vArmour

DORA is coming fast. Are you ready?

The countdown to DORA is on. DORA will go into full effect in January 2025 and EU financial entities must be ready or face dire financial and legal consequences.

How vArmour Can Help

Serving financial entities around the globe, vArmour helps customers meet the stringent operational and cyber resilience demands of regulations like DORA through our automated monitoring and application mapping service, the **Relationship Cloud**.

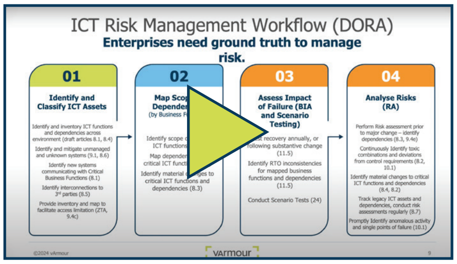
Here's how the Relationship Cloud can specifically help you meet the requirements of DORA:

DORA ARTICLE 8: IDENTIFICATION

vArmour addresses requirements 8.1 through 8.6

DORA Requirements		How vArmour Helps
Identify on a continuous basis all sources of ICT risk	➡	Identifies all ICT assets as they occur within your environment
Map the configuration of critical information and ICT assets, including the links and interdependencies between the assets	➡	Maps your ICT assets and infrastructure to the business functions they provide

Click on the short videos to the right to learn more about how vArmour can help you address DORA's identification requirements.



ICT Risk Management Workflow (DORA)

Enterprises need ground truth to manage risk.

01 Identify and Classify ICT Assets

Identify and inventory ICT functions and dependencies across environment (draft articles 8.1, 8.4)

Identify and mitigate unmanaged and unknown systems (9.1, 8.6)

Identify new systems communicating with Critical Business Functions (8.1)

Identify interconnections to 3rd parties (8.5)

Provide inventory and map to facilitate access limitation (ZTA, 9.4c)

02 Map Scop Dependen (by Business F

Identify scope o ICT functions

Map dependen critical ICT functi

Identify material c ges to critical ICT functions and dependencies (8.3)

03 Assess Impact of Failure (BIA and Scenario Testing)

st recovery annually, or following substantive change (11.5)

Identify RTO inconsistencies for mapped business functions and dependencies (11.5)

Conduct Scenario Tests (24)

04 Analyse Risks (RA)

Perform Risk assessment prior to major change – identify dependencies (8.3, 9.4e)

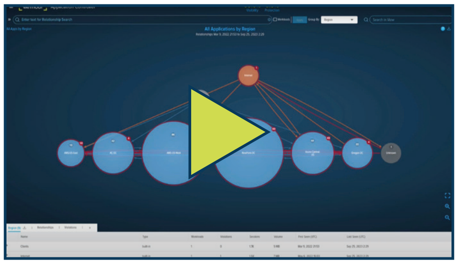
Continuously Identify toxic combinations and deviations from control requirements (8.2, 10.1)

Identify material changes to critical ICT functions and dependencies (8.4, 8.2)

Track legacy ICT assets and dependencies, conduct risk assessments regularly (8.7)

Promptly Identify anomalous activity and single points of failure (10.1)

©2024 vArmour varmour 9



DORA ARTICLE 9: PROTECTION & PREVENTION

vArmour addresses requirements 9.1, 9.4 (c), and 9.4 (e)

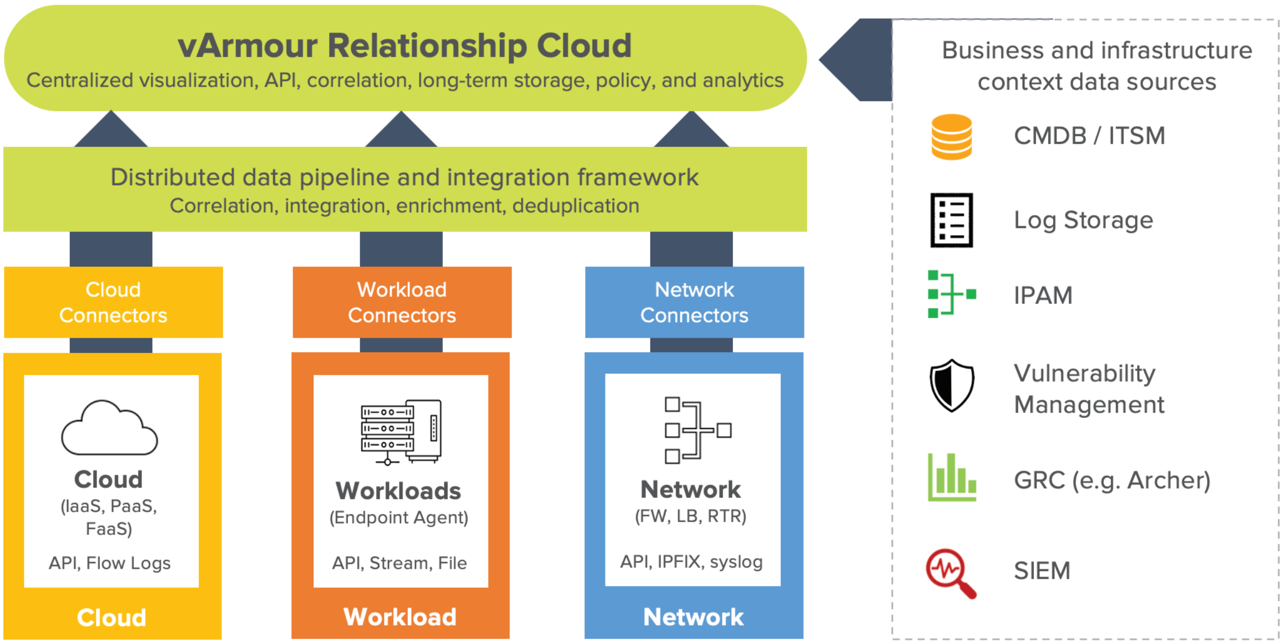
DORA Requirements

- 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

How vArmour Helps

- Monitors and alerts when applications become non-conformant through new non-declared communications and dependencies, and through new non-declared access
- Helps with change management planning by showing all relationships and dependencies between ICT assets

By observing application and infrastructure activity, the vArmour Relationship Cloud helps organizations understand business function behavior that introduces third party risk, which can be used alongside emerging procurement procedures to provide the ‘complete picture’ of third party risk in ICT systems.



vArmour Relationship Cloud

Centralized visualization, API, correlation, long-term storage, policy, and analytics

Distributed data pipeline and integration framework

Correlation, integration, enrichment, deduplication

Cloud Connectors	Workload Connectors	Network Connectors
Cloud (IaaS, PaaS, FaaS) API, Flow Logs	Workloads (Endpoint Agent) API, Stream, File	Network (FW, LB, RTR) API, IPFIX, syslog
Cloud	Workload	Network

Business and infrastructure context data sources

- CMDB / ITSM
- Log Storage
- IPAM
- Vulnerability Management
- GRC (e.g. Archer)
- SIEM

varmour

DORA ARTICLE 10 & 11: DETECTION, RESPONSE, AND RECOVERY

vArmour addresses requirements 10.1 and 11.5

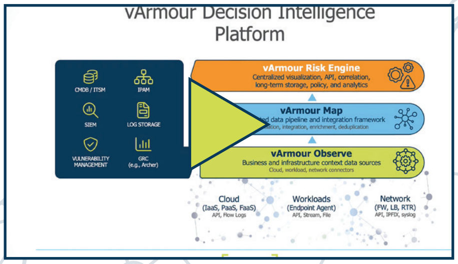
DORA Requirements

- Promptly detect anomalous activities such as ICT-related incidents and identify potential single points of failure
- Conduct a business impact analysis (BIA) of exposures to severe business disruptions

How vArmour Helps

- Constant monitoring provides alerts when applications drift out of non-conformance
- The Relationship Cloud's mapping makes it easy to detect potential single points of failure and enables the immediate detection of asset mismatches as required for BIA processes

Click on the short video to the right to see how the vArmour can help you execute, streamline, and automate DORA's business impact analysis process and continuous risk assessment requirements.


vArmour Decision Intelligence Platform
CMDB / ITSM
IPAM
SIEM
LOG STORAGE
VULNERABILITY MANAGEMENT
GRC (e.g., Archer)
vArmour Risk Engine
Centralized visualization, API, correlation, long-term storage, policy, and analytics
vArmour Map
…ed data pipeline and integration framework
…ation, integration, enrichment, deduplication
vArmour Observe
Business and infrastructure context data sources
Cloud, workload, network connectors
Cloud (IaaS, PaaS, FaaS)
API, Flow Logs
Workloads (Endpoint Agent)
API, Stream, File
Network (FW, LB, RTR)
API, IPFIX, syslog

vArmour: Your Path to Operational Resilience

vArmour offers organizations an alternative path to operational resilience through our automated Relationship Cloud service.

Unlike traditional approaches that require teams to manually draw upon and compile siloed and fragmented data, the Relationship Cloud automatically collects and unifies that data into a visual map that enables teams to easily see the relationships between all their digital assets in a singular view. As a result, organizations using vArmour achieve continuous and accurate observability of their environments that allows them to identify risks as they happen and where they happen.

✓

AUTOMATIC & CONTINUOUS ASSET INVENTORY

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

✓

MONITOR APPLICATION BEHAVIOUR IN REAL-TIME

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

✓

IMMEDIATE VISIBILITY & INSIGHTS

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

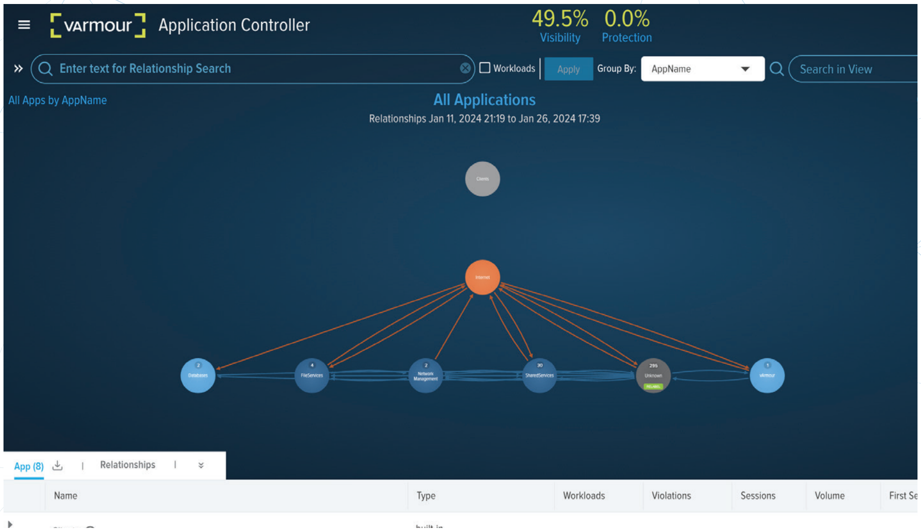
vArmour’s Relationship Cloud

Automated & Visualised Risk Mapping

vArmour’s Relationship Cloud services provides a continuously updated and automated map of an organization’s digital architecture in order to facilitate sound operational, cyber, and risk management practices as required by DORA.

How It Works

The Relationship Cloud integrates with an organization’s existing telemetry feeds and transforms that information into a visual map that continuously monitors for any risk or impact tolerance violations occurring between applications, workloads, and across the entire enterprise operating environment.



Name	Type	Workloads	Violations	Sessions	Volume	First Se

The Relationship Cloud interface — Relationship Graph Visualization View

vArmour: Your Automated Asset Mapping Solution for DORA Compliance

Identifying and mapping application behaviours and risks is just the start. The vArmour Relationship Cloud gives DORA-impacted entities and their risk teams the ongoing monitoring and analytics tools needed to ensure the compliance requirements of DORA are continuously met.

Contact us today to get started on the smarter, automated path to DORA compliance.

Key Contact

Marc Woolward
CTO & CISO
mwoolward@varmour.com