



SOLUTION BRIEF

Securing Critical Infrastructure in Federal Government

Federal agencies need to achieve their missions while ensuring service continuity and combat-readiness -- all while facing escalating cyber threats. The recent U.S. White House Executive Order, with its expedited schedule for improving cyber defenses, signals the urgency of confronting the growing cybersecurity challenge.

There is a need to advance cyber visibility, detection and monitoring capabilities, especially for the automation and industrial control systems that deliver critical services and capabilities.

Critical infrastructure (CI) networks include OT (operational technology) and IoT (Internet of Things) assets, both of which have very different characteristics, communications and behaviors from IT assets. Securing these networks requires tools designed to meet their unique needs – and ensure availability.

The Nozomi Networks solution is specially designed for critical infrastructure and today secures the world's largest commercial organizations. It also protects critical civilian and military control networks with network and asset visibility, threat detection, and monitoring for continuous diagnostics and mitigation (CDM).

The First Step to Protecting Your Networks is Knowing What You Have

“ The level of trust we have in our systems has to be directly proportional to the visibility we have. And the level of visibility has to match the consequences of the failure of those systems.

If you can't see a network, you can't defend a network, and if you can't see a network quickly, you certainly don't have a prayer of defending the network. And that applies to both IT and OT.

Anne Neuberger, U.S. Deputy National Security Advisor for Cyber and Emerging Technology

You Can't Protect What You Can't See

See and Secure Critical Infrastructure Systems

Government agencies use automation systems to keep everything from bases to commissaries to aircraft carriers functioning properly.

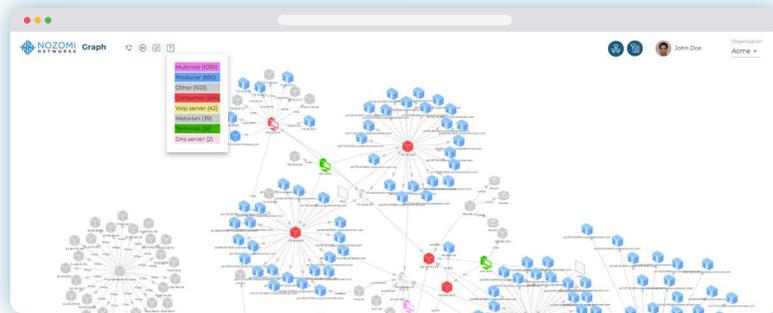
The complex and often aging technology environments make consolidated OT/IoT visibility difficult.

To keep things running smoothly, agencies need a simple way to see and inventory assets and networks.

The Nozomi Networks solution automates asset identification and inventory and provides real-time network visualization. Benefits include:

- Comprehensive visibility into critical infrastructure networks and systems
- Network-wide situational awareness
- Better oversight of vulnerabilities and risks to reliability
- Faster troubleshooting of system changes and issues

Immediately Visualize Your Networks



Quickly Detect and Disrupt Threats

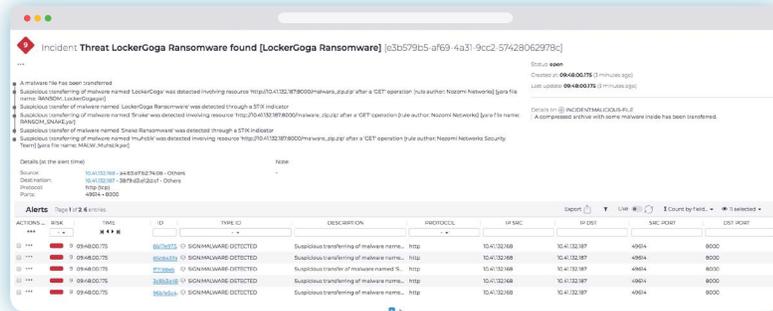
Recent cybersecurity incidents such as SolarWinds, Microsoft Exchange and Colonial Pipeline are a harsh reminder that U.S. public entities face malicious threats from nation-states and cyber criminals.

To improve the detection of cybersecurity incidents on federal government networks, up-to-the-minute threat detection is needed.

The Nozomi Networks solution uses innovative and advanced technology to detect cyber threats, vulnerabilities, risks and anomalies. It results in:

- Fast threat and anomaly detection
- Proactive identification of unauthorized activity
- Accelerated incident response by security staff
- Rapid threat containment and remediation

Rapidly Identify Malware and Hasten Incident Response



Respond Quickly with Continuous Monitoring

Efficiently Manage the Threat of Cyber Vulnerabilities

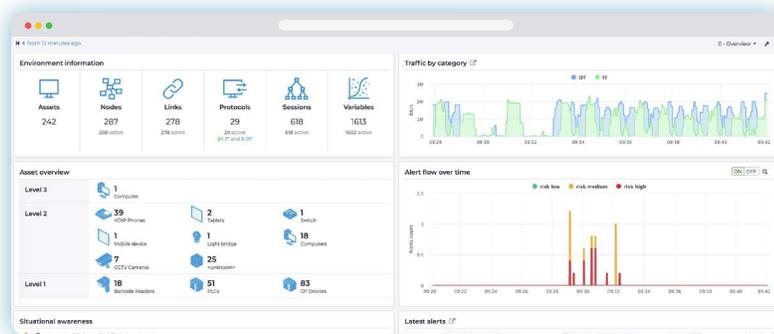
Government networks are rapidly evolving to meet today's missions and citizen demands. Automated systems that have been in service for years include disparate legacy technologies. Now, they are being updated to include IoT devices and are increasingly connected to other systems.

The result is an increased attack surface, leaving agencies vulnerable to sophisticated cyberattacks.

The Nozomi Networks solution constantly monitors heterogeneous OT, IoT and IT environments. It continually analyzes network traffic and communications and results in:

- Network-wide situational awareness
- Better oversight of vulnerabilities and risks
- Higher operational reliability
- Improved investigative and remediation capabilities
- Robust and consistent logging

Effectively Monitor Mixed Environments



Cyber Defense Initiatives with U.S. Federal Agencies



DOD entity

Nozomi Networks innovations are being tapped to help solve national security problems.



Federal agency for threat assessments

The Nozomi Networks solution is used by Peregrine for critical asset cybersecurity assessments.



U.S.-based Army Installation

The Nozomi Networks Solution is deployed for building automation cybersecurity.



MOSAICS

The Nozomi Networks solution is part of the reference architecture for OT/IoT sensor technology.



Project Spectrum

The Nozomi Networks solution is part of a packaged product designed to help companies comply with the CMMC.



The Nozomi Networks solution helps organizations efficiently achieve and maintain compliance.

Contract Vehicles and Resellers

Authorized Resellers and Distributors

The Nozomi Networks solution is available through authorized Resellers and Distributors on the following contracts and purchasing Schedules:

- **GSA** – available through Exclusive Networks
- **NASA SEWP** – available through Carahsoft
- **ITES** – availability is in process

Nozomi Networks works with the following organizations on U.S. federal agency projects:

 **accenture**

carahsoft.

Deloitte.

 **EXCLUSIVE NETWORKS**

 **Goldbelt**

Honeywell

 **IMPRES**

 **NETCENTRICS**

 **Peregrine**
TECHNICAL SOLUTIONS
A subsidiary of Goldbelt, Inc.

Certifications



ISO 27001: 2013 Certified

Nozomi Networks' information security management systems are certified to manage and reduce identified risks to an acceptable level.



SOC 2 Type 1 & 2 Certification

Nozomi Networks has certified the Vantage SaaS platform for SOC 2 Type 1 & 2.

NIST

FIPS 140-2 Compliant

The Nozomi Networks cryptographic modules are fully compliant with the FIPS 140-2 specifications from NIST.

Nozomi Networks

The Leading Solution for OT and IoT Security and Visibility

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.