Strengthening Cybersecurity Resilience

The Xage Approach to Addressing NCSC CAF Alignment and NIS2 Requirements

Increasing Threats and Changing Legislation

As organisations face increasing cybersecurity threats, compliance with regulatory frameworks such as the National Cyber Security Centre's Cyber Assessment Framework (CAF) and the European Union's Network and Information Systems Directive (NIS2) is crucial. Xage, a pioneer in decentralised cybersecurity solutions, offers a comprehensive approach to address the requirements of both the NCSC CAF and NIS2. This paper examines how Xage's innovative technologies and methodologies align with the principles and objectives of these regulatory frameworks, enabling organisations to enhance their cybersecurity resilience and regulatory compliance simultaneously.

What Are NCSC CAF and NIS2?

The NCSC CAF and NIS2 are two prominent regulatory frameworks aimed at bolstering cybersecurity resilience within organisations.

NCSC CAF

The National Cyber Security Centre (NCSC)

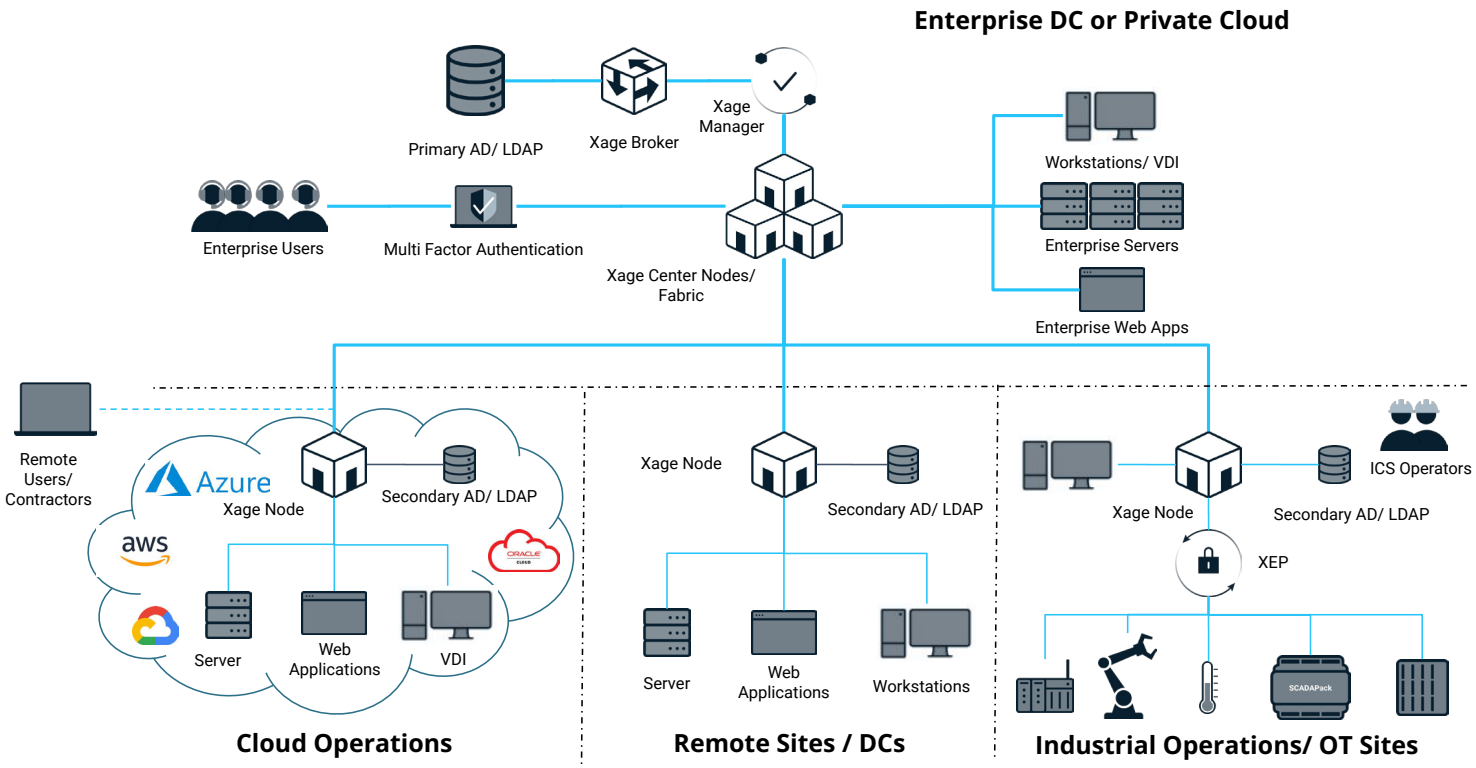
The CAF provides guidance to organisations on assessing and improving their cybersecurity posture across various domains, including governance, risk management, technical security measures, incident response, and supply chain security. It emphasises the importance of implementing robust cybersecurity controls and practices to mitigate cyber risks effectively.

NIS2

NIS2 mandates operators of essential services (OES) and digital service providers (DSPs) to implement cybersecurity measures to ensure the security and resilience of network and information systems. It sets out requirements related to risk management, security measures, incident reporting, and cooperation with competent authorities to address cyber threats effectively.

Xage's Approach to Addressing NCSC CAF and NIS2 Requirements:

Xage employs a decentralised architecture built on distributed ledger technology, which ensures secure and tamper-proof communication, authentication, and access control. This approach aligns with the principles of both the NCSC CAF and NIS2 by providing robust security measures to protect critical assets and systems. Xage is particularly helpful at addressing supply chain and vendor-related risks highlighted in Section 85 and in implementing zero trust architectures noted in Section 89.



NIS2 Section 85

"Addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important given the prevalence of incidents where entities have been the victim of cyberattacks and where malicious perpetrators were able to compromise the security of an entity's network and information systems by exploiting vulnerabilities affecting third-party products and services. Essential and important entities should therefore assess and take into account the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures. Essential and important entities should in particular be encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers. Those entities could consider risks stemming from other levels of suppliers and service providers."

Zero Trust

Governments and organisations around the world are recognizing the importance of zero trust principles and beginning to implement them. That shift is reinforced in NIS2 in section 89 which calls out zero trust specifically and lists many practices and principles that are part of a zero trust strategy.

NIS2 Section 89

"Essential and important entities should adopt a wide range of basic cyber hygiene practices, such as zero-trust principles, software updates, device configuration, network segmentation, identity and access management or user awareness, organise training for their staff and raise awareness concerning cyber threats, phishing or social engineering techniques. Furthermore, those entities should evaluate their own cybersecurity capabilities and, where appropriate, pursue the integration of cybersecurity enhancing technologies, such as artificial intelligence or machine-learning systems to enhance their capabilities and the security of network and information systems."

Xage: Key Capabilities for Aligning with NIS2 and NCSC CAF

Granular Access Control: Xage's distributed access control mechanisms enable organisations to implement granular access permissions with zero trust, least-privilege policies as the default based on identity, role, and context, thereby reducing the risk of unauthorised access and insider threats. This capability addresses the access control requirements outlined in Section 89 of NIS2. Xage's access control also fulfils many of the requirements laid out in NCSC CAF Objective B ("Protecting against cyber attack"), including:

- Principle B2 - Identity and Access Control
  - B2.a Identity Verification, Authentication, and Authorization
  - B2.b Device Management
  - B2.c Privileged User Management
  - B2.d Identity and Access Management (IdAM)

Immutable Audit Trails: Xage creates immutable audit trails that record all interactions and transactions within the system. These tamper-proof logs provide organisations with visibility into system activity, facilitating compliance monitoring, incident investigation, and reporting obligations under NIS2. Xage's activity monitoring, audit logs, and the access controls applied to them also fulfil many of the requirements laid out in Principle C1 (Security Monitoring), and C2 (Proactive Security Event Discovery) of NCSC CAF.

Threat Prevention: Xage's decentralised monitoring and device protection capabilities enable organisations to prevent and respond to cyber threats in real time, minimising the impact of security incidents and ensuring timely incident reporting as required by NIS2.

Interoperability and Integration: Xage's platform is designed to integrate seamlessly with existing IT infrastructure and cybersecurity solutions, enabling organisations to leverage their investments while enhancing overall cybersecurity resilience and compliance with the NCSC CAF and NIS2.

Meet NCSC CAF and NIS2 Requirements with Xage

Xage offers a comprehensive approach to address the requirements of both the NCSC CAF and NIS2, enabling organisations to strengthen their cybersecurity posture, mitigate cyber risks, and achieve regulatory compliance. By leveraging decentralised technologies, granular access controls, immutable audit trails, and real-time threat detection capabilities, Xage empowers organisations to protect critical assets and infrastructure while navigating the complex regulatory landscape effectively. As organisations strive to enhance their cybersecurity resilience and regulatory compliance, solutions like Xage play a pivotal role in safeguarding against cyber threats and ensuring the security and resilience of digital ecosystems.

Please contact us for more details on how Xage can help your organisation achieve the goals set out in NSCS CAF and comply with the requirements of NIS2.

About Xage Security

Xage is a global leader in zero trust access and protection on a mission to pioneer a secure tomorrow. Control access and prevent attacks in the cloud, in the data center, at the remote operational edge anywhere on Earth, and even in orbit with the Xage Fabric Platform. Xage is easy to manage and can be deployed in a day, giving users easy and secure access to the assets they need from anywhere, while preventing advanced adversaries and insider threats at every stage of the attack chain. Learn why organizations like the U.S. Space Force, PETRONAS, and Kinder Morgan choose Xage at xage.com.