

Strengthening Digital Operational Resilience: The Critical Role of API Security and Posture Governance in DORA Compliance

Introduction

In today's digital age, financial institutions rely on interconnected systems to deliver services efficiently and securely. However, with increased digital transformation comes heightened exposure to cyber threats. In response, the European Union introduced the Digital Operational Resilience Act (DORA), a regulatory framework designed to strengthen the operational resilience of financial entities against IT-related incidents.

DORA mandates that financial entities adopt robust measures to ensure the continuous operation of their critical functions, even in the face of severe operational disruptions. This white paper explores the core principles of DORA and underscores the importance of API security and posture governance in ensuring compliance and safeguarding digital infrastructure.

Overview of DORA

DORA is a regulation that aims to harmonize and improve the operational resilience of financial entities across the EU by focusing on several key areas:

- 1. ICT Risk Management:** Financial entities must establish comprehensive frameworks to manage Information and Communication Technology (ICT) risks.
- 2. Incident Reporting:** Organizations are required to report major ICT-related incidents to regulators.
- 3. Resilience Testing:** Regular testing of systems and controls to assess resilience against cyber threats is mandatory.
- 4. Third-Party Risk Management:** Firms must ensure that third-party providers, especially in ICT, follow stringent security protocols.

5. Operational Continuity: Financial institutions must ensure the continuity of their operations during a cyber disruption or other significant event.

Given the scope of DORA, **API security**, and **posture governance** emerge as critical elements in protecting digital financial ecosystems. APIs are the backbone of modern financial systems, connecting services, applications, and data across various platforms and institutions. Any vulnerability within API ecosystems can expose financial institutions to cyber threats, leading to service disruptions, data breaches, and financial loss. Simultaneously, posture governance helps organizations maintain a comprehensive and consistent security posture, ensuring the effective management of API vulnerabilities and risks in real-time.

The Role of APIs in Financial Systems

APIs (Application Programming Interfaces) are essential tools that enable different software systems to communicate and exchange data seamlessly. In financial services, APIs enable interoperability between institutions, facilitate digital payments, and enhance customer experiences through open banking.

However, APIs also introduce significant security challenges, including:

- **Exposed Endpoints:** APIs often expose sensitive data or services, creating attack surfaces that hackers can exploit.
- **Zombie & Shadow APIs:** Unmanaged or forgotten APIs, often called zombie and shadow APIs, increase the risk of unauthorized access or data leaks.
- **Inadequate Authentication & Authorization:** Weak API security practices can lead to improper authentication mechanisms, allowing malicious actors to bypass safeguards.

These challenges highlight the importance of robust API security measures, which align closely with DORA's goals of strengthening operational resilience and protecting financial systems from cyber threats.

The Role of Posture Governance in API Security and DORA Compliance

Posture governance refers to continuously managing and assessing an organization's security posture to ensure compliance, risk management, and operational resilience. In the context of DORA, posture governance plays a vital role in enhancing API security and financial institutions' broader resilience.



Posture governance encompasses:

- 1. Continuous Monitoring and Assessment:** Regularly assessing APIs' security posture ensures that organizations can detect and address vulnerabilities as they arise. This proactive approach aligns with DORA's continuous risk management and operational resilience requirements.
- 2. Risk Prioritization:** Posture governance allows organizations to prioritize risks based on potential impact. This means that the most critical API vulnerabilities that pose the greatest threat to operations or regulatory compliance are addressed first, helping meet DORA's stringent risk management requirements.
- 3. Policy Enforcement and Compliance:** Posture governance ensures that security policies are consistently applied across all APIs, reducing the likelihood of shadow or zombie APIs operating outside the established governance framework. This ensures compliance with DORA's focus on operational continuity and third-party risk management.
- 4. Holistic Visibility Across the Ecosystem:** By continuously monitoring and maintaining posture governance across the API ecosystem, financial entities clearly understand their overall security posture. This holistic view is essential for meeting DORA's reporting and resilience testing mandates.

Incorporating posture governance strengthens API security and helps institutions navigate the complexities of DORA compliance by providing a structured approach to managing operational resilience.

Why API Security and Posture Governance are Critical for DORA Compliance

To meet the stringent requirements of DORA, financial institutions must adopt a proactive approach to securing their API ecosystems and maintaining strong posture governance. The following reasons illustrate why API security and posture governance are indispensable for DORA compliance:

- 1. Preventing Data Breaches:** Secure APIs, governed by a robust security posture, ensure that only authorized users can access sensitive financial data. With strict data protection rules under DORA, organizations must mitigate the risk of unauthorized data access through well-secured and continuously governed APIs.
- 2. Ensuring Service Availability:** APIs power many financial services, and any disruption to their functionality can result in downtime, impacting service continuity. DORA mandates



financial entities to maintain operational continuity, making API security and posture governance critical to preventing service outages.

- 3. Third-Party Risk Management:** DORA emphasizes the importance of managing third-party risks, including those posed by third-party APIs. Organizations must ensure that their partners follow API security best practices and maintain governance policies to avoid cascading risks that could affect their resilience.
- 4. Comprehensive Incident Response:** With DORA's focus on incident reporting and recovery, financial institutions must have detailed visibility into their API traffic and overall security posture. This ensures they can detect anomalies, respond swiftly to breaches, and report incidents in line with regulatory requirements.
- 5. Mitigating Zombie & Shadow API Risks:** Zombie and shadow APIs, often overlooked, can introduce hidden vulnerabilities. DORA requires thorough risk assessments, and by securing all APIs—both active and forgotten—through effective posture governance, institutions can close these security gaps.

How Salt Security and Posture Governance Address API Security Challenges in the DORA Era

Salt Security offers comprehensive API security solutions to protect financial institutions from cyber threats and ensure compliance with regulatory frameworks like DORA. Salt Security provides:

- **API Discovery and Posture Governance:** Automated discovery of all APIs, including zombie and shadow APIs, and ongoing governance to assess risks and ensure visibility.
- **Real-time Monitoring and Threat Detection:** Continuous monitoring of API traffic to detect and mitigate suspicious activity before it leads to a breach while maintaining strong governance policies.
- **Robust Authentication and Access Control:** Ensuring that only authorized users and applications can access APIs, safeguarding sensitive data, and supporting DORA compliance.
- **Compliance Reporting and Risk Management:** Comprehensive reporting tools that align with DORA's incident reporting requirements, enabling financial institutions to meet regulatory obligations and manage their overall security posture.



Conclusion

As financial institutions embrace digital transformation, ensuring the security and governance of their API ecosystems becomes increasingly vital. The Digital Operational Resilience Act (DORA) provides a comprehensive regulatory framework to safeguard the operational resilience of financial systems across the EU. By prioritizing API security and posture governance, financial entities can achieve DORA compliance and protect themselves from a growing range of cyber threats.

API security and posture governance should no longer be an afterthought—they are cornerstones of resilience in the evolving financial landscape. With the right security measures, such as those provided by Salt Security, organizations can confidently navigate the regulatory environment and fortify their operations against future disruptions.

