

Industry 4.0
**Solving the conundrum
of connectivity and security**



Contents

Executive summary	3
Introduction	5
1. How to get ready for Industry 4.0 with the right balance of connectivity	7
2. How to achieve OT asset visibility and management	9
3. The best route to integrating IT and OT security management for visibility and control	11
4. How to provide secure remote access to the OT environment	13
5. How to protect against supply chain risks	14
Conclusion	15
Why BT	16



Executive summary

The convergence of information technology (IT) and operational technology (OT) is often hailed as the route to unlocking the benefits of digitisation, and many organisations feel they won't see any of the rewards until this is achieved. However, there'll always be different systems and processes in both IT and OT. We believe that instead of actual IT / OT system convergence, the goal is to achieve sufficient integration and connectivity between your IT and OT systems to enable Industry 4.0, while maintaining a firm focus on security and safety.

We've identified five main challenges around achieving secure IT / OT integration amongst our customers:

1. Getting ready for Industry 4.0 with the right balance of connectivity.

Organisations looking to digitise their operations are learning that IT / OT integration can increase cyber risk because it means connecting things that were never designed to connect to the internet. Air-gapping and procedural controls have a role but shouldn't be exclusively relied upon. Instead, it's about realistically assessing your capability to implement OT connectivity safely and adopting a Zero Trust by design approach as part of your digital transformation strategy.



2. Achieving OT asset visibility and management.

The challenge of OT asset discovery is common to most industrial organisations and is a fundamental prerequisite for compliance with cybersecurity frameworks. While active detection was traditionally seen to adversely affect an OT network, modern scanning methods use the actual ICS protocols to collect detailed information from your assets. We recommend an initial focus on passive detection and then a considered use of active scanning as and when needed.



3. Integrating IT and OT security management for visibility and control.

Any integration initiative needs a single executive leader who can navigate the 'cultural divide' between IT and OT. We recommend a combination of a centralised resource such as the CISO coupled with on-site plant management and maintenance as the best approach for combining IT and OT operations. This will recognise the individuality of your OT systems on a site-by-site basis and will bring both OT and IT employees along on the journey. Additionally, integrating all your alerts into a single dashboard such as your corporate SIEM will support cost-effective and holistic security threat management.



4. Providing secure remote access to the OT environment.

A vital part of this is being alert for practices that can be considered risky so you can identify safer alternatives and help employees to follow guidelines. Consider only connecting your OT system intermittently to reduce risk. Handle remote connectivity centrally, managed by the security team. Plan to authenticate all remote connections, then actively monitor and log them, following Zero Trust principles. Implement scanning for externally / internet-visible remote connectivity platforms and anomalous traffic. And stay vigilant for configuration drift towards back-door access with regular penetration testing and visual audits of the OT control infrastructure.



5. Protecting against supply chain risks.

We see supply chain cyber risk as an extension of your broader supply chain risk management strategy and recommend the [UK National Cyber Security Centre's supply chain security guidance](#). When it comes to implementing protections in your organisation, form a cross-organisation committee to lead the initiative and design and develop your supply chain policies and procedures. Make sure you identify all assets deployed in your environment and get all suppliers and vendors across your supply chain to do the same. Underpin your security with a framework of regular supplier assessments and reviews.



Key to achieving a secure IT / OT integration is the right blend of technology, people and processes. As you implement security technologies into your OT environment, make sure to bring your OT and IT people along on the 'convergence' journey with tailored messaging. And wrap the whole initiative in robust processes to create a workforce that prioritises security hygiene and follows best practices and cybersecurity frameworks.

Introduction

Globally, manufacturing organisations are in the middle of a major transformation, thanks to the digitisation of their OT estates.

This transformation is so compelling that it's often referred to as the fourth industrial revolution, or Industry 4.0. Organisations see a huge opportunity in Industry 4.0, with this market valued at US\$86bn in 2020 and forecast to reach US\$267bn by 2026 – a CAGR of 20.71%.

However, it can be a significant challenge to secure an OT environment while still allowing enough connectivity to enable Industry 4.0, and we need to solve this conundrum to support a secure digital future.

Attacks on OT are increasing

A survey by IDC demonstrated that the lack of coordination between IT and operations is, on average, negatively impacting every measure of performance and resiliency.

For example, it increases energy costs, causes unscheduled asset downtime or outages as well as health and safety incidents, and slows the

speed of changeovers. And one of the highest metrics on this list was the prevalence of OT security incidents.

The last few years have seen a substantial increase in the number of attacks specifically targeted at OT or Industrial Control Systems (ICS) and in 2021 OT security threats went mainstream, including the [Florida water treatment facility hack](#), [SolarWinds](#), and of course, [the Colonial Pipeline attack](#).

While these attacks were widely covered in the news, many other, less visible, vulnerabilities are still being discovered. The Clarity biannual ICS risk and vulnerability report identified [893 new ICS vulnerabilities in 2020, compared with 716 in 2019 – an increase of 25%](#). More worryingly, 72% of these vulnerabilities were exploited through a network attack vector – in other words, remotely.

Regulators have their say

We're starting to see a range of governmental directives on protecting OT. In December 2020, the European Union proposed a revision to the 'Directive on security of network and information systems' (NIS Directive), focusing on critical infrastructure protection. And, in April 2021, the US National

Security Agency (NSA) released a Cybersecurity Advisory entitled 'Stop Malicious Cyber Activity Against Connected Operational Technology'.

The NSA's first recommendation in its Cybersecurity Advisory is to "holistically evaluate the value vs. risk vs. cost for enterprise IT-to-OT connectivity" because a standalone, unconnected OT system is safer from outside threats than one connected to an enterprise IT system.

However, this is where we first experience the conundrum of connectivity versus security: to reap the full benefits of digital transformation and Industry 4.0 you need connectivity between OT and IT systems to allow information-powered decision-making and increased efficiencies.





In this paper we explore the top five OT security issues that our customers talk to us about and discuss some potential approaches to resolving them:

1. How to get ready for Industry 4.0 with the right balance of connectivity.
2. How to achieve OT asset visibility and management.
3. The best route to integrating IT and OT security management for visibility and control.
4. How to provide secure remote access to the OT environment
5. How to protect against supply chain risks.

1. How to get ready for Industry 4.0 with the right balance of connectivity

The challenge

We regularly see two sub-challenges relating to the question of 'Industry 4.0 readiness':

- **Isolation vs. hyper-connection**
The traditional architectural approach to OT is to isolate and segregate, but Industry 4.0 seeks to hyper-connect devices for telemetry, analytics, prediction and optimisation – how do we deal with this paradox?
- **Unwanted device connectivity**
New OT technology often ships as 'Industry 4.0-ready', which essentially means with connectivity capabilities built in. Often there's no choice for customers who don't want these features, so the challenge is how to make sure these features aren't enabled once the product is installed.

These topics are tightly interlinked. As mentioned earlier, the NSA Cybersecurity Advisory recommended a detailed analysis of the risks versus the benefits of connecting OT systems. The problem is that even supposedly air-gapped networks can be breached. There are some highly inventive techniques for data exfiltration from air-gapped networks, such as using a [HDD's activity LED to extract data](#), taking advantage of the [infrared capabilities of security cameras](#), or turning [RAM into a wi-fi card](#). However, the majority of breaches are down to three less dramatic but much more common reasons: supply chain attack, malicious insiders, or deceived insiders.

[A recently published threat research blog by Mandiant](#) explicitly calls out the "increasing frequency of low sophistication operational technology compromises", where threat actors take advantage of the ample supply of internet-connected OT systems and use common IT tools and techniques to gain access to exposed OT assets.



Our recommendations

We believe that air-gapping and other procedural constraints such as blanket bans on removable media like USB drives will reinforce the perception that security is a blocker to productivity, rather than an enabler. Unfortunately, as has been proven repeatedly, people will find a way around most obstacles that they think are stopping them from carrying out their jobs efficiently. While USB drives are certainly a problem in OT, we recommend allowing them in a controlled way; for example, by only permitting the use of sanctioned and centrally registered company USB sticks.

It's possible to implement a maturity-based approach to Industry 4.0 which considers how ready you are to implement OT connectivity safely. This might follow vertical industry lines or, potentially, occur within verticals. As an example, the manufacturing industry already collects a vast amount of telemetry from its processes which is used to monitor downtime. However, if we look at the oil and gas vertical's efforts to realise the same kind of benefits, we find that the infrastructure they're using is around thirty years old and would need a radical re-architecture to be able to take advantage of similar telemetry.

As the focus on air-gapping as a primary defence mechanism decreases, one principle that's worth considering is Zero Trust. The premise behind this is that it's not safe to trust anything either inside or outside the network without first identifying and classifying all users and devices seeking access. From an OT network perspective, where things often run openly with default connections, this can represent a significant mind shift. It's also important to understand that Zero Trust is a philosophy, not a technology, and it can't be implemented overnight. So for these reasons we suggest that you include Zero Trust by design when considering your overall digital transformation strategy, and that you do this before implementing architectural changes to support IT / OT convergence.



2. How to achieve OT asset visibility and management

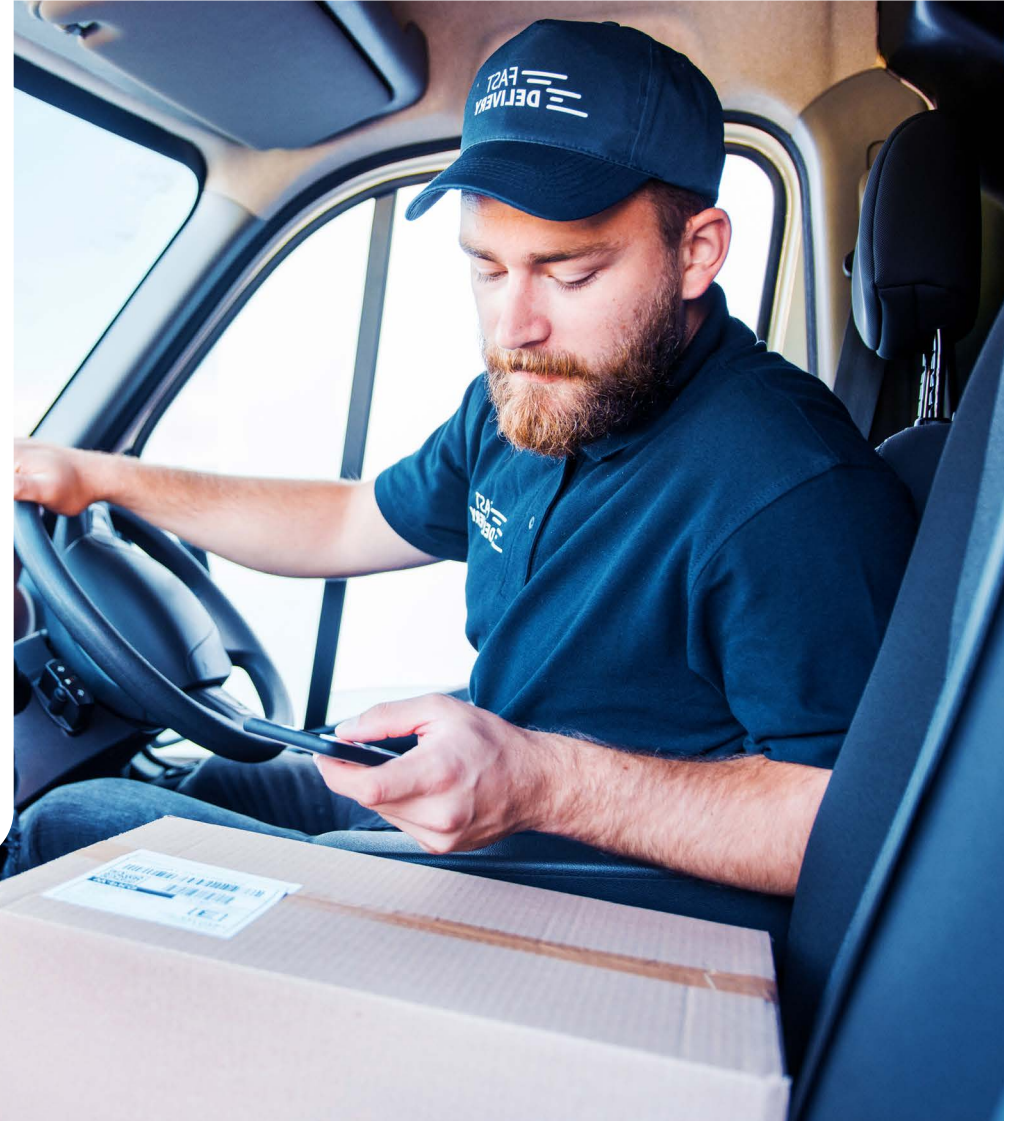
The challenge

Asset visibility and management is a foundational step in any cyber security programme and, if you intend to align to an ICS cybersecurity framework such as IEC62443, you'll need asset visibility to provide asset categorisation for zone definition. However, the sheer number of devices in many OT environments makes inventory management extremely challenging. Many of our customer engagements start from the fact that they have little to no idea of exactly what's connected to their OT network; as the old saying goes, 'you can't manage what you can't see'.

From an OT cybersecurity perspective, when we talk about asset visibility, we're referring to everything that's connected or can connect to the OT network. While the OT owners maintain an asset list of their OT control devices, we also need to make sure we capture the auxiliary connections, such as ERP, CRM, remote access, business continuity systems etc.

Many of the top OT platforms focus heavily on continuous asset discovery as an initial step towards security control, and it's often surprising to operators to find out just how many devices are able to connect into their supposedly air-gapped system.

We also often see debates around passive vs. active asset detection. Traditionally, passive detection was considered the only 'safe' way in OT environments, due to the risk of causing devices to malfunction. However, all OT security platform vendors have now added active asset detection capabilities to their products, as it's much more accurate. The risk is greatly reduced as the active component sends legitimate protocol requests to the devices, rather than relying on network scanning.



Our recommendations

We recommend starting with passive detection to initially map out your assets because this will be sufficient in most operational environments and can be achieved with negligible risk. After this phase you'll be able to decide whether you need to layer active scanning of your OT environment on top, perhaps because of hard-to-reach remote networks or quiet OT assets that don't reveal their details through traffic on the wire.

It's an often-repeated statement that OT environments are not suited to continuous scanning in the way you would implement an asset and vulnerability scanner within an IT environment. This may be true, but OT protocols are typically supportive of suitably crafted queries that can acquire metadata about the status of the OT asset (for example, its hardware, firmware and status). Similarly, IT assets within the OT environment can be queried using protocols such as WMI and SNMP with little risk.



3. The best route to integrating IT and OT security management for visibility and control

The challenge

Adopting appropriate security-related policies and tools and applying an overarching security policy to your organisation is an essential step in securing OT.

The responsibility for OT security is increasingly moving to the CISO, driven in part by increased demand for IT / OT integration, and by the need to provide an organisation-wide view of risk. However, there's a striking difference between IT / OT security management and IT / OT security operations.

[IDC's European Security Survey 2020](#) found that in 70% of European organisations, OT security is now managed by the security team - but only half of them had fully integrated IT / OT operations.

This suggests that the drive to make CISOs accountable for OT security is more due to an organisation's search for efficiencies or in recognition of the increased threat landscape,

rather than as part of a wider co-ordination effort - which can cause friction or leave the CISO exposed in this new area.

CISOs face several challenges with these new responsibilities. The first problem is how to integrate OT events into their enterprise Security Information and Event Management (SIEM) system. Once this is resolved, the bigger problem is exposed - how to respond effectively to OT alerts when their security operation centre (SOC) analysts don't understand the underlying OT processes and technology.

The other concern for organisations attempting to combine IT and OT operations is the organisational silos that currently exist. The 'cultural divide' between IT and OT is well documented and, if it's not tackled, can lead to integration initiatives failing.



Our recommendations

We suggest that a combination of centralised capability coupled with on-site plant management and maintenance can be the best approach for combining IT and OT operations.

Although the rise of IoT solutions that introduce IT-like attributes directly into OT operations is helping to force the two areas together, it's not the case for every organisation. It's important to take into consideration the fact that most OT operations aren't standardised across the organisation. Unlike IT, most OT operations use a wide variety of vendors and Operating System versions, sometimes even within the same site. Our approach works with the individuality of your site's OT systems.

We also suggest you explore how to integrate alerts into a single dashboard for cost-effective and easy holistic network management. We're seeing an increased demand from customers who want to centralise alerts in this way.

Typically they're looking to use their IT SIEM as the host dashboard, because their SOC staff are familiar with it. We believe integrating in this way will be the best approach going forward, as most organisations have invested in IT SOC capabilities and won't want to duplicate this to set up a dedicated OT SOC.

First seek to understand

One of our customers asked for help to deploy an endpoint security product at some of their remote sites.

One of the first challenges we faced was the 'head office vs. plant' mentality that saw our engineers very much categorised as part of head office. However, after spending time face-to-face with the plant management to understand their environment, we were able to win the plant's support to install the solution. Not a moment too soon: shortly after the system had been deployed it detected an advanced persistent threat and commodity ransomware within the site, which may have gone undetected if the solution hadn't been deployed.

Converging IT and OT alerts

We've helped several customers to integrate OT alerts into the managed SIEM tools that we're operating on their behalf. The alerts are seen as another log source in our SIEM, which then can be additionally triaged using specific OT tuning rules. One of the keys to success is the ability to work closely with the organisation to develop a good understanding of their ICS alerts so that the rules can be tuned properly.

Bringing the OT alerts into the IT SIEM also allows us to correlate across both IT and OT datasets. On several occasions we've detected commodity malware moving into OT using IT data sources. This correlation also lays the foundation for customers to introduce Industry 4.0 and cloud technologies.



4. How to provide secure remote access to the OT environment

The challenge

Secure remote access underpins many of the Industry 4.0 initiatives that organisations are interested in exploring. However, remote monitoring and diagnostics of operations and assets, remote product servicing, and a remote workforce all rely on connectivity – and this can cause difficulties. In the natural resources sector, this use case is felt even more acutely. How can an engineer get access to a Programmable Logic Controller (PLC) on an oil rig in the middle of the North Sea? Or how can a mining company drive towards zero harm for its workforce without enabling autonomous mining operations?



Our recommendations

We believe it's always better to shine a light on practices that can be considered risky so you can identify alternative solutions to help employees do the right thing. It's important to be clear about the risks of remote access.

Take the [Florida water treatment facility breach](#), for example. The consequences of remote access capability weren't considered. Instead, the installing engineer was just focused on solving an administrative problem, inadvertently creating a security risk in the process. This left the door open for a malicious actor to log into the facility's computer system through the remote desktop software, TeamViewer.

The NSA Advisory acknowledges that an intermittently connected OT system can be a good compromise because it's only at risk when it's connected. It recommends that all remote connections should be fully authenticated, actively monitored and logged. Authentication, monitoring and logging also aligns

with the best practice principles of Zero Trust that we outlined earlier.

The UK's NCSC has also published a set of secure design principles which include guidance to make compromise detection easier by collecting all relevant security events and logs.

Further potential mitigations we recommend for providing secure remote access include:

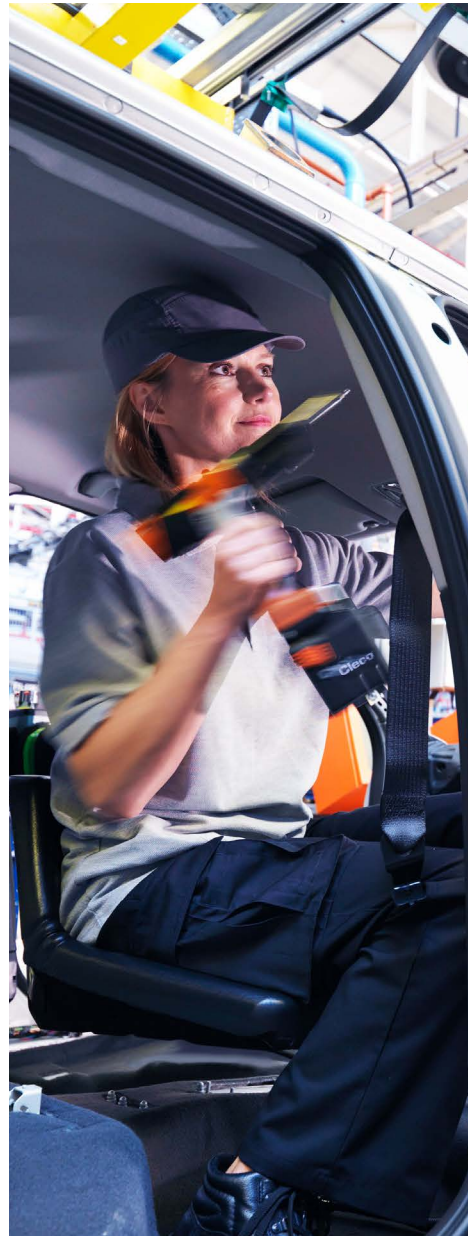
- Scanning for externally / internet-visible remote connectivity platforms and anomalous traffic.
- Provisioning a centrally managed remote access capability, possibly wrapped with conditional access (Zero Trust), managed by the security team.
- Regular penetration testing and visual audit of the OT control infrastructure to ensure it meets architectural blueprints and avoids configuration drift towards back-door access. Use tooling to scan and detect unusual configuration drift.

5. How to protect against supply chain risks

The challenge

The nature of many OT controlled facilities is that, by design, they're supported by a plethora of third parties, expanding risk beyond the borders of the organisation. A good example is the oil and gas industry where, given the many steps involved in energy processing, the supply chain is understandably complex. Yet, with global competition on the rise and prices fluctuating, energy companies are focusing on supply chain improvements that can be delivered via digital transformation. However, with tighter digital integration between suppliers comes increased risk, as there's simply no buffer if things go wrong. Equally, the specialist nature of the control and monitoring equipment can make skills hard to build and retain, creating more reliance on an organisation's suppliers.

The [SolarWinds hack](#) is a good example of the knock-on effects of supply chain compromise. While this was an IT software supply chain compromise, it's especially relevant to OT professionals given the level of interest in national critical infrastructure and industrial control systems from nation-state hackers.



Our recommendations

New recommendations from the US Cybersecurity and Infrastructure Security Agency (CISA) are a good starting point. Promoting National Supply Chain Integrity Month in April 2021 – a call for a united effort by organisations to strengthen global supply chains – it shared a report entitled '[Defending Against Software Supply Chain Attacks](#)'. The report provides an overview of software supply chain risks, along with detailed recommendations for how critical infrastructure organisations can integrate cyber-supply chain risk management into their overall security posture.

We see supply chain cyber risk as an extension of your broader supply chain risk management strategy. Here is one example of the steps that you could take to assess and address your supply chain risk:

1. Identify a cross-organisation committee of subject matter experts from relevant teams (e.g. cybersecurity, plant, governance, procurement, legal, etc.).
2. Design and develop your supply chain policies and procedures, most likely based on frameworks such as NIST.
3. Identify all assets currently deployed in your environment including supplier details.
4. Understand your suppliers and vendors and, in turn, their suppliers, to map out the full extended supply chain.
5. Work out how you will assess your suppliers and how you will be able to verify their responses with regular reviews.



Conclusion

This paper has discussed some of the key challenges that organisations face when considering how to secure their operational technology estate while exploiting the power of new technologies such as cloud, 5G and IoT.

While this is commonly referred to as IT / OT convergence, we believe that this is a misnomer. 'Convergence' implies that organisations must merge IT and OT systems together into a single technology stack. This is simply not the case – there will always be different systems and processes in both IT and OT. However, we do want to consider how to connect, or integrate, the two together in the most appropriate way, so that we can reap the benefits of Industry 4.0, while maintaining the focus on security and safety.

In our opinion, successful 'convergence' will come from an appropriate combination of technology, people and process, supported by an organisational structure that both converges and diverges where necessary:

- Technology – comprehensive security coverage is needed for both IT and OT systems and assets to balance security, risk and operational priorities.
- People – support integration by appealing to both OT personnel (who need to understand the value of adding security to their environment) and to the IT security team (who need to mitigate risks to acceptable levels across the entire organisation).
- Process – focus on basic security hygiene and implement best practices and cybersecurity frameworks that support your organisation's business objectives.



Why BT?

Today, organisations of all sizes are struggling to deal with the sheer scale and pace of today's cyber threats, with many security teams pushed to their limits. It's no longer feasible for organisations to go it alone; instead, by focusing on collaboration and co-management using trusted partners you can achieve an enhanced security posture and a wider view than just that of your organisation or the vertical that you operate in.

At BT, we've been delivering cybersecurity services to nation states and blue-chip organisations for over 70 years. Our customers rely on us to protect their critical infrastructure covering thousands of devices across the globe.

Our security portfolio is divided into three areas:

1. Our Security Advisory Services helps organisations at all stages of their security journey to assess and test their defences and select the solutions that match their security needs, including solutions to cover both OT and IT environments.

2. Our security controls portfolio offers managed services covering the major areas of network, device, application, data and identity security. We combine our years of experience and tradecraft with solutions from market-leading vendors.
3. Our threat management portfolio provides threat detection and response for OT and IT networks with solutions from threat detection and response vendors.



To find out more about how we can help you secure your OT environment while still allowing enough connectivity to enable Industry 4.0 and realise a secure, digital future, contact your account manager.



Offices worldwide

The services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to the respective British Telecommunications plc standard conditions of contract. Nothing in this publication forms any part of any contract.

© BT Communications Ireland Ltd Registered office: Grand Canal Plaza, Upper Grand Canal Street, Dublin 4. Registered in Ireland No. 141524

February 2022