White Paper

A CISO's Guide to DORA Compliance with Akamai Guardicore

Achieving digital operational resilience by stopping the spread



Contents

Executive summary: The new mandate for financial resilience 4

Understanding the DORA framework 5

Who does DORA apply to? 5

The shift from business continuity to operational resilience 5

The modern financial attack surface: A paradigm of complexity 6

The failure of the perimeter in a hybrid world 6

Lateral movement: The silent killer of cyber resilience 6

The ship analogy: Why a strong hull isn't enough 6

Microsegmentation: The foundation of a Zero Trust strategy 7

Assuming breach: The core tenet of Zero Trust 7

Microsegmentation: The engine of a Zero Trust architecture 7

Contrasting with legacy controls: VLANs and internal firewalls 7

Contents

A deep dive: Mapping the Akamai Guardicore platform to the five pillars of DORA 8

Pillar 1: Proactive ICT Risk Management 8

Pillar 2: Rapid ICT-Related Incident Management 9

Pillar 3: Continuous Digital Operational Resilience Testing 10

Pillar 4: Comprehensive ICT Third-Party Risk Management 10

Pillar 5: Actionable Information and Intelligence Sharing 11

Comprehensive support for all five DORA pillars 11

Practical application: Key use cases for DORA compliance 12

From theory to practice: Voices from the financial front line 13

The Akamai advantage: Simplifying segmentation, accelerating resilience 14

Conclusion: Building a resilient future, today 15

Executive summary: The new mandate for financial resilience

The global financial system operates on a foundation of trust and availability. In the digital age, this foundation is under constant assault. High-profile cyberattacks have demonstrated that an incident at a single financial entity can have cascading effects, disrupting critical markets and eroding public confidence.

In response, the European Union has enacted the **Digital Operational Resilience Act (DORA)**, a landmark regulation that came into full effect in January 2025. DORA is not merely an extension of existing guidelines; it is a fundamental rethinking of how financial entities and their critical technology partners must approach cybersecurity. It moves beyond data protection to mandate a comprehensive framework for *digital operational resilience* — the ability to withstand, respond to, and recover from all types of ICT-related disruptions and threats.

This white paper serves as a strategic guide for CISOs and security leaders. It explores the core tenets of DORA and outlines how a Zero Trust strategy, enabled by the **Akamai Guardicore** platform, provides the most effective path to not only achieve compliance but to build a truly resilient and secure enterprise. The central thesis is simple but powerful: **To achieve the resilience that DORA demands, you must shift your focus from solely preventing the initial breach to definitively stopping its spread.**

> **Achieving DORA compliance requires more than strengthening perimeter defenses. True resilience comes from the ability to contain threats, preserve critical operations, and prevent the spread of attacks. Microsegmentation offers the control and visibility necessary to meet DORA's demanding operational standards.**

Understanding the DORA framework

DORA harmonizes a fragmented regulatory landscape, creating a single, binding set of rules for all EU member states. Its primary goal is to ensure that the financial sector can maintain resilient operations through a severe operational disruption.

Who does DORA apply to?

The scope of DORA is extensive, covering traditional financial institutions and the critical technology providers they rely on. This includes:

- Credit institutions (banks)
- Investment firms
- Payment and electronic money institutions
- Crypto-asset service providers
- Central securities depositories and central counterparties
- **Critical third-party ICT service providers**, including cloud service providers, data centers, and managed service providers

This last point is a significant departure, as it places direct regulatory oversight on the technology supply chain, making third-party risk management a critical focus area.

The shift from business continuity to operational resilience

Traditional business continuity and disaster recovery (BC/DR) plans often focused on recovering from physical events or system failures. DORA reframes this discipline around **operational resilience**, which presupposes a hostile cyber environment. It's a proactive stance that focuses on the ability to continue performing critical functions *during* a sophisticated cyberattack, not just after an outage. This requires a security architecture built for containment and continued operation under duress.

The modern financial attack surface: A paradigm of complexity

The traditional model of a fortified network perimeter has been rendered obsolete. Digital transformation, cloud adoption, and the rise of fintech ecosystems have created a distributed, dynamic, and complex attack surface.

The failure of the perimeter in a hybrid world

Critical applications and sensitive data are no longer confined to on-premises data centers. They are distributed across a mix of private and public clouds. This hybrid environment creates significant visibility gaps and makes it nearly impossible to enforce consistent security policies using traditional, network-based firewalls, which were never designed for the east-west traffic that dominates modern architectures.

Lateral movement: The silent killer of cyber resilience

Legacy security assumes that everything inside the network can be trusted. This creates a "flat" network where, once an attacker breaches the perimeter, they can often move laterally with ease, escalating privileges and seeking out high-value assets like payment systems, customer databases, and core banking applications. **It is this unchecked lateral movement — the spread — that turns a minor incident into a catastrophic breach.** Ransomware, for example, relies almost entirely on the ability to spread laterally to encrypt critical systems.

The ship analogy: Why a strong hull isn't enough

Think of a traditional network as a ship with a single, strong outer hull (the perimeter firewall). If that hull is breached, water floods the entire ship, and it sinks quickly. A resilient, modern ship, however, is built with multiple watertight compartments. If the hull is breached, the flooding is contained to a single compartment, allowing the rest of the ship to remain afloat and operational. **Microsegmentation provides these watertight compartments for your network.**

Microsegmentation: The foundation of a Zero Trust strategy

A modern, resilient security posture must be built on the principles of **Zero Trust**, which operates on the mantra of "never trust, always verify."

Assuming breach: The core tenet of Zero Trust

Zero Trust assumes that threats can and will exist both inside and outside the network. It assumes a breach is not a matter of *if*, but *when*. Therefore, every user, device, and application request must be authenticated and authorized before access is granted, regardless of its location. The goal is to make a breach irrelevant by ensuring it cannot spread.

Microsegmentation: The engine of a Zero Trust architecture

Microsegmentation is the core technology that enables a true Zero Trust architecture internally. Instead of creating large, trusted network zones, microsegmentation allows you to create secure, isolated segments around individual applications or even workloads. By enforcing granular, identity-based policies, you can ensure that applications can only communicate with the resources they absolutely need to function. This dramatically reduces the attack surface and, most critically, **contains threats by preventing lateral movement**.

If an attacker compromises a single workload in a properly segmented environment, they are trapped. They cannot scan the network, they cannot discover other systems, and they cannot spread their malware. The "blast radius" of the attack is minimized, transforming a potential disaster into a manageable incident.

Contrasting with legacy controls: VLANs and internal firewalls

Older segmentation methods like VLANs and internal firewalls are cumbersome, expensive, and lack the granularity needed for modern environments. They are tied to network topology, making them difficult to manage and impossible to scale in the cloud. Software-defined microsegmentation, like that offered by Akamai Guardicore Segmentation, is decoupled from the network, allowing policies to be applied based on workload identity (e.g., application name, environment, role) and to follow the workload wherever it goes.

A deep dive: Mapping the Akamai Guardicore platform to the five pillars of DORA

The unified, AI-driven Akamai Guardicore platform directly addresses the requirements of each of DORA's five core pillars, with microsegmentation as the foundational control.

Pillar 1: Article 9 (Prevention and Protection): Proactive ICT Risk Management

DORA requires a comprehensive ICT risk management framework to identify, classify, protect, and monitor all ICT assets and to implement security policies based on risk.

The challenge: You cannot protect what you cannot see. Hybrid environments are rife with blind spots, making it impossible to understand dependencies and map risk.

The Akamai solution:

- **Microsegmentation (core control):** The journey begins with visibility. The Akamai Guardicore platform provides a real-time, interactive map of your entire IT ecosystem, visualizing every application, workload, and data flow across on-premises, cloud, and container environments. This eliminates blind spots and provides the foundational understanding for risk management. From this map, our **AI-powered Generative Policy Engine** recommends granular microsegmentation policies. This allows you to:
  - **Isolate critical assets:** Create secure enclaves around "crown jewel" applications like SWIFT or payment gateways.
  - **Enforce least privilege:** Ensure workloads can only communicate with explicitly authorized assets, preventing unauthorized lateral movement.
  - **"Virtually patch" legacy systems:** Protect unpatchable systems by creating a protective bubble around them, blocking access to vulnerable ports.
- **DNS firewall:** As an additional layer of risk reduction, our integrated DNS firewall prevents workloads from communicating with known malicious domains, blocking command and control (C2) callbacks and phishing attempts at the earliest stage.

Pillar 2: Article 11 (Response and Recovery): Rapid ICT-Related Incident Management

DORA mandates robust processes to detect, manage, classify, and report on ICT-related incidents promptly and effectively.

The challenge: In a flat network, detecting an active breach is difficult, and containment is often slow and manual, allowing attackers ample time to spread.

The Akamai solution:

- **Microsegmentation (core control):** By design, microsegmentation is the ultimate incident response tool. It contains the breach to the initially compromised asset. Furthermore, it allows security teams to **instantly quarantine a workload**, programmatically severing all network connections to contain a threat while investigation proceeds.
- **Threat hunting (Hunt service):** Our platform's rich data telemetry feeds the Akamai Hunt team, a service of dedicated experts who proactively hunt for hidden threats, misconfigurations, and policy violations within your environment, acting as a powerful extension of your security team to find incidents that other tools miss.

Key metrics

152% ROI

70% reduced risk

6-month payback

Akamai Guardicore Segmentation delivers measurable business value with rapid payback and significant risk reduction, validated by independent analysis.

> **DORA changes how financial institutions must think about cyber risk. Microsegmentation enables organizations to limit blast radius, protect critical assets, and operate securely — even during a cyberattack.**

Pillar 3: Continuous Digital Operational Resilience Testing

DORA requires financial entities to conduct regular, advanced testing of their ICT systems, including threat-led penetration testing (TLPT) for critical entities.

The challenge: Testing must go beyond simple vulnerability scanning to validate that security controls and response plans actually work under pressure.

The Akamai solution:

- **Microsegmentation — A detailed map of your system:** The Akamai Guardicore platform map provides a real-time view of your security posture, allowing you to continuously validate that segmentation policies are being enforced as intended.
- **Integrated deception:** The platform includes integrated deception capabilities, deploying decoys that mimic real assets. Any interaction with a decoy is a high-fidelity alert that an attacker is active. This serves as a powerful tool for testing and validation, allowing red teams to safely simulate attack paths and confirm that containment policies work as expected.
- **AI assistant:** Security teams can use natural language to query the platform (e.g., "Show me all blocked traffic to the production database"), dramatically speeding up the data gathering required for testing and audits.

Pillar 4: Comprehensive ICT Third-Party Risk Management

DORA places significant emphasis on managing the risks associated with the ICT supply chain, requiring entities to have contractual arrangements and security controls in place for their third-party providers.

The challenge: Third parties, from cloud providers to fintech partners, require access to your network, but this access often grants far more trust than is necessary.

The Akamai solution:

- **Microsegmentation — map of data flows:** Visualize and control all data flows between your environment and your third-party partners. Apply specific, least-privilege segmentation policies to third-party connections to ensure they can only access approved applications and data.
- **Zero Trust Network Access (ZTNA) and multi-factor authentication (MFA):** The Akamai Guardicore platform includes a fully integrated ZTNA solution (Enterprise Application Access) and supports MFA. This allows you to provide granular, application-level access to contractors and vendors without giving them broad network access via a traditional VPN, perfectly aligning with a Zero Trust approach to supply chain security.

Pillar 5: Actionable Information and Intelligence Sharing

DORA encourages participation in trusted communities and arrangements for sharing cyberthreat information and intelligence.

The challenge: Threat intelligence is often just a passive feed of data that is difficult to operationalize into active defenses.

The Akamai solution:

- **Microsegmentation — reputation feeds:** The Akamai Guardicore platform can operationalize threat intelligence. You can integrate reputation feeds to automatically create policies that block communication with known malicious IPs, turning intelligence into an active defense.
- **Platform intelligence:** You benefit from the vast threat intelligence gathered from Akamai's global network, one of the world's largest distributed computing platforms. This intelligence actively powers our **DNS firewall** and informs our **Hunt** team, providing a powerful community-based defense.

Comprehensive support for all five DORA pillars

While articles 9 and 11 are central, the Akamai Guardicore platform supports all five DORA pillars, including **Digital Operational Resilience Testing** (via integrated deception), **ICT Third-Party Risk Management** (via integrated ZTA), and **Information and Intelligence Sharing** (via operationalized threat intelligence).

How microsegmentation strengthens resilience



Contains lateral movement



Reduces attack surface by 70%



Protects legacy systems



Enables Zero Trust policies



Visualizes all application flows

Practical application: Key use cases for DORA compliance

Protecting "crown jewel" applications: Use microsegmentation to create a secure enclave around your most critical systems, such as SWIFT infrastructure, payment processing applications, or core banking platforms. Policies can ensure these systems only communicate with explicitly authorized sources over approved protocols, effectively making them invisible to the rest of the network.

Securing legacy systems: Many financial institutions rely on legacy systems that can no longer be patched. Microsegmentation allows you to "virtually patch" these systems by creating a protective bubble around them, blocking access to known vulnerable ports and services without touching the underlying system itself.

Controlling cloud and container environments: In dynamic cloud and Kubernetes environments where IPs are ephemeral, traditional security fails. Our identity-based policies attach to the workload itself, ensuring that security persists regardless of how the application is scaled or where it is moved.

Consider:

How resilient is your current architecture?

Can your network withstand internal breaches?

Are your crown jewels fully isolated?

From theory to practice: Voices from the financial front line

The effectiveness of this approach is validated by leading financial institutions that are already on their DORA compliance journey.

Achieving regulatory confidence: Proving compliance to regulators is a key challenge. As one **major European bank** stated, "Regulators expect an increasingly secured network, and with the ability to rapidly secure essential applications individually that we've gained via Guardicore, we've been deemed by regulators to be on the right track." This demonstrates that a microsegmentation strategy is not just technically sound but is recognized by regulatory bodies as a valid and effective approach to resilience.

Unprecedented speed in incident response: The ability to respond swiftly during a crisis is the ultimate test of resilience. After a major global supply chain attack, a **global systemically important bank** reported: "It took us 10 min to identify and disconnect servers affected with Solarwinds." This is a powerful, real-world testament to how visibility and segmentation can transform incident response from a days-long process into a matter of minutes.



Digital transformation has expanded the financial sector's attack surface, making traditional perimeter defenses insufficient. DORA mandates a proactive, intelligence-driven approach to operational resilience that assumes breach and demands containment. Microsegmentation plays a pivotal role by enforcing least-privilege communication, isolating critical applications, and preventing lateral movement. With Akamai Guardicore Segmentation, organizations gain a unified platform for visibility, policy enforcement, threat detection, and testing. Its identity-based controls extend seamlessly across data centers, multicloud environments, and containers, ensuring consistent protection everywhere. By operationalizing Zero Trust principles, financial institutions can significantly reduce risk and maintain continuity — even during complex cyberattacks.

The Akamai advantage: Simplifying segmentation, accelerating resilience

Historically, microsegmentation projects have been perceived as complex and slow. Akamai has fundamentally changed this reality.

An AI-driven workflow: Our platform simplifies every stage of the segmentation journey. **AI labeling** helps identify and classify workloads automatically. The **Generative Policy Engine** provides intelligent, easy-to-understand policy recommendations. **Essential policies** provide immediate risk reduction from day one. And the **AI assistant** allows you to manage and investigate your environment using natural language.

Quantifiable business outcomes: The value of this approach is proven. A 2024 Forrester Consulting Total Economic Impact™ study commissioned by Akamai found that a composite organization using Akamai Guardicore Segmentation achieved:

- **152% return on investment (ROI)**
- **A payback period of less than 6 months**
- **70% reduction in the attack surface**
- **$4.1M in avoided downtime costs** due to preventing security breaches
- **70% net reduction in incident management effort** by Year 3
- **$1.4M savings** over three years due to streamlined cybersecurity operations

Stop the spread with Zero Trust controls

Microsegmentation is the cornerstone of a modern Zero Trust security model. By isolating applications and restricting communication to only what is explicitly required, organizations dramatically limit an attacker's ability to move laterally. Akamai Guardicore Segmentation provides the visibility and automated policy creation needed to enforce segmentation at scale across hybrid environments. This reduces operational risk, strengthens DORA compliance, and ensures resilience even when a breach occurs.

Conclusion: Building a resilient future, today

DORA should not be viewed as a compliance burden, but as a catalyst for transformation. It is an opportunity to move away from outdated, perimeter-based security and embrace a more effective, resilient Zero Trust architecture. By building your DORA strategy on a foundation of **microsegmentation**, you can gain the visibility to manage risk, the control to contain incidents, and the evidence to prove resilience.

Akamai provides the foundational platform to navigate the complexities of DORA, empowering your organization to not only meet the regulatory requirements but to emerge stronger, more agile, and fully prepared to stop the spread of malicious software.

To learn more about how the Akamai Guardicore platform can accelerate your journey to DORA compliance, visit us at akamai.com.

Akamai is the cybersecurity and cloud computing company that powers and protects business online. Our market-leading security solutions, superior threat intelligence, and global operations team provide defense in depth to safeguard enterprise data and applications everywhere. Akamai's full-stack cloud computing solutions deliver performance and affordability on the world's most distributed platform. Global enterprises trust Akamai to provide the industry-leading reliability, scale, and expertise they need to grow their business with confidence. Learn more at akamai.com and akamai.com/blog, or follow Akamai Technologies on X and LinkedIn. Published 02/26.