vArmour

SOLUTION BRIEF

Accelerate DORA Compliance with Automated Dependency Mapping

Driven by the criticality of electronic financial services in modern society, regulatory compliance best practices have recently evolved from requiring recovery planning to mandating operational resilience. That is, incorporating proactive measures to mitigate disruptive events to ensure the resilience of important business services in the face of a varied and fluid set of risks. This is to enable organizations to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, and compromises.

This document will provide an overview on where vArmour can be applied in DORA compliance. Specifically, vArmour can help automate compliance in the areas of identification, mapping, operational management, and ongoing risk assessment of ICT assets and critical business functions.

The Burdens of Manual Compliance Processes

While it's true some organizations may have operational or cyber resilience processes in place to address DORA compliance, they are often manual in approach, quickly outdated, and siloed across teams — which frequently leads to higher operational costs, lower accuracy and effectiveness, and greater risks of human error.

Expensive Labor

Requires large amounts of manual labor, time, and costs — either in the form of internal resources, or external consultants.

Greater Risk of Human Error

Increases risk of human error due to oversight, loss of tribal knowledge or miscommunication across business units

Outdated Inventories and Risk Assessments

Periodic identification, mapping and risk assessment exercises result in outdated information used to manage operational change, recover from incidents and respond to emerging risk conditions.

Increased Financial Exposure

The risk of failing compliance audits or being unprepared for an incident results in extremely expensive penalty fines, as well as reputational damage.

How vArmour Accelerates DORA Compliance

With most businesses now exposed to cyber threats and operational complexity, specific regulations have emerged to help keep those businesses and the public at-large safe from cyber crimes and operational failures. This includes the European Commission's Digital Operational Resilience Act (DORA) that covers financial service institutions operating in the EU, including banks, loan organizations, insurance companies, and auditors.

vArmour Relationship Cloud is an automated dependency mapping solution for accelerating DORA compliance. Relationship Cloud makes regulatory reporting processes more accurate, more efficient, lower in cost, and dramatically lowers the risk of regulatory fines. Additionally, Relationship Cloud provides a continuously updated map of the enterprises' digital architecture in order to facilitate sound operational, cyber and risk management practices as required by DORA. Designed for continuous monitoring using existing digital telemetry, vArmour helps to avoid the periodic fire drills we see today in many organizations.

vArmour Benefits

Automatic & Continuous Asset Inventory

Auto-discover assets to easily map infrastructure to the important business services they provide.

Baseline & Monitor Application Behavior in Real-Time

Using the observed reality of applications, workloads, dependencies, and relationships, all in an intuitive user interface.

Immediate Visibility & Insights

Quickly determine key application dependencies to increase resilience and demonstrate compliance; identify where anomalies and deviations occur.

DORA Requirements and How vArmour Helps

DORA Article	Key Requirements	How vArmour Helps
Article 8 **IDENTIFICATION** vArmour addresses requirements under article 8, including 8.1 through 8.7	Identify on a continuous basis all sources of ICT risk. Sources include all ICT supported business functions, information and ICT assets, exposure to/from other financial entities, as well as exposure from other third-party service providers that support important business functions. Map the configuration of critical information and ICT assets, including the links and interdependencies between the assets. Perform a risk assessment upon each major change in the information system infrastructure, including the processes affecting ICT supported business functions, as well as the ICT assets themselves. Identify, classify and adequately document all ICT supported business functions.	vArmour identifies all ICT assets as they occur within the environment (including legacy and cloud), facilitating a process of inventory validation. vArmour maps ICT assets and infrastructure to the business functions they provide, uniquely using network telemetry to create an up-to-date, observations-based map of application behavior. This enables customers to see upstream dependencies of an application in order to ensure resiliency through many types of digital transformation projects, including cloud migration, data center consolidation, divestiture or zero trust segmentation. With a continuously updated map, enterprises will save time and money, accelerate success, and ensure service resiliency throughout the course of a transformation project or normal business operations. This has significant advantages over manual approaches. Relying on manual processes is error-prone and can take 100+ man hours only to end up with a static, point-in-time snapshot. vArmour accelerates this process to minutes, without new agents, using data from tooling you already own.
Article 9 **PROTECTION AND PREVENTION** vArmour addresses 9.1, 9.4(c), and 9.4(e)	Continuously monitor and control the security and functioning of ICT systems and tools. Implement policies limiting access to information and ICT assets to what is required. Implement policies, procedures and controls for ICT change management that are based on a risk assessment approach.	vArmour monitors and alerts when applications drift out of conformance through new or non-declared communications and dependencies, or through new or non-declared access. For change management planning, since vArmour understands all the relationships and dependencies between ICT assets, it is easy to understand the potential “blast radius” of an incident or operational change. This is especially helpful to understand what other assets might be in range of the incident, saving organizations significant cost by preventing unexpected downtime, and accelerating the speed of projects by instilling confidence in the commitment of changes.
Article 10 & 11 **DETECTION, RESPONSE and RECOVERY** vArmour addresses 10.1, 11.5	Promptly detect anomalous activities such as ICT-related incidents, and identify potential material single points of failure. Conduct a business impact analysis (BIA) of exposures to severe business disruptions. The BIA should consider the criticality of identified and mapped business functions, support processes, third-party dependencies and information assets, and their interdependencies.	vArmour monitors and alerts when applications drift out of conformance through new or non-declared communications. vArmour also enables an organization to understand where business flows have not exercised alternative availability zones in order to demonstrate resilience. By mapping all the relationships and dependencies between ICT assets, vArmour makes it easy to detect potential single points of failure and validate resilience within the architecture. This also enables the immediate detection of RTO (Recovery Time Objective) mismatches as required for BIA processes.

vArmour: The Dependency Mapping You Need for Today’s Regulatory Requirements

Identifying and mapping the behaviors and vulnerabilities to your business application ecosystem is just the start. Relationship Cloud provides operators and risk teams the ongoing monitoring and analytics tools required to ensure compliance demands are continuously met and that a proactive posture is taken to resilience in today’s dynamic hybrid environments. Contact us today to get started on saving time, money and risk with vArmour.

Find out more about vArmour