VENARI SECURITY

Whitepaper

DORA Compliance in the Age of Encrypted Traffic

How Venari Security Can Help

Introduction

The Digital Operational Resilience Act (DORA), implemented by the European Union, establishes a new regulatory landscape for the financial sector. DORA emphasizes the importance of robust cybersecurity measures to protect critical infrastructure and ensure operational resilience. One key challenge in achieving DORA compliance lies in monitoring and securing encrypted traffic, which forms a significant portion of modern communication.

This white paper explores the intersection of DORA regulation, encrypted traffic, and how Venari Security can assist organizations in achieving compliance through continuous TLS/SSL monitoring and management.

DORA and the Challenge of Encrypted Traffic

DORA mandates financial institutions to implement a comprehensive set of cybersecurity controls. These controls aim to safeguard critical operations, prevent disruptions, and ensure swift recovery from incidents. However, the widespread use of encryption, particularly Transport Layer Security (TLS) and Secure Sockets Layer (SSL), presents a challenge for regulators and institutions alike.

Limited Visibility:

Encrypted traffic masks the content being transmitted, hindering traditional methods of network monitoring and security analysis. This lack of visibility makes it difficult to detect potential threats hidden within encrypted communication channels.

Compliance Challenges:

DORA requires institutions to monitor for vulnerabilities, misconfigurations, and unauthorized certificates associated with TLS/SSL connections. Achieving this level of oversight becomes significantly more complex when dealing with encrypted traffic.

DORA Articles on Encrypted traffic

There are several articles mentioning the monitoring of external and internal encrypted traffic on an organization network and several challenges to solve:

Dora Requirement	Challenge to solve	Venari Security solution
General Principle	Encryption of Data in Transit	Analyse all the data in transit across an organisations network:
Article 5	Setup policy on encryption and cryptographic controls	Create and delivers a variety of regulatory frameworks that allow an organisation to report on encryption compliance to DORA
Article 6	Design the policy on encryption and cryptographic controls	
Article 9	Continuously monitor encryption	Venari Security continuously monitor encrypted traffic and communications
Article 9	Continuously monitor encryption	Venari Security continuously monitor encrypted traffic and communications

DORA Article 6:

Financial entities as defined in Article 2, points (a) to (t) shall design the policy on encryption and cryptographic controls referred to in paragraph 1 on the basis of the results of an approved data classification and ICT risk assessment. That policy shall contain rules for all of the following:

a. the encryption of data at rest and in transit;
b. the encryption of data in use, where necessary;
c. the encryption of internal network connections and traffic with external parties;
d. the cryptographic key management referred to in Article 7, laying down rules on the correct use, protection, and lifecycle of cryptographic keys.

Financial entities shall include in the policy on encryption and cryptographic controls referred to in paragraph 1 a requirement to record the adoption of mitigation and monitoring measures adopted in accordance with paragraphs 3 and 4 and to provide a reasoned explanation for doing.

DORA Article 9

For the purposes of adequately protecting ICT systems and with a view to organizing response measures, financial entities shall continuously monitor and control the security and functioning of ICT systems and tools and shall minimize the impact of ICT risk on ICT systems through the deployment of appropriate ICT security tools, policies and procedures.

DORA Article 10

Financial entities shall devote sufficient resources and capabilities to monitor user activity, the occurrence of ICT anomalies and ICT-related incidents, in particular cyber-attacks.

DORA Article 13

Financial entities shall monitor the effectiveness of the implementation of their digital operational resilience strategy set out in Article 6(8). They shall map the evolution of ICT risk over time, analyse the frequency, types, magnitude and evolution of ICT-related incidents, in particular cyber-attacks and their patterns, with a view to understanding the level of ICT risk exposure, in particular in relation to critical or important functions, and enhance the cyber maturity and preparedness of the financial entity.

Venari Security: Enabling DORA Compliance with Continuous TLS/SSL Monitoring

Venari Security offers a comprehensive solution that empowers organizations to navigate the challenges of encrypted traffic and achieve DORA compliance. Our platform provides continuous monitoring and management of TLS/SSL certificates and connections, ensuring robust security posture and regulatory adherence.

Key Features of Venari Security for DORA Compliance:

Deep Visibility into Encrypted Traffic:

Venari Security utilizes advanced techniques to gain insights into encrypted traffic without compromising data privacy. This allows for comprehensive threat detection and analysis, even within secured communication channels.

Continuous TLS/SSL Posture Assessment:

Our platform continuously monitors TLS/SSL certificates for vulnerabilities, expiration dates, and misconfigurations. This proactive approach ensures that certificates remain valid and secure, mitigating potential compliance risks.

Automated Compliance Reporting:

Venari Security automates the generation of detailed reports on TLS/SSL posture, providing valuable evidence for demonstrating compliance with DORA regulations. These reports simplify the auditing process and reduce administrative burdens.

Streamlined Certificate Detection:

Venari Security simplifies certificate lifecycle management, including detection ended, close to end or non-compliant certificates across all the network. This reduces the risk of expired or compromised certificates, a critical aspect of DORA compliance.

Benefits of Utilizing Venari Security for DORA Compliance

Enhanced Security Posture:

By gaining deep visibility into encrypted traffic, organizations can proactively identify and address potential threats lurking within secure connections.

Simplified Compliance Management:

Venari Security automates key tasks associated with TLS/SSL monitoring and reporting, streamlining the compliance process and reducing administrative overhead.

Reduced Risk of Regulatory Fines:

Continuous monitoring and adherence to DORA requirements minimize the risk of regulatory non-compliance and associated penalties.

Improved Business Continuity:

A robust TLS/SSL posture contributes to overall operational resilience, ensuring business continuity in the face of cyber threats.

Conclusion

DORA compliance necessitates a proactive approach to securing encrypted traffic. Venari Security provides a comprehensive solution that empowers organizations to achieve compliance while maintaining optimal security posture. By leveraging advanced TLS/SSL monitoring and management capabilities, Venari Security ensures continuous visibility, simplifies compliance management, and ultimately fosters a more secure and resilient financial ecosystem.

Bridge your knowledge gap.
Visit: www.venarisecurity.com

Venari Security Ltd.

16 Great Queen Street, London,
WC2B 5AH, United Kingdom
+44 (0)20 7294 7749
info@venarisecurity.com

About Venari Security

Venari Security provides organisations with advanced visibility into their encrypted attack surface, ensuring regulatory compliance and privacy adherence through our cryptographic discovery tool.

Our focus is on crypto agility which helps you assess both external and internal cryptographic risks, preparing your business now and for the quantum future.

VENARI SECURITY