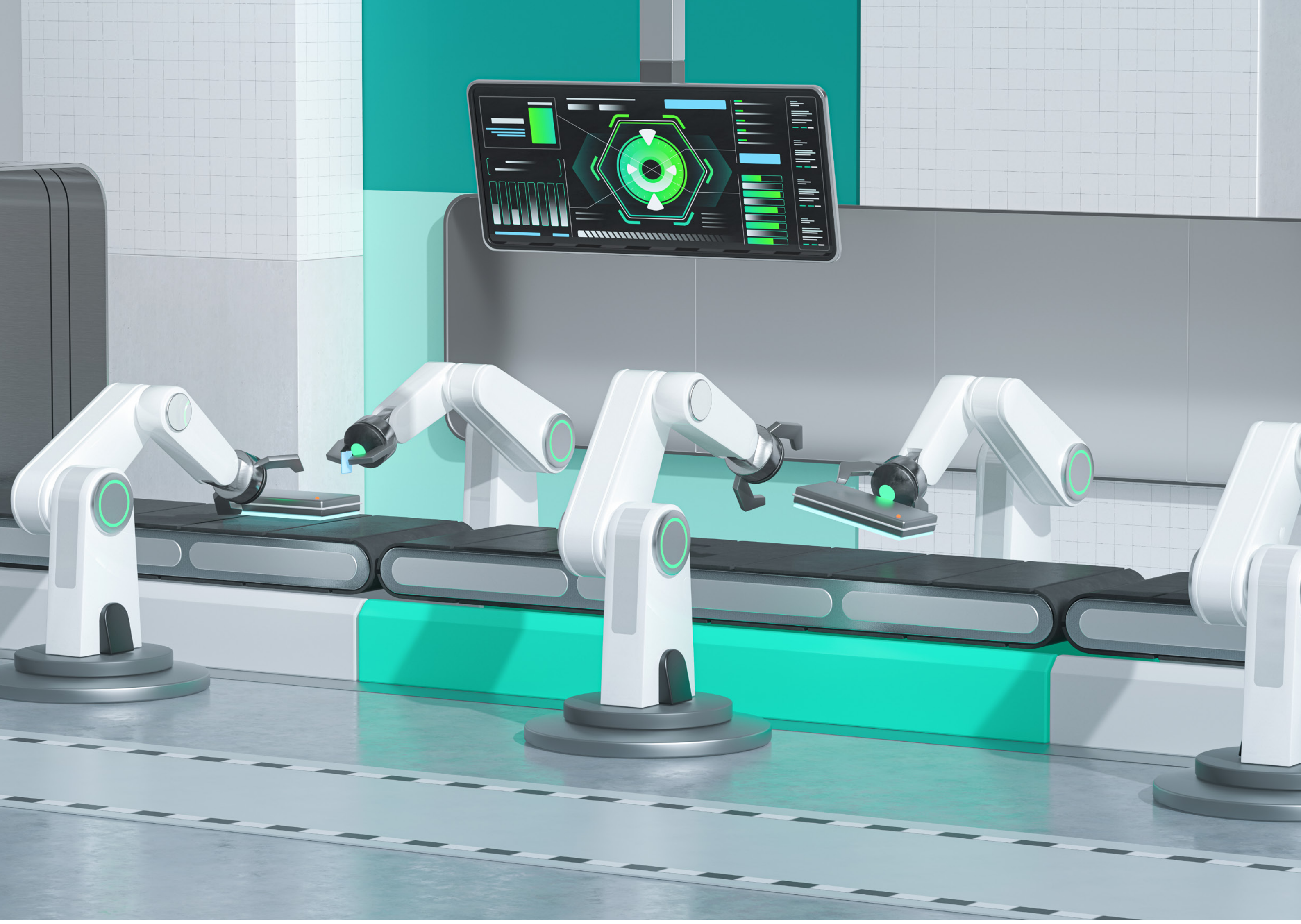


Building a safer future in Manufacturing

kaspersky BRING ON THE FUTURE

go.kaspersky.com/manufacturing

2021

Introduction

**“The first response to the global pandemic for many manufacturers was to go digital in their operations as fast as possible.”
Michelle Duerst, Research Vice President at Gartner**

The COVID-19 pandemic has resulted in great disruption to manufacturing. In response to wildly fluctuating demand, a worsening manufacturing skills shortage and chronic worldwide supply chain issues, the last two years have seen almost unprecedented adoption of technology. In addition to accelerating Industry 4.0 solutions (focusing on cyber-physical machine-to-machine automation and robotization), COVID-19 appears to have pushed manufacturing into the era of Industry 5.0.

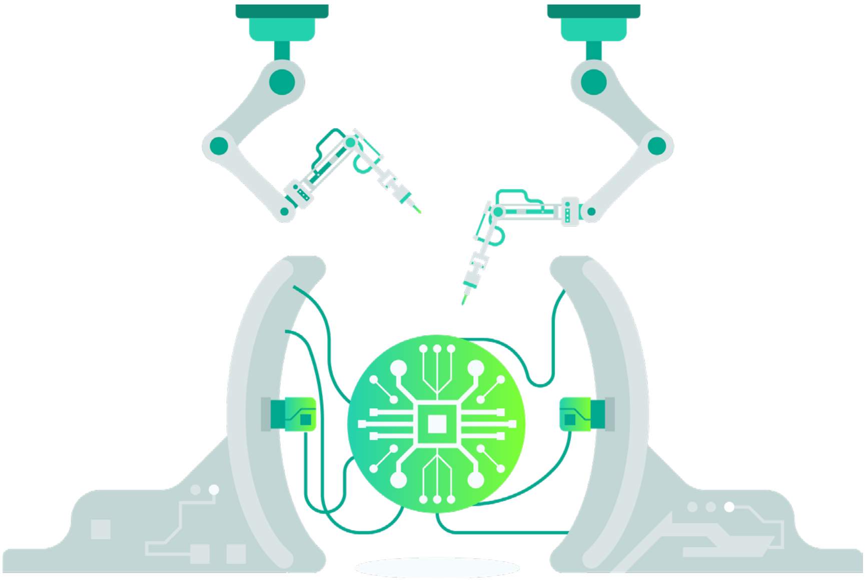
Industry 5.0., our collaboration with smart systems, harnesses human creativity, ingenuity and adaptability in tandem with intelligent manufacturing processes to optimise manufacturing resource-effciency and productivity. Computing design innovations leveraging the Internet of Things, AI, Industrial 5G and cloud computing have facilitated the roll-out of smart applications in Industry 5.0.

Almost every surface is being transformed into a sensor for data collection in order to generate real-time insights for manufacturers.

Manufacturers have responded fast and dynamically to the COVID-19 crisis and are set to reap the rewards offered by Industry 5.0.

A 2021 Deloitte survey concluded: 68% of manufacturing executives we surveyed report they are somewhat or very positive on business, up from 63% in 2020.

Each of the seven manufacturing trends highlighted in this paper cooperate with the other as part of a technology ecosystem to help enhance the other. This technology ecosystem means that the rate of new technologies is increasing exponentially.



Manufacturers have not in the past possessed or handled huge volumes of valuable digital data and sensitive information. This data is very tempting to cybercriminals but, in terms of cybersecurity, many manufacturers have not caught up with the increasing digitalization of their own industry. The CIO (or CISO) in the manufacturing industry has to adopt a perpetually future-ready mind-set. Alongside robust, proven cyberdefense systems, it is more important than ever that companies invest in cybersecurity training for every single member of staff according to their exposure and need.

In this paper, we will indicate some of the key cybersecurity risks associated with new manufacturing trends as a guide for manufacturers to focus on if they are to keep their operations (and bottom lines) safe in the age of Industry 5.0

Fast expansion of the Industrial Internet of Things (IIoT)

Supply chain – the importance of resilience

Reshoring manufacturing and near-sourcing suppliers

The significance of environmental, social, and governance (ESG) factors for manufacturing

The continued rise of Intellectual Property (IP) and data theft

Innovative opportunities with 3D printing

The benefits of design simulation technologies

Trend #1: Fast expansion of the Industrial Internet of Things (IIoT)

$1.1 trillion

The global IIoT market was valued at about $216.13 billion in 2020 and is expected to grow to about $1.1 trillion by 2028.
Source: Grand View Research

The Industrial Internet of Things continues to expand apace in 2021. During the COVID-19 pandemic applications, remote monitoring and preventative maintenance interactions reducing reliance on personnel have been growing exponentially. Manufacturers are fast producing items with their own devices and controllers to communicate with the world in which their customers operate. Spanning everything from supply chain to logistics and shipping, devices interact with the environment of products as they are used.

In 2022, 45% of manufacturing executives surveyed expect further increases in operational efficiency from investments in industrial Internet of Things (IIoT) that connect machines and automate processes.

The value of the IIoT lies in its power to enable manufacturers and their customers, to create an integrated automated ecosystem in which every product and element communicates to drive efficiencies unimaginable in traditional systems. IIoT devices facilitate informed strategic decisions and are routinely deployed to reduce costs through real-time monitoring, facilitate automation, digitalize inventory management and improve safety.

Current numbers of sensors at typical process plants cluster around 40,000 sensors. The IIoT will increase those numbers exponentially to something over 250,000 sensors per plant. Each of those sensors will be producing near real-time data at an update rate of four times a minute or 250 milliseconds per datum. That means each sensor will be producing over 5,000 data points per day. That's 1.44 billion data points per plant, per day.

How to manage the IIoT securely

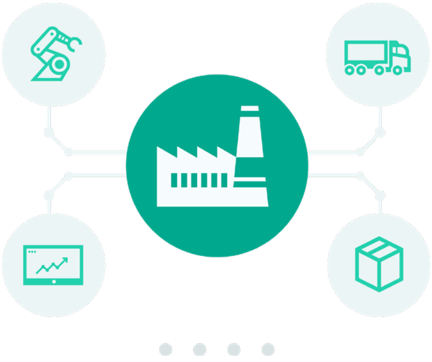
IIoT technologies are perceived to be the most crucial element of smart factories, and are fast becoming fully integrated into manufacturing and OT installations globally. Faced with growing cybersecurity threats, organizations urgently need to adopt a proactive prevention strategy in order to effectively secure IT/OT networks.

308%

In 2020, IIoT vulnerabilities increased by 308%, reflecting both emergent threats and the rapidly growing use of these sensors across industries.
Source: Skybox Research Lab

The IIoT brings with it multiple security issues. The probability of data breach grows in proportion to the increase in number of connected devices and expansion of an organization's network in the cloud. The sheer scale of connected hardware is multiplying cybersecurity risk. Industrial control systems are often operating on obsolete and vulnerable software. Exposed hardware also enables cyber intrusion, potentially affecting all connected IIoT devices. Insufficient data encryption is a further prevalent weakness in manufacturing systems and their connected devices.

Access to a single IIoT can facilitate access to the entire manufacturing process. Manufacturers need to ensure IIoT providers incorporate latest security systems and also to limit the extent to which each IIoT device is linked into the entire network. Manufacturers need to compile a complete, accurate, up to date inventory of IIoT devices/sensors deployed. This should include detailed information about their configuration and posture to assess where assets are vulnerable and to reshape security to address specific issues. To gain better visibility over the entire network alerts needed to be coordinated across IT/OT networks to gain complete visibility.



Trend #2: Supply chain – the importance of resilience

All modern applications are made up of services that are connected by APIs. Each of these services need to be authenticated and monitored as attackers can use your suppliers' API access to critical data to their advantage.
Source: Gartner

The COVID-19 pandemic and ongoing turbulence in global supply chains have highlighted just how important global manufacturing supply chain resilience is. Manufacturers are now hastily redesigning supply chains to withstand disruption. Current supply bottlenecks have been caused by less available and more costly labour, (take for example, the ongoing chronic shortage of truck drivers across Europe and the US), higher costs of raw materials and freight transport. Minimum inventories and unstable suppliers coupled with unexpectedly higher demand contribute to container port congestion. Delays cause price rises leading to inflation that in turn affects the global economy.

An integral part of Industry 5.0 collaboration between humans and smart systems, the supply chain is extended to encompass the full range of software, RFID chips, devices and other technology that must be sourced externally in order to maintain competitive edge with efficiency. Data integration and data analytics are the key to the visibility and transparency of supply chains. A fully integrated supply chain ensures a far more flexible response to potential disruptions.

Reliant on 4PL and 3PL providers, as well as on software and components from an expanding range of suppliers, manufacturers must act now to ensure that every single link of their supply chain is as secure as their own.

How to manage supply chains securely

It is estimated that there will be four times more supply chain attacks in 2021 than in 2020. With half of the attacks being attributed to Advanced Persistence Threat (APT) actors, their complexity and resources greatly exceed the more common non-targeted attacks, and, therefore, there is an increasing need for new protective methods that incorporate suppliers in order to guarantee that organizations remain secure.
Source: ENISA

The more organizations involved in a manufacturing process, the higher the probability that a cyberattack on one organization spreads to their manufacturing partners.

Hardening internal endpoints is a far easier endeavor than hardening resources sourced externally. As well as packing cybersecurity guarantees into the fiber of every SLA and purchase agreement, manufacturers must implement cyber defense systems that keep track of how every devices and entity is integrated into the supply chain system as it shifts and evolves. This is further complicated by components built on unsecure legacy devices. Unintentional flaws lead to vulnerabilities and inevitably to system compromise.

Steps to take include putting in place a zero-trust approach where all applications and user accounts have to be verified. Manufacturers need to regularly audit all vendors' compliance with applicable cybersecurity standards and implement a least-privilege policy to restrict every user's access to data to the minimum required to carry out necessary work.

Trend #3: Reshoring manufacturing and near-sourcing suppliers

"COVID-19 has revealed the U.S. dependency on offshore manufacturing, especially China. [...] As the pandemic shows, we can suddenly be in the impossible position of not having enough critical supplies." Harry Moser, President of the Reshoring Initiative

Reshoring of manufacturing components and complete plants to domestic production is accelerating. The wage gap between traditionally lower income countries and the US and Europe is shrinking. This is especially true for China. Manufacturing has become more complex and lower income countries are less able to invest in the necessary infrastructure. At the same time, global transportation costs have gone up. New technology — automation platforms, AI and robotics – continually reduce the amount of human involvement (number of workers) needed in a manufacturing facility.

The COVID-19 pandemic has also led to supply disruptions, especially from China. Manufacturers are looking to bolster supply resilience by onshoring or near-sourcing raw materials and suppliers. The US and Europe, mindful of security and public welfare concerns, are also actively encouraging industry to localize key supply chains.

How to manage reshoring securely

"Speed also lessens security and if production is ramped up too quickly, infrastructure could be inadequately secured. Legislation and regulation also take time, many years in some cases, so it will likely lag behind the actual risk."
Tony Howlett, CISO at SecureLink

Increased onshore investment in onshore manufacturing attracts cyberattackers looking for lucrative targets. The exponential growth of connection and digitalised equipment in smart factories make threats and vulnerabilities more likely. The pace at which manufacturers are reshoring and near sourcing suppliers also means cybersecurity lags behind.

Compromised OT systems will halt or delay production and can result in faulty or sabotaged goods. The number one cybersecurity priority of a recently reshored manufacturing facility is to gain complete visibility into all OT and IT connected devices.

Trend #4: The significance of ESG for manufacturing

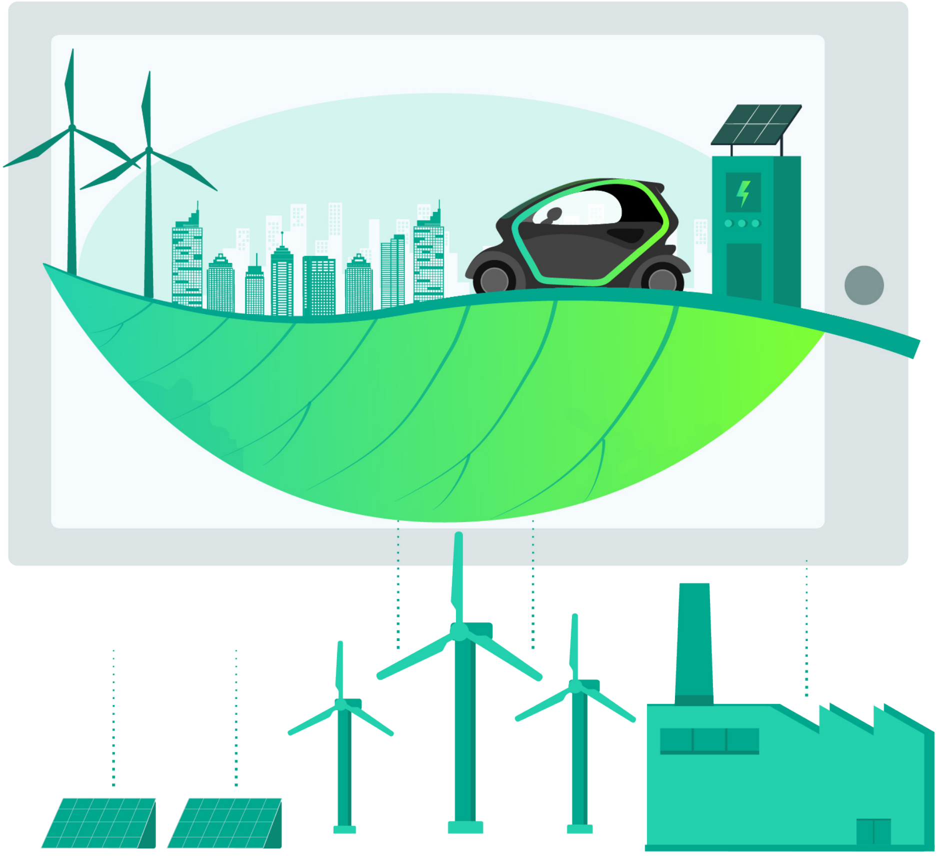
95%

"95% of manufacturing executives we surveyed expect their organizations will invest more in ESG areas in 2022 than in 2021".
Source: Deloitte's 2022 manufacturing industry outlook.

Environmental, social, and governance factors (ESG) are beginning to reshape manufacturing. Sustainable manufacturing as defined by the EPA is: "the creation of manufactured products through economically-sound processes that minimize negative environmental impacts while conserving energy and natural resources. Sustainable manufacturing also enhances employee, community and product safety."

The pressure to adopt more sustainable development is growing in the manufacturing industry. EPA data reveals the manufacturing and industrial sector were responsible for 23% of greenhouse gas emissions in 2019.

Major manufacturers globally (notably the automotive industry) have pledged to go green and launched initiatives to meet ambitious ESG commitments and implement best practices. Legislation and regulatory changes issues also play a part in pushing forward the adoption of ESG efforts.



The evolving concept of Ecosystem Partnerships, networks of partners working for common objectives, is shaping up to be an integral part of ESG facilitating shared emission reduction and investments in sustainable initiatives.

Consumer behaviour is also changing fast and manufacturers are having to adapt to new consumer requirements for production transparency and bringing products to market in an environmentally friendly manner.

A May 2021 published global report by the Economist Intelligence Unit and the WWF found that online searches for sustainable goods have risen 71% in the past five years.

Crucially also investors like organizations embracing ESG. Investment capital is more freely available for manufacturers taking steps to implement sustainable development. Large investors have shifted their focus to making sustainable investment a priority.

A US SIF Foundation 2020 "Report on US Sustainable and Impact Investing Trends" revealed sustainable investing assets totalling $17.1 trillion, a 42% increase over 2018.

In conclusion, manufacturing organizations have come to understand that prioritizing ESG is a key step towards future profitability and competitive advantage.

How to manage ESG and sustainable development securely

Cybersecurity is now viewed as a key environmental, social and governance issue. Manufacturers store huge amounts of data and data governance is an integral part of ESG. Companies factoring ESG into their operations face a greater fallout risk from investors regarding data privacy issues. Data breach revealing confidential personal information will likely jeopardize investor funding and even the future of the entire operation. Government regulators are also constantly reviewing demands related to data privacy. Manufacturers will need to intensify data security and focus more attention on protecting their customers.

The first step is a data discovery audit. It does not matter how rigorous an organizations' security procedures are if there is insufficient visibility into the scale of stored sensitive private data and who currently has access to this data. Secondly it is necessary to limit access to private data on a strict, need-to-know basis. Thirdly, where possible, organizations need to remove not-needed or redundant data from their infrastructure altogether.

Trend #5: The continued rise of IP and data theft

Intellectual Property theft is not a new trend but a growing one. Internal errors and misuse (such as privileged access) are responsible for more breaches than malware according to the 2020 Verizon Data Breach Investigations Report.

Manufacturing relies on proprietary know-how, research and inside information to stay competitive, enter new markets and expand business. Intellectual property theft and insider threat has the potential to destroy a manufacturing company over the longer term.

Threat actors act for a variety of motives — copying (to save on R&D costs and allow for targeted disruptive innovation), undercutting a competitor, gain leverage in purchase negotiations.

Product and design fake is getting easier in the digital age and penetrating the global market. Once out in a digital format, a design cannot be returned to the exclusive domain of its rightful owners. Years of R&D can be lost. It's harder than ever for consumers to tell a fake product from an original — and many no longer care.

State-sponsored IP theft accounts for billions of dollars of intellectual property theft each year. One of the reasons US manufacturers are reshoring operations from China is the perception that they have been subjected to systematic IP theft.

The FBI estimates that cyberattacks targeting IP and critical business data cost US businesses alone up to $600 billion a year.

The competition to develop COVID-19 vaccines illustrates the global problem of IP theft. In 2020, more than 200 attacks on pandemic infrastructure and vaccine research were recorded by the UK's National Cyber Security Centre (NCSC). In October of the same year, Indian drug manufacturer, Dr Reddy's Laboratories, shut key plants worldwide after a cyberattack targeting vaccine research. IBM also discovered cyberattacks on vaccine distributors.

How to secure against IP theft and Insider risk

To prevent insider IP theft, companies need to fully segment their manufacturing systems, allowing access on a strictly need-to-know basis. But segmentation is insufficient. Need-to-know access has to work hand-in-hand with robust cybersecurity measures that harden and protect every single element in the manufacturing chain.

Robust cybersecurity measures must be based on an awareness of the interoperability and reliance on other players within the supply chain. Manufacturers have to undertake frequent audits of their supplier and vendor security measures to ensure IP and data are protected throughout an increasingly complex chain. In addition, manufacturers need to audit their entire digital estate, to categorize, prioritize and protect data in the most appropriate way.

All manufacturing personnel potentially have exposure to IP secrets and need to receive necessary cybersecurity training and awareness. Manufacturers need to implement robust compliance policies, with detailed expectations and a clear understanding of the penalties for breaching those policies.

Trend #6: Innovative opportunities with 3D printing

Covid-19 has provided "a glimpse into how 3D printing can be used temporarily to alleviate the strain on supply chains during demand surges and shortages, as it did with medical equipment."
Source: Manufacturing Global

The efficiency, flexibility, speed and ecology of 3D printing and additive manufacturing represent a huge opportunity for manufacturers everywhere. Innovators are integrating 3D printing into traditional production processes to achieve more sustainable, cheaper components, and remain closer to customers. With an initial investment in the right machines, 3D printing democratizes manufacturing, putting it within reach of small start-ups who leverage the technology to enter new markets and grow exponentially.

Additive manufacturing market grew by 21% in 2020 and is expected to continue to grow by 17% annually over the next three years.

By 2029, the industrial 3D printing business is expected to generate about $55 billion per year.

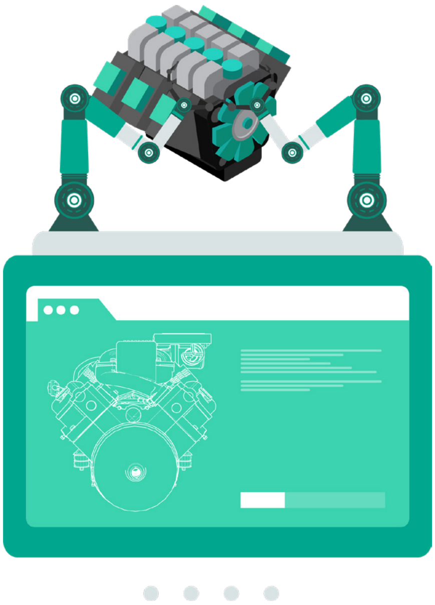
In 2021 the United States Department of Defence announced a drive to accelerate the adoption of additive manufacturing technology explaining: “It is distributed and accessible through its smaller footprint, and lower cost. It’s innovative, allowing us to create new designs like we’ve never seen before. And it allows us to iterate and prototype more quickly, supporting rapid design cycles.”

How to manage 3D printing securely

The digitized world of additive manufacturing is made possible by the transfer and storage of vast amounts of data, much of it highly confidential, for example complete manufacturing networks. The wide scale adoption of IIoT devices in 3D manufacturing facilities makes them vulnerable.

Cybercriminals can breach servers and cloud facilities or reverse-engineer 3D printed parts in order to steal IP, causing the manufacturer significant financial losses. Process sabotage can be effected by infiltrating 3D printers to modifying part data, leading to potentially catastrophic failures.

Much of the risk is associated with users not securing 3D printer and AM systems sufficiently because they perceive them to be a tool, not information technology requiring the same cybersecurity controls as other connected systems. This underscores the need for cybersecurity training within 3D facilities to better understand the risks and how to combat them. Encrypting all CAD Files and regular inspections to confirm a printed item matches the CAD are necessary security conditions within the environment of a secure network.



Trend #7: The benefits of design simulation technologies

Manufacturers' use of design simulation technology, or computer-aided design, continues to soar. Improvements in design simulation technology modeling real-world product behaviour have led to its wide-scale adoption. Manufacturers gain competitive edge from stimulating innovation at lower cost and offering product designers' unique insights into how to better manufacture parts. Leveraging complex mathematical equations to simulate the performance and quality of potential product and packaging designs can shave precious dollars off the R&D process, and reduce the potential for producing products that turn out to be duds.

The IIoT ecosystem's feedback potential also adds to the power of such technology. Sensors can relay performance information back to the manufacturer in real-time, including limitations and highly pinpointed opportunities for design improvement and refinement.

Organizations are applying design simulation technology across a whole spectrum of uses including measuring fuel economy, thermal and flow analysis, structural behaviour, crash-worthiness, controls and structural development and more.

Products created off the back of design simulation technology are 100% accurate representations of the manufacturing company's ideal design. Liberated from the conceptual confines of assumptions and prototyping, manufacturers can take a direct route to product perfection, provided their systems are robustly defended from cybercriminals.

How to manage design simulation technologies securely

The enormous software cost is not the only challenge that manufacturers face when it comes to deploying design simulation technology. Design simulation technology opens up more attack entry points for cybercriminals to attack.

The algorithms on which design simulation is built are an example of the universal trend towards a level of complexity which lies far beyond the understanding of all but a highly specialized set of experts. Their expertise is procured externally, rather than being part of a manufacturer's internal human resource pool, opening up another avenue of cyber risk.

Whilst empowering manufacturers to design 'pre-prototyped' products, the software also risks removing human monitoring from the process, and (thanks to its complexity and sophistication) adding a barrier to entry that prevents humans from identifying and responding to errors caused by cyberattacks.

Failing to wake up to the changing environment of this new technology could make manufacturers significantly more vulnerable to threats that could potentially decimate everything they design and produce.

Summary

Disruptions to manufacturing rapidly affect the worldwide economy leading to long delays, chronic shortages, price inflation and potential economic decline and social unrest. Manufacturing is a global business, more than any other. A cyberattack on a manufacturing facility can have immediate consequences on the other side of the world. The COVID-19 pandemic has accelerated the pace of digitization of manufacturing technology and opened up new frontiers for cyberattack. Now more than ever, manufacturers need effective security against the potentially devastating consequences of cybercrime.

In today's extremely volatile and challenging environment, Kaspersky is a pioneer in helping the manufacturing industry adapt best security strategies in today's volatile and challenging environment. Our perfectly engineered, tailored solutions and services – assisted by world-leading security intelligence – protect data and business continuity 24/7 against advanced threats and targeted attacks – mitigating risks, detecting attacks earlier, dealing effectively with live attacks and fortifying future protection.

Our **stage-by-stage** cybersecurity approach designed to clarify which level of security as well as which specific solutions suit your organization best. The stages provides a set of easily managed threat protection measures coordinating seamlessly with one another to meet the needs of each individual organization, and offer a cybersecurity roadmap assuring smooth transition from one IT security maturity level to another when the time comes.

Kaspersky's step-by-step cybersecurity approach

1

Kaspersky Security Foundations – essential core of cloud-based, automated protection for all devices, VDI and hybrid server infrastructures, before organizations advance seamlessly to …

2

Kaspersky Optimum Security – for organizations requiring more specialized security against new and evasive threats, before effortlessly implementing …

3

Kaspersky Expert Security – for organizations with established mature IT security teams combatting the most complex targeted attacks.

Cybersecurity maturity level	Solution
IT Smaller organizations without a specialized IT security team	**What** Kaspersky Security Foundations **How** Implement fundamental security for organizations of any size and infrastructure complexity, delivering cloud-managed automatic prevention of commodity cyberthreats on any devices, VDI and hybrid server infrastructures. ▪ **Endpoints:** Protect every endpoint in your organization with Kaspersky Endpoint Security for Business; Kaspersky Embedded Systems Security ▪ **Cloud:** Benefit from borderless security with Kaspersky Hybrid Cloud Security ▪ **Network:** Secure your perimeter with Kaspersky Security for Mail Server; Kaspersky Security for Internet Gateway ▪ **Data:** Safeguard valuable and sensitive data with Kaspersky Security for Storage ▪ **Security Management:** Access expertise with Kaspersky Premium Support; Kaspersky Professional Services
IT security Organizations in need of advanced defenses, but with limited specialist IT security resources	**What** Kaspersky Optimum Security **How** Combat evasive threats with effective endpoint detection and response and continuous security monitoring – but without prohibitive costs or complexity ▪ **Advanced detection:** Boost ML behavior analysis, sandboxing, threat intelligence and automated threat hunting* with Kaspersky Sandbox, Kaspersky Threat Intelligence Portal and Kaspersky Managed Detection and Response Optimum ▪ **Analysis and investigation:** Enhance threat visibility and simplified investigation process with Kaspersky Endpoint Detection and Response Optimum ▪ **Rapid response:** Deploy automated in-product response options, as well as guided and managed response scenarios* with Kaspersky Endpoint Detection and Response Optimum **and** Kaspersky Managed Detection and Response Optimum ▪ **Security awareness:** Equip employees with automated tools at all levels and develop key cybersecurity skills with Kaspersky Security Awareness Training *Supported by Kaspersky experts

Mature and fully formed IT security team and/or dedicated SOC

- Have a complex and distributed IT environment
- Are a highly likely target for complex and APT-like attacks
- Have a low risk appetite due to high costs of security incidents and data breaches
- Are concerned about regulatory compliance

What
Kaspersky Expert Security

How
Complete mastery over the most complex and targeted cyberattacks

- **Equipped:** Equip your in-house experts to address complex cybersecurity incidents. Benefit from a unified cybersecurity solution. Kaspersky Anti Targeted Attack Platform with Kaspersky EDR at its core empowers your team with XDR capabilities.

- **Informed:** Enrich your knowledge pool with threat intelligence and upskill your experts to deal with complex incidents:
  - Integrate actionable, immediate threat intelligence into your security program. Kaspersky Threat Intelligence gives you instant access to technical, tactical, operational and strategic threat Intelligence.
  - Develop your in-house team's practical skills, including working with digital evidence, analyzing and detecting malicious software, and adopting best practices for incident response, with Kaspersky Cybersecurity Training.

- **Reinforced:** Call upon external experts for security assessment, immediate support and back-up:
  - Take advantage of immediate support from the Kaspersky Incident Response team of highly experienced analysts and investigators to fully resolve your cyber-incident, fast and effectively.
  - Bring in a second opinion and managed threat hunting expertise from a trusted partner with Kaspersky Managed Detection and Response, so your in-house IT security experts have more time to spend reacting to the critical outcomes requiring their attention.
  - Understand just how effective your defenses would really be against potential cyberthreats, and whether you're already the unwitting target of a long-term stealth attack, through Kaspersky Security Assessment.

Targeted Solutions

What	How
Kaspersky Industrial Cybersecurity	KICS offers a holistic approach to industrial cybersecurity, bringing value to any stage of the customer's OT security process – from cybersecurity assessments and training to advanced technologies and incident response. An ecosystem of integrated products and services allows to secure operational technology layers and elements of your organization — including SCADA servers, HMIs, engineering workstations, PLCs, network connections and even engineers — without impacting on operational continuity and the consistency of industrial process.
Kaspersky ICS Threat Intelligence	Kaspersky ICS Threat Intelligence provides in-depth intelligence and greater awareness of malicious campaigns targeting industrial organizations, as well as information on vulnerabilities found in the most popular industrial control systems and underlying technologies. All threat intelligence research is done by the Kaspersky ICS CERT, a member of FIRST – the leading international technical group of 540 government and private accredited CERTs. The intelligence is provided in both machine-readable and human-readable formats enabling its smooth integration into existing security processes.

Cyberthreats News: www.securelist.com

IT Security News: www.kaspersky.com/blog

Threat Intelligence Portal: opentip.kaspersky.com

Technologies at a glance: www.kaspersky.com/TechnoWiki

Awards and recognitions: media.kaspersky.com/en/awards

Interactive Portfolio Tool: kaspersky.com/int_portfolio

kaspersky BRING ON THE FUTURE