Deloitte.

Zero Trust implementation in operational technology

Navigating the Zero Trust journey for industrial environments

MAKING AN IMPACT THAT MATTERS since 1845

As businesses navigate the move from digital transformation to hyperconnectivity, the need for robust security has intensified. This has led to the widespread adoption of Zero Trust architectures in IT, a stark contrast to its relative obscurity in the late 2010s.

The successful implementation of Zero Trust in IT is paving the way for its adoption in Operational Technology (OT). However, practitioners recognise the considerable difficulties in applying this security model to the critical technologies that keep businesses running.

The key question is: 'Is it justified to implement Zero Trust into OT environments?' In this paper, we explore the benefits and challenges with implementation and use the Deloitte Zero Trust Framework to define what is possible.

What's inside

1. Helping you navigate the Zero Trust journey

The pursuit of operational efficiency and cost savings fuels continuous technological change and advancement. The adoption of Zero Trust in IT environments to secure and enable these changes delivers a flexible and modern approach. To create value from Zero Trust investment in OT, businesses must first understand the applicability to their industrial environment and how to implement with confidence.

1.1 Embarking on a Zero Trust journey

The Zero Trust model has exploded in popularity especially over the last five years, as a more robust and new way of thinking about security, and as an enabling framework which re-defines how and where technology resources, are consumed.

Key drivers for adoption include:

OT automates and manages physical processes in critical industries and infrastructure, prioritising real-time operations, safety, and reliability. Disruptions to this technology and supporting infrastructure in sectors including energy, utilities, manufacturing, and transportation can severely impact critical services and supply chains.

The shift toward Zero Trust in OT is being accelerated by:

1. **Increasing migration of OT** services to the cloud and the use of AI. Organisations to carefully consider how access is controlled and enforced, and that OT considerations and good practice are applied to meet regulatory and business needs.
2. **Increased connectivity and dependencies** between networks, coupled with hybrid workforces and third-party access. This expands the attack surface and elevates security risks for both environments, particularly in OT where additional security considerations apply.
3. **Convergence of services and changing operating models** that bring IT teams and approaches deeper into OT and shopfloor architecture and risk management decisions. This is motivated by the pursuit of cost efficiencies, improved resilience, standardised processes, and centralized security.

Zero Trust is based on the principles of **'never trust, always verify'**. This principle complements the requirements to ensure OT cyber security controls are implemented **to maintain** the **safety, quality, and reliability** of operations while preserving the availability, integrity and confidentiality of the industrial control systems and their data.

1.2 The need to secure the new era of connected OT systems

As part of the digitalisation journey (including machine learning and AI), organisations can develop smart factories capable of increased manufacturing efficiencies; build more sustainable smart cities; connect OT locations in renewable energy production and secure remote access for a hybrid workforce and remote maintenance providers. The convergence between IT and OT needed to enable hyperconnectivity has enabled the business. It has also introduced a potential pathway for attackers to move between environments, for example, from a breached IT environment to OT and vice versa.

Hyperconnectivity driven by greater volumes of captured data, integration of modern IP-based protocols, and adoption of IoT and 5G, increases internal and external security threats.

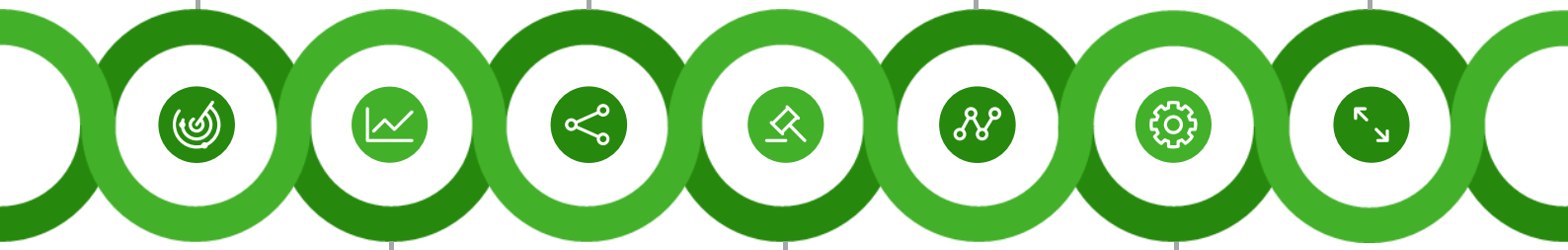
This new era of OT connectivity brings new benefits:

Real-time visibility
Allowing operators, management and decision makers further afield to monitor processes, machinery and sensors.

Inventory and supply chain management
Providing up-to-date information on inventory levels and supply chain activities, incl. controls for remote support.

Robust data analytics
Allowing organisations to analyse operational data and track performance metrics such as sustainability and environmental impacts.

Scalability and flexibility
To accommodate changing organisational needs and adapt to evolving industry requirements.



Enhance production efficiency
Integrating and automating processes to reduce manual efforts and eliminate redundant tasks.

Maintaining regulatory compliance
Generating documentation and reporting with greater accuracy and efficiency.

Integration with enterprise business systems
Creating streamlined workflows, reducing manual data entry, optimising spend, and enhancing collaboration.

The where, what, and when to implement Zero Trust while working around the technical limitations of OT is a fundamental challenge. It is important to gain an understanding of why it is relevant in OT when for many it has mostly been associated with IT transformation.

1.3 How can Zero Trust help you?

Taking a Zero Trust approach manages risk by focusing on verifying every user, device, and workload regardless of their location and granting each request only as needed.

Zero Trust is a combination of capabilities that can be implemented as a holistic strategy or part of a transitional journey. When integrated well in OT environments, these can yield significant security and operational benefits.

Practical benefits of a Zero Trust approach to secure OT connectivity:

Supply chain risk	Reduce risk of third-party compromise with secure remote and least privilege access for third party access to systems.
Identity check	Improved access with more granular based controls management tied with right to access checks.
Increased verification	Frequently verify the identity, permissions and security posture of devices accessing the network or applications throughout their lifecycle.
Cloud enablement	Support secure implementation of digital solutions and cloud migration for OT services.
Breach containment	Limit impact of a breach by dynamically restricting or blocking access to critical systems or network segments quickly to minimise loss.
Network segmentation	Enforce strict control on the communication between the segments limiting lateral movement dividing networks into smaller, managed segments.
Asset visibility	The journey provides a deeper understanding of devices on the network and communications between systems which may identify shadow IT / IoT.

Implementing Zero Trust requires careful consideration of the differences between IT and OT environments. A robust security posture must balance the benefits of Zero Trust with the risks of new technologies and third-party dependencies, while integrating relevant principles with OT good practice. Practical application demands careful planning to address the security needs of both IT and OT.

2. Zero Trust challenges in OT

A robust security posture must balance the benefits of Zero Trust with the risks of new technologies and third-party dependencies, while integrating with OT standards.

2.1 Challenges of implementing Zero Trust in OT

Despite ongoing standardisation efforts, OT deployments remain highly variable across different sites. Multiple original equipment manufacturer (OEM) systems, often integrated locally to meet local asset owner and business needs, rely on non-corporate networks and third-party providers. These create significant technological challenges to implementation, especially when migrating from traditional defence-in-depth security models. A cost-benefit analysis, aligned with OT security best practices, is essential to assess deployment and operational costs against security improvements. Brownfield and remote sites with non-standard technologies present further complexities.

Main challenges organisations face during implementation:

Strategic fit and alignment	Implementing new security measures requires employees to embrace change and apply previously considered IT concepts within the OT environment. Change can be complex and risks operational impact, making the correct strategy and starting point fundamental for organisations wanting to adopt Zero Trust in OT. Where IT teams design and manage OT, a key challenge is ensuring that OT requirements are included and the relevant policies applied. Conversely, where OT teams manage their own systems, the approach should align with the overall Enterprise Architecture and Technology Strategy.
System requirements	Zero Trust within OT environments presents unique challenges due to real-time operational requirements for health, safety, environment, quality, and production. New technologies must avoid intolerable disruptions, such as latency impacting safety and operations. Legacy systems in brownfield sites and lower-level systems may lack the technical and computational resources needed for Zero Trust solutions, including logging, monitoring, and implementation of Policy Enforcement Points (PEPs). The reliance of many PEPs on internet connectivity further complicates implementation in isolated or bandwidth-constrained environments.
Verification	Many OT devices lack self-authentication capabilities and human identities, instead relying on inherent network trust, directly contradicting the Zero Trust principle of "never trust, always verify“. The prevalent use of shared and local accounts for system users and third parties, often assigned at group, role or responsibility level, weakens application of least privilege within OT. Furthermore, the time-bound nature of industrial work permits further complicates the continuous verification required by Zero Trust deployments.
Scalability	OT systems are often purpose-built resulting in unique architectural and technical variations. Scaling a Zero Trust solution to cover a complex, diverse OT environment requires careful planning and consideration of unique use cases. Brownfield sites may use several vendors and proprietary protocols that are incompatible with standard security policies and PEPs. A combination of Multi-Protocol Label Switching, third-party providers, and vendor solutions are used for connectivity which can be difficult to modify. Architectural variation, such as both local and centralised DMZs or varying vendor designs further complicate end-to-end Zero Trust.
More than technology	No single vendor can provide a complete Zero Trust solution. Achieving Zero Trust in OT environments necessitates a multi-faceted approach. Success hinges on a robust combination of people, processes, and technologies. This requires strong cross-functional partnerships between IT and OT teams, meticulous planning, and careful alignment across the business. Crucially, factors such as regulatory compliance (e.g. NERC CIP, NIS, GXP) can significantly impact technology selection and implementation, as architecture decisions can affect certification and operating licenses, or lead to fines.

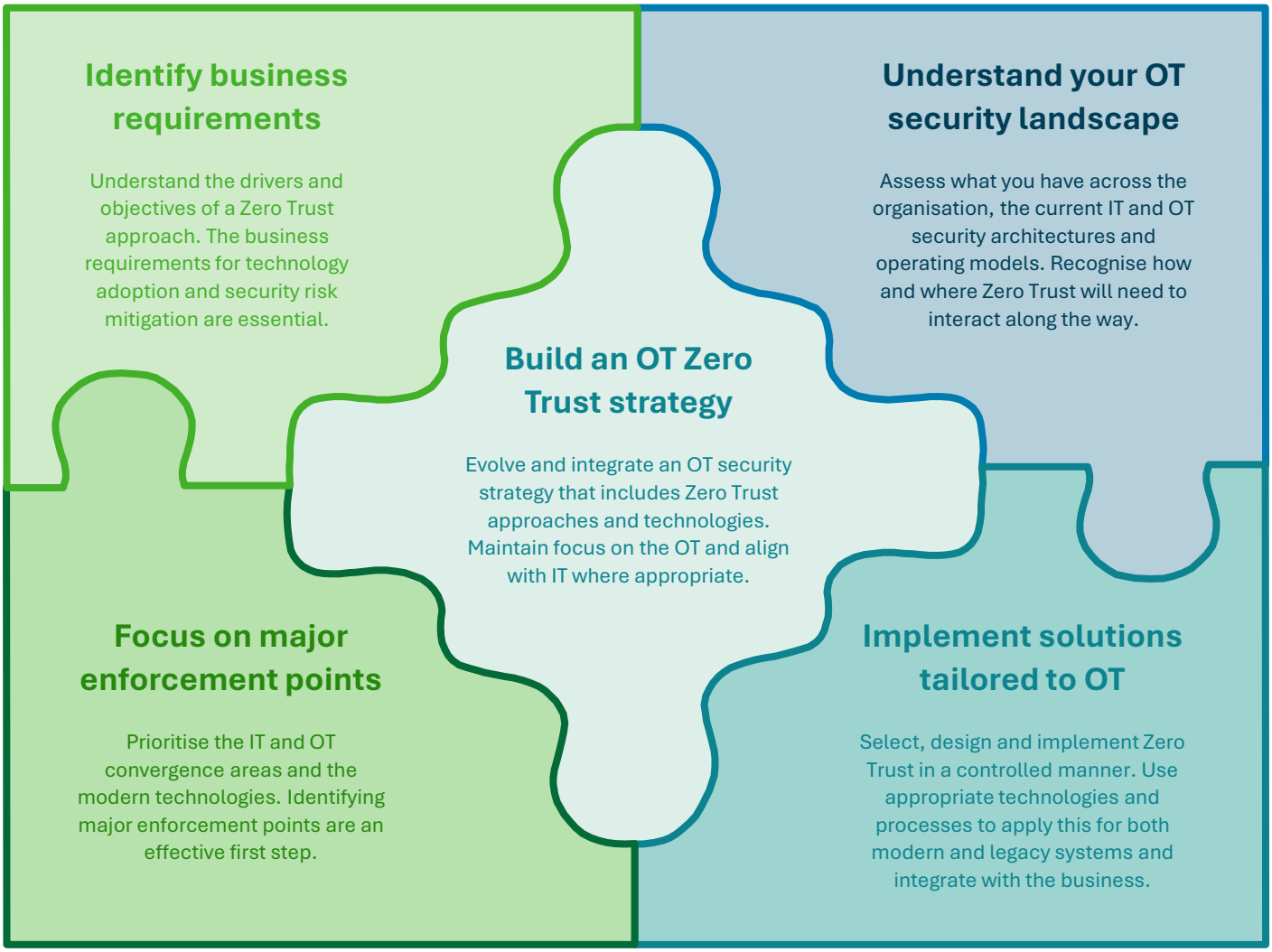
3. A strategic approach to Zero Trust in OT

Adopting Zero Trust principles requires adjustments to people, process, and technology to effectively safeguard modern OT environments. Achieving complete coverage across the entire estate presents challenges and may not always be feasible. Embracing a strategic and adaptable approach is crucial to effectively realise its benefits.

3.1 Key steps on your implementation journey

Zero trust implementation considers the unique business structure, industry demands, and existing technology landscape. Organisations should tailor the specific where, what, and when to implement this for their business.

It is necessary to overcome the challenges and realise the benefits of increased connectivity in OT. There are ways to innovate and deploy Zero Trust to secure OT environments while maintaining operational resilience, reliability and performance. It is not a single solution but a security model that can integrate into the existing security frameworks to enhance security posture and adapt to different environments, risk profiles and business objectives. Organisations that have already adopted international standards for industrial security are likely already implementing principles aligned to Zero Trust.



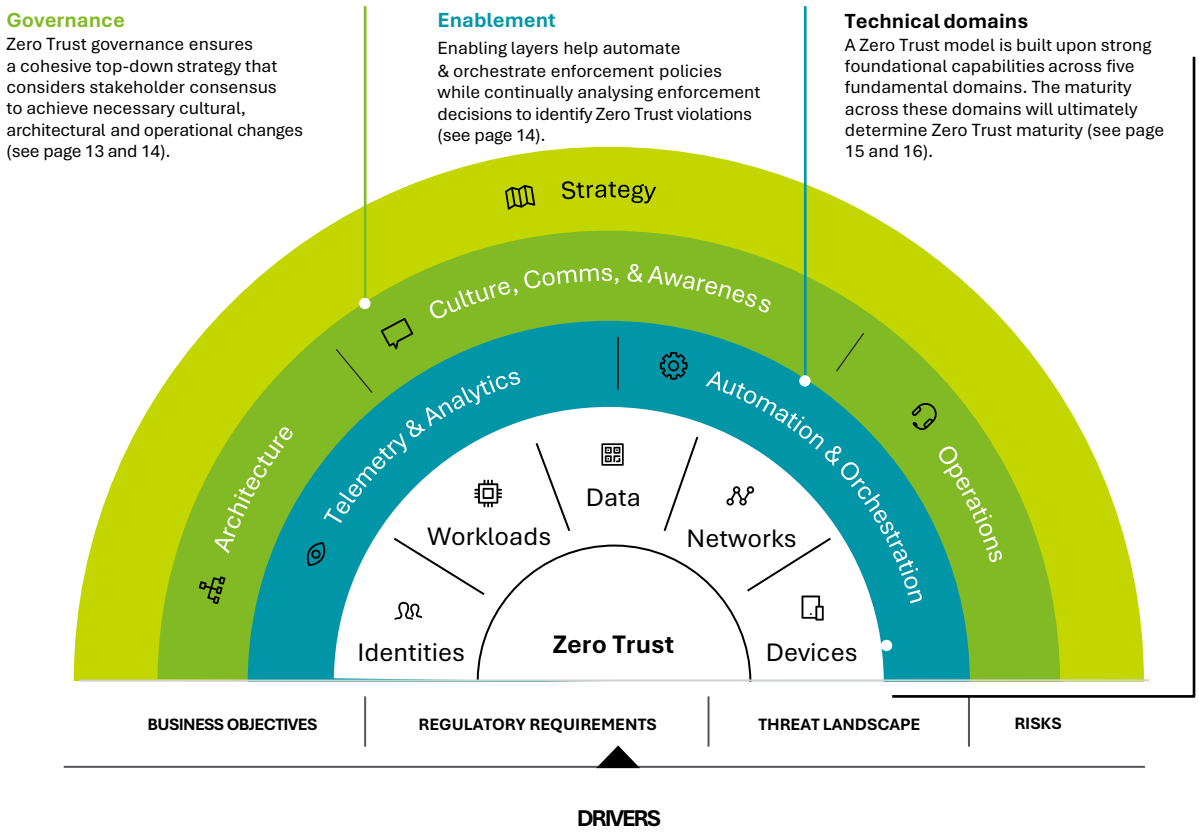
3.2 Deloitte Zero Trust Framework

Our tried and tested framework for implementing Zero Trust in organisations considers all aspects and guides the journey. The Deloitte Zero Trust Framework (DZTF) is informed by relevant cyber security frameworks and aligns with OT security standards to approach adoption in these environments.

The framework formalises the tenets of Zero Trust such as the principle of least privilege and the use of network segmentation to limit potential damage and prevent unauthorised lateral movement.

A common view is that the concept is vague or is simply a technology solution. It is much about unlocking digital capabilities securely, as it is about reframing how one manages cyber risk across the organisation.

The Deloitte Zero Trust Framework is informed by internationally accepted standards including IEC 62443 and NIST 800-82, and leverages cybersecurity frameworks (NIST and CISA) to guide Zero Trust implementation in OT.



3.3 Applying the capabilities for OT environments

The DZTF is a structured way of thinking to deliver a successful initiative. The journey to realise benefits for OT involves understanding these environments and apply this to all the domains during design and implementation. It is an initiative that achieves operational efficiency and cost optimisation and requires technology transformation from strategy through to management and technical implementation.

Implementing Zero Trust requires careful consideration of the differences between IT and OT environments. Practical application demands careful planning to address the security needs of both IT and OT and integration with relevant principles from OT standards.

Governance – Applying security to the management domains for OT

Strategy

Supports business initiatives, encompassing vision, objectives, scope and applicability whilst addressing constraints, risk and operational needs.

To guide adoption, organisations must develop a comprehensive enterprise-wide strategy. This strategy should explicitly address regulatory compliance, ambition, and the alignment of OT security with Zero Trust objectives and overall business goals. It should encompass risk management, compliance practices, reporting mechanisms, and operational considerations.

Prioritisation is crucial, identifying which business units, sites, and technologies will initially benefit from Zero Trust implementation, and which can be addressed later. A thorough cost-benefit analysis should be conducted, alongside preparatory initiatives such as technology simplification and operational standardisation.

Architecture

A robust, mature, and flexible enterprise security architecture enables appropriate risk appetite while incorporating security by design and cutting-edge security solutions.

The architecture must align business processes, information systems, and technology infrastructure with the overall strategy in accordance with industry standards and adoption of enabling technology. It defines the roles and responsibilities for design, implementation, management, and enforcement.

While OT traditionally prioritises resilient architectures, IT/OT convergence is altering risk profiles and dependencies.

Key architectural elements to consider include:

Convergence: Address the integration of tools and technologies where OT infrastructure migrates to the cloud and is increasingly managed by IT or IT/OT teams. Collaboration and knowledge sharing become essential from the outset of design to overcome silos and prepare for new ways of operating.

Tooling: Address the need for tooling that meets OT requirements and supports uninterrupted real-time operation, e.g. employing a trust broker that supports on-premises hosting to mitigate connectivity, integrity, and IT service disruption. “Island mode” designs deliver OT resilience to this.

Preparation: Identify transitional initiatives such as standardisation of site network infrastructure, modernisation of OEM systems and underlying technologies and determining whether to implement integrated solutions or to maintain dedicated OT infrastructure for business units.

Culture, comms and awareness

Manage impact to end user experience through active engagement and embed the principles into the security DNA of the organisation, whilst addressing the cultural change needed for transition.

The clash between OT's safety-first, reliability-focused culture and IT's agile, innovation-driven approach must be managed. Implementing Zero Trust security in highly regulated, critical OT systems (often subject to strict change control and certifications like GXP or SIL) necessitates careful planning and execution to avoid operational disruptions and costly re-certifications.

Across sectors, successful implementation hinges on:

Bridging the cultural divide: Joint training, cross-functional teams, and leadership buy-in aligns objectives and foster collaboration.

User enablement: Embed security and awareness into daily operations to minimise resistance and circumvention of controls, and train OT users on new workflows and technologies e.g. remote access, frequent logins and multi-factor authentication, and stricter access controls.

Skills uplift: Ensure adequate training and expertise are available to manage and maintain new security technologies and respond to incidents effectively

Prioritised implementation: A staged rollout minimises risk and can avoid the need for complete system re-certification.

Operations

Enable IT and OT teams to adapt to the changes caused by a Zero Trust model and facilitate alignment to its core principles through People, Process, and Technology improvements.

The increasing involvement of IT in managing OT infrastructure (e.g. cloud or on-premises) necessitates a reassessment of roles, responsibilities, and operating models. It is important that OT context is provided at all stages to ensure systems stay compliant with relevant regulations or standards.

Effective operations management involves:

Redefining roles and responsibilities: Updates to reflect the shared ownership of IT and OT infrastructure and security. This includes OT representation in relevant IT design authorities and change boards.

Harmonising security operations: Creating joint IT/OT ownership of security processes, including shared visibility into security events and coordinated incident response protocols.

Standardising policies and procedures: Developing consistent policies and procedures that address variations in implementations across different sites and working practices, ensuring a unified approach.

Enablement – Managing Zero Trust security technologies for OT

Telemetry and analytics

Drive visibility across all digital assets to deliver meaningful insight and analytics from different sources of digital infrastructure.

The implementation must use the features of modern tooling to optimise operations and effectively manage the estate. Artificial intelligence and machine learning (AI/ML) based analytics are mature enough to identify policy violations and anomalous access patterns by querying rich and complex datasets, helping protect the business.

Cyber risk management is enhanced by:

OT enablement: Telemetry agents and trust brokers consume user, device and context data, apply external threat intelligence and enforce access policies, these must be tailored appropriately for OT.

Tooling: Combine specialised OT tools and capabilities to identify assets, enhance visibility and gain operational insight. In converged IT/OT environments, these analytics can occur and integrate with an enterprise SIEM system.

Following architecture principles: Adhere to defined guidance. It may be necessary to rely on dedicated Policy Enforcement Points or OT solutions to protect security zones or maintain necessary separation and segmentation.

Automation and orchestration

Enable continuous security and compliance monitoring of digital Infrastructure by deploying automated use cases across the technology domains.

Automation of tasks like security policy enforcement and user provisioning and vulnerability remediation drives operational efficiency, especially when integrating disparate solutions. Orchestration builds on this by optimising workflows for OT and between IT and OT systems.

Leverage modern technologies to:

Manage efficiently: Integration of disparate OT solutions to enhance the ability to automate processes, optimise performance and enhance operational efficiency.

Identify anomalies: Use technology to identify deviations from normal operating baselines, suspicious communication patterns, and potential threats in real-time.

Respond effectively: Allow orchestration of remedial actions for technologies securing OT to enable coordinated responses to security events to shorten incident response times.

Technical capabilities – Applying security to the technology domains

Identities

Identify devices, users and workloads as a fundamental element to manage access.

Robust identity and access management (IDAM) must be implemented. This requires real-time visibility, management control, and potentially the ability to integrate with existing enterprise IT solutions, to deliver continuous verification of OT user and device identities, coupled with granular access controls. Addressing OT constraints is key to achieving this:

Deploy an IAM system: Verify user identities and access privileges throughout their sessions where possible, even for previously authorised actions.

Modernise OT identity solutions: This may involve retrofitting existing systems with dedicated tools, leveraging existing security capabilities, or completely replacing legacy systems with modern, integrated solutions.

Address integration challenges: Utilise specialised connectors, gateways, or middleware to overcome integration difficulties posed by disparate systems and proprietary technologies.

Enforce strong policies: Implement Role-Based Access Control (RBAC) and least privilege principles. Mandate MFA and utilise proxy sessions to remove direct access to critical systems. Implement session recording for traceability.

Select appropriate solutions: Tools must provide effective management of diverse permission groups and access needs, and support for a wide range of OT devices and systems. Prioritise vendor-agnostic solutions with flexible integration capabilities, and Privileged Access Management (PAM) capabilities.

Workloads

Security configurations resolve risks and vulnerabilities while supporting reliable cyber-physical operations.

Applications and services must be hardened to help protect against cyber threats, maintain operational integrity and comply with best practices. Take a proactive approach to make workloads less vulnerable through:

Assessment: Consider the landscape and future technology changes as well as technology limitations and workload constraints (e.g. no non-operational view interruptions on HMIs or maintaining technology independence).

Strengthen workload security: Apply security configurations, firmware and software patches, and install agents or connectors to verify device configurations before granting access. These must adhere to OEM guidelines.

Secure remote access: Implement secure remote access mechanisms with robust authentication to manage and maintain OT systems

Data

Data security to identify and classify sensitive data, encrypt data in transit and at rest, and implement access controls to protect critical systems and sensitive information.

It is essential to safeguard sensitive business information and maintain the integrity of data used for business decisions and process control.

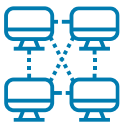
Implement robust data protection measures to prevent breaches through:

Data security measures: Implement data encryption, enforce least privileged based access controls and data loss prevention (DLP) where appropriate.

Technology integration: Leverage the capabilities of access and trust brokers to enhance security and ensure adherence to data protection controls. Enable encryption (e.g. secure protocols) and device protection mechanisms. Carefully consider the impact of these measures on latency, computational power, and bandwidth, prioritising these attributes and OT services where necessary.

Remote access management: Isolate remote access for support and file transfer to enhance security. Perform integrity checks and scan files.

Networks



Utilise public networks, identity-based access and micro perimeter (i.e., software-defined perimeters), instead of virtual private networks and perimeter-based security where appropriate.

Network security improvements must be implemented to mitigate cyber risks associated with lateral movement and unmanaged access. Traditional security measures are often insufficient to address the complexities of interconnected systems, remote access, and the growing reliance on cloud services.

Activate next-gen capabilities and align with industry good practice by:

Strengthen network security: Introduce additional access controls, segmentation and micro-segmentation to create isolated zones and sub-zones. Establish secure communication channels and implement policy-driven access controls. Build on IEC 62443 standards and integrate technologies to enhance security granularity, coverage, and enforcement.

Maintain separation: Enhance existing IT/OT separation using improved iDMZs, firewalling, and incorporate next-generation Zero Trust security capabilities. Implement domain separation, OT-specific policy and OT cloud enclaves to increase resilience and enable centralised services while prioritising critical OT where necessary.

Secure remote environments: Protect non-corporate WANs (e.g., site-to-site MPLS, distributed SCADA) using secure edge capabilities and leverage 5G security features to support containment, and trust brokering. Implement application and protocol-defined remote access for vendors and OT XaaS breakouts, replacing broad access methods, and implement heightened user and behaviour monitoring.

Devices

Assess device health and establish conditional criteria to enable real-time device trust for access to OT environments.

Device security must be elevated which requires implementation of enhanced verification mechanisms regardless of user location or device. Endpoint agents, applications and trust brokers work together to deliver device protections and monitoring capability.

Strengthen device security: Embrace device authentication, assessment of device security posture and security compliance, enforcing least privilege access, and support for device isolation through micro-segmentation. Device protections include host-based firewalls, up-to-date anti-malware software, operating system and application patches.

Operate within constraints: Managing systems with limited agent support or connectivity challenges requires a tailored approach. Standard IT policy and update deployment practices are often unsuitable. Authorisation for all system changes and remote access must remain with onsite engineering and operations teams to mitigate process interruptions, safety risk and other factors, e.g. site held MFA tokens.

Engage with third parties: Clearly defined support arrangements and responsibilities are crucial. Greenfield deployments offer the advantage of selecting and deploying secure devices from the start. Engagement with procurement is essential to ensure standardised configurations, facilitate regular patching, and implement security-by-design.

Regardless of whether leveraging new technologies or undertaking modernisation, a Zero Trust approach should guide decision-making. This prioritises verification of all users, devices, and practices, and enables the monitoring of any anomalous activity. OT environments are inherently static and predictable due to the long operational lifecycles of cyber-physical systems (CPS); this makes detection easier and as systems are updated.

4. Conclusion – An enabling approach

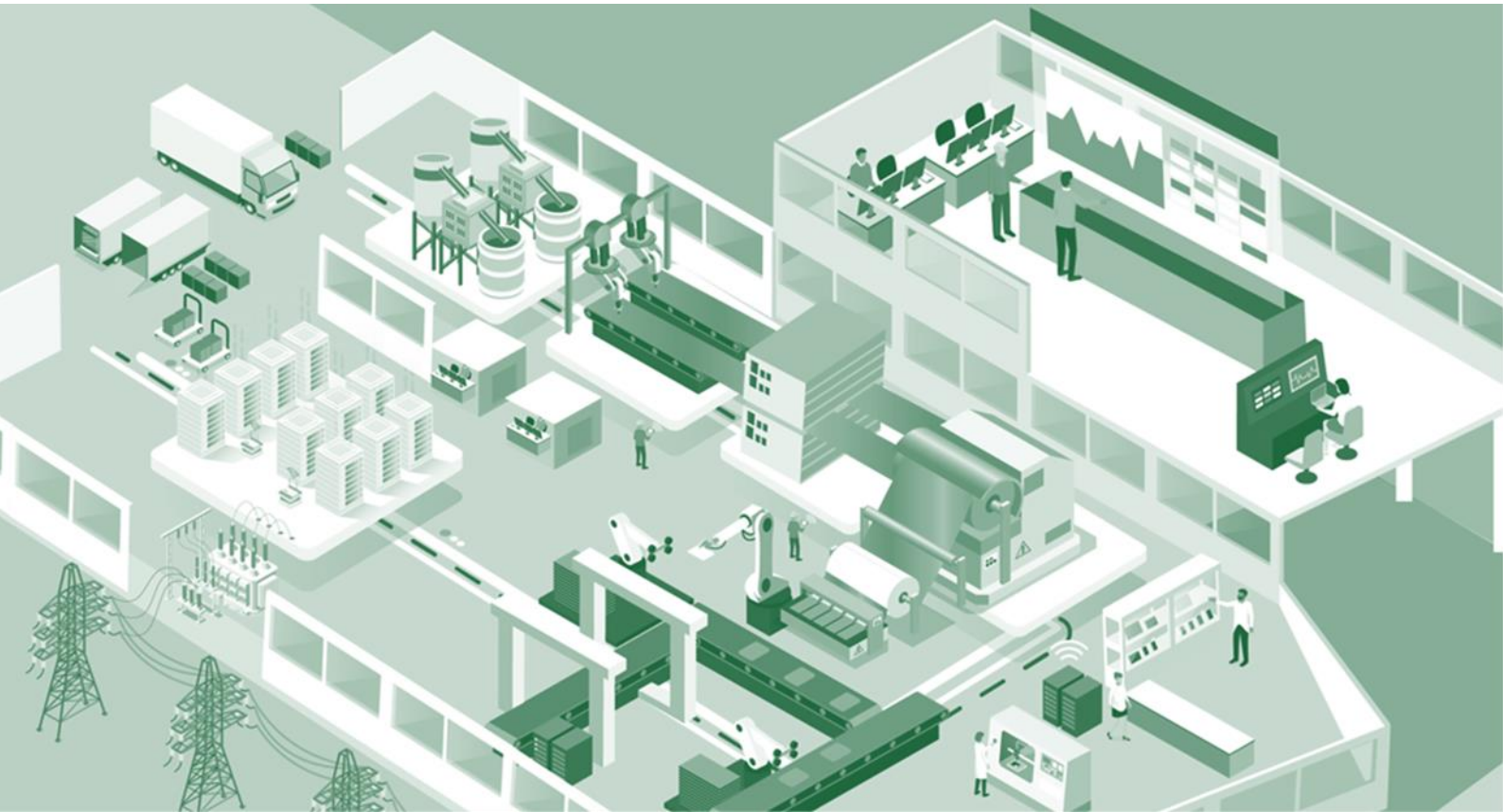
Zero Trust adoption within operational technology (OT) environments doesn't necessitate a complete system overhaul. Many organisations already possess foundational cybersecurity elements compatible with a Zero Trust framework. A successful OT Zero Trust implementation leverages and enhances existing capabilities through integration and strategic additions of next-generation technologies tailored to the unique characteristics and constraints of OT systems.

Zero Trust adoption will continue in OT environments to support ongoing digital and cloud migration trends, as well as providing a stronger security model. However, this needs to be a more considered journey than in the enterprise network, and the implementation will look different.

Implementing Zero Trust in OT environments provides different challenges when compared to an enterprise network. The Deloitte Zero Trust framework helps you consider the challenges that many face, and the organisational and technical change required to build robust security capabilities that unlock value.

Our approach prioritises a phased rollout, guided by clearly defined architectural principles and a roadmap aligned with specific business objectives. This phased approach allows for a pragmatic and cost-effective transition to a more secure OT environment. The focus is on establishing robust identity and access management (IAM), improved segmentation, secure remote access solutions and enhanced monitoring. Careful consideration must be given to the impact on operational availability and the need for continuous monitoring and incident response capabilities.

By making it easier for organisations to carry out operations, Zero Trust helps safeguard your business. This is a critical step forward in ensuring a safer and more resilient future for all.



5. How can we help?

Unlock the full potential of Zero Trust for your IT and OT. We will help you define a clear roadmap and architectural principles, ensuring a common blueprint to confidently build capabilities and realise the benefit.

Zero Trust your way - and with you every step of the way

We understand that no two client journeys are the same, which is why we work with you to implement Zero Trust on your own terms – with an iterative, incremental approach that allows you to:

- **Leverage** your existing investments alongside new tools and processes to address potential capability gaps
- **Prioritise** Zero Trust activities based on business impact and potential risk reduction
- **Minimise** the potential for operational disruption
- **Demonstrate** value before scaling to other parts of the enterprise
- **Access** Our industry-leading cyber services at every step – across every layer and in every area of your business – thought leaders deliver our advise-implement-operate offerings and industry-specific insights.

A closer look at our capabilities supporting OT and Zero Trust:

Advise

- Explore use cases and technologies through interactive labs, workshops and the Zero Trust Experience Centre.
- Develop your strategic vision for a modern security architecture that enables your business and takes into account operational need.
- Create a detailed roadmap for turning your vision into a reality.
- Build the business case for Zero Trust and build consensus within your organization.
- Continuously evaluate and prioritize activities to align with evolving business needs and objectives.

Implement

- Leverage proprietary accelerators to reduce time to value of technology modernization and implementation efforts, from shopfloor to cloud.
- Deploy and integrate leading solutions to modernize capabilities in each of the Zero Trust technical domains: Identity, Workloads, Data, Networks, Devices.
- Integrate cyber solutions with other enterprise apps and third-party solutions (e.g. ITSM platform).
- Develop automation and orchestration capabilities to enable a shift to a more proactive security posture.

Operate

- Periodic cyber risk assessments and services such as Cyber incident Readiness, Response and Recovery (CIR3) services.
- Outcomes-based managed services to streamline and operate capabilities that support a modern Zero Trust architecture, including Deloitte Cyber Operate services:
- Managed Secure Access Service Edge (M-SASE) by Deloitte
- Managed Extended Detection and Response (MXDR) by Deloitte
- 24x7 Security Operations Centre (SOC) services through Deloitte's Global Cyber Intelligence Centres.

Deloitte.

Contact us

Anna Burrell
aburrell@deloitte.co.uk
Director
Author - UK

Jonathan Lam
jdlam@deloitte.co.uk
Senior Manager
Author - UK

Wil Rockall
wrockall@deloitte.co.uk
Partner
Sponsor - UK

Dana Spataru
dspataru@deloitte.nl
Partner
Sponsor - NL

Luís Silva Abreu
labreu@deloitte.pt
Partner
Sponsor - PT

Marius von Spreti
mvonspreti@deloitte.de
Partner
Sponsor - DE

Francesco Tozzi
ftozzi@deloitte.it
Partner
Sponsor - IT

Martijn Maatman
rmaatman@deloitte.de
Director
Sponsor - DE

Other acknowledgments

André Correia Sousa, Vikash Mukesh Laxmidas, David Andrade, Euan Ballantyne, Daniel Usman, and Sadeq Ahmed.

Deloitte.