NOZOMI NETWORKS

INDUSTRY BRIEF

Mining: Securing Operational Resilience Through OT and IoT Visibility and Security

Table of Contents

1. Introduction

Securing Operational Resilience for Mine Operators Through OT and IoT Visibility and Security

Mining companies are working diligently to maintain competitiveness and profitability in a challenging business environment. Declining commodity prices and limited untapped natural resources are forcing them to improve operational efficiency.

As mine operators begin to integrate enterprise-wide systems in order to gain efficiencies, cybersecurity risks are increasing. To combat this, mines must implement real-time visibility and cybersecurity solutions designed to reduce risk and build operational resilience.

On their path to operational efficiency, mining companies have embraced digitization, automation and the Industrial Internet of Things (IIoT). But the integration of operational systems with broader business systems has highlighted operational technology's (OT's) visibility challenges and increased exposure to cyber threats. Protecting profits, personnel and intellectual property (IP) despite insecure legacy systems requires a delicate balance.

Fortunately, the mining industry has evaded the large-scale cyberattacks experienced in the critical infrastructure sector. Even so, a 2019 Ernst & Young survey reported that 54% of mining and metals companies have suffered a significant cybersecurity incident in the last year.[1]

Mine operators need to ensure they can detect and contain cyber threats and incidents, regardless of the cause, before they disrupt production, compromise the safety of personnel and equipment, or cause a loss of IP. This includes combatting internal mistakes or deliberate attacks from foreign governments, hackers, third-party vendors or activists.

While mining leaders have often been late adopters of cybersecurity best practices, they are now beginning to recognize the gravity of potential cyber threats and are working to build resilience. In 2017, a group of Canadian mining companies formed the Mining and Metals Information Sharing Analysis Center to protect members against cyber incidents.[2] Other countries are putting data protection regulations in place, and global cybersecurity researchers are also collaborating with industry and institutions to defend industrial systems against cyber risk.

THE ROAD TO OPERATIONAL RESILIENCE

Read this paper to learn how a unified OT and IoT monitoring and threat detection solution can be used to **achieve operational availability, visibility and security.**

To stay ahead of looming regulations and thrive during market volatility, mining operators need to take proactive steps to protect their operations. Fortunately, technology such as the Nozomi Networks real-time visibility and cybersecurity solution can be used to build operational resilience quickly and easily.

2. Top Mining Industry Challenges

As mine operators adopt intelligent mining practices, they face challenges that, if not properly addressed, leave them exposed to significant business risks.

2.1 Defending an Expanding Threat Surface

To improve profitability and decrease costs, mining companies are incorporating new IIoT applications into their operational environment. These applications use processors and sensors to collect and share data wirelessly. However, they also create interconnectivity between legacy OT and IoT systems and the corporate IT system – a change that increases the mine's vulnerability to cyberattacks across the entire network.

Legacy OT and IoT systems weren't originally designed to be networked. Often, they lack basic security standards, such as firewalls, user restrictions or authentication mechanisms. These gaps in security expose mining companies to enterprise-wide cyber risk from external and internal origins, including threat actors with economic or political motivations.

In the 2016 data breach of a Canadian mining company, hackers went undetected in the organization's internal network for months, accessing 15 GB of personal and customer data in the process.[3] Although it is one of the world's largest gold mining producers, the organization didn't have a system in place to successfully monitor for possible breaches.

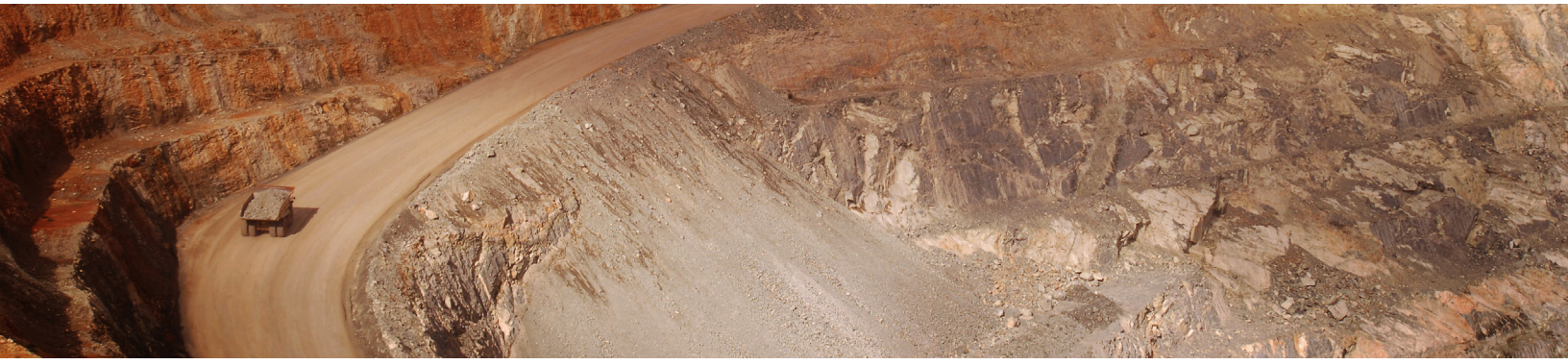
Yet not all cyber threats are intentional. From weak passwords to malware-infected personal devices and accidental misconfigurations, even employees who mean no harm can expose a vulnerable network to threats.

BEING PROACTIVE IS A BEST PRACTICE

Digitization of legacy OT and IoT assets is creating interconnectivity between a mine's IT and OT systems – increasing its vulnerability to cyberattacks. Mine operators must take steps to mitigate this exposure, by implementing

security processes designed specifically to protect the OT and IoT environment.

Defending this expanded threat surface requires advanced security solutions capable of providing complete operational visibility and threat detection – and ones specifically tailored to defend the OT and IoT environment.



2.2 Reducing Unplanned Downtime and Resulting Losses

With commodity prices in flux and natural deposits in decline, mine operations are striving to achieve profitability through operational efficiencies. A common – yet costly – obstacle to productivity is unplanned downtime and the resulting losses.

Caterpillar, the construction machinery and equipment company, estimates that "the total cost of unscheduled downtime in mining can be as much as 15 times that of a scheduled event." [4]

Even successful operations can be sidetracked by equipment breakdown and failure. And with many production processes relying on automation, a malfunction in a single device can have repercussions across the entire system.

Unplanned downtime happens for a variety of reasons, from undetected equipment wear-and-tear to sophisticated cyberattacks. Monitoring the state of all equipment in a mine in real-time is challenging. Typically, operators conduct monthly assessments on production system operations. But this cadence doesn't allow staff to spot problems as they develop over time, or react to invisible changes in behavior.

These equipment review processes also don't adequately address the growing threat of malware designed to bring OT systems to a halt. While most large-scale cyberattacks have targeted IT systems, mine operations are a growing target.

In fact, in March 2019, one of the largest aluminum producers in the world experienced a crippling cyberattack. The attack paralyzed the company's computer networks, forcing it to isolate plants and switch some mining operations to manual. Altogether, the attack is reported to have cost the company up to $70 million.[5]

THE COST OF UNSCHEDULED DOWNTIME

Anticipating equipment wear-and-tear, and preventing unplanned downtime, is critical.

One estimate puts the total cost of unscheduled downtime in mining at 15 times that of a scheduled event.[4]

THE HIGH COST OF A CYBER INCIDENT

COMPANY

Norsk Hydro

CYBER INCIDENT

Ransomware: LockerGoga

IMPACT

- **Forced to switch to manual operations and workarounds**
- **Product output of one business unit reduced by 50%**
- **Reporting, billing, invoicing and other systems delayed**
- **Lost margins and low production volumes**

COST

$70M

2.3 Protecting IP and Business Assets from Corporate Espionage and Activists

Mining companies are a treasure trove of intelligence: geological exploration research containing data on the location and value of natural deposits, pricing information, and proprietary extraction and processing technology, to name a few.

Corporate interest groups and nation states have both been known to engage in cyber espionage to access this type of data to gain long-term competitive advantage. For example, insight into mine value and pricing could be leveraged in M&A negotiations to lower the price of the acquisition target or outbid a competitor in a sales contract.

IP assets are another attractive target for cyber crime. Access to proprietary production and processing methods and mining equipment design can be used to cut R&D costs and gain access to lucrative market segments.

In 2015, for example, an Australian mining technology manufacturer disclosed that it took a heavy hit from Chinese cyber hackers; they had stolen the design of its metal detector and flooded the market with cheap counterfeit devices. The company had to slash the price of its detector by almost half to compete and lost nearly 80% of its profit in one year.[6]

In addition, due to the nature of their operations, mining companies have been scrutinized for their impact on the environment. Hacktivists, with an interest in exposing alleged environmental damage to natural habitats and drawing public attention to their causes, also present an added cybersecurity threat.

CYBER THREATS TARGET CORPORATE DATA

Corporate interest groups and nation states are targeting mining companies to gain access to sensitive corporate data.

Such insights can be leveraged in M&A negotiations, R&D and other business situations to gain competitive advantage or disrupt operations.

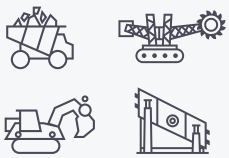
3. The Nozomi Networks Solution

3.1 How the Nozomi Networks Solution Improves Operational Resilience

Nozomi Networks helps mining companies accelerate the pace of digital transformation. Our solution unifies visibility and threat detection across OT, IoT, IT and cyber-physical systems.

We make it possible for organizations to tackle escalating cyber risks to operational networks while modernizing their businesses to succeed in the future.

MINING INDUSTRY LEADERSHIP



Deployed in
5 of Top 10 Global Mining Companies

Nozomi Networks delivers network visibility, threat detection and operational insight to thousands of the largest industrial sites around the world. Through the innovative use of artificial intelligence, our solution automates the hard work of inventorying, visualizing and monitoring OT and IoT networks.

Mine operators benefit from the real-time visibility and threat detection needed to ensure high cyber resilience and reliability.

Following is a short description of our product line, for complete information, visit **our website**.

SAAS

Vantage

Vantage accelerates security response with unmatched threat detection and visibility across your OT, IoT and IT networks. Its scalable SaaS platform enables you to protect any number of assets, anywhere. You can respond faster and more effectively to cyber threats, ensuring operational resilience.

Requires Guardian sensors.

EDGE OR PUBLIC CLOUD

Guardian

Guardian provides industrial strength OT and IoT security and visibility. It combines asset discovery, network visualization, vulnerability assessment, risk monitoring and threat detection in a single application. Guardian shares data with both Vantage and the CMC.

EDGE OR PUBLIC CLOUD

Central Management Console

The Central Management Console (CMC) consolidates OT and IoT risk monitoring and visibility across your distributed sites, at the edge or in the public cloud. It integrates with your IT security infrastructure for streamlined workflows and faster response to threats and anomalies.

SUBSCRIPTION

Threat Intelligence

The Threat Intelligence service delivers ongoing OT and IoT threat and vulnerability intelligence. It helps you stay on top of emerging threats and new vulnerabilities, and reduce your mean-time-to-detect (MTTD).

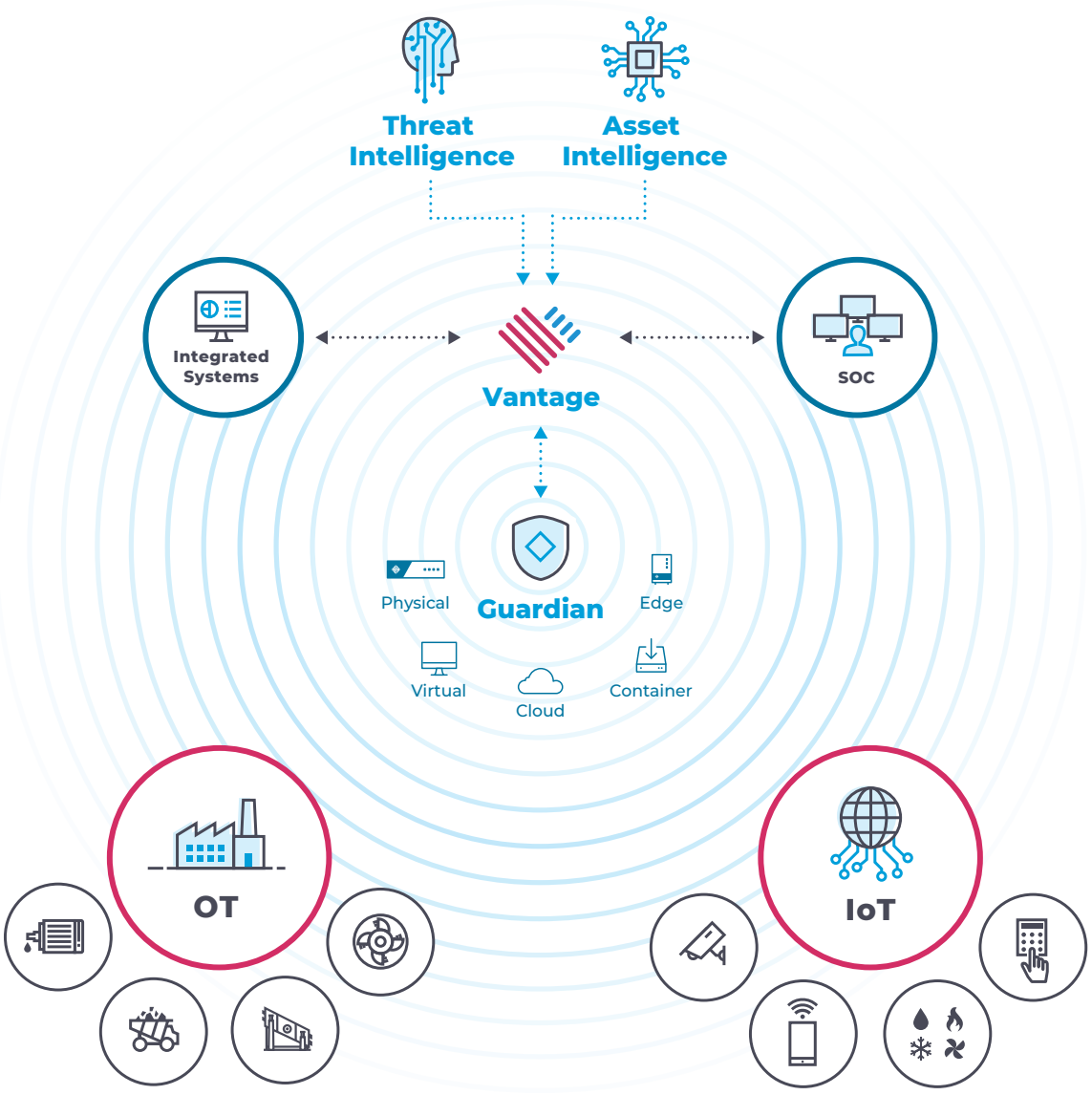
SUBSCRIPTION

Asset Intelligence

The Asset Intelligence service delivers regular profile updates for faster and more accurate anomaly detection. It helps you focus efforts and reduce your mean-time-to-respond (MTTR).

3.2 Diagram: OT and IoT Security and Visibility

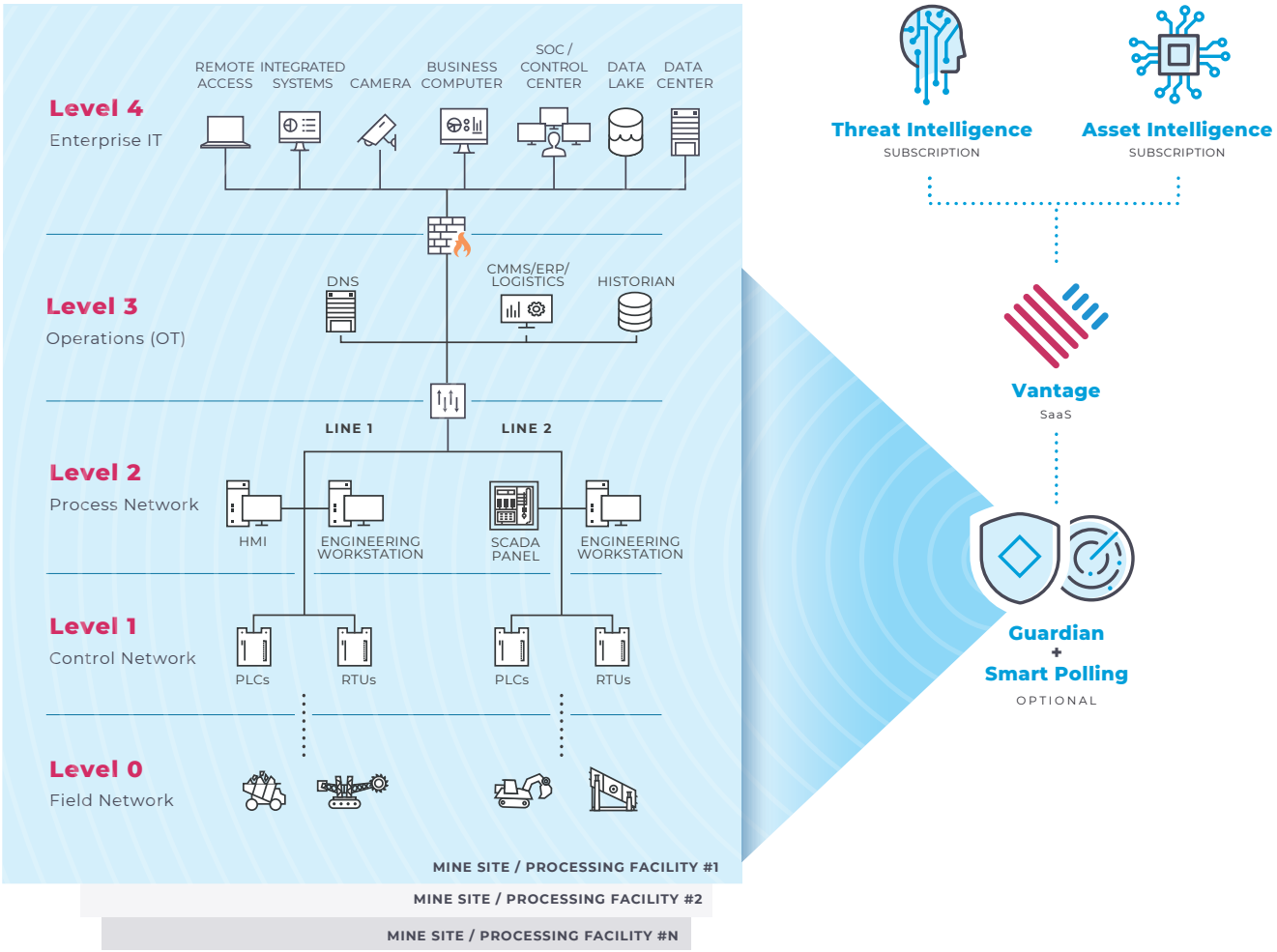
You can protect a wide variety of mixed environments with rapid asset discovery, real-time network visualization and up-to-date threat intelligence.



3.3 Deployment Architecture: Purdue Model Example

You can tailor the Nozomi Networks solution to meet your needs by utilizing its flexible architecture and integrations with other systems.

Additionally, **Remote Collectors™** can be added to Guardian sensors to capture data from remote and offsite locations.



4. Improving Network and Operational Visibility

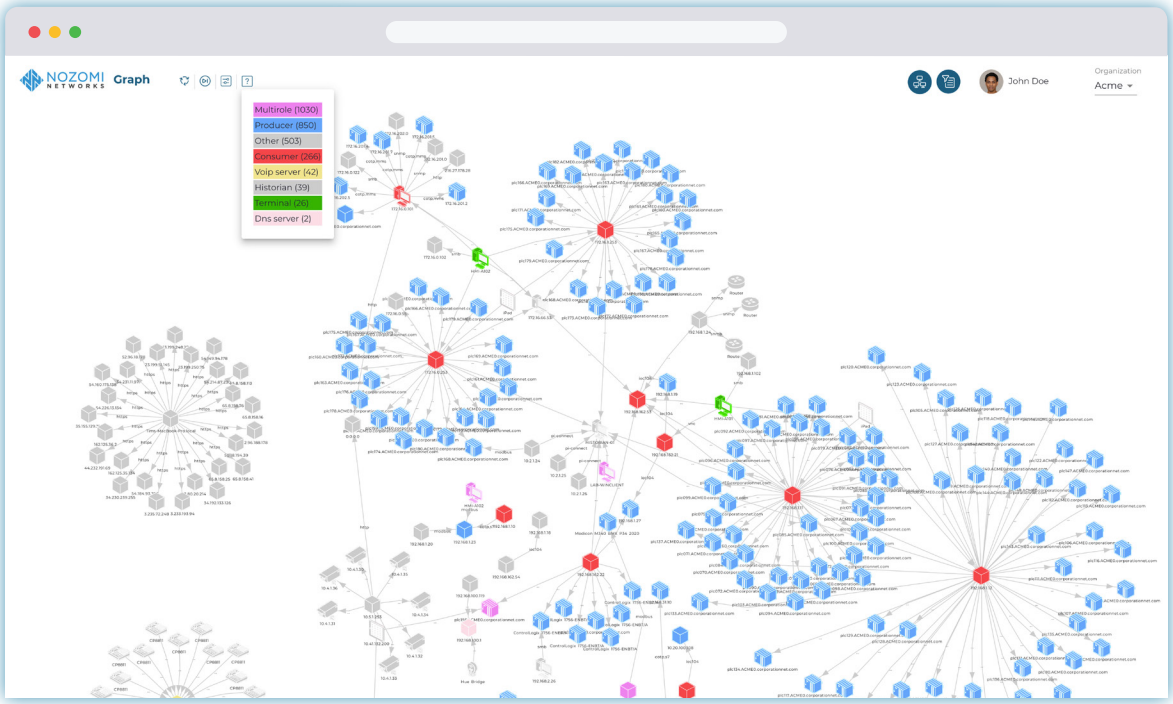
4.1 Use Case: Effectively Monitoring my SCADA Network

The complex nature of the mining industry means that one small process change can have a significant effect on equipment, safety and profitability. Thus staying on top of what's happening in the industrial control network, and responding to changes fast, is mission critical.

But mine operators can't monitor and manage a technology landscape that's not visible or documented. To spot and troubleshoot networking and communication issues that threaten reliability, industrial operators need real-time visibility into their assets, connections, communications, protocols and more.

Many common operational visibility challenges can be addressed through real-time network visualization and monitoring that surfaces useful information, such as:

- A macro view of the entire industrial control network, including zones, topology, nodes, links, sessions, and traffic
- Different subnets and network segments
- The role of each node and the traffic between nodes
- The protocols used to communicate between nodes and zones
- Network traffic information such as throughput, protocols and open TCP connections
- The detailed attributes of endpoints and connections



Nozomi Networks Solution: Network Graph View
This visualization displays all assets on your network for real-time awareness.

THE CHALLENGE

- Staying on top of SCADA network monitoring

THE SOLUTION

Using Real-time Network Visualization to Improve Mining Process Awareness

- The Nozomi Networks solution provides comprehensive visibility into an operator's industrial network and OT and IoT assets.
- Manufacturers can efficiently monitor industrial networks and easily troubleshoot problems before they impact operations.

RESULTS

Network-wide situational awareness

Faster troubleshooting of system changes and issues

Better oversight of vulnerabilities and risks

Higher operational reliability

4.2 Use Case: Proactively Identifying Equipment Wear

Unplanned downtime happens for multiple reasons – a component breaks down from operating under harsh conditions, a networking change impacts automated processes, or a cyber incident brings the entire business to a halt.

Here's an example of how equipment failure can impact operations in multiple ways: The hub of each $60K tire on a $5M haul truck contains a small orbital motor. Operating under 4,000 PSIs of constant pressure can cause the fluid in the motor to overheat, damaging the hydraulic system and reducing the component's life expectancy.

In the asset-intensive mining industry, equipment maintenance and repairs can hit productivity and margins hard. According to Gartner, production downtime cost adds up to somewhere between $300k - $500k an hour.[7]

Imagine the benefits of proactively identifying temperature and pressure anomalies, or other preventative maintenance issues before they bring operations to a halt, hurting the bottom line.

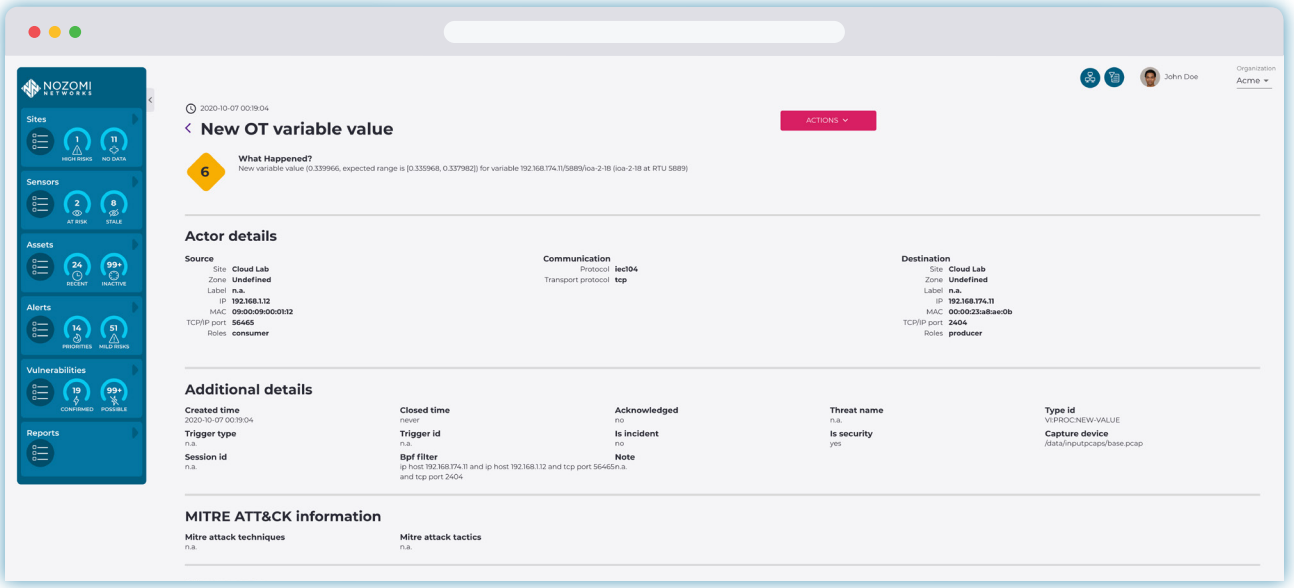
The Nozomi Networks solution tackles preventative maintenance head-on with OT and IoT network monitoring and anomaly detection that identifies normal behavior and alerts industrial operators to deviations.

Baselining Variables

In the initial Dynamic Learning phase, the solution uses machine learning and AI to observe mine network traffic and create asset and process baselines. It models behavior and correlates multiple types of data, including information about similar assets within the mine, to determine what normal activity looks like.

Detecting Anomalies

In the second phase, monitoring, the solution automatically detects when a specific component or process is deviating from its baseline and moving towards a state that could disrupt mining operations. It uses advanced correlation and operational context to deliver a simple, consolidated view of what's happening in the network, and proactively alerts operators that remediation may be necessary.



Nozomi Networks Solution: OT Variable Alert
Unusual device or system behavior could lead to operational disruption and serious safety incidents.

THE CHALLENGE

- Preventing process disruption and costly repairs.

THE SOLUTION

Using anomaly detection to identify at-risk equipment before it fails

- The Nozomi Networks solution monitors the OT and IoT network, determines behavior baselines, detects anomalies and alerts operators to deviations.
- Mine operators spend less time troubleshooting and can take action before a component or process failure incident occurs.

RESULTS

Proactive detection of potential equipment failure

Faster problem resolution

Maximized production line uptime

5. Detecting Cyber Risks and Improving Cyber Resilience

5.1 Use Case: Segmenting the OT Network for Cyber Resilience

Earlier this year, a ransomware called LockerGoga hit one the largest aluminum producers in the world. According to media reports, the malicious phishing attack forced the organization to take computer systems offline and switch to manual operations, leading to costly outages and production slowdowns.

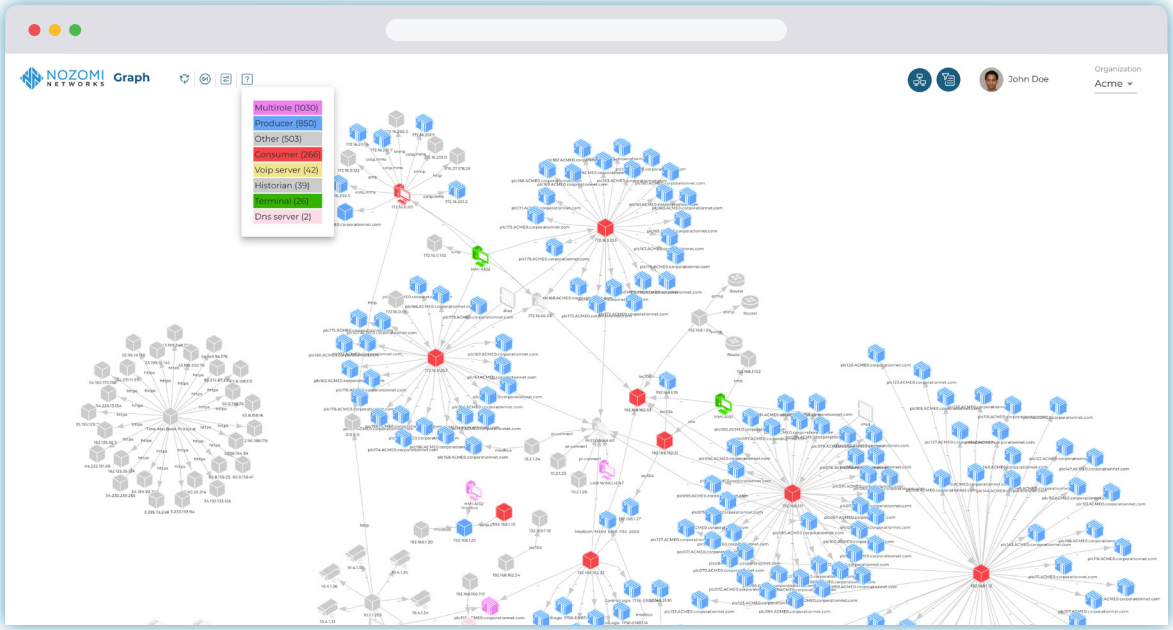
But LockerGoga isn't the only cyber threat to impact industrial operations. A new type of OT and IoT malware called TRITON recently reprogrammed a facility's Safety Instrumented System (SIS) controllers, causing an automatic shutdown of the industrial process.

Regardless of whether a cyber incident originates on the IT side of the business, or was introduced intentionally or accidentally on the OT side, a single firewall separating IT and OT is no longer enough.

Without effective segmentation of OT and IoT and SCADA networks, ransomware and other cyber threats gain free flowing lateral access to operational systems, enabling potentially dangerous disruption or damage.

As outlined in IEC 62443 standards, OT segmentation is considered best practice when it comes to controlling communications across OT and IoT and SCADA systems. OT zone segmentation is an effective way to mitigate perimeter breaches, as well as prevent intentional and accidental OT cyber incidents from spreading. But achieving effective network segmentation requires visibility into your OT network structure, and insight into where vulnerabilities lie.

The Nozomi Networks advanced network visualization and vulnerability assessment capabilities help identify opportunities for mining operators to strengthen cyber resilience and prevent a network infection from spreading.



Nozomi Networks Solution: Network Visualization Topology

The Network View pane on the left allows users to easily navigate and filter by different subnets and network segments. The views on the right show details of the network area selected.

THE CHALLENGE

- Improving cyber resilience with OT network segmentation

THE SOLUTION

Real-Time Network Visualization

- The Nozomi Networks solution automatically creates a network map, identifying opportunities to build cyber resilience.
- Mine operators can then use segmentation as a risk mitigation measure for groups of devices with the same vulnerabilities or security requirements.

RESULTS

Easier planning and review of network segmentation projects thanks to up-to-date network visualization

Better segmentation decision-making based on informed vulnerability assessments

Rapid identification of improper traffic between segments, faster troubleshooting and mitigation

5.2 Use Case: Defending the Mine Against Malicious Data Theft

In a world of fierce competition over dwindling accessible reserves, corporate data can be just as valuable as gold or diamonds. Cyber espionage could be a potential threat if a mine operator wanted to gain unfair advantage in M&A negotiations or when bidding for drilling rights.

In 2016, one of North America's largest gold producers was the target of a cyberattack where a significant amount of corporate and personal information, including budget and payroll data, was held for ransom. When hackers didn't receive the payoff, they posted the information online for all to see.

To protect the organization's competitive position and its reputation, it is critical to keep IP, business plans, financial performance and other confidential operational data under wraps.

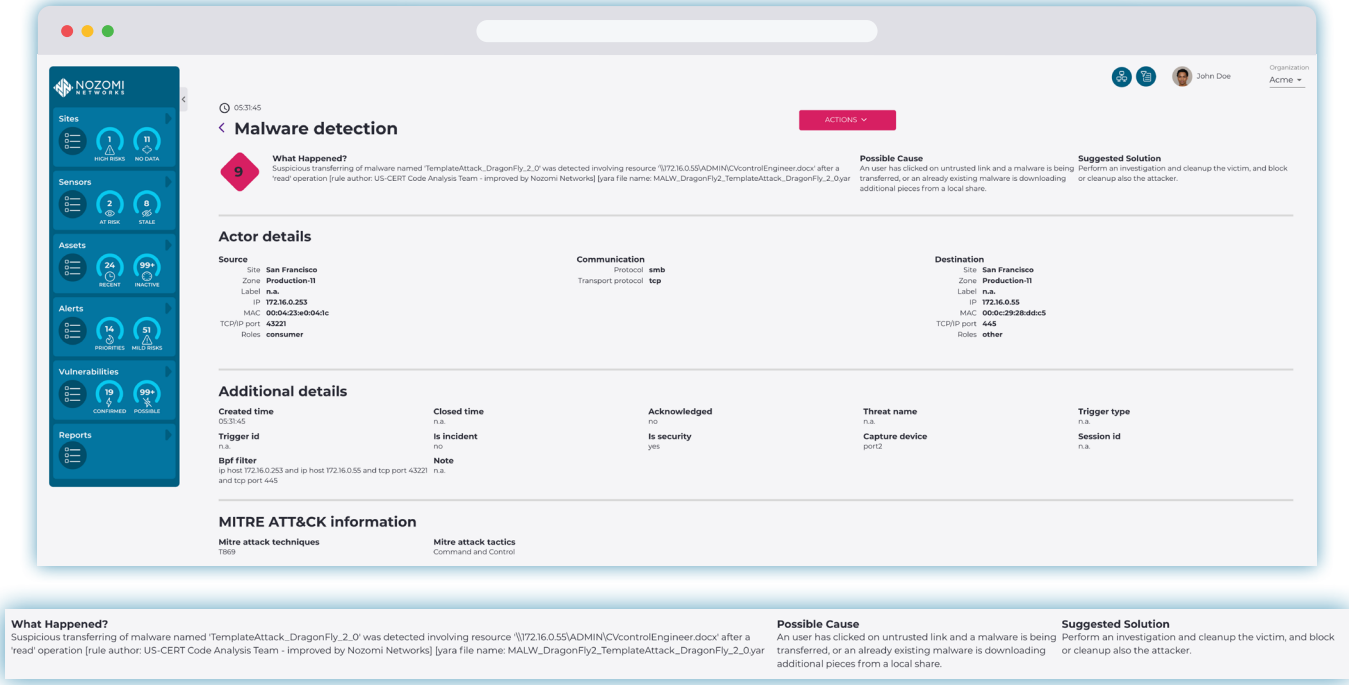
Nozomi Networks takes a multi-pronged approach to identifying suspicious activity – whether it's accidental or intentional.

Through behavior-based anomaly detection and multiple types of signature and rules-based detection, the solution identifies unauthorized activity such as:

- Remote access
- Log file deletions
- Configuration changes
- Downloads
- Controller logic changes
- Edits to PLC projects and more

All threat detection results are correlated with operational context for detailed insight. For example, the solution checks baselines for network peculiarities such as VPN access and IP ranges assigned to known asset vendors. If activity occurs outside those ranges, an alert is triggered.

When suspicious activity is identified, the solution sends high priority alerts to mine security and operations staff, who can then execute the incident response plan to contain or eradicate the threat.



What Happened?
Suspicious transferring of malware named 'TemplateAttack_DragonFly_2_0' was detected involving resource '\\172.16.0.55\ADMIN\CVcontrolEngineer.docx' after a 'read' operation [rule author: US-CERT Code Analysis Team - improved by Nozomi Networks] [yara file name: MALW_DragonFly2_TemplateAttack_DragonFly_2_0.yar

Possible Cause
An user has clicked on untrusted link and a malware is being transferred, or an already existing malware is downloading additional pieces from a local share.

Suggested Solution
Perform an investigation and cleanup the victim, and block or cleanup also the attacker.

Nozomi Networks Solution: Alert Detail

The Nozomi Networks solution takes a multi-dimensional approach to detecting cyber risks and threats. It uses both threat signatures and anomaly detection to identify attacks in process, and deliver clear, actionable information.

THE CHALLENGE

- Keeping confidential corporate information confidential

THE SOLUTION

A Comprehensive Approach to Detecting Cyber Risks and Threats

- The Nozomi Networks solution uses behavior-based anomaly detection and multiple types of signature and rules-based detection to identify unauthorized activity.
- Based on alert details, mine operators can execute an incident response plan to contain or eradicate the threat.

RESULTS

Proactive identification of unauthorized activity

Faster execution of cyber incident response plans

Prevention or mitigation of data theft

6. Conclusion

Deep Visibility into Mining OT and IoT Environments Builds Operational Resilience

Mining companies are rapidly embracing tools that help them gain operational efficiencies, such as digitization, automation and IIoT. However, these advances come with increased vulnerability to cyber risks due to connectivity between the OT environment and enterprise or external systems.

To combat increased cyber threats, mining operators will inevitably need to address common operational cybersecurity challenges – such as gaining visibility into their OT and IoT networks and closing security gaps.

MINING INDUSTRY LEADERSHIP

Deployed in

5 of Top 10 Mining Companies

Without OT and IoT visibility, it's difficult to stay on top of risks. One small change or networking issue can increase exposure to cyber threats and impact production, profits and IP security. While a fast response to anomalies is critical, spotting issues before they impact the business requires real-time visibility into network assets, connections, communications and more. Unfortunately, mine operators often lack these core capabilities.

Security gaps related to people, process and technology can impact operational resilience too. For example, the lack of visibility into OT and IoT assets can lead to cybersecurity blind spots. But, with the right technology and a focus on best practices, mining operators can build resilience.

Fortunately, complete visibility into the OT and IoT environment and real-time monitoring of systems for threats is achievable today thanks to innovative technology.

The Nozomi Networks solution delivers improved OT and IoT visibility by automatically creating an up-to-date inventory of all assets on the network. It then monitors device behavior for anomalies and alerts operators to changes that could indicate potential problems. The solution also provides advanced vulnerability and threat detection, along with detailed insights that lead to faster prioritization and remediation.

Tailored to meet the unique challenges of mining operations, the Nozomi Networks solution helps operators gain deep OT and IoT visibility, minimize production downtime, defend against malicious data theft and improve operational resilience.

FIND OUT MORE

The world's top mining companies are benefiting significantly from their investment in our innovative network visibility, monitoring and security solution.

Find out how quickly the Nozomi Networks solution can build resilience for your industrial operation.

Contact us at **nozominetworks.com/contact**

7. Customer Reviews

Customers Give Nozomi Networks Top Score

★★★★★

Exceeded Expectations. Deeper Visibility Than Expected.

We place an emphasis that every vendor we engage with understands we are not a set up for a “cookie cutter” type of solution. I honestly expected this to be a problem for most if not all vendors. And I was correct, with Nozomi being the sole exception. Not only has their solution done as advertised, and then some.

Senior Industrial Security Manager ›

Once You Try Nozomi And Its Rich Feature Set You Cannot Imagine Operating Without It!

We put Nozomi head to head against other similar products and the Nozomi platform was able to pick out and properly categorize more L2 devices than any other tool in the market place at the time of test.

Security Analyst ›

Great Solutions For ICS.

The solution still has many features that manage the OT environment, such as inventory and vulnerability analysis capabilities. An extra point for the solution is the communication flow map of the neural network, containing information of great relevance for an incident response.

IT Analyst ›

For more reviews, visit our website. See All Reviews

What to Look for in an OT and IoT Security and Visibility Solution

Technology advancements, such as those found in the Nozomi Networks solution, can dramatically improve security and reliability.

When choosing a solution, look for the following characteristics:

- Comprehensive OT and IoT visibility
- Advanced threat detection
- Accurate anomaly alerts
- Proven scalability across thousands of sites
- Easy IT/OT integration
- Global partner ecosystem
- Exceptional customer engagement and support

See the Nozomi Networks Solution in Action

If you would like to see our solution in action, and experience how easy it is to work with Nozomi Networks, please contact us at **nozominetworks.com/contact**

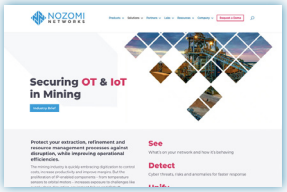
Contact Us

Want to Know More?

SOLUTION BRIEF

Nozomi Networks

DOWNLOAD



WEBPAGE

Solution: Mining

VISIT

DATA SHEET

Vantage

DOWNLOAD

DATA SHEET

Threat Intelligence

DOWNLOAD

8. References

1. **"Is cybersecurity about more than protection? EY Global Information Security Survey 2018-19,"** EY, 2018.
2. **"Mining and Metals Information Sharing Analysis Center,"** MMISAC, 2019.
3. **"Hackers target Goldcorp Inc, release reams of private data online including payroll and passports,"** Financial Post, 2016.
4. **"Move to Zero Unplanned Downtime,"** Emmerson, 2012.
5. **"Hydro First Quarter 2019 Report,"** Hydro, 2019.
6. **"Australian metal detector company counts cost of Chinese hacking,"** Reuters, 2015.
7. **"The Cost of Downtime,"** Gartner, 2014.

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.

© 2021 Nozomi Networks, Inc.
All Rights Reserved.

IB-MNG-8.5x11-005

nozominetworks.com