Trellix

SOLUTION BRIEF

EU DORA Regulation

Achieve DORA compliance with Trellix®

What is DORA?

The Digital Operational Resilience Act (DORA) is an EU regulation designed to increase cybersecurity and resilience across financial institutions and third-party service providers in the EU. Like the NIS2 Directive, it is not a framework for specific security controls but mandates a continuous risk management approach that will consistently improve cybersecurity maturity, incident management, and information sharing across financial institutions and their technology supply chain. DORA shifts the focus from compliance-based security to operational resilience as the outcome, ensuring financial institutions can withstand cyber threats while maintaining service continuity. Find a complete overview of DORA Articles here.

Who is affected by the DORA regulation?

DORA applies to all financial entities operating in the EU, including banks, insurance companies, payment service providers, investment firms, credit rating agencies, crypto-asset service providers, and their critical third-party technology providers worldwide. Find a full list of affected organizational types in Article 2. The inclusion of third-party suppliers is an important component as it aims to address technology supply chain risks, which is a growing attack vector for cyber threat actors.

DORA's requirements will impact information communications technologies (ICT) vendors offering products or services and forming part of the global supply chain supporting the European financial sector —whether or not those vendors are based within the EU. In other words, DORA's requirements encompass any enterprise anywhere in the world that provides ICT-related services such as critical software, cloud platforms, data analytics, or software-as-a service (SaaS) products and services to EU financial institutions. ICT vendors will no longer be just technology suppliers to a financial institution. Rather, they will become partners — subject to meeting the same operational resiliency tests and requirements, such as penetration testing, disaster recovery, and security controls.

Why Trellix for DORA compliance?

Trellix can help financial entities meet DORA requirements in 3 key ways:

1. Speed up incident detection and investigations
2. Provide advanced controls to prevent business disruption caused by ransomware or other emerging threats
3. Offer services to assess and build a continuous Information Security Management System

The goal of DORA compliance is to reduce cyber risk and improve operational resilience across the critical financial sector and the broader technology supply chain. While Trellix can help you reduce cyber risk in many ways, we describe the essential Trellix solutions below that will help you meet DORA requirements.

Trellix Helix Connect delivers extended threat detection and response capabilities across IT, OT, and Cloud, increasing your enterprise visibility and anomaly detection. Helix Connect combines insights from Trellix sensors and 600 + data sources with built-in threat intelligence and AI-powered automation to significantly reduce incident detection and response times. Trellix offers comprehensive forensic capabilities across endpoints and networks to provide the necessary log evidence to meet DORA incident management requirements. The complete Trellix Security Platform also delivers the advanced security controls required to strengthen cybersecurity across endpoint, servers, network, data, cloud, and mobile devices. Finally, Trellix Consulting Services can assess your current security program against international standards and provide readiness assessments and threat intelligence for continuous risk analysis.

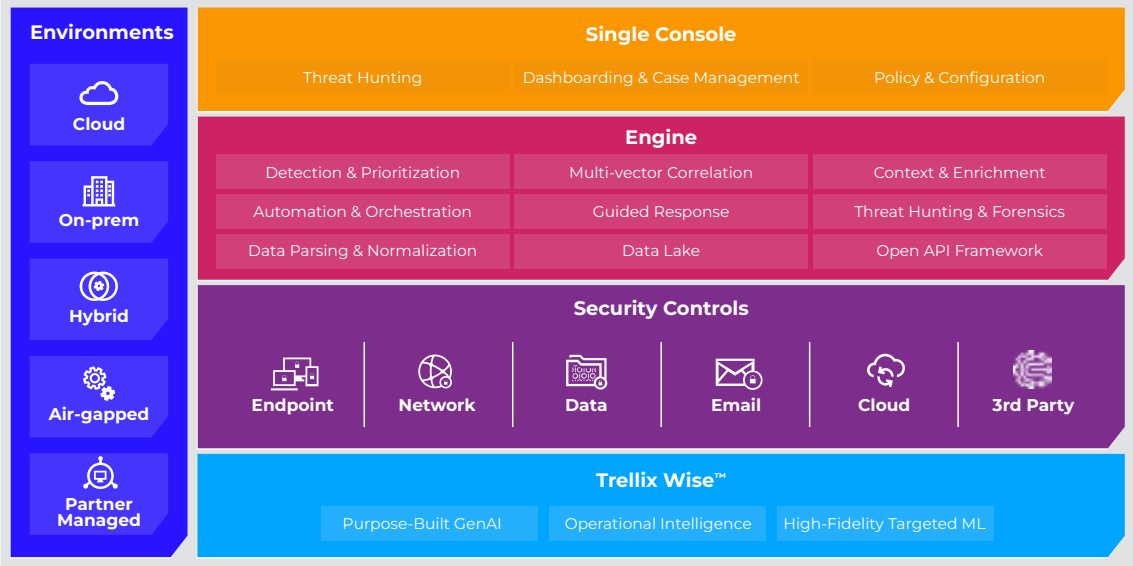

Figure 1: Trellix Security Platform

Develop an information risk management system with Trellix Services

The DORA regulation mandates that organizations implement comprehensive risk management strategies, conduct continuous assessments for ICT systems, and proactively adopt a security posture based on the changing threat landscape. Adopting International standards such as ISO27001 or the NIST Cybersecurity Framework to build your Information Security Management System (ISMS) is a good starting point. As a first step, assess your current state cyber security controls against one of those standards. However, DORA goes beyond control frameworks and into operational resilience, driving the need to assess readiness using threat informed penetration tests, business continuity tests, and incident response exercises. Trellix has an extensive array of services that can help you assess maturity against standards, develop an ISMS, design or optimise detection and response programs, and improve operational readiness against key threat vectors. We recommend immediately focusing on these 5 key assessments to meet your DORA compliance goals.

Trellix Services	Services Description	DORA Articles
ISMS Assessment and Program Development	Maturity assessment against international standards and establishment of an information security risk management system	2.1 a-d; 2.2 a-k; 3.a-f; 12.1; 24.1, 24.2; 24.3; 24.4; 26.1; 26.2; 29.1; 31.130.1; 30.2; 18.1; 19.1
Trellix Intelligence as a Service	Continuously identify new threats to your financial institutional and industry peers	3.e; 31.3; 23.2
Ransomware Resilience Readiness Assessment	Custom tabletop exercises to assess your ransomware risk	25.1; 25.2; 25.3; 25.4; 31.2; 36.1; 36.2; 36.3
SOC and Incident Response Readiness Assessments	Develop a structured incident detection and management program to reduce mean time to response. Provide emergency IR support, including forensics, for rapid remediation and return to service	22.a-e; 23.1; 23.2a-d; 12.1
Threat Led Penetration test services	Assess your control effectiveness and continually adapt your security posture	3.e; 31.3; 23.2
Critical Business Application Resilience Assessment	Assess DevSecOps processes and business applications protection against exploit, unauthorized access, data leakage, and malware upload	25.1; 25.2; 25.3; 25.4; 31.2; 36.1; 36.2; 36.3

You can schedule any Trellix Assessment Services through your Account Manager or on the website here

Accelerate incident detection, response, and reporting

One of the main goals of the DORA regulation is to improve incident detection and response across the financial enterprise. Common challenges entities face in their SecOps capabilities are visibility gaps, talent shortage, and lack of automation, which slow down the mean-time-to-respond (MTTR). Trellix SOC and IR assessments help expose those gaps and provide an action plan to mature the program. From a technology perspective, the Trellix Helix Connect reduces analyst workload and MTTR by ingesting data from Trellix sensors and over 600 integrations.

That data is enriched with built-in threat intel and AI-driven automation for rapid detection and response across IT, OT, and Cloud networks. In addition to Trellix Helix and SOC assessments, we recommend the following Trellix sensors solutions to provide forensic evidence capture, anomalous activity, and cyber threat detection capability across the enterprise.

Trellix SOC Solutions	Solution Description	DORA Articles
Trellix EDR and Trellix Endpoint Forensics	Use endpoint sensors to prevent malware and detect anomalies or malicious endpoint activity with full log capture for evidence storage	12.2; 22.c; 22.d; 22.e; 23.2; 23.3; 23.4; 23.5
Trellix NDR and Trellix Network Forensics	Network sensors prevent exploits and detect anomalies and malicious network activity with full packet capture for evidence storage	3.e; 31.3; 23.2
Trellix IVX Enterprise Applications	Malware detection sensor for cloud collaboration applications, storage services, and business applications with forensics reports for evidence storage	12.2; 22.c; 22.d; 22.e; 23.2; 23.3; 23.4; 23.5
Trellix Helix Connect	Unite signals from multiple tools to surface threats that might go undetected by individual point tools, reducing MTTD and MTTR	12.2; 22.c; 22.d; 22.e; 23.2; 23.3; 23.4; 23.5

Operational resilience from ransomware

The November 2024 Trellix Threat Report discusses the escalation in ransomware attacks, with new families from the year making an increasingly significant impact. Ransomware is a particular threat to the operational resilience of critical services provided by financial services. We have seen high-profile attacks that have disrupted operations. So, it's critical that organizations build an in-depth defense to prevent, detect, and respond quickly to ransomware attacks. In particular, email security needs more resilience. Recent threat intelligence indicates that as much as 44% of all attacks detected in the financial sector used email. In addition to Trellix Ransomware Readiness Assessments, we recommend leveraging these Trellix solutions to close malware protection gaps and reduce the risk of ransomware affecting your business operations.

Trellix Solutions	Solution Description	DORA Articles
Trellix Endpoint and Trellix Mobile Security	Advanced ransomware protection on end user systems, servers, and mobile devices	11.2a; 11.2b; 11.2d; 11.2f; 11.2c;
Trellix IVS for Collaboration Platforms	Prevent and detect malware delivery from phishing and collaboration applications	11.2d; 12.2; 22.c; 22.d; 22.e; 23.2; 23.3; 23.4; 23.5
Trellix IVX Enterprise Application	Identify ransomware hiding in storage and custom business applications on prem or in the cloud	11.2d; 12.2; 22.c; 22.d; 22.e; 23.2; 23.3; 23.4; 23.5
Trellix Network Security	Prevent and detect lateral movement and late stage ransomware techniques	11.2d; 13.1d; 13.1g; 13.1j; 13.1k
Trellix Helix Connect	Unite signals from multiple tools to surface ransomware threats that might go undetected by individual point solutions	12.2; 22.c; 22.d; 22.e; 23.2; 23.3; 23.4; 23.5

To learn more about how Trellix can protect your business from ransomware, please visit our Ransomware Detection and Response website here.

Data and system security

Trellix is a leading provider of data and system protection. Our solutions prevent malicious code on end-user devices, servers, and legacy operating systems that may be in use. Additionally, Trellix Data Security prevents the loss of sensitive data. In addition to Trellix Data Protection program services, we recommend leveraging these Trellix solutions to meet DORA data and system security requirements.

Trellix Solutions	Solution Description	DORA Articles
Trellix Endpoint and Trellix Mobile Security	Advanced malware protection and software restrictions on end-user devices, legacy systems, servers, and mobile devices	11.2a; 11.2b; 11.2d; 11.2f; 11.2c
Trellix Data Loss Prevention and Trellix Device Control	Identify, classify, and protect against data loss or unauthorized removable media usage on end user devices and networks	11.2a; 11.2i; 11.2e, 11.2f; 23.2; 23.3; 23.4; 23.5; 14.1
Trellix Policy Auditor	Monitor end user devices and servers for configuration baseline set by the organization	11.2a; 11.2b

Operational resilience for third-party cloud systems

Many financial entities leverage third-party cloud infrastructure providers to host critical business and customer-facing applications. Spearphishing is the leading way attackers gain entry into these cloud-hosted applications followed closely by exploited vulnerabilities. Ensuring the operational resilience of these systems is critical to meeting DORA requirements.

Trellix Solutions	Solution Description	DORA Articles
Trellix Endpoint Security, Trellix EDR, and Trellix Endpoint Forensics	Malware protection, application allowlisting, and behavioural detections for cloud workloads	11.2a; 11.2b; 11.2d; 11.2f; 11.2c; 12.2; 22.c; 22.d; 22.e; 23.2; 23.3; 23.4; 23.5
Trellix Database Security	Identify vulnerabilities, prevent DB vulnerability exploitation, and detect anomalies on critical business applications	11.2d; 12.2; 22.c; 22.d; 22.e; 23.2; 23.3; 23.4; 23.5
Trellix IVX for Enterprise Applications	Identify malware hiding in storage and custom business applications on prem or in the cloud	11.2d; 12.2; 22.c; 22.d; 22.e; 23.2; 23.3; 23.4; 23.5
Trellix Intrusion Prevention System	Prevent application exploits and detect network anomalies on cloud platforms	11.2d; 13.1d; 13.1g; 13.1j; 13.1k
Trellix Helix Connect	Correlate data from multiple sources including OT and IoT devices to create the full picture of a threat	12.2; 22.c; 22.d; 22.e; 23.2; 23.3; 23.4; 23.5

Learn more about how Trellix can protect your cloud systems hosted on providers like AWS