Solution Brief

Applying Technical Controls to the EU NIS with Forescout

Protect critical infrastructure and simplify compliance with EU NIS

Who Does the NIS Directive Affect?

Companies and organisations identified as either OES or Competent Authorities (CAs). According to the International Association of Privacy Professionals (IAPP),[4] the list of specific sectors affected by NIS are:

- **Energy**: oil, gas and electricity supply, distribution, transmission and storage operators as defined under Directive 2009/72/EC and Directive 2009/73/EC.
- **Transport**: including air transport, rail transport, water transport and road transport, with emphasis on entities that manage traffic-control services as well as port, airport and rail authorities.
- **Banking**: specifically, credit institutions, defined under Regulation 575/2013 as “an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account.”

According to the European Commission (EC), critical infrastructure is defined as “an asset or system which is essential for the maintenance of vital societal functions.” Further, the EC states that “damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the European Union (EU) and the well-being of its citizens.”[1]

What is the EU NIS Directive?

The Directive on security of Network and Information Systems (the NIS Directive)[2] was adopted by the European Parliament on 6 July 2016 and entered into force in August 2016. Member States had 21 months to transpose the Directive into their national laws and six months more to identify operators of essential services. The aim of the NIS Directive is to provide legal measures to boost the overall level of cybersecurity in the EU.

The NIS Directive is a first essential step with a view to promoting a culture of risk management by introducing security requirements as legal obligations for the key economic actors, notably:

1. Operators providing essential services (Operators of Essential Services—OES), and
2. Suppliers of some key digital services (Digital Service Providers—DSPs).

DSPs are limited to only three types of services: cloud, online marketplaces and search engines (more below). The NIS Directive will help make sure operators of critical national infrastructure (electricity, transport, water, energy, health and digital infrastructure) are prepared to address the ever-increasing numbers of cyber threats. It will also cover other threats affecting IT, such as power failures, hardware failures and environmental hazards. Fines could be as much as £17 million or 4 percent of global turnover.[3]

Who Does the NIS Directive Affect? (con’t)

- **Financial market infrastructures**: including operators of trading venues and “central counterparties,” which are entities that interpose themselves between parties to contracts traded on financial markets, thereby reducing the risk exposure to the original parties to the contracts.
- **Health**: “any natural or legal person or any other entity legally providing healthcare on the territory of a Member State.”
- **Drinking water supply and distribution**: applies to suppliers and distributors of water intended for human consumption, but not to distributors whose general activity is the distribution of other commodities and goods.
- **Digital infrastructure**: Internet exchange points, domain name system service providers and top-level domain name registries.

What is the Difference Between NIS and General Data Protection Regulation (GDPR)?

To put it simply: The NIS Directive relates to loss of service rather than loss of data, which falls under the GDPR. While the NIS Directive and GDPR are clearly two distinct pieces of law, they overlap with respect to their jurisdiction over breaches caused by operators of essential services and digital service providers. NIS introduces breach notification requirements that extend beyond those of the GDPR. Unlike the GDPR, which mandates notification only when there is a risk to the processing of any personal data of EU residents, the Directive requires operators to notify competent authorities whenever there is a substantial impact on the provision of the operator’s service. Thus, while the GDPR includes security and notification provisions to protect personal data, the Directive seeks to improve security safeguards and the sharing of knowledge on cybersecurity threats.

Standards

Member states are “encouraged to use European or internationally accepted standards and specifications relevant to the security of network and information systems” with no bias towards any particular technology. The NIS directs the European Network and Information Security Agency (ENISA,) in collaboration with Member States, to draft advice and guidelines “regarding the technical areas to be considered in relation to paragraph 1, as well as regarding already-existing standards, including Member States’ national standards, which would allow for those areas to be covered.”[5]

Enforcement

NIS gives the power to investigate noncompliance, include undergoing a security audit, to “the competent authorities in each member state.”

Transposing the EU NIS in the UK

In support of the UK NIS Directive implementation, the National Cyber Security Center (NCSC) will work with lead government departments, regulators and industry to develop a method to assess whether an organization is adequately managing cybersecurity risks in relation to the delivery of essential services. This assessment method, otherwise known as the Cyber Assessment Framework (CAF), is intended to meet both NIS Directive requirements and wider needs.

The NCSC has also published implementation guidance and support to CAs to enable them to adapt the NCSC NIS principles for use in their sectors, plan and undertake assessments using the CAF, and interpret the results.

Implementing the Cyber Assessment Framework in the UK

The implementation of the EU Security of NIS Directive in May 2018 requires CAs to have the ability to assess the cyber security of OES through the use of the CAF.

Who Does the NIS Directive Affect? (con't)

The Directive also applies to "digital service providers,"[4] which include online marketplaces, search engines or cloud computing services. However, it does not apply to companies that are considered small- or micro-enterprises. Therefore, digital service providers with fewer than 50 employees and an annual balance sheet total under 10 million euros are exempt from the Directive's requirements. Digital services under the Directive are defined as:

- **Online marketplace**: a digital service that allows consumers and/or traders to conclude online sales and service contracts.
- **Online search engine**: a digital service that allows users to perform searches of all websites or websites in a particular language on the basis of a keyword, phrase or other input and which returns links to related content.
- **Cloud computing service**: "a digital service that enables access to a scalable and elastic pool of shareable computing resources."

Some sectors are exempt from aspects of the Directive where there are provisions within their existing regulations which are, or will be, at least equivalent to those the NIS Directive specifies (for example, finance or civil nuclear sectors).

The CAF consists of a collection of top-level NIS Principles who define fairly wide-ranging cybersecurity outcomes or objectives. Organizations will further define their approach to each principle. Each objective is associated with a set of indicators of good practice (IGPs). Each IGP is then assessed as 'achieved,' 'not achieved' or in some cases 'partially achieved.'

How Forescout Simplifies Implementing the UK CAF

There are four UK CAF objectives:

Objective A – Managing security risk	• Governance • Risk management • Asset management • Supply chain
Objective B – Protecting against cyberattack	• Service protection policies and processes • Identity and access control • Data security • System security • Resilient networks and systems • Staff awareness and training
Objective C – Detecting cyber security events	• Security monitoring • Proactive security event discovery
Objective D – Minimizing the impact of cybersecurity	• Response and recovery planning • Lessons learned

Objective A – Managing security risk: Forescout provides foundational visibility necessary to accurately identify assets and effectively manage corporate and supply chain risk. Forescout's ability to see and control managed and unmanaged devices, including IoT devices on a network, reduces the risk of potential attacks and remediates malicious code or high-risk devices. The Forescout platform can continuously acquire, assess and take action on new information in order to identify vulnerabilities, remediate noncompliant or compromised devices and minimize the window of opportunity for attackers.

Objective B – Protecting against cyberattack: Forescout can help you implement your security policies and processes by continuously monitoring authorized and unauthorized access to your network, creating policies to automatically isolate rogue access points, as well as notifying personnel of discoveries. By helping to ensure real-time vulnerability scans are perfomed and that relevant third-party protection software is installed,

What Does NIS Explicitly tell Covered Entities to do?[5]

For OESs

1. Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed. (*Note, this is as specific as the NIS gets as it does not prescribe specific controls).
2. Member States shall ensure that operators of essential services take appropriate measures to prevent and minimise the impact of incidents affecting the security of the network and information systems used for the provision of such essential services, with a view to ensuring the continuity of those services.

correctly configured and operational, Forescout addresses the outcome of ensuring resilient networks and systems.

The Forescout platform identifies users attempting to access information they are not authorized access to by their Active Directory group. It provides device- and role-based network authentication and authorization, allowing individuals and their devices to get their identified network access determined by VLANs or ACLs. The Forescout platform enables automated segmentation of network access by user, device classification and/or posture, regardless of how that device is connecting to the network—wired, wireless or VPN. These devices may be mobile, servers, virtual machines, OT or other IoT devices. Network segregation strategies can be deployed centrally through the Forescout platform

Objective C – Detecting cyber security events: Forescout Extended Modules for SIEM enable bi-directional integration with leading security information and event management systems and support the outcome to effectively detect cybersecurity events. Extended Modules for SIEM combine Forescout's device visibility, access control and automated response capabilities with the powerful correlation, analysis and search features of SIEM solutions. The result is enhanced threat insight, analytics-driven decisions and greater operational efficiency. With Forescout and popular SIEM solutions, security teams can:

- Store Forescout device visibility data in SIEM solutions for long-term trend analysis, visualization and incident investigation
- Correlate high-value endpoint context from the Forescout platform with other data sources to identify and prioritize incidents.
- Initiate Forescout control via network and host actions from a SIEM product to automate incident response, remediation and threat mitigation
- Demonstrate what data is accessed, by whom, how it is used and when it is deleted
- Forescout and Splunk® customers can leverage the joint solution and Adaptive Response framework within Splunk ES for closed-loop remediation and threat mitigation

Objective D – Minimizing the impact of cybersecurity: Does not apply to technical tools such as Forescout

What Does NIS Explicitly tell Covered Entities to do?[5]

For DSPs

- Member States shall ensure that digital service providers identify and take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems...[and] those measures shall ensure a level of security of network and information systems appropriate to the risk posed, and shall take into account the following elements:

  (a) the security of systems and facilities;

  (b) incident handling;

  (c) business continuity management;

  (d) monitoring, auditing and testing;

  (e) compliance with international standards.

Learn More

Link to Critical Infrastructure White Paper

Link to Implementing the Cyber Assessment Framework Matrix

Forescout Technologies is transforming security through visibility, providing Global 2000 enterprises and government agencies with agentless visibility and control of traditional endpoints, IoT devices and operational technologies the instant they connect to the network. Our technology continuously assesses, remediates and monitors devices and works with disparate security tools to help accelerate incident response, break down silos, automate workflows and optimize existing investments. As of June 30, 2018 more than 2,900 customers in over 80 countries improve their network security and compliance posture with Forescout solutions. See devices. Control them. Orchestrate system-wide threat response. Learn how at www.Forescout.com.

[1] Critical Infrastructure Definition: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en

[2] EU NIS Directive papers: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC

[3] EU NIS Fines (Government Response to Public Consultation): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/677065/NIS_Consultation_Response_-_Government_Policy_Response.pdf

[4] EU NIS Sectors reference – IAPP: https://iapp.org/news/a/nis-gdpr-a-new-breach-regime-in-the-eu/

[5] EU NIS Directive text: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN

ForeScout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support 1-708-237-6591