show compliance with policy requirements. This reduces the burden on IT teams and ensures accurate reporting of the organization's security posture.

3. Continuous Monitoring and Alerting

Armis Centrix™ offers continuous monitoring of network traffic and device behavior, providing real-time alerts for suspicious activity. This proactive approach helps organizations stay ahead of potential threats and maintain compliance with cyber insurance requirements.

4. Regular Implementation Reviews

Regular monthly implementation calls with the Armis team ensure that the organization's security measures are up to date and aligned with the latest industry standards and insurance requirements. This ongoing support provides IT professionals with the confidence that their security posture is robust and compliant.

8 Cyber Insurance Requirements (And How to Meet Them to Lower Premiums)

Insurers can reduce cyber insurance premiums when they see evidence that a business is effectively managing cyber risk. Here are some cybersecurity practices that can help:

Cyber insurance requirements:

How Armis can help:

1 Strong Security Controls

Armis sees, protects and manages all physical and virtual assets - from the ground to the cloud - ensuring the entire attack surface is both defended and managed in real time.

2 Cyber Hygiene

With intuitive interface and advanced analytics, Armis Centrix™ empowers organizations to efficiently gain deep situational awareness, track and manage their assets across diverse environments, ensuring optimal utilization and cost-effectiveness.

3 Incident Response Plan

Armis Centrix™ is a seamless, frictionless, cloud-based platform that proactively identifies and mitigates all cyber asset risks, remediates security findings and vulnerabilities, and protects your entire attack surface.

4 Network Security

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 medical, IoT, IT and OT systems.

5 Regular Vulnerability Assessments

Armis Centrix™ for Vulnerability Prioritization and Remediation focuses on finding risk, prioritizing response, identifying the owner, and operationalizing the remediation lifecycle. Armis Centrix™ for Actionable Threat Intelligence will empower the prioritization step - leveraging early warning detection and threat intelligence to address the vulnerabilities that are actually being exploited by threat actors.

6 Zero Trust

Continuously verify a user's identity and permissions, even after granting network access.

7 Access Management

Integrate with existing tools to establish end-to-end workflows and enforce security policies.

8 Security Awareness Program

Contextual asset intelligence empowers security teams with the confidence and capabilities required to orchestrate security operations at scale.

“ After implementing Armis, we saw a remarkable decrease in our cyber insurance premiums. The platform’s comprehensive security capabilities allowed us to address previously unresolved risk areas, leading to significant savings on our insurance costs. The continuous monitoring and proactive alerting have given us greater confidence in our cybersecurity posture. ”

Chief Information Security Officer // Fortune 500 Manufacturing Company

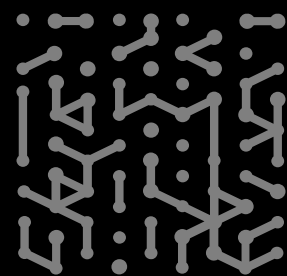
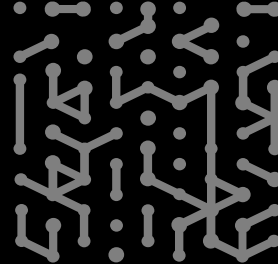
The Risk of Doing Nothing

Failing to improve asset visibility, risk prioritization, and security control over an organization’s entire attack surface can have severe consequences. Imagine an industrial operation experiencing a systematic compromise of its OT systems, leading to extensive outages, potential loss of life, significant revenue loss, and massive brand impacts. When filing a corresponding cyber insurance claim, the enterprise may face challenges if it failed to implement measures to ensure they can continuously see, protect, and manage all critical assets. The likelihood of insurance providers paying such claims decreases exponentially with every passing month of inaction. Enterprises should consider not only the immediate potential for costly operational impacts but also the inability to defer expenses in the event of a cyber incident.

Conclusion

In the current cybersecurity landscape, maintaining compliance with cyber insurance requirements is a critical component of an enterprise’s risk management strategy. Armis Centrix™ provides a comprehensive solution that helps organizations achieve this compliance by implementing insurer-recommended security technologies, leveraging direct security telemetry, and offering continuous monitoring and alerting. By adopting Armis Centrix™, enterprises can reduce cyber insurance costs, ensure compliance, and gain peace of mind knowing that their data and assets are protected. As cyber threats continue to evolve, the need for robust security measures and compliance with cyber insurance requirements will only grow more critical.

To learn more about how Armis can help your organization maintain compliance with cyber insurance requirements and enhance your overall security posture, contact us today. Let us help you navigate the complexities of cyber insurance and secure your enterprise for the future.



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

