Whitepaper

ThreatDown™
Powered by Malwarebytes

Preparing for NIS 2 Directive

Contents

ThreatDown Powered by Malwarebytes

The Reasons Behind NIS 2

Digital systems are the backbone of virtually every element of current-day society. Critical infrastructure is barely capable of providing their services when their systems are down. This makes them vulnerable to malware and, as a society, we want to keep them secure.

Cybercrime has become highly organized and profitable, and state actors have added cyberattacks to their arsenal of weapons.

What is NIS 2?

NIS 2 is short for Network and Information Security 2. NIS 2 is the European Union's (EU) answer to provide legislation around security measures that organizations and companies that are critical to our society are required to take.

The first version of NIS was approved in 2016 and the second version is expected to take effect in October of 2024. NIS 2 aims to keep critical infrastructure securely functioning with an ultimate goal of creating a higher common level of cybersecurity within the Member States of the EU.

NIS 2 is the European Union's (EU) answer to provide legislation around security measures

To Which Entities Does NIS 2 Apply?

The scope of NIS 2 has broadened when compared to the old version. The primary focus is on organizations that provide essential and important services and employ at least 50 employees or generate an annual revenue greater than €10 million.

The organizations in scope are divided into two main groups: essential entities and important entities.

Essential sector	Important sector
Threshold **≥ 250 employees** **> €50 million turnover** **> €43 million balance**	**Threshold** **50-249 employees** **€10 €50 million turnover** **€10 €43 million balance**
Energy	Postal and courier services
Transport	Waste management
Banking	Chemicals
Financial markets	Food
Health	Manufacturing
Drinking water	Digital providers
Wastewater	Research organizations
Digital infrastructure	
ICT service management	
Public administration	
Space	

As the table shows, essential entities are organizations with at least 250 employees, €50 million annual revenue, and €43 million in assets that provide services which are considered essential. In the important category, you will find smaller organizations primarily in the supply chain for essential entities. Other organizations can be ordered to comply, and all are encouraged to do so.

Any entity that exceeds the ceiling for the important sector but does not qualify as an essential entity is required to comply with this law as an important enterprise.

The cybersecurity requirements for both categories are the same, the difference is purely in supervisory and penalty regimes.

What Do These Entities Need To Do?

NIS 2 based laws will require affected entities to focus on:

- Managing security risks. The organization has appropriate management policies and processes in place to govern its approach to the security of network and information systems.
- Protecting against cyberattacks. The organization defines, implements, communicates, and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support operation of essential functions.
- Detecting cybersecurity events. The organization monitors the security status of the networks and systems supporting the essential functions to detect potential security problems and track the ongoing effectiveness of protective security measures.
- Minimizing the impact of cyber security incidents. There are well-defined and tested incident management processes in place that aim to ensure continuity of essential functions in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.
- Compulsory reporting. With the original NIS directive, organizations were only required to report incidents that had a **significant** impact on their operations. With NIS 2, organizations are required to report all cyber incidents, regardless of impact.

€10M

national authorities to impose maximum fine of at least €10,000,000 or 2% of the global annual revenue to essential entities

Serious Consequences

Besides the already potentially serious consequences of a cyberattack, failing to comply with NIS 2 regulations can have serious repercussions.

National supervisory authorities can impose non-monetary remedies, including compliance orders, binding instructions, security audit implementation orders, and threat notification orders to entities' customers.

Administrative fines are distinguished between essential and important entities within NIS 2. The new regulation requires national authorities to impose maximum fine of at least €10,000,000 or 2% of the global annual revenue to essential entities, whichever is higher. Important entities can be subject to a maximum fine of at least €7,000,000 or 1.4% of the global annual revenue, whichever is higher.

Also, managers can be held personally responsible for failure to comply.

The danger is that organizations will consider NIS 2 as another set of regulations that must be checked for a minimum of costs.

€7M

Important entities can be subject to a maximum fine of at least €7,000,000 or 1.4% of the global annual revenue

How ThreatDown Can Help

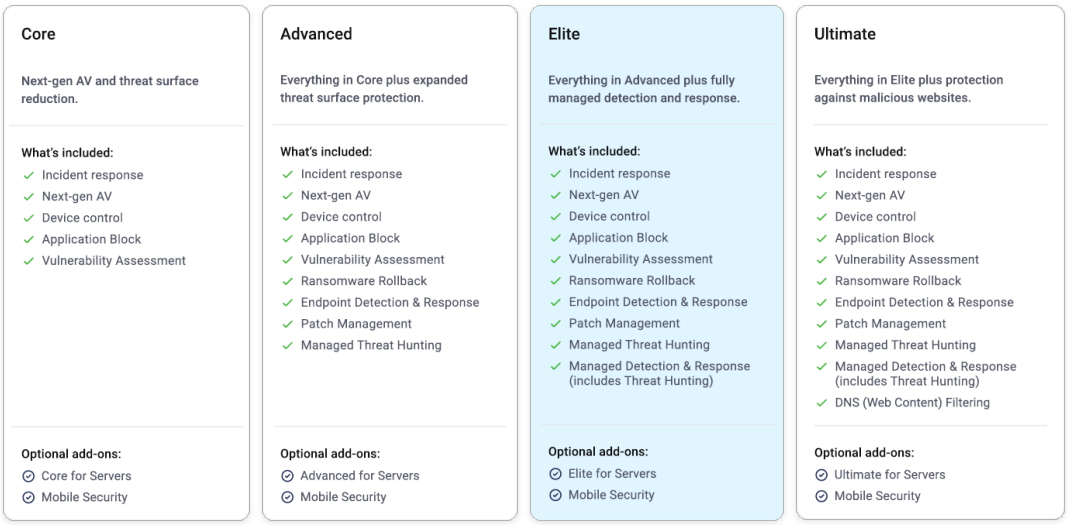
Given the breadth of requirements associated with the NIS 2 directive, it will be difficult for organizations to find a single vendor to provide all the technologies and services needed to obtain and retain compliance. ThreatDown can help with meeting many of the requirements in Article 21, Cybersecurity risk-management measures, as shown below:

Article 21, Cybersecurity Risk-management Measures

NIS 2 Requirement	ThreatDown Solution
2. 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.	ThreatDown Endpoint Detection and Response (EDR) ThreatDown Managed Detection and Response (MDR)
2. a) policies on risk analysis and information system security	ThreatDown Vulnerability Assessment ThreatDown Patch Management
2. b) incident handling	ThreatDown Managed Detection and Response (MDR)
2. c) business continuity, such as backup management and disaster recovery, and crisis management	ThreatDown Endpoint Detection and Response (EDR) ThreatDown Managed Detection and Response (MDR)
2. d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	ThreatDown Managed Detection and Response (MDR)
2. e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	ThreatDown Managed Detection and Response (MDR)
2. f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures	ThreatDown Managed Detection and Response (MDR)
2. i) human resources security, access control policies and asset management	ThreatDown Managed Detection and Response (MDR)

In addition, ThreatDown's MDR service can also provide much of the reporting required as part of Article 23, Reporting Obligations.

ThreatDown's Elite bundle includes all the products and services shown in the table above. This easy to install, simple to manage bundle helps organizations take down threats, complexity and cost.



ThreatDown Powered by Malwarebytes

Conclusion

Even though the compliance deadline isn't until October 17th, 2024, organizations need to prepare for the NIS 2 Directive now. The first step is to assess whether their organization falls under the directive's scope by reviewing the covered sectors and any size requirements. Next, a cybersecurity audit is crucial to identify weaknesses in their current defenses. Based on the audit, organizations should develop a plan to address any vulnerabilities. The plan may involve implementing additional security measures, updating their incident response procedures, and establishing clear protocols for reporting incidents as mandated by NIS 2. Finally, staying informed about specific implementation details from EU member states will be vital for ensuring full compliance.

Organizations need to prepare for NIS 2 Directive now

Talk to an expert