WHITEPAPER

NIS 2 Compliance with WatchGuard Technologies

Table of Contents

Contents

Introduction

The number of cyberattacks has skyrocketed in recent years, with some estimates pointing to a 600% increase since 2020. This surge is partly due to the rapid shift to remote work, which is creating vulnerabilities in newly digitized systems. Hackers also target a wider range of victims, from businesses to educational institutions, and their methods are constantly evolving.

This alarming trend highlights the critical need for robust cybersecurity measures. Businesses and organizations must invest in data protection, employee training, and updated security software to stay ahead of cybercriminals. Protecting our increasingly interconnected world requires a proactive approach to cybersecurity.

Background - NIS

The Network and Information Systems Directive (EU) 2016/1148 (NIS), implemented in 2016, was the European Union's first attempt at a unified cybersecurity law. It aimed to establish a baseline level of security across critical infrastructure sectors like energy, transport, and finance. NIS required member states to implement laws mandating operators to report security incidents and take measures to manage cybersecurity risks.

However, NIS had its limitations. It didn't cover a broad enough range of entities, and its reporting requirements were considered lax. Additionally, enforcement power resided with individual member states, leading to inconsistencies in implementation across the EU. These shortcomings paved the way for the introduction of the stricter Network and Information Systems Directive (EU) 2022/2555 (NIS 2) in 2022 (also known as NIS 2).

Background – NIS 2

NIS 2 is the successor to the original NIS (which was repealed by NIS 2). Adopted in December 2022 by the Council of the European Union and the European Parliament, EU member states must transpose the NIS 2 directive into national law by October 17, 2024.[1] However, they have until April 17, 2025, to determine the list of organizations that must comply.

NIS 2 significantly strengthens cybersecurity regulations across the European Union. It applies to a wider range of sectors, encompassing essential entities like waste management, postal services, and manufacturers of critical infrastructure.

The directive's key objectives are to enforce a baseline of cybersecurity measures across these sectors. This includes risk-management practices, incident reporting obligations, and supply chain security assessments. Secondly, NIS 2 aims to improve EU-wide cooperation on cybersecurity threats. It establishes an obligation for competent authorities, cyber crisis management authorities, single points of contact on cybersecurity, and computer security incident response teams (CSIRTs) in each member state and fosters information sharing among those authorities.

Regulation vs. Directive

An EU regulation directly sets the law for all member states, while an EU directive outlines a goal that each member state must achieve through its national laws (also known as transposition).

Understanding NIS 2 Compliance

The NIS 2 Directive categorizes entities into two groups based on the criticality of their services: "Essential" and "Important ." Entities are identified within Annexes I and II of the directive.

Important Entity	Essential Entity
Minimum of 50 employees	Minimum of 250 employees
Minimum 10M Euro turnover or 10M Euro annual balance sheet	Minimum 50M Euro turnover or 43M Euro annual balance sheet

Table 1. Entity Classifications by Size

Annex I lists sectors considered highly critical. Here, any large organization operating in these sectors falls under the Essential Entity category and must comply with NIS 2. These sectors include energy, transport, banking, wastewater, and digital infrastructure. Additionally, midsized organizations within these sectors can be deemed Essential depending on their size thresholds (e.g., number of employees).

Annex II covers other critical sectors, but entities here are classified as Important. This includes postal and waste management services, manufacturers of critical infrastructure, and specific public administration bodies. Unlike Annex I, only large or midsized entities in these sectors must comply with NIS 2.

[1] The Netherlands announced in January 2024 that they will miss the October date while encouraging organizations to take measures to protect the continuity of their business.

Annex I (Important AND Essential)	Annex II (Important ONLY)
Energy: Electricity, District Heating & Cooling, Oil, Gas, Hydrogen	Postal & Courier Services
Transport: Air, Rail, Water, Road	Waste Management
Banking	Manufacture, Production, and Distribution of Chemicals
Financial Market Infrastructures	Production, Processing, and Distribution of Food
Health	Manufacturing: Medical Devices, Computer/Electronic/Optical Products, Electrical Equipment, Machinery, Motor Vehicles, Trailers, Semi-Trailers
Drinking Water	Digital Providers
Waste Water	Research
Digital Infrastructure	
Information and Communication Technology Service Management	
Public Administration	
Space	

Table 2. Sectors and Subsectors for Each Annex

Multinational organizations operating in the EU and offering critical services must comply with NIS 2. Check the directive's Annex I and Annex II to see if your sector falls under Essential or Important entities. Don't forget that compliance requirements might differ by member state, so research the specific local regulations you must follow in each EU country in which you operate.

NIS 2 Compliance and Service Providers

The NIS 2 directive Annex I classifies ICT service management, which includes managed service providers (MSPs) and managed security service providers (MSSPs), as a highly critical sector. This means that MSPs and MSSPs are subject to stricter cybersecurity requirements under NIS 2.

These stricter requirements dictate that MSPs/MSSPs must implement suitable technical, operational, and organizational measures to handle cybersecurity risks, encompassing incident prevention, impact minimization, and reporting to authorities. In addition, with a heightened focus on supply chain security, organizations listed in Annex I, relying on MSPs/MSSPs, may have to assess their providers' cybersecurity practices as part of vendor risk management.

Baseline Cybersecurity Measures

The NIS 2 directive mandates a baseline of cybersecurity measures for Essential and Important entities across various sectors. These measures focus on a risk-management approach, requiring entities to conduct regular risk assessments, implement technical and organizational safeguards (like firewalls and access controls), and establish procedures for detecting, reporting, and responding to security incidents.

The NIS 2 Directive requires EU member states to ensure Essential and Important entities take appropriate cybersecurity measures. These measures should be tailored to the entity's network and information systems' specific risks. This includes measures to prevent incidents, minimize their impact on service recipients and other services, and ultimately maintain a security level that aligns with the potential risks.

Factors like technology advancements, relevant European and international security standards, and implementation costs should be considered when determining the appropriate measures. Additionally, the proportionality of these measures should be assessed based on the entity's size, the likelihood and severity of potential incidents (including societal and economic impacts), and the entity's overall exposure to cyber threats. Baseline measures outlined in the NIS 2 directive include:

- Risk analysis and information system security policies
- Incident handling
- A business continuity plan that includes backup management, disaster recovery, and crisis management
- Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers
- Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure
- Policies and procedures to assess the effectiveness of cybersecurity risk-management measures
- Basic cyber hygiene practices and cybersecurity training
- Policies and procedures regarding using cryptography and, where appropriate, encryption
- Human resources security, access control policies, and asset management

The core NIS 2 requirements follow the same principles for Essential and Important entities. However, the level of detail, stringency, and reporting obligations might be more demanding for Essential entities due to the heightened criticality of their services.

Reporting Obligations

NIS 2 mandates stricter incident reporting requirements compared to the previous NIS Directive. These requirements apply to both Essential and Important entities:

- **Early Warning:** Upon identifying a significant incident, entities must submit an "early warning" report to the relevant authority within 24 hours. This report should provide a preliminary assessment of the incident's nature and potential impact.
- **Incident Notification:** Following the early warning, a more detailed "incident notification" report must be submitted within 72 hours. This report should include details like the time and type of incident, affected systems and data, and the actions taken to mitigate the impact.
- **Final Report:** No later than one month after the initial notification, a final report with a comprehensive analysis of the incident, root cause, lessons learned, and implemented corrective actions needs to be submitted.

Beyond notifying the competent authority in their member state, entities may also be required to inform other member states, their customers, and the public.

NIS 2 Compliance Authority

The primary responsibility for enforcement falls on individual EU member states. Each member state designates a "competent authority" responsible for overseeing compliance within their territory or vertical market. Depending on the member state's structure, these authorities can be national cybersecurity agencies, sectoral regulators, or a combination. They conduct inspections, investigate reported incidents, and have the power to impose sanctions for non-compliance.

While enforcement occurs at the member-state level, NIS 2 fosters cooperation across the EU. Each member state establishes a single point of contact for communication with other authorities. This facilitates information sharing about cyber threats, best practices, and coordinated responses to large-scale cyber incidents. Additionally, the European Commission oversees the overall implementation and effectiveness of NIS 2 across the EU. They can initiate infringement procedures against member states deemed not adequately enforcing the directive.

Essential Entities	Important Entities
On-site inspections and off-site supervision, including random checks conducted by trained professionals.	On-site inspections and off-site ex post supervision conducted by trained professionals.
Regular and targeted security audits carried out by an independent body or a competent authority.	Targeted security audits carried out by an independent body or a competent authority.
Ad hoc audits, including where justified on the grounds of a significant incident or an infringement of this Directive by the Essential entity.	N/A
Security scans based on objective, non-discriminatory, fair, and transparent risk assessment criteria where necessary, with the cooperation of the entity concerned.	Security scans based on objective, non-discriminatory, fair and transparent risk assessment criteria where necessary, with the cooperation of the entity concerned.
Requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities.	Requests for information necessary to assess the cybersecurity risk-management measures adopted by the entity concerned, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities.
Requests to access data, documents, and information necessary to carry out their supervisory tasks.	Requests to access data, documents, and information necessary to carry out their supervisory tasks.
Requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.	Requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

Table 3. Supervisory and Enforcement Measures

Penalties for Violations of NIS 2

NIS 2 enforces hefty penalties for non-compliance, with the severity depending on the entity's classification (Essential vs. Important) and the member state enforcing the directive. These are maximum fines, and the actual penalty imposed will be determined by the competent authority in each EU member state based on the severity of the non-compliance.

It's important to note that financial penalties are not the only consequence of non-compliance. Significant reputational damage can also result from non-compliance, so Essential and Important entities must take the directive seriously and implement the necessary cybersecurity measures.

Essential Entities	Important Entities
Fine that is the greater of 10M Euro or 2% of the entity's worldwide turnover in the preceding year	Fine that is the greater of 7M Euro or 1.4% of the entity's worldwide turnover in the preceding year
Public disclosure of violations	Public disclosure of violations
Suspension of or restriction on operations	Restriction on operations
Management liability up to the CEO level	

Table 4. Administrative Penalties

NIS 2 and Security Frameworks

ISO 27001 is a globally recognized standard that specifies the requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). While not a guarantee of NIS 2 compliance, ISO 27001 certification demonstrates a strong information security posture and can help organizations meet many NIS 2 requirements. Organizations subject to NIS 2 can leverage ISO 27001 as a roadmap for achieving compliance.

WatchGuard has obtained ISO/IEC 27001:2013 certification for its ISMS. The scope of the certification is limited to the ISMS of the WatchGuard infrastructure for the configuration, management, support, and delivery of the WatchGuard ID, AuthPoint multi-factor authentication, Endpoint, and WatchGuard Cloud applications and services that support Firebox firewalls and Wi-Fi in WatchGuard Cloud.

Besides ISO 27001, EU member states are exploring other frameworks, like NIST CSF and CIS Controls. Implementation of these frameworks is expected to be considered sufficient proof that suitable security measures have been taken. Again, it is important to check the local regulations for the EU member states in which you operate.

How WatchGuard Technologies Supports NIS 2 Compliance

WatchGuard's Unified Security Platform can streamline compliance with NIS 2 regulations by offering a single platform to manage various security services, including intrusion prevention, endpoint protection, and multi-factor authentication. This consolidation simplifies reporting, threat detection, and overall security posture, making it easier for entities to meet the directive's strict cybersecurity requirements.

NIS 2 Directive Requirements	WatchGuard Solution	How it addresses the requirement
Risk analysis and information system security policies.	WatchGuard's Unified Security Platform®	WatchGuard recommends the implementation of an information security management system or framework like ISO27001 or CIS Critical Security Controls to best manage an entity's cybersecurity posture. We provide products in our Unified Security Platform that help implement controls and address cybersecurity risk areas.
	WatchGuard's ThreatSync (XDR)	ThreatSync utilizes a central platform to uncover, prioritize, and swiftly respond to cyber threats across the WatchGuard network and endpoint security products.

NIS 2 Directive Requirements	WatchGuard Solution	How it addresses the requirement
Risk analysis and information system security policies.	WatchGuard ThreatSync+ NDR	ThreatSync+ NDR helps in risk analysis by providing detailed insights into your network's vulnerabilities and potential threats. You can prioritize security measures by understanding your network's attack surface and identifying high-risk areas. The NDR solution also includes ISO27001 and NIST CSF security policies that support risk analysis. The solution generates comprehensive reports that can be used to inform and strengthen your organization's information system security policies. This data-driven approach ensures that your policies align with current threats and regulatory requirements.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	The Risks dashboard in EPP, EDR, EPDR, and Advanced EPDR shows the security risk level assigned to computers on your network. Software and hardware inventory provides information on unauthorized software and versions installed at the endpoints. Device Control governs the behavior when removable or mass storage devices are connected to the endpoints, authorizing or blocking them. Advanced EPDR allows you to monitor or deny the execution of system applications, such as PowerShell, the Linux shell, and the Windows cmd shell, which are typically used by threats. WatchGuard Cloud's endpoint manager and WatchGuard Endpoint Security plug-ins and integrations for popular RMM applications (ConnectWise, Kaseya, N-able, NinjaOne, etc.) enable partners to manage the security policies of multiple customer accounts.
	WatchGuard Patch Management	Enables setting up vulnerability management policies and performing automated vulnerability scans.
	WatchGuard Full Encryption	Enables setting up data protection policies through full disk encryption
	WatchGuard Advanced Reporting Tool	The Application Control dashboard displays details of applications installed and executed on the network, including legitimate software potentially used maliciously. It helps identify unwanted, unauthorized, unlicensed, or vulnerable applications and those consuming excessive bandwidth or used for scripting, remote access, or system tools. The Vulnerable Applications tab highlights networked applications with known vulnerabilities. The Bandwidth-Consuming Applications tab tracks programs with high data transfer volumes. Monitoring script-based applications like PowerShell, Linux shell, Windows cmd shell, remote access applications, or unwanted free applications is crucial to understand their usage patterns and mitigate potential threats.

NIS 2 Directive Requirements	WatchGuard Solution	How it addresses the requirement
Risk analysis and information system security policies.	WatchGuard MDR	Weekly security health reports provide key information on endpoint risk based on protection status and configuration, detections, and security patches pending installation. As part of onboarding the service, the WatchGuard MDR team assesses the attack surface at the endpoints to strengthen their security posture and immediately improve their overall resiliency to cyber threats.
	WatchGuard Data Control	With WatchGuard Data Control, you can search the content of files, whether or not they contain PII, hosted on your endpoints as part of compromise risk analysis and establish security policies.
Incident handling, including prevention, detection, response, recovery, and reporting.	WatchGuard's Firebox	Fireboxes continually monitor for threats that can be caused by malicious individuals or just employees who mistakenly click on a web link. The security services can detect threats, implement automatic remediation, and send the incident data to ThreatSync to correlate the incident across the WatchGuard platform.
	WatchGuard's ThreatSync (XDR)	ThreatSync provides a consolidated view of all detections across the WatchGuard portfolio into a singular security operations system that allows incident responders to work through the entire incident response cycle in a single pane of glass and automate repetitive remediation activities.
	WatchGuard ThreatSync+ NDR	ThreatSync+ NDR utilizes an advanced AI engine to detect and respond to potential attacks across your network threat surface. The solution helps you manage security incidents from start to finish. If an attack occurs within the network environment, it will quickly be detected and support an immediate and effective response, limiting damage. Finally, it provides detailed reports on what happened, helping you improve your security for the future.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	Integrate innovative technology such as anti-exploit in memory, contextual detections, malicious traffic detection, and managed services – Zero-Trust Application Services and the Threat Hunting Service – to automate prevention, detection, and remediation of threats across all endpoints. The Zero-Trust Application Service is a unique automated managed security service that classifies 100% of running processes on endpoints, ensuring that only safe applications execute. It employs AI/Machine Learning and deep learning to boost the automatic classification of unknown processes. Endpoint Access Enforcement (EAE) denies incoming connections to endpoints from unprotected ones.

NIS 2 Directive Requirements	WatchGuard Solution	How it addresses the requirement
Incident handling, including prevention, detection, response, recovery, and reporting.	WatchGuard Patch Management	Automates operating system and application patch management. It covers the entire patch management cycle, including automatic search for available patches, remediation, and monitoring.
	WatchGuard Full Encryption	Prevents unauthorized users from accessing sensitive data through disk encryption.
	WatchGuard Advanced Reporting Tool	WatchGuard Advanced Reporting Tool provides 365-day telemetry with visibility into what is being executed in the machines, by which users, and through which connections. It enables the identification of unusual and not-in-policy executions and behaviors.
	WatchGuard MDR	A WatchGuard skilled team of cybersecurity experts keeps customers' endpoints safe with 24/7 security monitoring, threat hunting, attack prevention, detection, and containment. WatchGuard MDR automatically delivers periodic service activity and security health status reports that help to prevent and reduce the attack surface at the endpoints and Office 365. In case of a cyberattack, the team notifies WatchGuard partners immediately, including an incident report and guidelines for the containment and remediation process to stop and remediate threats immediately. Contentment can be delegated to the MDR, which automatically isolates impacted endpoints through playbooks.
	WatchGuard Orion	It enables service providers to detect, prioritize, and investigate indicators of attack and compromise by automatically applying security analytics to the 365-day enriched telemetry gathered from monitoring endpoint activity and mapping them to MITRE ATT&CK framework tactics and techniques. Incident case management facilitates collaboration among analysts, responders, and hunters when investigating and correlating suspicious activities related to threats that could surpass other controls. Its containment and remediation tools, such as endpoint isolation, reboot, processes and services management, file transfer, and command-line operations through remote access to endpoints, enable rapid response to and recovery from threats acting at the endpoints. Orion APIs facilitate integration with other systems for streamlined operations.
	WatchGuard Data Control	With WatchGuard Data Control, you can know if compromised endpoints hosted files containing PII or critical business information.

NIS 2 Directive Requirements	WatchGuard Solution	How it addresses the requirement
A business continuity plan that includes backup management, disaster recovery, and crisis management.	WatchGuard Cloud	WatchGuard Cloud facilitates backups of critical security infrastructure configurations, such as Fireboxes and WatchGuard access points. Through integrations with Remote Monitoring and Management tools, endpoint devices can quickly be isolated, remediated, and redeployed if necessary.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	Shadow copies can be created every 24 hours to return a compromised system to its previous state. The Advanced EPDR (R16) forensic and Investigation console allows you to determine the assets being affected for the recovery and notification phases.
	WatchGuard Patch Management	The tight integration of patch management in the same management console enables the correlation of threat detections with endpoint vulnerabilities, allowing for immediate patching to prevent exploitation and mitigate the spread of threats across endpoints.
	WatchGuard MDR	Ensures business continuity management with 24/7 detection and collaboration with our MSPs in responding to security incidents across endpoints and Microsoft 365, leveraging a seasoned cybersecurity team, AI, and advanced technologies from WatchGuard SOC.
	WatchGuard Orion	It enables you to automatically identify suspicious activity, prioritize indicators of attacks, and quickly search for potential threats across your endpoints and servers through 365-day enriched telemetry. The forensic and Investigation console and incident case management allow analysts to investigate the assets being affected, the root cause of the compromise, and the TTPs being used. This critical information helps during recovery, security posture improvement decisions, and notification phases.

NIS 2 Directive Requirements	WatchGuard Solution	How it addresses the requirement
Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.	WatchGuard Cloud	Through WatchGuard Cloud, you can generate executive summary and configuration reports that can be used to document security controls to auditors and other entities in the supply chain when requested.
	WatchGuard ThreatSync+ NDR	Digital supply ecosystems depend on interconnected networks and communications among supply chain partners. ThreatSync+ NDR constantly monitors network communications within and across network boundaries, identifying and reporting risks and vulnerabilities while also watching for potential threats. The solution provides supply chain risk reports that third-party risk assessors can utilize to evaluate the cybersecurity practices of each member.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	WatchGuard Endpoint Security goes beyond traditional antivirus, offering deep detection, anti-exploit, and behavior monitoring to stop hidden threats, even those from third-party suppliers. Its Zero-Trust Application Service and Threat Hunting Service further fortify your defenses against advanced attacks.
	WatchGuard MDR	WatchGuard SOC threat hunters and analysts work around the clock to proactively hunt for, validate, and investigate potential supply chain threats and incidents, correlating abnormal application behaviors and providing guidelines for responding to our partners.
	WatchGuard Orion	It enables service providers to create their own hunting rules, to proactively hunt for, validate, and investigate potential supply chain threats and incidents.

NIS 2 Directive Requirements	WatchGuard Solution	How it addresses the requirement
Security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure.	WatchGuard's Firebox	WatchGuard's Firebox offers multi-layered network protection, simplified updates with WatchGuard Cloud, encrypted management with multi-factor authentication (MFA), secure remote access with MFA and Network Access Enforcement (NAE) via Firebox VPN, and intrusion detection/prevention (IDS/IPS) with traffic segmentation capabilities.
	WatchGuard's ThreatSync (XDR)	WatchGuard's ThreatSync is a Cloud-based service that analyzes data from your WatchGuard network devices and endpoint security products. By combining this information, it detects and prioritizes potential security threats across your entire network, helping you respond to them faster and more effectively.
	WatchGuard ThreatSync+ NDR	ThreatSync+ NDR solution helps with network and information systems security by providing advanced threat detection and response capabilities, including vulnerability detection and response. It uses AI and machine learning to identify and address network-based threats, reducing the risk of breaches and minimizing the impact of incidents. This helps organizations by ensuring the security of their systems and data throughout their life cycle.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	WatchGuard Endpoint Security solutions stop advanced cyberattacks on information systems.
	WatchGuard Patch Management	WatchGuard endpoint products can be used to discover vulnerabilities and EOL software. The Patch Management module reduces cybersecurity risks by providing the entire patch management cycle features. It enables administrators to create on-demand and scheduled tasks to push patches out to managed devices. The patch catalog is updated as new vulnerabilities are discovered and announced.
	WatchGuard MDR	The Managed Detection and Response (MDR) service oversees information systems from a 24x7 security operations center (SOC) operated by cybersecurity experts. Weekly security health reports provide key information on endpoint risk based on protection status and configuration, detections, and security patches pending installation.

NIS 2 Directive Requirements	WatchGuard Solution	How it addresses the requirement
Policies and procedures to assess the effectiveness of cybersecurity risk-management measures.	WatchGuard Cloud	WatchGuard Cloud provides extensive visibility and reporting on discrepancies in the configuration of the cybersecurity products. For example: a policy usage report for the firewall that shows unused policies.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	All WatchGuard Endpoint Security products enable you to establish configurations and policies to reduce the attack surface. The dashboards monitor endpoint security risks, detections, and other critical aspects before and after applying security risk-management measures, enabling the assessment of their effectiveness.
	WatchGuard Patch Management	Patch Management dashboards monitor security vulnerabilities with a patch to be applied, assessing the patch management policies and procedures.
Basic cyber hygiene practices and cybersecurity training.	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	All WatchGuard Endpoints Security solutions include technologies and policies to reduce the attack surface at the endpoints, such as the detection and notification of unmanaged endpoints, protection issues, unconnected endpoints to the Cloud management console, antitampering technologies, and many other mechanisms that make the application of basic cyber hygiene practices easier.
	WatchGuard Patch Management	WatchGuard Patch Management allows for identifying pending security patches to solve vulnerabilities and identifying EOL software installed at the endpoints, facilitating some of the most basic cyber hygiene practices.
	WatchGuard Full Encryption	WatchGuard Full Encryption facilitates the management of at-rest data encryption as a basic measure for data protection.
	WatchGuard Advanced Reporting Tool	WatchGuard Advanced Reporting Tool enables IT hygiene, helping to detect misuse of applications, including nonproductive, highly bandwidth-consuming, and living-of-the-land (LotL) techniques, users involved in the execution and unveiling of connections to non-desired countries. IT Hygiene policies can be implemented to control this.
	WatchGuard MDR	Weekly health reports uncover endpoints at risk and recommend that cyber hygiene practices be implemented.
	DNSWatch	Although WatchGuard does not provide a cybersecurity training suite, the DNSWatch product presents a phishing education video in the browser to end users when it blocks a phishing attempt.

NIS 2 Directive Requirements	WatchGuard Solution	How it addresses the requirement
Policies and procedures regarding using cryptography and, where appropriate, encryption.	WatchGuard's Firebox	WatchGuard's Fireboxes allow administrators flexibility in the way policies are created to allow the most secure deployment with deep visibility into network events. Along with the security policies, the Firebox offers the latest FIPS-level encryption methods for traffic that needs to be encrypted in transit. Fireboxes with IKEv2 VPN support pre-logon, combined with MFA.
	WatchGuard Cloud	All management of products from WatchGuard Cloud is delivered by secure, encrypted communications.
	WatchGuard Full Encryption	WatchGuard Full Encryption prevents unauthorized access and data breaches by providing complete disk encryption for Windows and macOS devices. All recovery keys are securely stored on our Cloud-based platform.
	WatchGuard MDR	WatchGuard SOC analysts monitor encryption library usage to detect any attempts at ransomware cyberattacks as soon as possible.
	WatchGuard Orion	WatchGuard Orion monitors when potential threat actors invoke encryption libraries, maps that activity to corresponding MITRE ATT&CK techniques, and informs security analysts. This allows them to investigate whether the suspicious activity is related to ransomware, or another potential cyberattack.
Human resources security, access control policies, and asset management.	WatchGuard Cloud	WatchGuard Cloud simplifies asset management by offering a centralized console to track and manage all your WatchGuard devices, including firewalls, endpoints, and access points. This provides a clear overview of your network security posture, allowing you to efficiently allocate licenses and respond to threats.
	WatchGuard EPP WatchGuard EDR WatchGuard EPDR WatchGuard Advanced EPDR	For asset management, WatchGuard Endpoint Security solutions include an inventory facility for hardware across managed devices and with details per device: CPU, RAM, storage, TPM, BIOS information, system type, virtual or physical, OS details, private and public IP, and MAC addresses. Software inventory per device includes details like name, publisher, version, etc. Network Access Enforcement (NAE) feature for WatchGuard Fireboxes and Wi-Fi access points, ensures that only protected endpoints can connect to the network. This feature blocks network access from devices not running WatchGuard Endpoint Security Solutions with the appropriate configuration.

NIS 2 Directive Requirements	WatchGuard Solution	How it addresses the requirement
Multi-factor authentication or continuous authentication solutions, secured voice, video, and text communications, and secured emergency communication systems within the entity, where appropriate.	WatchGuard's AuthPoint	WatchGuard AuthPoint provides multi-factor authentication (MFA) for a large ecosystem of 3rd-party applications. Users can authenticate right from their own phone or using an optional hardware token. AuthPoint supports Push notification, QR Code challenge and response, and OTP (one time password) as a second factor. The mobile token is tied to the specific mobile phone used by the user and cannot be copied or cloned to another phone. MFA can be configured for VPN access by simply integrating AuthPoint in WatchGuard Cloud. AuthPoint MFA extends to custom-developed applications through RESTful APIs. It also offers user inheritance to simplify access control for service providers by allowing them to easily revoke resource access upon service provider employee departure.
	WatchGuard's Firebox	WatchGuard's Fireboxes include many options to configure secure encrypted VPN tunnels between sites or remote (mobile) user VPN access to corporate data, all using the latest standards of IKEv2 cryptography.

Table 5. WatchGuard Solutions for NIS 2

Conclusion

While the core of NIS 2 remains consistent across the EU, staying compliant will require agility as member states define their specific implementation. WatchGuard Technologies remains committed to staying abreast of these evolving regulations. We will continue to provide informative resources and ensure our security solutions adapt to the ever-changing NIS 2 landscape, empowering your organization to navigate compliance confidently.

Reference Links

- NIS 2 Directive 2022/2555 (choose your language in HTML or PDF)
- European Commission NIS 2 Policy Page
- European Commission Guidelines – Application of NIS 2 Directive Article 4 (1) and (2)
- European Commission Guidelines – Application of NIS 2 Directive Article 3 (4)
- European Union Agency for Cybersecurity (ENISA) NIS Directive Page
- More information on WatchGuard products

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.