Securing SaaS under DORA Regulations

The European Union's Digital Operational Resilience Act (DORA) came into force on 16 January 2023, but organisations have until 17 January 2025 to become compliant.

Financial institutions, including banks, insurance companies, and investment firms, must comply with the legislation's strict rules for cybersecurity protection, detection, containment, recovery, and repair capabilities or face penalties.

DORA was created by the EU to strengthen the operational resilience of its financial entities. The EU recognised that the digital transformation taking place in the financial services industry placed an unprecedented reliance on technology. Should that technology be compromised by a cyber attack, financial services would be impacted. DORA covers Information and Communications Technology (ICT), which includes cloud-based SaaS applications.

DORA's Impact on SaaS Platforms and Apps

DORA encompasses five main areas: ICT risk management, reporting, digital operational resilience testing, management of third-party risk, and information and intelligence sharing. SaaS security falls under ICT risk management.

Financial service providers must be capable of the following:

- Identification – ability to document all users, their roles, and their responsibilities within the application
- Protection and prevention – develop policies and deploy tools that monitor configurations to ensure the resilience and continued availability of the application
- Detection – promptly monitor user behaviour to detect indications of compromise (IOC) for the application
- Learning and evolving – build an audit trail for the purpose of post-breach analysis following any cybersecurity incident
- Manage third-party risk – ensure that all integrated applications maintain the same security standards that are applied to the hub SaaS applications

How Adaptive Shield Enables DORA Compliance

Adaptive Shield's SaaS Security Platform provides the visibility and analysis of SaaS applications needed to comply with DORA.

Misconfiguration Management

Identify settings whose configurations introduce risk to the application and trigger alerts based on thousands of security checks

Identity Security Posture Management

Identify all application users, audit permissions, detect dormant users, discover former employees who retained access, monitor non-human users, and track external users

Connected Apps

Discover third-party integrated applications, review their scopes, and assess their threat level

Data Management

List all documents, files, repositories, and calendars that are shared with external users or publicly shared

Identity Threat Detection & Response

Monitor user activities from across the SaaS stack to detect anomalies and indications of compromise that signify a threat

ADAPTIVE SHIELD

Adaptive Shield is GDPR compliant.
The company maintains an EU environment to ensure data sovereignty for EU customers.

Adaptive Shield secures over 150 applications out of the box, and our Integration Builder enables monitoring of any custom, homegrown, or niche application!

Salesforce · ServiceNow · M365 · Workday · Teams · DocuSign · Box

Zoom · Azure · Okta · GitHub · Jira · Snowflake · CrowdStrike

www.adaptive-shield.com

Follow us on LinkedIn

Request a Demo