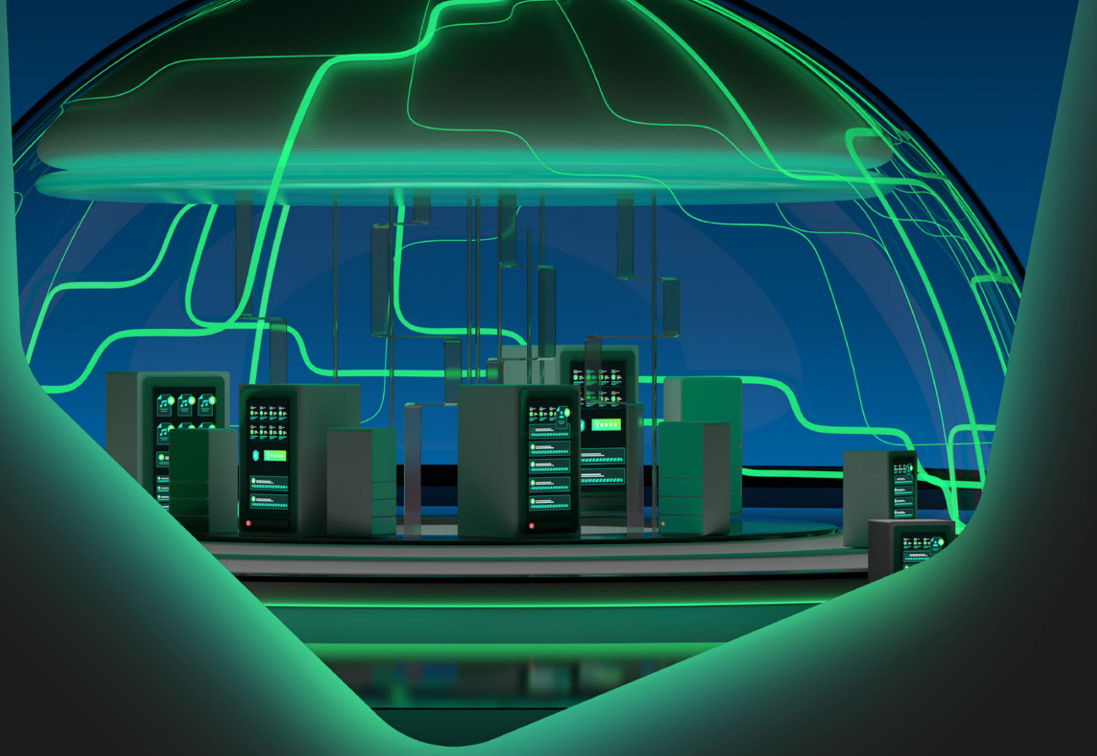
kaspersky

NIS 2 Solution Map



What is the NIS 2 Directive about?

The NIS 2 Directive[1] went into force on January 16th, 2023, and Member States will have to transpose the Directive by October 17, 2024. In addition to other goals, the NIS 2 Directive requires the main operators in key industries to take security measures and report incidents.

Who does NIS 2 apply to?

An entity is covered by the scope of the directive if it operates in one of the sectors and types of services listed in the annexes of the Directive and if it is of a certain size. For all the details, exceptions and nuances, see the Articles 2 & 3 and Annexes I & II of the Directive[2].
NIS 2 Directive establishes two categories for entities within its scope: essential entities and important entities. Both categories must adhere to the same requirements. The differentiation lies in the supervisory measures and penalties.

Sectors that will be regulated

Sectors of high criticality

(Essential entities*)

- Energy
- Drinking water
- Transport
- Digital infrastructure
- Banking
- Waste water
- Financial market infrastructure
- ICT Service management (B2B)
- Health
- Public administration
- Space

Other critical sectors

(Important entities*)

- Postal and courier services
- Production and distribution of food
- Waste management
- Manufacturing
- Manufacture and distribution of chemicals
- Research
- Digital providers

What are the NIS 2 cybersecurity requirements?

According to Article 21 (1) of the Directive 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.

As a cybersecurity vendor, Kaspersky leverages all of its expertise to help organizations build robust cyber defenses and be compliant with NIS 2. We can support you with our leading solutions and services.

[1] 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
[2] https://eur-lex.europa.eu/eli/dir/2022/2555

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 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.	**Kaspersky Security Awareness Portfolio**	**Kaspersky Security Awareness** – a new approach to mastering IT security skills Kaspersky Security Awareness is a proven, efficient solution with a longstanding international track record of success. Used by businesses of every size to train over a million employees across more than 75 countries, the solution brings together more than 25 years of Kaspersky's cybersecurity expertise with extensive experience in adult education. The highly engaging and effective training solutions boost the cybersecurity awareness of your staff so that they all play their part in the overall cybersafety of your organization. Because sustainable changes in behavior take time, our approach involves building a continuous learning cycle with multiple components	https://www.kaspersky.com/enterprise-security/security-awareness
	Kaspersky Expert Training	**Kaspersky xTraining** is a response to a constantly evolving cyber threat landscape. We deliver up-to-date knowledge on effective threat detection and mitigation strategies from comprehensive and well-known experiences of the Kaspersky Global Research & Analysis Team (GReAT)	https://xtraining.kaspersky.com/
	ICS Training	**Kaspersky ICS CERT** is a global project established in 2016 to coordinate the efforts of industrial automation system vendors and industrial facility owners and operators. The team includes more than 30 experts in ICS threat and vulnerability research, incident response and security analysis. We provide training in industrial cybersecurity essentials and practical skills to investigate cybersecurity incidents and perform vulnerability research. Our programs are based on the practical experience and real-life cases.The Kaspersky ICS CERT team delivers trainings for different operators of the ICS secotr, starting from field operators up to C-Level, including Cybersecurity professionals dedicated to the OT.	https://ics-cert.kaspersky.com/media/services/Kaspersky-Industrial-Cybersecurity-training-program-En.pdf
Chapter IV, Art. 21, Cybersecurity risk-management measures			
1. 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.	**Kaspersky Next**	With **Kaspersky Next** is the Kaspersky solution to protect your infrastructure from ransomware, malware, evasive and complex threats. There's EDR functionality in every tier, tailored to your requirements and resources. Our EDR and XDR technologies are built on the foundation of award-winning endpoint protection and enterprise-grade controls. Gain newfound efficiency with automation of simple and complex tasks along with guided response to boost your efficiency and reduce the resources you need to run your cybersecurity. Cloud and on-premise options adapt to your specific requirements, and when the times comes, control your entire infrastructure with fully-fledged open XDR.	
	Kaspersky MDR	**Kaspersky Managed Detection and Response** delivers a fully managed, individually tailored ongoing detection, prioritization, investigation and response. As a result, it allows you to gain all the major benefits from having your own security operations center without having to actually establish one. The main purpose of the MDR service is to detect threats at every stage of a cyberattack, both prior to actual compromise and after malicious actors have penetrated the corporate infrastructure. SOC analysts investigate alerts and notify the customer about the malicious activity, providing tool-based response and advice, Based on a 24x7 security monitoring empowered by automated threat hunting, incident investigation and guided and managed responses	https://www.kaspersky.it/enterprise-security/managed-detection-and-response
	Kaspersky XDR	**Kaspersky XDR** is an open platform, a universal tool for creating a unified ecosystem of cybersecurity products. the platform acts as an ALL-In-One Anti APT solution powered by Kaspersky Threat Intelligence that monitors all potential cybercriminal entry points, correlating information and orchestrating all infrastructure protection components. Kaspersky XDR includes a wide range of out-of-the-box integrations, with Kaspersky and third-party products	https://www.kaspersky.com/enterprise-security/xdr

Kaspersky understands the needs of different industries and company sizes and **protects over 220,000 companies worldwide** against cyber threats. Kaspersky's reliable all-in-one cyber protection covers multiple protection dimensions. **Protect now!**

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 21, Cybersecurity risk-management measures			
1. 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.	**Kaspersky Industrial Cybersecurity**	**Kaspersky Industrial CyberSecurity (KICS)** is a native Extended Detection and Response (XDR) Platform for industrial enterprises, specially designed and certified to protect critical OT equipment, assets, and networks from cyber-initiated threats. The platform comprises integrated technologies that secure core Industrial Automation and Control System components on every level. KICS for Nodes is endpoint protection, detection and response software with compliance audit and endpoint sensor functionality. KICS for Networks is designed for OT network-traffic analysis, detection and response. Site-level centralized management function, essential for scaling OT Security Operations to a high volume of large, diverse and geo distributed industrial infrastructures, is integrated into the platform. Seamless integration across platform components provides full visibility of multiple geographically distributed OT networks and automation systems, delivering an improved customer experience, situational awareness and deployment flexibility. With Extended Detection and Response the KICS Platform enables IT-OT convergence and delivers numerous single-vendor benefits	https://www.kaspersky.it/enterprise-security/industrial-cybersecurity
	Kaspersky Container Security	**Kaspersky Container Security (KCS)** is a security solution that covers every stage of a containerized app's lifecycle, from development to operation. It protects your organization's business processes in line with security standards and regulations, and supports implementation of the DevSecOps approach. Kaspersky Container Security delivers comprehensive protection from the latest cyberthreats, and automates your compliance audits, freeing up the resources of your information security team to focus on other tasks, and shortening time to market. Kaspersky Container Security has been developed specifically for containerized environments, ensuring protection at different levels from container image to host OS.	https://www.kaspersky.com/enterprise-security/container-security
	Kaspersky Threat Intelligence	**Threat Intelligence** from Kaspersky gives you access to the intelligence you need to mitigate cyberthreats, provided by our world-leading team of researchers and analysts. Kaspersky's knowledge, experience and deep intelligence of every aspect of cybersecurity has made us the trusted partner of the world's premier law enforcement and government agencies, including INTERPOL and leading CERTs. Kaspersky Threat Intelligence gives you instant access to tactical, operational and strategic Threat Intelligence. Kaspersky Threat Intelligence empowers you Proactively identify and prevent threats, keeps you informed about the latest threats and vulnerabilities, empowering you to take proactive measures to protect your systems before an attack occurs.	https://www.kaspersky.com/enterprise-security/threat-intelligence
	Kaspersky Web Traffic Security	**Kaspersky Web Traffic Security** (hereinafter also referred to as "the application" or "KWTS") is a solution designed for protecting HTTP-, HTTPS-, and FTP traffic passing through a proxy server. The application protects users of a corporate network when accessing web resources. For example, it deletes malware and other threats from the data stream that enters the corporate network via the HTTP(S) and FTP protocols, blocks infected and phishing websites, and controls access to web resources based on web resource categories and content types.	https://www.kaspersky.it/enterprise-security/internet-gateway

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 21, Cybersecurity risk-management measures			
1. 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.	**Kaspersky Mail Security**	**Kaspersky Security for Mail Server** applications help build resilience to mail-based attacks by: Identifying and filtering out suspicious or unwanted mail at gateway level Most mail attacks only begin to activate at endpoint level – Kaspersky Security for Mail Server sets out to stop them long before they get that far. Our award-winning protection strengthens your resilience by detecting and intercepting attacks right at the beginning of the killchain, before they can breach your perimeter and head for your endpoints and users. Swiftly and accurately processing legitimate emails The core role that email plays in business communications means that security processing has to be fast, agile and accurate – without impeding legitimate communications. Kaspersky Security for Mail Server offers the most effective protection technologies in the industry against everything from phishing emails and spam to Business Email Compromise (BEC) attacks and ransomware, with near-zero false positives, enabling legitimate emails to travel uninterrupted. Protecting email beyond the gateway Kaspersky Security for Mail Server detects malicious or undesirable content not only at the gateway, but also at the level of individual Microsoft Exchange Server mailboxes– or/and Microsoft Exchange Online. Delayed phishing attacks designed to evade gateway level countermeasures, BEC messages generated after account takeovers, and insider threat scenarios that need never pass through the gateway – all these can be identified and eradicated, making server mailbox protection a 'must-have'.	https://www.kaspersky.it/enterprise-security/mail-server-security
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: a) policies on risk analysis and information system security;	**Kaspersky Incident Response**	**Incident response** — obtains a detailed picture of the incident. The service covers the full incident investigation and response cycle:from early incident response and evidence collection to identifying additional traces of hacking and preparing an attack mitigation plan.	https://www.kaspersky.it/enterprise-security/incident-response
	Kaspersky Next	With **Kaspersky Next** is the Kaspersky solution to protect your infrastructure from ransomware, malware, evasive and complex threats. There's EDR functionality in every tier, tailored to your requirements and resources. Our EDR and XDR technologies are built on the foundation of award-winning endpoint protection and enterprise-grade controls. Gain newfound efficiency with automation of simple and complex tasks along with guided response to boost your efficiency and reduce the resources you need to run your cybersecurity. Cloud and on-premise options adapt to your specific requirements, and when the times comes, control your entire infrastructure with fully-fledged open XDR.	
	Kaspersky Industrial Cybersecurity	**Kaspersky Industrial CyberSecurity (KICS)** is a native Extended Detection and Response (XDR) Platform for industrial enterprises, specially designed and certified to protect critical OT equipment, assets, and networks from cyber-initiated threats. The platform comprises integrated technologies that secure core Industrial Automation and Control System components on every level. KICS for Nodes is endpoint protection, detection and response software with compliance audit and endpoint sensor functionality. KICS for Networks is designed for OT network-traffic analysis, detection and response. Site-level centralized management function, essential for scaling OT Security Operations to a high volume of large, diverse and geo distributed industrial infrastructures, is integrated into the platform. Seamless integration across platform components provides full visibility of multiple geographically distributed OT networks and automation systems, delivering an improved customer experience, situational awareness and deployment flexibility. With Extended Detection and Response the KICS Platform enables IT-OT convergence and delivers numerous single-vendor benefits	https://www.kaspersky.it/enterprise-security/industrial-cybersecurity
	Kaspersky Vulnerability Assessment	This service provides information on existing vulnerabilities, the consequences of their exploitation, evaluates the effectiveness of implemented security measures and allows you to plan further actions to correct detected defects and improve security. Performing security assessments regularly allows you to clearly understand the status of your cybersecurity and ensures compliance with industry best practices.	https://www.kaspersky.it/enterprise-security/cybersecurity-services

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 21, Cybersecurity risk-management measures			
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: a) policies on risk analysis and information system security;	**Kaspersky Digital Footprint Intelligence**	**Kaspersky Digital Footprint Intelligence** is a comprehensive digital risk protection service that helps customers monitor their digital assets and detect threats from the Surface, Deep and Dark Web. With real-time alerts, Kaspersky Digital Footprint Intelligence enables organizations to respond quickly and effectively to potential threats. Analytical reports integrate this data with comprehensive intelligence from our experts that provides insights into cybersecurity risks and recommendations on how to mitigate them.	https://dfi.kaspersky.com/
	Kaspersky APT, Crimeware, ICS Reporting	With **Intelligence Reporting**, Kaspersky customers will benefit from constant and exclusive access to analytics and insights, including comprehensive technical data (in a wide range of formats) on APT actors targeting your industry and geography , learn about and appropriately counter crimeware and cyber threats affecting industrial organizations (including threats that will never be made public). The reports contain a summary of immediate and relevant information that illustrates every detail of the attack as well as offering a detailed technical description with the relevant YARA and IOC rules, offering security researchers, malware analysts, security engineers, security analysts network and APT researchers, applicable data that enables an accurate and fast response to threats.	https://www.kaspersky.it/enterprise-security/threat-intelligence
	Kaspersky Vulnerability Threat Data Feeds	By integrating up-to-date **Threat Intelligence feeds** containing IP, URL and hash information of suspicious and malicious files into existing security systems, such as SIEM systems, SOAR and Threat Intelligence platforms, security teams can automate the initial triage process and provide relevant specialists with the context needed to immediately identify alerts that require in-depth analysis, or that need to be escalated to incident response teams for further investigation and response. Data feeds are aggregated from highly reliable and heterogeneous sources, such as Kaspersky Security Network and our Web Crawlers, Botnet Monitoring Service (24/7/365 monitoring of botnets and their activities and objectives), spam traps, partners and research teams.	https://www.kaspersky.it/enterprise-security/threat-intelligence
	KUMA	**Kaspersky Unified Monitoring and Analysis Platform (KUMA)** is an advanced SIEM solution for managing security data and events. KUMA analyzes information security events in real time significantly increases situational awareness. KUMA receives security events from various sources, including Kaspersky products, operating systems, third-party applications, and security tools. It correlates these events with each other and with threat intelligence feeds to identify suspicious activity in corporate network infrastructure and provides timely notification of security incidents. By collecting logs from all security controls and correlating the resulting data in real time, KUMA aggregates all the information needed for further incident investigation and response.	https://support.kaspersky.com/help/KUMA/1.6/en-US/217694.htm
	Kaspersky Container Security	**Kaspersky Container Security (KCS)** is a security solution that covers every stage of a containerized app's lifecycle, from development to operation. It protects your organization's business processes in line with security standards and regulations, and supports implementation of the DevSecOps approach. Kaspersky Container Security delivers comprehensive protection from the latest cyberthreats, and automates your compliance audits, freeing up the resources of your information security team to focus on other tasks, and shortening time to market. Kaspersky Container Security has been developed specifically for containerized environments, ensuring protection at different levels from container image to host OS.	https://www.kaspersky.com/enterprise-security/container-security

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 21, Cybersecurity risk-management measures			
2. b) incident handling;	**Kaspersky Incident Response**	**Incident response** — obtains a detailed picture of the incident. The service covers the full incident investigation and response cycle:from early incident response and evidence collection to identifying additional traces of hacking and preparing an attack mitigation plan.	https://www.kaspersky.it/enterprise-security/incident-response
	EDR Optimum	Limited visibility and lack of resources work in the attackers' favor. **Kaspersky Endpoint Detection and Response (EDR) Optimum** offers advanced detection, simplified investigation capabilities and automated response in an easy-to-use package to protect your business from the latest threats.	https://www.kaspersky.it/enterprise-security/edr-security-software-solution
	EDR Expert	Cyberattacks are becoming increasingly sophisticated and capable of evading existing security measures. **Kaspersky Endpoint Detection and Response (EDR) Expert** provides complete visibility into all endpoints of the corporate network and offers superior defenses by automating routine EDR tasks and enabling analysts to quickly detect, prioritize, analyze and neutralize complex threats and APT type attacks. Kaspersky EDR Expert uses a single agent that can be managed from both a single cloud-based management platform and an offline console in air-gap environments, leveraging threat intelligence technologies and integrating customizable detection strategies.	https://www.kaspersky.it/enterprise-security/endpoint-detection-response-edr
	Kaspersky XDR	**Kaspersky XDR** is an open platform, a universal tool for creating a unified ecosystem of cybersecurity products. the platform acts as an ALL-In-One Anti APT solution powered by Kaspersky Threat Intelligence that monitors all potential cybercriminal entry points, correlating information and orchestrating all infrastructure protection components. Kaspersky XDR includes a wide range of out-of-the-box integrations, with Kaspersky and third-party products	https://www.kaspersky.it/enterprise-security/xdr
	Kaspersky MDR	**Kaspersky Managed Detection and Response** delivers a fully managed, individually tailored ongoing detection, prioritization, investigation and response. As a result, it allows you to gain all the major benefits from having your own security operations center without having to actually establish one. The main purpose of the MDR service is to detect threats at every stage of a cyberattack, both prior to actual compromise and after malicious actors have penetrated the corporate infrastructure. SOC analysts investigate alerts and notify the customer about the malicious activity, providing tool-based response and advice, Based on a 24x7 security monitoring empowered by automated threat hunting, incident investigation and guided and managed responses	https://www.kaspersky.it/enterprise-security/managed-detection-and-response
	Kaspersky Threat Lookup	**Kaspersky Threat Lookup** provides all of Kaspersky's knowledge about cyber threats and the relationships between them, brought together in a single, powerful web service. The goal is to provide security teams with as much data as possible, to prevent attacks computer scientists before they compromise the organization. The platform retrieves the latest threat intelligence insights into URLs, domains, IP addresses, file hashes, threat names, statistical/behavioral data, WHOIS/DNS data, file attributes, geolocation data, chains download, timestamp. The result is global threat visibility new and emerging: this allows you to better protect your company, significantly improving the quality and efficiency of incident response activities.	https://www.kaspersky.it/enterprise-security/threat-intelligence
	Kaspersky Threat Analysis	When faced with a potential cyber threat, making a timely decision becomes essential. In addition to threat analysis technologies such as sandboxing, **Kaspersky Threat Analysis** provides cutting-edge attribution technologies (a multi-layered approach that provides efficient analysis of threats, so you can make fully informed decisions to defend against attacks even before they are launched). Multiple threat analysis tools combine to allow you and your team to analyze the situation from all angles with a complete picture of the threat landscape and respond quickly and effectively.	https://www.kaspersky.it/enterprise-security/threat-intelligence

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 21, Cybersecurity risk-management measures			
2. b) incident handling;	**Kaspersky Threat Data Feeds**	By integrating into existing security systems, such as SIEM, SOAR, and Threat Intelligence platforms, up-to-date **Threat Intelligence feeds** containing information on IPs, URLs, and hashes of suspicious and malicious files, security teams can automate the initial triage process and provide relevant specialists with the context they need to immediately identify alerts that require in-depth analysis, or that should be forwarded to incident response teams for further investigation and response. Data feeds are aggregated from highly reliable and heterogeneous sources, such as Kaspersky Security Network and our Web Crawlers, botnet monitoring service (24/7/365 monitoring of botnets and their activities and targets), spam traps, partners, and research teams.	https://www.kaspersky.it/enterprise-security/threat-intelligence
	KUMA	**Kaspersky Unified Monitoring and Analysis Platform (KUMA)** is an advanced SIEM solution for managing security data and events. KUMA analyzes information security events in real time significantly increases situational awareness. KUMA receives security events from various sources, including Kaspersky products, operating systems, third-party applications, and security tools. It correlates these events with each other and with threat intelligence feeds to identify suspicious activity in corporate network infrastructure and provides timely notification of security incidents. By collecting logs from all security controls and correlating the resulting data in real time, KUMA aggregates all the information needed for further incident investigation and response.	https://support.kaspersky.com/help/KUMA/1.6/en-US/217694.htm
	Kaspersky Container Security	**Kaspersky Container Security (KCS)** is a security solution that covers every stage of a containerized app's lifecycle, from development to operation. It protects your organization's business processes in line with security standards and regulations, and supports implementation of the DevSecOps approach. Kaspersky Container Security delivers comprehensive protection from the latest cyberthreats, and automates your compliance audits, freeing up the resources of your information security team to focus on other tasks, and shortening time to market. Kaspersky Container Security has been developed specifically for containerized environments, ensuring protection at different levels from container image to host OS."	https://www.kaspersky.com/enterprise-security/container-security
2. c) business continuity, such as backup management and disaster recovery, and crisis management;	**Kaspersky Next**	With **Kaspersky Next** is the Kaspersky solution to protect your infrastructure from ransomware, malware, evasive and complex threats. There's EDR functionality in every tier, tailored to your requirements and resources. Our EDR and XDR technologies are built on the foundation of award-winning endpoint protection and enterprise-grade controls. Gain newfound efficiency with automation of simple and complex tasks along with guided response to boost your efficiency and reduce the resources you need to run your cybersecurity. Cloud and on-premise options adapt to your specific requirements, and when the times comes, control your entire infrastructure with fully-fledged open XDR.	
	Kaspersky MDR	**Kaspersky Managed Detection and Response** delivers a fully managed, individually tailored ongoing detection, prioritization, investigation and response. As a result, it allows you to gain all the major benefits from having your own security operations center without having to actually establish one. The main purpose of the MDR service is to detect threats at every stage of a cyberattack, both prior to actual compromise and after malicious actors have penetrated the corporate infrastructure. SOC analysts investigate alerts and notify the customer about the malicious activity, providing tool-based response and advice, Based on a 24x7 security monitoring empowered by automated threat hunting, incident investigation and guided and managed responses	https://www.kaspersky.it/enterprise-security/managed-detection-and-response

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 21, Cybersecurity risk-management measures			
2. c) business continuity, such as backup management and disaster recovery, and crisis management;	**Kaspersky Incident Response**	**Incident response** — obtains a detailed picture of the incident. The service covers the full incident investigation and response cycle:from early incident response and evidence collection to identifying additional traces of hacking and preparing an attack mitigation plan.	https://www.kaspersky.it/enterprise-security/incident-response
	Kaspersky Incident Communication	From the instant a cyber-incident is discovered, every action counts. How your communications are managed – externally and internally – is critical, particularly when dealing with unknown attack vectors and advanced persistent threats (APTs). Any enterprise can fall victim to a cyberattack, which is why there needs to be a crisis team – ideally made up of specialists from the information security department, the operations division, and corporate communications – ready to minimize the damage. This can be done through authoritative, appropriate, accurate and imely actions. Kaspersky has developed best-of-breed training that empowers top management, information security and corporate communications professionals to handle crisis communications, including developing and applying appropriate assets, while under attack from an unknown cyber-incident or advanced persistent threat (APT).	https://www.kaspersky.com/enterprise-security/cyber-incident-response-communication
2. d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;	**SD-Wan**	**Kaspersky SD-WAN** is designed to build fault-tolerant and secure networks with unified management – essential for today's distributed businesses. The solution allows you to use diverse communication channels, optimize cloud connections, enhance the security and improve the performance of applications, and speed up implementation of new services.	https://www.kaspersky.com/enterprise-security/sd-wan
	Kaspersky Threat Intelligence	**Threat Intelligence** from Kaspersky gives you access to the intelligence you need to mitigate cyberthreats, provided by our world-leading team of researchers and analysts. Kaspersky's knowledge, experience and deep intelligence of every aspect of cybersecurity has made us the trusted partner of the world's premier law enforcement and government agencies, including INTERPOL and leading CERTs. Kaspersky Threat Intelligence gives you instant access to tactical, operational and strategic Threat Intelligence. Kaspersky Threat Intelligence empowers you Proactively identify and prevent threats, keeps you informed about the latest threats and vulnerabilities, empowering you to take proactive measures to protect your systems before an attack occurs.	https://www.kaspersky.it/enterprise-security/threat-intelligence
	Kaspersky MDR	**Kaspersky Managed Detection and Response** delivers a fully managed, individually tailored ongoing detection, prioritization, investigation and response. As a result, it allows you to gain all the major benefits from having your own security operations center without having to actually establish one. The main purpose of the MDR service is to detect threats at every stage of a cyberattack, both prior to actual compromise and after malicious actors have penetrated the corporate infrastructure. SOC analysts investigate alerts and notify the customer about the malicious activity, providing tool-based response and advice, Based on a 24x7 security monitoring empowered by automated threat hunting, incident investigation and guided and managed responses	https://www.kaspersky.it/enterprise-security/managed-detection-and-response
	Scan Engine	**Kaspersky Scan Engine (KSEn)** provides comprehensive protection for web portals and applications, proxy servers, network attached storage and mail gateways. It is easy to manage and deploy through HTTP and ICAP as a standalone service, scalable cluster, or Docker container. KSE uses the latest detection methods for detection and removal of malware including Trojans, phishing threats, worms, rootkits, spyware and adware.	https://www.kaspersky.com/scan-engine

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 21, Cybersecurity risk-management measures			
2. e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	**Kaspersky Vulnerability Assessment**	This service provides information on existing vulnerabilities, the consequences of their exploitation, evaluates the effectiveness of implemented security measures and allows you to plan further actions to correct detected defects and improve security. Performing security assessments regularly allows you to clearly understand the status of your cybersecurity and ensures compliance with industry best practices.	https://www.kaspersky.com/enterprise-security/cybersecurity-services
	Kaspersky Vulnerability Threat Data Feeds	By integrating up-to-date **Threat Intelligence feeds** containing IP, URL and hash information of suspicious and malicious files into existing security systems, such as SIEM systems, SOAR and Threat Intelligence platforms, security teams can automate the initial triage process and provide relevant specialists with the context needed to immediately identify alerts that require in-depth analysis, or that need to be escalated to incident response teams for further investigation and response. Data feeds are aggregated from highly reliable and heterogeneous sources, such as Kaspersky Security Network and our Web Crawlers, Botnet Monitoring Service (24/7/365 monitoring of botnets and their activities and objectives), spam traps, partners and research teams.	https://www.kaspersky.it/enterprise-security/threat-intelligence
	Kaspersky Next	With **Kaspersky Next** is the Kaspersky solution to protect your infrastructure from ransomware, malware, evasive and complex threats. There's EDR functionality in every tier, tailored to your requirements and resources. Our EDR and XDR technologies are built on the foundation of award-winning endpoint protection and enterprise-grade controls. Gain newfound efficiency with automation of simple and complex tasks along with guided response to boost your efficiency and reduce the resources you need to run your cybersecurity. Cloud and on-premise options adapt to your specific requirements, and when the times comes, control your entire infrastructure with fully-fledged open XDR.	
	Kaspersky Industrial Cybersecurity	**Kaspersky Industrial CyberSecurity (KICS)** is a native Extended Detection and Response (XDR) Platform for industrial enterprises, specially designed and certified to protect critical OT equipment, assets, and networks from cyber-initiated threats. The platform comprises integrated technologies that secure core Industrial Automation and Control System components on every level. KICS for Nodes is endpoint protection, detection and response software with compliance audit and endpoint sensor functionality. KICS for Networks is designed for OT network-traffic analysis, detection and response. Site-level centralized management function, essential for scaling OT Security Operations to a high volume of large, diverse and geo distributed industrial infrastructures, is integrated into the platform. Seamless integration across platform components provides full visibility of multiple geographically distributed OT networks and automation systems, delivering an improved customer experience, situational awareness and deployment flexibility. With Extended Detection and Response the KICS Platform enables IT-OT convergence and delivers numerous single-vendor benefits	https://www.kaspersky.it/enterprise-security/industrial-cybersecurity
	Kaspersky Digital Footprint Intelligence	**Kaspersky Digital Footprint Intelligence** is a comprehensive digital risk protection service that helps customers monitor their digital assets and detect threats from the Surface, Deep and Dark Web. With real-time alerts, Kaspersky Digital Footprint Intelligence enables organizations to respond quickly and effectively to potential threats. Analytical reports integrate this data with comprehensive intelligence from our experts that provides insights into cybersecurity risks and recommendations on how to mitigate them.	https://dfi.kaspersky.com/

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 21, Cybersecurity risk-management measures			
2. e) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;	**Kaspersky MDR**	**Kaspersky Managed Detection and Response** delivers a fully managed, individually tailored ongoing detection, prioritization, investigation and response. As a result, it allows you to gain all the major benefits from having your own security operations center without having to actually establish one. The main purpose of the MDR service is to detect threats at every stage of a cyberattack, both prior to actual compromise and after malicious actors have penetrated the corporate infrastructure. SOC analysts investigate alerts and notify the customer about the malicious activity, providing tool-based response and advice, Based on a 24x7 security monitoring empowered by automated threat hunting, incident investigation and guided and managed responses	https://www.kaspersky.it/enterprise-security/managed-detection-and-response
2. f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	**Kaspersky Digital Footprint Intelligence**	**Kaspersky Digital Footprint Intelligence** is a comprehensive digital risk protection service that helps customers monitor their digital assets and detect threats from the Surface, Deep and Dark Web. With real-time alerts, Kaspersky Digital Footprint Intelligence enables organizations to respond quickly and effectively to potential threats. Analytical reports integrate this data with comprehensive intelligence from our experts that provides insights into cybersecurity risks and recommendations on how to mitigate them.	https://dfi.kaspersky.com/
	Kaspersky Vulnerability Assessment	This service provides information on existing vulnerabilities, the consequences of their exploitation, evaluates the effectiveness of implemented security measures and allows you to plan further actions to correct detected defects and improve security. Performing security assessments regularly allows you to clearly understand the status of your cybersecurity and ensures compliance with industry best practices.	https://www.kaspersky.com/enterprise-security/cybersecurity-services
	Kaspersky Next	With **Kaspersky Next** is the Kaspersky solution to protect your infrastructure from ransomware, malware, evasive and complex threats. There's EDR functionality in every tier, tailored to your requirements and resources. Our EDR and XDR technologies are built on the foundation of award-winning endpoint protection and enterprise-grade controls. Gain newfound efficiency with automation of simple and complex tasks along with guided response to boost your efficiency and reduce the resources you need to run your cybersecurity. Cloud and on-premise options adapt to your specific requirements, and when the times comes, control your entire infrastructure with fully-fledged open XDR.	
	Kaspersky Vulnerability Threat Data Feeds	By integrating up-to-date Threat Intelligence feeds containing IP, URL and hash information of suspicious and malicious files into existing security systems, such as SIEM systems, SOAR and Threat Intelligence platforms, security teams can automate the initial triage process and provide relevant specialists with the context needed to immediately identify alerts that require in-depth analysis, or that need to be escalated to incident response teams for further investigation and response. Data feeds are aggregated from highly reliable and heterogeneous sources, such as Kaspersky Security Network and our Web Crawlers, Botnet Monitoring Service (24/7/365 monitoring of botnets and their activities and objectives), spam traps, partners and research teams.	https://www.kaspersky.it/enterprise-security/threat-intelligence

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 21, Cybersecurity risk-management measures			
2. f) policies and procedures to assess the effectiveness of cybersecurity risk-management measures;	**Kaspersky Industrial Cybersecurity**	**Kaspersky Industrial CyberSecurity (KICS)** is a native Extended Detection and Response (XDR) Platform for industrial enterprises, specially designed and certified to protect critical OT equipment, assets, and networks from cyber-initiated threats. The platform comprises integrated technologies that secure core Industrial Automation and Control System components on every level. KICS for Nodes is endpoint protection, detection and response software with compliance audit and endpoint sensor functionality. KICS for Networks is designed for OT network-traffic analysis, detection and response. Site-level centralized management function, essential for scaling OT Security Operations to a high volume of large, diverse and geo distributed industrial infrastructures, is integrated into the platform. Seamless integration across platform components provides full visibility of multiple geographically distributed OT networks and automation systems, delivering an improved customer experience, situational awareness and deployment flexibility. With Extended Detection and Response the KICS Platform enables IT-OT convergence and delivers numerous single-vendor benefits	https://www.kaspersky.it/enterprise-security/industrial-cybersecurity
	Kaspersky MDR	**Kaspersky Managed Detection and Response** delivers a fully managed, individually tailored ongoing detection, prioritization, investigation and response. As a result, it allows you to gain all the major benefits from having your own security operations center without having to actually establish one. The main purpose of the MDR service is to detect threats at every stage of a cyberattack, both prior to actual compromise and after malicious actors have penetrated the corporate infrastructure. SOC analysts investigate alerts and notify the customer about the malicious activity, providing tool-based response and advice, Based on a 24x7 security monitoring empowered by automated threat hunting, incident investigation and guided and managed responses	https://www.kaspersky.it/enterprise-security/managed-detection-and-response
2. g) basic cyber hygiene practices and cybersecurity training;	**Kaspersky Security Awareness Portfolio**	**Kaspersky Security Awareness** – a new approach to mastering IT security skills Kaspersky Security Awareness is a proven, efficient solution with a longstanding international track record of success. Used by businesses of every size to train over a million employees across more than 75 countries, the solution brings together more than 25 years of Kaspersky's cybersecurity expertise with extensive experience in adult education. The highly engaging and effective training solutions boost the cybersecurity awareness of your staff so that they all play their part in the overall cybersafety of your organization. Because sustainable changes in behavior take time, our approach involves building a continuous learning cycle with multiple components	https://www.kaspersky.com/enterprise-security/security-awareness
	Kaspersky Expert Training	**Kaspersky xTraining** is a rsponse to a constantly evolving cyber threat landscape. We deliver up-to-date knowledge on effective threat detection and mitigation strategies from comprehensive and well-known experiences of the Kaspersky Global Research & Analysis Team (GReAT)	https://xtraining.kaspersky.com/
	ICS Training	**Kaspersky ICS CERT** is a global project established in 2016 to coordinate the efforts of industrial automation system vendors and industrial facility owners and operators. The team includes more than 30 experts in ICS threat and vulnerability research, incident response and security analysis. We provide training in industrial cybersecurity essentials and practical skills to investigate cybersecurity incidents and perform vulnerability research. Our programs are based on the practical experience and real-life cases.The Kaspersky ICS CERT team delivers trainings for different operators of the ICS secotr, starting from field operators up to C-Level, including Cybersecurity professionals dedicated to the OT.	https://ics-cert.kaspersky.com/media/services/Kaspersky-Industrial-Cybersecurity-training-program-En.pdf

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 21, Cybersecurity risk-management measures			
2. h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;	**Kaspersky Next**	With **Kaspersky Next** is the Kaspersky solution to protect your infrastructure from ransomware, malware, evasive and complex threats. There's EDR functionality in every tier, tailored to your requirements and resources. Our EDR and XDR technologies are built on the foundation of award-winning endpoint protection and enterprise-grade controls. Gain newfound efficiency with automation of simple and complex tasks along with guided response to boost your efficiency and reduce the resources you need to run your cybersecurity. Cloud and on-premise options adapt to your specific requirements, and when the times comes, control your entire infrastructure with fully-fledged open XDR.	
2. i) shuman resources security, access control policies and asset management;	**Kaspersky MDR**	**Kaspersky Managed Detection and Response** delivers a fully managed, individually tailored ongoing detection, prioritization, investigation and response. As a result, it allows you to gain all the major benefits from having your own security operations center without having to actually establish one. The main purpose of the MDR service is to detect threats at every stage of a cyberattack, both prior to actual compromise and after malicious actors have penetrated the corporate infrastructure. SOC analysts investigate alerts and notify the customer about the malicious activity, providing tool-based response and advice, Based on a 24x7 security monitoring empowered by automated threat hunting, incident investigation and guided and managed responses	https://www.kaspersky.it/enterprise-security/managed-detection-and-response
	Kaspersky Digital Footprint Intelligence	**Kaspersky Digital Footprint Intelligence** is a comprehensive digital risk protection service that helps customers monitor their digital assets and detect threats from the Surface, Deep and Dark Web. With real-time alerts, Kaspersky Digital Footprint Intelligence enables organizations to respond quickly and effectively to potential threats. Analytical reports integrate this data with comprehensive intelligence from our experts that provides insights into cybersecurity risks and recommendations on how to mitigate them.	https://dfi.kaspersky.com/
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.	**Kaspersky Next**	**Kaspersky Next** solution management platforms include dual-factor authentication configuration as a tool for secure access control.	
	Kaspersky Threat Intelligence	The **Threat Intelligence** portal provides access to the web platform and access via Open API	https://www.kaspersky.it/enterprise-security/threat-intelligence

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 23, Reporting requirements			
4. d) 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; (ii) the type of threat or root cause that is likely to have triggered the incident;	**Kaspersky Incident Response**	**Incident response** — obtains a detailed picture of the incident. The service covers the full incident investigation and response cycle:from early incident response and evidence collection to identifying additional traces of hacking and preparing an attack mitigation plan.	https://www.kaspersky.it/enterprise-security/incident-response
	Kaspersky APT, Crimeware, ICS Reporting	With Intelligence Reporting, Kaspersky customers will benefit from constant and exclusive access to analytics and insights, including comprehensive technical data (in a wide range of formats) on APT actors targeting your industry and geography , learn about and appropriately counter crimeware and cyber threats affecting industrial organizations (including threats that will never be made public). The reports contain a summary of immediate and relevant information that illustrates every detail of the attack as well as offering a detailed technical description with the relevant YARA and IOC rules, offering security researchers, malware analysts, security engineers, security analysts network and APT researchers, applicable data that enables an accurate and fast response to threats.	https://www.kaspersky.it/enterprise-security/threat-intelligence
	Kaspersky Threat Lookup	**Kaspersky Threat Lookup** provides all of Kaspersky's knowledge about cyber threats and the relationships between them, brought together in a single, powerful web service. The goal is to provide security teams with as much data as possible, to prevent attacks computer scientists before they compromise the organization. The platform retrieves the latest threat intelligence insights into URLs, domains, IP addresses, file hashes, threat names, statistical/behavioral data, WHOIS/DNS data, file attributes, geolocation data, chains download, timestamp. The result is global threat visibility new and emerging: this allows you to better protect your company, significantly improving the quality and efficiency of incident response activities.	https://www.kaspersky.it/enterprise-security/threat-intelligence
	Kaspersky Threat Analysis	When faced with a potential cyber threat, making a timely decision becomes essential. In addition to threat analysis technologies such as sandboxing, **Kaspersky Threat Analysis** provides cutting-edge attribution technologies (a multi-layered approach that provides efficient analysis of threats, so you can make fully informed decisions to defend against attacks even before they are launched). Multiple threat analysis tools combine to allow you and your team to analyze the situation from all angles with a complete picture of the threat landscape and respond quickly and effectively.	https://www.kaspersky.it/enterprise-security/threat-intelligence
	Kaspersky MDR	**Kaspersky Managed Detection and Response** delivers a fully managed, individually tailored ongoing detection, prioritization, investigation and response. As a result, it allows you to gain all the major benefits from having your own security operations center without having to actually establish one. The main purpose of the MDR service is to detect threats at every stage of a cyberattack, both prior to actual compromise and after malicious actors have penetrated the corporate infrastructure. SOC analysts investigate alerts and notify the customer about the malicious activity, providing tool-based response and advice, Based on a 24x7 security monitoring empowered by automated threat hunting, incident investigation and guided and managed responses	https://www.kaspersky.it/enterprise-security/managed-detection-and-response

NIS2 Requirement	Kaspersky Solution	Advantages	Information
Chapter IV, Art. 23, Reporting requirements			
4. d) 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; (ii) the type of threat or root cause that is likely to have triggered the incident;	**EDR Optimum**	Limited visibility and lack of resources work in the attackers' favor. **Kaspersky Endpoint Detection and Response (EDR) Optimum** offers advanced detection, simplified investigation capabilities and automated response in an easy-to-use package to protect your business from the latest threats.	https://www.kaspersky.it/enterprise-security/edr-security-software-solution
	EDR Expert	Cyberattacks are becoming increasingly sophisticated and capable of evading existing security measures. **Kaspersky Endpoint Detection and Response (EDR) Expert** provides complete visibility into all endpoints of the corporate network and offers superior defenses by automating routine EDR tasks and enabling analysts to quickly detect, prioritize, analyze and neutralize complex threats and APT type attacks. Kaspersky EDR Expert uses a single agent that can be managed from both a single cloud-based management platform and an offline console in air-gap environments, leveraging threat intelligence technologies and integrating customizable detection strategies.	https://www.kaspersky.it/enterprise-security/endpoint-detection-response-edr
	Kaspersky XDR	**Kaspersky XDR** is an open platform, a universal tool for creating a unified ecosystem of cybersecurity products. the platform acts as an ALL-In-One Anti APT solution powered by Kaspersky Threat Intelligence that monitors all potential cybercriminal entry points, correlating information and orchestrating all infrastructure protection components. Kaspersky XDR includes a wide range of out-of-the-box integrations, with Kaspersky and third-party products	https://www.kaspersky.it/enterprise-security/xdr
	Kaspersky Industrial Cybersecurity	**Kaspersky Industrial CyberSecurity (KICS)** is a native Extended Detection and Response (XDR) Platform for industrial enterprises, specially designed and certified to protect critical OT equipment, assets, and networks from cyber-initiated threats. The platform comprises integrated technologies that secure core Industrial Automation and Control System components on every level. KICS for Nodes is endpoint protection, detection and response software with compliance audit and endpoint sensor functionality. KICS for Networks is designed for OT network-traffic analysis, detection and response. Site-level centralized management function, essential for scaling OT Security Operations to a high volume of large, diverse and geo distributed industrial infrastructures, is integrated into the platform. Seamless integration across platform components provides full visibility of multiple geographically distributed OT networks and automation systems, delivering an improved customer experience, situational awareness and deployment flexibility. With Extended Detection and Response the KICS Platform enables IT-OT convergence and delivers numerous single-vendor benefits	https://www.kaspersky.it/enterprise-security/industrial-cybersecurity
	Kaspersky Container Security	**Kaspersky Container Security (KCS)** is a security solution that covers every stage of a containerized app's lifecycle, from development to operation. It protects your organization's business processes in line with security standards and regulations, and supports implementation of the DevSecOps approach. Kaspersky Container Security delivers comprehensive protection from the latest cyberthreats, and automates your compliance audits, freeing up the resources of your information security team to focus on other tasks, and shortening time to market. Kaspersky Container Security has been developed specifically for containerized environments, ensuring protection at different levels from container image to host OS.	https://www.kaspersky.com/enterprise-security/container-security

Cyberthreat News: securelist.com/
Kaspersky Blog: kaspersky.co.uk/blog/
Cybersecurity for large enterprises: kaspersky.com/small-to-medium-business-security
Cybersecurity for mid-size companies: kaspersky.com/enterprise-security

Kaspersky understands the needs of different industries and company sizes and **protects over 220,000 companies worldwide** against cyber threats. Kaspersky's reliable all-in-one cyber protection covers multiple protection dimensions. **Protect now!**