Bitdefender

WHITE PAPER

Online & English Version Only

The NIS2 Directive: Enforcing Cybersecurity Capabilities

An overview of NIS2 requirements and how Bitdefender's tools and solutions can help meet regulatory compliance.

Trusted. Always.

Contents

ABSTRACT **3**

INCREASING CYBERATTACKS HIGHLIGHT THE NEED FOR NIS2 ..... **3**

NIS2 DIRECTIVE: ENHANCING THE FOUNDATIONAL PILLARS OF NIS1 ..... **4**

Industries and Organizations in Scope of NIS2 4

The Key Elements of the NIS2 Directive 5

Strengthening Security and Incident Reporting Under NIS2 6

NIS2 REQUIREMENTS AND BITDEFENDER SOLUTIONS FOR ORGANIZATIONS **7**

How Can Bitdefender Help Organizations Comply With NIS2 12

1. Risk Management and Threat Detection 12
2. Supply Chain and Vendor Security 12
3. Governance and Accountability 12
4. Incident Response and Recovery 12
5. Audits and Compliance 13

Legal Disclaimer for using the Bitdefender marketing content 14

About Bitdefender 14

Endnotes: 14

Abstract

This comprehensive guide offers an in-depth examination of the NIS2 requirements from a cybersecurity perspective, delineating how the Bitdefender solutions and services incorporate essential functionalities designed to assist organizations in ultimately achieving compliance with the NIS2 Directive.

Increasing Cyberattacks Highlight the Need for NIS2

The Network and Information Security Directive (NIS2) is the EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the European Union (EU).

The cybersecurity rules introduced in 2016 (through NIS) were updated by the NIS2 Directive that came into force in 2023. It modernizes the existing legal framework to keep up with increased digitization and an evolving cybersecurity threat landscape. By expanding the scope of cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities, and the European Union as a whole.

The NIS Directive (first EU cybersecurity law) is the first horizontal internal market instrument aimed at improving the resilience of network and information systems in the EU against cybersecurity risks. Despite its notable achievements, the NIS Directive has shown certain limitations. The digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape. New challenges have appeared, which require adapted and innovative responses.

Since the COVID-19 crisis, the European economy has grown more dependent on digital solutions than ever before. Sectors and services are becoming increasingly interconnected and interdependent. This has resulted in a growing and rapidly evolving cybersecurity threat landscape: any disruption, even one initially confined to one entity or one sector, can have cascading effects more broadly, potentially resulting in far-reaching and long-lasting negative impacts in the delivery of services across the whole internal market.

The COVID-19 pandemic has shown the vulnerability of our increasingly interdependent societies in the face of unexpected risks. It intensified the already emerging issues in the current NIS Directive and served as a catalyst for its revision. A concrete change to the NIS Directive in view of this crisis was to expand the scope of the new Directive, covering more specific elements in the health sector, such as entities carrying out research and development activities of medicinal products.

The European Commission carried out extensive stakeholder consultation to analyze the impact and identify the deficiencies of the NIS Directive, highlighting the following main issues:

- Insufficient level of cyber resilience among businesses operating in the EU
- Inconsistent resilience across Member States and sectors
- Insufficient common understanding of the main threats and challenges among Member States
- Lack of joint crisis response

As a result, and to respond to the growing threats due to digitalization and interconnectedness, in December 2020 the Commission proposed a revised set of future-proof rules aiming to strengthen the level of cyber resilience in the Union, on which the co-legislators have reached a political agreement on May 13, 2022 and formally adopted the new NIS2 Directive in late November 2022.

NIS2 Directive: Enhancing the Foundational Pillars of NIS1

The NIS2 Directive provides legal measures to boost the overall level of cybersecurity in the EU, in order to contribute to the overall functioning of the internal market. It builds on the three main pillars that were the basis of the NIS1 Directive:

- Building on the NIS1 strategy on the security of network and information systems, in order to achieve a high level of preparedness of Member States, the NIS2 Directive requires Member States to adopt a national cybersecurity strategy. Member States are also required to designate national Computer Security Incident Response Teams (CSIRTs), who are responsible for risk and incident handling, a competent national cybersecurity authority, and a single point of contact (SPOC). The SPOC must exercise a liaison function to ensure cross-border cooperation between the Member State authorities with the relevant authorities in other Member States and, where appropriate with the Commission and ENISA (European Network and Information Security Agency) as well as to ensure cross-sectorial cooperation with other competent authorities within its Member State.
- The NIS2 Directive also continues the NIS1 framework establishing the NIS Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States, and the CSIRTs Network, which promotes swift and effective operational cooperation between national CSIRTs.
- The NIS1 Directive ensures that cybersecurity measures are taken across seven sectors, which are vital for our economy and society, and which rely heavily on ICT, such as energy, transport, banking, financial market infrastructures, drinking water, healthcare and digital infrastructure.

Public and private entities identified by the Member States as operators of essential services (OES) in these sectors are required to undertake a cybersecurity risk assessment and put in place appropriate and proportionate security measures. They are required to notify serious incidents to the relevant authorities. Furthermore, providers of key digital services (digital service providers or DSPs), such as search engines, cloud computing services and online marketplaces, have also to comply with the security and notification requirements under the Directive. At the same time, the latter are subject to a so-called ‘light-touch’ regulatory regime, which entails that those entities are not subjected to ex-ante supervisory measures.

NIS2 Directive significantly expands the scope of sectors and introduces a size threshold to define which entities fall in its scope and would be required to report significant cybersecurity incidents to the national competent authorities.

Industries and Organizations in Scope of NIS2

The NIS2 covers entities from the following sectors:

Sectors of high criticality: energy (electricity, district heating and cooling, oil, gas and hydrogen); transport (air, rail, water and road); banking; financial market infrastructures; health including manufacture of pharmaceutical products including vaccines; drinking water; waste water; digital infrastructure (internet exchange points; DNS service providers; TLD name registries; cloud computing service providers; data center service providers; content delivery networks; trust service providers; providers of public electronic communications networks and publicly available electronic communications services); ICT service management (managed service providers and managed security service providers), public administration and space.

Other critical sectors: postal and courier services; waste management; chemicals; food; manufacturing of medical devices, computers and electronics, machinery and equipment, motor vehicles, trailers and semi-trailers and other transport equipment; digital providers (online marketplaces, online search engines, and social networking service platforms) and research organizations.

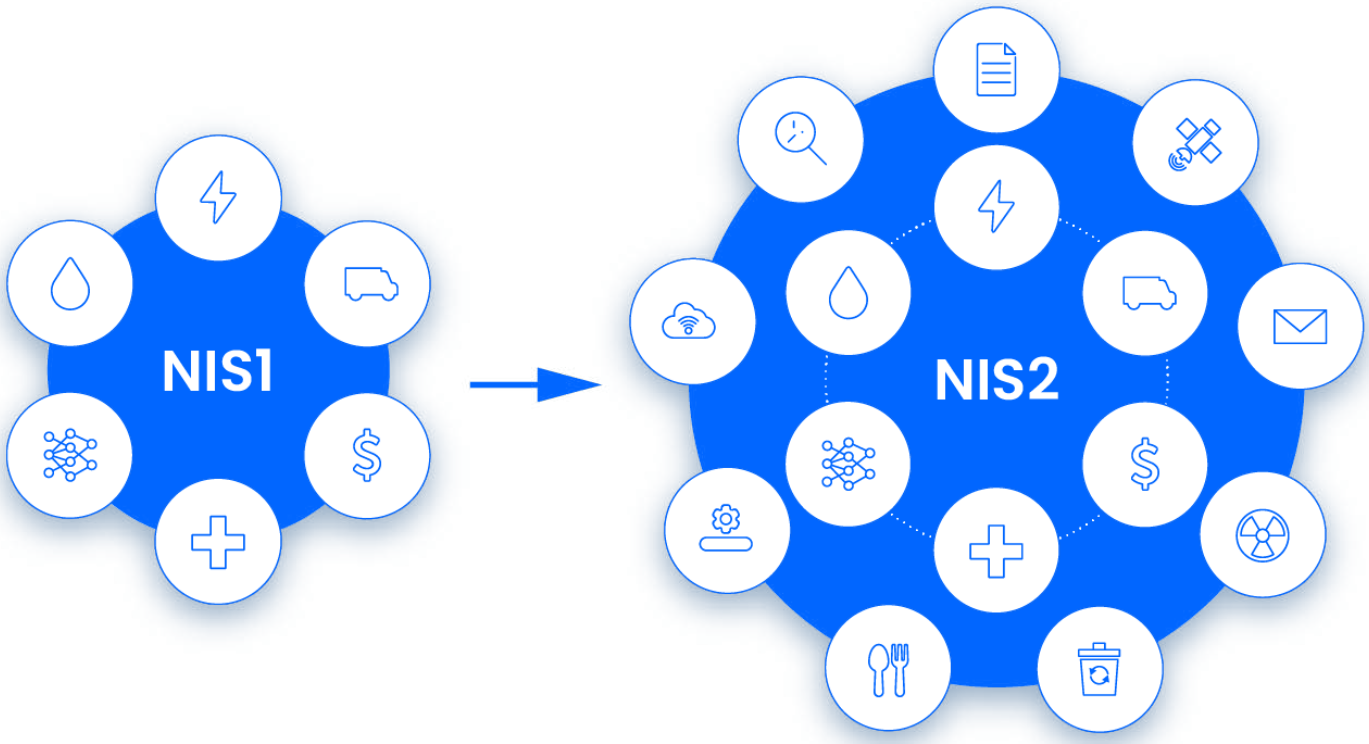

Image source: nis2directive.eu

The Key Elements of the NIS2 Directive

NIS2 aims to address the deficiencies of the previous NIS Directive rules, to adapt it to the current needs and make it future-proof.

To this end, the Directive expands the scope of the previous rules by adding new sectors based on their degree of digitalization and interconnectedness and how crucial they are for the economy and society, by introducing a clear size threshold rule— meaning that all medium and large-sized organizations in selected sectors will be included in the scope. At the same time, it leaves certain discretion to Member States to identify smaller entities with a high security risk profile that should also be covered by the obligations of the new Directive.

The new Directive also eliminates the distinction between operators of essential services and digital service providers. Entities would be classified based on their importance and divided into two categories: essential and important entities, which will be subjected to different supervisory regime.

It strengthens and streamlines security and reporting requirements for organizations by imposing a risk management approach, which provides a minimum list of basic security elements that must be applied. The new Directive introduces more precise provisions on the process for incident reporting, content of the reports and timelines.

Furthermore, NIS2 addresses security of supply chains and supplier relationships by requiring individual organizations to address cybersecurity risks in the supply chains and supplier relationships. At European level, the Directive

strengthens supply chain cybersecurity for key information and communication technologies. Member States in cooperation with the Commission and ENISA, may carry out Union level coordinated security risk assessments of critical supply chains, building on the successful approach taken in the context of the Commission Recommendation on Cybersecurity of 5G networks.

The Directive introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonizing sanctions regimes across Member States.

It also enhances the role of the Cooperation Group in shaping strategic policy decisions and increases information sharing and cooperation between Member State authorities. It also enhances operational cooperation within the CSIRT network and establishes the European cyber crisis liaison organization network (EU-CyCLONe) to support the coordinated management of large-scale cybersecurity incidents and crises.

NIS2 also establishes a basic framework with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creates an EU vulnerability database for publicly known vulnerabilities in ICT products and ICT services, to be operated and maintained by the EU agency for cybersecurity (ENISA).

Strengthening Security and Incident Reporting Under NIS2

The evaluation of the current rules on security and incident reporting requirements has shown that in some cases Member States have implemented these requirements in significantly different ways. This has created an additional burden for organizations operating in more than one Member State.

Furthermore, when it comes to cybersecurity requirements, the European Commission wants to be sure that all organizations address the necessary core set of elements in their cybersecurity risk management policies.

For this reason, NIS2 includes a list of 10 key elements that all companies must address or implement as part of the measures they take, including incident handling, supply chain security, vulnerability handling and disclosure, the use of cryptography and where appropriate, encryption.

When it comes to incident reporting, it’s essential to strike the right balance between the need for swift reporting to avoid the potential spread of incidents, and the need for in-depth reporting to draw valuable lessons learned from individual incidents. The new Directive foresees a multiple–stage approach to incident reporting. Affected organizations have 24 hours from when they first become aware of an incident to submit an early warning to the CSIRT or competent national authority which would also allow them to seek assistance (guidance or operational advice on the implementation of possible mitigation measures) if they request it. The early warning should be followed by an incident notification within the 72 hours of becoming aware of the incident and a final report no later than one month later.

NIS2 Requirements and Bitdefender Solutions for Organizations

NIS2 DIRECTIVE REQUIREMENTS		BITDEFENDER SOLUTION	HOW CAN IT HELP
Chapter II, Article 11 **Requirements, technical capabilities and tasks of CSIRTs**	3. The CSIRTs shall have the following tasks: (a) monitoring and analyzing cyber threats, vulnerabilities and incidents at national level and, upon request, providing assistance to essential and important entities concerned regarding real-time or near real-time monitoring of their network and information systems;	Bitdefender IntelliZone (Threat Intelligence)	Bitdefender IntelliZone (also known as the Threat Intelligence portal) is an easy-to-use solution designed to assist security professionals in proactively identifying, monitoring, and mitigating cyber-threats.
	(d) collecting and analyzing forensic data and providing dynamic risk and incident analysis and situational awareness regarding cybersecurity;	ERA - Endpoint Risk Analytics	Bitdefender's integrated Endpoint Risk Analytics (ERA) solution identifies, assesses, and remediates Windows endpoints weaknesses via security risk scans (on-demand or scheduled via policy), taking into account a vast number of indicators of risk. After scanning the network for indicators of risk, an overview of the network risk status is delivered through the Risk Management dashboard. Risk Management generates a risk score unique to each organization and provides insights into various endpoint misconfigurations, application vulnerabilities, and user-related risks in a consolidated security posture overview. The prioritized list enables the security team to focus on the essential items that expose the organization to cyber risks. The platform dynamically adjusts the company risk score based on vulnerabilities that have already been exploited within the organization's industry.
	(e) providing, upon the request of an essential or important entity, a proactive scanning of the network and information systems of the entity concerned to detect vulnerabilities with a potential significant impact;	Offensive Security Services	Bitdefender Offensive Security Services provides organizations with Penetration (Pen) Testing and Red Teaming services to ensure key security weaknesses and vulnerabilities are identified in order to improve and strengthen the security of IT environments.
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.	Bitdefender GravityZone Webinars	Bitdefender GravityZone webinars offer live or pre-recorded sessions and trainings led by highly experienced Bitdefender professionals, focusing on specific topics such as: ransomware defense, product updates (GravityZone) or cyber security services (Managed Detection and Response, Offensive Security – Pen Testing and Red Teaming, Security Assessment etc.).
		Ransomware & Phishing Defense Services	Ransomware Defense service includes a Ransomware Defense Assessment against our framework, for assessing your organization's readiness against a ransomware attack, and advisory in implementation of policies and security controls towards the Ransomware Defense Framework, built on decades of experience investigating global ransomware attacks and international security frameworks. The framework zeroes in on the specific security controls that directly contribute to your defense against and recovery from ransomware attacks. Phishing simulations cover Spear Phishing campaigns - highly realistic, simulated cyber-attacks and security awareness training to test resilience and vigilance, to both educate employees about this prevailing cyber threat and always keep them vigilant.
		Cybersecurity Advisory Services	Cybersecurity Advisory Services include a Cyber Security Review (CSR), a comprehensive and objective analysis of your organization's current security posture (across core business processes, endpoints, digital and physical footprint, threats, and all other plausible risks) with a unique methodology refined over decades of diverse expertise from security leadership and threat forensics to regulatory and legal compliance. By uncovering the gaps in your security posture and comprehensively understanding your business challenges, we can put forth a tailored strategy to fit into your organization's bigger picture.

NIS2 DIRECTIVE REQUIREMENTS		BITDEFENDER SOLUTION	HOW CAN IT HELP
Chapter IV, Article 21 **Cybersecurity risk-management measures**	1. Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organizational 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 minimize the impact of incidents on recipients of their services and on other services. 2. The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:		
	(b) incident handling;	EDR - Endpoint Detection and Response	Bitdefender GravityZone EDR continuously monitors networks for suspicious activity and gives security teams the tools to fight off even the most evasive attacks, including a set of automated tasks in GravityZone (enabled via custom detection rules) that can help mitigate threats and automatically deal with incidents by executing one or more of the following actions: Isolate, Collect investigation package, Add to Sandbox, Antimalware scan, Quarantine, Risk scan, Kill process.
		MDR - Managed Detection and Response	Bitdefender MDR offers end-to-end incident and breach response services, with automated actions to terminate intrusions once the malicious activity is confirmed. It also provides customized notifications and expert recommendations, featuring personalized alert systems notifying you of potential threats and offering expert guidance on risk handling.
	(c) business continuity, such as backup management and disaster recovery, and crisis management;	Bitdefender's Ransomware Mitigation	Ransomware Mitigation is an integrated GravityZone feature designed to mitigate the impact of an active ransomware attack, using detection and remediation technologies to keep your data safe. Whether the ransomware is known or new, it detects abnormal encryption attempts and blocks the process. Afterwards, it recovers the files from backup copies and restores them to their original location.
		EDR - Endpoint Detection and Response	Bitdefender GravityZone EDR empowers security teams to uncover attacks in their early stages, including automated response capabilities such as isolating infected devices (Quarantine) or terminating malicious processes (Kill process), which helps reduce response time and ensure continuous business operations.
		MDR - Managed Detection and Response	Bitdefender MDR provides uninterrupted cybersecurity operations, offering round-the-clock protection against evolving threats. This also involves Threat Management, encompassing comprehensive threat oversight (detection, analysis, and swift risk mitigation), and Pre-Approved Actions (PAAs), facilitating prompt responses to identified threats through pre-authorized actions, helping reduce response times ensuring that business operations remain uninterrupted and secure
	(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	XDR - Extended Detection and Response	Bitdefender GravityZone XDR enhances supply chain security by automatically triaging, correlating, and contextualizing incidents across various platforms, hybrid infrastructures and security tools, providing a holistic view of potential threats across the entire supply chain and helping to identify and mitigate risks early.
		MDR - Managed Detection and Response	Bitdefender MDR service combines cybersecurity for endpoints, network and security analytics with the threat-hunting expertise of a SOC fully staffed by security analysts with expertise from a wide range of environments, including global intelligence agencies, to help maintaining the integrity and security of the supply chain.

NIS2 DIRECTIVE REQUIREMENTS		BITDEFENDER SOLUTION	HOW CAN IT HELP
Chapter IV, Article 21 **Cybersecurity risk-management measures**	(e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	XDR - Extended Detection and Response	Bitdefender GravityZone XDR consolidates monitoring information and insights in a single dashboard, automating an appropriate response, providing recommendations into how vulnerabilities can be fixed, and giving security teams visibility into the security status of digital assets, intelligence into emerging threats, and the ability to efficiently muster a response when attacks occur.
		MDR - Managed Detection and Response	Bitdefender MDR provides 24/7 system monitoring to ensure proper and prompt detection of vulnerabilities and offers access to a team of security experts who analyze them, provide detailed reports, and recommend corrective actions to prevent future issues.
	(f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	Cybersecurity Advisory Services	Cyber Security Review (CSR), part of the Cybersecurity Advisory Services, is a holistic analysis of cybersecurity gaps across people, processes, and technology, with the objective of empowering business processes of the organizations by deploying specific solutions for digital footprint or fixing processes to mitigate threats in and out of the organization.
	(g) basic cyber hygiene practices and cybersecurity training;	Bitdefender GravityZone Webinars	Bitdefender GravityZone webinars frequently offer comprehensive guidelines and critical strategies for safeguarding and preserving the security and integrity of digital ecosystems.
		Ransomware & Phishing Defense Services	Phishing simulation campaigns highlight the attention to detail that real threat actors employ in order to trick humans, the weakest link in every organization's security posture, to educate employees about this ongoing cyber threat and ensure they remain vigilant at all times.
		Cybersecurity Advisory Services	The Security Awareness Training, developed and continuously updated by in-house consultants, includes topics that address current threats and scams, email security, and best practices for working remotely.
	(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;	Volume Encryption	The Volume Encryption feature provides full disk encryption of your Windows and macOS systems through centralized policies. The GravityZone management console also shows the encryption status of volumes, to provide evidence of compliance.
		Email Security (TLS)	Bitdefender GravityZone Email Security add-on includes Transport Layer Security (TLS) usage to encrypt the tunnel between sending and receiving SMTP servers. This increases the security of emails and makes interception less likely. There are two methods of setting up the TLS encryption using message rules: - Enforced TLS – it will cause the server to only send an email if TLS is supported by the remote site. - Opportunistic TLS - it will cause Email Security to attempt a TLS connection if TLS is advertised by the remote site; if this fails, Email Security will fall back to a non-TLS connection (and plain-text SMTP).
	(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.	Bitdefender GravityZone 2FA	Bitdefender GravityZone 2FA (two-factor authentication) is mandatory for all user accounts and it cannot be disabled.
		Cloud Security Posture Management (CSPM+)	Bitdefender GravityZone CSPM+ is a cloud-native security solution capable of detecting numerous key configurations on cloud resources and identities, including whether multi-factor authentication is enabled.

NIS2 DIRECTIVE REQUIREMENTS		BITDEFENDER SOLUTION	HOW CAN IT HELP
Chapter IV, Article 23 **Reporting obligations**	1. Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability. 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: (a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact; (b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise; (c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates; (d) a final report not later than one month after the submission of the incident notification under point (b), including the following:		
	(i) a detailed description of the incident, including its severity and impact;	MDR - Managed Detection and Response	Bitdefender MDR service provides a detailed description of each incident. This includes outlining the nature of the threat, the detection process, the steps taken for mitigation, and the resolution strategy. This comprehensive documentation helps organizations understand the incident thoroughly and equips them for future threat prevention.
	(ii) the type of threat or root cause that is likely to have triggered the incident;	EDR - Endpoint Detection and Response	Bitdefender GravityZone EDR provides detailed information about the type of threat and the root cause of an incident through real-time attack visualization. It uses behavioral analytics to detect sophisticated threats and offers comprehensive visibility into endpoint activities. This allows security analysts to understand how a breach occurred, track the movements of threat actors within the network, and respond effectively.
		XDR - Extended Detection and Response	Bitdefender GravityZone XDR provides a comprehensive view of threats and incidents by correlating data from multiple sources across the network. It performs root cause analysis to determine how the threat entered the network, its progression, and the tactics, techniques, and procedures (TTPs) used by the attackers, helping security teams to quickly identify, understand, and respond to complex threats.
		MDR - Managed Detection and Response	Bitdefender MDR service offers detailed insights into the type of threat and the root cause of an incident through several key processes, including threat identification, incident investigation, root cause analysis and comprehensive reports which include the type of threat, the root cause, and the steps taken to mitigate the incident.

NIS2 DIRECTIVE REQUIREMENTS		BITDEFENDER SOLUTION	HOW CAN IT HELP
Chapter IV, Article 23 **Reporting obligations**	(iii) applied and ongoing mitigation measures;	EDR - Endpoint Detection and Response	Bitdefender GravityZone EDR provides comprehensive reports that include information on applied and ongoing mitigation measures, offering insights into the actions taken to address detected threats, helping security teams understand the steps that have been implemented to mitigate risks. The reports typically include incident details, mitigation actions and the continuous actions to monitor and prevent further damage.
		XDR - Extended Detection and Response	Bitdefender GravityZone XDR provides detailed reports designed to help security teams effectively manage and respond to security incidents, including the actions taken to address detected threats and the continuous measures in place to prevent further incidents.
		MDR - Managed Detection and Response	Bitdefender MDR service include robust, actionable reports powered by big data analytics, artificial intelligence, and human expertise, providing meaningful insights into security incidents, highlighting cybersecurity trends, and guiding remediation efforts. The After Actions report is an all-inclusive document that provides a comprehensive analysis of a cybersecurity incident that has transpired within an organization's environment, detailing the severity of the incident and concluding concludes with an in-depth list of recommendations to prevent such incidents from happening in the future. These could range from strengthening security controls and improving incident response procedures, to employee training and awareness programs. It serves as a learning tool, helping organizations to enhance their cybersecurity posture and resilience against future attacks.

How Can Bitdefender Help Organizations Comply With NIS2

The NIS2 Directive introduces several key requirements to enhance cybersecurity across the European Union:

- **Risk Management and Incident Reporting:** Organizations must adopt risk-based security measures and report incidents to the relevant authorities within 24 hours.
- **Supply Chain Security:** Requires better security measures and awareness for third-party vendors and supply chains.
- **Governance and Accountability:** Clear lines of accountability for cybersecurity management at the executive level.
- **Incident Response:** Organizations must have incident response and recovery plans in place.
- **Audits and Compliance:** Periodic audits and assessments of cybersecurity measures to ensure compliance.

Bitdefender provides several solutions and services that can help organizations meet the key requirements of the NIS2 Directive:

1. Risk Management and Threat Detection

- **GravityZone Security Platform:** Bitdefender offers advanced threat detection, response, and prevention tools with real-time risk analytics. It supports NIS2's requirement for adopting risk-based security measures by continuously monitoring and assessing threats.
- **Endpoint Detection and Response (EDR):** Detects suspicious activities and helps organizations contain potential threats, aligning with NIS2's proactive risk management expectations.

2. Supply Chain and Vendor Security

- **Extended Detection and Response (XDR):** Provides visibility into the entire supply chain and network, ensuring comprehensive coverage and threat detection.
- **Bitdefender Managed Detection and Response (MDR):** The service provides continuous monitoring, ensuring quick identification and mitigation of supply chain risks in compliance with NIS2.
- **Bitdefender also achieved ISO 27001 certification and is SOC2 Type 2 certified, proving commitment to closely safeguarding customer data and managing information security in an operationally effective manner.**

3. Governance and Accountability

- **Security Orchestration and Reporting:** Bitdefender's solutions offer centralized reporting and management, ensuring that cybersecurity measures are visible and accountable at the executive level, which is required under NIS2.
- **Compliance and Reporting Tools:** Helps with auditing and creating compliance reports that can be presented to regulators.

4. Incident Response and Recovery

- **Incident Response Services:** Bitdefender offers Incident Response and Forensics services, which can support organizations in addressing incidents in a timely manner as required by NIS2.
- **Backup and Data Recovery Solutions:** Provides backup solutions that ensure organizations can recover data after a cyberattack, aligning with the NIS2 requirements for incident recovery.

5. Audits and Compliance

- **Security Audit Features:** Bitdefender's solutions provide tools for performing regular security assessments, vulnerability management, and audits, which are essential for NIS2 compliance.

Bitdefender's comprehensive cybersecurity solutions, from advanced threat intelligence to risk management and incident response, help fit seamlessly with NIS2's objectives of improving security across critical sectors and digital services.

Legal Disclaimer for using the Bitdefender marketing content

The marketing content is owned by Bitdefender and its affiliates and is subject to copyright, trademark, patents and trade secrets and other intellectual property rights under United States, foreign laws, and international conventions.

All the information presented is provided AS IS, only for information purposes. The marketing content presented implies no legal liability, no express representations and warranties or any assumptions. You have an obligation to have your own assessment.

Bitdefender and its affiliates retain ownership of the marketing content and all right, title, and interest, including all feedback provided, modifications, derivative works, developments, improvements, enhancements, translations, and all intellectual property rights.

The marketing content can be used if prior authorized by Bitdefender in written.

Thereinafter You will have the following usage rights of Bitdefender provided marketing content:

1.1 if such marketing content is limited to 250 characters (short format), then such content can be reproduced “as is” (original marketing content);

1.2 if such marketing content is larger than 250 characters (extended format), then, a maximum of 30% of Bitdefender full marketing content can be reproduced “as is” and the rest of the marketing content to be published by Partner will have to be re-worded. Such re-worded part shall not distort the purpose of the Marketing Content and shall not bring any negative impact on Bitdefender image and brand.

About Bitdefender

Bitdefender is a cybersecurity leader delivering best-in-class threat prevention, detection, and response solutions worldwide. Guardian over millions of consumer, enterprise, and government environments, Bitdefender is one of the industry’s most trusted experts for eliminating threats, protecting privacy, digital identity and data, and enabling cyber resilience. With deep investments in research and development, Bitdefender Labs discovers hundreds of new threats each minute and validates billions of threat queries daily. The company has pioneered breakthrough innovations in antimalware, IoT security, behavioral analytics, and artificial intelligence and its technology is licensed by more than 180 of the world’s most recognized technology brands. Founded in 2001, Bitdefender has customers in 170+ countries with offices around the world. For more information, visit https://www.bitdefender.com

Endnotes:

- “Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)” - https://digital-strategy.ec.europa.eu/en/policies/nis2-directive
- “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)” - https://eur-lex.europa.eu/eli/dir/2022/2555

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071
T: +40 21 4412452
F: +40 21 4412453

US HQ
3945 Freedom Circle,
Suite 500, Santa Clara,
CA, 95054

bitdefender.com

Bitdefender-BSG-NIS2-Whitepaper-NoPrint-creat8266-en_EN
CD-06/12/24 • MD-January 17, 2025 9:56 am