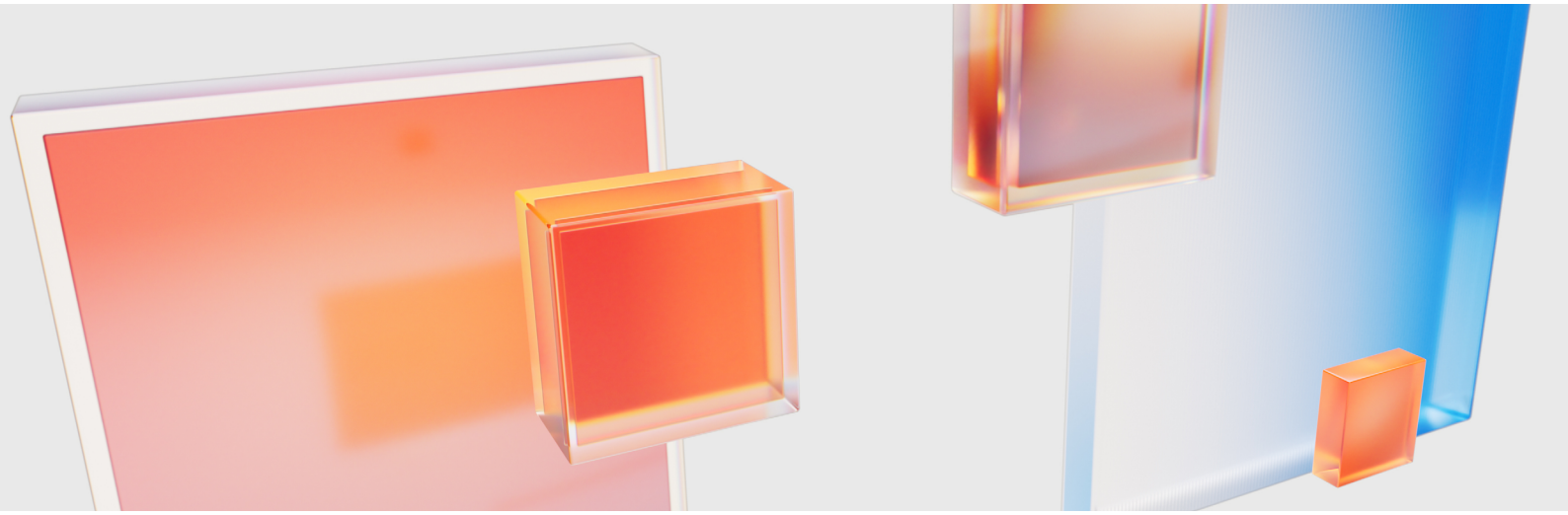
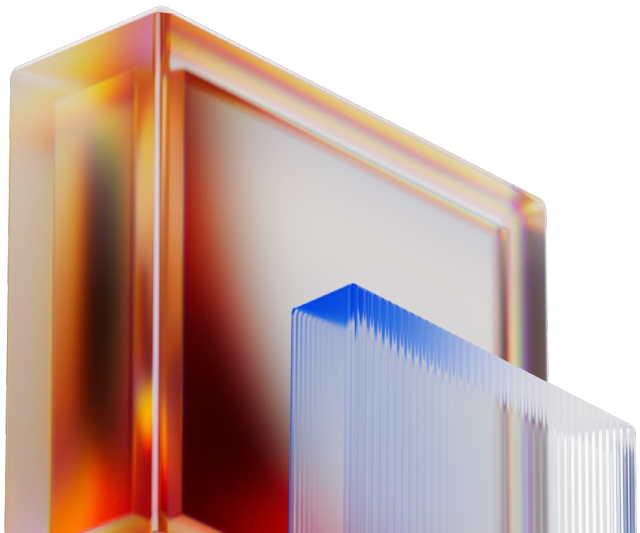


Navigating NIS2: SonicWall's Guide to Compliance

As of October 17. 2024, all member states of the European Union (EU) are legally compelled to fulfill the obligations set forth in the second iteration of the Network and Information Security Directive (NIS2).

This updated version, first introduced in 2020, implements stricter security protocols, expands the scope of the directive to include more critical sectors as well as digital service providers, and requires operators of critical infrastructure and essential services to implement enhanced security measures and reporting. It also calls for more stringent penalties and for senior management and all employees to undergo regular training in cybersecurity.

SonicWall and its partners are ready to support those organizations impacted by the new directive and have prepared this briefing to more fully inform customers as to what is expected of them, what the consequences of non-compliance would be, and how extensively we are prepared to help them achieve and maintain compliance.



What is NIS2

With data addressed by the General Data Protection Regulation (GDPR), the EU also introduced a Network and Information Security (NIS) directive to address cybersecurity requirements across networks. In 2023, the NIS directive was updated, with the update being dubbed NIS2. This directive became EU law on October 17, 2024. The objective, most simply stated, is to boost and establish a high common level of cybersecurity across the EU.

The key objective of NIS2 is to achieve "a high common level of cybersecurity across the Union." Given the nature of the internet (being a "network of networks"), NIS2 is designed to directly address the connections at which point each individual network accesses the public internet.

Member states are required to fully adopt published national cybersecurity strategies. They must also designate competent authorities to be responsible for cyber crisis management and be a single point of contact for all cybersecurity-related issues for their organization.

These authorities will be subject to very specific reporting obligations which vary based on the stated level of criticality that characterizes their organization. There are also requirements set forth regarding the cybersecurity of information sharing, and the supervision and enforcement of the directive among EU Member States.

NIS2 Drivers

The European Parliamentary Research Service (EPRS) has stated that cyber-attacks are among the fastest-growing forms of crime worldwide and continue to grow not only in scale and sophistication but also in terms of cost to victims. Businesses, as a result, have been forced to invest significantly more in hopes of making the entire cyber environment safer, more secure and more private for themselves, their customers and their business partners. They estimate that cybersecurity spending exceeds $150 billion and expect it to rise to well above $400 billion by 2026.

Another key element to the NIS2 Directive is the identification of critical sectors, including transport, energy health and finance, which have become increasingly dependent on networks and digital technologies to run their core business. While this increased connective brings with it tremendous business opportunities, it also exposes whole societies and their economies to damage and theft.

The sheer number, complexity and scale of cybersecurity incidents are all growing, and along with them their economic and social impact. Cybersecurity issues are an ongoing day-to-day struggle for the EU.

NIS2 is the result of several rounds of effort over several years that constitute the EU response to these growing challenges.

Who Does NIS2 Impact?

Recognizing that different organizations have different requirements for their networks and different levels of activity both in society and on networks, it establishes rules that are scaled to these requirements and to the criticality of each organization. The directive describes these as "public or private entities... which qualify as medium-sized enterprises and those who exceed the ceilings for medium-sized enterprises... and which provide their services or carry out their activities within the Union."

It also highlights entities who, regardless of their size, are providers of public networking and communication services, top-level domain internet name registries, and other "trust service providers."

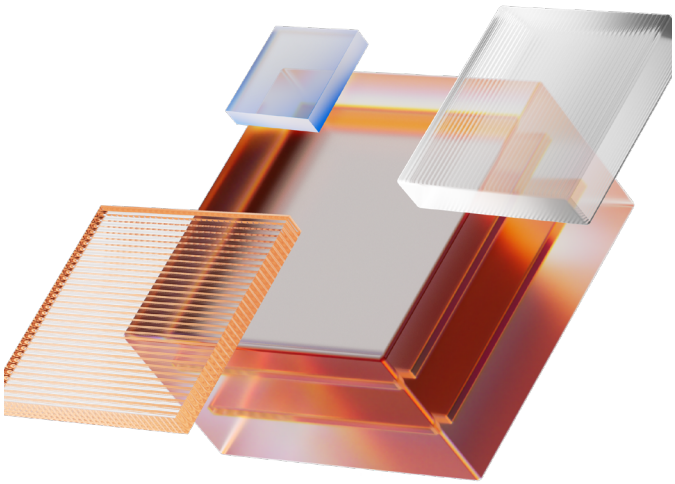
The directive also takes care to exempt "public administration entities that carry out their activities in the areas of national security, public security defense or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences."

These entities are generally presented in two different categories:

High Criticality Sectors

These include:

- **Energy** – Including electricity, district heating and cooling, oil, gas, and hydrogen.
- **Transport** – Including by air, rail, water, and road.
- **Banking** – Including credit institutions.
- **Financial Market Infrastructures** – Including trading venues (2014/65/EU) and central counterparties (CCPs).
- **Health** – Including healthcare providers, EU reference laboratories, R&D medicinal products, pharmaceutical products NACE C21, and critical medical devices.
- **Drinking water** – Including suppliers and distributors of water.
- **Waste water** – Including collecting, disposing of or treatment.
- **Digital infrastructure** – Including Internet Exchange Points (IXP), DNS, TLD registries, cloud providers, data centers, CDNs, Trust Service Providers (TSP), and electronic communications.
- **Information Communications & Technology (ICT)** – Including managed service providers and managed security service providers.
- **Public Administration** – Including central government and regional administration.
- **Space** – Including ground-based infrastructure.



Other Critical Sectors (a.k.a. Essential Services)

These include:

- **Postal and courier services**
- **Waste management**
- **Chemicals** – Including manufacture and distribution of substances and mixtures.
- **Food** – Including wholesale distribution, industrial production, processing.
- **Manufacturing** – Including medical devices and in vitro diagnostic medical services; computer, electronic, and optical products; electrical equipment; machinery and equipment; motor vehicles, trailers, and semi-trailers; and other transport equipment.
- **Digital Services** – Including market places, search engines and social networks.
- **Research** – Including research organizations.

Consequences of Non-Compliance

Executives and others who are responsible for the operation of an organization must pay special attention to Article 32 Section 6, which specifies that "natural persons" who are designated as responsible for acting as the legal representative of and making decisions for any essential entity may be held liable for any breach of their duties to ensure compliance.

This makes NIS2 perhaps the first legislation to go beyond holding the organization responsible for non-compliance, holding natural persons of responsibility and authority liable.

Penalties

This EU directive assigns the imposition and management of non-compliance penalties to the member states, requiring them to specify "penalties applicable to infringements of all national measures adopted under NIS2." They specify that the penalties provided for must be "effective, proportionate and dissuasive." Member States must notify the Commission of those rules by 17 January 2025."

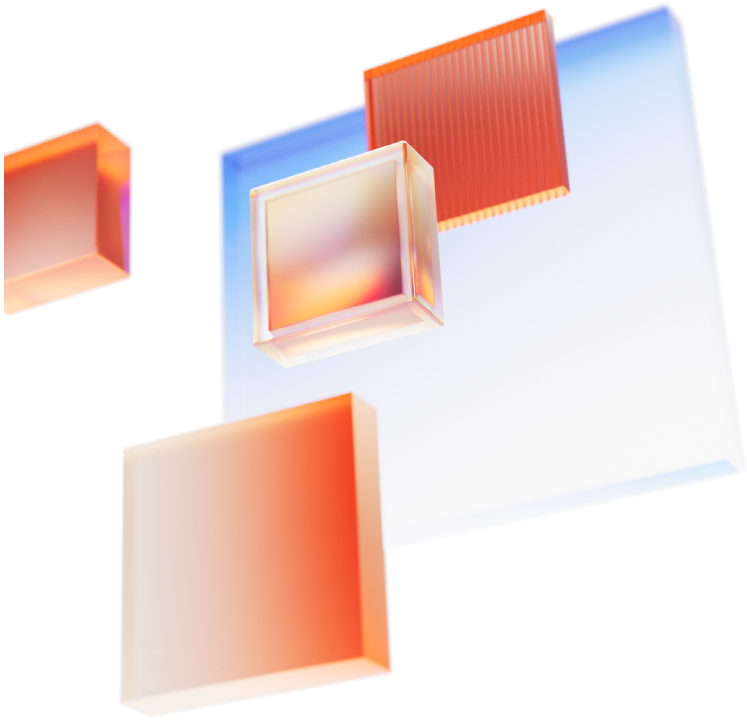
What Impacted Organizations Need to Comply with NIS2, and By When!

It is very likely that many medium-sized companies who will clearly be impacted by NIS2 lack the internal resources required to plan, design, deploy, implement and maintain compliance with the directive when it becomes law. Even larger enterprises are not likely to have those resources or to have those resources readily available given their current workloads.

Impacted businesses will need to fulfill requirements according to the deadlines specified by the EU in the NIS2 directive. SonicWall and its partners are fully prepared to provide whatever support and assistance is needed, including subject matter expertise in the NIS2 requirements.

It is worth noting that Article 20 states that "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."

This suggests that the first service customers will need from SonicWall Partners will be the training herein specified.



Deadlines

By **17 October 2024**, Member States must adopt and publish the measures necessary to comply with the NIS 2 Directive.

They shall apply those measures from **18 October 2024**.

Directive (EU) 2016/1148 (the NIS Directive) is repealed with effect from **18 October 2024**.

By **17 July 2024** and every 18 months thereafter, EU-CyCLONe shall submit to the European Parliament and to the Council a report assessing its work.

By **17 October 2024**, the Commission shall adopt implementing acts laying down the technical and the methodological requirements of the measures with regard to DNS service providers, TLD name registries, cloud computing service providers, data center service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers.

The Cooperation Group shall, on **17 January 2025**, establish, with the assistance of the Commission and ENISA, and, where relevant, the CSIRTs network, the methodology and organizational aspects of peer reviews with a view to learning from shared experiences, strengthening mutual trust, achieving a high common level of cybersecurity, as well as enhancing Member States' cybersecurity capabilities and policies necessary to implement this Directive. Participation in peer reviews is voluntary. The peer reviews shall be carried out by cybersecurity experts. The cybersecurity experts shall be designated by at least two Member States, different from the Member State being reviewed.

By **17 April 2025**, Member States shall establish a list of essential and important entities as well as entities providing domain name registration services. Member States shall review and, where appropriate, update that list on a regular basis and at least every two years thereafter.

By **17 April 2025** and every two years thereafter, the competent authorities shall notify the Commission and the Cooperation Group of the number of essential and important entities for each sector.

By **17 October 2027** and every 36 months thereafter, the Commission shall review the functioning of this Directive, and report to the European Parliament and to the Council.

Important obligations: According to Article 20 (Governance), the **management bodies** of essential and important entities must approve the cybersecurity risk-management measures taken by those entities, oversee its implementation and **"can be held liable for infringements."**

Services Customers Will Require:

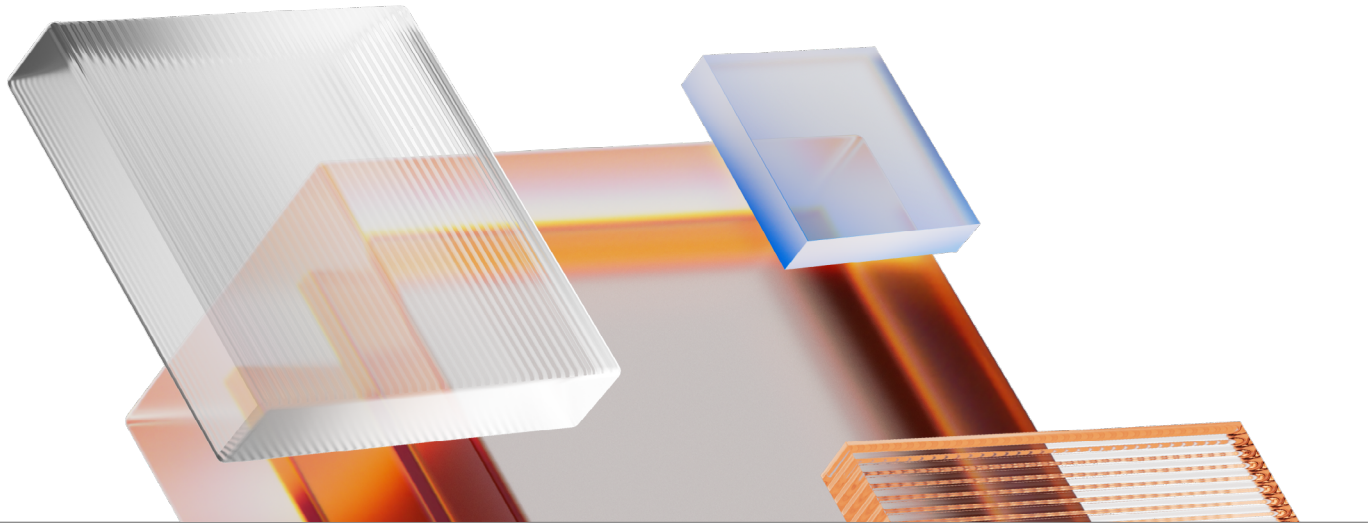
The first essential step in responding to the NIS2 Directive is ensuring that senior executives and affected organizations receive the training necessary to understand and fulfill their responsibilities under the regulation. This will be new territory for many, and it's crucial to emphasize the potential penalties for non-compliance.

This guide outlines a full lifecycle of service requirements, providing a clear roadmap of what is needed to achieve compliance. It also highlights how SonicWall solutions can support these efforts effectively. Whether you're a partner helping your customers navigate this directive or a customer seeking guidance, these steps will ensure you're prepared to meet the challenges of NIS2 successfully.

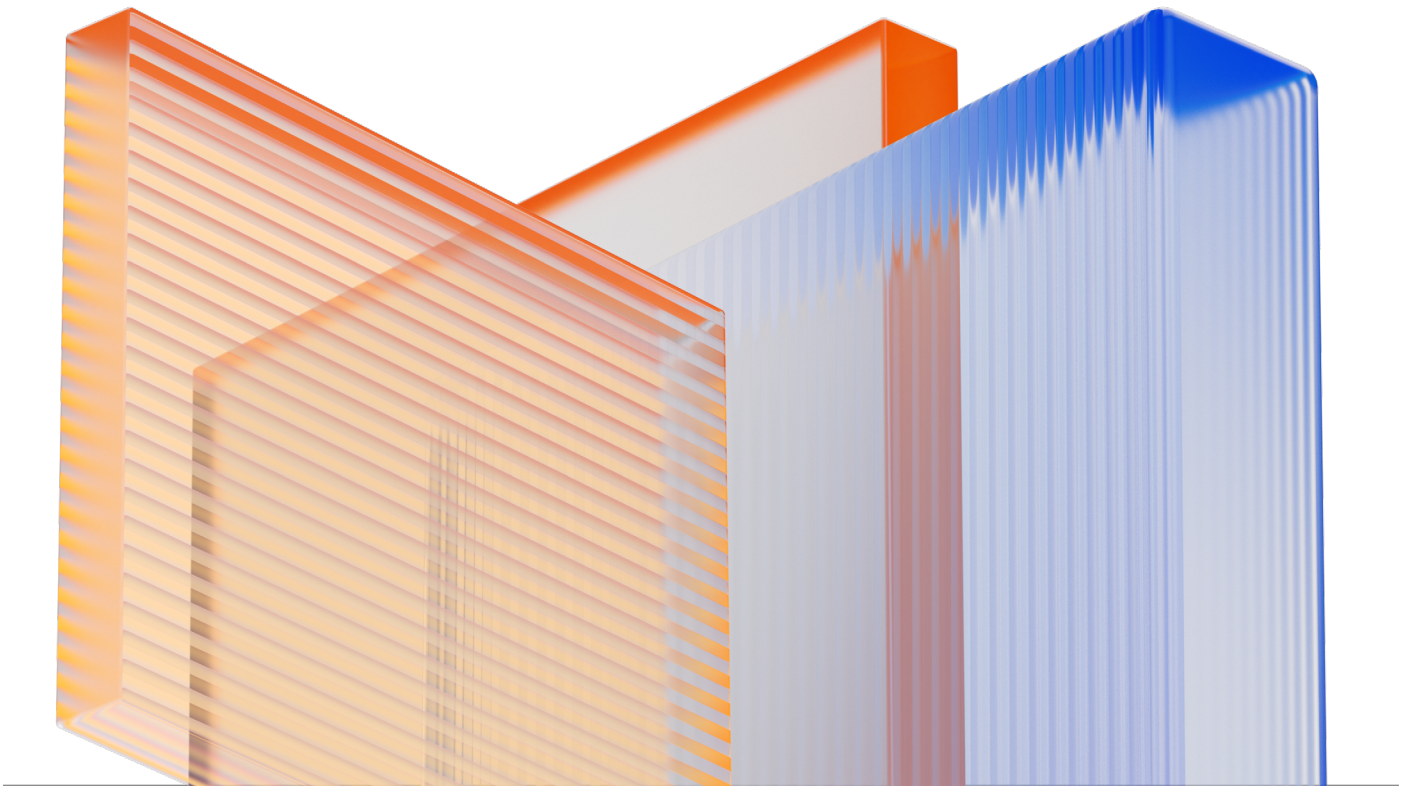
NIS2 Directive Requirements	What does this mean?	SonicWall Solution	How it addresses the requirement	How SonicWall Partners should apply it
1. Policies on risk analysis and information system security	Organizations need a formal procedure to identify, assess, and manage cybersecurity risks, as well as protect their IT systems and data from threats.	SonicWall's Managed Extended Detection and Response (MXDR)	SonicWall's SOC provides 24x7 expert monitoring across an organization IT security stack, 2x monthly configuration audits and integration of threat intelligence from multiple sources to help organizations analyze risk and quickly remediate any breaches.	Partners need to ensure that their customers: 1. have a holistic security architecture in place to defend their cloud, network and endpoints. 2. invest in a MXDR solution to add 24x7 human expertise to correlating data and risk across multiple security layers.
		SonicPlatform	SonicPlatform is a tool that brings a unified console experience to SonicWall's cybersecurity solutions. It provides a single pane of glass to view security alerts, manage renewals, deploy new licenses, and manage multiple tenants from a single portal. This efficiency leads to better management and response to cybersecurity risks.	
		Next-Generation Firewall (NGFW)	SonicWall's next-generation firewalls (NGFWs) provide the security, control and visibility needed to maintain an effective cybersecurity posture for specific security and usability needs.	
		Wireless Access Points (AP)	SonicWall Access Points (APs) provide an enhanced user experience with advanced industry leading security and wireless features, helping to secure an organization's wireless connectivity needs.	
		Secure Mobile Access (SMA)	SonicWall Secure Mobile Access (SMA) is a unified secure access gateway that enables organizations to provide access to any application, anytime, from anywhere and any devices, ensuring security policy enforcement for remote and hybrid use cases.	
		Cloud Secure Edge (CSE)	SonicWall Cloud Secure Edge (CSE) enables your workforce to securely access any resource from any device. It delivers simple, secure, zero trust access to private and internet resources for all your employees and third parties, regardless of network location which helps enforce security posture of every user whenever and wherever.	
		Capture Client	SonicWall Capture Client is an easy-to-deploy endpoint security solution powered by a dual-engine. Capture Client secures endpoints effectively with a combination of EPP, EDR, and integrated network security tools. Capture Client provides a layered security approach at the endpoint for an air-tight defense.	

NIS2 Directive Requirements	What does this mean?	SonicWall Solution	How it addresses the requirement	How SonicWall Partners should apply it
2. Incident handling	Organizations need structured processes and the appropriate tools to respond to a breach or attack. The goal of incident handling is to reduce the damage and ultimately cost of a security breach.	SonicWall's Managed Extended Detection and Response (MXDR)	SonicWall's SOC provides 24x7 expert monitoring across an organization IT security stack, 2x monthly configuration audits and integration on threat intelligence from multiple sources to help organizations better respond to incidents and remediate threats faster.	Partners should educate customers on what tools can provide threat response, analytics, and reporting capabilities needed to adequately handle incidents. Partners should also encourage organizations to invest in a MXDR service that can assist in mitigating and responding to incidents and breaches quickly.
		SonicPlatform	SonicPlatform is a tool that brings a unified console experience to SonicWall's cybersecurity solutions. It provides a single pane of glass to view security alerts, manage renewals, deploy new licenses, and manage multiple tenants from a single portal. This efficiency leads to optimized security and better management of threats and incidents.	
		Capture Client	SonicWall Capture Client includes powerful threat detection and response tools to stop, detect and prevent threats. Powered by a dual-engine, these capabilities are key to providing a layered defense at the endpoint and appropriately responding to incidents and reducing the overall impact of a cyberattack.	
3. Human resources security, access control polices and asset management	Organizations implement controls and practices that ensure anyone involved in a business' operations is given the appropriate level of access to assets before, during, and after their interaction with the organization.	Next-Generation Firewall (NGFW)	SonicWall's Next-Generation Firewall (NGFW) supports the following: multi-factor authentication and firewall segmentation to better control and enforce appropriate access to users across a network.	Partners should encourage customers to adopt tools that support multi-factor authentication and granular access controls across their organization, ideally adopting a zero-trust security model.
		Secure Mobile Access (SMA)	SonicWall's Secure Mobile Access (SMA) enables secure, role-based access to corporate resources, ensuring that employees and contractors only access systems and data appropriate to their roles, in line with access control policies. It also supports asset management by providing visibility into devices accessing the network, allowing organizations to enforce security policies and manage the security of mobile and remote devices.	
		Cloud Secure Edge (CSE)	SonicWall Cloud Secure Edge is a Security Service Edge (SSE) solution which delivers simple, secure, zero trust access to private and internet resources for all your employees and third parties, regardless of their network location. Based on a zero-trust model of security, CSE helps organizations grant the appropriate level access to organizational assets and resources.	

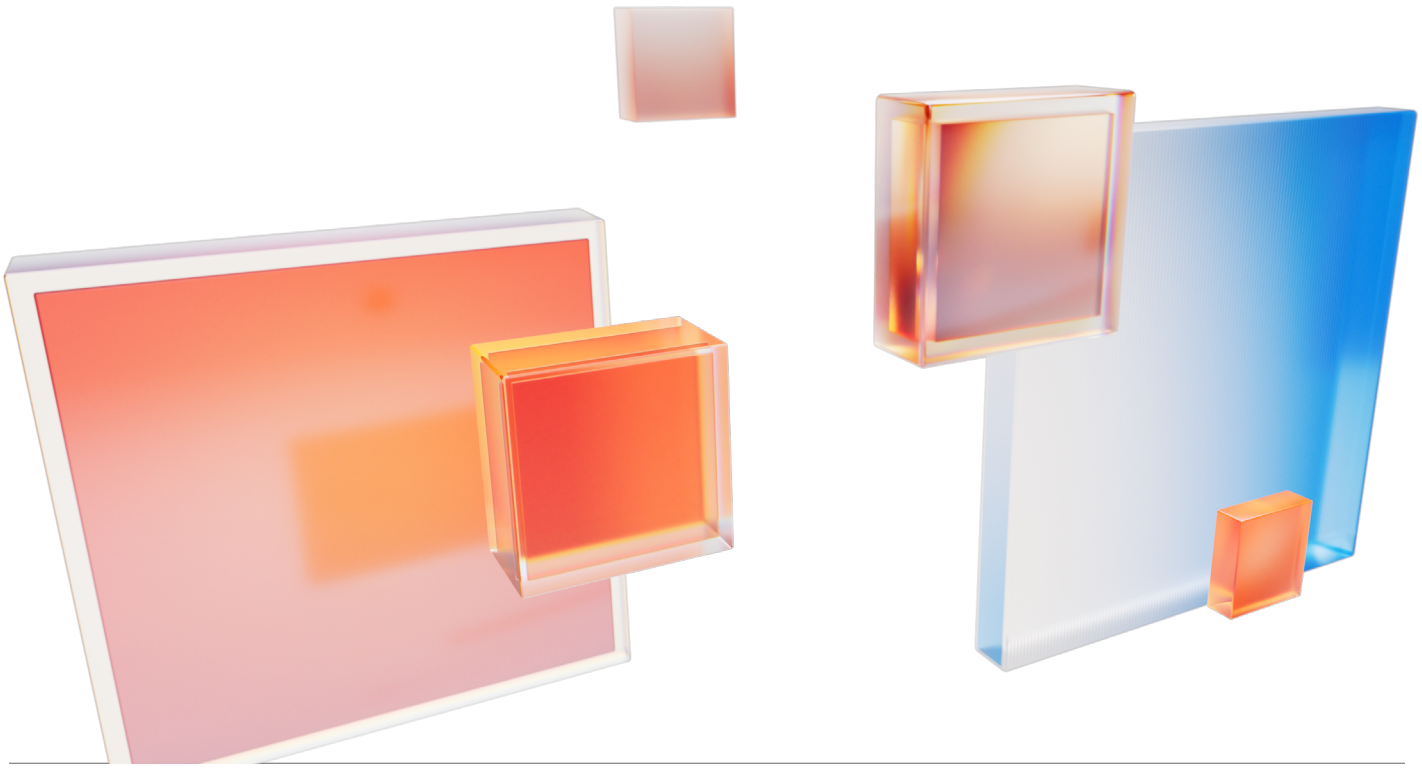
NIS2 Directive Requirements	What does this mean?	SonicWall Solution	How it addresses the requirement	How SonicWall Partners should apply it
4. Policies and procedures to assess the effectiveness of cybersecurity risk-management measures	Organizations must have a standardized process to regularly evaluate and audit how their current security posture is mitigating risks and protecting assets.	SonicWall's Managed Extended Detection and Response (MXDR)	SonicWall's Managed Extended Detection and Response (MXDR) is a co-managed service offering that helps organizations with the people and processes needed to evaluate the alerts and information across an organization's security stack. With 2x/monthly audits, partners can help organizations regularly audit their cybersecurity posture and identify any gaps in risk management measures.	Partners should adopt and offer a MXDR service to bolster their customer's security posture and take advantage of 2x/monthly audits to assess the effectiveness of the security posture and address gaps in risk management measures for their customers. In addition, partners can take advantage of services like SonicWall's Security Health Check Service, Professional Service Offering, and Partner Enabled Services (PES) which provide comprehensive reviews of your security posture with actionable recommendations to address security gaps.
5. 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	Organizations must secure access to IT assets and communication channels through the use of multi-factor authentication.	Next-Generation Firewall (NGFW)	SonicWall Next-Generation Firewalls (NGFWs) support the use of single-sign on and multi-faction authentication to provide an extra layer of security for appliances while securing an organization's network.	Partners should recommend security tools that support multi-factor authentication.
		Secure Mobile Access (SMA)	SonicWall Secure Mobile Access (SMA) supports multi-factor authentication and uses a model of zero trust network access to grant granular access controls to ensure that appropriate users can access the assets wherever and whenever.	
		Cloud Secure Edge (CSE)	SonicWall Cloud Secure Edge is a cloud-based solution which supports multi-factor authentication to allow users to securely access any resource from any device. It accomplishes this by delivering zero trust network access, micro-segmentation, and granular access capabilities which all contribute to securing an organization's access to resources.	



NIS2 Directive Requirements	What does this mean?	SonicWall Solution	How it addresses the requirement	How SonicWall Partners should apply it
6. Business continuity, such as backup management and disaster recovery, and crisis management	Organizations ensure operations can continue during and after IT disruption through strategies that safeguard critical data by creating regular backups and restore systems and data after a cyberattack or other incidents.	SonicPlatform	SonicPlatform consolidates alerts from across all SonicWall to one unified console so that organizations can quickly address critical alerts to prevent breaches. This reduced operational complexity leads to greater efficiency and optimized security for business continuity needs.	Partners should recommend solutions that provide features that can assist in creating regular backups of data and seamlessly restore IT systems after an incident. In addition, partners should invest in a managed security service offering to provide real-time threat detection and response to mitigate cyber risks before operations are disrupted. To best enable these tools and services, partners should also provide training and education on how to use these tools during a breach/ incident to safely restore operations.
		Capture Client	Capture Client's dual engine powers multiple prevention, detection, and remediation capabilities at the endpoint. Capture Client's rollback capabilities allow infected machines to be remotely restored to a pre-infected state and can be isolated from the network to prevent lateral movement of threats. This makes it easier for an organization to recover endpoints during disaster recovery efforts.	
		SonicWall's Managed Extended Detection and Response (MXDR)	SonicWall's Managed Extended Detection and Response service offering works with partners to detect and mitigate threats that could disrupt operations at any hour of the day or week. By detecting and neutralizing threats before they can cause significant damages, MXDR minimizes downtime and ensures system availability. The SOC team proactively identifies vulnerabilities in 2x/monthly audits to identify vulnerabilities which can help in maintaining secure backups and data integrity, ensuring that organizations can quickly resume operations in event of a cyber incident.	



NIS2 Directive Requirements	What does this mean?	SonicWall Solution	How it addresses the requirement	How SonicWall Partners should apply it
7. Supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers	Organizations must assess and manage security risks associated with third-party partners to minimize potential threats within a supply chain network.	Next-Generation Firewall (NGFW)	SonicWall's Next-Generation Firewalls (NGFWs) enhance supply chain security by providing advanced threat protection, including intrusion prevention, deep packet inspection, and real-time monitoring of network traffic. By controlling access to sensitive resources, blocking malicious traffic, and inspecting encrypted connections, NGFWs help secure the communication channels between an organization and its suppliers or service providers. This reduces the risk of supply chain-related vulnerabilities, such as malware or data breaches, ensuring that each entity in the supply chain adheres to strong cybersecurity practices.	In an environment when securing third-party users, partners can recommend tools which can safely grant remote access and granular controls wherever a user is. They should also encourage the adoption of a zero-trust model to minimize threats within a supply chain network.
		Secure Mobile Access (SMA)	SonicWall Secure Mobile Access (SMA) helps to connect remote and third-party users securely to a network or an organization's internal assets through encrypted access for suppliers and partners so that only authorized users can access specific resources. It reduces the risk of third-party vulnerabilities or compromised devices affecting the organization by enforcing strict access control and continuous monitoring.	
		Cloud Secure Edge (CSE)	SonicWall's Cloud Secure Edge provides users or third-parties access to private and internet resources regardless of their network location. Users are constantly verified to prevent bad actors or unauthorized users from taking advantage of supply chain vulnerabilities.	

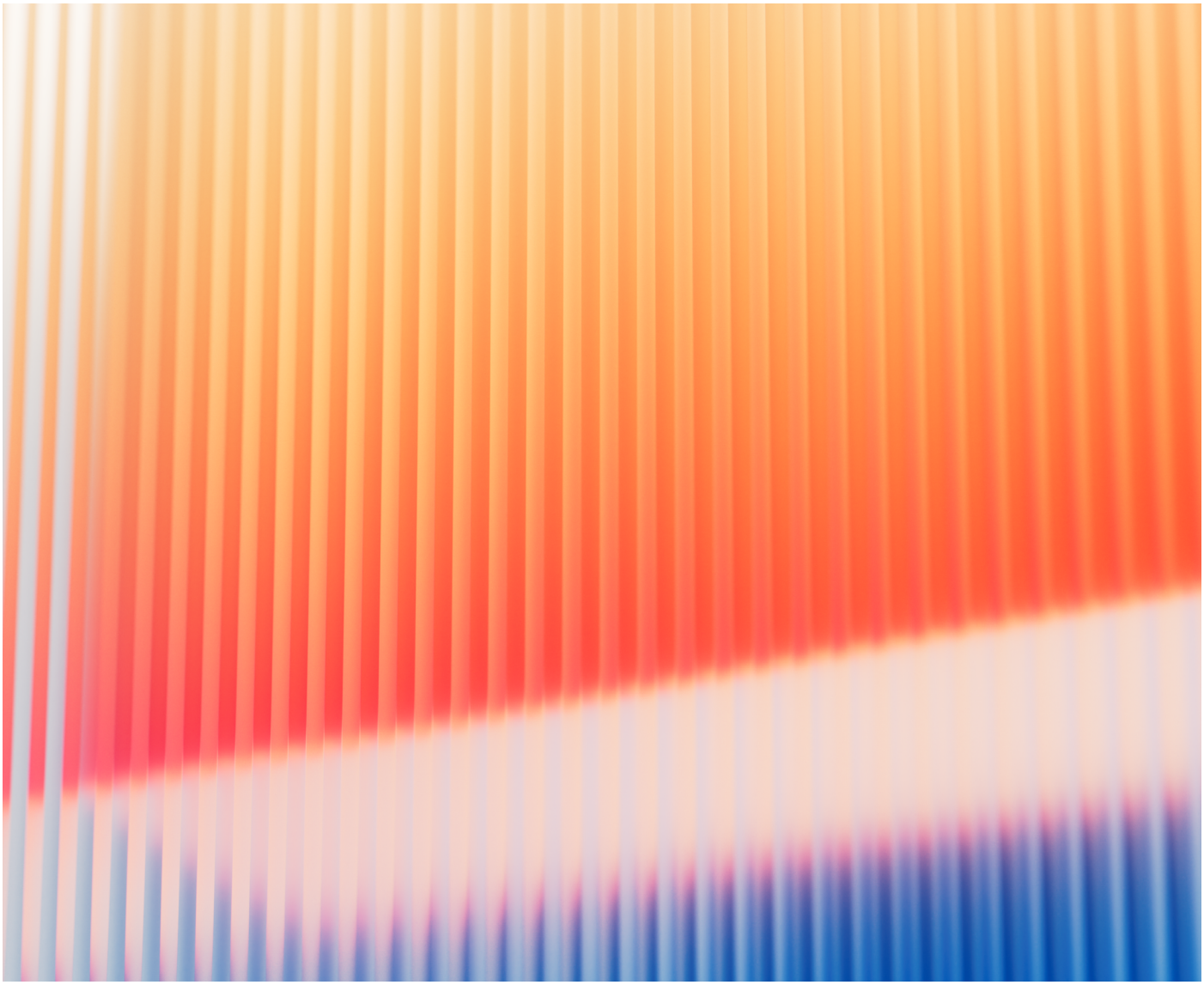


NIS2 Directive Requirements	What does this mean?	SonicWall Solution	How it addresses the requirement	How SonicWall Partners should apply it
8. Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure	Organizations must integrate security measures throughout the lifecycle of an IT system. This includes timely disclosures of any security breaches that are detected while also proactively managing vulnerabilities and remediating security flaws.	SonicWall's Managed Extended Detection and Response (MXDR)	SonicWall's Managed Extended Detection and Response (MXDR) is a co-managed security service offering that utilizes a 24/7/365 SOC team that will continuously monitor and detect threats in real-time across an organization's network and information systems. It also supports handling and disclosures of incidents through providing automated alerts, detailed incident reports, and expert-led response efforts to mitigate threats.	Partners need to ensure customers: 1. Have a holistic security architecture that secures their network, cloud, and endpoints. 2. invest in a MXDR service offering to optimize their security tools across each layer. Partners should also adopt platform-centric solutions that grant visibility and reduce complexity when managing all the security layers of their customer's environment.
		Capture Client	Capture Client secures your networks and information systems by providing advanced endpoint protection, monitoring for vulnerabilities, and enforcing security postures across an organization's devices – regardless of whether they're on or off-prem. By automatically detecting and isolating threats, it helps in managing network vulnerabilities at the endpoint while offering detailed reports for effective disclosure and timely remediation.	
		Secure Mobile Access (SMA)	SonicWall Secure Mobile Access (SMA) ensures secure, role-based access to network and information systems by preventing unauthorized access. In addition, SMA provides secure maintenance access for service providers by enabling encrypted, controlled access for patching and updates, ensuring vulnerabilities are managed without exposing systems to additional risks.	
		Cloud Secure Edge (CSE)	Cloud Secure Edge (CSE) securely connects users across a network using a zero-trust framework, ensuring that only authorized users and devices can access critical systems and data throughout the IT lifecycle. When vulnerabilities are detected, CSE enables organizations to configure device posture remediation instructions to the user.	
		SonicPlatform	SonicPlatform offers one single platform of unified visibility for SonicWall network, cloud, and endpoint solutions across multiple tenants. This consolidation leads to decreased complexity and thus increased efficiency in detecting and addressing vulnerabilities.	
		Next-Generation Firewall (NGFW)	SonicWall's Next-Generation Firewalls (NGFWs) provide networks with comprehensive threat protection which includes intrusion prevention and deep packet inspection, and application control. The NGFWs continuously monitor and analyze network traffic to detect and block potential threats, while also providing detailed reporting and alerts for vulnerabilities to promptly address and remediate security issues.	

NIS2 Directive Requirements	What does this mean?	SonicWall Solution	How it addresses the requirement	How SonicWall Partners should apply it
9. Basic cyber hygiene practices and cybersecurity training	Organizations must provide and maintain fundamental security measures for all users to protect against common threats and provide training to educate users within the organization on cybersecurity best practices.	SonicWall's Managed Extended Detection and Response (MXDR)	SonicWall's Managed Extended Detection and Response (MXDR) service offering can support basic cyber hygiene practices by providing real-time continuous monitoring, threat detection. Through its 2x/monthly audits, SonicWall's SOC team offers reports with actionable insights to help organizations address their system vulnerabilities. Incident reports generated can also help to educate employees on security incidents and thus best practices to prevent these incidents again.	Partners should recommend tools that have web content filtering capabilities which can promote basic cyber hygiene practices by preventing access to known malicious sites. In addition, partners should invest in providing a MDR service on top of their cybersecurity offerings which can help in ensuring the cybersecurity posture is maintained at a baseline level.
		Capture Client	Capture Client offers advanced endpoint protection, application vulnerability intelligence, and policy enforcement across all endpoints both on and off-prem to ensure that devices are secure and compliant to organizational policies. Capture Client's web content filtering can prevent users from accessing known malicious sites, facilitating basic cyber hygiene practices.	
10. Policies and procedures regarding the use of cryptography and, where appropriate, encryption	Organizations must establish formal guidelines for what, how, and when sensitive information is protected.	Next-Generation Firewall (NGFW)	SonicWall's Next-Generation Firewalls (NGFWs) enforce encryption standards for data in transit by inspecting and managing all encrypted traffic, ensuring that only compliant encryption methods are used, and protecting sensitive information according to organizational policies and regulatory requirements.	Partners should ensure that the customer has a holistic security architecture across the cloud, network, and endpoints in order to ensure that sensitive information remains protected. It is important for partners to adopt solutions that ultimately provide a layered security approach to establish adequate defenses against threats and data exfiltration.
		Secure Mobile Access (SMA)	SonicWall Secure Mobile Access (SMA) provides secure, encrypted access to network resources for remote users. It ensures that data transmitted between remote devices and the network is protected with strong encryption standards set by organizational policies for secure communication and safeguarding sensitive information from unauthorized access.	
		Cloud Secure Edge (CSE)	SonicWall Cloud Secure Edge (CSE) ensures that all data exchanged between users and the internet, private resources, and cloud services is encrypted and complies with any organizational security policies and adheres to requirements protecting sensitive information.	

Get Started Now

Compliance with the NIS2 Directive will be an ongoing journey that requires agility from organizations and their trusted partners. SonicWall is here to help you stay on top of these evolving regulations and provide the expertise and solutions needed to empower your organization to navigate these compliance requirements. Reach out to SonicWall to learn more.



About SonicWall

SonicWall is a cybersecurity forerunner with more than 30 years of expertise and a relentless focus on its partners. With the ability to build, scale and manage security across the cloud, hybrid and traditional environments in real time, SonicWall can quickly and economically provide purpose-built security solutions to any organization around the world. Based on data from its own threat research center, SonicWall delivers seamless protection against the most evasive cyberattacks and supplies actionable threat intelligence to partners, customers and the cybersecurity community.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL