White Paper *Feb 2026*

NIS2: The Hour of Responsibility

How companies can implement cybersecurity effectively now – and why the browser plays a key role

Island

The Enterprise Browser

Table of Contents

1. **Foreword**

Prof. Dr. Dennis-Kenji Kipker
Positioning NIS2 as a turning point for cybersecurity, responsibility at the executive level, and urgency of implementation

2. **NIS2 at a glance – what it means for companies**

Classification of the directive, expanded scope, core obligations, and organizational and operational implications for companies

3. **The blind spot of traditional security architectures**

Why existing security approaches reach their limits at the interface between the user and application – and why the browser has so far been underestimated

4. **The Enterprise Browser as an answer to NIS2**

The Enterprise Browser as a new security layer and an element of prevention, making attacks visible, and concrete support for the NIS2 reporting phases (24 hrs / 72 hrs / 1 month)

5. **Compliance, cost, and resources – why NIS2 does not have to reduce efficiency**

The widespread misconception of compliance as a cost factor, compliance through architecture instead of checklists, effects on cost and operations, reducing organizational burdens, and investing in controllability

6. **Conclusion and outlook – from obligation to control**

Bringing together regulation, architecture, and practice, and the role of the Enterprise Browser for sustainable cyber resilience

7. **Sources**

1. Foreword

With the NIS2 Directive, Europe is entering new territory in security policy. Not because the threat landscape is new, but because legislators are now drawing comprehensive consequences from it. Cybersecurity is no longer treated as a technical specialist topic, but as a leadership responsibility. Accountability gains a name, an address, and a deadline.

This is a necessary step. The past years have shown that voluntary standards and isolated measures are not enough. Attacks are becoming more professional, more interconnected, and faster. At the same time, companies are more digitally dependent than ever before. In this environment, anyone who merely delegates security loses control. NIS2 helps companies acknowledge this reality.

The directive pursues two key objectives. First, it aims to sharpen security awareness within organizations – not abstractly, but concretely. Cybersecurity becomes a matter of organizational design, responsibilities, and decision-making processes. Second, NIS2 aims to improve the quality of implementation. Rules only have impact if they can be implemented in practice and verified. This has so far been one of the greatest weaknesses of European IT security law.

NIS2 makes IT security a leadership responsibility

NIS2 therefore deliberately places responsibility at the executive level. Managing directors must understand risks, initiate measures, and report incidents. They must be able to explain what happened, why it happened, and what will be done differently going forward. This is not a vote of no confidence in companies. It is a realistic response to the fact that cybersecurity does not happen on the side – it must be actively governed.

It quickly becomes clear: responsibility without control remains ineffective. Anyone required to report within 24 hours needs processes. Anyone required to report within 72 hours needs reliable data. And anyone expected to explain after one month what lessons were learned needs systems that not only protect, but also document events in a comprehensible way. The NIS2 Directive therefore demands more than technology and organization. It demands controllability of cyber risks.

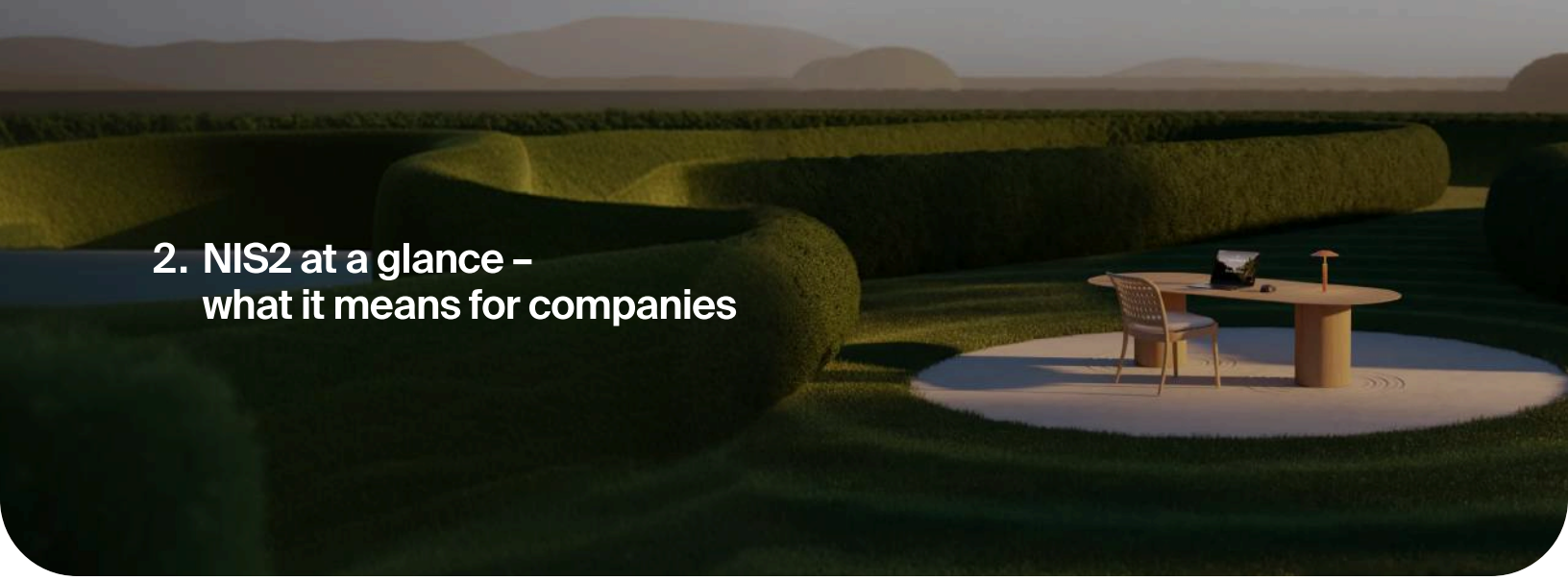
For many companies, this means a change in perspective. Security architectures have long been built around infrastructure: servers, networks, clouds. The place where attacks begin was often overlooked: the digital workplace, the browser, the interface between humans and systems. Yet this is precisely where it is decided whether security is effective – or exists only on paper.

2026 is not a transition year in this context. It is the beginning of practical enforcement. Supervision, reporting obligations, and liability questions will become reality. Companies that hesitate today will have to react tomorrow – under time pressure, under regulatory scrutiny, and with significant risks to reputation and operations. That is why now is the right time to build reliable and sustainable structures instead of fighting symptoms later.

This white paper does not aim to explain a piece of legislation. It aims to show how the requirements of the NIS2 Directive can be implemented in practice. It is directed at decision-makers who carry responsibility and are looking for solutions that combine security, compliance, and feasibility. Because NIS2 will not be measured by how well the directive is written, but by whether it actually improves the digital resilience of companies at scale.

Prof. Dr. Dennis-Kenji Kipker

Frankfurt, January 2026



2. NIS2 at a glance – what it means for companies

What is the Enterprise Browser?

NIS2 marks a clear break with previous practice in IT security regulation. The directive is less a technical rulebook than an organizational and leadership framework. It no longer primarily asks for individual safeguards, but whether companies can control their overall digital dependency. Risks should be identified, decisions made transparently, and incidents handled in a structured manner.

In doing so, legislators are responding to a development that has long been reality. Cyberattacks are no longer exceptional events. They are part of everyday life. At the same time, business processes, supply chains, and value creation are deeply digitally interconnected. Outages rarely remain local. NIS2 accepts this situation and draws consequences from it. Security becomes an ongoing task and a question of corporate governance.

More companies affected

One central difference to earlier frameworks lies in the expanded scope. NIS2 is no longer limited to a narrow group of traditional critical infrastructure organizations. The circle of affected organizations is significantly expanded to around 30,000 companies. Many that previously did not consider themselves security-critical must now deal with binding requirements for the first time. Size, economic relevance, and societal role are decisive.

Substantively, NIS2 consolidates requirements into three closely interlinked areas.

Companies must:

1. **Systematically manage risks**
2. **Report security incidents within clearly defined timeframes**
3. **Anchor responsibility at the executive level**

Risk management means more than technology. What is required are appropriate organizational and technical measures that are documented, reviewed, and adapted. Reporting obligations follow a fixed timeline: an initial assessment within 24 hours, a qualified interim report after 72 hours, and a final report including root-cause analysis and remediation measures within one month. At the same time, supervisory authorities are granted significantly expanded audit and intervention powers.

The full security "keyboard:" from prevention to proof

For companies, this represents a noticeable shift in perspective. Prevention alone is no longer sufficient. Responsiveness becomes equally important. The question is no longer whether an incident can be prevented, but rather how quickly an organization can respond in a controlled and transparent manner. Documentation thus becomes not an end in itself, but a prerequisite for operational capability. Those who must report need reliable information. Those who are responsible need transparency.

These requirements cannot be fulfilled by a single department. NIS2 affects the entire organization. The following areas are especially challenged:

- **Executive management**
  This group bears overall responsibility. NIS2 explicitly addresses leadership because security does not work without prioritization, resources, and clear responsibilities.

- **IT and information security**
  They identify risks, implement technical and organizational measures, and provide the data for decisions and reports. Their role becomes more operational and more visible.

- **Compliance and legal**
  They align teams on deadlines, structure documentation, and ensure measures are regulatorily robust. Without this function, NIS2 quickly becomes a liability risk.

- **Communications and crisis management**
  They prepare external and internal communication. Reporting obligations mean not only technology, but also clear, consistent information to authorities and stakeholders.

NIS2 is therefore not an IT project and not a pure compliance topic. It is an organizational initiative. Companies that try to fulfill the requirements in isolation will fail. The real challenge lies not in the regulation itself, but in practical implementation.

This is exactly where a weakness of many existing security architectures becomes apparent. They protect infrastructure but often do not provide end-to-end visibility into what actually happens in day-to-day operations. They detect incidents, but not always their origin. A gap emerges between aspiration and reality. How this gap can be closed – and why the browser plays a central role – is the focus of the next chapter.

3. The blind spot of traditional security architectures

Most modern attacks do not begin in the data center. They begin with the user. With a click. A login. A file. A website. The browser is now the central access point to applications, data, and processes. It is a workspace, integration layer, and entry point at the same time.

Yet the browser remains a blind spot in many security concepts. It is assumed as a given. A neutral surface. A tool that sits outside the actual security architecture. This is precisely where the gap between aspiration and reality emerges.

Phishing, malware, identity theft, and unauthorized access occur at the interface between humans and applications. Traditional browsers were developed for individual use. They prioritize openness, convenience, and compatibility. Control, traceability, and governance were not design goals.

Why this is a problem for NIS2

NIS2 requires more than protection. It requires controllability. Companies must not only prevent incidents, but also be able to explain them: What happened? Who is affected? Which systems were accessed? Which data may have been compromised?

This is where traditional security architectures reach their limits. They provide signals, but often no context. They report anomalies, but not necessarily causes. That is insufficient for NIS2 reporting obligations.

This gap becomes particularly visible under tight deadlines. Within 24 hours companies must provide an initial assessment. Within 72 hours they must submit a reliable interim report. Anyone who only starts collecting data during this period loses time and control.

Fragmentation as a structural risk

Another issue is the fragmentation of the security landscape. Many companies operate a wide range of specialized tools. Each makes sense on its own. Taken together, however, they become difficult to oversee.

Typical consequences include:

- Delayed root-cause analyses because data has to be consolidated from different systems
- Contradictory information between IT, security, and management
- High operational burden in an incident
- Uncertainty in communication with supervisory authorities

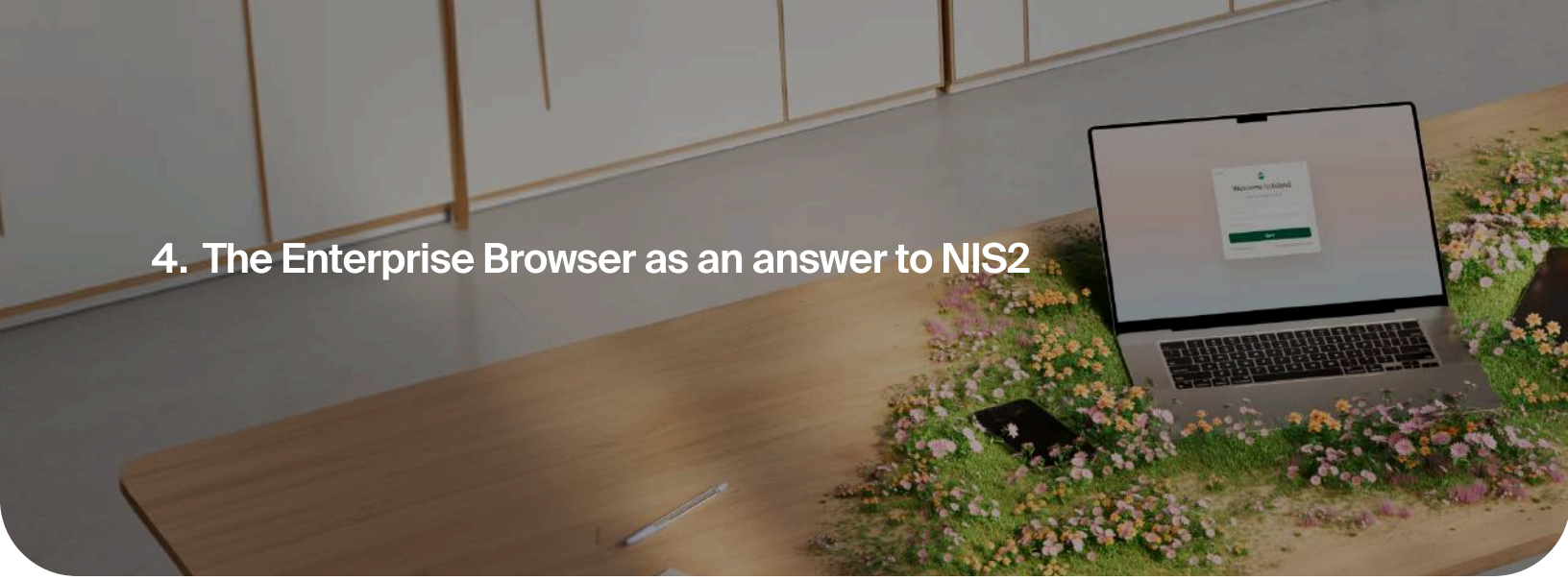
This fragmentation directly contradicts the requirements of NIS2. The directive relies on clarity, speed, and traceability. This is hard to achieve with numerous point solutions.

The digital workplace as a security factor

If NIS2 is taken seriously, the focus shifts away from the question of which systems are protected and toward the question of where decisions, access, and risks actually arise. Today, the digital workplace is where security is either practiced or circumvented. Those who do not control this place do not control the incident. Those who do not see it cannot explain it.

As a result, the browser moves from a side issue to a strategic element of the security architecture. Not as a replacement for existing systems, but as a connecting layer. As the place where security becomes visible, enforceable, and documentable.

What role the Enterprise Browser plays in practice – and why it opens up new possibilities specifically in the context of NIS2 – is the focus of the next chapter.



4. The Enterprise Browser as an answer to NIS2

NIS2 does not demand new security ideals. It demands control. Visibility. Traceability. And it demands that all of this works in everyday operations. This is where the Enterprise Browser comes in. Instead of building security around applications and infrastructures, it anchors security directly at the interface between user, application, and data: where work happens, where decisions are made, and where attacks begin.

An enterprise browser is not just another security tool. It is a new layer in the architecture – a layer that complements existing systems rather than replacing them, and that delivers exactly what NIS2 presupposes: operational controllability.

Prevention as part of everyday work

Many security measures are reactive: they take effect after something has happened. The Enterprise Browser shifts this approach forward. It makes prevention an integral part of working.

Malware downloads are prevented before they can cause damage. Phishing sites are blocked. Password entry is only possible on approved domains. Multi-factor authentication works even for applications that were never designed for it. Privileged access can be secured without integrating additional specialized solutions. External users can be granted controlled access, including to sensitive IT and OT systems.

All of this happens directly in the browser – transparently for users and centrally managed by IT and security

Visibility instead of assumptions

A core requirement of NIS2 is the ability to understand and explain incidents. The Enterprise Browser provides a decisive foundation for this. It makes user activity visible without disrupting the flow of work. Access, logins, and interactions can be traced – not generically, but contextually. This creates a realistic picture of what actually happens in the company: not in a lab, but in everyday operations.

This visibility is critical for reporting obligations. It replaces assumptions with facts and accelerates decision-making in situations where time is the scarcest resource.

Support across the NIS2 reporting chain

NIS2 reporting obligations follow a fixed timeline. The Enterprise Browser supports all three phases without requiring additional tools or special processes.

1. In the early warning phase (within 24 hours), live monitoring from the user perspective enables rapid assessment. Suspicious activity is detected. Access can be revoked immediately. URLs can be blocked. Even in this phase, a reliable overview can be created of which users and systems are affected.
2. In the interim report (after 72 hours), logs and analyses from the central management console provide the basis for reporting. Activities can be placed in time and context. Causes can be narrowed, especially for attacks at user or endpoint level.
3. For the final report (no later than one month), the Enterprise Browser opens additional options for action. Fine-grained access controls and “last-mile” measures enable concrete improvements that can be implemented and documented. An incident becomes a traceable learning process

Less complexity, more controllability

A frequently underestimated aspect of NIS2 is the demand on resources. Fragmented security architectures tie up time, personnel, and budget.
The Enterprise Browser reduces this complexity by bundling multiple functions and integrating them directly. This has effects on several levels:

- Lower integration effort, because security and access functions are anchored in the browser
- Fewer additional agents and specialized solutions
- Clearer responsibilities through central management
- Reduced effort for audits and assessments

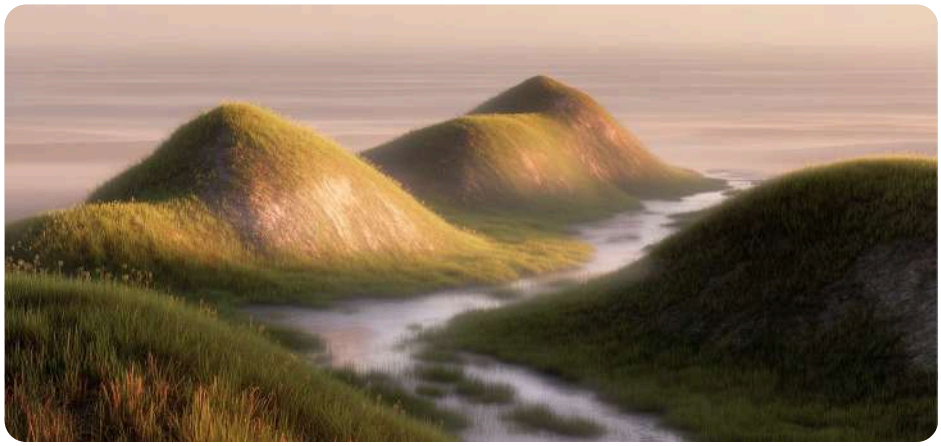
Compliance is thus achieved not through additional processes, but through improved architecture.

From obligation to control

The Enterprise Browser translates NIS2 from a regulatory requirement into a practical capability. Imagine you are in the middle of an active attack and have the ability to immediately exclude affected applications and users from access while the incident is ongoing. Instead of acting purely reactively, you have a tool that allows you to actively contain the threat.

Twenty-four hours later, you do not have to compile fragmented and incomplete information for reporting under time pressure. Instead, you have a detailed, reliable overview of what happened, which systems and users were affected, and all relevant information to share in a structured and secure way with supervisory authorities.

The Enterprise Browser makes security visible. It makes responsibility manageable. And it enables companies not only to respond, but to steer. This turns the browser from an underestimated tool into a strategic building block of cyber resilience: transparent, controllable, and audit-ready.



The Enterprise Browser as an NIS2 enabler – the five key benefits

1 Control where it matters

The Enterprise Browser anchors security directly in the interface between user, application, and data. This creates control where attacks begin and where NIS2 requires transparency.

2 Prevention instead of reaction

Block malware downloads, phishing, and unauthorized access directly in the browser, reducing risks before they become reportable.

3 Meeting reporting obligations under time pressure

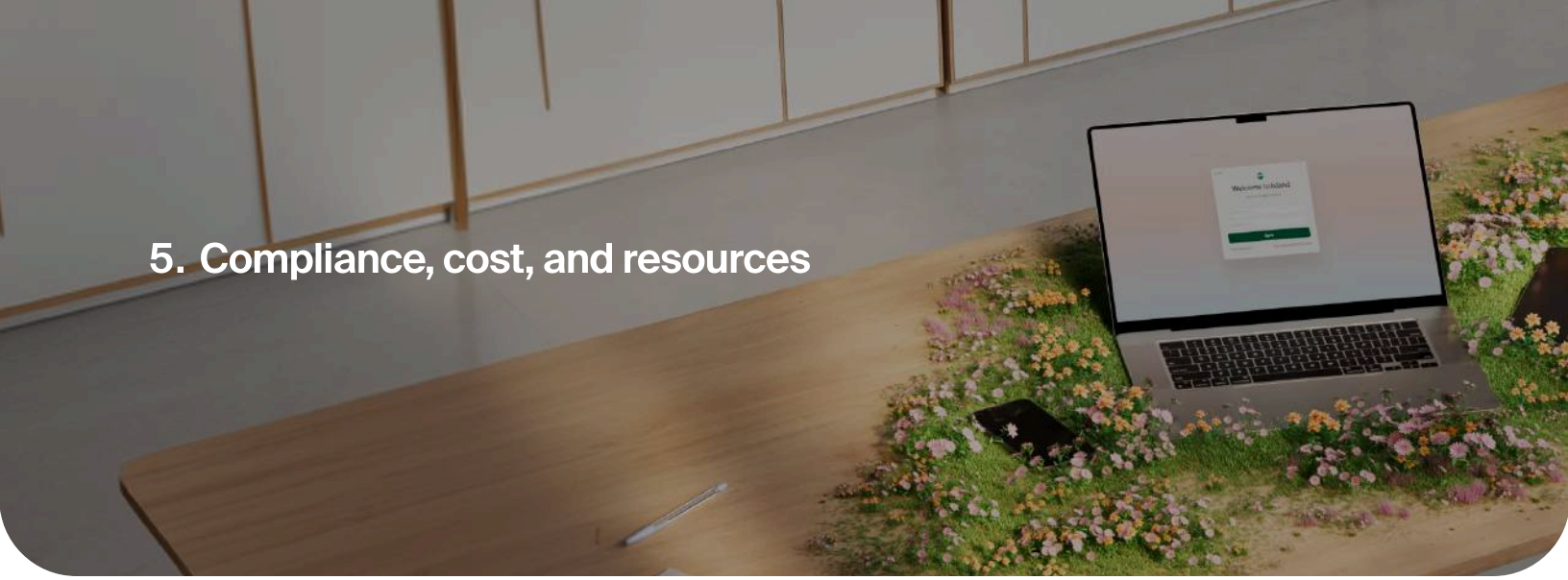
Live monitoring, logging, and analytics enable reliable reporting within 24 hours, 72 hours, and one month – fact-based and traceable.

4 Less complexity, lower resource demand

Security, access, and governance functions are natively integrated. This reduces additional tools, lowers operating costs, and lowers burdens on IT, security, and compliance teams.

5 Auditability and proof

Activities, access, and measures are documented and auditable. Compliance is created during normal operations, not only during audits.



5. Compliance, cost, and resources

Why NIS2 does not have to reduce efficiency

In many companies, regulation is still seen as a necessary evil: additional effort and a brake on business. NIS2 is often viewed in this light. More obligations, more documentation, more control. The concern is understandable, but it falls short. The true cost driver is not regulation. It is the way companies attempt to comply with it.

Fragmented architectures, parallel tools, and manual processes create complexity. This complexity ties up resources, increases the likelihood of errors, and slows decision-making. NIS2 makes this model visible – and therefore risky

Compliance through architecture instead of checklists

The Enterprise Browser fundamentally changes this approach. It shifts compliance from after-the-fact documentation into operational execution. Rules are not merely checked – they are enforced. Evidence is not created in the audit – it is created in everyday work. The effect is straightforward: what happens automatically does not need to be explained manually. What is centrally managed does not need to be reconstructed later. Compliance becomes part of the work environment, not an additional layer on top.

Integrating security, access, and governance functions directly into the browser reduces structural redundancies. Companies need fewer specialized point solutions. Integration effort decreases. Dependency on complex additional infrastructures declines.

In practice, this approach shows several concrete effects. The effort required to operate and maintain distributed security tools decreases noticeably, because central functions are bundled directly in the browser and no longer have to be orchestrated across numerous point solutions. At the same time, training requirements decrease, as employees work in a familiar browser environment and security mechanisms operate in the background without forcing new ways of working.

Costs for additional agents, gateways, or complex VDI solutions can also be reduced, because central access and protection functions are provided natively. In an incident, central management accelerates response actions, and since access can be adjusted immediately, activities can be reviewed and measures can be coordinated and implemented. These effects are not created by reducing security, but by bundling it more effectively.

Reducing organizational burden

A frequently underestimated aspect of NIS2 is the burden on the teams involved. In an incident, IT, security, legal, and management collaborate under significant pressure. The more fragmented the information situation, the higher the coordination effort. The Enterprise Browser provides a shared point of reference. Activities are visible. Access is traceable. Measures are documented. This reduces alignment effort and accelerates decisions.

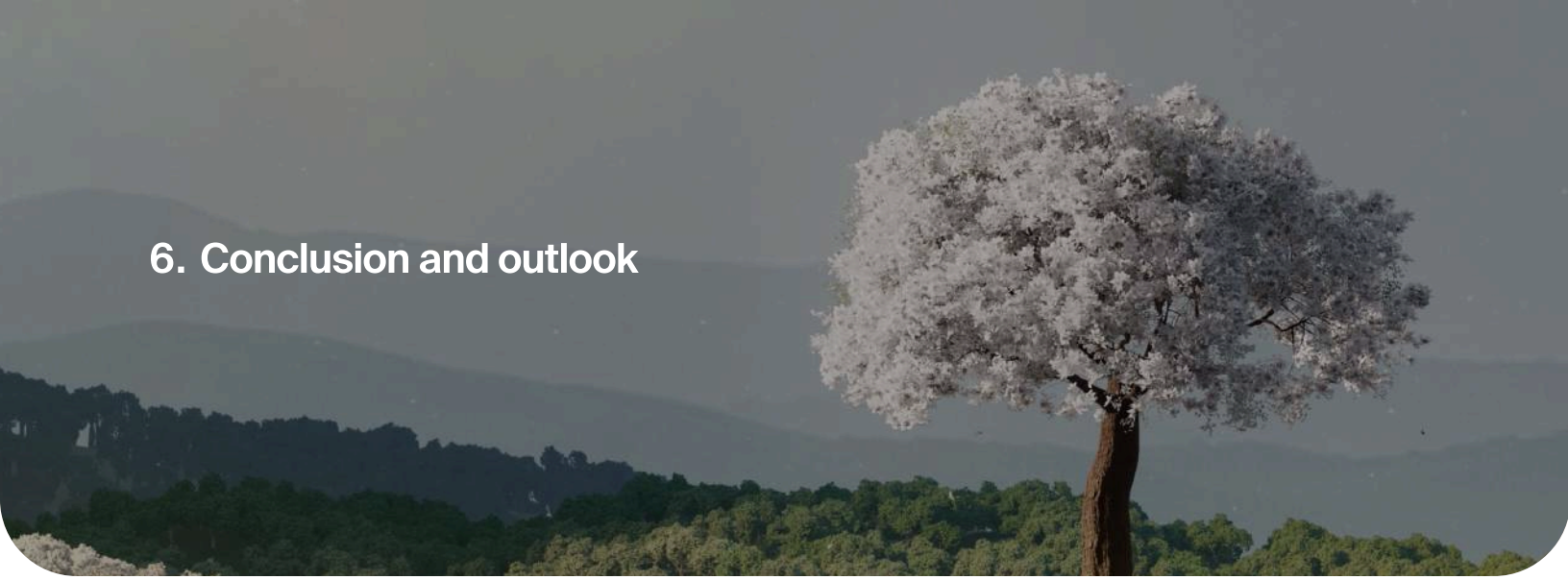
For executive management, this means greater confidence in accountability. For IT and security, less operational chaos. For compliance and legal, a robust basis instead of assumptions.

Investing in controllability

NIS2 forces companies to reassess their security architecture. In this context, the Enterprise Browser is not an additional investment, but a structural decision. It replaces complexity with clarity. It reduces operational friction. And it makes responsibility controllable.

This also changes how compliance is viewed. It is no longer understood merely as an obligation, but also as a capability – a prerequisite for remaining operational under regulatory requirements.

Companies that take this step do not only comply with NIS2. They regain control. And that is exactly what lies at the core of this regulation.



6. Conclusion and outlook

NIS2 is more than a new chapter in IT security law. The directive marks a structural shift. Cybersecurity becomes a leadership responsibility. Accountability becomes concrete. And implementation quality determines whether regulation has real impact or remains stuck in formalism.

For companies, this requires a shift in perspective. Security can no longer be thought of solely in terms of infrastructure. It is created where people work, use applications, and make decisions. Those who do not control this place cannot explain it in an incident. This is exactly where the Enterprise Browser comes in.

The Enterprise Browser translates the abstract requirements of NIS2 into a practical capability. It makes security visible without hindering work. It enables prevention where attacks emerge. And it provides reliable information across the entire reporting chain. Compliance therefore does not become a downstream process, but an integral part of digital work.

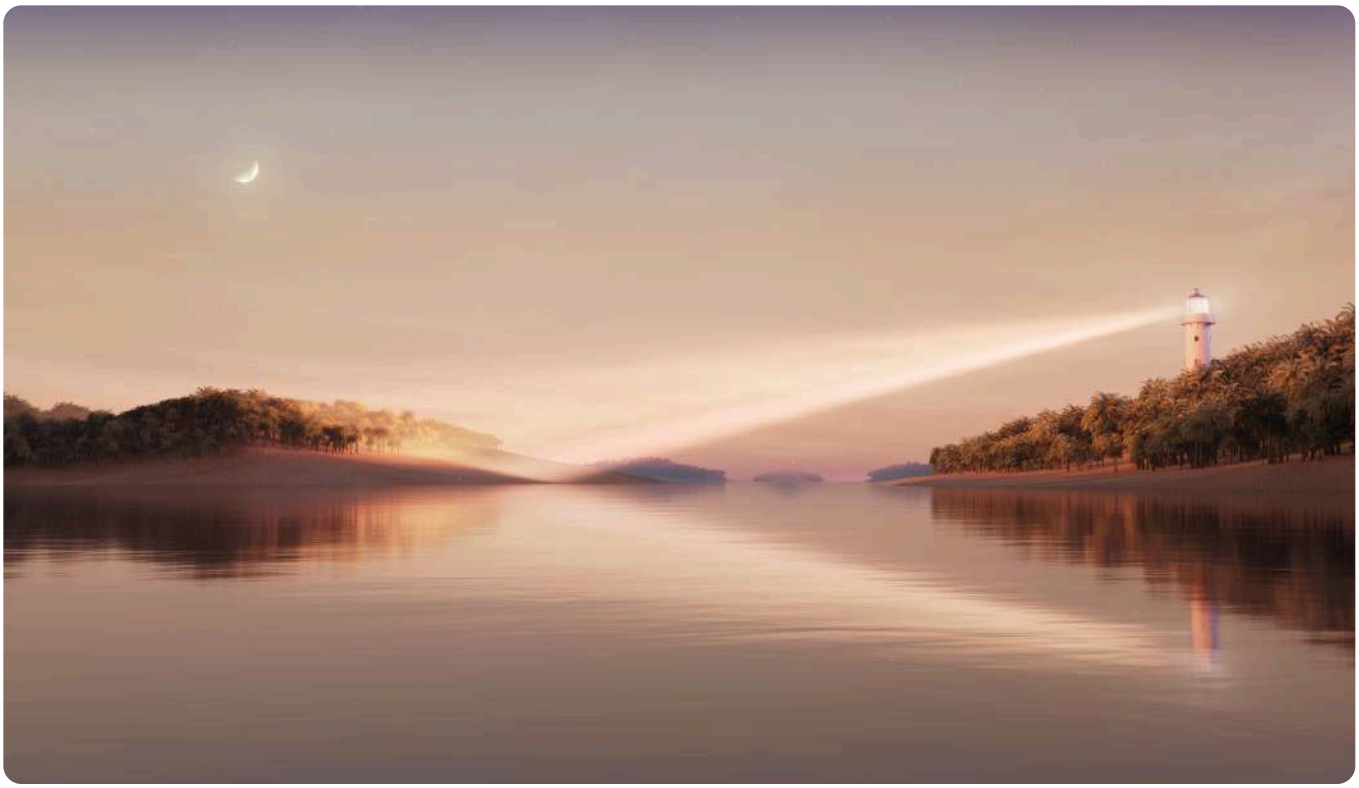
At the same time, it becomes clear that NIS2 does not necessarily tie up more complexity, cost, or resources. On the contrary: those who anchor security cleanly in the architecture reduce operational friction. Responsibility becomes controllable. Decisions become faster. Communication becomes clearer. Compliance is not created through checklists, but through structure.

Finally, NIS2 will not be the last requirement from Brussels that companies will face in 2026. The EU AI Act will also require companies to precisely control and audit employees' use of AI. To meet these requirements, IT must be able to control data flows at the application level.

The outlook is clear. 2026 will not be a year of interpretation, but of enforcement. Supervision, audits, and reporting obligations will become reality. Companies that act today gain time, control, and room to maneuver. Companies that hesitate risk being forced to react under pressure.

The Enterprise Browser is not a silver bullet. But it is a crucial building block to not only comply with NIS2, but to control it: transparent, manageable, and audit-ready.

The hour of responsibility has begun. Those who accept it now strengthen not only their own resilience, but digital stability overall.



7. Sources

Legal and regulatory foundations
Directive (EU) 2022/2555 (NIS2 Directive)

Directive of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity in the Union.Official Journal of the European Union, L 333, 27/12/2022.
Act implementing the NIS2 Directive and regulating key aspects of cybersecurity
Adopted by the German Bundestag in November 2025; approval by the Bundesrat completed.
Amendment of the BSI Act and expansion of the group of affected companies.
Federal Office for Information Security (BSI) Information on NIS2, reporting obligations, risk management and supervisory powers.
https://www.bsi.bund.de

Expert classification and context
Haar, Tobias
Legal Outlook 2026: What will change for IT professionals next year.
iX – Magazine for Professional Information Technology / heise medien, 2025.
Classification of practical implications of NIS2, CRA, AI Act and Data Act for companies.
European Commission
The NIS2 Directive – Strengthening cybersecurity across the EU.
Background and objectives of the directive from the European Commission's perspective.

Technical and conceptual references (Enterprise Browser)
Island
Press Kit: Island – The one solution that changes everything, 2025.
Description of the Enterprise Browser, its architecture and its security, governance and compliance functions.
Island
NIS2 – The Hour of Responsibility, internal background document.
Conceptual rationale for the role of the Enterprise Browser in the context of regulatory requirements.