White Paper

OT Visibility:

Key Considerations

What is OT visibility?

OT Visibility is the critical capability of gaining comprehensive insights into the operational technology (OT) landscape of an organisation. It involves a holistic view of all assets, processes, and protocols within industrial environments, ensuring that every element is visible, understood, and monitored. OT Visibility is an essential foundation for enhancing cybersecurity, optimising performance and ensuring the safety and reliability of OT systems.

Benefits of OT visibility

OT Visibility provides valuable tools for regulatory compliance, maintenance efficiency, and incident response time. By providing a comprehensive view of operational technology assets and their associated risks, it enables organisations to meet industry compliance requirements and avoid costly penalties.

Early threat detection

OT Visibility acts as a proactive defence, identifying security threats in their infancy, preventing potential damage, and minimising costly downtime.

Business optimisation

OT Visibility aligns operational technology processes with overarching business objectives, bolstering productivity, sustainability, overall equipment effectiveness, and competitiveness.

Safety assurance

By safeguarding critical networks against threat actors, OT Visibility plays a pivotal role in ensuring the safety and uninterrupted operations of industrial environments.

Harnessing technological advancements

OT Visibility empowers organisations to seamlessly adopt emerging technologies like cloud computing and digital twin technology, harnessing their benefits while maintaining robust security measures.

Real-world impact

Real-world examples demonstrate the tangible impact of OT Visibility, allowing organisations to identify vulnerabilities, implement remediation plans, and proactively prevent security incidents.

Innovative solutions enhanced

Advanced technologies such as Virtual Edge and 5G are seamlessly integrated, further enhancing system performance and readiness for the evolving technological landscape.

Competitive advantage

OT Visibility equips organisations with a competitive edge by ensuring compliance, sustainability, and enhanced overall efficiency, paving the way for a brighter future for businesses and societies alike.

Escalating threat landscape in OT environments

Increasing connectivity of OT environments has created a brand-new attack surface that is reflected in recent threat attack reports. The UK National Cyber Strategy highlights that ransomware has now become the most significant cyber threat facing the UK. Attacks and other security interruptions cannot be overlooked in OT due to the costs of downtime and the possibility of damage to equipment and the environment and the ever-present concern of safety impacts. This is especially relevant as Gartner suggests that by 2025 malicious cyber attackers are likely to weaponise OT creating physical damage and potentially causing harm to human life.

Recognising the evolution of ransomware

Recently UK's HM Treasury reported an interesting finding where they recognised how ransomware has evolved into a serious cybercrime threat to the UK. They referred to NCSC to help mitigate the risk which include filtration however you can only filter, monitor and protect assets that are visible to you. Even now, a significant proportion of businesses do not have good visibility of their assets in OT with companies like Fujitsu continuing to see clients asking for discovery on brownfield sites. Without visibility, companies cannot have assurance in their approach to securing themselves against these risks.

This indicates the importance of OT visibility.

The significance of OT visibility

Many attacks could be prevented by a suite of basic remediations including clear visibility of an organisations whole OT estate to maximise early detection. OT processes are crucial to Organisations' overarching business aims of productivity, sustainability, overall equipment effectiveness, and competitivity as they control the machines that produce the organisation's products or implements their service. Security is key to maximise uptime and maintain safety by protecting networks against threat actors both intentional.

The impact of technological advancements

This is crucial as organisations rush to catch up with technological advancements such as cloud and digital twin technology to take advantage of their business benefits. Introduction of connectivity increases attack surface and increases complexity which makes having a comprehensive system visibility even more crucial.

Although there are existing visibility solutions for OT networks they are often limited, creating a high-risk blind spot which could be resolved with our synergistic solution that leaves room for growth. Assurance cannot be achieved without visibility, as it is impossible to adequately determine if all assets are suitably protected with the appropriate mitigations in place.

Real-world example: enhancing security with OT visibility

This has been proven from our own research conducted with a client in packaging manufacture who has over 200 factories spanning 30 countries. Here it was discovered that they lacked visibility of their OT estate, leaving them vulnerable.

We carried out an OT asset discovery and OT cyber security assessment to provide visibility of the estate and implemented ServiceNow to help them make use of their OT asset data. During our security assessment, we found that over 30% of OT assets were exposed to vulnerabilities of high severity, so we put in place remediation plans to address them. With end-to-end visibility of OT assets, from the shop floor to C-Level enterprise operations, we were able to help our client detect and remediate security issues before they impacted operations. Visibility and the control of assets and identities being at the heart of production is a prerequisite for successful digitisation.

Innovative solutions for enhanced visibility

This was implemented using Virtual Edge technology hosting IDS to identify information about OT assets including manufacturer, model, operating system version, vulnerabilities, and its context within the network.

Additionally, we recognise that it's important to capture OT site personnel's knowledge of the system into the data capture as they are often using undocumented processes and excellent system knowledge to remediate issues before they impact operations. This information can give knowledge of additional systems which are not connected to the main system including contextual information regarding processes that are used to support operational resilience.

This is important as it allows personnel to continue focusing on their individual role in the organisation and alleviate the pressure of them performing a dual role as a security measure via enabling full visibility.

Fujitsu's forward-thinking technological advancements

This solution's performance can be further enhanced using Fujitsu's own unique values with our solution being space efficient, cost efficient and energy efficient. We have also invested in our virtual edge technology that has potential capabilities within digital twin technology and 5G technology to enable smart manufacturing. We are ready for the present and prepared for the future as 5G will extend the future use of blockchains and edge computing and increase the efficiency of data processing and the confidence about the functioning of the supply chain.

OT's significant increase in connectivity is met with an even steeper interest from threat actors as operational environments become tempting targets as geopolitical tensions continue to rise. They are tempting because of the impact and the ease of compromise.

Our role is to ensure a seamless transition whilst supporting customer growth. We will help each organisation succeed in achieving its business objectives as we aim to maximise overall equipment effectiveness using our competitive advantage with our unique technologies following the compliance standards and with an excellent track record in sustainability. Through innovation and technology, we deliver a brighter future with the peace of mind to our customers and societies around the world.

Checklist: things to look for in an OT visibility solution

When looking for a visibility solution, consider including the following requirements when contacting suppliers or issuing invitations to tender:

- The solution can identify assets and protocols in the industrial space
- The solution provides visibility deep into the process. Consider solutions that can track process variables to determine if they are in normal parameters
- Solution supplier can provide a threat feed to ensure Indicators of Compromise are up to date

- Solution can integrate with your chosen SIEM product for unified management of security events across IT and OT
- The solution can integrate with identity access management solution for secure authenticated role-based access control
- Enough support is available within the organisation or within the supplier to support the maintenance of the solution and to monitor and respond to alerts.
- Solution should support rule-based detection, and support a machine learning solution to alert on traffic outside of normal parameters
- Solution provider should assist in creation of playbooks to assist the triage and treatment of cyber security incidents

About Fujitsu

Our Purpose is to make the world more sustainable by building trust in society through innovation.

To fulfill the Fujitsu Group Purpose, we will enhance our ability to stay in tune with global society, while continuing to make agile changes, and creating value. We offer a broad range of products, services and solutions, and have approximately 130,000 employees supporting customers from over 50 countries and regions.

To find out more about Key Considerations with Operational Technology Visibility, please email askfujitsu@fujitsu.com and/or +44 (0) 1235 79 7711 and quote 4221

Contact
Fujitsu
The Lantern
75 Hampstead Road
London
NW1 2PL

This document is current as of the initial date of publication and subject to be changed by Fujitsu without notice. This material is provided for information purposes only and Fujitsu assumes no liability related to its use.