efficient iP®

White Paper

Achieving NIS 2 Compliance with DDI and Advanced DNS Security

In an ever-evolving cybersecurity threat landscape, the rapid evolution of digitization has heightened the need for robust cybersecurity measures.

The NIS 2 Directive enhances Europe's cybersecurity framework by expanding the scope of the original NIS Directive and enforcing stricter security measures. With compliance measures taking effect in 2024, organizations must prepare well in order to avoid substantial fines.

Key NIS 2 security requirements include risk management, incident handling, business continuity, and transparent reporting. DNS, DHCP, and IPAM (DDI), along with advanced DNS Security, are crucial for meeting these requirements, by ensuring service availability, data integrity, and effective incident response. These solutions protect users, data, and networks against the growing number of cyber attacks, helping organizations achieve NIS 2 compliance.

Outline:

Executive Summary

The NIS 2 Directive aims to enhance cyber resilience across Europe by unifying cybersecurity standards and enforcing stringent security measures. Compliance measures must be applied by Member States starting on October 17, 2024, and regular audits will begin in early 2025. In a nutshell, this directive broadens the scope of cybersecurity requirements, mandates more rigorous security measures, and enforces top management accountability.

Key cybersecurity requirements in the NIS 2 Directive include ensuring comprehensive risk management, establishing robust incident handling procedures, maintaining business continuity plans, and achieving transparent reporting and disclosure. These use cases help organizations be proactive in the face of cyber attacks, better manage cyber threats, minimize downtime, and ensure accountability.

DNS, DHCP, and IP Address Management (IPAM) solutions with advanced DNS Security capabilities play a critical role in providing comprehensive visibility and control across hybrid multicloud environments, delivering a resilient, scalable, and automated DNS and DHCP infrastructure, as well as protecting users, data, and networks. Acting as the first line of defense, advanced and innovative DNS Security enables organizations to stay ahead of cyber threats by proactively preventing them with DNS-centric threat intelligence, detecting malicious DNS activity leveraging breakthrough AI-driven algorithms, and effectively recovering from attacks with automated response to ensure data integrity and maintain service availability.

To prepare for NIS 2 and achieve compliance, organizations need to implement DDI and advanced DNS Security to help them meet essential NIS 2 requirements for comprehensive risk management, robust incident handling, business continuity, and transparent reporting to strengthen their cyber resilience and protect their digital infrastructure.

Struggling in an Increasingly Complex Cybersecurity Landscape

In 2023, the cybersecurity landscape saw a significant rise in threats, with malware incidents increasing by 30% and ransomware attacks involved in 33% of cases. IoT malware spiked 107%, and encrypted threats surged by 92%. Phishing attacks affected 54% of organizations. Attackers became more sophisticated and faster in executing their campaigns, underscoring the escalating challenge of defending against these evolving threats across various industries.

The rapid adoption of generative AI technologies has outpaced the industry's ability to manage associated risks. Cybercriminals are using AI to automate phishing, create deepfake audio for social engineering, and develop sophisticated malware. Attackers are increasingly leveraging AI to rapidly develop and deploy new attack methods, complicating defense efforts. Google Cloud's 2024 forecast highlights a rise in AI-driven phishing. Nearly 96% of business leaders believe AI adoption increases security breach risks, with 84% prioritizing AI cybersecurity solutions.

The financial impact of these cybersecurity threats is significant. In 2023, the global average cost of a data breach increased by 10% to $4.88 million. These costs not only include direct financial losses but also long-term reputational damage, legal fees, and the cost of implementing more robust security measures post-incident. Nearly 45% of data exfiltration occurred within 24 hours of the initial compromise, underscoring the increasing speed and complexity of cyberattacks and further contributing to the rising costs associated with these incidents.

DNS is of concern because it is both a target and an attack vector. The IDC 2023 Global DNS Threat Report revealed that 90% of organizations experienced at least one DNS attack in the past year, with the average cost of such an attack reaching $1.1 million.

In 2023, Europe was the most impacted region, accounting for 32% of the incidents according to IBM. This highlights the region's vulnerability and underscores the need for enhanced cybersecurity measures.

The NIS 2 Directive aims to address these challenges by reinforcing cybersecurity protections across Europe, promoting information sharing, and uniting efforts within the European Union against cyber attacks.

Understanding the NIS 2 Directive

NIS 2 Overview

The NIS 2 Directive builds upon the original Network and Information Security (NIS) Directive adopted in 2016, modernizing the existing EU's cybersecurity framework.

Recognizing the growing complexity and frequency of cyber threats in an ever-digital landscape, the new directive introduces more stringent cybersecurity measures. Its scope is expanded to cover new sectors and entities. It emphasizes risk management and supply chain security, improves incident response capacities, and requests mandatory incident reporting. The directive places accountability on top management to promote a security centric culture and ensure that cybersecurity is a strategic priority. Finally, it mandates regular audits and harmonizes cybersecurity practices across member states, reducing fragmentation and fostering cooperation.

These measures aim to create a unified and resilient cybersecurity environment, making the NIS 2 Directive crucial for protecting Europe's digital landscape against evolving cyber threats.

Key Provisions

The NIS 2 Directive includes several key provisions aimed at strengthening cybersecurity:

Fines can be significant, reaching "a maximum of at least EUR 10 000 000 or of a maximum of at least 2% of the total worldwide annual turnover"

- **Expanded Scope**
  The directive covers a broader range of sectors, including but not limited to digital infrastructure (Telecom, DNS, data centers, cloud services), healthcare, and critical manufacturing.
- **Supervision and Penalties**
  The definition of the system of penalties, its supervision, and implementation in case of infringement of the national provisions of the directive is under the responsibility of Member States. Fines can be significant, reaching "a maximum of at least EUR 10 000 000 or of a maximum of at least 2% of the total worldwide annual turnover..., whichever is higher", for essential entities.
- **Accountability of Management**
  Management bodies are explicitly accountable for compliance with cybersecurity measures.

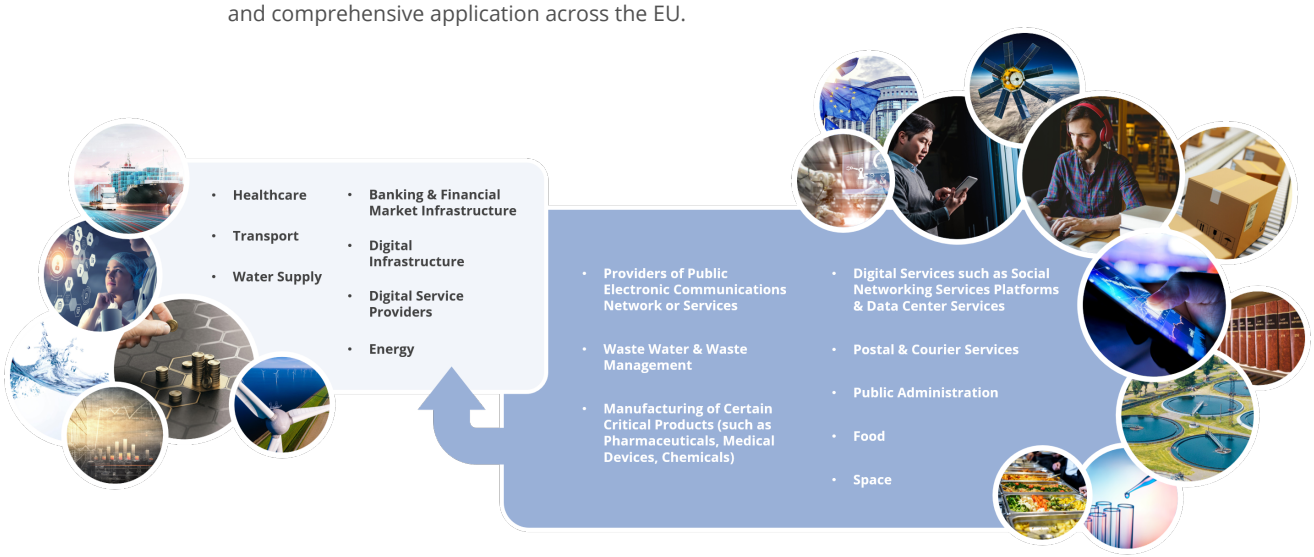
NIS 2 Cybersecurity Measures

The NIS 2 Directive lists minimum cybersecurity measures that organizations must implement to manage risk and minimize impact of incidents. These need to protect network and information systems, as well as the physical environment of those systems. Key requirements include:

- **Risk Management**
  Appropriate operational and organizational measures to identify, assess, and mitigate risks posed to the security of networks, supply chains, and the use of encryption.
- **Incident Handling**
  Actions and procedures aiming to prevent, detect, analyze, and contain or to respond to and recover from an incident.
- **Business Continuity**
  Definition and implementation of business continuity plan, including backup management, disaster recovery, and crisis management.
- **Reporting and Disclosure**
  Notification within 24 hours of any incident that significantly impacts service delivery, including cross-border effects, with a final report due within one month.

Identifying Impacted Entities

The directive categorizes impacted entities into two groups: essential entities and important entities. Essential entities include sectors like energy, transport, banking, healthcare, and digital infrastructure. Important entities cover sectors such as postal and courier services, waste management, food production, and digital providers like online marketplaces and social networks. The directive applies to entities depending on their size and significance to the economy and society, ensuring a broad and comprehensive application across the EU.



Sectors covered by NIS 2

Important Compliance Deadlines

27 December 2022:
NIS 2 Directive formally adopted by the European Union

17 October 2024:
NIS 2 Directive transposed into national law by Member States

18 October 2024:
Member States start applying Compliance measures

17 January 2025:
Operational cooperation assessment and peer review methodology

17 April 2025:
Entity List and Notifications

- Member States establish a list of essential and important entities as well as entities providing domain name registration services and notify the Commission

17 October 2027:
Commission Review to assess the effectiveness of the directive and propose updates to ensure its continued relevance

The Critical Role of DDI and DNS Security in NIS 2 Compliance

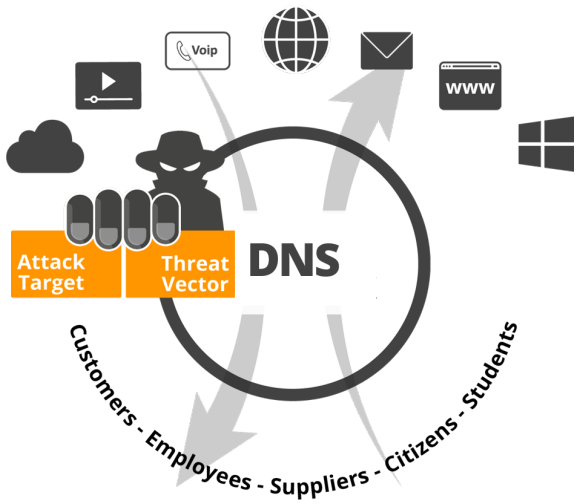
As the NIS 2 Directive mandates comprehensive cybersecurity measures to protect critical infrastructure, including DNS, organizations need to increase their cyber resilience to avoid significant impact and fines. This is where DNS, DHCP, and IP Address Management (DDI), along with advanced DNS Security, are instrumental in providing comprehensive visibility, preventing cyber threats, and protecting users, data, and networks.

Why DDI and DNS Security are Essential

DDI solutions provide network and cloud assets discovery, consolidation, and repository of all network-related objects including VLAN/VXLAN/VRF, applications, and devices across disparate hybrid multicloud and on-premise environments. This helps create a comprehensive Network Source of Truth (NSoT) for efficient management of network operations and global visibility. All changes are tracked and reconciled for accurate and up-to-date asset inventory. This ensures effective asset management critical for cyber risk assessment, enabling organizations to easily identify, continuously monitor, and report on any anomalies or vulnerabilities.

By offering centralized and integrated management of DNS, DHCP, and IPAM, DDI solutions bring a robust framework that streamlines the deployment of DNS and DHCP services, even in distributed, multi-vendor, and hybrid multi-cloud environments, thanks to scalable, flexible architecture templates. This ensures consistent policies, error-free configurations, and the use of best practices across DNS providers for utmost reliability and security. In addition, the centralized management platform simplifies the recovery of crashed DNS servers with automated detection, installation, and reconfiguration. This accelerates disaster recovery and ensures service continuity, which is further enhanced by the use of DNS Global Server Load Balancing (GSLB), providing automatic cross-site failover in the event of a failure.

Acting as the first layer of defense, DNS Security elevates network security against sophisticated attacks, enabling organizations to protect data, users, and networks globally, proactively detect malicious DNS activity, and effectively respond to cyber threats. With Protective DNS (PDNS) service, an advanced DNS Security solution specifically addresses the need for secure DNS operations by analyzing DNS queries in real-time to identify, filter, or block access to suspicious domains using DNS-centric threat intelligence, AI-driven threat detection, and other innovative technologies. This provides end-to-end protection against evolving DNS-based attacks such as phishing, malware, data exfiltration, DDoS attacks and more, with no additional latency.



DNS Security Role under NIS 2

It is worth remembering that DNS is a favorite target and threat vector, with 85% of malware using DNS to develop their attacks. Organizations cannot neglect their DNS protection and, as emphasized by NIS 2, are required to implement robust security measures to safeguard their DNS infrastructure, including advanced threat prevention, detection, and mitigation techniques.

A robust DNS Security solution brings several foundational built-in features, such as a secure DNS platform with a hardened operating system, easy and flexible update management, policy-driven architecture implementations that ensure error-free configuration automation, and automated DNSSEC deployment that guarantees data integrity and authenticity. In addition, advanced DNS Security solutions offer key breakthrough capabilities that align with NIS 2 requirements, including:

- **Advanced Real-time Threat Detection**
  Real-time threat detection is crucial for minimizing the impact of cyber incidents. Protective DNS Security solutions help organizations identify suspicious activities before and as they infiltrate their networks. By leveraging advanced techniques such as EfficientIP's DNS Transaction Inspection for in-depth, real-time DNS traffic analysis combined with user behavior analysis, and AI-driven algorithms for detecting Domain Generated Algorithms (DGAs) or phishing, organizations can enhance their cyber resilience and comply with the NIS 2 Directive's requirements for threat prevention and detection. This enables detection of advanced attacks such as data exfiltration through zero-day malicious domains, DNS tunneling, command and control exchanges, phantom or sloth attacks, cache poisoning, DNS hijacking, amplification and reflection attacks, and DNS flooding.

- **DNS-Centric Threat Intelligence**
  Implementing a high-quality, comprehensive, and consolidated DNS threat intelligence feed that provides real-time updates on malicious domains helps organizations stay ahead of emerging threats. Integrating DNS analytics with DNS Intelligence services facilitates investigation with Indicators of Compromise (IoC), domain name risk scoring, and other metrics to qualify alerts and confirm the threat is real. These insights into DNS traffic can also help enrich and augment DNS threat intelligence, strengthening the security posture and enabling proactive defense.

Harnessing DNS analytics and metrics provides complete visibility of DNS threats and the ability to activate the right countermeasure at the right time for each specific type of attack

- **Advanced Domain Filtering**
  DNS filtering prevents access to known malicious domains, reducing the risk of malware infections and phishing attacks by blocking harmful websites before a connection is established and any traditional, in-line security kicks in. Advanced solutions enable data-rich client-based policy definition and management leveraging a DNS-threat intelligence feed, allowing organizations to control application access with unprecedented granularity for effective threat protection, aligning with NIS 2's preventive measures.

- **Automated Response & Recovery**
  Harnessing DNS analytics and metrics provides complete visibility of DNS threats and the ability to activate the right countermeasure at the right time for each specific type of attack, automating predefined actions such as blocking IP addresses, quarantining suspicious devices, or activating specific measures such as EfficientIP's Rescue Mode to ensure cache continuity and DNS service availability even if the source of the attack cannot be identified. These adaptive countermeasures help mitigate threats, minimize business disruption, and restore operations in disaster cases, ensuring compliance with regulatory requirements.

- **Integration with the Security Ecosystem**
  When designed as an open solution, advanced DNS Security solutions can integrate with the security ecosystem using APIs and events to feed security platforms and tools such as SIEM, SOAR, NAC, TIP… with actionable DNS insights, gain visibility into threats, accelerate investigations and decisions for a more adaptive response, and automate the security response for more efficient remediation. This improves Mean Time To Resolution (MTTR) for a better user experience and greater infrastructure resilience.

- **High-Volume DDoS Protection**
  Robust DNS Security solutions offer protection mechanisms such as a fast, high-performance cache against high-volume Distributed Denial of Service (DDoS) attacks, ensuring the continuous availability of critical services and network reliability.

- **Bolstered Zero Trust Security**
  By leveraging all of the key capabilities listed above, a DNS Security solution makes a significant contribution to Zero Trust architectures. As the entry point to an organization's networks, DNS is ideally positioned to become the first checkpoint to apply the «never trust, always verify» principle, using comprehensive DNS threat intelligence feeds to identify and block DNS resolutions for known malicious destinations at the client or group level. The solution enforces micro-segmentation and application zoning by ensuring that only authorized users and devices can access resources or services through rich user-based filtering policies for least privilege access. Continuous monitoring, DNS analytics, and user behavior analysis provide true deep visibility and real-time understanding of DNS traffic for effective threat detection. Finally, centralized security policy management simplifies the design, deployment, and management of security policies down to the individual, consistently across networks. Implementing Zero Trust measures leveraging DNS Security strengthens cybersecurity defenses and helps meet NIS 2 requirements.

DDI Benefits for NIS 2

DDI and advanced DNS Security solutions deliver the following benefits to meet NIS 2 risk reduction and expectations:

Enhanced Network Visibility

DDI solutions bring effective asset management leveraging IPAM as a NSoT and observability, enabling organizations to easily view, continuously monitor, and report on any anomalies or vulnerabilities. Combined with advanced DNS Security solutions incorporating DNS-centric threat intelligence and AI-driven threat detection capabilities, organizations can quickly identify, investigate, and analyze anomalies, providing comprehensive network visibility and control for proactive threat management.

Elevated Security Posture

Implementing DDI and an advanced DNS Security solution allows organizations to benefit from faster and more efficient threat prevention, detection, and remediation, protecting users and data integrity. As a result, security teams can build a holistic, more integrated infrastructure and improve security posture. This also helps achieve compliance and alignment with other regulatory frameworks like DORA, PCI DSS, GDPR, and HIPAA, or recommendations from the NSA, CISA, and NCSC.

Ensured Service Availability

With integrated, scalable, and reliable DNS and DHCP services, high availability and multi-vendor disaster recovery capabilities, and robust, advanced DNS Security features, DDI solutions help IT teams strengthen business resilience in order to maintain service availability in the event of a cyber attack.

Improved Operational Efficiency

By leveraging open, highly customizable DDI and advanced DNS Security solutions, IT teams can automate processes and streamline workflows to save time and improve efficiency across all network and security operations. Specifically, integrating threat detection, response, and recovery with the security ecosystem streamlines security operations. This frees up security teams by reducing human interventions, errors, and delays, and improves incident response times.

NIS 2 Use Cases Unlocked by Innovative DDI and DNS Security

Innovative DNS, DHCP, and IP Address Management (DDI), along with advanced DNS Security, are critical to meeting key NIS 2 requirements for risk management, incident handling, business continuity, and transparent reporting. Below are example use cases for each requirement.

USE CASE 1

Ensuring Risk Management: The directive mandates entities to adopt comprehensive risk management practices. This involves implementing measures to identify, assess, and mitigate risks to their network and information systems. DDI solutions with advanced DNS Security enhance risk management with comprehensive, accurate, and up-to-date asset inventory and advanced analytics, providing deep visibility. Implementing a protective DNS Security service provides a first layer of defense to secure DNS and significantly reduce the risk of cyberattacks. This risk is further lowered when combined with DNS-centric threat intelligence, advanced application access control with fine-grained DNS filtering enabling micro-segmentation, and high-volume DDoS prevention. These capabilities enable organizations to monitor their DNS traffic, efficiently restrict access according to Zero Trust principles, and proactively mitigate the associated risks and impacts.

USE CASE 2

Effective Incident Handling: NIS 2 emphasizes the importance of having robust incident handling procedures. Entities must establish mechanisms to prevent, detect, analyze, and respond to cybersecurity incidents promptly. This includes defined and automated processes for incident identification, escalation, and response, helping to minimize impact and restore operations swiftly. Advanced DNS Security solutions help IT teams defend against any type of DNS-based threat, including but not limited to phishing, malware, DDoS, DNS tunneling, zero-day DNS attacks, or cache poisoning, and at any stage of the threat lifecycle. Leveraging real-time threat detection, automated response and recovery, and integration with the security ecosystem, security teams can quickly and effectively thwart cyber threats globally.

USE CASE 3

Maintaining Business Continuity: The directive requires entities to develop and implement business continuity plans. These plans should include backup management, disaster recovery, and crisis management strategies. By ensuring that critical processes can continue during and after a cyber incident, organizations can reduce downtime and minimize business impacts. As a robust, secure, and scalable platform, DDI along with DNS Security and DNS GSLB, sustains business continuity by ensuring the availability and reliability of DNS services, which are crucial for uninterrupted internet-based operations, and accelerating disaster recovery with failure detection and automated failover across multiple sites.

USE CASE 4

Achieving Transparent Reporting & Disclosure: NIS 2 mandates reporting significant incidents within one day and detailed reports within a month, ensuring accountability and cooperation. Regular reporting and disclosure of cybersecurity incidents promote a culture of awareness and continuous improvement in cybersecurity practices. DDI and DNS Security solutions that deliver insightful DNS intelligence, metrics, and analytics facilitate real-time incident investigation and provide the detailed reporting needed to meet these stringent requirements. Integration with the broader cybersecurity ecosystem also ensures comprehensive threat visibility and efficient incident reporting.

By implementing these four NIS 2 use cases with DDI solutions, organizations can better protect themselves against cyber threats, ensure a higher level of security and resilience, and effectively prepare for the NIS 2 compliance.

Conclusion and Next Steps

The NIS 2 Directive represents a significant step forward in enhancing Europe's cybersecurity landscape. Organizations must elevate their cyber resilience and accelerate their compliance efforts by focusing on comprehensive risk management, improving incident handling, ensuring business continuity, and achieving transparent reporting and disclosure. By implementing robust, secure, and scalable DDI and DNS Security solutions, organizations can deliver on these use cases, improve their cyber resilience, lay a solid foundation for future network evolution, and protect their digital infrastructure while achieving NIS 2 compliance.

efficient iP®

REV: C-240626

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752