VARONIS

WHITEPAPER

How Varonis Helps with **NIS Compliance**

Contents

What is NIS?

The European Union's Network and Information Systems (NIS) Directive is EU-wide cybersecurity legislation that aims to protect critical infrastructure from cyber threats. The United Kingdom (UK) adopted the NIS Directive into law in May 2018. This law provides the legal footing to ensure that member states have a national Cyber Assessment Framework (CAF) in place to be ready and capable of dealing with cybersecurity incidents.

NIS provides the legal foundation to:

- Ensure the UK has a national framework in place to manage cybersecurity incidents
- Promote cooperation among the UK member states to share information about cybersecurity risks and coordinate responses to events
- Identify operators of essential services (OES) that are required to take security measures to manage risk to their networks and information systems

NIS applies to companies and organisations that operate digital services or provide essential services. NIS does have extra-territorial jurisdiction, meaning that it applies to any organisation that stores data or serves UK member states.

A few examples of digital services are:

- Online marketplaces
- Online search engines
- Cloud computing services

NIS defines OES as companies from these sectors:

- Energy
- Transport
- Banking
- Financial markets
- Health sector
- Water supply
- Digital infrastructure

Competent authorities (CA) are specific individuals responsible for oversight of government bodies over each of these essential services. For example, the Secretary of State for Environment, Food and Rural Affairs is a CA for England.

The **Cyber Assessment Framework (CAF)** and the NIS Directive

The Cyber Assessment Framework (CAF) guides organisations responsible for complying with the NIS directive by providing direction that they can follow to ensure they can protect themselves from cybersecurity incidents.

CAF is not a requirement per se, but it does reflect cybersecurity best practices. And if you experience a cybersecurity incident and you don't follow CAF, you could get fined up to **£17 million,** per the penalties section of the legislation.

In summary, organisations should implement CAF to prove compliance with NIS.

CAF Objectives

- **A** Managing Security Risk
- **B** Protecting Against Cyber Attacks
- **C** Detecting Cyber Security Incidents
- **D** Minimising Impact of Security Incidents

CAF Principles

Governance A1.a A1.b **A1.c**	Service Protection and Policies **B1.a B1.b**	Security Monitoring **C1.a C1.b C1.c C1.d C1.d**	Response and Recovery Planning **D1.a D1.b D1.c**
Risk Management **A2.a A2.b**	Identity and Access Control **B2.a B2.b B2.c B2.d**		
Asset Management **A3.a**	Data Security **B3.a B3.b B3.c B3.d B3.e**	Proactive Security and Event Discovery **C2.a C2.b**	Lessons Learned **D2.a** D2.b
Supply Chain **A4.a**	System Security **B4.a B4.b B4.c B4.d**		
	Resilient Networks and Systems **B5.a** B5.b B5.c		
	Staff Awareness and Training B6.a B6.b		

▲ Varonis applies to the bolded requirements

Source

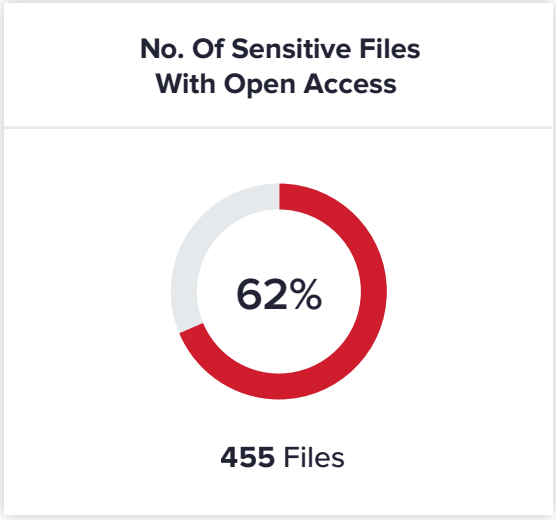
How Varonis Maps to **CAF Objectives**

Varonis is a data security solution that helps organisations protect critical information. Varonis finds critical organisational information across on-prem and cloud data stores automatically and can help you control and limit access to it. We also monitor data access activity in context with Active Directory activity and perimeter telemetry to flag potential threats proactively. **Here's how Varonis can help with various aspects of CAF compliance:**

CAF Objectives

A. Managing Security Risk

Organisations need to understand and identify where critical information and systems could be at risk of cyberattack throughout the network and across the entire supply chain.



How Varonis Helps

Data Protection

Varonis identifies and highlights areas of risk across multiple data stores, on-premise and in the cloud.

Key functionality includes:

- A scalable classification engine that identifies critical information automatically across on-prem and cloud data stores
- Dynamic dashboards and custom reports that show where critical data is overexposed and where the organisation is exposed to other security vulnerabilities
- A bi-directional permissions view that shows who can access critical data and where critical data might be overexposed
- The ability to simulate and commit permissions changes to achieve least privilege with minimal business interruption
- An Automation Engine which can automatically remediate overpermissive folder access

CAF Objectives

B. Protecting Against Cyber Attacks

Organisations need to secure systems that support essential functions by auditing access to those systems and monitoring for suspicious activity that could indicate a cyberattack.

How Varonis Helps

Comprehensive Data Security

Varonis ensures critical information isn't overexposed by eliminating open access and monitoring for potential threats.

Key functionality includes:

- Scheduled entitlement reviews & re-certifications to keep access control limited on an ongoing basis
- Ability to automatically delete, archive, or move files after a certain time period or if the files meet certain criteria
- Actions can be performed ad-hoc or automatically as part of a rule
- Varonis labeling enables data protections like encryption and rule-based transfer limitations
- Discover and remediate misconfigurations in AD to reduce risk of compromise

CAF Objectives

C. Detecting Cyber Security Incidents

Organistations need to implement systems to detect and prevent cyberattacks and data breaches.

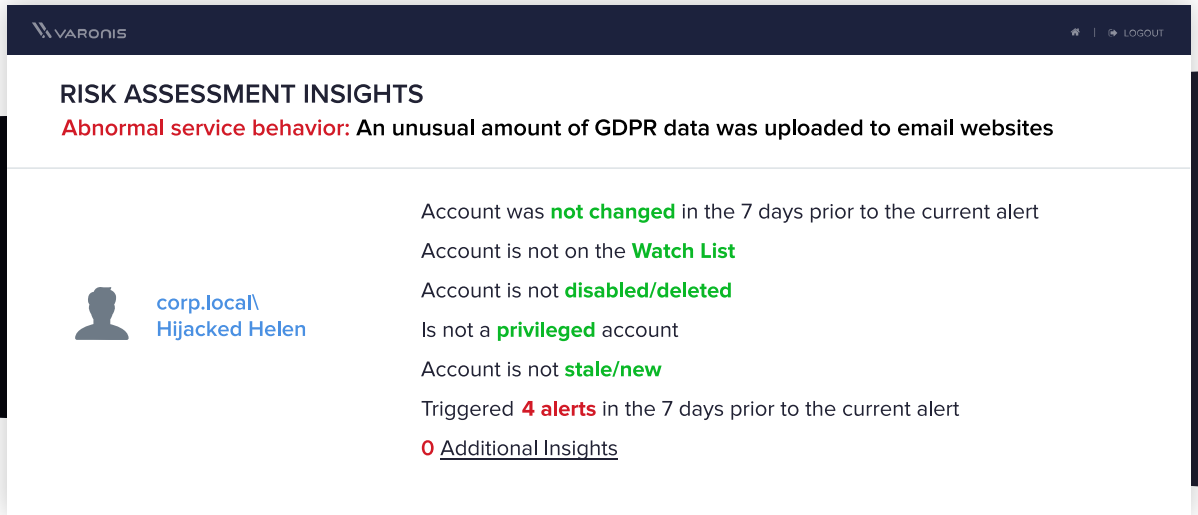
How Varonis Helps

Data-Centric Threat Detection & Response

Varonis monitors user activity from several metadata streams, correlates that information, and compares it to user activity baselines and threat models to detect potential threats to critical data.

Key functionality includes:

- A unified audit trail showing who's been opening, creating, deleting, or modifying important files, sites, Azure Active Directory objects, emails, and more
- Comprehensive alerting flags unauthorised data access, whether it's from a malicious insider or an external threat actor
- High-fidelity alerting on suspicious access activity & policy violations based on behavioral deviations and out-of-the-box threat models
- Context from correlating critical file access activity, Active Directory activity, and DNS, VPN, and proxy telemetry for faster investigations
- Threat models detect abnormal activity related to lateral movement, privilege escalation, and data exfiltration over email, DNS, or file copy



VARONIS

CAF Objectives

D. Minimising Impact of Security Incidents

Organisations need to establish a response and recovery plan in the event of a cyberattack to ensure essential services can withstand and persist.

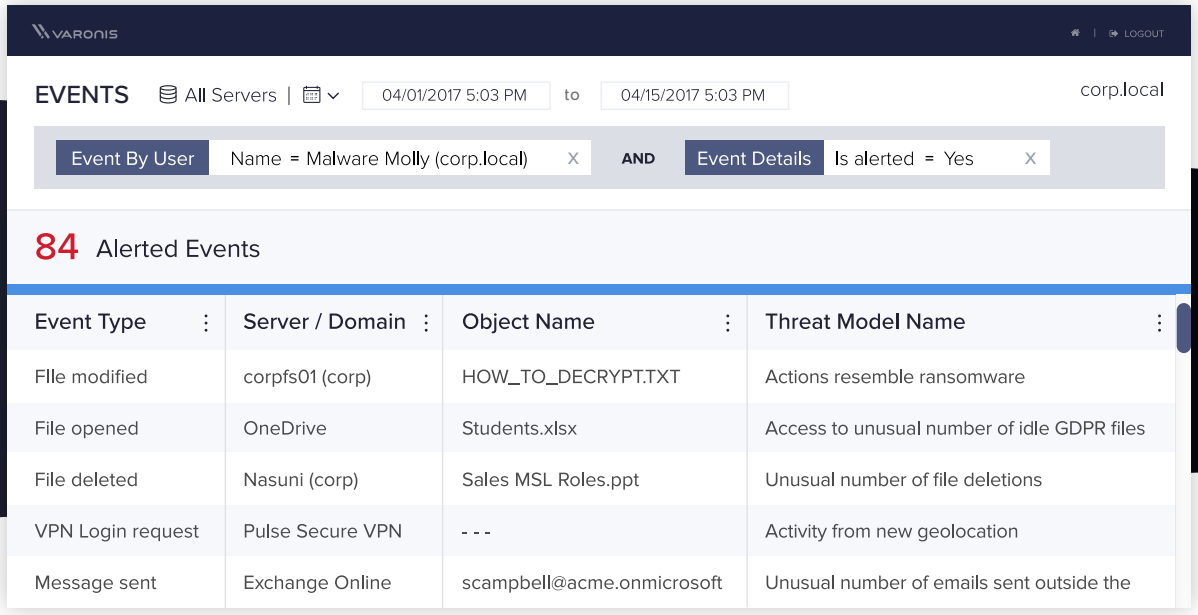
How Varonis Helps

Automated Responses & Expert Help

Varonis can quickly spot and stop malicious behavior, helping you limit potential damage from cyberattacks. Our Incident Response Team will help you investigate any incident, free of charge.

Key functionality includes:

- Automated response capability (e.g., lock accounts, shut down machines) to stop security incidents immediately
- Complimentary incident response team that is available to assist with any incident investigations
- Pre-built and customisable playbooks for efficient Incident Response and Investigation workflows
- Normalised and enriched event logs for user-friendly and efficient investigations between users, devices, data, and platforms



Getting Started with a **Free CAF Data Risk Assessment**

Aligning to CAF is a key first step in complying with NIS Regulations. Varonis can help manage your security risk by identifying where you have sensitive data, reducing the attack surface of that data, and monitoring that data for potential threats. To see where your sensitive data might be exposed and where you have vulnerabilities, sign up for a free risk assessment. Our engineers will do all the heavy lifting—setup, configuration, and analysis—and provide you with a customised report that's yours to keep, obligation-free.

Fast & Hassle-Free

A dedicated engineer will do all the heavy lifting for you: setup, configuration, and analysis. Your time investment is minimal.

Completely Customised

Your security assessment is completely tailored to your needs, regulations, and configurations to deliver insights you can act on.

Invisible and Nonintrusive

Varonis monitors millions of events per day for the biggest enterprises on the planet. We won't slow you or your system down.

VARONIS

Try Varonis free

Set up Varonis in your own environment.
Fast and hassle free.

info.varonis.com/risk-assessment-request

ABOUT VARONIS

Varonis is a pioneer in data security and analytics, fighting a different battle than conventional cybersecurity companies. Varonis focuses on protecting enterprise data on premises and in the cloud: sensitive files and emails; confidential customer, patient and employee data; financial records; strategic and product plans; and other intellectual property.

The Varonis Data Security Platform detects insider threats and cyberattacks by analysing data, account activity and user behaviour; prevents and limits disaster by locking down sensitive and stale data; and efficiently sustains a secure state with automation. With a focus on data security, Varonis serves a variety of use cases including governance, compliance, classification, and threat analytics. Varonis started operations in 2005 and has thousands of customers worldwide — comprised of industry leaders in many sectors including technology, consumer, retail, financial services, healthcare, manufacturing, energy, media, and education.