White paper

BLUECAT

Complying with the NIS 2 cybersecurity directive

BlueCat solutions: Unified DDI, protective DNS solutions, and network observability and health

Executive Summary

As cybersecurity threats and risks evolve, so does the regulatory environment. The second iteration of the European Union's Network and Information Security Directive, called NIS 2, is an updated cybersecurity regulatory framework set to be transposed into member states' laws in October 2024.

Designed to tackle the escalating cybersecurity challenges and vulnerabilities facing its member states, NIS 2 regulations will impact many organizations. The NIS 2 directive outlines the requirements placed upon medium- to large-sized public and private entities that provide critical infrastructure or services vital to the European Union economy and society. Covered entities are divided into two categories, essential and important.

Compared to its predecessor, the updated NIS 2 directive has stricter requirements for cybersecurity risk management and incident reporting, expands the scope of entities that it covers, and imposes stiffer penalties for non-compliance.

The NIS 2 directive aims to boost cybersecurity with requirements across four key areas: risk management, corporate governance, incident reporting, and business continuity. To support these four overarching areas, the directive spells out 10 baseline security measures that entities must implement to manage risks. Penalties for non-compliance include non-monetary remedies, administrative fines, and criminal sanctions for management bodies.

According to the NIS 2 directive, upholding and preserving a reliable, resilient, and secure DNS is crucial to maintaining the integrity of the internet and is essential for its continuous and stable operation. But as networks grow increasingly complex and expand to the cloud, it becomes an even greater challenge to maintain a single source of truth for DNS.

A consolidated, automated, and streamlined approach to managing the core network services of DNS, DHCP, and IP address management (together known as DDI), particularly when combined with protective solutions and network observability tools, offers a robust answer to meeting the NIS 2 mandate. Together, these solutions address many elements of the directive, including risk management, incident handling, operational security, and reporting obligations.

Three of BlueCat's products—Integrity, Edge, and Infrastructure Assurance—offer core capabilities and features that can help enterprises comply with NIS 2 directive requirements. A mapping table provides detailed descriptions of how BlueCat products can help address specific mandates in NIS 2 directive articles.

Supported by BlueCat's solutions for unified DDI, protective DNS, and network observability and health, organizations can more easily rise to the mandate to meet NIS 2 requirements.

Table of contents

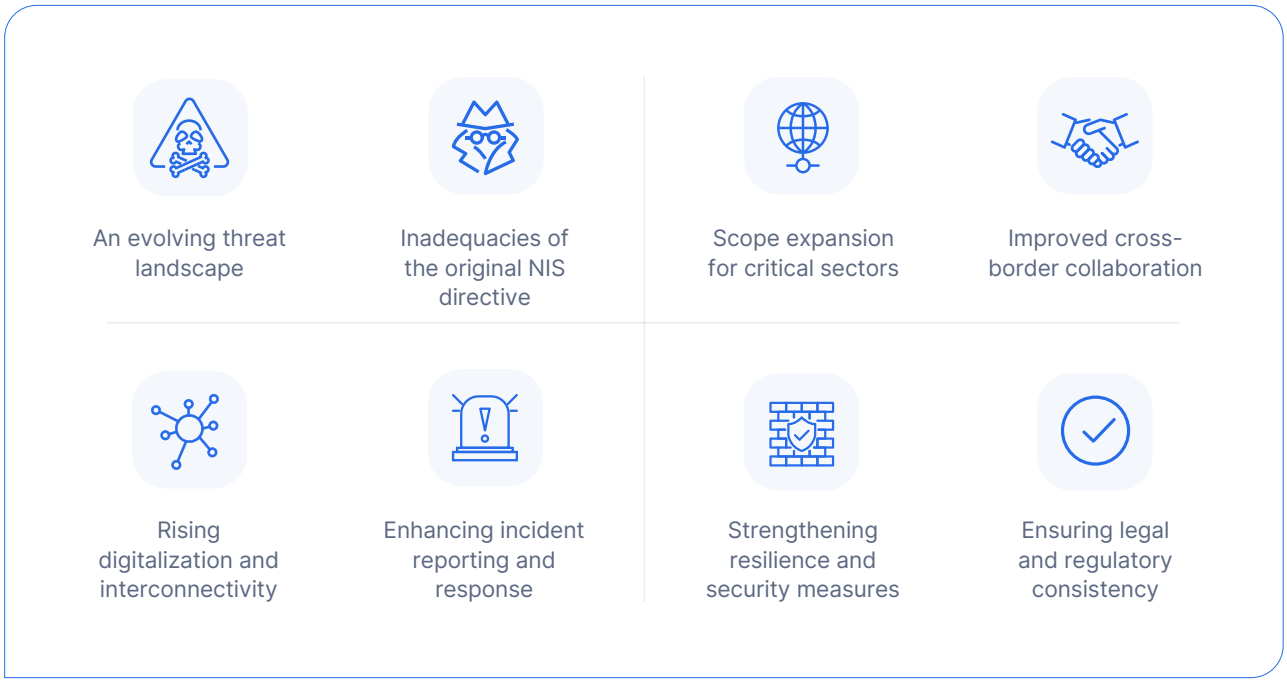
Introduction to the NIS 2 directive

The Network and Information Security (NIS) Directive was a landmark cybersecurity regulatory framework established in the European Union (EU) in 2016.

The EU recently introduced a second iteration, Directive (EU) 2022/2555, known as NIS 2, to tackle the escalating cybersecurity challenges and vulnerabilities facing its member states, particularly those relating to critical infrastructure and services. The NIS 2 entered into force in January 2023, and each member state must transpose this updated directive into national law by October 17, 2024.

As our reliance on digital systems continues to grow, so does related risk. The risk of exploitation by bad actors and the potential impact on society from critical sector cyberattacks requires heightened security postures. NIS 2 seeks to reinforce and build better foundations for all aspects of network and information security, from coordinated incident response and reporting to fortifying cybersecurity defenses and practices. Our growing interconnectedness also means we must be able to trust and rely on our critical supply chains as they form networks at organizational, national, and regional levels.

Some reasons why the NIS 2 directive was developed were to address:



Under the NIS 2 directive, member states are tasked with creating or improving their:

- National cybersecurity frameworks
- Competent authorities
- Crisis management frameworks
- Computer security incident response teams
- Vulnerability databases
- Cooperation
- Risk assessments
- Reporting
- Certification schemes

Compared to its predecessor, the updated NIS 2 directive features stricter requirements for cybersecurity risk management and incident reporting, expands the scope of entities that it covers, and imposes stiffer penalties for non-compliance.

Does the NIS 2 directive apply to my organization?

Much of the NIS 2 directive covers the responsibilities and requirements placed upon medium- to large-sized public and private entities that provide critical infrastructure or services vital to the EU economy and society. NIS 2 significantly expands the list of covered sectors from just seven in the original directive. In NIS 2, covered entities are divided into two categories, **essential** and **important**, which are defined by size and type.

Essential and important entities

Under the NIS 2, an **essential** entity is a large organization that operates in a **sector of high criticality** (see the list of high criticality sectors below). While it can vary slightly by sector, the NIS 2 generally defines the threshold for a large organization as one with at least 250 employees and an annual turnover of at least €50 million or an annual balance sheet of at least €43 million.

High criticality sectors for essential entities include:

- Energy
- Transport
- Banking and financial market infrastructure
- Health
- Drinking water and wastewater
- Digital infrastructure
- Information and communication technology (ICT) service management (business-to-business managed service providers and managed security service providers)
- Public administration
- Space

Digital infrastructure refers to services that are crucial to network operations. It includes internet exchange point providers, DNS service providers, top-level domain name registries, cloud computing services, data center service providers, content delivery networks, trust services, public electronic communications networks, and publicly available electronic communications services.

Meanwhile, an **important** entity is an organization that is at least medium-sized and operates in **other critical sectors** that don't fall under the essential category. Again, while the definition can vary slightly by sector, the threshold for medium-sized is having at least 50 employees and an annual turnover of at least €10 million or a €10 million balance sheet.

Other critical sectors for important entities include:

- Postal and courier services
- Waste management
- Manufacture, production, and distribution of chemicals
- Production, processing, and distribution of food
- Manufacturing
- Digital providers (search engines, online marketplaces, and social networks)
- Research

It's important to note that critical sector organizations that do not meet the minimum size requirements of the 'essential' category are still deemed to be 'important' entities.

Did You Know?
Essential entities are subject to additional supervision requirements, such as ad-hoc audits and proactive monitoring, and higher fines for non-compliance. Supervision of important entities is reactive, such as upon evidence of non-compliance.

NIS 2 essential vs. important entities

	Sector	Headcount	Annual turnover	OR	Balance sheet total
Essential entity	• Energy • Transport • Banking and financial market infrastructure • Health • Drinking water and wastewater • Digital infrastructure • ICT service management • Public administration • Space	250 employees	€50 million		€43 million
Important entity	• Postal and courier services • Waste management • Manufacture, production, and distribution of chemicals • Production, processing, and distribution of food • Manufacturing • Digital providers • Research *Plus, all sectors that fall under essential but are within the size threshold for important entities.*	50 employees	€10 million		€10 million

Mandatory applicability regardless of size

The NIS 2 has mandatory applicability for certain organizations **regardless of their size.** This includes:

- Providers of public electronic communications networks or publicly available electronic communications services
- Trust service providers
- Top-level domain name registries and DNS service providers

Applicability is also mandatory for smaller organizations in cases such as if the entity is the sole provider of a service in a member state that is essential for maintaining critical societal or economic activities, or if disruption of the entity's services would induce systemic risk or have a significant impact on public safety, security, or health. Member states may also deem an entity critical because of its specific importance at the national or regional level.

Determining jurisdiction

Under NIS 2, essential and important entities fall under the jurisdiction of the member state in which they are established. If entities provide services in more than one member state, they fall under the separate and concurrent jurisdiction of each member state.

However, the NIS 2 also accounts for the somewhat borderless nature of digital entities. Public electronic communications networks or publicly available electronic communications services fall under the jurisdiction of the member state in which they provide their services.

The entities below fall under the jurisdiction of the EU member state in which they have their main establishment. The NIS 2 defines a main establishment as where decisions related to cybersecurity risk management measures are predominantly made, where cybersecurity operations are carried out, or where the greatest number of EU-based employees are located. This applies to:

- DNS service providers
- Top-level domain name registries
- Entities providing domain name registration services
- Cloud computing service providers
- Data center service providers
- Content delivery networks
- Managed service providers and managed security service providers
- Online marketplaces
- Search engines
- Social networks

Applicability to supply chains

An entity's supply chain and its suppliers, such as providers of data storage and processing services, play an important role in cybersecurity. Numerous times, entities have been the victim of cyberattacks wherein malicious perpetrators compromised the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. According to the NIS 2, essential and important entities must assess and consider the overall quality and resilience of products and services they procure, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Entities are encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers.

Finalizing entities that fall under the scope of NIS 2

By April 17, 2025, member states must identify the essential and important entities in their state that fall under the scope of NIS 2. Organizations will need to determine if they fall within the scope of NIS 2, identify which member states they provide in-scope services to, and register before the deadline.

Did You Know?
In addition to submitting basic organizational details to a member state's competent authority, registered in-scope entities will also be required to submit their assigned IP address ranges. If entities make any changes, they will have to notify authorities about them within two weeks. How robust is your IP address management tool, and does it include all the IP address ranges you route or administer?

It is important that your organization carefully reviews the language of the NIS 2 directive to understand specific criteria and thresholds and determine if you fall within its scope.

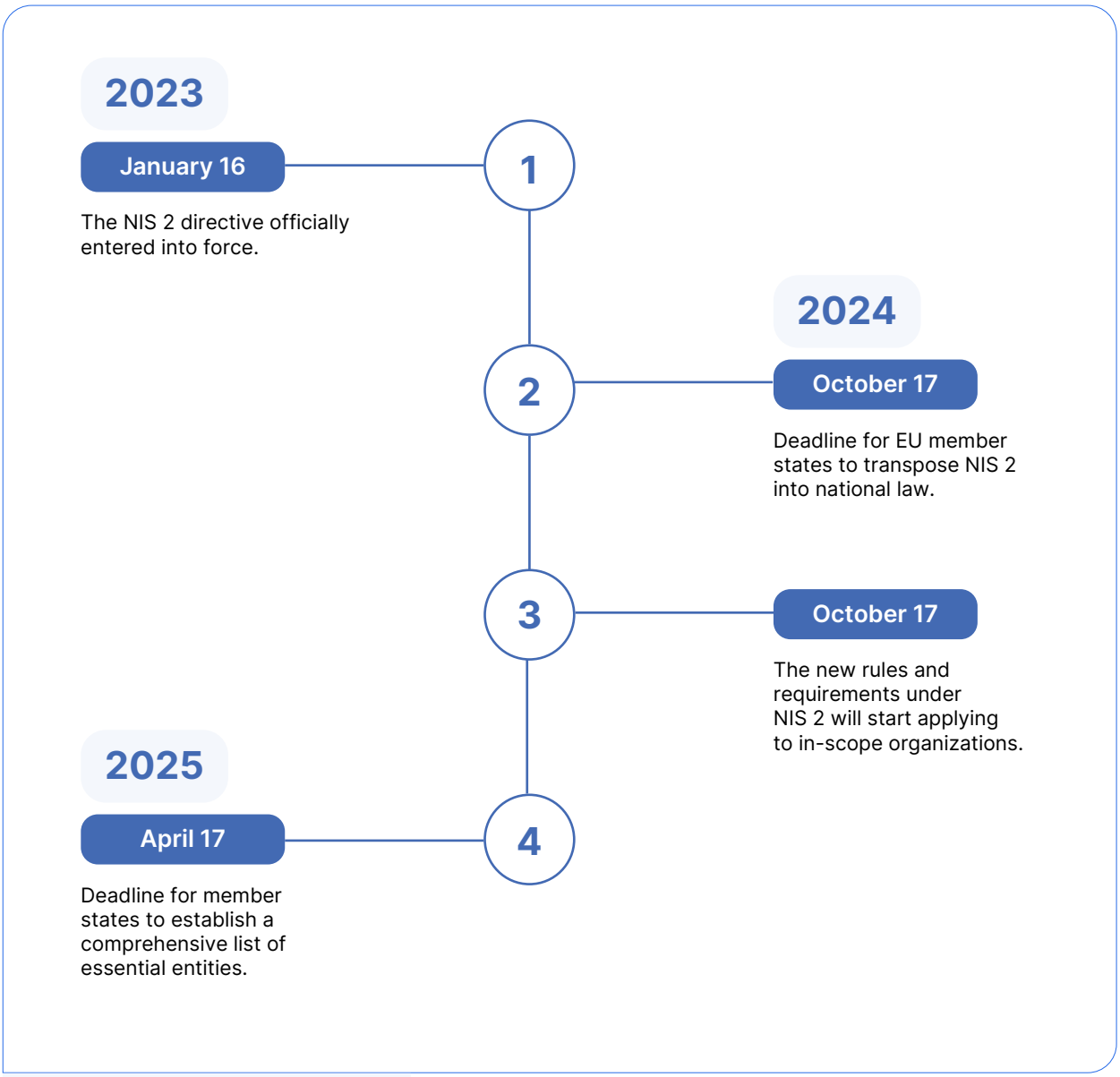


Figure 1. NIS 2 timeline for key dates

Key requirements and impacts of the NIS 2 directive

The NIS 2 directive aims to boost cybersecurity with requirements across four key areas: risk management, corporate governance, incident reporting, and business continuity.

Four areas of focus to boost cybersecurity

Risk management

Organizations are required to implement comprehensive risk management strategies to minimize cyber threats. They must conduct regular risk assessments, establish security policies, and implement measures to protect the integrity, confidentiality, and availability of their systems. Entities are also obligated to monitor and document their security practices on an ongoing basis, ensuring they can quickly identify and address emerging threats.

Corporate governance

Management bodies are responsible for overseeing and approving their respective entities' protocols for cybersecurity risk management. They must also ensure they are implemented effectively. Management bodies are also required to undergo cybersecurity training and should offer similar training to their employees.

Incident reporting

Covered entities must report significant incidents to relevant authorities promptly, providing detailed information about the nature of the incident and the mitigation measures taken. Entities must provide initial notification no later than 24 hours after learning of a cyber incident, a full report no later than 72 hours after, and a final report one month later.

Business continuity

Entities are required to create a strategy that details how they will respond to and recover from incidents, with a goal of minimizing disruptions and ensuring business continuity following an attack.

Baseline security measures that entities must implement

To support these four overarching areas, the directive spells out 10 baseline security measures that organizations must implement to manage risks. They include:

1. Policies on risk analysis and information system security
2. Incident handling
3. Business continuity, such as backup management and disaster recovery, and crisis management
4. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
5. Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure
6. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
7. Basic cyber hygiene practices and cybersecurity training
8. Policies and procedures regarding the use of cryptography and, where appropriate, encryption
9. Human resources security, access control policies, and asset management
10. The use of multi-factor authentication or continuous authentication solutions; secured voice, video, and text communications; and secured emergency communication systems within the entity, where appropriate

Sanctions for non-compliance

The NIS 2 directive has much harsher penalties for non-compliance than its previous iteration, including non-monetary remedies, administrative fines, and criminal sanctions for management bodies.

Non-monetary remedies

The NIS 2 gives member states' supervisory authorities the power to levy non-monetary remedies against non-compliant entities, including compliance orders, binding instructions, security audit implementation orders, and threat notification orders to entities' customers.

Administrative fines

Fines can vary by member state, but the NIS 2 directive sets maximum fine levels for essential and important entities.

Fines for essential entities	Fines for important entities
A maximum fine of up to **€10,000,000** or **2% of global annual revenue**, whichever is higher.	A maximum fine of up to **€7,000,000** or **1.4% of global annual revenue**, whichever is higher.

Criminal sanctions for management bodies

To reduce the pressure on IT and security teams, the NIS 2 directive includes measures that can hold top management personally liable if gross negligence is proven after a cybersecurity incident. Supervisory authorities can order organizations to publicly disclose violations or make public statements identifying the person(s) responsible for the incident. If the organization is an essential entity, an authority can temporarily ban executives from holding management positions.

DNS: A core element of a secure network under NIS 2

The Domain Name System (DNS) is a hierarchical naming system that allows communication across devices on a network. Most commonly, it translates human-readable domain names (like bluecatnetworks.com) to computer-friendly Internet Protocol (IP) addresses (like 104.239.197.100). Essentially, it allows us to connect to websites without having to memorize a string of numbers. With DNS, all we need to know when we open web browsers are websites' names.

According to the NIS 2 directive, "Upholding and preserving a reliable, resilient and secure domain name system (DNS) are key factors in maintaining the integrity of the internet and are essential for its continuous and stable operation, on which the digital economy and society depend."

DNS was built first and foremost to correctly and efficiently respond to queries, not question their intent. As a result, DNS has inherent limitations and potential to be used as a vector for cyberattacks. In a DNS attack, a bad actor either tries to compromise the infrastructure that provides DNS services or takes advantage of its inherently open attributes to conduct a broader attack. A well-orchestrated DNS attack against an unprotected network can bring an organization to its knees.

As networks grow increasingly complex and expand to hybrid and multicloud environments, it becomes an even greater challenge to maintain a single source of truth for DNS.

A consolidated, automated, and streamlined approach to managing DNS, dynamic host configuration protocol (DHCP), and IP address management (together known as DDI), particularly when combined with protective DNS and network observability tools, offer a robust answer to meeting the NIS 2's mandate.

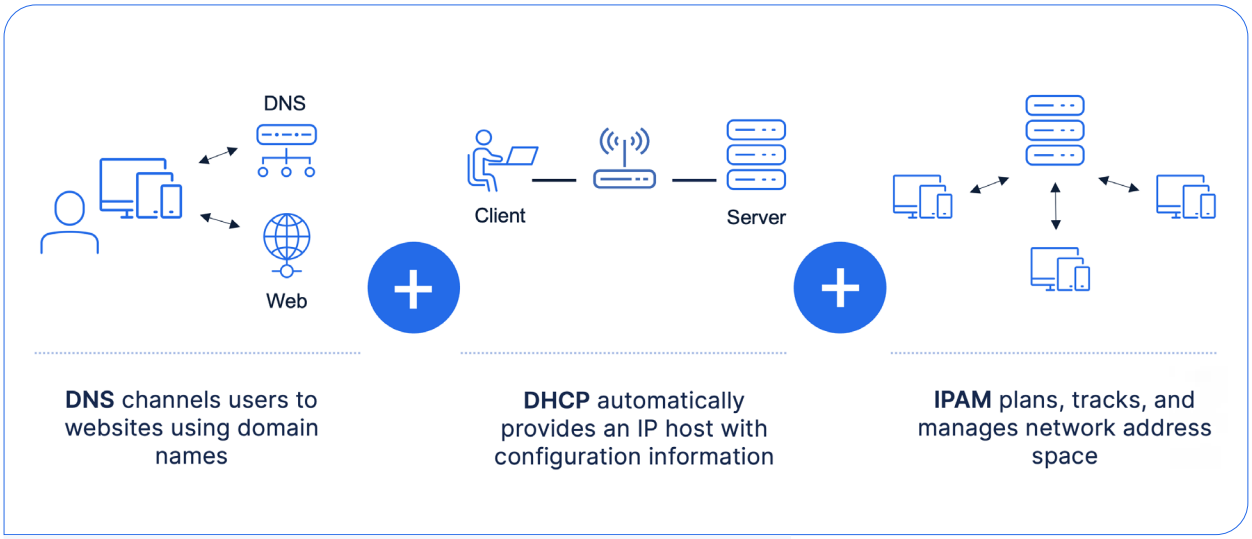


Figure 2. DNS, DHCP, and IP address management are at the heart of the digital enterprise.

Unified DDI

Unified DDI solutions integrate DNS, DHCP, and IP address management (IPAM) functionalities into a single platform, providing centralized visibility and control of IP resources and core network services. Unified DDI supports NIS 2 requirements by offering:

- **Improved network visibility**: A centralized and unified view of your DDI data provides comprehensive visibility into network assets, their configurations, and their interactions. This is essential for identifying vulnerabilities and ensuring robust network security.
- **Automated network management:** Automation reduces the risk of human error and enhances the efficiency of managing namespaces, IP addresses, and related services, ensuring that configurations are consistent and secure.
- **Compliance and auditing:** Unified DDI platforms often come with auditing and logging capabilities, which help organizations maintain detailed records of network configurations and changes. This facilitates compliance with NIS 2 requirements for documentation, reporting, and accountability.

Protective DNS solutions

Protective DNS solutions enhance network security by monitoring and filtering DNS traffic to block malicious queries and prevent access to harmful sites or attackers' command-and-control channels. When considering NIS 2 requirements, protective DNS solutions help with:

- **Threat detection and mitigation:** DNS security solutions often offer what is known as protective DNS: a service that analyzes DNS queries and mitigates or blocks connections to malicious domains. By blocking access to known malicious domains and records, protective DNS helps with early detection and prevention of cyber threats, reducing the risk of security incidents.
- **Incident response**: Protective DNS solutions provide deep visibility into DNS traffic, enabling quicker identification of—and incident response to—anomalies and potential threats.
- **Compliance and reporting:** Logging and monitoring DNS queries and responses helps with maintaining records required for compliance with NIS 2 and facilitates reporting to regulatory authorities.

Network observability and health

Network observability and health solutions focus on ensuring that your network infrastructure is secure, reliable, and resilient. Network observability and health capabilities that can help meet NIS 2 requirements include:

- **Continuous monitoring and assessment:** These tools continuously monitor the network for vulnerabilities and compliance with security policies, helping to identify and remediate issues before they can be exploited.
- **Resilience and redundancy:** Network observability and health solutions help you design and maintain a resilient network infrastructure with adequate redundancy, ensuring that critical services remain available even during incidents or outages.
- **Incident response and recovery:** These solutions provide tools and processes for effective incident response and recovery, ensuring that organizations can quickly restore normal operations after an operational or security incident.

Together, these types of solutions and capabilities address many elements of the NIS 2 directive. They provide actionable and demonstrable utility for:

- **Risk management**: Unified DDI, protective DNS, and network observability and health solutions help identify and mitigate risks through enhanced visibility, threat detection, and automated prevention.

- **Incident handling:** These solutions provide tools for quick detection, response, and reporting of cybersecurity incidents, aiding in effective incident handling and reducing the mean time to recovery.
- **Operational security:** By automating and centralizing network management, these solutions ensure consistent, fresh, and secure configurations, reducing vulnerabilities and enhancing operational security.
- **Reporting obligations:** The logging and auditing capabilities of these solutions help meet reporting obligations under NIS 2, ensuring that organizations can provide the necessary information to authorities when required.

BlueCat products that help meet the NIS 2 directive

Three of BlueCat's products—Integrity, Edge, and Infrastructure Assurance—offer core capabilities and features that can help enterprises comply with NIS 2 requirements.

Integrity

Integrity is BlueCat's platform for integrated DDI management for large enterprises. It simplifies and consolidates DDI visibility and control across the most complex network infrastructures. Powered by RESTful APIs, Integrity automates all aspects of DDI management. Integrity is comprised of BlueCat Address Manager and BlueCat DNS/DHCP Server (BDDS). Address Manager performs IP address management and acts as the main DNS and DHCP management platform (cluster or single node). Depending on your requirements, architecture, and footprint, BDDSes are single instances or clusters that selectively provide authoritative DNS and/or DHCP services. Each component is flexible and can be deployed physically or virtually.

Cloud Discovery & Visibility, an application add-on for Integrity, discovers the entirety of your on-premises and multicloud footprint and streams that data to Address Manager for up-to-date information.

Edge

Edge brings additional IP forwarding, discovery, resolution, and security capabilities to standard DDI infrastructure in three key areas: networking, security, and cloud. Edge is a lightweight, cloud-managed software solution that delivers advanced DNS capabilities via service points deployed across the edge of your network.

For networking
Edge uses intelligent forwarding via service points to set conditions and direct queries to the right destination.

For security
Edge provides advanced threat protection that also blocks malicious queries, policy enforcement, and intelligence from cutting-edge threat data feeds.

For cloud
Network teams can resolve DNS queries across complex cloud deployments with ease using Cloud Resolver.

Edge provides an intelligent layer of control to address threats, solve namespace collisions, and optimize query response latency based on organizational policies. By mapping directly to these frameworks, Edge assits users in meeting security and compliance requirements.

Infrastructure Assurance

Infrastructure Assurance provides proactive observability, troubleshooting, and remediation for network and security infrastructure, including Integrity, firewalls, and load balancers. It identifies hidden issues, conducts automated diagnosis, and offers expert-recommended remediation steps.

With deep visibility and automation, it prevents network disruptions and streamlines tasks like maintenance and high availability validation, efficiently analyzing critical data based on best practices. Key capabilities include:

- Auto-detection
- Auto-triage
- Automated configuration backup
- Anomaly detection
- Automated operations maintenance
- Benchmarking for infrastructure

Figure 3. Unified DDI, protective DNS, and network observability and health tools offer a robust answer to NIS 2 requirements.

Mapping NIS 2 articles to BlueCat products

The NIS 2 directive is broken into nine chapters, made up of consecutively numbered articles that cover topics applicable to member states and public and private entities.

Chapter	Title	Articles
I	General Provisions	1-6
II	Coordinated Cybersecurity Frameworks	7-13
III	Cooperation at Union and International Level	14-19
IV	Cybersecurity Risk-Management Measures and Reporting Obligations	20-25
V	Jurisdiction and Registration	26-28
VI	Information Sharing	29-30
VII	Supervision and Enforcement	31-37
VIII	Delegated and Implementing Acts	38-39
IX	Final Provisions	40-46

The table below offers detailed descriptions of how BlueCat products can help address specific mandates in NIS 2 directive articles.

NIS 2 article	BlueCat product	How it helps
Chapter I, Article 3, Essential and Important Entities		
4. For the purpose of establishing the list referred to in paragraph 3, Member States shall require the entities referred to in that paragraph to submit at least the following information to the competent authorities: (b) the address and up-to-date contact details, including email addresses, IP ranges and telephone numbers;	Integrity	Visibility of full IP footprint and namespaces, including public and private clouds, automated network discovery, and a single source of truth that stretches across all network footprints. Cloud Discovery & Visibility removes the need for manually updating managed ranges.
	Edge	Edge's Cloud Resolver gives full visibility into any cloud changes related to zones, virtual private clouds, or delegations, no matter how much they churn. Changes are automatically synchronized to Integrity's core IP address management functionality.
Chapter IV, Article 20, Governance		
2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.	Infrastructure Assurance	Continuous measurement of security, performance, and configuration metrics, cross-referenced with benchmark data defined by internal policies or external standards.
Chapter IV, Article 21, Cybersecurity Risk-Management Measures		
Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimise the impact of incidents on recipients of their services and on other services.	Integrity	Full operational management of DDI-related tasks and services across native and hybrid footprints. Cloud discovery and visibility, early detection, and prevention of threats.
	Edge	Intelligent and protective DNS that incorporates threat feeds with enumeration and resolution across churning assets or ephemeral entities.
	Infrastructure Assurance	Auto-triage and root-level diagnosis of issues—like errors, misconfigurations, vulnerabilities, and downtime—as soon as they occur, with contextual awareness of related issues.

NIS 2 article	BlueCat product	How it helps
2. (b) incident handling	Integrity	Digital asset lookup (IP prefixes or namespaces, including user-defined fields for arbitrary assets or tags). Forward and reverse resolution, including event enrichment for manual or automated investigation (via APIs plus integrations with security information and event management (SIEM) tools). Blocking and policy enforcement.
	Edge	Intelligent DNS, including DNS firewalling, threat feeds for real-time blocking, deep querying for identifying malicious or infected nodes, and protective policy enforcement. DNS forensics and investigation.
	Infrastructure Assurance	Performs auto-triage, issues alerts for detected anomalies, and provides recommended remediation steps that IT or security teams can follow to resolve identified issues.
2. (c) business continuity, such as back-up management and disaster recovery, and crisis management	Integrity	Application layer clustering, crossover high availability pairs, database replication, and, if required, manual system failover.
	Edge	Cloud-based management service with as many service points as desired for architectural redundancy and resiliency.
	Infrastructure Assurance	Health and capacity checks, external critical services and dependencies checks, high availability readiness, automated configuration backups, and misconfiguration identification.
2. (d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	Edge	Protection against an exploit's payloads, particularly for command-and-control channels, leveraging threat feeds, block lists, and domain generation algorithm detection.
	Infrastructure Assurance	Detection of anomalies and common vulnerabilities and exposures (CVEs) across multi-vendor environments, including auto-triage, reporting, and alerting.
2. (f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Edge	Reporting on potential distributed denial-of-service attempts and ability to isolate potentially infected user endpoints due to types of DNS queries and related data. These reports and data bolster or highlight the efficacy of other security devices, policies, or procedures.
	Infrastructure Assurance	Ongoing reporting and alerting on vulnerabilities and related proliferation across security infrastructure. Analysis using Mitre's CVE database and NIST's National Vulnerability Database.
2. (h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;	Edge	Block DNS over HTTPS resolvers with threat feeds or custom block lists.
2. (i) human resources security, access control policies and asset management	Integrity	Primary asset management for IP prefixes and addresses, namespaces, and zones, including role-based access control for managing DDI assets and services.

NIS 2 article	BlueCat product	How it helps
2. (i) human resources security, access control policies and asset management	Integrity	Supports single sign-on (SSO) via SAML 2.0 and acts as a service provider for SSO.
	Edge	Custom policy enforcement for intelligent DNS resolution based on source IP, site, or content.
2. (j) the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.	Edge	Supports configuration as a service provider in a SAML 2.0 federation, enabling an SSO user experience.
Chapter IV, Article 23, Reporting Obligations		
4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority (d) a final report not later than one month after the submission of the incident notification under point (b), including the following:		
4. (d) (i) a detailed description of the incident, including its severity and impact;	Integrity	Provides the underlying IP, digital asset management, and service logs for incident investigation and event enrichment across multiple systems. Without an IP address management tool and related fresh DNS entries, incident logs lack context and meaning.
	Edge	Intelligent DNS with extensive logging and deep querying allows for DNS forensics when rebuilding timelines and actions for digital events across an enterprise (including across private or public clouds).
	Infrastructure Assurance	Customizable dashboard for top 10 alerts to prioritize troubleshooting efforts based on the severity and frequency of identified issues.
4. (d) (ii) the type of threat or root cause that is likely to have triggered the incident;	Integrity	Provides core services and the context around netblocks, prefixes, namespaces, zones, and individual resource records to make sense of IPs, hostnames, and services throughout an organization.
	Edge	With historical DNS query and response logging and deep DNS forensics capabilities, incident investigations can look deeper and further into what led to flows and connections being made.
	Infrastructure Assurance	Performs observability based on triggers like performance metrics, security flaws, or configuration drift. Once a trigger condition is met, auto-triage follows a root cause analysis workflow to surface related issues and determine the cause(s).

NIS 2 article	BlueCat product	How it helps
4. (d) (iii) applied and ongoing mitigation measures;	Integrity	Detect and block DNS-based threats and mitigate security risks associated with DNS hijacking and cache poisoning, DHCP snooping, and IP address conflicts.
	Edge	Ongoing and intelligent mitigation delivered via DNS using ongoing threat intelligence feeds, automated blocking, SIEM integrations, policy enforcement, and machine learning (applied to evasion techniques like domain generation algorithms).
	Infrastructure Assurance	Codified domain expertise and community-contributed experience are used to auto-triage and recommend remediation steps, mitigating the risk of major outages for detected issues.

The outlook

Digital services and their secure operation are critical to the fabric of society. But with increased interdependence comes increased risk. Our responsibility to protect essential and important entities in critical sectors requires more accountability and cooperation than ever before.

Supported by BlueCat's solutions for unified DDI, protective DNS, and network observability and health, organizations can rise to the mandate to meet NIS 2 requirements.

As threats evolve and regulations become more complex, organizations will need to continually adapt their cybersecurity strategies. The integration of advanced solutions like BlueCat's will be crucial for maintaining security and compliance with NIS 2 and future regulations.

Learn more about how BlueCat can help you meet NIS 2 requirements.

This document is of a general and summary nature, provided for informational purposes only, and is not intended to be a substitute for professional advice and a detailed analysis of the Network and Information Security Directive (NIS 2) requirements. While we discuss how BlueCat products can assist with broader compliance efforts related to NIS 2, responsibility for ensuring compliance with all applicable laws and regulations remains with users of our products. Please review the full capabilities of BlueCat products, which can be found on our product documentation portal, and consult with your internal and external professional advisors regarding the appropriateness of BlueCat products for your intended purposes, including with respect to NIS 2 compliance.

Headquarters
4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
Phone: 1-416-646-8400 I 1-866-6931

bluecat.com

Ready to learn more?

Connect with a BlueCat representative and see how we can help you manage, build, and secure your network.

Contact us

WP-NIS 2-08-23-2024