WHITE PAPER

The Importance of True Visibility Across Information Technology and Operational Technology

Visibility as a Performance Enhancer

Visibility into key performance indicators in information technology (IT) and operational technology (OT) systems allows operators and managers to make informed decisions. Operators need to see metrics that help them determine whether production targets are being met, equipment and applications are performing, and cybersecurity is in place so they can make adjustments in real time to ensure optimum performance and outcomes.

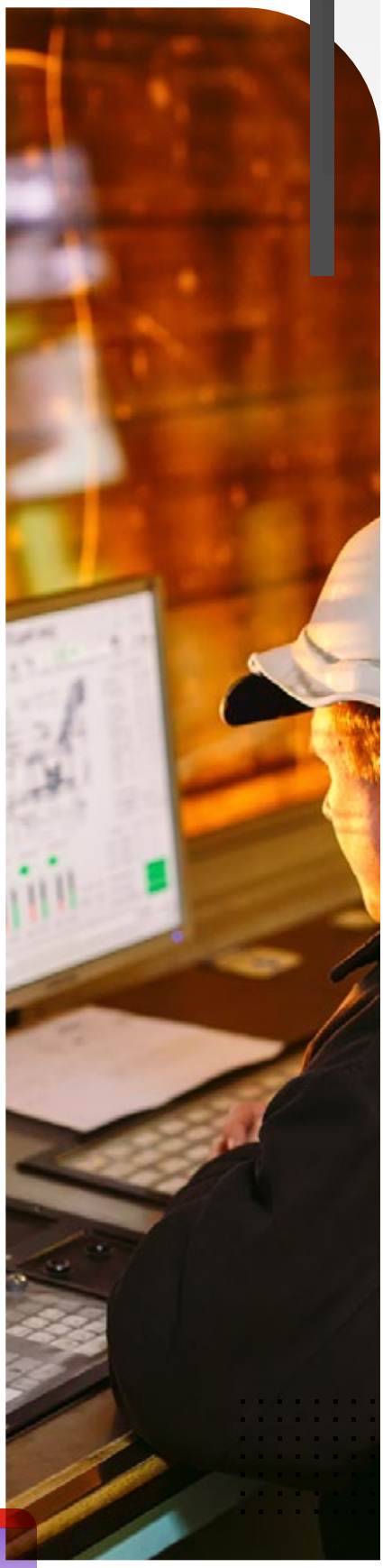
There are many areas of operations where organisations require visibility. All visibility projects should start with a risk assessment to confirm assets in scope, any vulnerabilities to be monitored, and log generation capability. The four key areas that require visibility are: equipment performance; application performance; cybersecurity; and key operating metrics or business performance metrics.

Equipment performance metrics are key indicators that systems are performing at their desired state. In OT systems this is usually done by observing factors such as temperatures, inflow and outflow, pump speed, watts produced, engine speed, tonnes produced, etc.

Control system vendors provide measuring devices and sensors integrated with their systems. Traditionally, most measurements were taken manually, taking time and effort. Now, sensors and/or unit measurement observation can be generated in real or near-real time and be sent to operators for immediate action.

Human-machine interface (HMI) displays can be onsite or controlled via network control rooms and/or operation centres thousands of kilometres away from the operation they control. The key benefit is that operators can monitor if equipment is performing at operational expectations in real time and, if not, act immediately to remediate the situation, without having to be onsite.

Visibility into application performance allows operators to check if the software driving or managing equipment is operating as intended. If equipment is underperforming, it may be necessary to adjust the way applications are being managed. Conversely, over-performance may increase maintenance requirements or reduce intended operational life. In both instances, without visibility over key metrics, the operator will not have the required data to make informed decisions.



Cybersecurity visibility is vital to provide operators with information such as: who has access to key systems; whether the users connected are authorised and authenticated; whether the users are from the expected geo zone; and whether their access is limited to authorised segments.

Cybersecurity teams need access to multiple metrics and correlation rules to understand what their normal operating environment looks like. This level of visibility lets the security team investigate abnormal events.

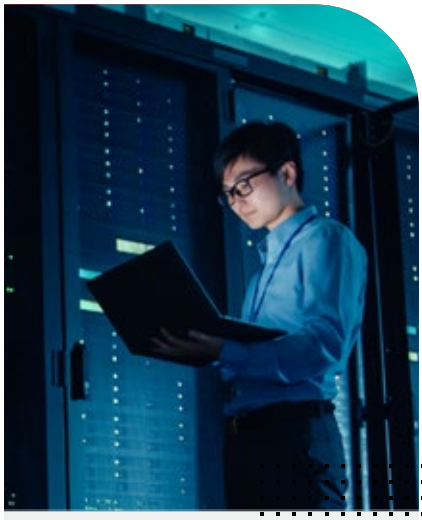
OT operators use key metrics to measure and manage key outputs and operate their environment. For example, metrics such as litres of water stored, information and outflow of water measures, chlorine or fluoride added, tonnes of ore or coal shipped, or items produced on a production line, are key performance indicators and/or business measures.

As OT and critical infrastructure (CI) environments evolve to become more accessible, this creates opportunities for threat actors to compromise or interfere with operations.

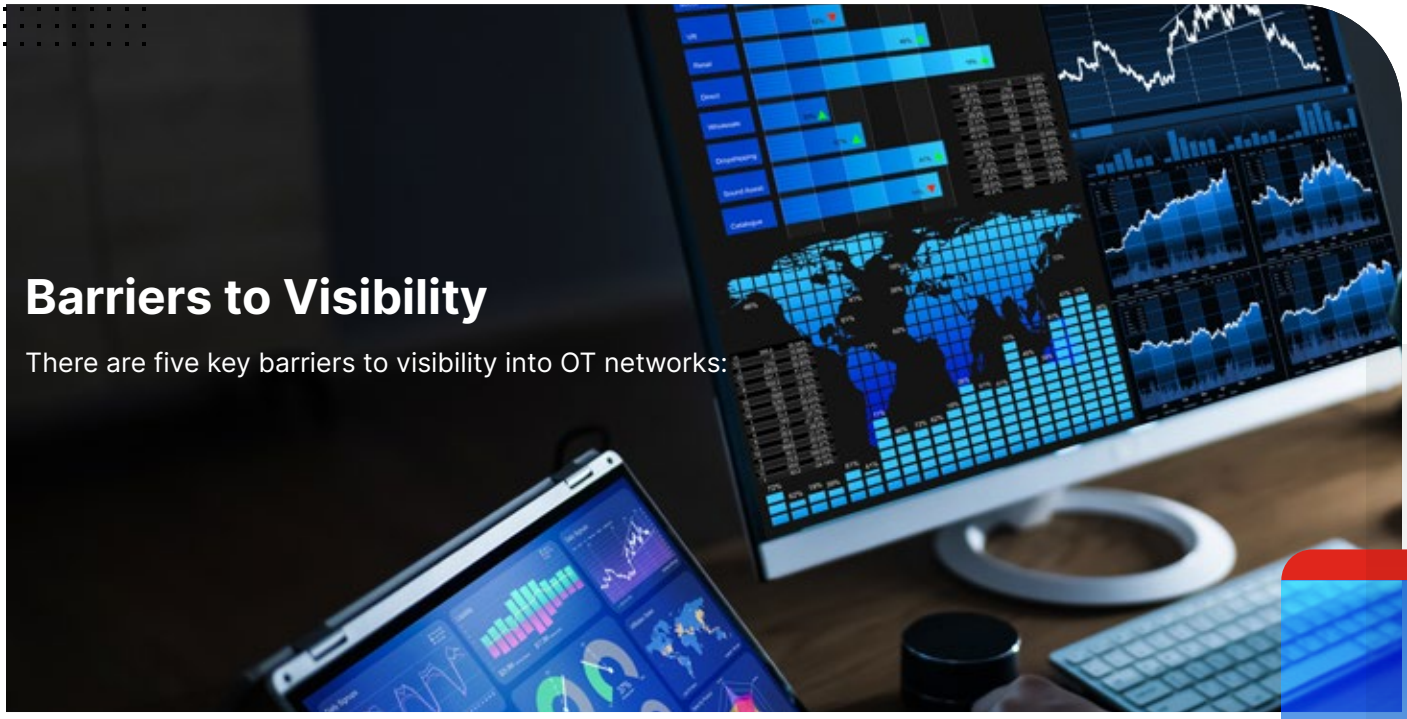
While many organisations have invested substantially in their cybersecurity posture, some have fallen behind and require security programs of work that can uplift their ability to prevent or detect and manage a cyber incident. To this end, the Australian government's *Security Legislation Amendment (Critical Infrastructure) Bill 2020* (Cth), intends to ensure organisations that are operators of CI have sufficient cybersecurity measures in place to protect OT systems.

As parliament prepares to vote on the amendment to the Bill, organisations are getting ready to meet the three main requirements of the Bill by:

- conducting a risk assessment to identify assets, confirm vulnerability status, and document a program of work to achieve a desired state of capability and maturity
- ensuring visibility across the architecture to be able to detect a cybersecurity incident. And, having an incident response plan that documents the process of managing incidents and how to re-establish normal operations
- establishing reporting capability to be able to report to government when required.



Cybersecurity teams need access to multiple metrics and correlation rules to understand what their normal operating environment looks like.



Barriers to Visibility

There are five key barriers to visibility into OT networks:

1. Complexity

IT equipment and software has a lifespan of just a few years. Systems are regularly upgraded and patched, then modernised in line with the organisation's growth. As such, most organisations can be relatively confident that their systems are protected by and compatible with the latest information security tools.

By contrast, OT equipment is built to last. Many OT systems have a lifespan of decades, which means there are many legacy OT systems in operation today that were deployed before the concept of OT security became known.

This complexity is compounded by the fact that most organisations have a mix of OT systems and devices at various sites, at different stages in their lifecycles, and from a myriad of providers. This may preclude a one-size-fits-all approach to visibility.

2. Uniqueness

Most OT uses software and protocols that are unique to that vendor and system and may not be able to be managed or monitored using traditional IT security tools. Even when OT systems are connected to the organisation's IT network, it may be impossible to gain a level of visibility that would make it possible to protect the system, even with some of the latest detection and monitoring tools.

It may be impossible to gain a level of visibility that would make it possible to protect the system, even with some of the latest detection and monitoring tools.

3. Criticality

The criticality of OT systems can't be overstated, even within a CI provider. In many cases, just a few minutes of downtime could be devastating. These systems must remain available and perform according to their specifications. Moreover, these systems are usually not robust enough when it comes to bandwidth. This means that deploying a vulnerability scanning system intended for IT networks could be so disruptive as to cause an OT device to fail. Since this is usually unacceptable, the cost of securing these critical systems can become substantial.

4. Access

Organisations are increasingly relying on remote access connections to monitor and manage OT systems so that workers don't have to be onsite to make changes. These remote sessions can provide an entry point for cyberattackers and are difficult to monitor effectively.

Supervisory control and data acquisition (SCADA) systems were created to be open and easy to access. When SCADA systems were not connected to the network, this openness delivered ease of use and efficiency benefits; however, today's network connectivity has increased risk. Moreover, monitoring SCADA systems can be challenging, and updates are few and far between. Over time, more devices are connected to SCADA systems, creating a technology sprawl that is often hard to track and even harder to secure.

5. Culture

Many organisations still consider cybersecurity to be an IT problem instead of a whole-of-business concern. Without a strong cybersecurity culture in place, driven from the top and permeating all levels of the business, it can be difficult to extend security to cover OT systems. It's important to classify cybersecurity as a risk area and incorporate it into the organisation's risk framework similar to how a strong culture of health and safety has become an essential requirement for CI operators.

Training and accountability are key to an organisation's cybersecurity culture. It's vital to determine who will have accountability for keeping OT systems secure and what resources they can call on to do this. Without transparency over accountability and resources, cybersecurity becomes everyone's problem and no one's problem at the same time, making it hard to develop and implement a consistent approach.

Many organisations still consider cybersecurity to be an IT problem instead of a whole-of-business concern.

Overcoming Barriers to Visibility

Converged networks require a unified approach to security. Too often, one team is responsible for IT security while another is responsible for managing OT. This means each team is only managing half of the network and, even if the teams collaborate relatively effectively, blind spots can emerge.

It's important for organisations to work through six key steps to managing OT security:

1. Identify, classify, and prioritise assets through a risk assessment.
2. Develop an overall strategy that aims to meet IT and OT in a converged state.
3. Segment the network dynamically and develop a security architecture and documentation.
4. Implement and test cybersecurity solutions.
5. Conduct monitoring and develop incident response (IR) capability.
6. Conduct training to improve awareness and develop internal policies and procedures.

Organisations concerned about OT security should consider a security fabric approach that delivers visibility, continuous monitoring, and management capability.

Visibility and Continuous Monitoring

Visibility into the network is an essential part of securing OT and CI. This includes being able to detect any device connecting to the IT-OT network from any location, then determining the degree of trust allocated to that device. Visibility should also encompass traffic so that security teams can determine what activity is happening regarding traffic, ports, protocols, applications, and services.

Once the organisation has visibility into the entire network with no dark spots, it will become possible to detect and manage issues in real time as they occur.

No security posture is a set-and-forget proposition and it's essential to continuously monitor the activity on the IT-OT network to identify malicious behaviour. Effective monitoring means continually analysing behaviours to determine what falls outside the usual patterns and benchmarks and could, therefore, indicate an attack. This should be automated wherever possible to minimise the amount of human effort and involvement required.

Once the organisation has visibility into the entire network with no dark spots, it will become possible to detect and manage issues in real time as they occur.

Using machine learning and artificial intelligence lets an organisation build deep knowledge and statistical confirmation of what a normal operating environment looks like. Once the normal operating zone is established, alerting can be customised to only report events that occur outside of the normal zone to minimise false positives and increase efficiency. Organisations will need time to build, test, and manage this level of visibility and proactive management in real time.

Managing SCADA Systems

SCADA systems create a raft of vulnerabilities and should be managed as part of an OT security strategy. A tailored solution can include a mix of OT-specific security solutions and threat protection for corporate IT environments to ensure the entire organisation is protected. OT-specific security systems are essential for SCADA protection because they provide the visibility, control, and continuous monitoring that is required for an effective security posture.

The Way Forward

OT systems present significant challenges in terms of establishing visibility and control. Organisations need to proactively approach these challenges or risk falling victim to hazardous and costly cyberattacks.

Visibility, control, and continuous monitoring are essential parts of an OT security program.

CI operators should act now to gain visibility and control over their OT systems. To secure their future, CI operators should choose a cybersecurity partner with extensive experience in OT and CI environments with the ability to provide a cohesive security fabric that delivers the visibility and control required to protect OT systems.

Fortinet's security fabric approach integrates a broad set of automated solutions that work together to deliver state-of-the-art security operations. Together, these solutions create a comprehensive, reliable, and cost-effective approach to protect the entire organisation, including OT systems. By adding a security fabric strategy, CI operators can lower the risk of undetected security vulnerabilities and leverage the power of automated solutions to achieve a more secure state.