White Paper

NIS2 Compliance in the AI Age

Four key challenges for organisations — and how segmentation addresses them all

Akamai Security

Akamai Security

Contents

Executive summary 3

Rapid breach containment 5

Supply chain risk mitigation 7

Operational continuity and minimised disruption 8

Simplified audits, compliance, and reporting 10

An at-a-glance summary 12

Executive summary

The NIS2 directive has prioritised cybersecurity in European boardroom agendas, introducing personal executive accountability and a strict 24-hour incident reporting window. In an era where AI-driven attacks compress exploitation timelines from days to minutes, perimeter defences and static compliance are no longer sufficient.

We live in a hyperconnected economy in which stopping every attack is unrealistic. Today's organisations require a dynamic safety net that actively contains threats and provides instant, provable visibility into a breach's blast radius to protect leadership from liability claims.

In this paper, we explore four key areas that organisations find particularly challenging when working towards NIS2 compliance.

1. Evidencing their ability to limit the impact of a breach
2. Having confidence in supply chain security
3. Being able to guarantee business continuity
4. When an attack happens, rapidly disclosing the details and impact

We show how segmentation — done right — can address all four of these challenges, providing fast and automated containment, maintaining business continuity, and supporting NIS2 compliance efforts.

Providing evidence to support compliance and accountability

The introduction of NIS2 has brought cybersecurity to the fore in more boardrooms across Europe — an important move for the continuity of critical services. In today's world, where machine-speed threats outpace human defences, perimeter-based security and checkbox compliance aren't enough.

Now, the real challenge for impacted organisations is: How do you *prove* your internal defences are working?

With personal executive accountability on the line and a 24-hour window to report significant incidents, point-in-time compliance has become a risk rather than a defence. True operational resilience relies on dynamic risk containment that's fit for an age where the time to exploit an attack using AI and ransomware has gone from days to minutes.

Premier segmentation can address all of these challenges. Traditional segmentation relied on a complex, static infrastructure that worked at human speed, which no longer meets organisational needs, including:

- A safety net that doesn't just watch for threats but actively contains them before they become catastrophes
- An adaptive, automated risk-containment framework
- Continuous exposure analysis

Research indicates that the EMEA region experiences the highest global incidence of ransomware but has the weakest segmentation maturity globally. Attackers are exploiting vulnerabilities faster than humans can patch them. On top of that, organisations are struggling to integrate legacy systems across hybrid work environments and AI-driven expansion.

Akamai Guardicore Segmentation transforms this approach: It rapidly defines breach impact boundaries within the 24-hour NIS2 reporting window and provides evidence that can help support executives' compliance and accountability obligations.

Four key challenges around NIS2 compliance in the AI era

1. Containing breaches rapidly.
2. Mitigating supply chain risk
3. Guaranteeing business continuity
4. Simplifying audits and reporting

This paper explores these specific challenges and demonstrates how segmentation supports compliance, protecting leadership and essential services.

1. Rapid breach containment

The challenge

Under NIS2, companies must prove they can contain a breach to prevent societal or economic impact, using "appropriate and proportionate technical measures".

Common obstacles to achieving NIS2 compliance include:

- Siloed security teams using different tools for cloud native assets versus on-premises data centres, leading to visibility gaps
- Difficulty prioritising threats due to security tools surfacing high volumes of alerts without business context
- Rapid lateral movement in AI-driven attacks, which expand before internal teams can detect and respond
- Static network choke points that cannot adequately segment dynamic workloads, Kubernetes environments, or east-west cloud traffic
- Exposure analysis and response (ExAR) capabilities operating independently of enforcement mechanisms, preventing automated risk containment
- Policies that drift as underlying infrastructure changes, creating unmapped exposure paths

With the ever-increasing reliance on AI for high value tasks, it's never been more important for organisations to have a containment-first security model that ensures breaches cannot spread beyond the initial compromise. Teams need support with prioritisation, so they can focus on containing assets that pose a risk, rather than evaluating severity scores.

How segmentation provides the solution

AI-driven attacks can be halted faster with AI-powered containment. To this end, we've developed Akamai Guardicore Segmentation, a platform that's software-defined and asset-centric. It's designed for hybrid infrastructure and functions across cloud, data centre, Kubernetes, operational technology (OT), and AI workloads. By capturing full-stack telemetry, from the network packet down to OS processes and DNS requests, the platform ensures segmentation is based on real behaviour and continuously validated against emerging exposure paths.

Threat alerts are prioritised by calculated blast radius and business impact, reducing alert fatigue. Akamai Guardicore Segmentation feeds its findings directly into automated policies to contain threats before they can spread. This AI-driven automation accelerates the dependency mapping that frequently delays traditional segmentation projects.

The goal is no longer to stop every attack — it is to control how far attacks can spread. With Akamai Guardicore Segmentation, when a breach occurs, it can be contained in alignment with the chosen segmentation, and then breach mitigation actions can be taken as appropriate, including timely reporting as expected under NIS2.

2. Supply chain risk mitigation

The challenge

Historically, security incidents originating from a direct supplier, maintenance contractor, or cloud vendor were treated as external issues and managed through legal frameworks and insurance policies. Under NIS2, that loophole is closed. Senior leadership must ensure the organisation complies with NIS2 requirements, including supply chain security management, and can be held accountable for failures to do so.

How segmentation provides the solution

Proper segmentation keeps operations running smoothly even when a third-party business partner is compromised. Rather than relying on network-edge access controls such as VPNs — which historically grant broad, implicitly trusted access once breached — organisations must restrict vendor access to only the specific servers or applications required for their contracted use.

Akamai Guardicore Segmentation makes this simple through identity-driven, asset-centric microsegmentation. Security teams can create granular policies based on user identity and application labels, so a compromised vendor credential can only reach its designated workload on a specific port — sharply limiting the potential for lateral movement into critical infrastructure.

Critically, the platform's real-time visual mapping gives regulators and auditors clear evidence that third-party connections are enforced on a least-privilege basis and remain verifiably isolated. For higher-risk vendor connections, Akamai Guardicore Segmentation's Multi-Factor Segmentation (MFS) capability goes a step further, embedding MFA directly into the segmentation policy itself. Rather than authenticating once at a network perimeter, a vendor identity is challenged at the connection level, for the specific service or port being accessed.

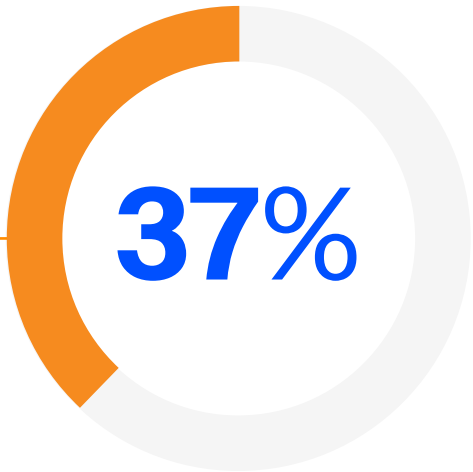
3. Operational continuity and minimised disruption

The challenge

NIS2 isn't just about data privacy. It's about protecting the critical services provided by sectors such as financial services, energy, water, and transportation, which have all experienced cybersecurity breaches in recent years. These events have posed a significant threat to the broader economy, critical infrastructure, and public safety. They also, clearly, have a huge impact internally in the affected organisations. In many cases, the time it takes to detect and respond to an incident is what exposes the business to prolonged operational disruption.

An effective way to speed up response time — and assist with NIS2 compliance — is by adopting microsegmentation. But we know that fear of *causing* business disruption is the single biggest obstacle to taking that step. Given that only 37% of enterprises report shared ownership of segmentation between security and infrastructure teams, it's clear that segmentation is frequently managed in silos, leading to action paralysis.

37% of enterprises report shared ownership of segmentation between security and infrastructure teams



How segmentation provides the solution

Business risk can be reduced by combining segmentation with automated detection, response, and exposure analysis and management. By learning how applications behave, the segmentation platform can understand real communication paths, and identify what is truly reachable and exploitable. It is then able to automate the enforcement steps that typically require manual intervention during an active incident.

Akamai Guardicore Segmentation is the first platform to do this. And because Akamai understands the fear that exists around “breaking” applications, the platform utilises a simulation-first deployment model. Security policies run in a draft mode using live traffic, allowing teams to mathematically validate that a rule will not disrupt applications before activating a block command. In this way, Akamai Guardicore Segmentation allows teams to spend less time writing rules and enforce with confidence, leading to faster Zero Trust adherence and lower costs.

The platform includes an application owner portal that allows business unit managers to review and validate specific connection rules. This cross-departmental validation supports the strict containment measures mandated by NIS2, without interrupting operations.

Akamai Guardicore Segmentation also enables secure AI adoption, ensuring high-value model assets and sensitive datasets are not exposed to unnecessary lateral access, even as GPU infrastructure scales. It stops the spread phase, drastically reducing the impact of security incidents.

The system is designed to continuously learn application behaviour, map dependencies, and generate precise segmentation policies for human approval. This consistent policy enforcement works across on-premises, cloud, and container platforms from a single control plane, removing the security gaps caused by architectural silos.

4. Simplified audits, compliance, and reporting

The challenge

C-level executives are now personally accountable for NIS2 compliance, and organisations must report any significant incident within 24 hours of becoming aware of it. Auditors and senior leadership want continuous assurance that controls are capable of containing real threats.

Traditional executive reporting on cybersecurity focuses on alerts and vulnerabilities, but a long list of unpatched vulnerabilities doesn't tell the board what actually poses a threat to your critical business functions. Traditional endpoint tools can isolate a single machine, but they lack the network and workload context to instantly contain a breach's blast radius across a hybrid cloud or data centre infrastructure.

Static maps and raw flows from legacy tools do not capture real risk. Rather than needing proof that tools have been deployed, executives require clear visibility into exposure and attack paths, and evidence that security controls are actively and continuously reducing operational risk.

> **When ANSSI [France's National Cybersecurity Agency] demands an incident report within 24 hours, you cannot afford to spend three days performing manual network discovery to see what was hit. You must have instant, provable visibility into your blast radius.**
>
> Yann Fralo, Regional Sales Manager, Akamai

How segmentation provides the solution

In this age, organisations need a segmentation platform that can translate technical telemetry into risk-aligned, executive-level reporting. This both fulfils the primary criteria for NIS2 auditors and provides a measurable reduction in business risk.

This is something that Akamai addresses. Organisations can easily demonstrate control over hybrid and regulated environments without manual documentation or brittle rulesets. Instead of showing an auditor thousands of lines of firewall code, Akamai Guardicore Segmentation provides an intuitive, real-time visual map as proof of isolation and least-privilege enforcement.

Furthermore, the Insight Query feature with ExAR allows teams to use simple, natural language searches to instantly assess the blast radius of an incident. It provides the exact data needed to help meet the strict 24-hour NIS2 reporting window without days of manual forensic work.

It also drastically speeds up the adoption of microsegmentation. While legacy segmentation can take years, Akamai Guardicore Segmentation uses AI-powered labelling and templates to reach NIS2-ready segmentation status in weeks, which reduces the window of regulatory exposure for the board.

Finally, it provides the required containment infrastructure for high-value AI training clusters, mitigating risks such as an expanded blast radius, unauthorised data exfiltration, and illicit model access.

An at-a-glance summary

NIS2 challenges	NIS2 article	Traditional approach	Akamai Guardicore Segmentation
Breach containment	Articles 21(1) and 21(2)(f)	Static perimeters and choke points overlook east-west cloud/ Kubernetes traffic	Software-defined, asset-centric microsegmentation that stops lateral drift
Supply chain security	Article 21(2)(d)	Treating vendor vulnerabilities as a legal or insurance risk	Software-defined, least-privilege Zero Trust access that strictly restricts third-party vendors to assigned server assets MFA at the connection level, so stolen credentials alone can't grant access
Operational continuity	Article 21(2)(c)	Action paralysis driven by fear of breaking the business	A simulation-first deployment engine to test draft policies against live traffic
Accountability	Article 23	Manual network discovery requires multiple days to identify compromised assets	Instant, natural-language scoping of a breach's blast radius and rapid policy enforcement to satisfy 24-hour reporting mandates Real-time visual mapping to replace lines of code

Microsegmentation for AI-powered breach containment

The NIS2 directive has shifted personal accountability into the boardroom. And when it comes to cybersecurity attacks, AI has fundamentally changed the equation. Vulnerabilities can be discovered, weaponised, and exploited in minutes, eliminating the response window organisations once relied upon. In our hyperconnected global economy, an organisation's digital footprint extends to its supply chain, cloud environments, OT networks, and high-value AI training clusters. Everything is deeply intertwined.

Today's organisations need a dynamic, automated safety net that ensures the business keeps running even when a breach occurs, and the ability to provide almost instant evidence of rapid containment.

Granular segmentation can successfully address all of these challenges, but any platform that organisations adopt needs to be designed for how cybersecurity is today, and how it's set to evolve.

Akamai Guardicore Segmentation is an industry-leading microsegmentation platform that protects organisations from the next generation of sophisticated cyberthreats while supporting NIS2 compliance. It provides rapid, AI-powered breach containment, reduces supply chain risk, is quick to adopt compared to legacy tools, and actively supports business continuity rather than disrupting it.

Shifting the security focus

Akamai Guardicore Segmentation fundamentally changes the game by accelerating microsegmentation deployment and shifting the security focus from stopping every attack to controlling how far it can spread.

It supports NIS2 compliance across four critical pillars:

Rapid AI-powered breach containment

The asset-centric platform captures full-stack telemetry across hybrid workloads. It automatically isolates threats based on calculated business impact, stopping rapid lateral movement.

Supply chain risk mitigation

Akamai Guardicore Segmentation restricts vendor access to specific, required servers and provides the visual mapping necessary to prove critical infrastructure is isolated.

Operational continuity

To eliminate the action paralysis caused by fear of disrupting business operations, the platform utilises a simulation-first deployment model. Security teams can mathematically validate draft rules against live traffic before activation.

Simplified audits and reporting

Akamai Guardicore Segmentation provides real-time visual maps that serve as proof of isolation for auditors. It translates technical telemetry into risk-aligned, executive-level reporting, delivering continuous assurance of compliance.

In an AI-driven world, preventing every attack is unrealistic — but controlling the outcome is not.

Accelerate your NIS2 readiness with automated microsegmentation. See Akamai Guardicore Segmentation in action and learn how to secure critical assets in minutes.

Schedule a custom assessment.

Notice: The information provided here is for general informational purposes only. It should not be construed as legal advice and does not create any commitments from Akamai. Laws and regulations can vary, and legal interpretations may change over time. No guarantees are made regarding the accuracy, completeness, or suitability of the information provided. If you require legal advice or have specific legal concerns, please consult with a qualified legal professional who can provide advice tailored to your situation and jurisdiction.

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 08/26.