ZERO TRUST

FOR DEVICES AND OPERATIONAL TECHNOLOGY

A TRANSFORMATIONAL SECURITY PHILOSOPHY FOR SMART DEVICES AND THE FACTORY FLOOR

INTRODUCTION

Legacy Operational Technology (OT) Networks were often isolated from the corporate IT environment in order to reduce risk and deliver on stringent operational availability metrics. While confidentiality can be an important increasingly targeting OT Environments. According to InfoSec Institute, 63% of manufacturing organizations experienced a SCADA/ICS security breach. Air gaps and “security by obscurity” can no longer be relied The global Secure OT market is expected to grow at a CAGR 16.3% between now and 2028. Factors driving this expected growth include: metric, it is usually availability and integrity that are more important in the OT environment. Outages come with significant cost, while integrity errors can result in poor quality product or risks to operator safety. However, technology has moved on and, as enterprises look to adopt a more connected, more intelligent approach to industrial environments, there is a need to secure OT in a more advanced manner. Adversaries have become much more sophisticated and are upon to provide adequate security.

The modern OT environment has many of the same needs as the modern IT environment with respect to the need to provide secure remote access, to provide increased segmentation and to enable the sharing of data with cloud services. This being the case, why should we not look to apply modern security practices to the OT environment? Why not Zero Trust?

THE CHALLENGES

The global Secure OT market is expected to grow at a CAGR 16.3% between now and 2028. Factors driving this expected growth include:

CYBER-ATTACKS ON FACTORIES

We need to improve the resilience of our OT systems to increasing numbers and varieties of attacks, in particular, the threat of ransomware.

LEGACY TECHNOLOGY

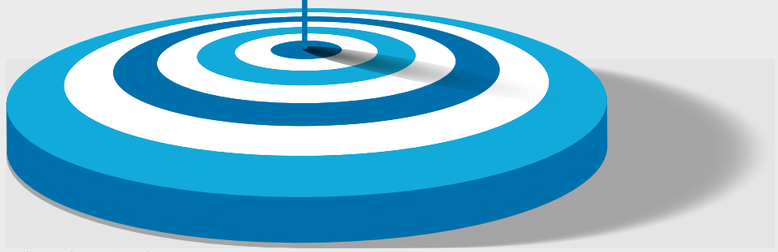
OT Systems can be difficult to keep up to date and fully patched (Certification requirements may prevent updates, older technologies may be out of support, the need for 24x7 operation may cause patch windows to be viewed as uneconomic).

INCREASED ATTACK SURFACE

SSecurity vulnerability increases as industrial systems become more connected to the outside world.

REGULATORY COMPLIANCE

Compliance with national, international and sector-specific business regulations may place constraints on the technology and process options available to enterprises.



https://www.prnewswire.com/news-releases/operational-technology-ot-security-market-worth-38-2-billion-by-2028---exclusive-report-by-marketsandmarkets-301860767.html

OUR SOLUTION

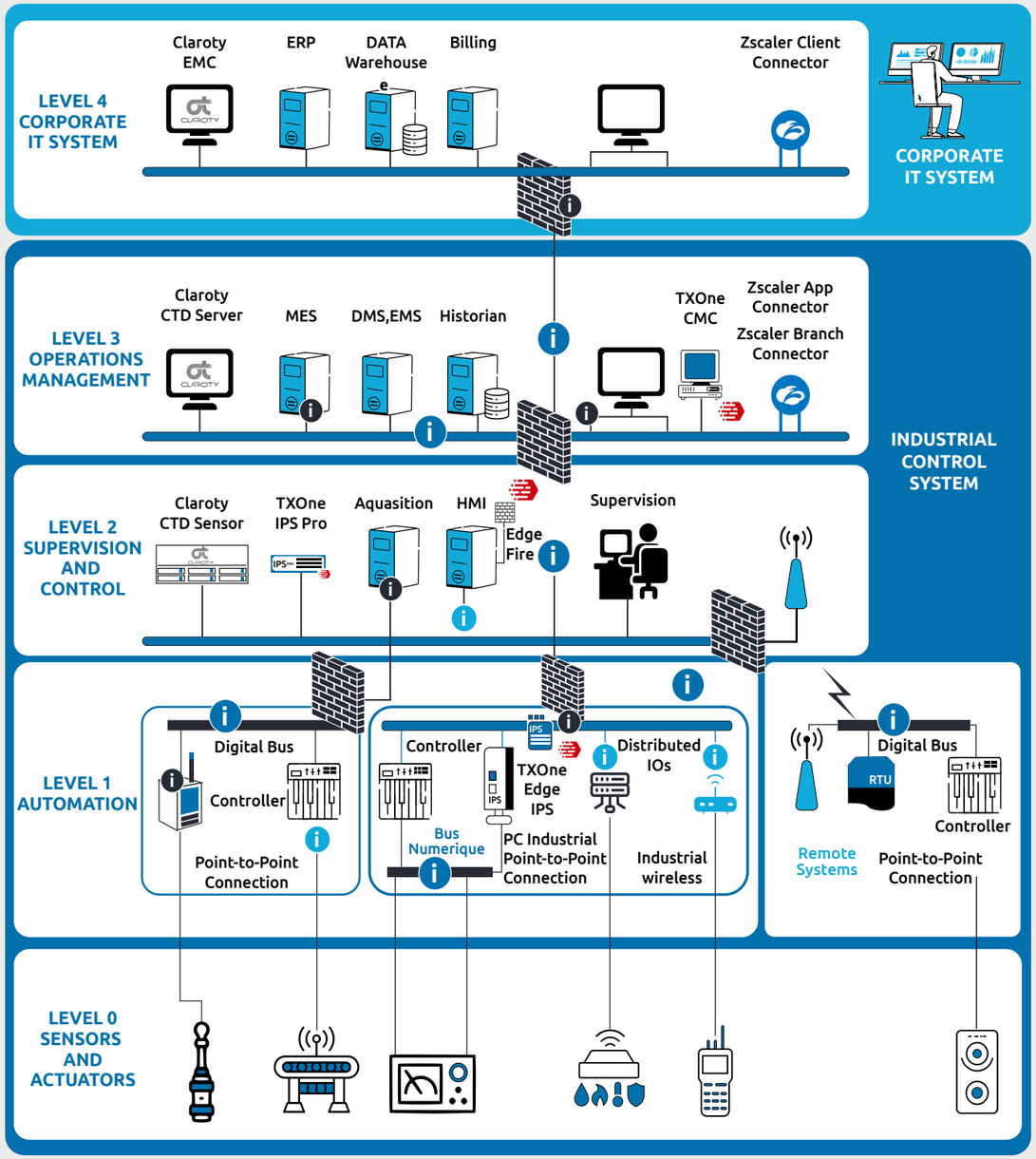
Capgemini solves the challenges of applying Zero Trust principles to the OT environment by implementing the below technology solutions:

Zscaler enables plant operators to increase uptime, improve people and plant safety, and enable new business models by securing OT environments against cyberthreats. It provides remote access into the OT environment using zero trust principles.

Claroty delivers purpose-built cybersecurity controls that identify, protect, monitor, and optimize the assets, systems, & processes in the OT environment. It provides insight into normal behavior in the environment, highlighting potential compromises.

TXOne provides cybersecurity solutions to protect industrial control systems, ensuring reliability and safety from cyberattacks. It provides the enforcement capability to reduce the blast radius in event of compromise.

The below diagram illustrates how our chosen security solutions (Zscaler, Claroty, and TXOne) can be deployed in the OT environment within the structure of the Purdue model. We recognize that the actual solutions require tailoring for the requirements of each organization (and indeed facility)



DELIVERY
APPROACH

A true Zero Trust strategy is broad in scope and is not simply a question of technology selection, design and implementation. Capgemini has adopted the US Cybersecurity and Infrastructure Security Agency (CISA) model of Zero Trust as it provides a well-structured illustration of the wide-ranging nature of a Zero Trust transformation, as shown below. Zero Trust can be applied across the five different pillars but must be supported by the three horizontal foundations of visibility, orchestration and governance. Governance is a key issue to address at the outset of the program as a move toward Zero Trust can result in changes to organizational responsibilities and accountabilities for security; such changes always require extensive stakeholder engagement in order to agree and then embed new ways of working.

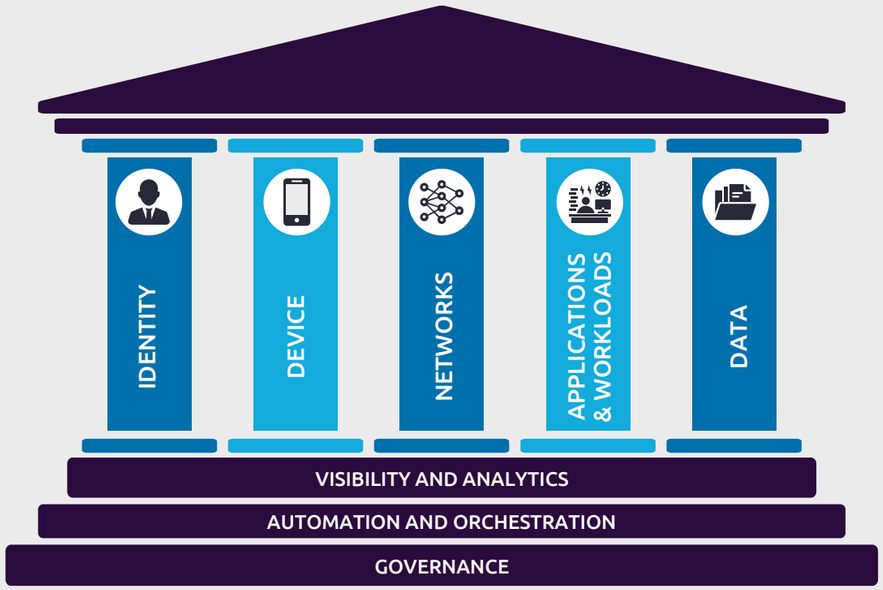


Figure 2

To move to a zero-trust solution for devices there are 4 key elements that needs to be considered:

- **PLANNING AND INITIATION**
- **DESIGN**
- **IMPLEMENTATION**
- **OPERATIONS HAND OVER** (including the option of a managed security service)

The activities supporting our delivery approach are illustrated below:

(4 weeks)	(4 - 8 weeks)	(8 - 12 weeks)	(4 weeks)
PLANNING & INITIATION	**DESIGN**	**IMPLEMENTATION**	**OPERATIONS HAND OVER**
Assessing customer ICS environment and ZT requirements	**ICS infrastructure zero trust architecture design**	**Configuration of Zscaler, Claroty, TXOne**	**Provide security operations support services to the Clients**
• Project kick-off. • Determine the relevant entities and stakeholders. • Confirm the locations, systems and processes in scope. • Plan and schedule workshops. • Produce Vision to drive the wider program. • Governance setup.	• Review existing ICS architecture and means of segregation from the IT environment. • Prepare the • High Level Design for integration of zero trust principles into the ICS landscape via Zscaler, Claroty and TXOne solutions. • Document the Low Level Designs and agree SLAs.	• Implement/ Configure Zscaler, Claroty and TXOne (depending on the use cases required by the client). • Validate all the configurations and perform testing to ensure all the features/modules are working as intended, including integration with wider client environment.	• Early life support and hand over from project to RUN • Monitor the SLA's and provide required service management support. • Reporting to the client on scheduled basis.

One key element of the successful adoption of Zero Trust, whether in OT, IT, or both, is in the derivation and agreement of the overall Vision for the end-state position. The Vision is a critical tool, providing:

1. A common, widely accepted, view of what the program must deliver and, crucially, why those capabilities must be delivered.
2. The structure for the program and the associated technology components, providing a framework upon which to elaborate and a communications tool to help drive the overall transformation.
3. A measurable set of outcomes that can be used to determine when the program has been successfully completed.

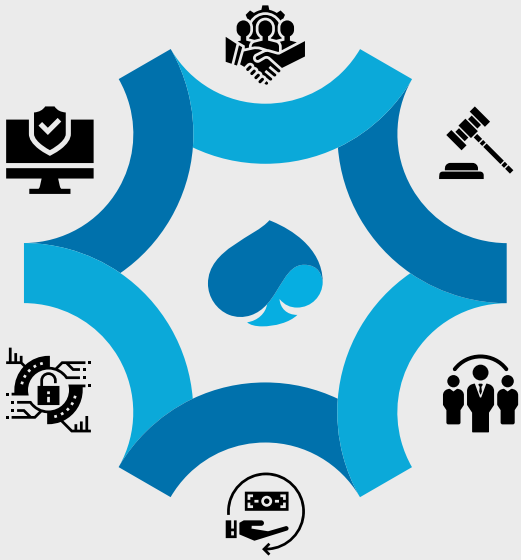
Involving key stakeholders in the creation of the Vision helps to obtain the buy-in and support that is needed to drive what can be a substantial change throughout the organization. The importance of executive sponsorship cannot be over-estimated, with the lack of such evidenced support often leading to stalled or failed transformation initiatives – a situation we avoid through careful stakeholder management.

WHY CAPGEMINI?

A very strong partnership with **ZSCALER** and **TREND MICRO.**

Assurance through adoption of vendor agnostic **ZERO TRUST FRAMEWORKS.**

ALLIGNMENT with several Industry Standards (e.g., IEC 62443) that helps our clients protect themselves in a connected economy.



END-TO-END SECURITY MANAGEMENT SERVICES to assess, protect, and maintain your critical IT/OT ecosystem.

ELITE R&D TEAM specializing in the identification and remediation of vulnerabilities in connected products and industrial systems.

OPTIMISE COST OF SECURITY through a pragmatic approach towards tooling, phasing and management of residual risk.

BUSINESS BENEFITS

Clients will achieve the below business benefits after implementing Zero Trust for OT/ devices:

Reduced risk of production outages.

Easier and more secure working with maintenance suppliers.

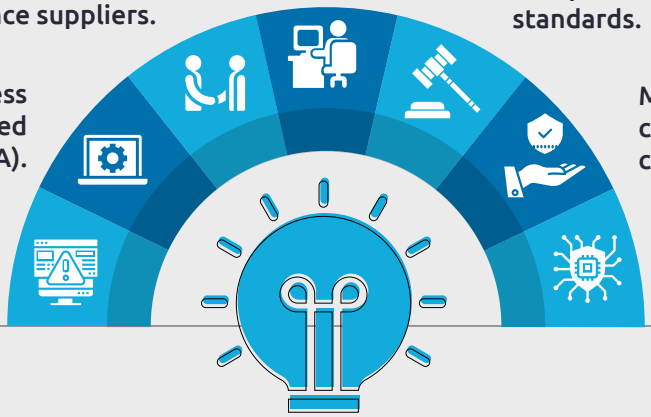
Compliance with regulatory standards.

Secured remote access via Zscaler privileged Remote Access (PRA).

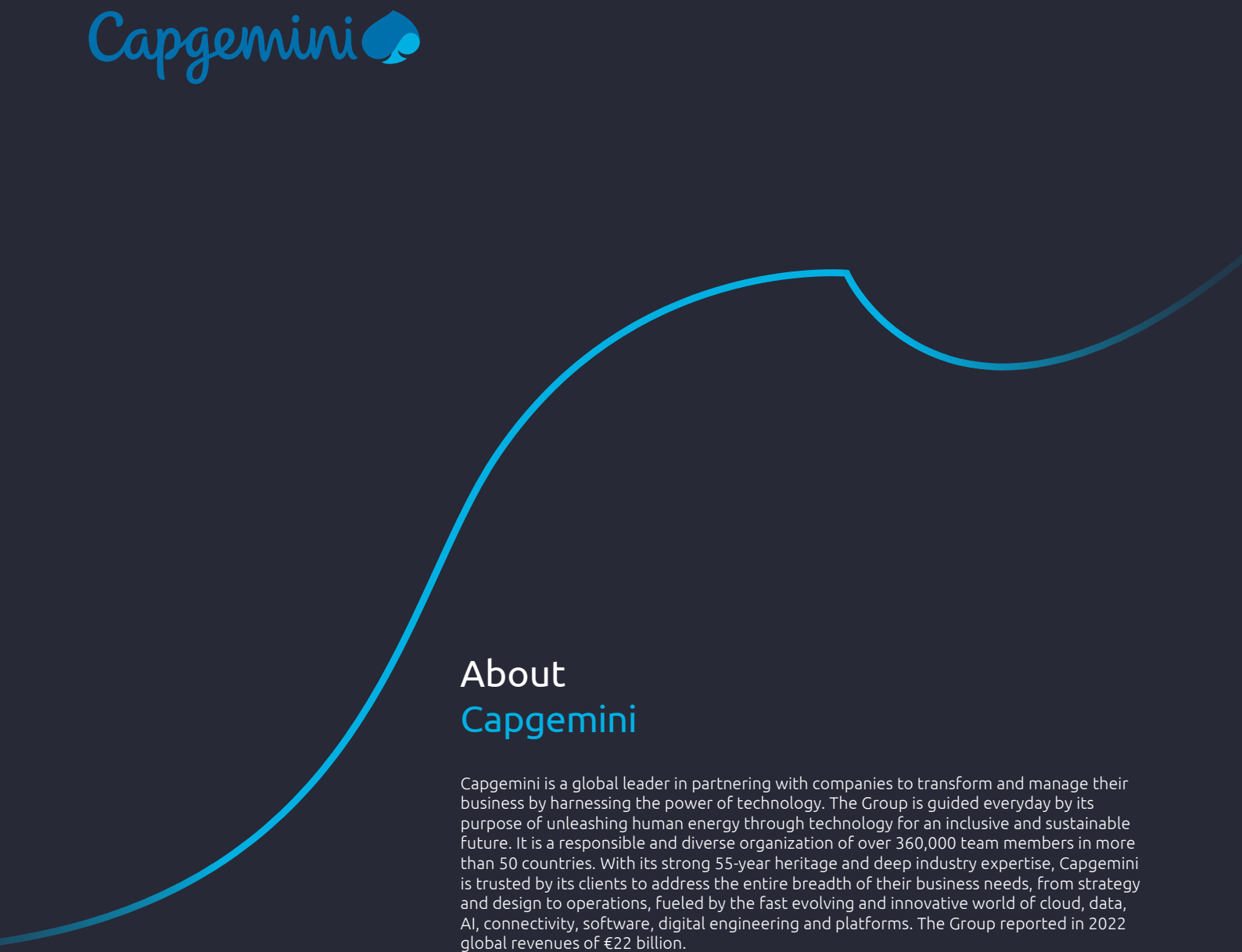
More secure access to cloud-baseddata processing capabilities.

Reduction in attack surface and blast radius.

Increased security for legacy services.



Evolve your OT Security with Capgemini's ZERO TRUST:
Protect your legacy environments whilst preparing to make the most of Intelligent Industry
Reduce your blast radius and so protect your up-time
Secure remote access into your OT environment via dynamic, context-based, access control



About Capgemini

Capgemini is a global leader in partnering with companies to transform and manage their business by harnessing the power of technology. The Group is guided everyday by its purpose of unleashing human energy through technology for an inclusive and sustainable future. It is a responsible and diverse organization of over 360,000 team members in more than 50 countries. With its strong 55-year heritage and deep industry expertise, Capgemini is trusted by its clients to address the entire breadth of their business needs, from strategy and design to operations, fueled by the fast evolving and innovative world of cloud, data, AI, connectivity, software, digital engineering and platforms. The Group reported in 2022 global revenues of €22 billion.

Get the Future You Want | www.capgemini.com

For further information please contact:
lee.newcombe@capgemini.com