Secure IoT/OT Services

Securing your critical IoT/OT infrastructure

Connectedness: The curse and the cure

World-renowned author T.S. Eliot once wrote **"Hell is a place where nothing connects with nothing."** Those who are responsible for securing critical infrastructure today might argue that **"Hell is a place where everything connects with everything."**

The explosive growth of the IoT (Internet of Things) has dramatically increased security vulnerabilities—particularly in industries with critical OT (operational technology) processes and networks. Last year 90% of industrial companies said they had experienced a cybersecurity breach[1], and 80% of security professionals agreed that IoT breaches were more expensive to find and fix than traditional security incidents[2].

While connectedness is the culprit for the spike in security issues, it must also be the solution—because we are not going back. Convergence is reality, and the benefits are worth the risks. Capgemini is uniquely capable of using convergence to secure your critical enterprise IoT/OT deployments. We combine deep expertise in OT, IT, and IIoT (industrial IoT). And we call our portfolio of services, Secure IoT/OT Services.

Introducing Secure IoT/OT Services

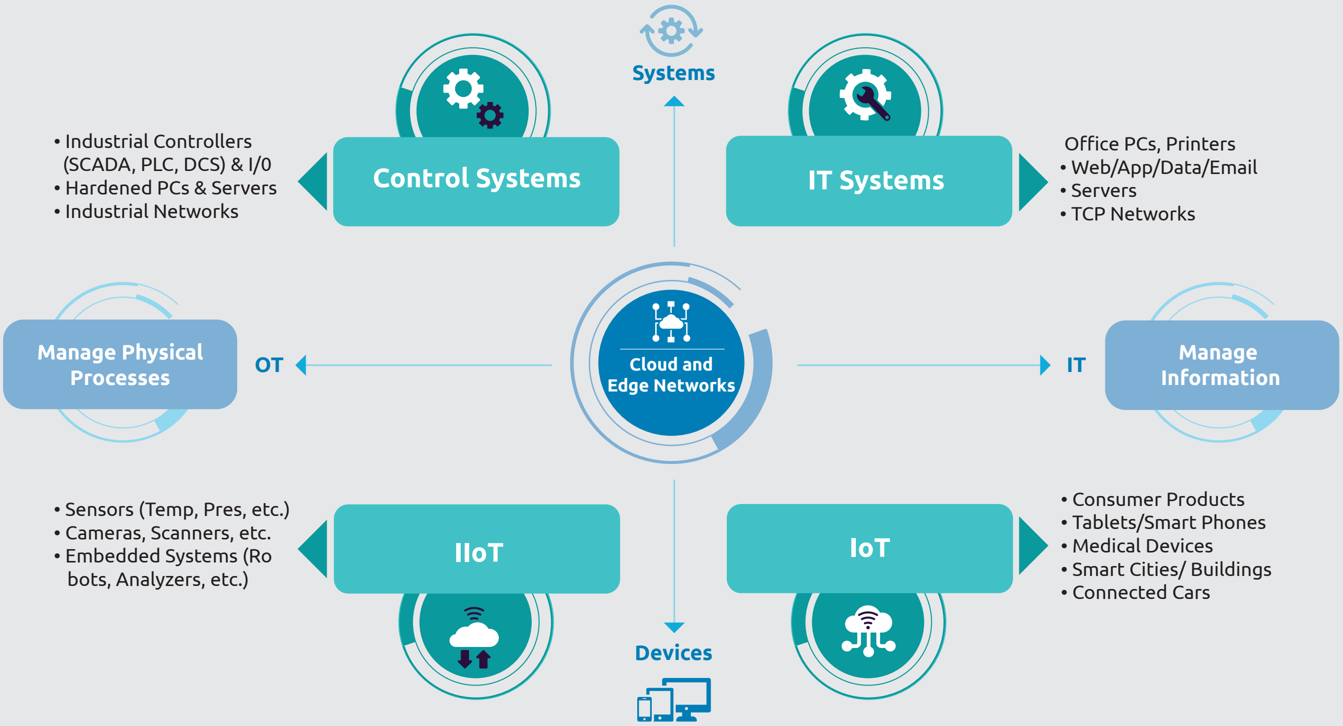
Capgemini's Secure IoT/OT services bridge the siloes of legacy IoT/OT security, bringing together everything needed to see, understand, and mitigate the risks in your environment.

Capgemini provides services to improve the IoT/OT security posture of your whole installation (Networks, Machines, EndPoints, devices, PLC, Applications, etc.)

Our approach is to reuse proven solutions in IT and adapt them to the industrial context:

- **Avaibility and Integrity** before confidentiality
- **Security consistent with Safety**
- **Operational use cases driven** (operations constraints and production shutdown risks)
- **Maintain system performance** (despite real time constraints, old technologies)

In short, we converge OT/IT/IoT/IIoT security so you can focus on **mitigating the risk of production losses** while exploiting digital transformation and Industry 4.0 business opportunities—rather than worrying about the next breach.



[1] Gartner: **"Scenarios for the IoT Marketplace, 2019."**
[2] IDC: "The State of IoT Security, December 2018.

This convergence has fundamentally changed the threat landscape because OT networks are very different from IT networks. That explains why many companies now see the addition of network devices as the top threat to industrial control security (ICS), and why many have experienced a sharp increase in attacks. The result is an inability to safely adopt IoT and IIoT use cases on an enterprise scale.

The key issue is that despite OT/IT convergence, OT and IT systems and devices are still secured separately through siloed security processes and solutions. All too often, there are disparate security mechanisms for control systems, OT devices, IT systems, and IoT devices, as depicted below.

That means there is limited visibility into security issues, no consistency in managing the security of industrial systems, and no ability to safely scale IoT security. And that leads to significant challenges, including:

- **Higher risks:** Cyberattacks can cause physical damage or have fatal consequences; they can also target the heart of your value chain.
- **Critical outages:** Because of their vital process importance, equipment is often operated full time, increasing security vulnerabilities.
- **Shortages of skilled security professionals:** The teams operating OT equipment aren't always up to speed on cybersecurity, and traditional cybersecurity teams don't know the operation use cases and related risks.
- **Difficulties with data protection and compliance:** With more published attacks on critical Infrastructure, government and industrial bodies keep increasing the requirements.

Capgemini's Secure IoT/OT Services provide convergence—and more effective security for IoT/OT deployments—in three key dimensions:

1. Our services align with your business challenges.

Capgemini approaches each engagement from a business perspective. We want to understand where IoT/OT security fits within your Industry 4.0 and Digital Transformation strategies. We communicate with all key stakeholders—from business leaders to technical teams—to assess your security posture, create an effective strategy to address your challenges, and provide services tailored to your unique requirements. Typically, our Secure IoT/OT Services fit within three broad categories:

Define

We help you assess your current IoT/OT security and compliance status so you can clearly understand your risks and prioritize remedial actions. We tailor specific service offerings to address your key security issues and questions. For example:

- **What are the risks if I do not have visibility into my IoT/OT network?**

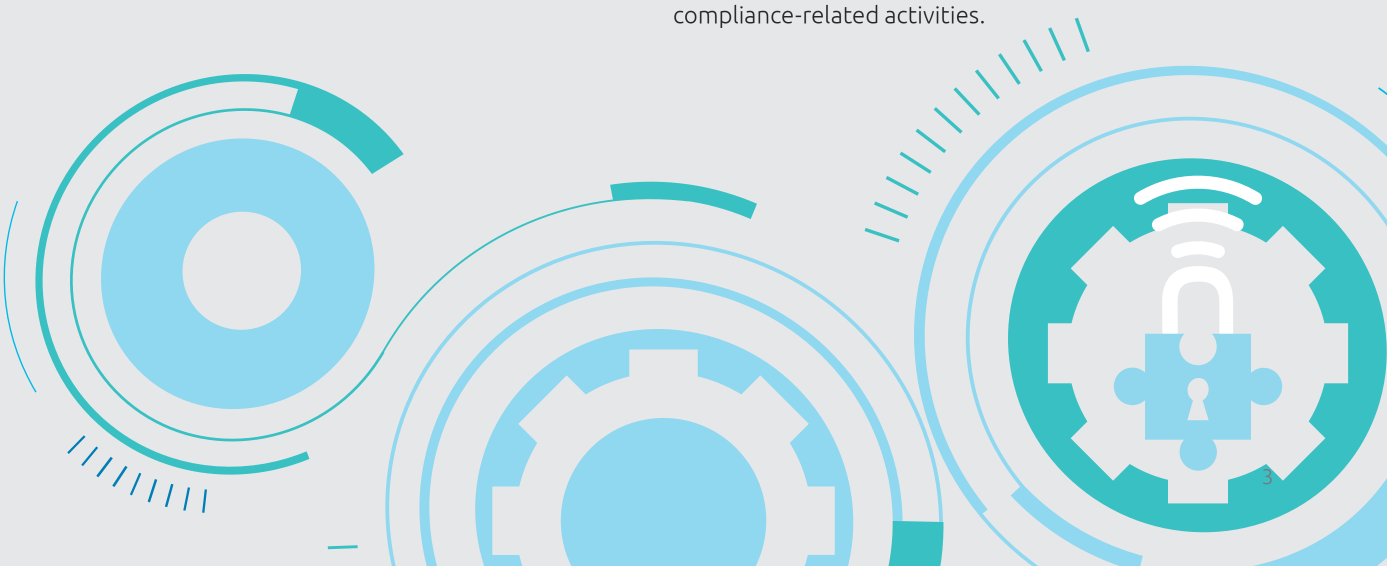
– Capgemini's IoT/OT Risk & Maturity Assessment service and Industrial Asset Visibility, Classification & Management service work together to provide a comprehensive inventory of your IoT assets, identify security risks, and benchmark your risks compared with peers in your industry—so you can clarify and prioritize needed investments in security solutions.

- **How do I prevent unauthorized access to my production environment?**

– Our IoT/OT Cybersecurity Training & Awareness service enables your teams to understand access-related vulnerabilities and deploy more effective authorization policies and practices specific to your IoT use cases.

- **Are we compliant with our global data privacy and OT/IoT regulations?**

– Capgemini's Data Privacy and OT/ICS Compliance service evaluates your current compliance status and makes recommendations for streamlining compliance-related activities.



Protect

Based on findings from the Define phase, our experts assist you with security solutions that will address your highest-priority security questions and issues. After benchmarking and choosing the right solutions we proceed with the first Proof of Concept on a pilot site and then prepare the large-scale deployment.

For example:

- **How do I protect critical industrial assets?**

– Our Endpoint Protection for OT, ICS, and EOL Systems offering provides guidance and specific recommendations for securing industrial assets according to the severity of identified risks and vulnerabilities.

- **What are the threats to my production line?**

– Services such as Zero Trust & Zero Touch Network Segmentation go far beyond so-called "air gaps" and deliver innovative, effective protections for production line vulnerabilities.

- **How can I protect production from my supply chain?**

– Extending security beyond the walls of your enterprise is an inevitable IoT requirement, and Capgemini helps you accomplish this with a variety of sophisticated offerings such as Industrial Policy Enforcement and OT/ICS Access Management.

Defend

Capgemini can assist you with ongoing monitoring of your IoT/OT environment so you can continuously identify and respond to threats, addressing your key issues. For example:

- **How do I monitor my global IoT/OT networks?**

– Our Global 24/7 IoT/OT SIEM/SOAR Operations Management service provides reliable, real-time analysis of security alerts generated by applications and network hardware.

- **How do I secure my Industry 4.0 transformation?**

– Capgemini's Industrial & Operational Threat Management service combines the broad business perspective and detailed, expert technical analysis capabilities needed to secure your digital transformation and Industry 4.0 initiatives at all levels and security layers, virtually anywhere in the world.

- **How do I continuously prevent, respond & detect IoT/OT threats?**

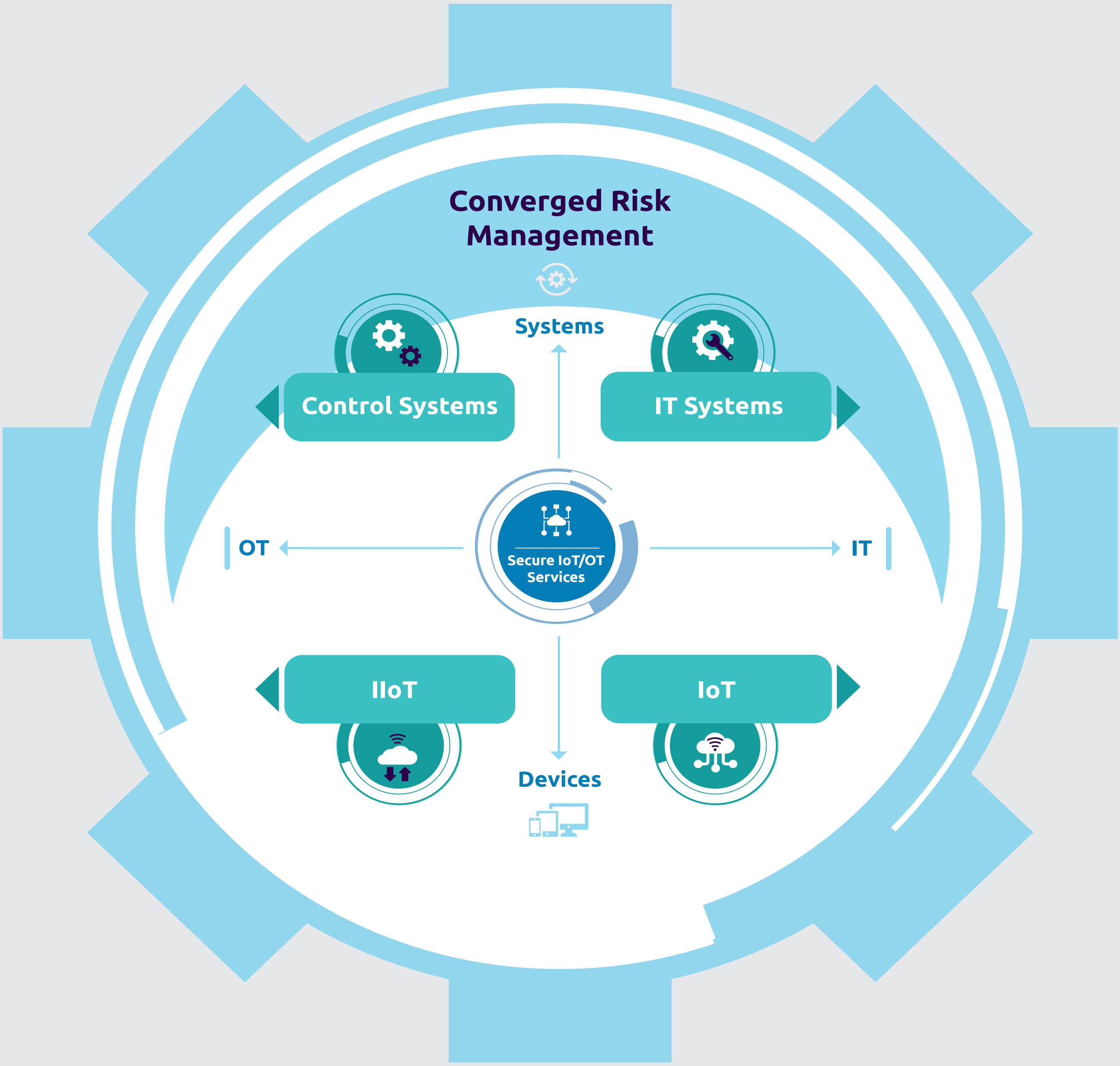
– Our OT Incident Prevention, Response & Detection service monitors your environment and provides the detailed, real-time information needed to move from occasional or "snapshot" threat prevention to continuous detection and response capabilities.

2. We provide protection at the level you require.

Unlike service providers whose expertise is as siloed as their security solutions, Capgemini can help you protect all levels of OT/IT/IoT/IIoT deployments. Our experts will assist you with your most immediate security requirements in Levels 3-4 ("Common Core" as defined by ISA/IEC 62443), but we are also experienced in Levels 2, 1 and 0, enabling you to expand protection seamlessly through a single partner.

Moreover, our converged risk management approach extends to all elements of your enterprise IoT/OT implementation—from OT control systems and IIoT devices to IT systems and IoT devices.

Level 4	Level 3	Level 2	Level 1	Level 0	
Cloud: " Common Core"	Supervisory/ Gateway: " Common Core"	Supervise and Control (SCADA)	Process Control Level (PCL)	Sensory Level	ISA/IEC 62443

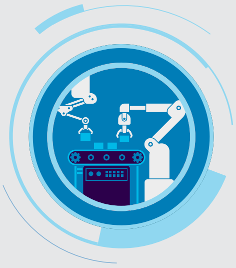


Oil & Gas Company Raises Cybersecurity Maturity and Operational Effectiveness

Operational excellence is paramount to this global conglomerate. The company operates and maintains equipment with critical health, safety, and environmental control considerations. In support of a 3-year transformation effort, Capgemini performed an exhaustive assessment of security controls at approximately 50 operational facilities worldwide, followed by strategic guidance and advice for improving both cybersecurity awareness and effective defenses. Capgemini also tested and validated OT and IT-based activities, executing penetration testing against the company's entire global I network. The result: the company raised its operational level and developed more mature and effective cybersecurity delivery across the enterprise.

Large Electric Utility Protects Power Grid, Employees, and Customers

Operational uptime is of the utmost importance to this leading electric utility, and mature security intelligence operations are vital to maximizing uptime of critical systems. Capgemini assessed the company's current operations and organizational capabilities and provided a roadmap to more robust and effective intelligence operations. Capgemini also assisted with knowledge transfer in the form of workshops and training on threat monitoring and metrics/ reporting. The result: a more mature and effective cybersecurity organization and the development of the people, processes, and technologies needed to run their own security intelligence center.



Energy Management and Automation Specialist Cuts Risks through Operational Transformation

One of the world's leading energy management and automation specialist had embarked on an industrial cybersecurity program to: protect their assets from cyber-attacks, ensure their customers are not impacted by malicious software embedded in their products, ensure business continuity of its Industrial sites and prevent leakage of sensitive information.

Capgemini helped them establish network segmentation and baseline controls for 200+ global industrial sites. Capgemini is also running the security monitoring of those sites.

The result: The company was able to execute live cut-over with zero impact and Capgemini subsequently provided managed services to address specific security requirements.

The Capgemini difference

Many companies claim to have IoT/OT security expertise. Why is truly unique about Capgemini's experience and capabilities in this arena? Here are just a few examples.

OT expertise: Capgemini has many years of experience securing enterprises with critical OT processes and infrastructure, and provides a holistic end- to- end services (Assess, Protect, Check, Maintain and Monitor).

Deep, sector-specific cybersecurity experience: Capgemini has the breadth and depth of skills to cover security requirements in virtually every industry and market segment, including natural resources, energy and utilities, manufacturing, healthcare and life sciences, automotive, telecommunications, and more—with negligible operational impact and zero downtime.

Business-first approach: Our expertise is not limited to security technology. We see the big picture from a business perspective and can help you implement IoT/OT security that advances your digital transformation and Industry 4.0 goals.

Strong partnerships: We work with the "Who's Who" of IoT-related security partners, and their offerings complement and add value to our Secure IoT/OT Services. Our partners include Claroty, Fortinet, IBM, Microsoft, Nozomi, Otorio, TrendMicro, Zentera and many more.

Global scale: Capgemini is everywhere your development teams, networks, devices and users are with near-shore delivery capabilities worldwide and our integration expertise enables you to scale on demand whenever, wherever you want.

Satisfied clients: Our clients are achieving tremendous business value and are highly satisfied with the services they receive. We encourage you to ask us for references in your industry sector.

Take the next step toward secure enterprise IoT/OT

Let Capgemini help you implement digital transformation and Industry 5.0 initiatives with confidence.

Contact us today. Let's discuss your business objectives and explore how our Secure IoT/OT Services can advance your strategic priorities.

About Capgemini and Sogeti

A global leader in consulting, technology services and digital transformation, Capgemini is at the forefront of innovation to address the entire breadth of clients' opportunities in the evolving world of cloud, digital and platforms. Building on its strong 50-year heritage and deep industry-specific expertise, Capgemini enables organizations to realize their business ambitions through an array of services from strategy to operations. Capgemini is driven by the conviction that the business value of technology comes from and through people. It is a multicultural company of over 200,000 team members in more than 40 countries. The Group reported 2018 global revenues of EUR 13.2 billion.

Visit us at

www.capgemini.com

Sogeti is a leading provider of technology and engineering services. Sogeti delivers solutions that enable digital transformation and offers cutting-edge expertise in Cloud, Cybersecurity, Digital Manufacturing, Digital Assurance & Testing, and emerging technologies. Sogeti combines agility and speed of implementation with strong technology supplier partnerships, world class methodologies and its global delivery model, Rightshore®. Sogeti brings together more than 25,000 professionals in 15 countries, based in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Capgemini SE., listed on the Paris Stock Exchange.

For more information please visit

www.sogeti.com

For further information please contact:

infra.global@capgemini.com