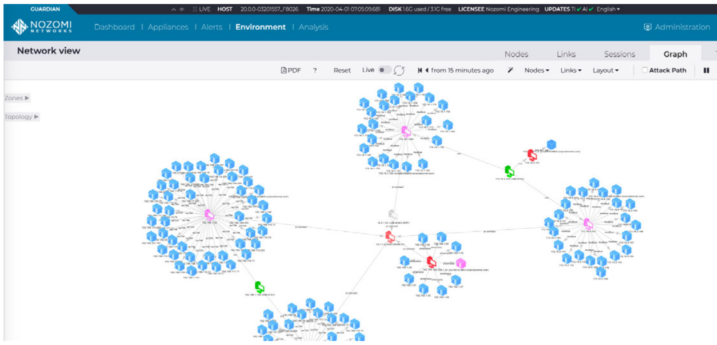
Securing Critical Infrastructure in Federal Government

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 must 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*



Immediately Visualize Your Networks

Challenge: You Can't Protect What You Can't See

US Government agencies use automation systems to keep everything from bases to agency buildings 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.

Recent cybersecurity incidents such as SolarWinds, the Oldsmar, Florida water supply hack, Microsoft Exchange, and Colonial Pipeline are stark reminders that U.S. public entities face real and malicious threats from nation-states and cyber criminals. Up-to-the-minute threat detection is needed on all federal government networks to improve the detection of cyber threats and incidents.

Government networks are rapidly evolving to meet today's missions, as well as 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.

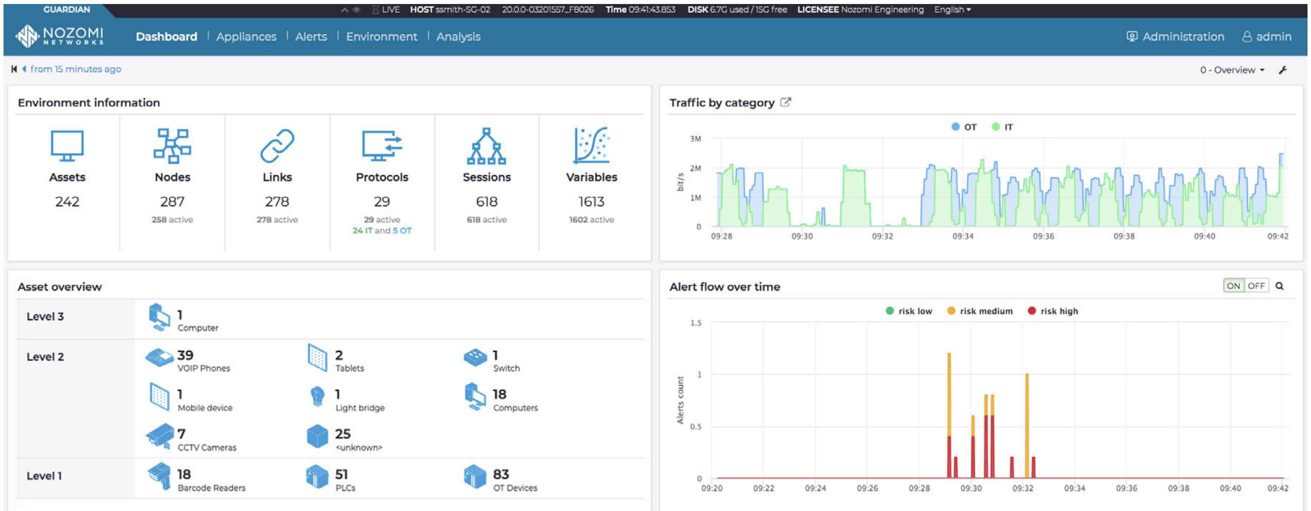
The result is an increased attack surface, leaving all these government networks and devices vulnerable to cyberattacks. There is a need to advance cyber visibility, detection, and monitoring capabilities, especially for the automation and industrial control systems that deliver critical services and 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.

Solution: Immediately See and Secure Critical Infrastructure

The Nozomi Networks solution automates asset identification and inventory and provides real-time network visualization. With innovative advanced technology to detect cyber threats, vulnerabilities, risks and anomalies, you can proactively identify unauthorized activity and accelerate incident response by security staff.

With the constant monitoring of heterogenous OT, IoT and IT environments through analysis of network traffic and communications, rapid threat containment and remediation becomes a reality. Network-wide situational awareness and better operational reliability is acheivable, and when integrated with rest of the CSOI infrastructure, it provides improved investigative and immediate notification and remediation capabilities within your diverse environments.



Environment information

Assets	Nodes	Links	Protocols	Sessions	Variables
242	287	278	29	618	1613
	258 active	278 active	29 active 24 IT and 5 OT	618 active	1602 active

Asset overview

Level 3	1 Computer		
Level 2	39 VOIP Phones	2 Tablets	1 Switch
	1 Mobile device	1 Light bridge	18 Computers
	7 CCTV Cameras	25 <unknown>	
Level 1	18 Barcode Readers	51 PLCs	83 OT Devices

Effectively Monitor Mixed Environments

Customer Success: Operational Visibility into More Than 400 Field Sites

Midstream oil and gas companies operate within complex environments. Their industrial control systems (ICS) include dozens of equipment types and cover vast distances. This makes it challenging to monitor, manage and secure pipeline systems that aren't thoroughly documented or easy to visualize. Covering over 9000 kilometers of pipeline and 420 gas distribution sites for natural gas transportation, storage and distribution can be unbearable.

There became a need for real-time monitoring of distribution stations spread across the country. This also required integration with a managed service provider's control center technology, and fast implementation of communications link monitoring capabilities. Prior to field deployment, testing needed to prove that the operational visibility solution could meet use case requirements within a lab environment. Lastly, MSP systems were integrated to monitor communications link service levels.

Completion of the successful PoC led to the purchase of over 420 Nozomi Networks R50 sensors for deployment at gas wells, tie points and compressor stations. The MSP/TSP also bought two Nozomi Networks Central Management Consoles™ (CMCs) to deliver consolidated and remote access to the ICS data from Guardian sensors deployed in the field.

The MSP/TSP now uses Nozomi Networks Guardian sensors and CMCs to measure and document the availability of its communications links. It shares monthly reports with the natural gas distributor to confirm it is meeting the agreed upon service levels.

Let's start a conversation

1-800-652-9686

isg@imprestechnology.com
imprestechnology.com