Deloitte.

Operational Technology Tools
Enhancing Site Resilience

Resilience of Operational Technology (OT) environments are becoming increasingly reliant on security tooling. The adoption of dedicated tooling provides enhanced security and improved visibility of the OT estate aiding early identification of potential issues against baselines. Deployed properly, OT tools provide you with the right data to support good decision-making, process optimisation, day-to-day management of the technology estate, and enable effective lifecycle and risk management. To maximise benefits and optimise investment, selection and deployment of tooling should align to organisational strategic need, architectural good practices, consider built-in resilience and be accessible by the right people, at the right time, and in the right place.

Organisational strategic need

Tooling selection and deployment in the OT estate should align with the organisation's strategic need. OT tooling provides a near real-time view of assets for effective risk management. A set of requirements to meet should be defined and assessed against. Organisations should consider whether to extend existing capability and coverage of IT tooling or use dedicated OT tooling, taking a view from key stakeholders across the business.

Architectural good practices

Many tool deployments in OT estates struggle to achieve the desired objectives and coverage due to architectural constraints. Limitations may also result from the perceived risk to operations resulting from a deployment. It is vital that designs meet current needs and account for future capability and integrations. This ensures tools can be enhanced and expanded with minimal architectural changes in the future.

Built-in resilience

OT tooling is increasingly implemented centrally and inaccessible by local sites when the central network is down or disconnected. By making these tools available to onsite personnel, operational resilience is enhanced with overheads and workloads minimised. Site resilience is enhanced as sites are provided with an understanding of their environment that can help prevent and support the response to a cyber incident. Each site can support itself without the constraint of central IT.

Provide appropriate access to tooling

Providing the right people, both on site and across the enterprise, with appropriate access will ensure that OT tooling is fully leveraged. When deploying, it is important to consider who requires access, what type of access is needed and when will they access it. Without appropriate access and visibility of your OT estate, there is an operational risk that sub-optimal decisions are made that could contribute to increased downtime during an incident, and full benefits from investment are not realised.

Examples of tools deployed in an OT estate

OT Tools

1. Asset Management
2. Vulnerability Management
3. OT Monitoring
4. Backup & Recovery Management
5. Remote Access & File Transfer
6. Endpoint Protection
7. Network Security

Tooling usage delivers:

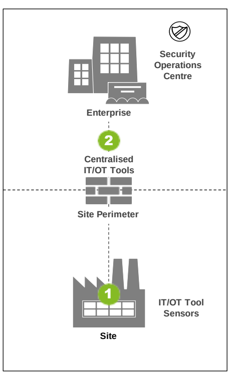
- ❑ Uplift in organisational security in a consistent and repeatable manner.
- ❑ Centralised and site OT estate understanding to aid risk management and decision making.
- ❑ Visibility, monitoring and logging of assets, performance, and events.
- ❑ Capability to protect assets through hardening of systems.
- ❑ Recovery capability with minimised potential for downtime in the event of a cyber incident.
- ❑ Secure, timely remote support and file transfer capability to limit production outage.

Deploy according to your needs

The needs of an organisation for OT tooling will vary and depend heavily on where they are on their digital or cyber security transformation journey. Deployment in industrial environments are affected by different architectures across sites and regions of operation and types of systems on the shopfloor. Increasing convergence means enterprise technology is also a factor.

Centralised architecture without resilience

Centralised architecture without site resilience takes the data from the sensors or appliances installed in the OT environment at sites passing data through the firewall to deliver visibility to the enterprise interface.



Numbered components

1. OT Tool Sensor: installed at sites to gather information on the OT challenge being addressed
2. Centralised OT Interface: interface installed at Enterprise level for visibility of information from the OT tool sensor

Pros

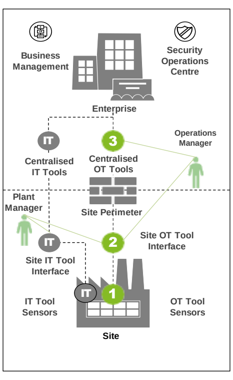
1. Enterprise visibility
2. Less configuration of technology

Cons

1. Enterprise does not understand site OT/asset
2. Enterprise cannot maintain data integrity for sites
3. Not available for site use during enterprise outage
4. Management overhead of information requests

Centralised architecture with resilience

Centralised architecture with site resilience takes the data from the sensors or appliances installed in the OT environment, aggregates it for site visibility at the site interface, then pushes available data to the enterprise interface.



Numbered components

1. OT Tool Sensor: installed at sites to gather information on the OT challenge being addressed
2. Site OT Tool Interface: interface installed at site for visibility of information from the OT tool sensor
3. Centralised OT Tool Interface: interface installed at Enterprise level for visibility of information from the OT tool sensor

Pros

1. Site visibility
2. Enterprise visibility
3. Availability during enterprise outage / island mode operation
4. Site ownership and accountability of data/ information integrity
5. Site responsibility to act on alerts

Cons

1. Additional configuration of the site tool interface

There are a set of **good practices that should be considered** when selecting and deploying OT tooling.

Review existing capabilities

Current tools, coverage, and compatibility with the OT estate should be checked for reusability. Consider usability, existing partners and pricing models when shortlisting options.

Architect for best coverage

The architecture and deployment should give the best coverage of the assets and have built in site resilience. It should be designed with the management in mind.

Develop and sign off requirements

A set of requirements that the tool must, should or could meet should be developed and signed off by stakeholders. Engineering and security teams should be consulted as part of the process.

Develop and agree post deployment activities

The tools should not be deployed and left like an artefact, post deployment activities should be defined with roles and responsibilities clearly state. One activity that must not be missed is the tuning of the tool for continuous benefit.

Options and compatibility with your environment

Check out the various solutions and vendors in the market for compatibility with your objectives, OT environment, business integrations, licence model etc.

During an incident, our clients have been reliant on tools. Lack of local/site visibility has impacted the ability of the central organisation to effectively respond. While designing and implementing tools, this should be considered early on to improve response capability, should it be needed. Design for resilience enables sites to be engaged actively in the management of their cyber security risk supporting the organisation's cyber security goals.

How can Deloitte help?

Our team combines technology and engineering expertise with business strategic skills that allow us to be a unique partner for the whole IT and OT transformation journey

- Best in class advisory **in OT tool deployment**, with a proven methodology from assessment to design and implementation.
- **Unique technology and engineering offerings**, with strong track record in OT cyber risk advisory and transformation.
- Multidisciplinary specialised teams, which combine the high technical expertise with **business and strategic consulting teams.**

Contact

Sydney Grenzebach
Partner, Cyber
sgrenzebach@deloitte.co.uk

Anna Burrell
Director, Cyber
aburrell@deloitte.co.uk

Jonathan Lam
Senior Manager, Cyber
jdlam@deloitte.co.uk

Special thanks to those that also contributed to this publication:

Daniel Segun Usman, Moojan Pordelkhaki, and Shanaia Saju

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte LLP accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte LLP is a limited liability partnership registered in England and Wales with registered number OC303675 and its registered office at 1 New Street Square, London, EC4A 3HQ, United Kingdom.

Deloitte LLP is the United Kingdom affiliate of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NSE LLP do not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.