FORESCOUT

A Smarter, Safer Grid

How asset performance management, supported by enhanced ICS visibility, can increase reliability, improve security and reduce costs for utility companies

Executive Summary

The utility industry has embraced the digitalization of their infrastructures, investing significant amounts of money in technology. In an industry where margins are tight, this investment has been driven by the potential cost savings, efficiency gains and downtime avoidance that sensor-enabled remote monitoring and preventative maintenance can achieve.

To fully leverage these benefits, utility companies need better ICS asset visibility and security across a converged IT/OT environment. On the IT side, existing solutions usually have this covered, but the OT environment needs an innovative approach to optimize ICS visibility.

This white paper describes how using an enhanced network monitoring and situational awareness platform for industrial networks in the utility sector improves asset visibility and performance management. It also explains how OT managers who utilize this type of solution can simplify their work significantly, while delivering increased value to their organizations by establishing cyber resilience.

Opportunity Is a Complex Business

The electric power industry has proactively adopted closer integration between Information Technology (IT) and Operational Technology (OT) infrastructures, which has also coincided with the broader adoption of alternative power generation technologies such as solar and wind power. The potential benefits of these transformations include greater operational efficiency and a reduction in downtime by using preventative maintenance solutions that monitor equipment and identify potential failures before they occur. However, progress has varied widely between regions because of various local and organizational factors, such as market structures, resource capacity, electricity pricing, regulatory requirements and others.

This heterogeneity and the potential for other influential trends to emerge mean that uncertainty is the new normal in the electric power industry. In addition, the network convergence required to realize the potential advantages outlined above generates a new level of complexity for IT and OT managers within the utility industry. The effects of opening up previously siloed industrial control systems (ICS) networks to an increasingly broad range of IT technologies, is illustrated in Figure 1.

DIGITALIZATION DIVIDEND

Asset performance management has the potential to contribute $387 billion of value from 2016 to 2026 *(World Economic Forum)*

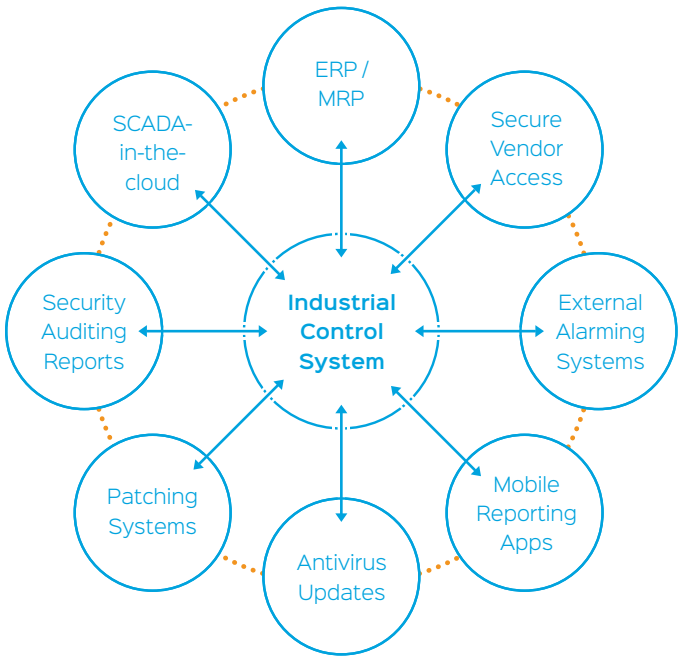


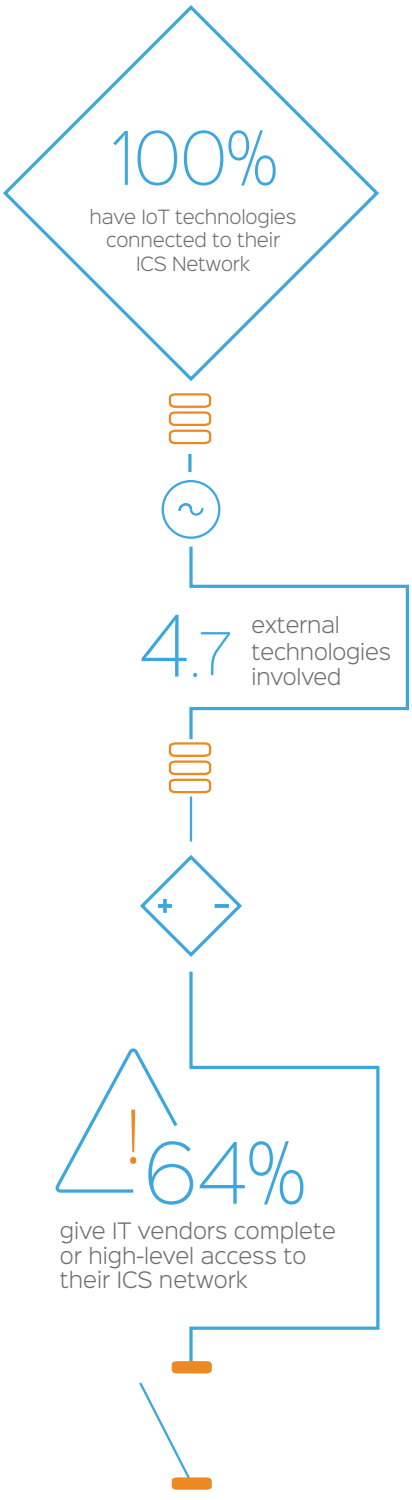
Figure 1: New business needs are driving the exposure of ICS networks to multiple technologies

Initially, integration with ERP systems helped businesses align resource allocation more closely with production. Since then, increasing security threats and the importance of mobile technology in managing operations have required multiple alarming, reporting and update systems to be given access to the ICS network.

Today, as Deloitte [1] states in its "2018 Outlook on Power and Utilities" report, there are several industry-specific trends that are driving this deeper integration, including:

- The development of a communications-centric grid that increasingly manages itself
- The automation and integration of corporate services to minimize manual interventions and streamline organizations

These trends also reflect the increasingly connected nature of IT and OT environments in all industries. In fact, Forrester [2] reported in January 2018 that 100% of organizations now have IoT technologies connected to their ICS networks, and the average number of external systems involved is more than four. Moreover, 64% of organizations surveyed in the same report said they provide third-party IT vendors with complete or high-level access to their ICS networks. The next generation of systems to be integrated into ICS will be cloud-based supervisory control and data acquisition (SCADA) systems, which will add yet another layer of complexity.



At the same time, a diverse range of teams and roles including C-level executives, business managers, engineers, and IT, OT and IS experts are needed to define power generation networks in their entirety. Most of these stakeholders do not have deep insight into the technologies and processes of their counterparts' environments, and none of them has a complete picture of all the assets connected to the converged network. Without knowledge about current asset performance, vulnerabilities, status and configuration, the network can't be protected or efficiently maintained. With enhanced ICS visibility, utility companies have the ability to detect and prevent potential incidents before they cause damage to the network and the business. So, it's clear that the need for effective, proactive control over asset performance management has never been greater. However, before looking at how to achieve that, it's important to define the challenges and risks associated with a lack of asset visibility in a converged IT/OT network environment.

The Challenges and Risks of IT/OT Convergence

1. Rising Costs

2. Unplanned Operational Downtime

3. Increasing Cyber Threats

4. IT-OT Relationship Puzzle

5. Limited Resources / Increasing Workloads

6. High-Effort Compliance Fulfillment

1. Rising Costs

According to a 2015 report by the Institute for Electrical Innovation [3], industry participants will have invested around $2 trillion globally in upgrading electric grid infrastructure by 2020. To maximize ROI and maintain operational efficiency, the assets in these infrastructures need to be monitored and measured in real time.

Not having visibility into ICS network assets can generate direct costs, such as additional man hours required to manage and achieve compliance across a more complex environment or the revenue lost during unplanned downtime caused by an 'invisible' network asset. These costs can also be indirect, such as the reputational damage caused by a security breach that could not be identified in advance. Cumulatively, they can represent millions of dollars in unplanned expenditure.

2. Unplanned Operational Downtime

According to a recent report by technology market research specialists Vanson Bourne [4], achieving zero unplanned downtime is high board-level priority among almost three-quarters (72%) of organizations surveyed. This is unsurprising, given the huge costs generated when operations are disrupted.

Unfortunately, the risk of unplanned downtime, caused by the network complexity described above, particularly by a lack of asset visibility, is increasing. In fact, the Vanson Bourne report states that asset ignorance, caused by a lack of visibility, affects around 70% of organizations.

3. Increasing Cyber Threats

As we have seen, the number of Internet-connected devices and IT technologies has increased dramatically. As a result, OT networks, proprietary systems and legacy technologies that were isolated from cyber incidents in the past now need protection from Internet-based threats. Moreover, the effectiveness of the Stuxnet worm proved that even segregated networks can be attacked successfully. Sensors, wi-fi enabled controllers, and the latest cloud-based industrial control systems such as SCADA-as-a-Service all provide potential entry points for cyber criminals. The Forrester survey [5] cited above revealed that 79% of SCADA/ICS operators reported a breach in the past 24 months. Every breach of this kind can potentially compromise the safety of employees and the financial stability of the organizations affected. In fact, looking at the Repository of Industrial Security Incidents, it is evident that the energy and utilities are the most targeted industries.

79%

of SCADA/ICS operators reported a breach in the past 24 months

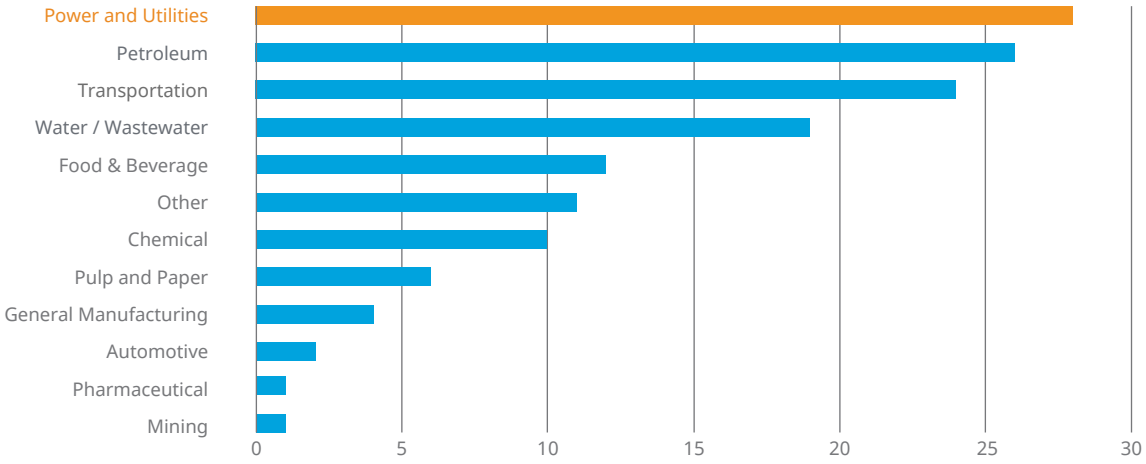


Figure 2: Most targeted industries (global)
Source: RISI Online Incident Database

In the US, utility companies are collaborating with each other and with the government to prepare for increased risks. These efforts include undertaking risk assessments and creating cybersecurity programs in accordance with frameworks set out by the National Institute of Standards and Technology (NIST) or the North American Electric Reliability Corporation (NERC). These activities will likely intensify well into the future as the number and range of potential threats increases.

44%

were never able to identify its source

The lack of asset visibility is one of the main sources of cyber threat risk, and one of the reasons why the SANS [6] Institute recently reported that 15% of companies affected by a breach needed more than a month to realize they were afffected, and 44% were never able to identify its source. As noted above, the direct and indirect financial consequences of downtime caused by a breach can be severe.

4. The IT-OT Relationship Puzzle

IT TOP PRIORITY
Protecting data

OT TOP PRIORITY
Protecting the availability and integrity of the industrial process

IT and OT are very different departments with very different responsibilities. IT's top priority is protecting data. OT's top priority is protecting the availability and integrity of the industrial process. However, modern business requirements dictate that IT and OT managers cooperate to protect the ICS network. CIOs and CISOs now have to accept responsibility for any unexpected downtime, equipment damage or safety hazards in their industrial environments caused by cyber incidents. To fulfill this responsibility, they need to have more visibility into ICS network assets.

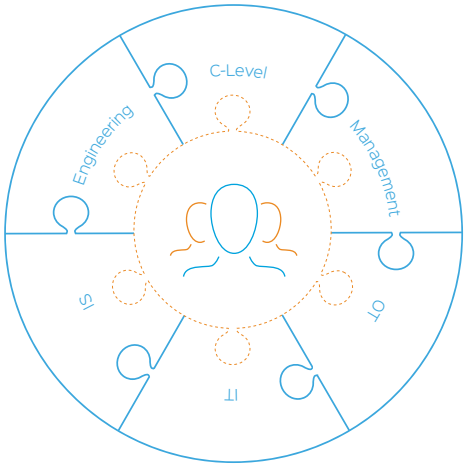


Figure 3. Multiple teams and roles are required to define the network accurately.

> "The less you can see, the more you pay."

5. Limited Resources and Increasing Workloads

Utility IT and OT managers already have heavy workloads without the additional layer of complexity that IT/OT convergence generates. Moreover, while IT and OT network visibility solutions exist individually, they rarely intersect. Manually piecing together information from such solutions is imprecise and gaining contextual intelligence from them is an even bigger task that can break already overstretched teams. Unless complete visibility and control is established over IT/OT environments, it is inevitable that their jobs will become even more difficult and stressful. And where IT visibility has already been achieved, it's often OT visibility that is the missing link.

6. High-Effort Compliance Fulfillment

Any framework for achieving compliance requires solid asset management and inventory visibility as a foundation. Increased network complexity, as well as constantly changing internal policies and external regulations, make this task more difficult and time-consuming. This in turn exacerbates the resource and workload challenge described above. Despite the costly and labor-intensive compliance efforts many companies implement, the possibility of fines being imposed remains relatively high. Moreover, future compliance costs and efforts are likely to rise. One cause is illustrated by a recent Ponemon Institute report [7], which highlights the fact that that two-thirds of senior IT security leaders expect to increase the frequency of audits and assessments, with board directors becoming more involved in overseeing overall IT security effectiveness. Another factor is the increasing volume and stringency of regulations, such as the NERC CIP requirements for securing electricity supply in North America and the NIS directive in Europe. These factors tend to support the findings of the Ponemon Institute report, which also provided insight into the relationship between simplifying compliance and improving security. It revealed a 90% year-over-year increase in the number of survey respondents who believe that a reduction in compliance burden contributes to a stronger cybersecurity posture.

COMPLIANCE BECOMES MORE DIFFICULT BECAUSE OF

- Network complexity
- Changing internal policies
- External regulations

2/3

of senior IT security leaders expect an increase of audits and assessments

Increasing ICS Asset and Threat Visibility Is Key

A 2017 survey by the SANS Institute found that 40% of ICS security practitioners "lack visibility or sufficient supporting intelligence into their ICS network". So, how can organizations make informed decisions about how to prioritize spending and create security plans that will safeguard their employees, reputations, and bottom lines? They need to achieve complete asset visibility to gain comprehensive knowledge about their network assets and vulnerabilities.

However, traditional approaches to achieving this are flawed. For example, random network scanning can cause process interruption or system downtime that leads to financial loss. In more extreme cases, it can even damage the industrial environment or result in employee injury if safety controls are compromised. Physical inspections, on the other hand, are safer but extremely labor-intensive, time-consuming, costly and error-prone. Historically, it has been especially difficult and labor-intensive for ICS asset owners with "grid-edge" devices because legacy infrastructures are so complex, old and geographically dispersed. Fortunately, there is a technique that can identify assets accurately, safely and cost-effectively: ICS network monitoring.

TRADITIONAL APPROACHES TO VISIBILITY

- Random network scanning
- Physical inspections

OPTIMAL APPROACH

- Non-intrusive network security monitoring

An Optimized Approach to ICS Visibility Management

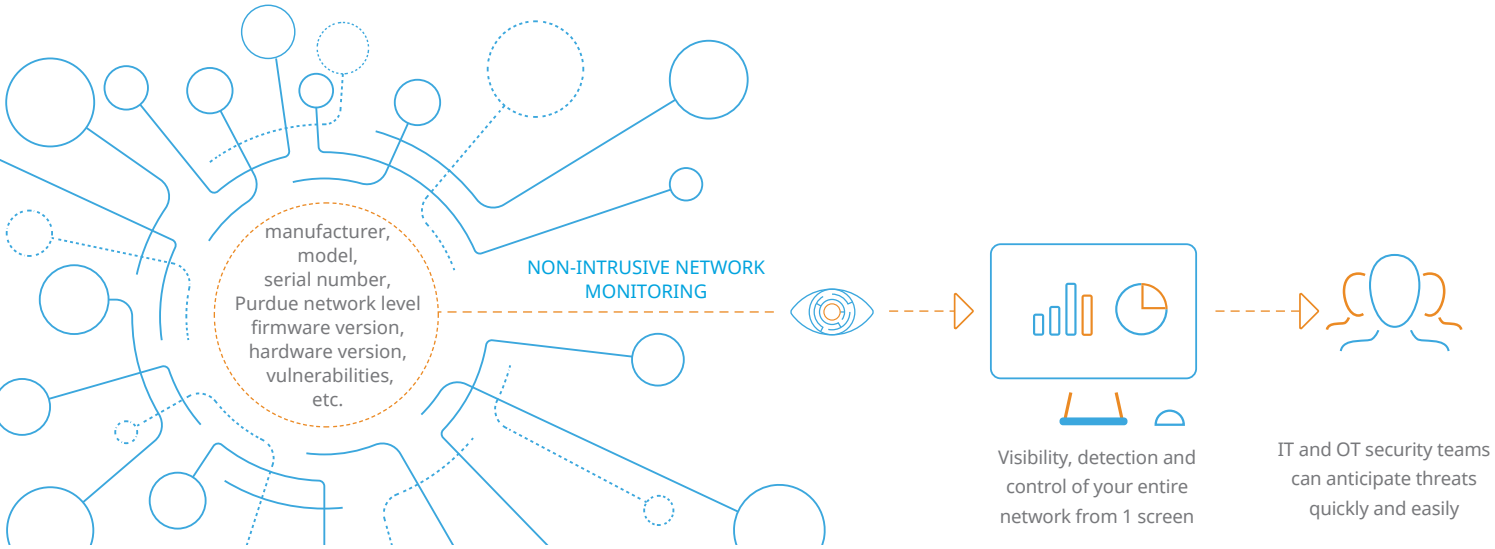
Optimizing ICS visibility to enable more effective asset performance management and enhanced security with network monitoring can give utilities a thorough understanding of the ICS environment and its connections, making it easier to design effective security architectures, identify attack vectors and locate blind spots, among other things. Improved visibility also enables utility OT managers to resolve unknown and unchecked operational security issues. These include vulnerabilities, misconfigurations, access policy violations, faulty design in the form of weak security controls, as well as unplanned or unauthorized changes.

A best practice approach to optimizing ICS visibility involves the adoption of an advanced and mature network monitoring and situational awareness platform for industrial networks:

- ICS network monitoring solutions are invisible to the network and have no impact on running processes.
- They collect asset information such as type, version and location by listening to traffic already traveling through the network.
- Because of the automated and passive nature of this method, operators can continuously track asset information and behavior, which greatly increases the efficiency of a traditionally expensive operation like maintaining an accurate asset inventory.
- The asset owner also has the option to deploy additional non-intrusive active modules. Driven by the passive system, these active modules can securely and selectively query specific hosts on the ICS network to gain additional information, with zero impact on the network.

NON-INTRUSIVE MONITORING

The collection of asset information such as type, version and location by listening to traffic already traveling through the network, combined with optional active modules for enhanced data collection.



Solutions like this leverage powerful machine learning capabilities called full deep packet inspection (DPI). This allows asset owners to access asset inventory information in real time from grid edge devices that communicate via serial or TCP/IP channels. They also feature vast libraries of ICS-specific threat indicators and vulnerabilities for analyzing standard and proprietary industrial protocols from all the major SCADA manufacturers.
Other key capabilities include:

- Asset inventory and management, including dynamic business asset classification
- Vulnerability management of OT vulnerabilities, including those with and without CVE identifiers
- Anomaly detection to detect not only new attacks and techniques, but also deviations from normal process behavior
- API integration with IT security management tools
- Broad ICS protocol support
- Optional non-intrusive active modules which can more extensively query specific nodes to gain additional information

These features enable ICS monitoring solutions to detect operational threats including network connectivity problems, device malfunction and misconfiguration, dangerous process operations, use of insecure protocols and default credentials, advanced cyber attacks, and exploit attempts. Alerts about potential threats to operational continuity are then delivered to a central visibility management platform in real time. From there, they can be escalated appropriately within the organizational ecosystem.

> "This gives OT managers total ICS visibility and a clear path towards achieving true cyber resilience."

By combining sensor-derived information from across the network with other data sources such as controls configuration and asset management, a comprehensive and interactive visual model can be constructed. This gives OT managers total ICS visibility and a clear path towards achieving true cyber resilience.

Enabling Asset Performance Management with Enhanced ICS Visibility

Enhanced ICS visibility management enables OT Managers to take control of the challenges and risks associated with greater IT/OT infrastructure convergence and achieve more effective asset performance management in the converged environment. The benefits range from cost savings to lower workloads and simplified compliance.

1. Significant Cost Savings

2. Reduced Unplanned Operational Downtime

3. Improved Cyber Resilience

4. Reduced Workloads

5. Simplified Internal and Regulatory Compliance

1. Significant Cost Savings

According to the 2016 World Economic Forum/Accenture Digital Transformation of the Electricity Industry report [8], asset performance management has the potential to contribute $387 billion of value within ten years. By replacing manual asset inspection with an automated, predictive and intuitive process, it can contribute to stronger profit margins for power companies. Predictive maintenance can also significantly reduce the likelihood and cost of equipment failures.

Additionally, increased ICS visibility means potential threats can be identified and addressed more quickly and cost-effectively. For example, when all assets can be viewed on a single pane of glass, the asset owner can check that the right asset is being monitored and that maintenance is progressing as it should, without expensive site visits. This also reduces the costs and effort involved in investigating attacks or vulnerabilities, as well as those associated with troubleshooting, mitigating and resolving them. Additional cost savings can be measured in the avoidance of downtime, service or delivery disruption and the reputational damage caused by successful attacks.

$387,000,000,000

The potential value of asset performance management

2. Reduced Unplanned Operational Downtime

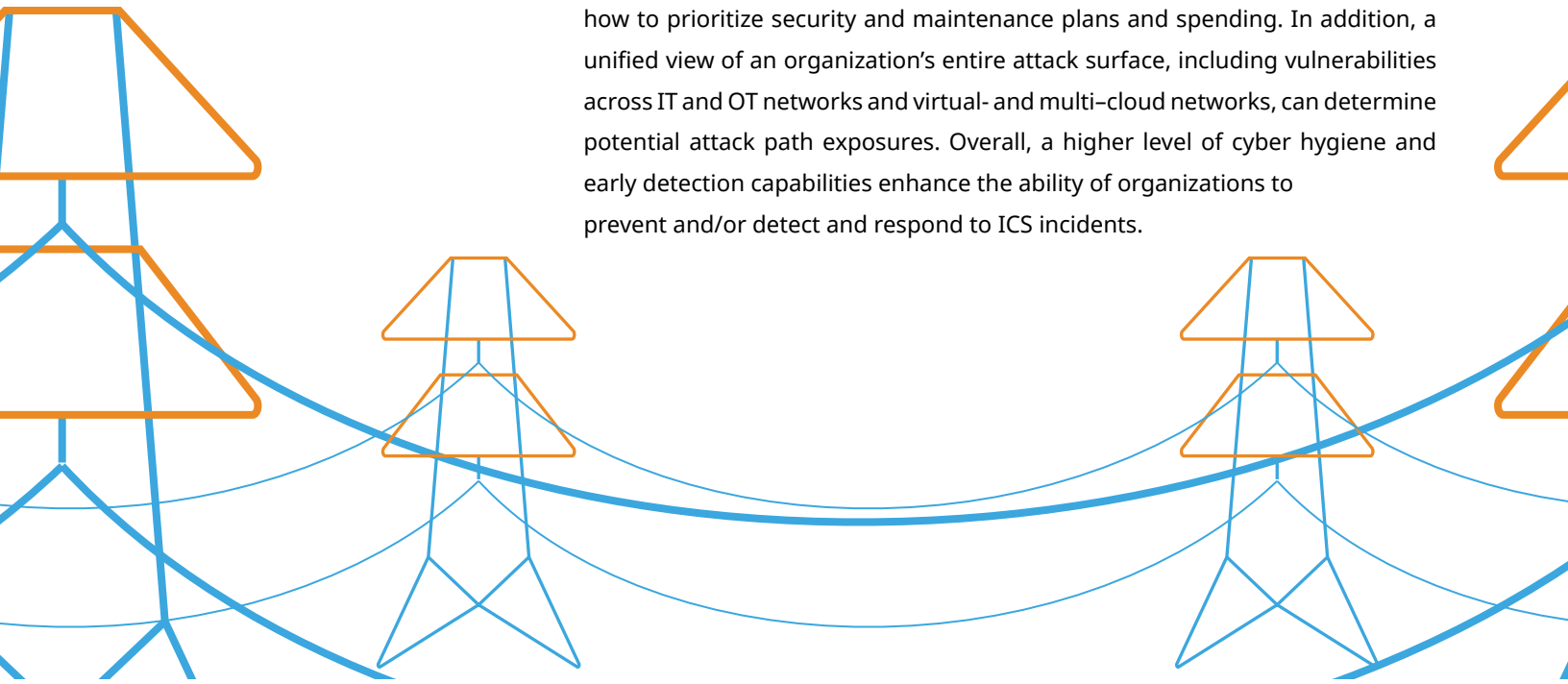
According to the Vanson Bourne report cited above, 49% of respondents believe that machines requesting assistance automatically would be helpful in avoiding downtime, and 45% would also like to enable engineers to access historical asset data. An optimized and non-intrusive monitoring approach to ICS visibility management provides the tools to achieve this.

- Continuous network health checks give OT managers a complete picture of current asset status within a single interface.
- Automated alerts help managers identify potential problems at their earliest stages and gather the information required to respond as quickly as possible.
- The history of all the config changes applied to assets is preserved and can be easily accessed to analyze behaviors and issues.
- The insight gained from every incident can be used to help managers pinpoint future weak spots and inefficiencies.

This means many potential problems can be anticipated and addressed before they cause downtime and any associated operational, financial or reputational damage. In addition, the World Economic Forum/Accenture report cited above indicates that many utility ICS vendors such as ABB, Siemens, GE, JCI and Schneider Electric are already benefiting from this kind of preventative approach.

3. Improved Cyber Resilience

Full knowledge of ICS assets, vulnerabilities, additions and changes ensures utility OT managers are no longer working blindly. This helps them make informed decisions about which controls to implement for risk mitigation, and how to prioritize security and maintenance plans and spending. In addition, a unified view of an organization's entire attack surface, including vulnerabilities across IT and OT networks and virtual- and multi–cloud networks, can determine potential attack path exposures. Overall, a higher level of cyber hygiene and early detection capabilities enhance the ability of organizations to prevent and/or detect and respond to ICS incidents.



4. Reduced Workloads and Improved IT/OT Collaboration

Using an optimized asset inventory solution based on network monitoring gives OT managers the insight they need to help the organization define the network accurately and maintain that precise definition continuously. As a result, a synergy is created that empowers them to collaborate closely with their IT and IS colleagues. This helps all stakeholders understand the interconnectedness of the environment, pinpoint the biggest risks and plan how to deal with them. All of which helps the organization protect network integrity and achieve cyber resilience across the board. And because enhanced ICS visibility makes the network easier to control and protect, OT managers are also better positioned to increase and prove the value they deliver to the business with less effort, and less cost.

SYNERGY BETWEEN IT AND OT

Helps the organization protect network integrity and achieve cyber resilience

ACHIEVING MORE WITH LESS STRESS - TOGETHER

5. Simplified Internal and Regulatory Compliance

The complete inventory information and controls delivered by ICS network monitoring simplify and reduce the cost of maintaining compliance with standards and frameworks such as the NIST Cybersecurity Framework, NERC CIP, IEC 62443 and FISMA. Asset inventory data must be made available through powerful, automated reporting capabilities that eliminate error-prone and costly manual data entry. The data includes critical information such as:

- Manufacturer
- Model
- Serial number
- Part/type (e.g. IO card, communication module)
- Firmware version
- Hardware version
- Device name
- Vulnerabilities
- Purdue network level and NERC CIP classification

A comprehensive inventory list and an interactive network map that groups assets and communications by device type and network also enables accurate reporting and auditing to help avoid potential penalties with minimal effort.

MAINTAINING COMPLIANCE WITH STANDARDS AND FRAMEWORKS SUCH AS:

- NIST CSF
- NERC CIP
- IEC 62443
- FISMA

Conclusion

Leveraging the potential benefits of a converged OT and IT infrastructure offers a competitive advantage, but only if ICS assets can be managed efficiently and possible cyber or operational incidents can be identified and prevented. While existing security management tools can cover the IT side of the IT/OT equation, the ICS world needs a dedicated solution. Using an optimized, non-intrusive network monitoring solution is the best approach to ICS visibility management.

ICS visibility gives OT managers greater insight into the status of loads, DERs and multi-directional flows in real-time, supporting maximum reliability and power quality. The benefits include complete asset transparency, a significant reduction in OT management workloads and costs, lower business risk through cyber and operational incident prevention, fewer power outages for customers, rapid repair and fault resolution and simplified compliance.

As a result, utility companies can make the grid more "secure, reliable, resilient, efficient, interactive and clean", as defined by the Institute for Electric Innovation. Ultimately, optimized asset performance management, enabled by optimized ICS visibility, helps utility businesses leverage all the advantages of IT/OT convergence, while significantly lowering the cost and effort required to achieve true cyber resilience.

Resources

1. "2018 Outlook on Power and Utilities", Deloitte Center for Energy Solutions, 2018
2. "Protecting Industrial Control Systems And Critical Infrastructure From Attack", Forrester Research 2018
3. "Key Trends Driving Change in the Electric Power Industry", The Edison Foundation, Institute for Electric Innovation, 2015
4. "After The Fall: Cost, Causes and Consequences of Unplanned Downtime", Vanson Bourne, 2017
5. "INDEPENDENT STUDY PINPOINTS SIGNIFICANT SCADA /ICS CYBERSECURITY RISKS", Forrester Research for Fortinet 2017
6. "Securing Industrial Control Systems", SANS Institute, 2017
7. "2018 STUDY ON GLOBAL MEGATRENDS IN CYBERSECURITY", Ponemon Institute 2018
8. "Digital Transformation of Industries, Electricity Industry", World Economic Forum in collaboration with Accenture, 2018

About Forescout

Forescout empowers critical infrastructure and manufacturing organizations with the ability to identify, analyze, and respond to industrial threats and flaws, minimizing troubleshooting costs and unexpected downtime. We leverage ICS-specific knowledge and understanding to provide visibility into critical assets and their activity, and detect operational problems and cyber security threats. Our revolutionary and comprehensive network monitoring platform has been successfully deployed by customers worldwide. And, unlike some other providers, we already offer the flexibility and completeness to effectively protect IT and OT assets in multiple industry-specific usage scenarios. In 2018 Forescout was recognized by Frost & Sullivan for its game-changing industrial cybersecurity solution, earning the 2018 Global Customer Value Leadership Award for protecting industrial companies' information/operational technology (IT-OT) system networks against malware and zero-day attacks.

Want to Learn More?

Click here to read more about eyeInspect (formerly SilentDefense) from Forescout and its benefits.

Talk to us today by sending an email to: info-ot@forescout.com

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com

APPENDIX 1

As is often the case when it comes to technical solutions to complex problems like network security management, different solutions use varying approaches to achieve a successful outcome. In the OT environment, some solution elements assume particular importance because the market for ICS visibility management solutions is relatively young, and the flexibility required to address customer-specific circumstances is especially acute. Some of the most important criteria to consider when selecting a solution are outlined below.

- Established track record: When dealing with a topic as sensitive as network security management, you don't want to risk your investment on a vendor that boasts innovation, but may not be around very long. Look for a vendor that has established itself over several years and has dozens of examples of successful installations. These should include large, permanent deployments across multiple industries and geographies. As public references are often difficult to access in the cybersecurity field, ask the vendor if you can speak confidentially to a reference customer in your industry.
- Proven reliability: The best vendors invest in continuous testing and development while simultaneously establishing strong, long-term partnerships with other leading technology vendors.
- Customer-centric multi-dimensional support program: This should encompass intelligence and the distribution of knowledge gained through operation, as well as continuous updates and assistance.
- Seamless integration: A successful integration requires smooth interfaces with enterprise systems, authentication services, ICS solutions, and a wide range of physical virtual and cloud-based IT devices and systems.
- Extensive industrial threat library: The level of protection achievable is largely dependent upon the breadth of the indicators and checks available within the solution. An extensive proprietary library ofz ICS-specific threat indicators, protocol checks, and ICS-specific host vulnerabilities is a must. This supports the identification of the biggest risks and malfunctions within minutes of deployment.
- Continuous, low-effort network monitoring and threat detection: Monitoring of external and internal device communications and protocols in real time, within the context of security policies for threat and anomaly protection, as well as easy-to-use policy customization.
- Flexible deployment: Fast implementation in hardware and/or software with minimal training and centralized management is essential for rapid ROI.
- Advanced capabilities: These include the ability to identify nested devices, automatic fingerprinting of devices and protocols, broad coverage of the cyber kill chain, patented anomaly detection and SDKs for run-time product customizations that enable maximum flexibility.
- Optional non-intrusive active modules which can query specific nodes more extensively to gain additional information. These modules enable Enhanced Asset Visibility with comprehensive but non-intrusively developed inventories that include but are not limited to: host status, OS Version, manufacturer, software and applications, serial numbers, network user behavior and installed patches. Selective scanning also allows for Multi-Factor Threat Detection. This effectively enables real-time search for information such as vulnerabilities, active services, dangerous files and known malicious hashes, in a non-intrusive manner.