NOZOMI NETWORKS

COMPLIANCE MAPPING GUIDE

How the Nozomi Networks Platform Supports the UK NCSC Cyber Assessment Framework 4.0

1. Introduction

Introduced in 2018 by the National Cyber Security Centre (NCSC), the **Cyber Assessment Framework** (CAF) is a tool to help Operators of Essential Services (OESs) in the U.K. assess and improve their cybersecurity and resilience by managing cyber risks and protecting essential services from cyber threats. Originally created to help OESs operationalise and measure compliance with the Network Information Systems (NIS) Regulations, today the CAF has broader application with the pending enactment of the Cyber Security and Resilience Bill (CSRB), which puts almost all OT systems firmly in scope as "national resilience" assets and establishes stricter requirements and penalties.

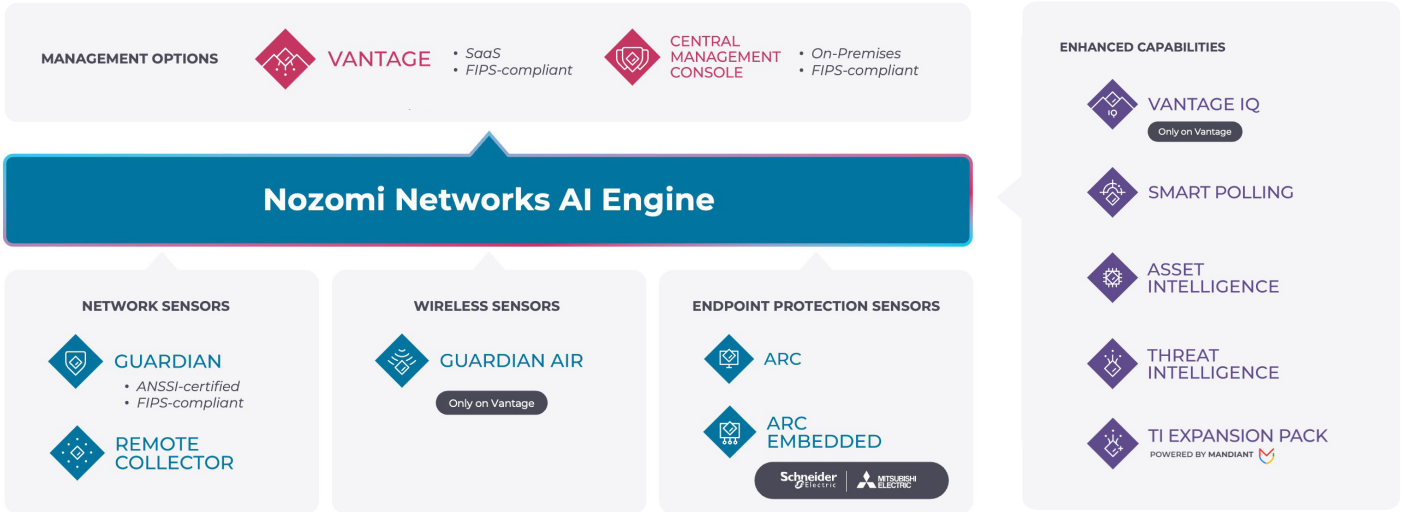
Now in its fourth iteration, the CAF is the definitive reference standard for achieving outcomes-based cyber resilience — and demonstrating compliance with both the NIS Regulations and the CSRB. CAF 4.0 includes four objectives and 14 principles.

Nozomi Networks is the leader in OT/IoT security and visibility. Customers around the globe rely on us to minimise risk and complexity while maximising operational resilience. This guide articulates how our platform maps to the CAF 4.0 objectives and principles and can help you implement effective industrial control system (ICS) cybersecurity policy.

2. Nozomi Networks Platform Overview

Purpose built for complex industrial and critical infrastructure environments, the Nozomi Networks platform combines visibility from the endpoint to the air with continuous monitoring and AI-powered analysis to minimise cyber risk and maximise operational resilience. It helps you:

- **See** all OT, IoT and IT devices on your network and understand their behaviour
- **Detect** and prioritise cyber threats, vulnerabilities and anomalies based on their risk
- **Respond** faster to critical breaches and process control issues with guided remediations



3. How the Nozomi Networks Platform Supports the CAF 4.0

Per the table below, the Nozomi Networks platform supports all four CAF objectives either in full (10 principles) or in part (four principles). For the principles that we support partially, we provide key support for other tools or processes, significantly reducing the overall compliance challenge.

Objective	Principles	Summary	Nozomi Networks Support
A. Managing Security Risk	**A1. Governance**	The organisation has appropriate management policies and processes in place to govern its approach to the security of network and information systems.	PARTIAL
	A2. Risk Management	The organisation takes appropriate steps to identify, assess and understand security risks to the network and information systems supporting the delivery of essential services.	COMPLETE
	A3. Asset Management	Everything required to deliver, maintain or support networks and information systems for essential services is determined and understood.	COMPLETE
	A4. Supply Chain	The organisation understands and manages security risks to networks and information systems supporting the delivery of essential services that arise as a result of dependencies on external suppliers.	PARTIAL
B. Protecting Against Cyberattacks	**B1. Service Protection Policies, Processes and Procedures**	The organisation defines, implements, communicates and enforces appropriate policies and processes that direct its overall approach to securing systems and data that support delivery of essential services.	COMPLETE
	B2. Identity and Access Control	The organisation understands, documents and manages access to network and information systems supporting the operation of essential functions. Users (or automated functions) that can access data or systems are appropriately verified, authenticated and authorised.	PARTIAL
	B3. Data Security	Data stored or transmitted electronically is protected from actions such as unauthorised access, modification, or deletion that may cause disruption to essential services.	COMPLETE
	B4. System Security	Network and information systems and technology critical for the delivery of essential services are protected from cyberattacks. An organisational understanding of risk to essential services informs the use of robust and reliable protective security measures.	COMPLETE
	B5. Resilient Networks and Systems	The organisation builds resilience against cyberattacks and system failure into the design, implementation, operation and management of systems that support the delivery of essential services.	COMPLETE
	B6. Staff Awareness and Training	Staff have appropriate awareness, knowledge and skills to carry out their organisational roles effectively in relation to the security of network and information systems supporting the delivery of essential services.	PARTIAL
C. Detecting Cyber Security Events	**C1. Security Monitoring**	The organisation monitors the security status of network and information systems supporting the operation of essential function(s) in order to detect security events indicative of a security incident.	COMPLETE
	C2. Threat Hunting	The organisation proactively seeks to detect, within networks and information systems, adverse activity affecting, or with the potential to affect, the operation of essential functions even when the activity evades standard security prevent / detect solutions.	COMPLETE

D. Minimising the Impact of Cyber Security Incidents	**D1. Response and Recovery Planning**	There are well-defined and tested incident management processes in place, that aim to ensure continuity of essential services in the event of system or service failure. Mitigation activities designed to contain or limit the impact of compromise are also in place.	**COMPLETE**
	D2. Lesson Learnt	When an incident occurs, steps are taken to understand its root causes and to ensure appropriate remediating action is taken to protect against future incidents.	**COMPLETE**

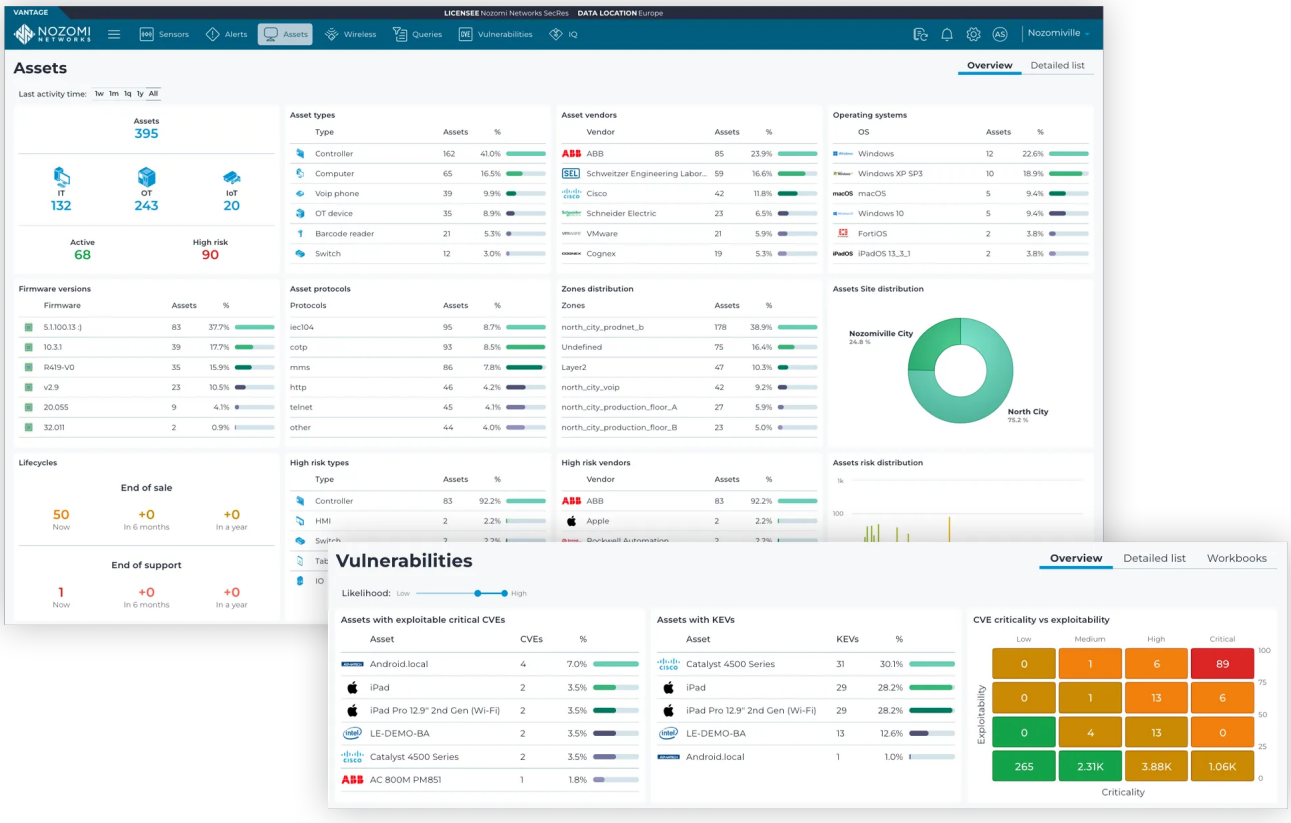
Following are detailed descriptions of how the platform addresses each CAF objective.

3.1. CAF Objective A – Managing Security Risk

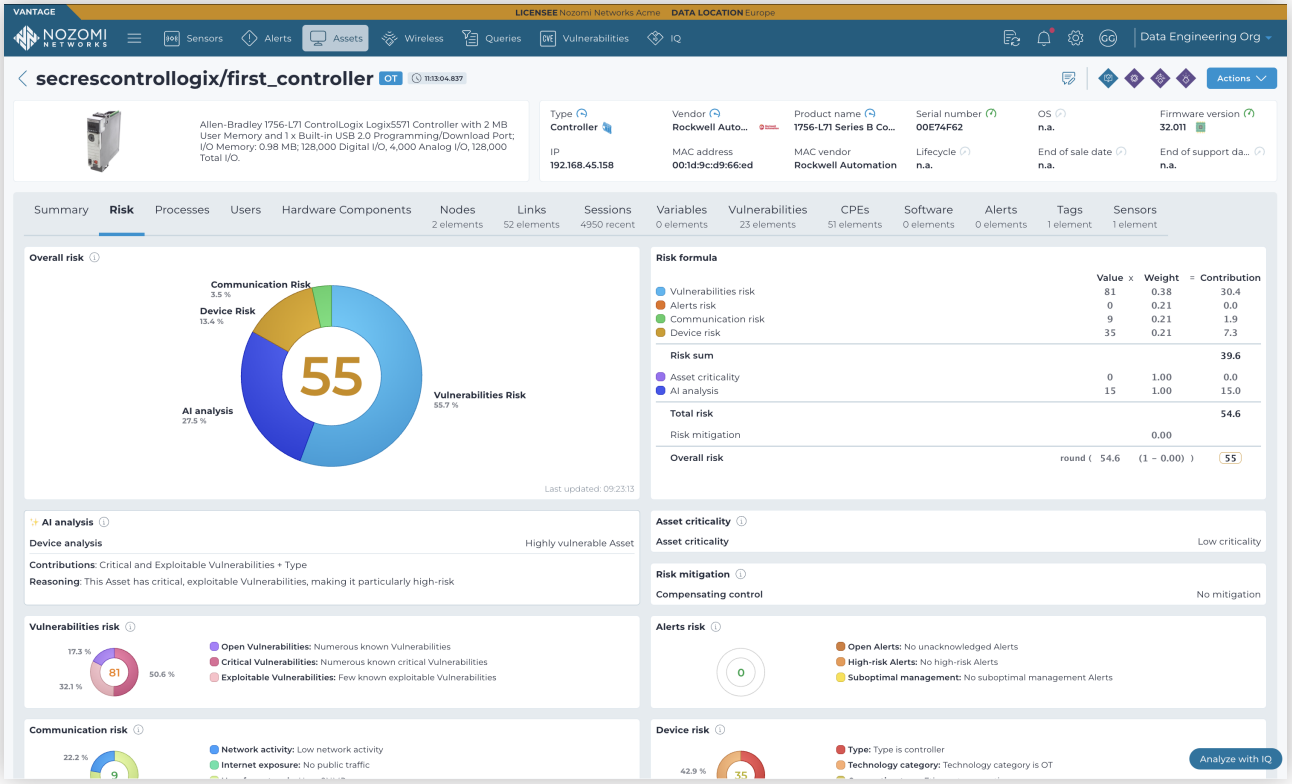
OT/IoT cyber risk is the potential for loss of life, injuries, equipment damage, environmental damage, revenue loss, and operational disruptions caused by the failure, misuse, or cyber compromise of connected OT/IoT systems that support industrial and critical infrastructure operations. Based on the definition alone, it's clear than managing OT/IoT cyber risk requires a different strategy than managing IT cyber risk.

There are four steps to continuous OT/IoT cyber risk management: Risk identification, risk assessment, risk mitigation and risk monitoring. The Nozomi Networks platform simplifies each phase in the cycle, enabling you to detect threats before they can cause harm, mitigate vulnerabilities before they can be exploited and minimise damage should an incident occur.

Risk identification starts with a complete asset inventory and visibility achieved through a variety of wire, wireless and endpoint sensors, active and passive discovery techniques, protocol fluency and third-party connectors to enhance asset profiles. Vulnerability identification is a critical component. Industrial networks can contain hundreds or even thousands of OT and IoT devices from a variety of vendors, many of which are insecure by design — lacking authentication, encryption and other security. Some assets have can only be patched during narrow maintenance windows, and others can't be patched at all. Vulnerabilities must be prioritised based on criticality and exploitability, including CVSS, EPSS and KEV scores, to ensure SOC teams focus on what matters most.

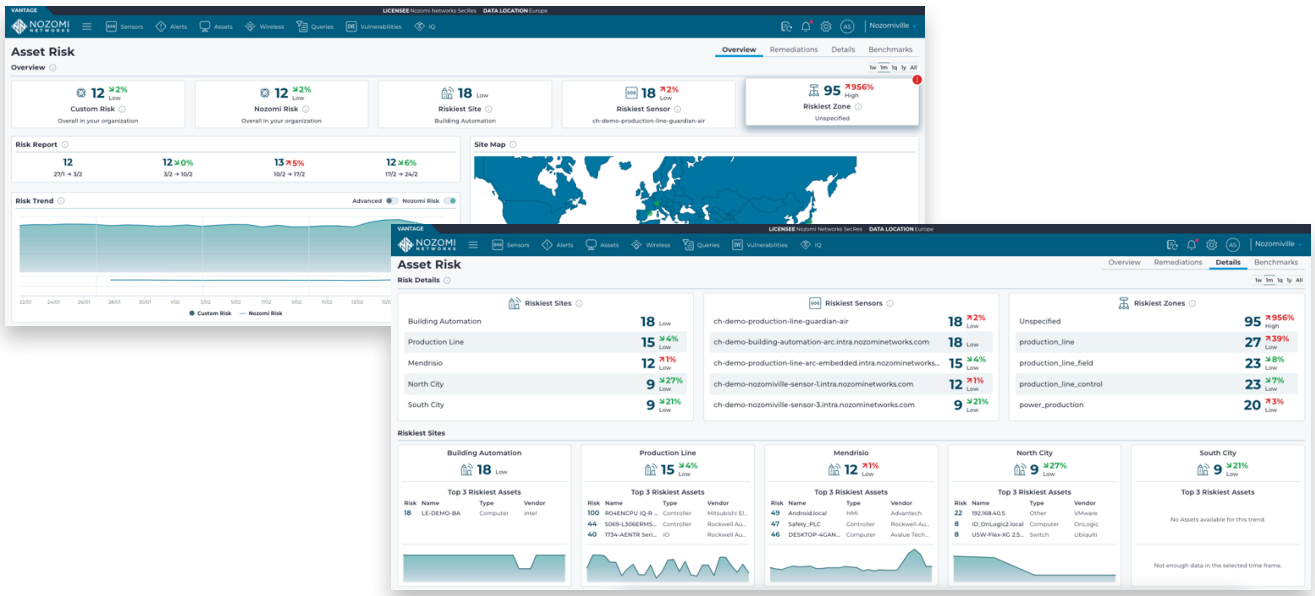


Risk assessment for OT and IoT environments must factor in not just vulnerabilities but also asset criticality, device risk, communication risk, alert risk and compensating controls. The Nozomi Networks platform assigns risk scores to each asset based on these five factors. You can use these scores out of the box or customise the weight of each variable until the calculation accurately reflects how your organisation assigns risk. Teams can use these scores to prioritise security efforts, address the most critical risks first and take the correct actions to mitigate potential threats effectively.



Risk mitigation requires collaboration between security and operations leaders who may have different priorities. The Nozomi Networks platform leverages AI to surface key risk reduction steps that these two teams can agree will have the biggest impact. They include specific recommended actions such as patching software, fixing communication gaps and updating hardware, prioritised based on their potential to reduce risk.

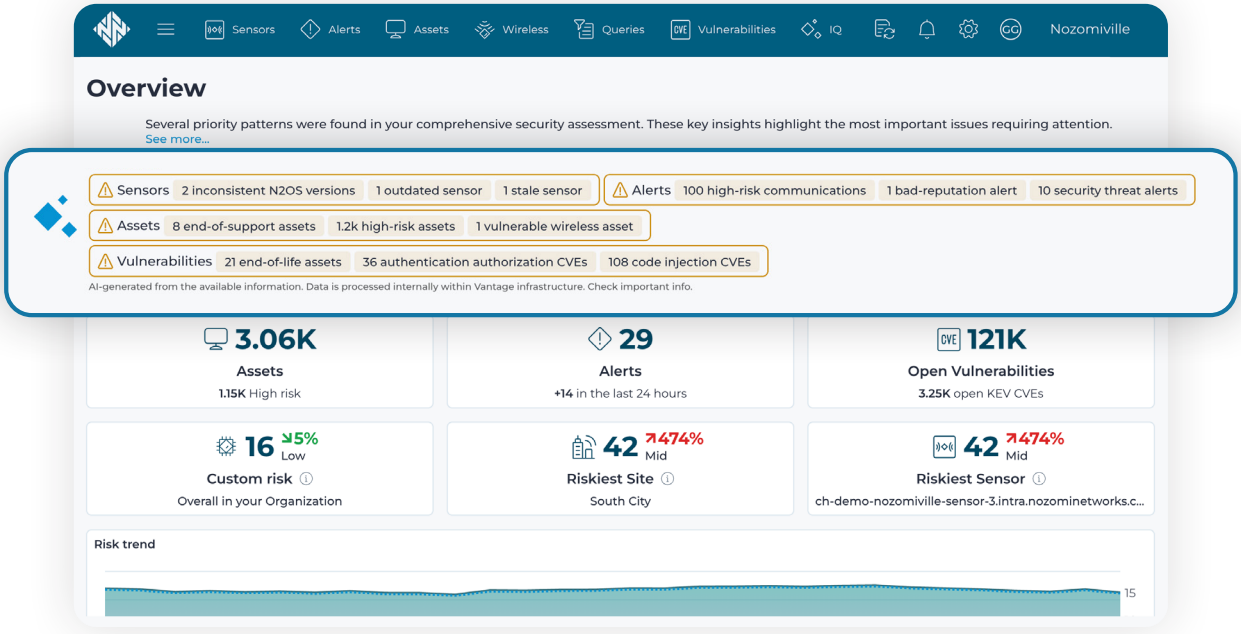
Risk monitoring, when based on accurate asset risk scores, enables you to track risk reduction over time at the asset, sensor, zone, site and enterprise level. The Nozomi Network platform features dashboards that show see at-a-glance what assets are riskiest by zone, site, vendor and other categories, and how individual risk scores contribute to higher-level scores. If your risk is trending in the wrong direction, you can drill down to see why and where you need to add controls. As you do, your risk score will change to reflect the impact your actions, providing evidence to justify resources and demonstrate ROI. You can even benchmark your risk levels and trends against Nozomi Networks customers in the same industry or region.



3.2. CAF Objective B - Protecting Against Cyber Attacks

By monitoring network traffic across wired, wireless and endpoint-connected OT/IoT assets, the Nozomi Networks platform discovers every device, identifies communication pathways and validates that network segmentation is operating as intended. DPI and protocol analysis confirm that only approved communications occur between in-scope assets and that those communications align with defined security policies. Unauthorised connections (such as covert wireless links, rogue access points or bypass routes around controlled boundaries) are identified and flagged for remediation.

The platform detects the use of insecure protocols, validating proper use of secure communication methods and alerting on deviations from established baselines. Continuous monitoring, asset profiling and cross-domain correlation provide real-time assurance that systems and communications remain within compliance parameters. This enables you to prove, with time-stamped and context-rich evidence, that protective measures for your OT/IoT environment are not only in place and functioning but actively reducing risk in your environment.



The platform's network mapping and visualisation capabilities support good network design; for example, leveraging information on how traffic flows in an existing network. Virtual segmentation can be used to develop an appropriate segmentation strategy that is both achievable and maintainable. This approach to virtual segmentation can enforce traffic flow, or provide alerts against policy breaches, providing an additional level of security in line with a defence-in-depth approach to security.

Network mapping also aligns with the CAF with respect to data storage and system dependency mapping. With this information, an organisation can better understand the impact of corruption or loss of availability of this data, enabling a focused and risk-based approach to the protection of critical services. Incident response processes can also be better informed and enabled to rapidly restore essential services following disruption.

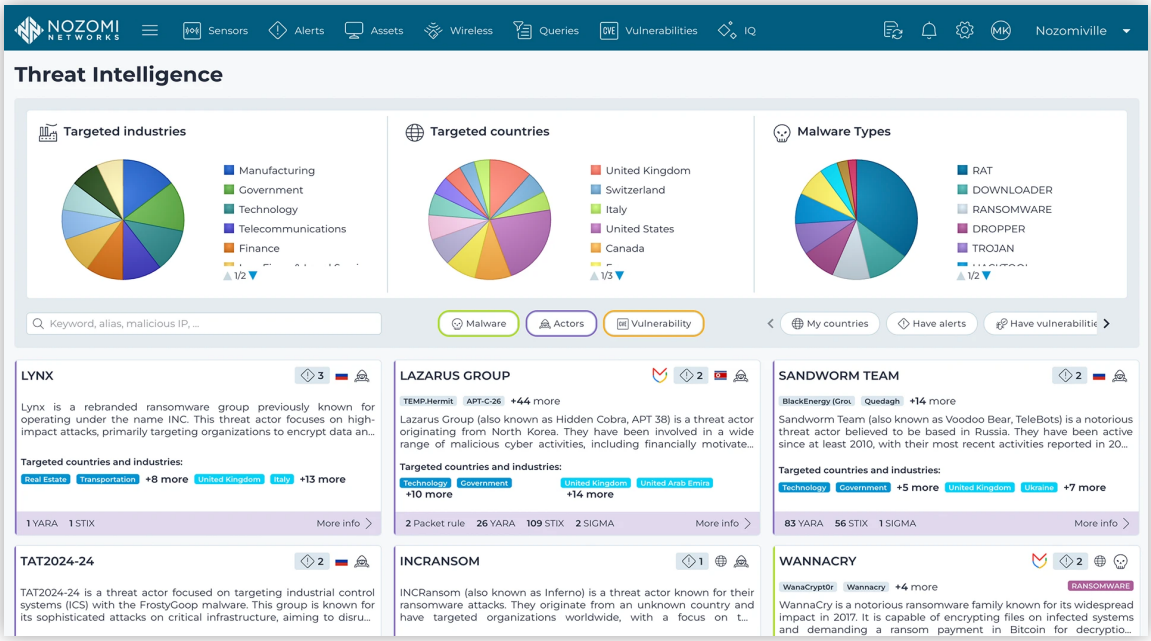
Our platform provides detailed information across all aspects of an industrial network, logging granular details about each asset, its activity and traffic patterns, amounts of transferred data, protocols and function codes, source and destination ports, connection attempts, software and firmware versions and updates in real time. Detailed information on network traffic flow and dependencies and packet traces can also be downloaded from appliances and made available to security and forensics teams for in-depth packet level analysis.

3.3. CAF Objective C – Detecting Cyber Security Events

The Nozomi Networks platform continuously monitors the operational environment to detect vulnerabilities, configuration weaknesses, malware indicators and anomalous behaviour across OT, IoT and connected systems. AI-enriched asset profiles provide real-time awareness of system flaws and known vulnerabilities. Our OT/IoT-focused threat intelligence feed helps ensure sensors can detect emerging malware and IOCs, while multi-factor risk scoring prioritises remediation efforts based on threat exposure and operational criticality. Threat intelligence, anomaly detection and behavioural analytics work together to identify potential compromises early, including sophisticated or low-and-slow attacks that could bypass traditional defences.

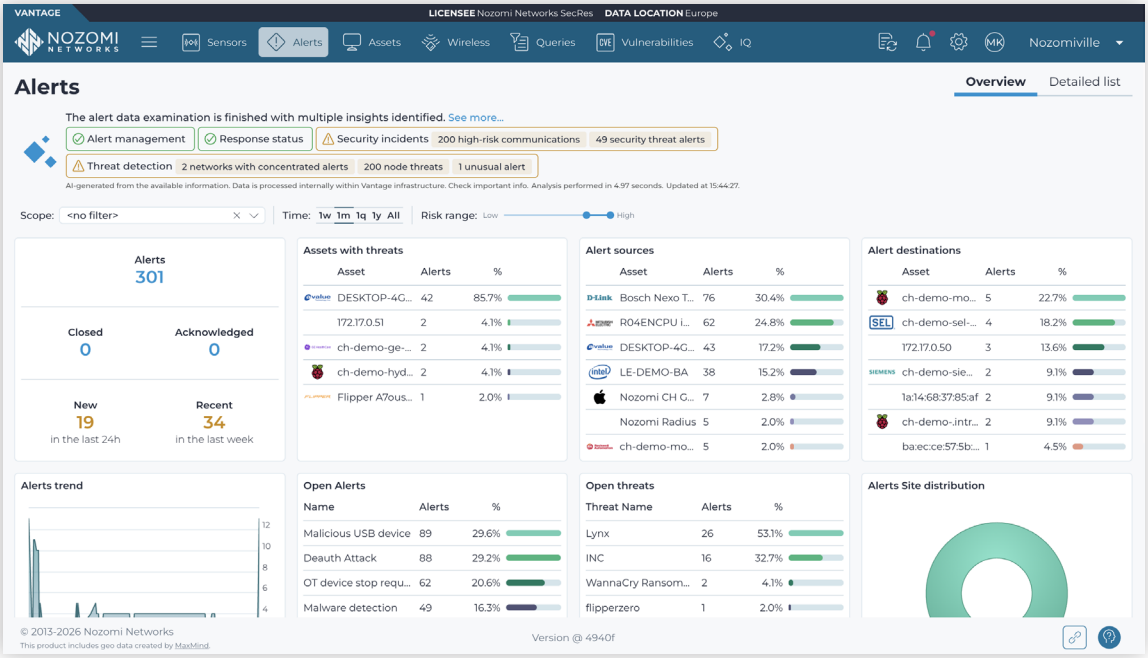
By correlating events from wired, wireless and endpoint monitoring, the platform accelerates detection, investigation and response to integrity violations. Configurable alerting ensures that deviations from baselines above established thresholds are reported immediately, while historical logging supports root-cause analysis and incident reconstruction.

More than just a raw IOC feed, our OT/IoT threat intelligence is tightly woven into the platform to enrich asset and network data and enable better detection of anomalies, malicious behaviour and threats. Information is distilled into At-a-Glance threat cards, with details on threat actors and associated exploits, malware, vulnerabilities and MITRE ATT&CK® TTPs, along with mitigation suggestions and links to external references. An optional expansion pack integrates relevant Mandiant IOCs and TTPs into the same feed to include IT-borne threats that can move into OT.



3.4. CAF Objective D – Minimising the Impact of Cyber Security Incidents

The Nozomi Networks platform reduces forensic efforts and speeds response time. Its advanced wired, wireless and endpoint monitoring identifies security and reliability risks and generates detailed, accurate alerts. Each alert describes what happened, provides possible causes and recommends actions to take, reducing investigative efforts.

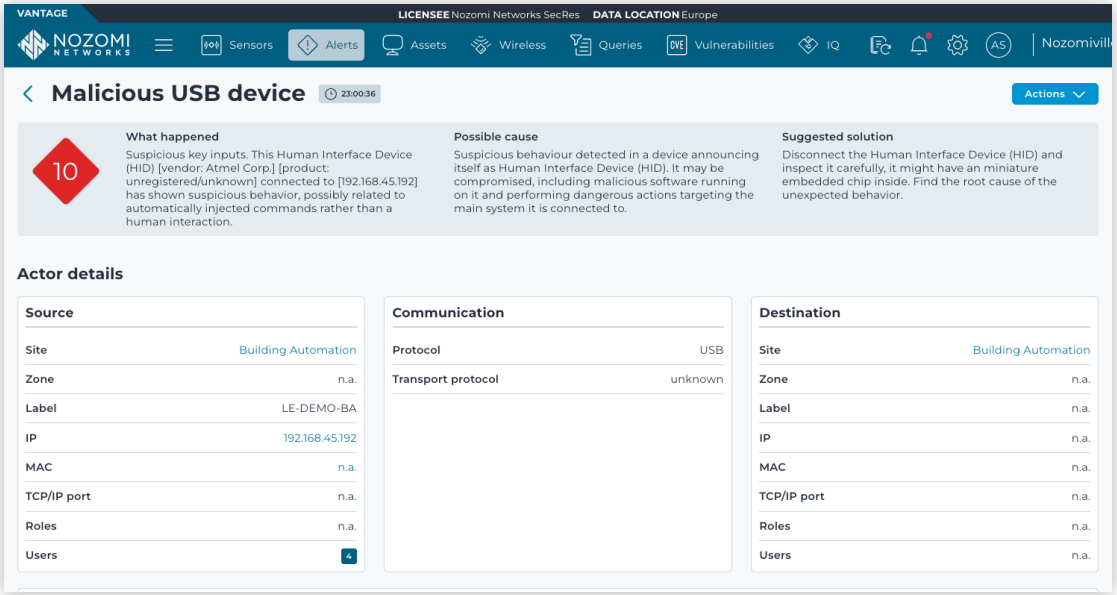


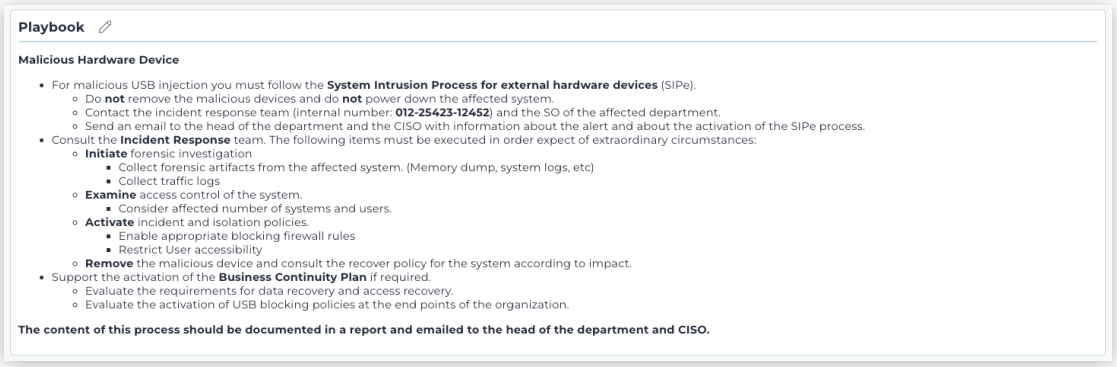
When further analysis is needed, additional tools are available:

- **Incident view of grouped alerts:** Across the platform, alerts are grouped into Incidents that are related in time, asset or cause into a single view. When an operator sees that a critical incident is underway, via an alert they can examine the PCAP related to the alert and download it. With one click they can also access a diff report to compare times before and after the alert. Once changed parameters are identified, staff can take action to stop or mitigate an attack.
- **Time machine forensic tool:** Diff reports are an aspect of the platform's time machine feature, which takes snapshots of the system at periodic intervals so it can be explored and investigated at many moments in time. Also available as graphical views, the snapshots allow investigators to replay network events around an incident to pinpoint when a device was connected or why one stopped communicating. This is invaluable for isolating the root cause and visualising the impact, which helps reduce mean time to repair.
- **AI-powered analysis:** Vantage IQ is Nozomi Networks' AI-powered analysis and response engine. It accelerates incident response in five key ways:
    - **Alert correlation and prioritisation:** Vantage IQ's Insights Dashboard automatically correlates numerous alerts into unified incidents, prioritising them based on risk and providing root-cause context. This enables IR teams to focus on the most critical issues without getting overwhelmed by noise.
    - **Root cause analysis:** Deep neural networks analyse network behaviour patterns to support efficient root-cause identification.
    - **Natural language queries:** Users can pose queries in plain language, such as "What are my high-risk vulnerabilities?" or "Which assets are most exposed?" They gain quick situational awareness that would otherwise require hours or days.
    - **Predictive monitoring:** Vantage IQ applies machine learning to detect deviations from baseline network behaviour. By alerting on unusual bandwidth and activity patterns, it can flag issues before they escalate into full-blown incidents.
    - **Guided remediation:** Vantage IQ suggests actionable remediation steps. It can also highlight suboptimal sensor placements and recommend adjustments to enhance visibility, improving incident readiness and response accuracy.

Given the premium placed on physical safety and continuous operation, incident response in industrial environments can't always be automated. The Nozomi Networks platform offers a combination of manual and automated approaches to use where appropriate. Out-of-the-box integrations and OpenAPI support powers automated responses through your existing tech stack, including SIEMS, SOARs, firewalls, endpoint agents, NACs, SDNs, ticketing systems, secure remote access and more.

Customisable playbooks guide users through detailed actions to follow when an associated alert is triggered.





For automated threat prevention on OT endpoints, the Nozomi Arc sensor can be set to not only detect threats such as malware and malicious software but to automatically quarantine or delete the malicious files altogether. Regardless of what protection mode you choose, Arc accelerates forensics by correlating suspicious user activity with specific devices.

Without endpoint security, there's no way to know who's plugging in when and what they're doing until their commands have been executed on the network.

5. Conclusion

Navigating regulatory change to ensure ongoing compliance with evolving standards can seem overwhelming. With the CAF poised to underpin not only the NIS Regulations but the CSRB, an expanded definition of “national resilience” asset owners must now maintain a defensible, continuously updated asset inventory that supports risk assessment, vulnerability management and incident response. You must also maintain logging, alerts and monitoring functions designed for industrial environments, not just IT. This includes ensuring SOC staff or service partners have OT-specific security skills. Finally, you must have proactive threat intelligence that keeps you informed about malicious threats that could impact your operations.

Nozomi Networks is the leader in OT/IoT security and visibility. With deployments across energy, manufacturing, transportation, building management and critical national infrastructure, we’re already helping UK OT asset owners strengthen resilience and stay ahead of emerging regulatory requirements. Our technical and regulatory experts are ready to help you strengthen your OT and IoT security posture in ways directly aligned with CAF requirements.

Let's get started

For more details on specific product support and deployment options, please reach out to your local Nozomi Networks sales teams or Nozomi Networks partner network.

Contact Us

nozominetworks.com/contact

Nozomi Networks protects the world’s critical infrastructure from cyber threats. Our platform uniquely combines network and endpoint visibility, threat detection, and AI-powered analysis for faster, more effective incident response. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com