



Securing Manufacturing

How we can improve speed and efficiency
while protecting from cyber threats



Empowering business
for what's next



Table of contents



04
The Changing Face of Manufacturing



23
How can we secure digital transformation?



12
What does this mean for security?



26
How can Microsoft Services help guide your secure transformation journey?



21
Solving the digital transformation challenge: OT & IT



30
Take the next step

The Changing Face of Manufacturing

Across the world, manufacturing is changing rapidly. The manufacturing industry is now at the leading edge of adopting digital platforms; automation and connected sensor technology are expanding rapidly across the globe. With more than 1.3 million industrial robots estimated to be in service at the end of 2018,¹ these technologies are now the norm at many factories. Increasingly, companies are taking advantage of the possibilities of new technology to customize their production leading to incredible results—California based cherry company Prima Frutta installed automated equipment and increased production by 50 percent² without increasing costs.

A huge piece of these efficiency gains comes via data. Through the complex global manufacturing supply chains that have evolved worldwide and the ever-increasing automation of the industry, there has been a massive increase in the availability and need for data. By using connected sensor technology and devices to build smart factories, manufacturing companies can continually monitor and streamline their production abilities.

With the massive increase in the capabilities of cloud computing through big data analytics and via the application of AI and machine learning, companies are realizing mounting productivity gains and driving an industrial internet of things (IIoT). With rapid data deployment across the supply chain and IIoT real-time alerts, smart factories have seen a 20% increase in production capacity.³ However, all of this new data and the new endpoints created within our systems are exposing the IIoT to very real security risks.

While digital technology is not new in any industry where speed and efficiency are crucial, the scale of today's IIoT innovation and the competitive nature of the industry has led some companies to ignore or to fail to take the time necessary to understand the potential risks of these new technologies. These technology-driven improvements are creating increased productivity and profit, yet we must consider that these same changes open our manufacturing infrastructure—and the legacy systems it contains—to cyber-attacks. Yes, IIoT is pushing manufacturing to new frontiers; however, newly connected devices and data-rich production cycles create potential security risks that many companies may not have addressed properly yet.

¹ <https://ifr.org/ifr-press-releases/news/-survey-13-million-industrial-robots-to-enter-service-by-2018->

² <https://www.smartindustry.com/articles/2017/worlds-largest-cherry-production-line-thrives-on-software-expansion/>

³ <https://www.forbes.com/sites/louiscolombus/2016/06/26/10-ways-machine-learning-is-revolutionizing-manufacturing/#5c5ab4c628c2>



You need to ask yourself

- How can my business protect the ever-increasing amount of data created, received, and sent by IIoT?
- How are we ensuring our IT and OT functions are communicating and working together?
- What will we do if a cyber attacker were to take down some of the connected devices in our factories?
- How can we stop cyber-attacks from causing line stoppages?
- How do we protect legacy equipment and systems that are running older software platforms?
- How do we protect our business data and systems that are connected to our plant equipment and data?

What are the key trends driving potential security vulnerabilities?

Digital transformation and Industry 4.0 (often referred to as the fourth industrial revolution) are changing the manufacturing industry like nothing else has since Henry Ford brought about the era of mass production. Through the usage of new technologies and the massive increase in available data, we are rapidly moving from mass production to customized production. With the increasing interconnectedness of the lives of consumers and access to information and services provided on a minute by minute basis, the expectations of consumers are now vastly different than they were 30 or even 20 years ago. Fueled by these changing consumer expectations, connected devices and platforms are bringing about the digital transformation of manufacturing and in doing so are exposing industrial control systems to new cybersecurity risks.



CASE STUDY. How Tapio is cultivating the rise of digital wood⁴

IIoT is leading to massive opportunities for businesses; HOMAG, a manufacturer of woodworking machines, built a global, scalable IIoT platform named Tapio. Tapio connects thousands of wood-industry machines to its technology platform, providing integrated solutions and a ready-made infrastructure while allowing companies of all sizes to improve their daily work and bolster production quality. Built with Azure, the portal analyzes data from any machine on the Tapio network to gain insights into distributed production environments. The Tapio platform connects the value chain of the woodworking industry—tree to kitchen cabinet.

Read More: <https://news.microsoft.com/transform/branching-out-how-tapio-is-cultivating-the-rise-of-digital-wood/>

IIoT and Industry 4.0

While Industry 4.0 refers to the broader trend of automation and data exchange occurring across manufacturing technologies, the crux of modern manufacturing transformation is IIoT, accounting for more than \$772.5 billion in 2018 spending⁵ and providing companies with a critical competitive edge. The manufacturing industry is leading in IIoT due to the way connected technology has streamlined and simplified various manufacturing processes. With an estimated 50 billion devices on pace to be connected to the internet by the end of 2020⁶, it is imperative that manufacturers lead the way to reap the benefits—ranging from predictive maintenance to real-time defect data from IIoT connected devices.

These IIoT implementations reduce cost and waste with proactive repairs cutting maintenance time by 20% to 50% and reducing overall maintenance costs by as much as 10%⁷. Further use of IIoT “represents the vision of the interconnected factory where equipment is online, and in some ways is also intelligent and capable of making its own decisions.”⁸ Industry 4.0 has also introduced a hybrid approach to warehousing, incorporating both virtual and actual content warehouses. With better data, employees throughout the production and collaboration side of the industry can be more productive and are in some cases freed up to do other higher-level work which allows employers to reduce costs and to focus their efforts on other important business opportunities.

⁴ <https://news.microsoft.com/transform/branching-out-how-tapio-is-cultivating-the-rise-of-digital-wood/>

⁵ <https://www.i-scoop.eu/internet-things-spending-2018/>

⁶ <https://www.iiotforall.com/iiot-devices-change-manufacturing-industry/>

⁷ <https://medium.com/datadriveninvestor/why-food-manufacturers-are-turning-to-industrial-ai-34b540875d81>

⁸ <https://www.digitalistmag.com/iiot/2017/04/25/industry-4-0-digital-transformation-in-manufacturing-05041191>

The impact of AI and Machine Learning

While AI research has been occurring for years, the reality is that the advanced algorithms used today are leaps and bounds ahead of past research—and they’re transforming the way the world collects and analyzes information. This is especially true in manufacturing through better prediction models for consumer behavior. As this technology continues to mature, customization and prediction of consumer behavior will likely accelerate.

With increased access to data and flexibility through IIoT, manufacturers are now using mass customization to efficiently react to consumer demand with AI/ML. Today’s consumers expect the products they use to be intuitive and easy to interact with; therefore IIoT’s mobilization and connectedness are continuing to push manufacturing innovation. Such innovation linked with customer expectations is particularly evident in the creation of software-enabled products. IIoT enabled smart products offer opportunities to reimagine post-sale service with immediate online support for problems or concerns.

The combination of IIoT with AI/ML is also revolutionizing how manufacturers perform skilled labor as efficiency and quality can go hand in hand with machine learning algorithms tracking the factors that impact service and production quality leading to less wasted time and materials and driving a 4% reduction in material consumption while increasing production capacity by up to 20%.⁹

Data and analytics

The IDC kicked off the decade in 2010 by predicting that there would be a 50 times increase in digital content by 2020¹⁰ and thus far they appear prophetic. With the massive increase in data and content, big data analysis is becoming increasingly time-consuming and challenging. As manufacturers continue to digitally transform, it is especially important to find an effective means of analyzing the data from IIoT as well as product and consumer information.

The need to take advantage of advanced analytics, machine learning, and AI is driving many businesses towards a hybrid (on-premise combined with cloud) approach to storing, managing, and processing data. This is leading to a streamlined ability to manipulate and analyze supply, delivery, and customer support data using AI/ML technology to drive a streamlined analysis environment that is accessible to stakeholders. Companies such as Tetra Pak are collecting operational data to help predict and optimize maintenance timing by connecting packaging

⁹ <https://www.forbes.com/sites/louiscolombus/2016/06/26/10-ways-machine-learning-is-revolutionizing-manufacturing/#5c5ab4c628c2>

¹⁰ <https://www.businesswire.com/news/home/20171101005220/en/IDC-Reveals-Worldwide-Digital-Transformation-Predictions>

lines to the Azure cloud.¹¹ To meet the expectations of production teams and consumers alike, manufacturers must transform both their Information Technology (IT) and Operational Technology (OT) environments.

// So if you're a service engineer and you arrive at the customer, you can use a simple app to pull up the significant performance information from that customer. You can drill down to see the performance, equipment by equipment. You are much more educated when you walk into the customer, and it becomes a much more informed and fact-based discussion between the service engineer and the customer. //

Johan Nilsson

VP of Tetra Pak Services, Tetra Pak¹²



¹¹ <https://news.microsoft.com/transform/total-package-tetra-paks-technology-keeps-food-drink-flowing-safely-from-farm-table/>

¹² <https://news.microsoft.com/transform/total-package-tetra-paks-technology-keeps-food-drink-flowing-safely-from-farm-table/>



Automation becomes the norm

Robotic systems have been used on assembly lines for some time now to perform repetitive tasks. However, with technological advances, robotic systems can perform more tasks allowing workers to work with the robotic system (cobots) or allowing workers to do other higher-level work. Robotic systems can learn through AI and machine learning, collaborate with workers (cobots) and often improve safety within an industrial facility. Vulcan Steel is a great example—they partnered with Microsoft to use AI and machine learning to build a proactive workplace safety solution to prevent accidents with focused safety education efforts.¹³



CASE STUDY. Empowering Vulcan Steel with Datacom and Microsoft AI

Vulcan Steel makes about 3,000 deliveries of steel a day to businesses throughout New Zealand and Australia—which means that each day, its employees need to use their training to figure out how to safely get large, heavy and unwieldy pieces of steel off of its trucks and into the hands of a very diverse group of customers.

Now, they're using artificial intelligence to try to proactively prevent accidents and near misses before they happen. The company recently started using Microsoft Cognitive Service's Custom Vision tools to evaluate camera footage from the company's trucks for actions that could be risky or lead to an accident.

Read More: <https://blogs.partner.microsoft.com/mpn-newzealand/case-study-empowering-vulcan-steel-datacom-microsoft-ai/>

¹³ <https://blogs.partner.microsoft.com/mpn-newzealand/case-study-empowering-vulcan-steel-datacom-microsoft-ai/>

// What we're hoping is we will measure the number of education discussions that take place as a result. From our point of view, if we add an additional number of safety discussions to our organization, there's not really any negative that can come of that. //

James Wells

CIO, Vulcan Steel



Another example of safety improvement via automation can be seen at Siemens Gamesa where AI-powered drones are now being used to evaluate wind turbines for repair needs, improving maintenance and worker safety on the sometimes 120 meters tall (390 feet) wind turbines.¹⁴ Robotic systems also convey major advantages when connected to IIoT. Their sensors provide extremely useful data and feedback—they can quickly “talk” to a central control to identify issues and potentially be taught to adjust quickly and accurately to fix issues. Through machine learning and AI, they can make recommendations about maintenance and potential issues to fix before an outage occurs.

¹⁴ <https://news.microsoft.com/transform/siemens-gamesa-renewable-energy-wind-power-ai-cloud/>

Digital transformation results in improved speed and efficiency

Advances in automated technology working in concert with AI/ML data applications and a connected IIoT is improving speed and efficiency across the board allowing manufacturers to optimize everything from inventory to production workflows while improving value chain decisions. Through the integration of IT systems, teams across the world have access to necessary data enabling faster, more collaborative, and transparent communication. With cloud computing's improved level of predictive accuracy and scale, conditioning monitoring processes have led to increased performance of overall equipment effectiveness at the plant level as high as 65% and even 85%.¹⁵ With this increased efficiency and speed come lower costs and better-quality control, driving a new industrial revolution for manufacturers.

¹⁵ <https://www.forbes.com/sites/louiscolombus/2016/06/26/10-ways-machine-learning-is-revolutionizing-manufacturing/#5c5ab4c628c2>



What does this mean for security?

With all these improvements driven by digital transformation and new technologies come increased security risks. As devices and systems are connected to networks to allow for IIoT innovation, the increased number of endpoints offer plentiful targets for attackers and undermines the traditional security perimeter. The same is true for internetworking between manufacturers and vendors—whenever your systems interface with others; you must consider their potential vulnerabilities in your defense posture. This is especially true given that many of our OT systems are running on legacy software.

Many in the industry are aware of these risks; in 2016 the China National Vulnerability Database documented 1036 loopholes¹⁶ within industrial control systems. Failure to address these increasing risks can lead to line closures costing hundreds of millions if not billions of dollars. The 2017 NotPetya ransomware attack is estimated to have cost over \$1.2 billion,¹⁷ a very realistic figure when you consider that line stoppages at complex manufacturing plants cost tens of thousands of dollars per minute. We expect to continue to see similar ransomware attacks—such as the 2018 WannaCry variant that cost TSMC 3% of their revenue in work stoppages¹⁸—continue to cripple companies and earn attackers millions—unless companies address their security vulnerabilities.¹⁹

¹⁶ <https://www.opengovasia.com/china-cert-report-highlights-rise-in-cyberthreats-associated-with-iiot-devices-and-networked-industrial-systems/>

¹⁷ <https://www.newsweek.com/russia-accused-massive-12-billion-cyber-attack-807867>

¹⁸ <https://www.zdnet.com/article/tsmc-says-variant-of-wannacry-virus-brought-down-its-plants/>






¹⁹ <https://threatpost.com/rsa-ransomware-payments-josh-zelonis/142645/>

Anatomy of an attack: NotPetya impact

Rapid Destruction

Example of technical impact—Petya
(Anonymous)

Publicly reported losses
(by different organizations)

 GEOGRAPHIES	All
 DURATION	~60 minutes
 62,000 IMPACTED COMPUTERS	 12,000 servers  50,000 workstations

\$200 Million
\$300 Million
\$310 Million

²⁰This type of attack represents a near worst case technical risk for a cybersecurity attack. While many of us in cybersecurity have grown accustomed to sales presentations on “doomsday scenarios,” this type of attack has many actual cases of significant business impact on organizations (changing operating results reported to shareholders).

- These numbers are a single anonymous example to illustrate what it’s like for a global organization to experience these types of IoT and technology attacks.
- The losses are publicly reported data to show the business impact of these attacks.
- CISO and senior management audiences may note that several of these reports include lost revenue that impacted operating results.

While the nature of the business impact will vary by each industry, organization, and their existing risk management controls, the total loss of IT systems for some time had a devastating impact on the customers we worked with. Most critical business operations were at a full stop while the IT team recovered systems.²¹

²⁰ <https://www.cyberscoop.com/notpetya-ransomware-cost-merck-310-million/>

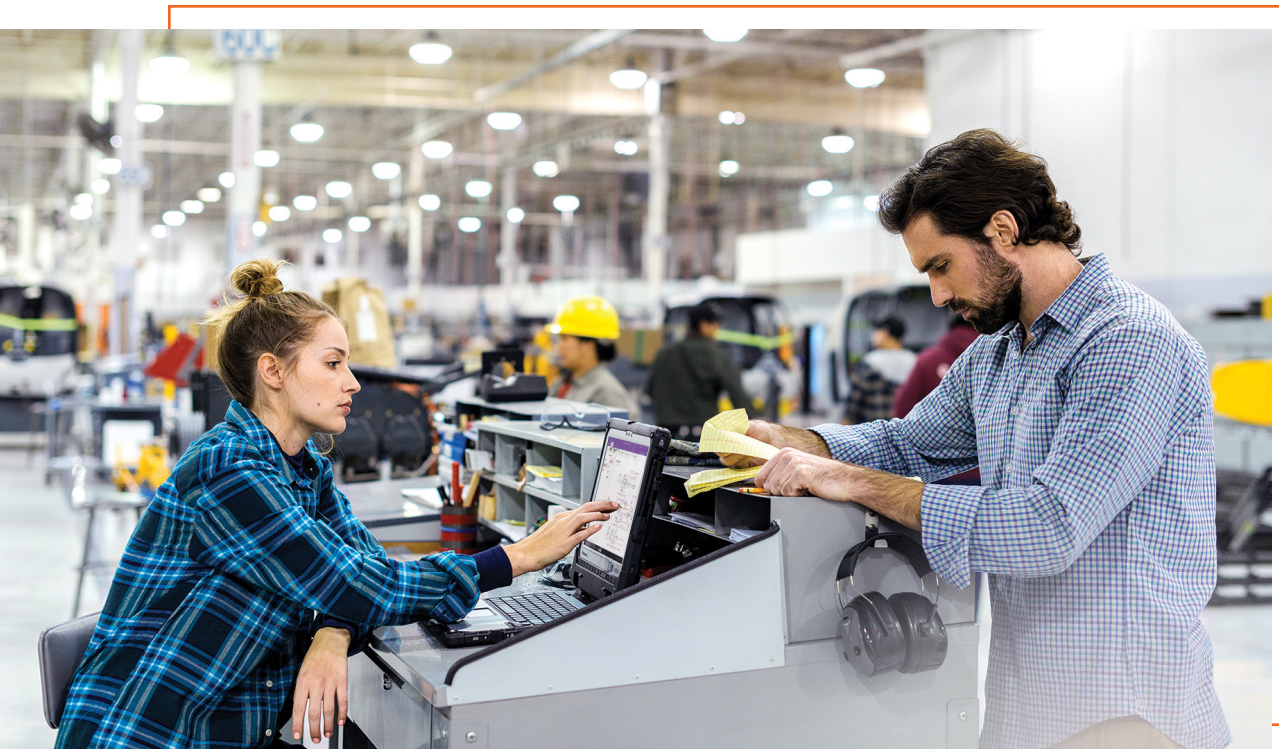
²¹ Microsoft cybersecurity engagement—Note that we cannot divulge any further details on the technical impact example (e.g. nature of business impact) without potentially identifying our customer(s).

It is not unheard of for cybersecurity attackers to hack into industrial systems which can cause production downtime, loss of production material, potential threats to safety, or be used to gain access to secure networks and data via these compromised industrial devices. Any connected system in an industrial setting must be accounted for in a security plan. Even the US government is warning that energy, manufacturing, and other sectors are dangerously vulnerable to cyber-attacks.²² As manufacturers move into the Industry 4.0 era and more devices and systems are being connected with IoT, there is a greater need to have ongoing security assessments and defenses in place in manufacturing otherwise unsecured OT devices can lead to cascading security failures.

Security risks in manufacturing

Traditional Manufacturing starts with devices, sensors, actuators, PLCs, RTUs, Scadas, etc. that are part of an industrial machine or process. These devices and systems are connected and running on legacy and real-time OS systems. Taking down a system to do a patch can mean taking down a

²² <https://venturebeat.com/2017/10/22/u-s-warns-about-hackers-attacking-nuclear-energy-aviation-water-and-manufacturing-industries/>



production line, so often patches are not applied or sometimes delayed, causing these systems to run on OS's that are not as secure as they should be. These systems are where cyber threats can get their opportunity.

When these devices are connected to the IIoT they offer opportunities for increased speed and efficiency through automation and analysis of the device's data. However, unless you update the device and software security when connecting devices, they are vulnerable to attack. Even devices that aren't actually connected to the IIoT can become vulnerable when other parts of the OT environment are connected—attackers can access your internal network via another device and gain access to your industrial control systems this way unless you secure your devices.

Part of what makes security so challenging is that the goals of cybercriminals can be different. Some want in to cause havoc and others want data or information. Such attacks can move into the Business, HR, and Financial systems of companies and potentially take down a plant or even an entire company. Some companies are held hostage and forced into paying a ransom to get access back to their systems and data.

OT also faces other security risks within traditional manufacturers. Sometimes OT systems are not on Linux or Windows and therefore don't have modern security measures even designed for them—if they're connected, they aren't secure. Even those that are Windows based are often legacy systems and equipment. These risks are further exacerbated by the possibility of having lots of different types and variations of equipment, whether due to plant acquisitions or thanks to equipment replacement timing or costs. All these factors can further complicate security measures.

Supply chain cybersecurity

Supply chain cybersecurity cannot be viewed solely as an IT or OT problem. Vendor management, supply chain continuity and quality, transportation security, and many other functions across the enterprise require a coordinated effort to address them.²³ While IoT, machine learning, and AI are creating more efficient supply chains—via the proliferation of end-to-end supply chains that promote extensive information sharing through digital means up and down the chain—these changes are also creating hefty targets for cyber-attacks.

Poor information security practices by lower-tier suppliers. Even if your company is entirely up to date with your information security practices—do you know that your vendors and partners are? Do you make sure that your lower-tier vendors and partners are up to date on emerging network, system, and application vulnerabilities?

²³ <https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Management/documents/briefings/Workshop-Brief-on-Cyber-Supply-Chain-Best-Practices.pdf>

Lack of cyber-security talent. A stunning 60% of organizations report having a shortage of information security professionals,²⁴ and this talent shortage is especially stark when it comes to security professionals with supply chain knowledge. Many universities have yet to include basic cybersecurity training in undergraduate or graduate logistics programs, and the lack of cybersecurity awareness up and down the supply chain can be shocking.

Counterfeit hardware/software with embedded malware. Another risk comes for small-scale supply chains that utilize build your own device within their supply chain. Unless your team is performing malware detection and protection, these devices are vulnerabilities that can be exploited. Devices must be built with security in mind.

Third-party service providers or vendors. Does your company have standardized cybersecurity practices for your upstream suppliers, vendors, and partners? How are you assessing adherence to these expectations? While your own company may have updated your security, a vendor's legacy systems might provide a route for attackers into your company's infrastructure. For example, vendors or employees using open or low-security Wi-Fi down the supply chain can eventually lead to compromise within your own systems.

Security vulnerabilities in the company's or supplier's system. While we may have hardened key entry points that we assume will be targeted, the reality is that cybercriminals are looking to identify the weakest link in a network and will probe to find it. Unless you apply security to every part of your digital transformation, there will be vulnerabilities left behind.

What can you do?

With systems as complicated as the ones we deal with in manufacturing, you need a hands-on approach. Managing complicated manufacturing processes requires a massive amount of data. Some of that data comes from manufacturing systems within the facility and some of that data sits outside in public networks. There are RFID tags, IoT devices, SCADA systems, automation controls with embedded sensors, real-time OS systems embedded in PLCs and RTUs, and Radio Data Terminals that use WLAN infrastructure to name a few potential entry points. All of these further increase the potential points of system compromise.

Despite these risks, 2018 research showed that the industry is at risk for overconfidence with 67% of IT Decision Makers in the manufacturing sector confident they are prepared for a cyber-attack.²⁵

²⁴ <https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf>

²⁵ <https://www.manufacturingglobal.com/technology/connectivity-driving-manufacturing-boom-beware-unwanted-attention-1>



Internal Awareness and Training. One cybersecurity risk that must always be accounted for is the lack of internal organizational awareness. One person clicking on a spam email can eventually lead to a cascade of issues that shuts down a production line. One of the best ways to begin to address this is through organizational security training that can help filter out a lot of more basic threats. You also need to ensure that operations teams have the resilience training necessary to swiftly resolve any vulnerabilities—if you don't spend some time upskilling your employees on the latest threats, they will get inside.

Curtail the domino effect. The innovations of IIoT have led to a multitude of endpoints and sensor touchpoints that enable digital operations – and increased the exposed attack surface of our businesses. If they can get into your system, the damage a hacker can do is widespread; unless you've prepared for this. To avoid stalled production lines and massive losses, industry security leaders need to prepare not just their IT teams, but their OT teams and devices or risk threats that cascade across the entire business.



Building & using highly secure devices. At Microsoft, we know that building secure devices is challenging—we're done the hard work to learn how. Thanks to the more than 1 billion we spend each year on cybersecurity research and development²⁶ and our extensive experience and observation with existing best-in-class devices, we've identified a set of seven properties that must be shared by all highly secure, network-connected devices. With these principles in place and rigorous practices, building secure devices is repeatable,²⁷ and necessary in order to secure OT environments.

1. **Hardware-based root of trust**—Hardware differs from software in having two important properties that we can use to establish device security. The first is that single purpose hardware will be immune to an attacker's desire to reuse for unintended actions. Second, hardware can be set up to detect and mitigate physical attacks; for example, pulse testing the reset pin to prevent glitching attacks is easily implemented in hardware. Together, these protect device secrets and provide physical countermeasures that provide a solid root of trust upon which we can safely and securely implement software functionality.²⁸

²⁶ <https://www.techrepublic.com/article/why-microsoft-spends-over-1-billion-on-cybersecurity-each-year/>

²⁷ <https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf>

²⁸ <https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf>

2. **Small trusted computing base**—The trusted computing base (TCB) consists of all the software and hardware used to create a secure environment for operation. By keeping the TCB as small as possible, we limit device exposure to attackers and significantly reduce the probability that attackers will find a bug or feature that can circumvent our security features.
3. **Defense in depth**—The threats we face are creative and multi-layered—they will succeed at times. Defense in depth can be the difference between a secure or compromised system. Systems that only implement a single supposedly invincible layer of defense run a massive risk; a single error leads to a catastrophic cascade of compromise. Highly secure devices must apply multiple mitigations to each threat.
4. **Compartmentalization**—By building in compartments protected by hardware-enforced boundaries, we prevent a flaw or breach in one software compartment from being multiplied across the rest of the system. This concept builds upon defense in depth as compartmentalization introduces additional protection boundaries. One common technique is to use independent virtual machines or different operating system processes to compartmentalize.
5. **Certificate-based authentication**—We've all heard—passwords are not secure. Instead, use certificates to authenticate identities when communicating with other local devices and cloud servers. Certificates are signed with a secret key and validated with a known public key forming a statement of identity and authorization. Unlike other authentication mechanisms (such as passwords) that are based on shared secrets, certificates cannot be stolen, forged, or otherwise used by an imposter.
6. **Renewable security**—We know that security threats evolve and attackers are constantly discovering new vectors from attack. Therefore devices that have renewable security are able to update automatically to a more secure state after the device has been compromised. We must renew device security regularly to counter new emerging threats, and in the worst case scenario where layers of a device are compromised, we can use lower layers to rebuild and renew the security of the systems higher levels. With remote attestation and protections for rollbacks, we can guarantee that once renewed devices will not revert to known vulnerable states.
7. **Failure reporting**—At Microsoft we are constantly collecting security data with more than 6.5 trillion threat signals analyzed daily and more than five billion threats detected on devices each month.²⁹ When a failure does occur on a device, it's essential that reporting occurs automatically and quickly to allow for analysis of what went wrong. Without this reporting, we wouldn't be able to analyze and adapt to new threats accurately. With a

²⁹ <https://www.zdnet.com/article/microsoft-were-detecting-5-billion-cybersecurity-threats-on-devices-a-month/>

sufficiently large reporting base, even extremely rare failure events can be both diagnosed and corrected, and we are able to identify and address new attack vectors before they are widely used.³⁰ The digital failure reporting and analysis ecosystem is essential to adapting to attackers and making devices highly secure—and nobody collects more security signal than Microsoft.

// Digital Transformation has raised the stakes, with 69% of senior executives telling Forbes that this is forcing fundamental changes to security strategies. If you're going to open your organization up to new customers, new markets, and anytime, anywhere access, you need to do it securely. //

Anne Johnson

Vice President Strategic, Enterprise and Cybersecurity at Microsoft



Solving the digital transformation challenge: OT & IT



When you add internet connectivity to a device, two things occur. Connected machines and devices create profoundly better manufacturing experiences, and it changes your relationships with your B2B and B2C customers.

As a customer, you want that type of connected machine in your plants. As a manufacturer, you want to create and sell that type of connected machine and the customer experience that goes with it as it helps drive better services and experiences with your customers. By incorporating IoT plus connecting with vendor and contractor networks, you improve and streamline your business and operations. However, this changes the network security architecture that you need to utilize. Yes, you need to secure portals with your contractors and suppliers to ensure vulnerabilities from your business associates don't make it easy for attackers to steal your trade secrets or access your network, but you also need to modernize and secure your OT environment the same way you have to your IT. Otherwise, the potential theft of your trade secrets, data, blueprints, or designs could potentially allow a competitor or cybercriminal to threaten your business.

Consider the risks:

- Do you know the key cyber threats that can harm your OT environment?
- Are you confident your security program protects OT infrastructure against modern threats?
- Are you confident only approved people have access to your OT infrastructure?
- Do you have the tools and process to protect, detect, and respond to modern, sophisticated attacks in your OT environment?

Modern threats require a modern cybersecurity strategy

Gone are the days when IT & OT security could be a locked castle with a moat around your network. With the digital innovation of today we have had to adjust how we address these threats. At Microsoft, we are making the effort to infuse modern cybersecurity strategy into OT environments where it can sometimes not be quite as strong as it should be. We think

³⁰ <https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/SevenPropertiesofHighlySecureDevices.pdf>

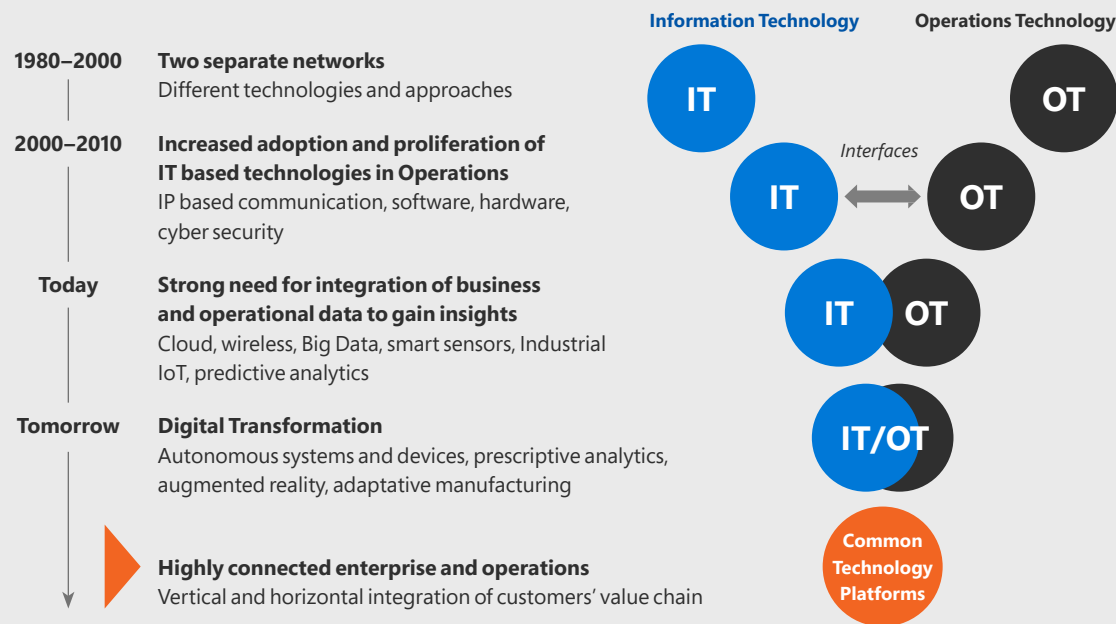
differently—we assume systems are compromised and develop an individualized and holistic plan for the challenge of securing your organization. That means protecting your organization from advanced cyber-attacks, detecting malicious activities, and responding to threats quickly.

What changed in OT?

At the turn of the millennia, IT and OT technology platforms were distinct and separate with different approaches and teams within organizations. However, with the Industry 4.0 wave and other innovations, things have changed—what used to be air-gapped and proprietary networks for OT are now connected and general purpose. The convergence of these formerly distinct technology areas has been gradual but is now increasing vulnerabilities at organizations that fail to consider the challenges brought about by Industry 4.0. To stay competitive companies need to become more autonomous, more data focused, and more adaptable—yet how do you transform from traditional to connected manufacturing while staying secure?

Converging IT & OT Technologies

IT and OT technologies have been converging towards common technology platforms from turn of the millennium



What used to be air-gapped and proprietary is now connected and general purpose.

How can we secure digital transformation?

Microsoft’s Manufacturing Journey helps manufacturers on the Path to Value of connecting, improving processes, reducing costs, opening new revenue streams, gaining new insights on your processes and products, and helping you achieve your strategic business goals. This journey takes time and can vary across manufacturers. No matter what path you take, you need to stay secure throughout your journey.

Recommended Digital Transformation Journey for Manufacturers

We recommend a digital transformation flow for manufacturers that proceeds from connected, to predictive, to cognitive.

- **Connected** equipment, plant, and data systems that provide visibility into asset productivity and performance metrics increase operational efficiency and lower costs by 1–5% while developing a new digital service platform.
- Next, your connected equipment or plant is optimized to **predictively** identify operating patterns and trends to improve reliability and utilization to enable optimal performance. Predictive integration in your operations and maintenance usually leads to an increase in overall equipment effectiveness of 7–10% while reducing maintenance costs by 20–30%.
- The third step is to enable intelligent equipment or plants to be capable of autonomous operations through **cognitive** processes. Autonomous operation and self-healing ensure maximum business benefit and opportunities leading to incremental revenue improvement of 6–15%.

Customer Reference: Global pump manufacturer Grundfos uses Microsoft 365 for improved business practices to help change lives³¹

³¹ <https://customers.microsoft.com/en-us/story/grundfos-discrete-manufacturing-office-365>

Recommended Journey for Manufacturers

1. CONNECTED	2. PREDICTIVE	3. COGNITIVE
Connected equipment, plant, and data systems that provides visibility into asset productivity and performance metrics.	Connected equipment or plant that identifies operating patterns and trends to improve reliability and utilization to enable optimal performance.	Intelligent equipment or plant that is capable of autonomous operation and self-healing to ensure maximum business benefit and opportunities.
EXPECTED FINANCIAL IMPACT		
Operational efficiency improvement and cost benefit 1–5%; New digital service platform.	Reduction in maintenance costs by 20–30%. Increase in overall equipment effectiveness 7–10%	% Incremental revenue (EBIT) improvement of 6–15%.

“ By standardizing file storage on OneDrive for Business, we get improved security, including the ability to provide—and control—easy access to data. ”

Henrik Jensen

User Experience Center Manager, Grundfos



Grundfos believes that clean drinking water is a universal right. The Danish pump manufacturer works all over the world, and it wanted to support easy collaboration among its global workforce, its many partners, and its headquarters in Bjerringbro, Denmark. Grundfos met that challenge with Microsoft 365 cloud-based services, using SharePoint Online, Yammer, and OneDrive for Business to boost communication across the planet, connect people and ideas, improve business processes, and safeguard important files and data.

Read more: <https://customers.microsoft.com/en-us/story/grundfos-discrete-manufacturing-office-365>

How can Microsoft Services help guide your secure transformation journey?

// As a company, we're focused on taking a holistic approach—protecting, detecting, and responding to security threats. //

Brad Smith

President, Microsoft



To secure your organization from cyber threats, Microsoft Services will work alongside you to guide you through the process of improving your security posture and modernizing your infrastructure against advanced attacks. At Microsoft, we have five security posture pillars designed to help guide you through a secure digital transformation.

Take the first step

Microsoft Services helps you improve your security posture and modernize infrastructure against advanced attacks.



GOVERNANCE

- OT level security risk assessment
- Identify critical assets and security priorities
- Establish a security program
- Align governance aspects of OA/OT



BOUNDARY PROTECTION

- Isolation between OT and IT environments
- "Hub and Spoke" networking model



IDENTITY

- Provide a secure identity platform
- Protect privileged identities against compromise
- Ensure clean source path for management



SECURITY CONFIGURATION

- Establish a strategic program for security configuration baselines
- Define update management process and tools



MONITORING

- Integrate OT security monitoring with SOC
- Use advanced threat protection technologies to rapidly detect and respond
- Establish response process and recovery procedures in partnership with IT and plant engineering

Governance. We provide OT level security risk assessments that help identify your critical assets. We'll work with you to figure out your ideal security priorities and to establish a security program. Then we'll align the governance aspects of your OA/OT for maximum efficiency.

Boundary Protection. If you're not careful, it's easy to create vulnerabilities between your OT and IT environments. We will work with you to create boundaries for isolation between those environments using the "hub and spoke" networking model. In this networking model, any communication or data from one spoke to another (for example from one connected manufacturing device to another) must travel through a hub. The hub can provide security checks and verify everything is working properly, avoiding the kind of cascading attacks that can tear through systems.

Identity. One of the most important pieces of modern-day digital transformation is identity. It forms the backbone of everything we do and is integral to the solutions we create. We will help you to create a secure identity platform that protects privileged identities against compromise. We'll also ensure a clean source path for identity management to make sure that you're always able to change what you need to.

Security Configuration. We'll work with your team to establish a strategic program for security configuration baselines. Together we'll define and update your management process and tools to ensure successful security operations.

Monitoring. Successful monitoring is a necessary part of successful cybersecurity. We'll work with you to integrate OT security monitoring within your systems. By using advanced threat protection technologies, we'll enable you to rapidly detect and respond to threats and even establish automated response process and recovery procedures to act in partnership with IT and plant engineering

Customer Reference: Global transport and logistics company goes digital to transform its operations³²

// Security was an aspiration that we weren't meeting. We needed to figure out how to better secure our business and our files and ensure that all of our data in every location was protected. //

Andy Laurence

Senior Director Head of Production Services, A.P. Moller – Maersk



32 <https://customers.microsoft.com/en-us/story/maersk-travel-transportation-microsoft-services>

Based in Copenhagen, A.P. Moller—Maersk is an integrated transport and logistics company with multiple brands and a global leader in container shipping and ports. The company is partnering with Microsoft Services on its digital transformation journey, moving five regional data centers to Microsoft Azure to improve performance and reduce its operational risk. Maersk selected Microsoft as its preferred cloud partner as it works to transform its operations, bolster its customer service, and generate new revenue streams.

// As we made the digital transformation, we needed a reputable partner with the right experience. Based on our selection criteria, we found that Microsoft Services came out the best. //

Andy Laurence

Senior Director Head of Production Services, A.P. Moller – Maersk



Read more: <https://customers.microsoft.com/en-us/story/maersk-travel-transportation-microsoft-services>

Why Microsoft Services?

Unlike some companies, we tailor our approach for each company – providing guidance and expertise in the areas that are most important to your company. With Microsoft Services as your partner, you'll have full access to our expertise in the Microsoft portfolio and our capabilities as well as those of our global network of professionals and partners. We are accountable for our solutions for the long term. We are flexible, working for you, and we have proven results that demonstrate our ability to lead change and deliver on our promise—to empower you to accelerate the value you imagine and realize from your digital experiences. We understand

the challenges you're facing and the products and services you use better than anyone; we built many of them.

Empowering business for what's next

Microsoft Services experts are on the leading edge of technology trends, providing thought leadership to help you develop innovative solutions for your business. Trusted by the world's largest organizations, our highly trained experts integrate decades of industry learnings, understanding of geographic constraints, and depth of knowledge of your organizations business needs to deliver exceptional service. Microsoft Services digital advisors, architects, engineers, consultants, and support professionals help you implement and adopt Microsoft products, services, software, and devices to solve, envision, and understand new possibilities for your business. We bring industry-leading knowledge of Microsoft products and how to secure your organization.

You can benefit from our more than 35 years of commitment to promoting security in our products and services, to helping our customers and partners protect their assets, and working to help ensure that your data is kept secure and private.

Take the next step

To secure your IT & OT environments, Microsoft Services has developed free 1-day and 3-day Solution Alignment Workshops designed to develop a secure modernization outlook for your operational technology. In this workshop we:

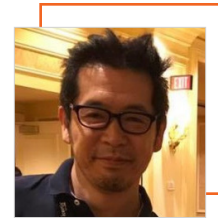
- **Discuss your top business priorities and concerns**
- **Evaluate your current Cybersecurity posture at a high level**
- **Determine where Microsoft can help modernize and secure your operational technology infrastructure**

By working with Microsoft to implement our Cybersecurity & Identity offerings, we drive immediate value for your business and help with crucial attack mitigation.

When will you invest in a safer future?

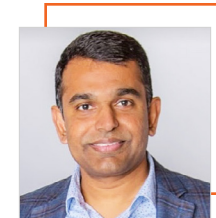
Contact your Microsoft representative to learn more. For more information about Consulting and Support Solutions from Microsoft, visit www.microsoft.com/services.

Credits



Kiyoshi Watanabe

Security Architect & Solutions Manager, Microsoft Services



Binil Arvind Pillai

Director Cybersecurity & Identity Solutions Strategy, Microsoft Services




Dottie Shaw

Architect, Manufacturing & Agriculture Solutions Strategy, Microsoft Services

Contributors

Conor Bronsdon

Olive + Goose



Microsoft Services empowers organizations to accelerate the value realized from their digital experiences.

Imagine. Realize. Experience.

microsoft.com/services

