



Faster, Easier **DORA Compliance** with Nagomi's Proactive Defense Platform

Compliance with the extensive requirements defined under the recently enacted Digital Operational Resilience Act (DORA), can be very taxing on an enterprise. The Nagomi platform not only fulfills specific DORA requirements but also makes the compliance process more efficient and reduces the opportunity for drift over time. Some of the specific areas Nagomi supports DORA and other compliance initiatives include:

Data Consolidation

Whether it is DORA or another statute specific to your industry, consolidating and normalizing the disparate data that exists in various silos across your information estate is one of the primary issues that makes cybersecurity compliance initiatives so challenging.

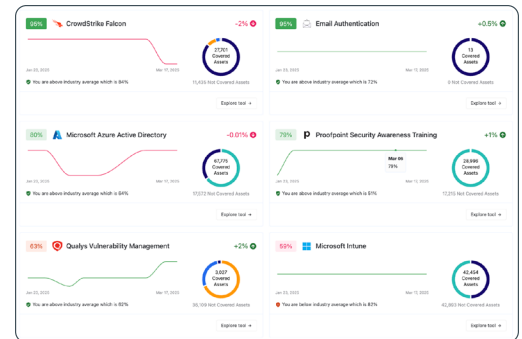
The Nagomi platform correlates and normalizes data from across your information assets, your security stack, and the external threat landscape, empowering security teams, executives and auditors to operate from a single, centralized source of truth. The Nagomi platform also applies business context specific to your environment, enabling security teams and auditors to easily identify which parts of the organization are meeting compliance requirements and which need improvement.

ICT Risk Management

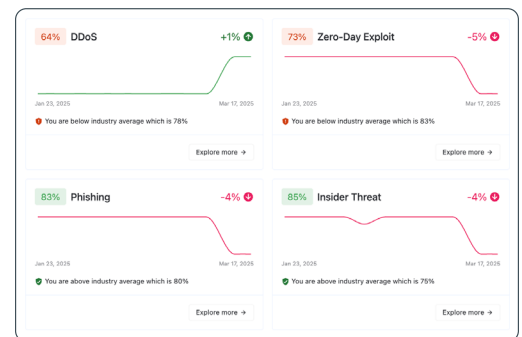
The Nagomi platform also provides benefits linked to several of the individual articles under DORA's Chapter II on ICT Risk Management including:

- Article 6: ICT risk management framework
- Article 7: Assess vulnerabilities in IT systems
- Article 8: Implementing cybersecurity controls
- Article 9: Identifying threats and anomalies
- Article 10: Response and recovery plans
- Article 11: Continuously improve resilience

Nagomi's proprietary data engine integrates information from across your information environment including assets, security tools and configuration databases to ensure tools are configured properly and security policies are adhered to. The Nagomi platform also maps your environment against NIST, CIS, and MITRE ATT&CK to ensure you are aligned with best practices and integrates your business context to ensure levels of risk fall within your acceptable ranges.



Track the effectiveness of your tools, with benchmarks and deep dives into their deployment and configuration.



Track your level of resilience against different threat scenarios.

Digital Operational Resilience Testing

DORA's Article 25 requires entities to conduct regular and thorough assessments to validate the effectiveness of security measures, ensuring weaknesses are identified and mitigated promptly. This testing is to follow a risk-based approach for "identifying weaknesses, deficiencies and gaps in digital operational resilience and of promptly implementing corrective measures".

The Nagomi platform identifies and prioritizes security weaknesses caused by policy noncompliance, vulnerabilities, misconfigurations, coverage gaps, and other factors. Instead of static, one-off resilience testing, Nagomi delivers an automated, data-driven approach—assessing your exposure from the inside out based on your assets, defenses, and the most relevant threats.

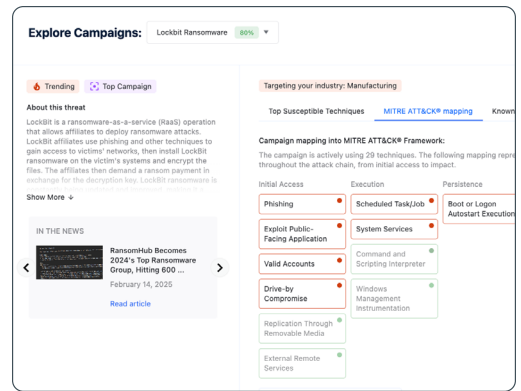
Executive and Board Reporting

DORA's Article 5 places heavy expectations on the "Management Body" (board) of EU financial entities stating it "bears the ultimate responsibility for managing ... ICT risk". This means the CISO needs to be part of board-level security discussions, and on-going reporting (as opposed to an annual audit report) must be produced to ensure the board is kept properly informed.

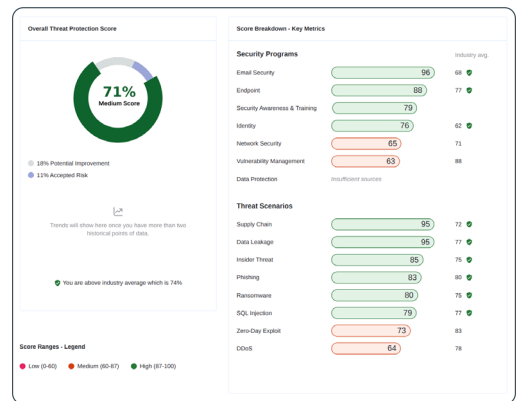
Nagomi's board-level dashboards and reports are generated automatically and updated continuously to provide always current insights into security posture, investment returns, and risk reduction. Reports link security performance to organizational objectives and can be customized to track whatever metrics are most relevant to the business ensuring alignment with board priorities and the organization's risk profile.

Nagomi Ensures You're Protected, Not Just Compliant

Nagomi automates the process of proving your security is actually working. Our platform unifies data across your assets, defenses, and threats to clearly illustrate your security program is both efficient and effective. This transparency helps you demonstrate measurable results with confidence. By maximizing existing investments, reducing threat exposure, and improving alignment across teams, Nagomi is the only Proactive Defense Platform that turns cybersecurity from a technical cost center into a strategic business enabler. With Nagomi, security goes from feeling fragmented and overwhelming to streamlined and effective—leveraging the tools you already have.



Deep dive into any threat actor and quickly be able to answer the question: How protected am I?



Build board reports to give contextual narratives around the effectiveness, progress and gaps in your Security Program.



Learn more at: nagomisecurity.com