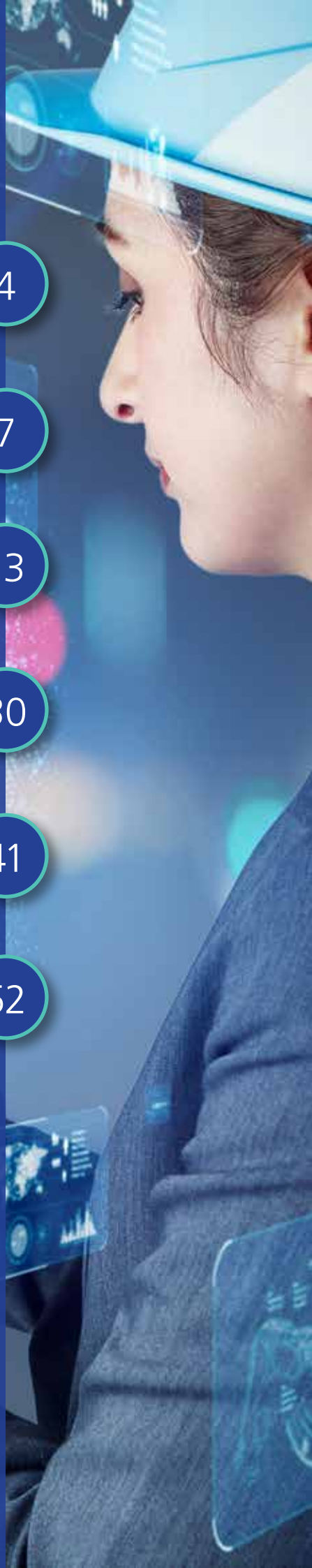
INTESA SANPAOLO
INNOVATION CENTER

INDUSTRY TRENDS REPORT
INDUSTRIAL & MECHANICS SECURITY OF THINGS

FROST & SULLIVAN

CONTENTS



EXECUTIVE SUMMARY

In 2022, there were 35.37 billion (b) connected Internet of Things (IoT) devices deployed globally with this number expected to reach 73.79 b by 2027, a compound annual growth rate of 17.3%. IoT devices are characterised by their capacity to measure data, grant identities, form interconnections and generate insights and encompass both *consumer* and *industrial* applications with machine-to-machine communication booming across sectors.

Whilst the industrial IoT (IIoT) brings many advantages, the proliferation of connected devices has inevitably opened companies' assets to malevolent cyber attacks.

Organisations face a growing range of security challenges and vulnerabilities with malware attacks alone leaping from 60 million (m) globally in 2021 to 112 m in 2022. Recent and high profile IoT security lapses across industries include victims such as Colonial Pipeline, Tesla and Abbot Healthcare. These and other incidents are heightening market participants' and third parties' focus on tightening cyber security in the context of the industrial IoT.

Across **industries**, the convergence of information and operational technologies (IT/OT) has created a wider "surface of attack" and puts companies at risk. In parallel, the need to comply with existing and emerging regulations means that cyber security issues are moving from the factory floor to the boardroom while the pandemic and its lasting impacts have meant that many employees notably gained and continue to enjoy remote access to critical OT.

In Italy, a 2022 Frost & Sullivan survey revealed that 85% of industrial companies have been negatively affected by a cyber-attack in the course of the last two years and 21% of respondents listed system vulnerabilities as their biggest concern.

As a result, industrial market participants across countries and regions are adopting cyber security strategies which safeguard IoT devices against threats. Concretely, players are shifting their focus from protection to detection with the deployment of effective OT alert management systems to reduce the risk of false positives forming a key part of this together with the use of active querying to discover dormant IoT devices across environments.

Early adopters of these and other approaches are critical infrastructure industries while uptake in general process and discrete manufacturing is much less mature.

Industrial players here and elsewhere are partnering with third parties to deliver fully integrated solutions that help to lower their risk while IT and OT cyber security vendors are, in turn, entering each other's spaces to expand their portfolios and provide scalable offerings.

Companies to watch include Claroty (US) which provides a comprehensive solution to secure IoT devices on industrial sites and Dragos (US) which focuses on enabling asset visibility as well as Nozomi (US) which launched Vantage, the first software as a service platform for addressing OT/IT threats in manufacturing. Other notable European players include Applied Risk (Netherlands), Darktrace (UK) and ICSEC (Poland) as well as Radiflow (Israel).

Moving forwards, cyber security solution vendors will look to artificial intelligence to detect advanced or unknown threats and also to differentiate themselves.

In the **healthcare** industry, the threat of cyberattack is particularly acute with 90% of data now managed through medical devices and the internet of medical things (IoMT).

Greater connectivity is coupled with an increase in the frequency and severity of threats as online scams, hacks and negligent insider incidents are all proliferating. At the same time, healthcare players currently take 150% more time to identify cyber risk than other industries which is resulting in disproportionately higher costs.

Market participants are therefore growing their spend on modernising infrastructure and networks, protecting cloud-native platforms, securing medical devices and IoMT enablers and safeguarding third-party applications from common cyber threat agents such as ransomware, phishing, credential harvesting and social engineering attacks.

Protecting application programme interfaces from preventable breaches will become the frontline of cybersecurity activity in the medium to long term with the overall healthcare space addressed by many of the same vendors that occupy the broader industrials sector and participants jockeying for space in an attractive segment.

The **automotive** industry, like healthcare, is particularly vulnerable as 95% of passenger cars are expected to call on embedded telematics by 2026.

Identifying all possible vulnerabilities within a *connected* vehicle is therefore becoming a key prerequisite to mapping and addressing every scenario with examples of recent breaches include vehicle and server hacks as well as data leaks.

In this context, many automotive manufacturers have found that high costs and limited expertise challenge their ability to develop effective security roadmaps. Their response to date has largely been to develop their in-house capabilities and/or to partner with external IT service vendors to mitigate cyber risk. However, the advent of WP.29 regulations, which place the onus on car makers to manage threats across the supply chain, changes the game.

Premium automakers are reacting by looking to partners for consulting services while mass market manufacturers are seeking end-to-end security solutions. Cybellum (Israel), for example, offers a digital twin platform for threat assessment whereas Upstream (USA) offers a cloud solution to deliver on all WP.29 needs.

In the future, the automotive cyber security picture will become even more complex as *autonomous* vehicles become a >$100 b market opportunity. Here, the scenarios for attack are multiple and still in the process of being defined. It is expected that, given the number of deep learning modules that *autonomous* vehicles will incorporate, addressing artificial intelligence-based threats will become essential.

This report examines the evolving threat landscape that stems from the connected IIoT and the emerging response to best safeguard the *"security of things"* across the industrials, healthcare and automotive sectors. It also takes into account the long-term strategies and short-term measures that are being put in place by direct market participants and third-party vendors to address the threat from cyber attacks.

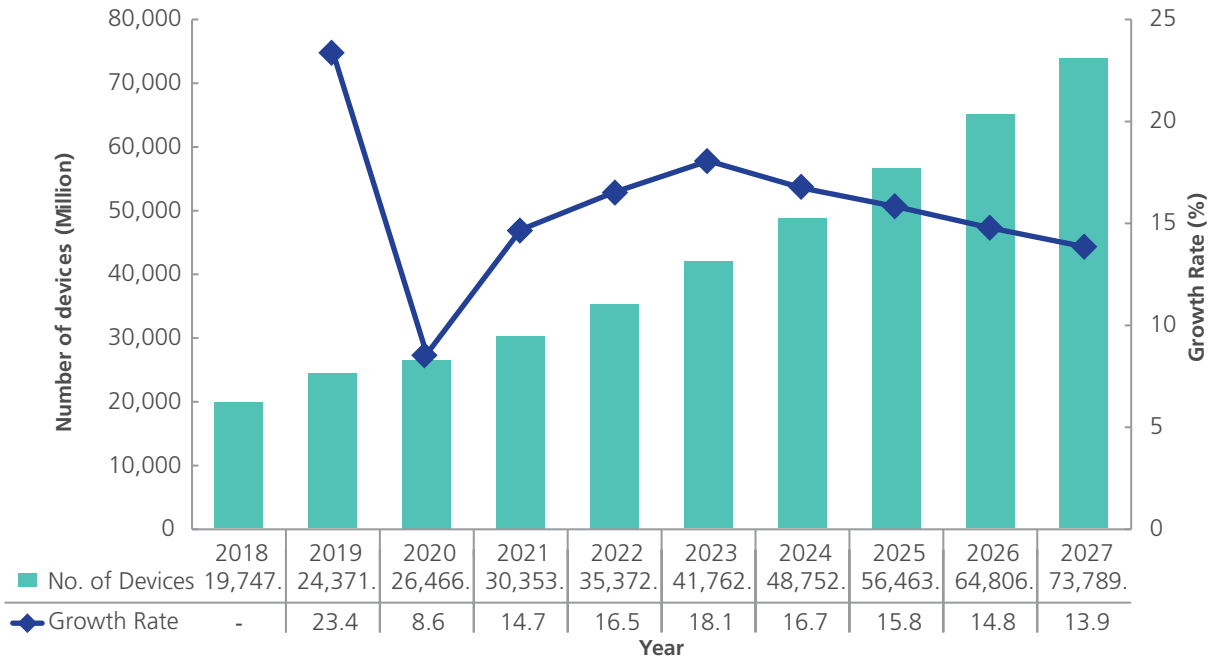
INTRODUCTION

In 2022, there were 35.37 billion (b) connected Internet of Things (IoT) devices deployed globally with this number expected to reach 73.79 b by 2027, a compound annual growth rate (CAGR) of 17.3%. IoT devices are characterised by their capacity to measure data, grant identities, form interconnections and generate insights

To qualify as an IoT device, any component, product, application or service must form part of a larger solution that comprises one of more of these four elements.

In 2021, the total IoT market, comprising professional and managed services, hardware, platforms and software and connectivity services, generated revenues of $190.26 b.

CONNECTED IOT DEVICES, GLOBAL, 2018-2027



Source: Frost & Sullivan

They encompass both *consumer and industrial* applications with machine-to-machine communication booming across sectors

Consumer IoT services include wearables and personal monitoring gadgets, such as smart watches or fitness trackers, and internet-enabled connected appliances and devices for the home, for example cloud-based intelligent personal assistants and smart speakers.

Industrial IoT (IIoT) services seek to leverage machine-to-machine (M2M) communication and quality control to increase the productivity and efficiency of industrial systems in units such as factories or manufacturing bases.

These include heating, ventilation and air conditioning (HVAC), supervisory control and data acquisition (SCADA) and M2M communication-based industrial monitoring systems.

Concretely, Frost & Sullivan defines the IIoT market as encompassing devices for portable asset tracking, third party commercial & fleet telematics, vehicle lending, smart grids, smart homes, factory & industrial automation, vending, point of sale (POS) & transaction terminals, healthcare & medical applications, consumer electronics, original equipment manufacturer (OEM) telematics (the "connected car"), usage based insurance, infotainment & aftermarket telematics, building automation, security & surveillance, fixed asset monitoring, digital signage and wellness applications amongst others.

Whilst the industrial IoT brings many advantages, the proliferation of connected devices has inevitably opened companies' assets to malevolent cyber attacks

Demand for cyber security solutions in the industrial sector is being driven by increasing digitization and connectivity. The convergence of *information and operational technologies* (IT/OT) is putting organizations and infrastructure at heightened risk of cyber attack.

Despite this, many industrial firms still lack adequate cyber security measures. Infrastructure owners and operators must increasingly safeguard their environment, ensure complete visibility of assets, identify vulnerabilities in their systems and implement solutions that identify and respond to potential threats while addressing the knowledge gap between IT/OT.

Source: Frost & Sullivan

Organisations face a growing range of security challenges and vulnerabilities … Challenges include;

- *Unique threats* with hyperconverged environments that simplify hybrid cloud deployment and orchestrate components, such as *application programming interfaces* (APIs), which provide programmability to and from public cloud locations
- *Device fragmentation* with the use of various proprietary protocols for communication making scaling security across verticals complicated
- *Unsafe deployments* with devices without perimeters allowing deployment in unsafe environments and providing virtual and physical access
- *Device constraints* with on-component security technologies and encryption for resource-constrained devices becoming an issue
- *Unwieldy operations* with inefficient security operations, especially due to the large volumes of real and false alarms, emerging as a challenge

Vulnerabilities include;

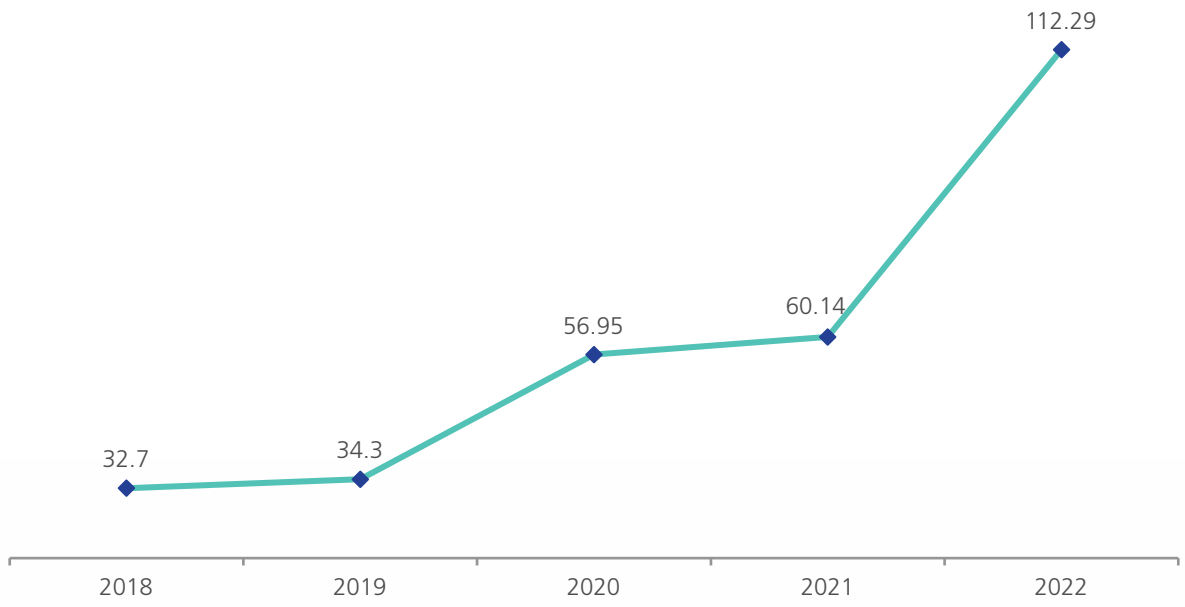
- *Hardcoded credentials* including the use of easily brute-forced, unchangeable credentials, such as backdoors in firmware or client software
- *Leaked keys* including insecure private key generation, storage and management and applications leaking private keys
- *Weak encryption* including limited on-device computing resources that result in insufficient entropy to generate private keys and encrypt data
- *Insecure ecosystems* including compromised devices through web, backend API, cloud or mobile interfaces in the network outside of the device
- *Missing updates* including a lack of firmware validations, anti-rollback mechanisms and notifications of security changes

Source: Frost & Sullivan

… with malware attacks alone leaping from 60 m globally in 2021 to 112 m in 2022

Malware, a portmanteau for *malicious software*, is specifically designed to disrupt, damage, or gain unauthorized access to a computer server, client or network and can infect industrial and consumer IoT devices. Malware is typically classified into one or more sub types and includes viruses, worms, ransomware, spyware, adware, wiper and keyloggers.

ANNUAL MALWARE ATTACKS, MILLIONS, GLOBAL, 2018-2022



Source: Frost & Sullivan

Recent and high profile IoT security lapses across industries include victims such as Colonial Pipeline, Tesla and Abbot Healthcare

In *2021*, a single password lapse caused the failure of the largest fuel pipeline in the United States (US), resulting in shortages along the East Coast. The compromised credentials of a dormant but usable account and the use of an outdated virtual private network (VPN) led to a ransomware attack on the **Colonial Pipeline**. The VPN account did not use the latest multifactor authentication, leading to its cancellation.

In *2018*, Lennert Wouters, a doctorate computer science student at the Catholic University of Leuven in Belgium, developed an approach to rewrite and hijack the firmware of **Tesla** Model X key fobs. He exploited a bug in the insecure updating procedure of the key fobs and was able to drive away with a car in under two minutes.

In *2017*, more than 450,000 pacemakers were recalled owing to security concerns after the US Food & Drug Agency (FDA) confirmed their vulnerability. The incident impacted several models and required **Abbot Healthcare** clients to visit a clinic for a patch. Security experts warned that cyber criminals could access wireless pacemakers and cause patients to experience an erratic heartbeat or even heart attack.

These and other incidents are heightening market participants' and third parties' focus on tightening cyber security in the context of the industrial IoT

OT industrial environments are no longer unattractive targets for cyber criminals.

Attacks on, for example, **Solarwinds**, Florida's water treatment facility, have put cyber security squarely on the map and attracted the attention of the media as well as the impacted companies and reinforced the interest of governments around the world in industrial cyber security as an emerging issue of national and international importance.

This report examines the evolving threat landscape that stems from the connected IIoT and industry's emerging response to best safeguard the "security of things"

Source: Frost & Sullivan

INDUSTRIAL
CYBER SECURITY

PRINCIPAL ABBREVIATIONS

AI	*Artificial Intelligence*
APAC	*Asia Pacific*
API	*Application Programme Interface*
B	*Billion*
CAGR	*Compound Annual Growth Rate*
CAN	*Control Area Network*
DDoS	*Distributed Denial of Service*
E2E	*End to End*
ECU	*Electronic Control Unit*
EV	*Electric Vehicle*
F&B	*Food and Beverage*
GDP	*Growth Domestic Product*
HIT	*Healthcare IT*
HVAC	*Heating, Ventilation and Air Conditioning*
IaaS	*Infrastructure as a Service*
ICU	*Intensive Care Unit*
IIoT	*Industrial Internet of Things*
IoMT	*Internet of Medical Things*
IoT	*Internet of Things*
ISC	*Industrial Control System*
ISOS	*Integrated Security Operating System*
IT	*Information Technology*
IVI	*In-vehicle Infotainment*
KPI	*Key Performance Indicator*
M	*Million*
M&A	*Mergers and Acquisitions*
M2M	*Machine to Machine*
ML	*Machine Learning*
MSSP	*Managed Security Service Provider*
MTTR	*Mean Time to Recovery*

Source: Frost & Sullivan

O&G	*Oil and Gas*
OBD	*On-board Diagnostic*
OEM	*Original Equipment Manufacturer*
OS	*Operating System*
OT	*Operational Technology*
OTA	*Over The Air*
PaaS	*Platform as a Service*
POS	*Point of Sale*
RoT	*Root of Trust*
SaaS	*Software as a Service*
SCADA	*Supervisory Control and Data Acquisition*
SOAR	*Security, Orchestration, Automation and Response*
SOC	*Security Operation Center*
SSL	*Secure Socket Layer*
TA	*Trusted Application*
TCU	*Telematics Control Unit*
TEE	*Trusted Execution Environment*
TLS	*Transport Layer Security*
TPM	*Tire Pressure Monitoring*
UEM	*Unified Endpoint Security Management*
US	*United States*
V2I	*Vehicle to Infrastructure*
V2V	*Vehicle to Vehicle*
V2X	*Vehicle to Everything*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*

Source: Frost & Sullivan

ABOUT INTESA SANPAOLO INNOVATION CENTER:

Intesa Sanpaolo Innovation Center is the company of Intesa Sanpaolo Group dedicated to innovation: it explores and learns new business and research models and acts as a stimulus and engine for the new economy in Italy. The company invests in applied research projects and high potential start-ups, to foster the competitiveness of the Group and its customers and accelerate the development of the circular economy in Italy.

Based in the Turin skyscraper designed by Renzo Piano, with its national and international network of hubs and laboratories, the Innovation Center is an enabler of relations with other stakeholders of the innovation ecosystem - such as tech companies, start-ups, incubators, research centres and universities - and a promoter of new forms of entrepreneurship in accessing venture capital. Intesa Sanpaolo Innovation Center focuses mainly on circular economy, development of the most promising start-ups, venture capital investments of the management company Neva SGR and applied research

For further detail on Intesa Sanpaolo Innovation Center products and services, please contact

businessdevelopment@intesasanpaoloinnovationcenter.com

ABOUT FROST & SULLIVAN:

For over five decades, Frost & Sullivan has become world-renowned for its role in helping investors, corporate leaders and governments navigate economic changes and identify disruptive technologies, Mega Trends, new business models and companies to action, resulting in a continuous flow of growth opportunities to drive future success.

For further details on Frost & Sullivan's coverage and services, please contact

LIVIO VANINETTI

Director of Frost & Sullivan's Italian operations

livio.vaninetti@frost.com

Published: February 2024