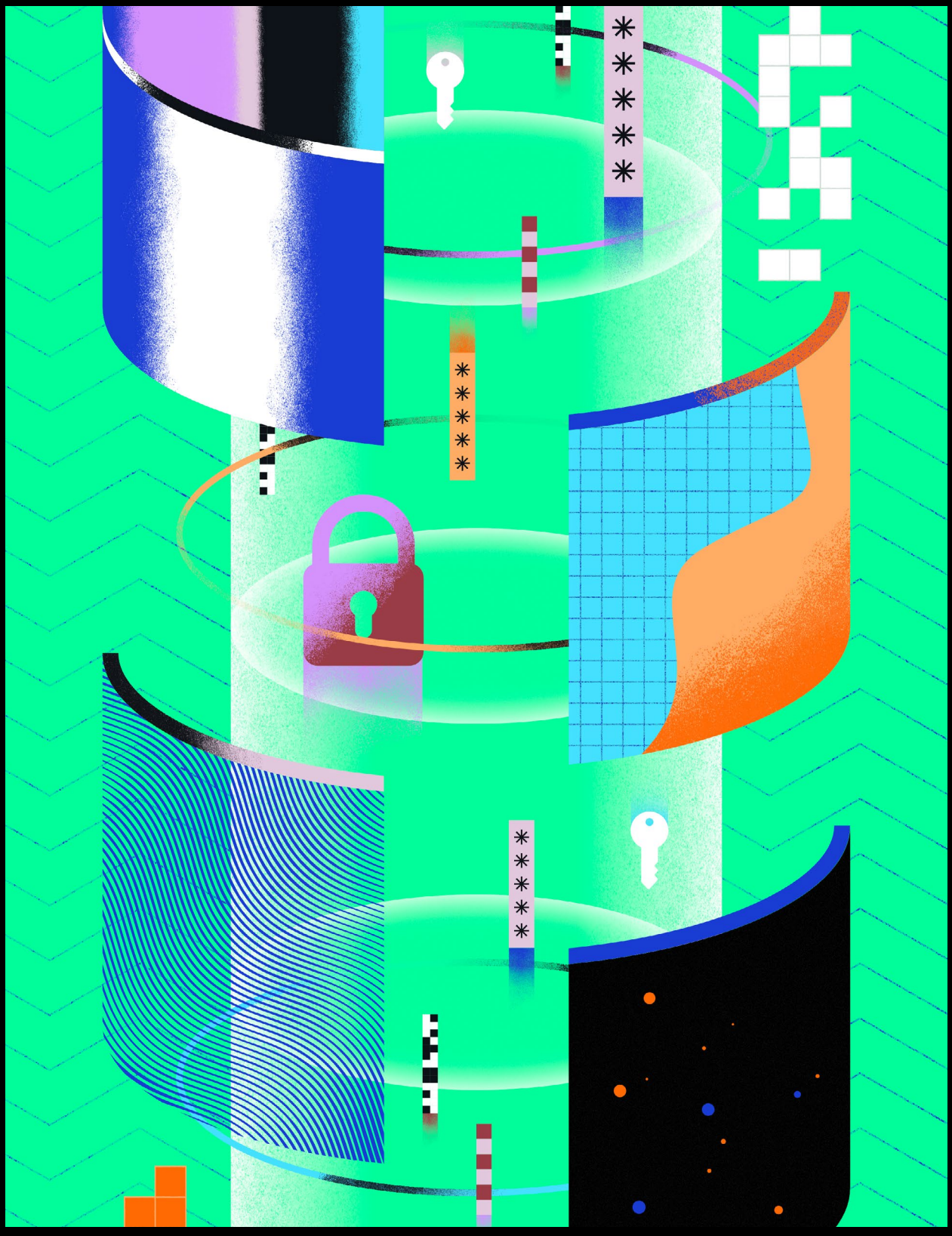
CYBERSECURITY AUTOMATION



APRIL 2022

REPLY

INDEX

EXECUTIVE SUMMARY

The increasing urgency of cybersecurity

While the technological developments in recent years have been remarkable, they have also revealed the lack of prioritization for a very important sector: cybersecurity. For years, it was regarded as an afterthought; first, we implement the new technology, then later we can figure out how to protect it.

However, cyber attackers have access to the same innovative technologies as the companies they target, meaning they can use them to circumvent security protections. As artificial intelligence (AI) technologies grow more powerful and versatile, organizations can expect that their future cybersecurity efforts will increasingly pit AI against attackers' AI. Ignoring these threats is impossible; in a world increasingly built on technology, it is no longer sufficient to act reactively rather than proactively.

Indeed, cybersecurity plays a crucial role in our personal and professional lives: the Internet of Things (IoT), for example, is as applicable for consumers with Smart Homes and Connected Cars as for professionals who employ Industrial IoT or building automation systems. Data protection is another issue growing in the public eye since breaches affect both employee and customer privacy in addition to enterprise data.

The operational downtime to websites and services caused by cyberattacks is undeniably disappointing for customers as well as the businesses who deal with subsequent profit losses. Cyberterrorism attacks are another growing threat that can not only allow attackers access to classified information but also concede control of vital services like water, power, banking, or healthcare.

The pandemic brought cybersecurity threats deeper into the home. Remote workers felt more secure in one sense, operating from the safety of their living rooms; but in another, many companies partially lost governance over their workers, who were often operating outside of company networks and combining work devices with personal devices. The awareness of the need to protect remote and hybrid work will likely have long-term impacts.

Businesses that lack proper security teams may underestimate the urgency with which cybersecurity threats must be addressed, and managers who are unsure how to proceed or what kind of equipment and software is necessary can often miscalculate the vulnerability of their organizations. Seeing as there is no one-size-fits-all solution for cybersecurity, Reply is equipped to help security teams face pressing decisions, such as determining the precise amount of technology, automation, upgrading, and manpower it will take to adequately protect their businesses.

The growing role of automation and AI

Reply used the Reply Sonar platform to identify relevant trends in cybersecurity automation and worked with PAC (Teknowlogy Group) to analyze the possible market evolution in two different geographic sectors, referred to as the Europe-5 (Germany, Italy, France, Belgium, and the Netherlands) and the Big-5, (USA, China, India, Brazil, and the UK).

Trends show that more and more businesses are turning to automation and AI to accelerate their response to emerging security issues, frequently delegating repetitive, monotonous jobs to robots who can handle them more efficiently. Companies are also aiming to mitigate the effects of a rampant skills shortage in the cybersecurity field.

As development teams were more frequently expected to integrate security efforts into their process, basic security by design principles proved to be largely insufficient against the growing amount of security threats; therefore, the field of DevOps expanded to include security and became DevSecOps. Now it involves conducting both automated and manual testing processes throughout the entirety of the application development lifecycle.

Penetration testing, vulnerability prioritization, and dynamic application security testing are emerging as opportune areas for automation or AI integration in the application development lifecycle. In fact, investments in application security automation are expected to grow substantially, reaching €669 million in the Europe-5 market and €881 million in the Big-5 market by 2026.

Investment in endpoint protection is also expected to grow. By 2026, investments in Endpoint Detection and Response (EDR) and Extended Detection and Response (XDR) solutions are expected to reach a total of €757 million in the Europe-5 market and €3.65 billion in the Big-5. These solutions automate much of the detection and information aggregation steps of endpoint detection as well as parts of the response.

Managers and/or security teams investing in these solutions, however, need to sort through all of the various options for protecting their endpoints (e.g., EDR and XDR, but also other tools and systems), or else they risk leaving their networks insufficiently protected. XDR can use AI and machine learning (ML) during the threat detection process to aggregate and analyze data and recognize attack patterns.

With the ever-growing complexity of networks, the additions of cloud and IoT technologies, and remote working complications, companies are frequently left unsecured. In particular, companies struggle to choose an optimal solution once faced with the realities of their current security capabilities. A renewed focus on asset management and upgrading security systems is imperative to protecting the network from all sources of entry.

The growing risk of the Internet of Things is worrying for many companies as well. Despite a predicted 80 billion networked devices on earth by 2026 with an impressive range of abilities, many organizations are still fearful of adopting the technology due to concerns about its security. While IoT automation can and should include endpoint protections like EDR and XDR, additional measures need to be explored for protecting smaller IoT devices that cannot support such heavy tools.

Proper data discovery, classification, encryption, and identity and access management have become essential areas of investment for protecting sensitive data from exfiltration and misuse. These sectors will more than triple their market share between 2021 and 2026 in both the Europe-5 and Big-5 clusters, going from €251 million to €915 million and €1.2 billion to €4.4 billion, respectively.

Following the automation of data discovery and classification, AI-based tools like User and Entity Behavior Analytics (UEBA) can be employed to further prevent unauthorized access to sensitive data.

Inattention to installing adequate data protection measures can result in data breaches with staggering consequences: failure to adhere to data protection laws can result in fines, failure to protect sensitive customer data can result in a tarnished brand reputation, and failure to protect enterprise data can result in loss of competitive advantages; as a whole, failure to protect a company's data can result in hours of lost labor and incur huge costs from mitigating and remediating the aftermath of these breaches. AI-based solutions are shown to lower the overall cost of a data breach.

Looking to the future of cybersecurity really means addressing the issues currently right in front of our faces. Cybersecurity cannot be overlooked; particularly when other technological developments only serve to make it even more crucial. Furthermore, automation and AI need to be considered the future of cybersecurity thanks to their capacity to go beyond human capabilities, increase efficiency in testing and remediation, and reduce the skills shortage.

INTRODUCTION

Cybersecurity automation is becoming crucial for both our private and professional lives

As the world is moving at an accelerating pace towards a digital-first and connected reality, cyberattacks such as hacking, phishing, ransomware and malware have become more widespread and sophisticated, amounting to trillions of euros in global damages for organizations. Since hardware, network and software security are turning into major and pervasive challenges to deal with in both our personal and professional lives, we estimate that the global cybersecurity market size will grow to €300 billion in the next five years.

Because of trends toward the Internet of Things (IoT), multiple cloud infrastructures and distributed workforces, we are seeing an increasing complexity of networks and the overall threat surface, meanwhile the persistent skills shortage in cybersecurity

in public and private organizations has been intensifying. In 2021, there were 4.1 million cybersecurity professionals globally [ISC^2, 2021], and another reported 3.5 million unfilled cybersecurity jobs [Morgan, 2021].

Cybersecurity automation became the solution for many security fields in the last decade; now, the convergence of global efforts on cybersecurity and the adoption of “hyperautomation” techniques make artificial intelligence and machine learning improve the potential of cybersecurity automation, with a broad range of uses at every stage of software, infrastructure, device, and hardware security.

The purpose of this study is to explore the emerging threat landscape in cybersecurity. For organizations to navigate it, they must shift toward an intelligent security automation approach and bring the issue of IT security to the direct attention of C-level management. To gain a better understanding of current cybersecurity-related trends, we used Reply Sonar, an AI-based tool that was developed together with the German Research Center for Artificial Intelligence, DFKI. The tool analyzes more than 50 million articles taken from relevant expert media, such as scientific journals, patents, papers, and B2B content platforms.

Read more about Reply Sonar

Thanks to Reply Group companies from various industries and countries that shared their cybersecurity expertise and their experiences with customers, we were able to integrate an overview of global trends with a focus on lessons learned and best practices. This research paper will focus on the main Reply markets, so data will be presented in two clusters:

- Europe-5, which includes Germany, Italy, France, Belgium and the Netherlands
- Big-5, including the USA, China, India, Brazil and the United Kingdom.

A collaboration with Pierre Audoin Consultants (PAC, Teknowlogy Group) allowed us to compare the “software” and “services” segments in four main cybersecurity automation domains: application security, endpoint detection & response (EDR) and extended detection & response (XDR), Internet of Things security, and data security. The data uses 2021 as a baseline and forecasts investments up to 2026.

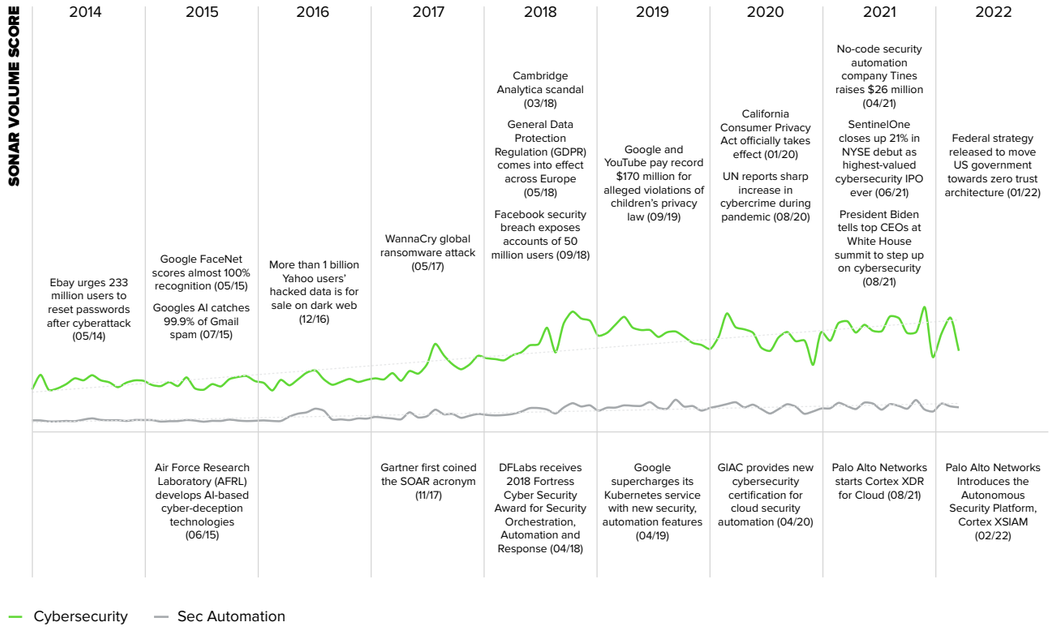
CYBERSECURITY AND AUTOMATION TRENDS

> **AI-driven security automation is the next big thing in cybersecurity. Even though the current offerings are not perfect, they pave the way to more automation and allow human security analysts to focus more on complex issues. Fully automated cybersecurity will not be viable in the foreseeable future, but monitoring, detection, and parts of response actions can and will be automated in the interest of talent availability.**

Wolfgang Schwab, Head of Cybersecurity at PAC (Teknowlogy Group)

The top topics in the global debate about cybersecurity

Reply Sonar – Cybersecurity and Cybersecurity Automation: timeline analysis



The increasing importance of cybersecurity is well reflected in the development of expert media sources over the last few years. The cybersecurity narrative has been defined by major cyberattacks, data breaches, and their financial consequences, as well as legislative attempts to regulate the field. The whole discussion is increasingly infused by the topic of intelligent cybersecurity automation, corresponding solutions and their relevance in fighting persistent cyber threats.

By using our Sonar platform, we created an overview of relevant trends related to cybersecurity based on their occurrence within expert media articles, mass media, patents, and scientific publications. We scouted and clustered the most debated topics from different fields: from the guideline/governance area to operational security activities, to data- and privacy-related hot topics.

SECURITY ARCHITECTURE & ENGINEERING

- Cybersecurity Automation
- Security by design
- Decentralized Security
- Software-defined Security
- Cybersecurity Mesh
- Zero Trust Security
- Real-Time Security Visibility
- Security as a Service

IDENTITY & ACCESS MANAGEMENT

- Bring Your Own Identity
- Identity & Fraud Analytics
- Federated Identity
- Behavioral Monitoring
- Identity & Access Management
- Multifactor Authentication
- Biometric Authentication
- Machine Identity Management
- Decentralized Identity
- Passwordless Verification

RISK ASSESSMENT & MANAGEMENT

- Vulnerability Management
- Third-Party Risk Management
- Penetration Testing
- Ethical Hacking
- Breach & Attack Simulation (BAS)
- Security Analytics & Intelligence
- Cyber Resilience Testing

THREAT INTELLIGENCE

- Threat & Zero Day Hunting
- Threat Remediation
- Intrusion Detection
- Malware/Virus Detection & Analysis
- Detection as Code
- Incident Response
- Threat Intelligence
- Extended Detection and Response (XDR)
- Security Information & Event Management (SIEM)
- Security Orchestration, Automation & Response (SOAR)

DIGITAL & FRAUD DECEPTION

- Disinformation Detection
- Deepfake Detection
- Bot Detection
- Social Engineering Defense

DATA SECURITY & COMPLIANCE

- Data Protection & Compliance
- Digital Forensics
- Data Discovery & Classification
- Data Defense & Loss Prevention
- Cryptography & Data Encryption
- Privacy by Design
- Confidential Computing
- Real Time Data Visibility

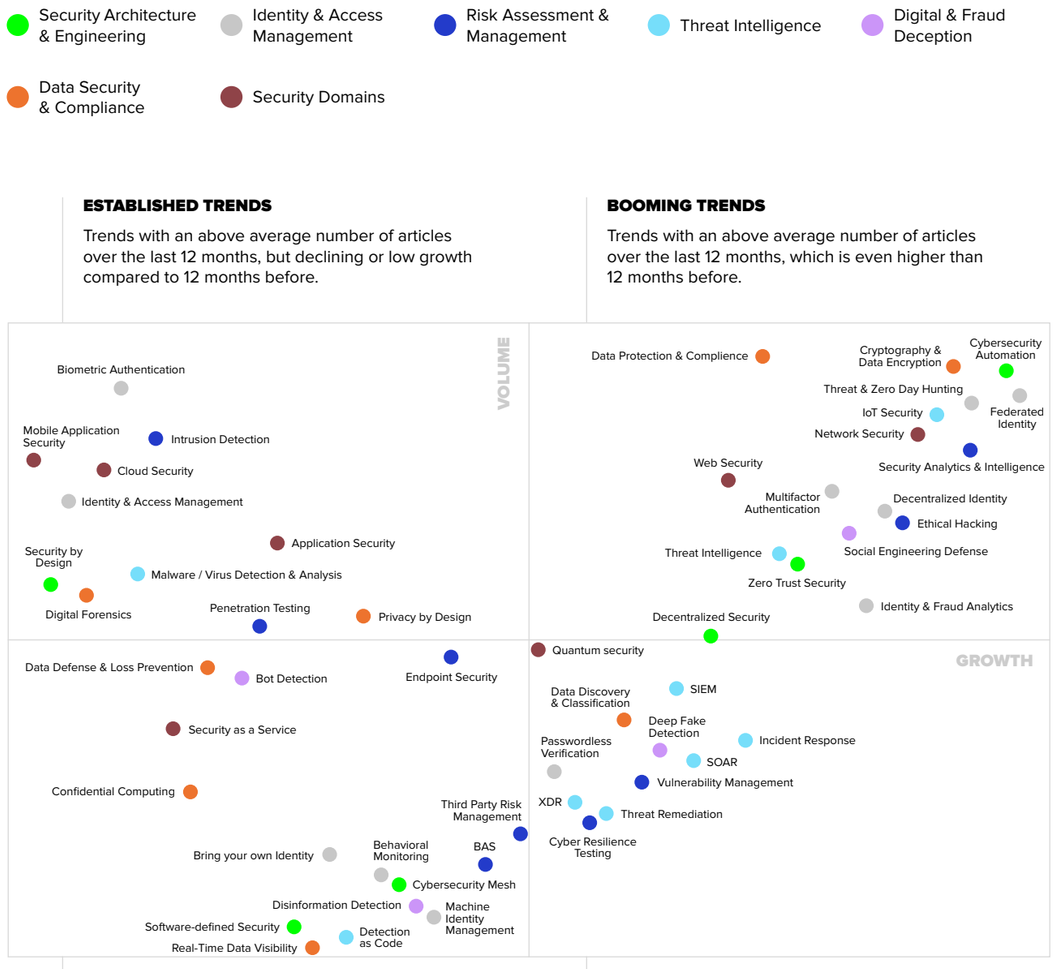
SECURITY DOMAINS

- Cloud Security
- IoT Security
- Web Security
- Mobile Application Security
- Endpoint Security
- Network Security
- Application Security
- Quantum Security

According to our analysis of expert media sources, high volume discussions center on data protection, cybersecurity automation, cryptography, and biometrics. Top growing trends comprise federated identity, cybersecurity automation, threat & zero-day hunting, AI-based security, as well as cryptography & data encryption. We mapped each mentioned topic on a matrix where its volume of mentions and its annual growth are the main axes.

Reply Sonar – Main trends in Cybersecurity

Timeframe: February 2021 - January 2022



ESTABLISHED TRENDS

Trends with an above average number of articles over the last 12 months, but declining or low growth compared to 12 months before.

BOOMING TRENDS

Trends with an above average number of articles over the last 12 months, which is even higher than 12 months before.

EARLY TRENDS

Trends with a low number of articles over the last 12 months, and declining or low growth compared to 12 months before.

UPCOMING TRENDS

Trends with a low number of articles over the last 12 months, but with a higher growth compared to 12 months before.

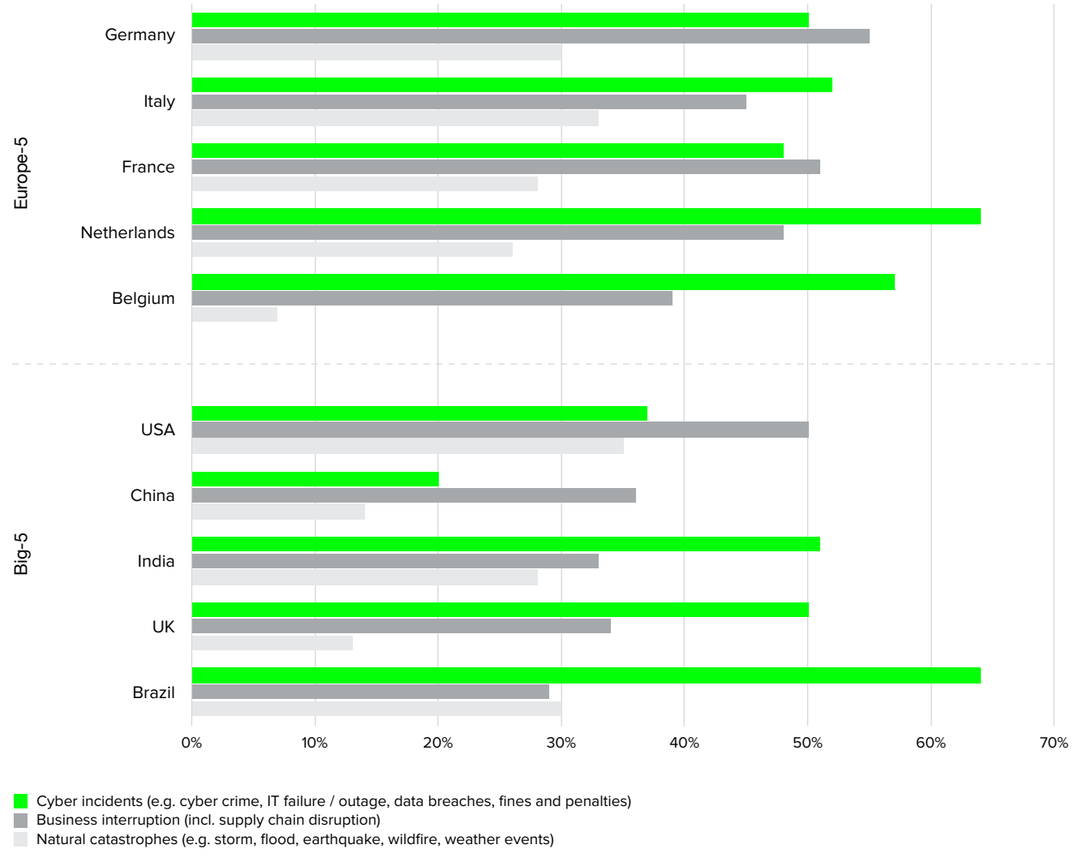
The upper part of the matrix shows how the fight against rising cybercrime is putting cybersecurity automation top of mind, reducing the need for human intervention, accelerating response times and resulting in timely identification of security issues. Moreover, growing attention is dedicated to the topic of protecting data from unauthorized access and corruption. The push towards a remote workforce has renewed the attention on identity and access management, for business continuity and employee and data protection. It also plays a vital role within the trend toward zero trust security frameworks.

As cyberattacks grow in frequency and sophistication, passing from “classic” automation to AI-based cybersecurity can integrate real-time threat intelligence into agile security. Within threat intelligence, special attention is dedicated to the topics of threat & zero-day hunting, proactively and systematically identifying malicious activities, as well as handling threats by social engineering.

The lower part of the matrix is useful for looking forward. Threat & deception intelligence and increasingly risk intelligence, continuously enhanced through technologies like AI and automation, are moving organizations’ security strategies from protection to prevention. Thereby, an overwhelming tech stack of cybersecurity solutions, tools and applications has been emerging, focusing on continuous and automated anomaly detection or vulnerability screenings, proactive decision-making and response support, and disaster recovery. Moreover, deepfake and disinformation detection technology will be turning into a topic of future concern, as we see a surge in the use of these methods by cybercriminals and within the cybercrime-as-a-service field.

Executives are facing the harsh reality of cybersecurity threats

Interviewed managers mentioning cyber incidents, business interruption and natural catastrophes in the top 3 risks (%) Source: [Allianz, 2022]

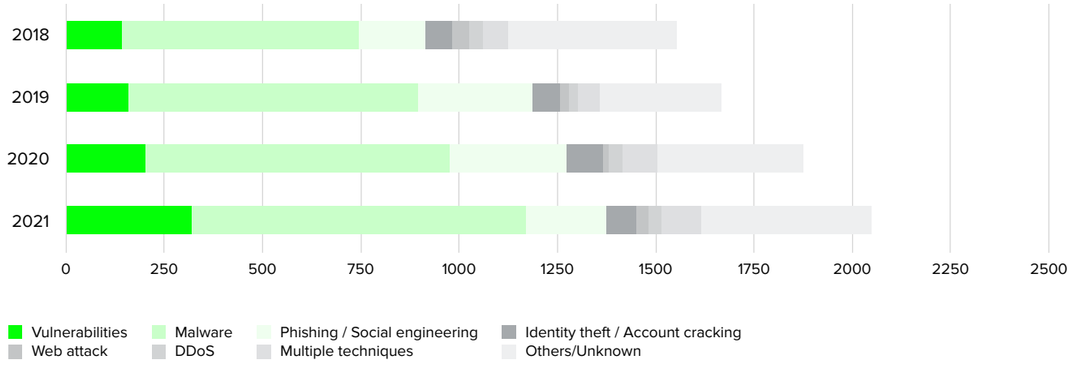


According to Allianz Global Corporate & Specialty, cyber incidents are perceived as the most important business risk in 2022: up to 44% of managers mentioned it as the number one threat, regaining its spot after a brief dip in the rankings due to Covid-19. In 2022, cyber incidents ranked first or second (usually alternating with business interruption) in every country we monitor, with the exception of China where they came in fourth. Globally, they are top of mind for large-size companies (50%), mid-size (36%), and small ones (39%) [Allianz, 2022].

Ransomware attacks and data breaches are the main concerns, both mentioned by 57% of interviewed managers. Direct experiences along with increasing media attention are augmenting the awareness towards cybersecurity. An example that made global news in 2021 was the exploitation of the Log4j vulnerability.

Because its primary function of logging is fundamental to most software, the impact of such a vulnerability is felt across the software ecosystem: it is used in cloud services as well as software development and security tools, meaning that everything from e-commerce sites to water utility systems could be attacked. Hackers in this case attempted to abuse the vulnerability to mine cryptocurrencies, gain access to sensitive political information, and more.

Source: [Clusit, 2022] **Evolution of attack techniques (cases on Clusit dataset)**



A global study from Clusit [Clusit, 2022] monitoring the evolution of different attack techniques in the last four years shows a constant increase of threats along with a steady growth of vulnerabilities. The global pandemic saw an explosive growth in cyber incidents: up to 40% of desktop PCs appeared unsecured while remote working was rapidly increasing; a peak of +400% brute-force attacks was reached during the global lockdown months in early 2020 [Statista, 2022]. As we mentioned in our "Hybrid Work" Research, companies are replying with a relevant upswing in investments in the end-user device security market, resulting in an expected growth of 34% in the Europe-5 cluster and 45% in Big-5 countries (2025 vs. 2020).

Download Reply Research "Hybrid Work"

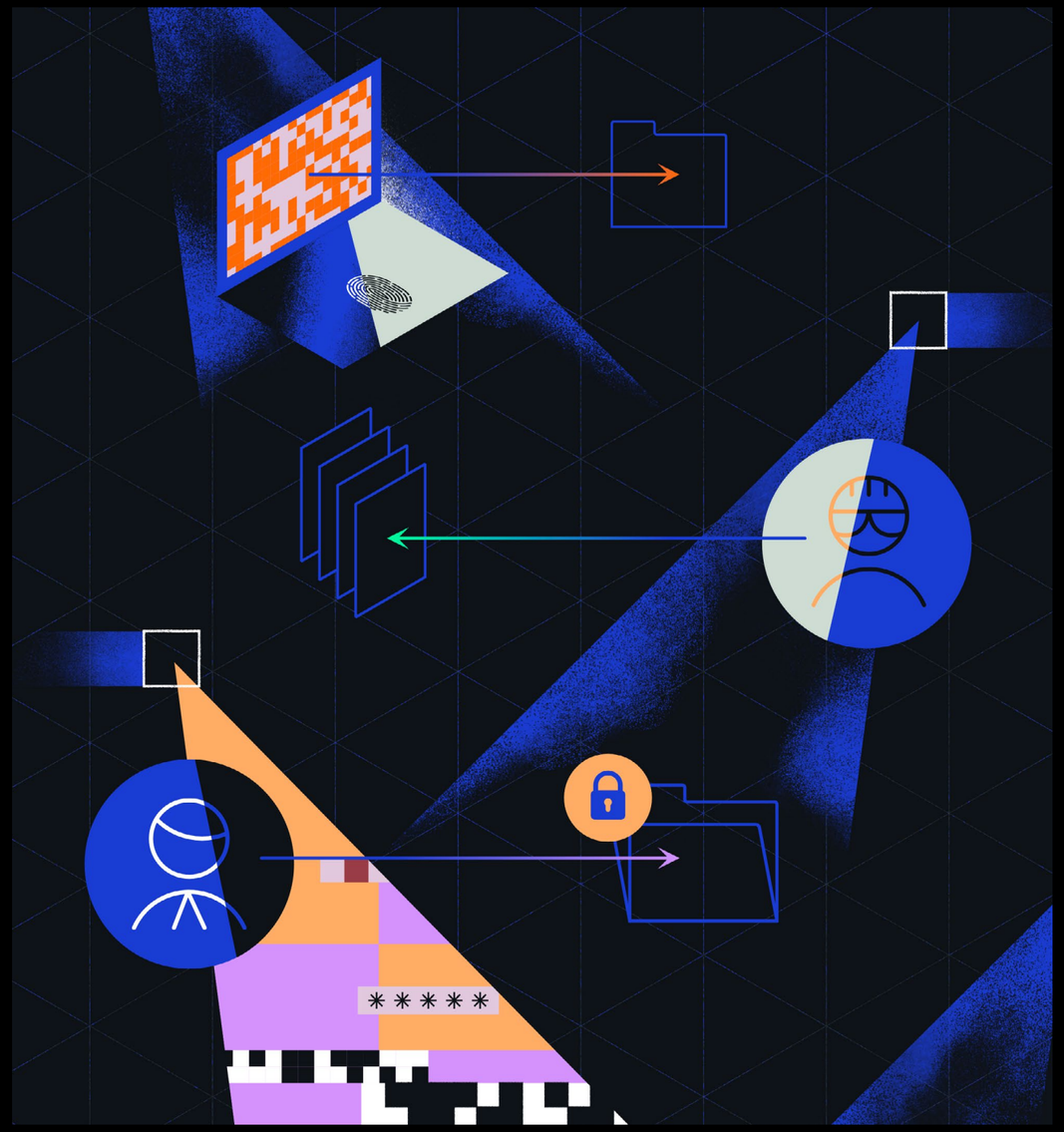
During the pandemic, cloud computing confirmed its role as new-standard architecture and enabler for flexible solutions. After years of looking at cloud platforms as black boxes and underestimating the need for cybersecurity, organizations are finally concerned about cloud security; more than one out of four experienced a cloud-related security incident in the last year. Among those, 23% suffered from wrongly configured resources or accounts: now 20% of ICT managers are mentioning preventing cloud misconfigurations and 16% are listing securing major cloud apps as top priorities for 2022 [CheckPoint, 2022].

As for data breaches, their average cost is estimated at $4.24 million (USD), peaking at $9.23 million (USD) for healthcare players. The cost includes both lost business and the operation costs of detection, escalation and post-breach response. Customers' personally identifiable information is the most common type of record lost or stolen and is affected in up to 44% of cases. Compromised business credentials account for 20% of breaches, with an average cost of $4.37 million (USD) [IBM, 2021].

Building an increased understanding of cybersecurity across organizations should lead to further automation of risk mitigation, prevention and defense; human agents in these arenas are at

a disadvantage to machines in speed, force and compliance. Leveraging the power of machine automation to mitigate security risks, detect and evaluate cyberattacks, and defend vulnerabilities will make or break business operations in any digitalized industry, and implementing artificial intelligence will only further optimize these processes. For this reason, a quarter of cybersecurity professionals are now pursuing professional development in AI/ML [ISC^2, 2021]. Though automation has been in play for many years, AI and ML are clearly beginning to play a more vital role in cybersecurity.

Index



Humans, automation, and AI

> AI will potentially impact our digital and Internet lives in the future, as the major trend is the emergence of increasingly new malicious threats from the Internet environment; likewise, greater attention should be paid to cybersecurity. Accordingly, the progressively more complexity of business environment will demand, as well, more and more AI-based support systems to decision making that enables management to adapt in a faster and accurate way while requiring unique digital e-manpower.

Ricardo Raimundo (ISEC) and Albérico Rosário (GOVCOPP) [Sensors, 2021]

The cybersecurity automation market is evolving at different speeds

Based on interviews with Reply customers and Reply specialists, we built a conceptual diagram of different approaches to cybersecurity actually found on the market. It does not pretend to be exhaustive, and it is important to note that when it comes to addressing investments and architectural choices: there is not a one-size-fits-all solution. The complexity comes from a variety of factors, from the layers of necessary protection (e.g., software, hardware, network, data), to the organization's business specialization, size, or geographical coverage.

	TRADITIONAL APPROACH TO CYBERSECURITY	"CLASSIC" CYBERSECURITY AUTOMATION	AI-POWERED CYBERSECURITY AUTOMATION	AI VS. AI
FOCUS	▸ Finding vulnerabilities in code ▸ Reaction to breaches ▸ Manual penetration tests	▸ Code control routinized/ triggered ▸ Endpoint monitoring and automatic alerts for security analysts ▸ Automated application security tests ▸ Adoption of "off-the-shelf" solutions	▸ Real-time monitoring of code by bots ▸ Automatic Detection and Response ▸ Alert prioritization and eventual response based on history and patterns recognition	▸ Monitoring of AI-driven attacks ▸ Real-time response based on machine learning algorithms
STATE OF THE ART	▸ Widely adopted, especially in organizations adopting waterfall development methodology	▸ Standard in medium/ big companies, often following the adoption of DevOps and Agile methodologies	▸ Increasingly proposed by cybersecurity product vendors ▸ Adopted from medium/ large companies as a part of the adoption of DevSecOps methodology	▸ Rapid increase of AI-based solutions adoption, particularly by financial institutions, due to steady increase of AI-based attacks
STARTUP INVESTMENTS	▸ Low	▸ Medium, thanks to a wide range of "off-the-shelf" solutions	▸ Medium-high, due to the need to integrate different sources and systems	▸ High, due to the need to adopt a big data platform and design effective algorithms
RUNNING COSTS	▸ Medium-high, due to high human involvement	▸ Low-medium, thanks to a lower amount of human involvement	▸ Medium, mainly due to the need to keep updated data and algorithms	▸ High, mainly due to the need for real-time collection of data and algorithm training & adaptation to new threats ▸ Continuing costs due to constantly developing threats
STRENGTHS	▸ Implementation time ▸ Independence from vendors	▸ Effective coverage for SME ▸ Reduced need for human intervention	▸ High coverage of threats and vulnerability, virtually growing in the long term ▸ Unique control dashboard for all security platforms	▸ Fast response to AI-driven attacks ▸ Coverage virtually increases with the training of algorithms and the growth of databases
WEAKNESSES	▸ Low coverage of threats ▸ High risk of missing vulnerabilities ▸ Long reaction time to threats	▸ Possible lock-in from software vendors ▸ Medium coverage of threats ▸ Medium risk of missing vulnerabilities ▸ Potentially high number of alerts and/or false positives	▸ Possible long time from inception to high coverage of threats ▸ Constant need for machine learning and artificial intelligence experts to fine-tune the system	▸ Need to set up and maintain a big data platform ▸ Data privacy issues to be evaluated to guarantee wider/ deeper input data sets

Each scenario in the chart is not necessarily the evolution of the one to its left. The adoption of powerful cybersecurity tools requires a different mix of skills from human specialists, not to get rid of them. The setup of complex AI-based systems often relies on existing data coming from specialized tools and requires heavy intervention by security analysts and AI experts to improve the effectiveness of solutions. Even for smaller companies that require comparatively simpler solutions, the stakes are high enough that they should not rely on “do-it-yourself” techniques.

Bigger organizations use a common model for Security Operations teams, in which the three tiers of activities handled by security experts are triage, investigation and threat hunting. The first tier, triage, is where the majority of analysts reside and spend long hours poring over logs and searching for suspicious activity. This model is not ideal because alert fatigue may lead to errors. Moreover, many analysts would prefer to advance their skills and work on more meaningful projects in the investigation or threat hunting tiers.

Security Operations Centers (SOC) are pushing to at minimum intelligently automate their detection and response procedures, a move that can reduce remediation times by hours. While this is expected to perhaps change the role of security analysts and ease their workload, experts do not anticipate a massive reduction in the SOC workforce. Threat hunters will still be needed to defend against a growing number of attack strategies.

Business E-mail Compromise Incidents in 2021 (%, multiple choices)

Source: [SonicWall, 2022]

Humans, however, can be the weakest link in the cybersecurity wars. An example comes from e-mail phishing campaigns and business e-mail compromises (BEC), among the main channels for spreading malware and ransomware. Business users are prone to opening e-mails from “known” identities, which can be easily spoofed. Automated filtering of incoming e-mails is a solid practice run by most relevant vendors and is usually successful at filtering out the vast majority of spam and compromising e-mails. Interviews reveal that business users feel protected; however, this false sense of security can lead them to opening any remaining messages, assuming that they are safe to open if not caught by the software.

Automation and AI are an opportunity for cybersecurity

One of the main reasons for the growing attention to the use of automation and AI for cybersecurity comes from the increasing “attack surface” in both enterprise and consumer contexts. The wide availability of devices for personal, business, and industrial uses on one side creates the grounds for increasingly

sophisticated algorithms; on the other side, it requires the ability to process massive volumes of data not just for business goals, but also to identify latent or explicit threats.

As long as there is enough computing power and they are opportunely configured in terms of privacy and compliance, automated systems infused with artificial intelligence systems can monitor 100% of network traffic, user behavior, and attack events, analyzing all the details: nothing similar could be done by human beings. Moreover, humans tend to show increasing error rates for tedious and repetitive tasks; well-trained artificial intelligence systems do not, resulting in incredibly low error rates even for monotonous tasks.

Overall, organizations wishing to develop their cybersecurity strategy should seek tools that automate repetitive tasks and simplify the investigation process, thereby helping less experienced security analysts to be more effective and efficient in their own roles. For now, human intervention is still vital in many cybersecurity tasks, but automation and AI offer a helping hand to accelerate various monitoring and analytical processes along the way.

Well-known for its business value, Robotic process automation (RPA) is showing its potential in the cybersecurity field, too. It uses basic automation capabilities to conduct cybersecurity activities like data capturing, reporting, log management and data migration. Intelligent process automation (IPA) powers RPAs with “smart technologies” so that they can view data in a company’s specific context and make more complex decisions.

Some ML-enabled RPA bots can be equipped to scan logs to track potential security breaches, recognize patterns, and identify abnormal activities; while this can reduce remediation times, their limitations still necessitate human management of threat hunting and remediation responses. Regardless, RPA and other cybersecurity automation technologies can now deal with monotonous tier-1 tasks, thus providing support to cyber security specialists to focus on more complex issues and ultimately mitigating the skills shortage in a field where experts are scarce.

The next logical step for artificial intelligence systems will be to take action after recognizing a threat. This will reduce response times as well as mitigation times and limit potential damage. Currently, most organizations do not employ these systems after identifying threats or unusual behavior but rather pass on the information to a human security analyst; they decide if the threat is real or if the behavior requires further investigation and any decisions are followed by manually triggering appropriate actions.

AI can improve over time with continuous use to recognize even the smallest risk indicators. Hackers, and especially the so-called advanced persistent threat (APT) attackers, have learned to move very carefully so as not to attract any attention. Up against a human-controlled environment, these attackers are frequently successful and APTs are discovered very late. Artificial intelligence systems can be much more sensitive even with small data packages.

New technology breeds new security threats

As AI and automation revolutionize cybersecurity solutions, the ultimate goal will be to not only mitigate escalating threats but to shift the focus from detection to prediction, and thus prevention, of threats. However, developments in proactive defense and attack prevention are flanked by an arms race on the part of cybercriminals. Attackers are professionalizing their sector and leveraging the same emerging technologies for the offensive.

Consequently, the future of cybersecurity is expected to be AI versus AI. Malware is more evasive, pervasive and scalable than ever as it capitalizes on natural language processing (NLP) to evade algorithmic detection. On the other hand, AI used on the defensive side can then employ the same machine learning tools to detect automatically-generated text created by malware algorithms, and the vicious cycle begins.

Another area of concern is the immense vulnerability of AI systems which, when infiltrated, can be retrained by cyber attackers. Not only can AI be employed by cybercriminals for attacks, but it can also be exploited as a weakness when organizations fail to implement it together with strong security features. AI and ML open up fresh vulnerabilities that attackers can use to gain access to crucial systems and data.

Thus, as machine learning gains traction, companies have to keep in mind that systems implemented with ML may be vulnerable at every stage of the learning process, facing attacks against either the data set or the model itself. Implementing machine learning typically involves a five-step process: collect data, prepare data, train the model, evaluate the model, and improve.

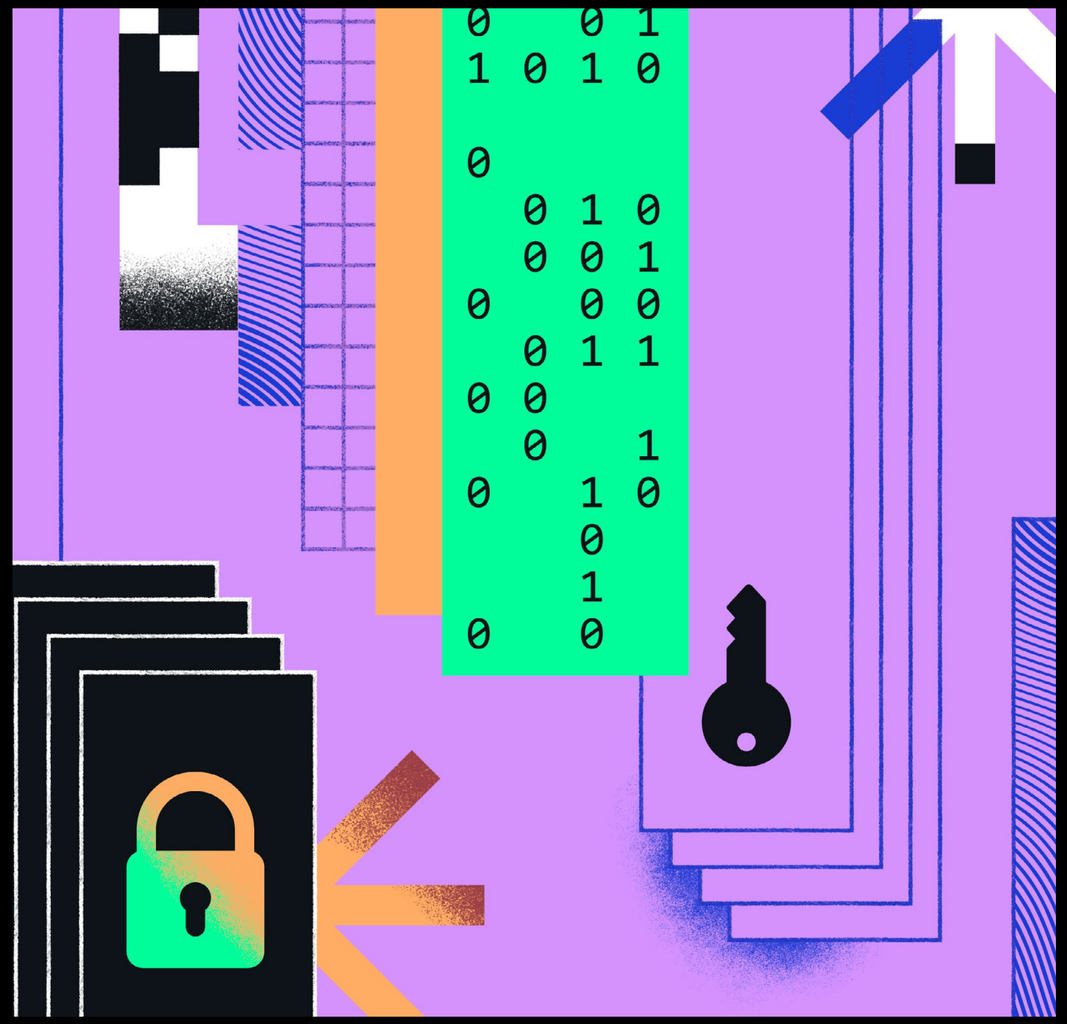
Attacks during any of these five steps can incur significant costs for a company; however, attacks during the first and third phases, in particular, can draw high costs due to remediation processes that require redesign or re-instrumentation of the ML system or even necessitate switching to an alternative model. In adversarial machine learning (AML) attacks, cybercriminals attempt to exploit or trick a machine learning tool to either force a misbehavior or seize information. These attack methods are therefore becoming an active field of research in cybersecurity.

Read more about Reply's view on Adversarial Machine Learning (AML) threats

Cyberattacks on AI systems are commonly categorized by their intended target, the techniques they use, the influence or capability of the attacker, the security violations (i.e., consequences) caused, and the specificity of their attack scope. However, all of the various attacks ultimately belong to two categories: attacks at training time and attacks at inference time. Attacks at training time can corrupt a model even before its release into production because they affect the data used to train the model; attacks at inference time afflict the model after its release.

Examples of the former include poisoning or backdoor attacks, while examples of the latter include evasion attacks, model stealing, and data extraction. Poisoning, for example, attempts to manipulate training data for the AI system early on in development. Effectively, attackers can use this as a way to construct a backdoor through which they can enter later to control the AI model. Then, an attacker may poison either the dataset, the algorithm, or the model itself.

Defense is a tricky issue to approach because there is no one-size-fits-all defense algorithm and there is no theoretical method to guarantee the defender's advantage. Even a well-defended AI model can be attacked again via counter-counter measures, hence the vicious cycle and need for a strong security by design approach throughout the AI development and operation processes. Hopefully, emerging tools will employ AI to improve defenses or even identify their own potential vulnerabilities.



Application security

> Integration of dynamic and automated security audits into agile application development which is used by developers embraces DevSecOps culture. An application is created which integrates all the security scanners in a single application to reduce manual efforts by using various scanners from a single application. Testing of vulnerabilities is done in the early stages of the pipeline i.e., after integration testing, thereby reducing the cost of further processes. Hence, CI/CD (continuous integration/continuous deployment) pipeline is converted to CI/CD/CS (continuous integration/continuous deployment/continuous security)
>
> Kriti Mittal, Maryada Sharma, Manvi Gupta and Kavita Sheoran (Maharaja Surajmal Institute of Technology) [Mittal et al., 2021]

Shifting left: from waterfall methodology to DevSecOps

In traditional development life cycles, developers created first versions of applications with limited or no oversight from security; they focused entirely on functionality. Even in the best cases, inputs from security were limited to static checklists or one-size-fits-all best practices documents. Only after operations finalized their part would security be informed of the new product and the need to fix it before its release to the market. This “waterfall” method saw the product move down a pipeline with little collaboration between units.

A first evolution took place with the introduction of basic security by design practices, in which application security starts in the initial design phase and ensures that the security of the final application is a vital part of the initial project plan. In the basic security by design approach, security for support, verification, and testing tasks is involved throughout the whole product lifecycle but still concentrated in well-defined, critical moments. Therefore, basic security-by-design practices are often insufficient for more recent, agile, DevOps-oriented paradigms.

Following the spread of agile culture across organizations, the development and operations units were pushed to collaborate more throughout the lifecycle; DevSecOps proponents advocated for that collaboration to include security as well. This newer approach aims to integrate security in an automated and continuous way that would not slow down product development.

DevSecOps environments now adopt shift-left testing as a fundamental principle for security by design. The shift-left approach pushes teams to move security even further from the right side, or end of the delivery process, to the left, or beginning. The development team is asked to actively implement security

measures during the initial building phases of a product, the goal being to find and prevent defects earlier in the software delivery process.

The “Pervasive Security” framework for DevSecOps

Based on Reply experience, we defined a framework we named Pervasive Security including procedures, tests, and checks that should be considered at every step of the development lifecycle, assuming DevSecOps as standard thanks to its growing adoption following the success of cloud architectures.

The incentive for teams to adopt a shift-left mindset is strong. Removing defects earlier in the process costs substantially less than when defects are discovered later. A defect removed only after a product has gone into production may cost up to 100 times more, depending on the complexity of the platform, costs related to the damages, and fines imposed on the company.

The benefits of the shift-left approach extend beyond cost savings, by increasing the capacity for teams to adopt automation and increase their delivery speed and overall product quality. Cybersecurity teams practicing shift-left can take full advantage of automation during the beginning stages of development, though it should also play a vital role at every stage of the lifecycle.

To ensure a proper security posture in these new contexts, the following pillars must be respected:

- Pervasive and continuous security presence within projects teams
- Threat-modeling based security requirements identification
- Security tools integration within DevOps and CI/CD toolchains
- Automation of security tasks.

The current reality of application development and subsequently security is that they rely on a software supply chain. While code may be either custom or imported, a growing number

of developers today import at least some of their code from places like open-source software or code repositories; even more, third-party software integrated into company systems could also contain insecure code. This poses a risk down the line because the supply chain of code becomes too complex for organizations to easily verify the security of every component.

Tools like software composition analysis (SCA) are a helpful solution. They automatically analyze the assorted codes for vulnerabilities; some even have the capability of offering updated codes as a solution. However, the final processes of updating or deleting code and remediating require human assistance. Before implementing SCA, organizations also need a complete asset inventory, which requires proficient asset management. It involves continuously tracking the IT assets of your organization and all their relevant potential security risks.

Unfortunately, because supply chains are often so complex, examples like the aforementioned Log4Shell vulnerability must be treated on a case-to-case basis. The remediation process depends entirely on how this kind of external software was incorporated into the system and requires the full cooperation of developers, software distributors, system operators, and even users. DevSecOps teams need comprehensive visibility across all applications, including cloud-native workloads.

DevSecOps is a standard in larger organizations in which the level of automation in continuous delivery and deployment is usually high. For automating the whole DevSecOps cycle, here are some insights coming from Reply's experiences.

- Incorporate security standards and guidelines through integrated development environments (IDE) in order to support DevSecOps automation.
- Utilize automated asset management tools to track assets and standardize the process of updating software.
- Define the code review process to make the code review more efficient and consistent, allowing developers and stakeholders to save valuable time.
- Analyze security testing as part of the move to DevSecOps automation and strive to automate some of those tests in combination with the existing functional tests as part of rolling out automated regression testing.
- Implement Kubernetes or some other container orchestration solution to apply, deploy, and manage repeatable best practices for security through container orchestration.
- Introduce software bills of material into the DevSecOps pipeline using automated scanning tools in order to provide the best possible picture of proprietary and open-source software dependencies in the software to be developed.

PAC (Teknowlogy Group)'s market forecast on application security automation

According to PAC (Teknowlogy Group), the awareness for application security is of high importance, especially for innovative new applications that drive new business models. These applications are often implemented in a DevOps model, starting from a first prototype that is improved over many iterations.

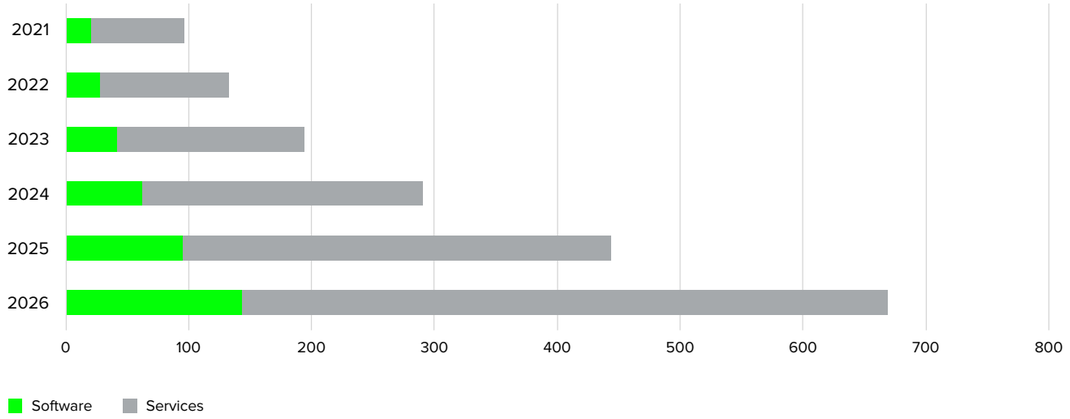
PAC often sees a rather rough start without any security constraints, which leads to semi-finished solutions that are not secure. It takes substantial time and budget to fix the security part. According to them, a better approach is to integrate security right from the

beginning, use automated testing, and integrate automation as well as breach and attack simulations and automated penetration testing into the DevSecOps lifecycle. This leads to better results and lower costs.

In collaboration with PAC, we forecast the possible evolution of the application security automation market in Europe-5 and Big-5 clusters. Estimates include automated application security program management, software composition analysis, static and dynamic application security testing, and web application firewall/runtime application self-protection, split by software and services (consulting, system integration, and managed services).

Source: Teknowlogy Group for Reply, 2022

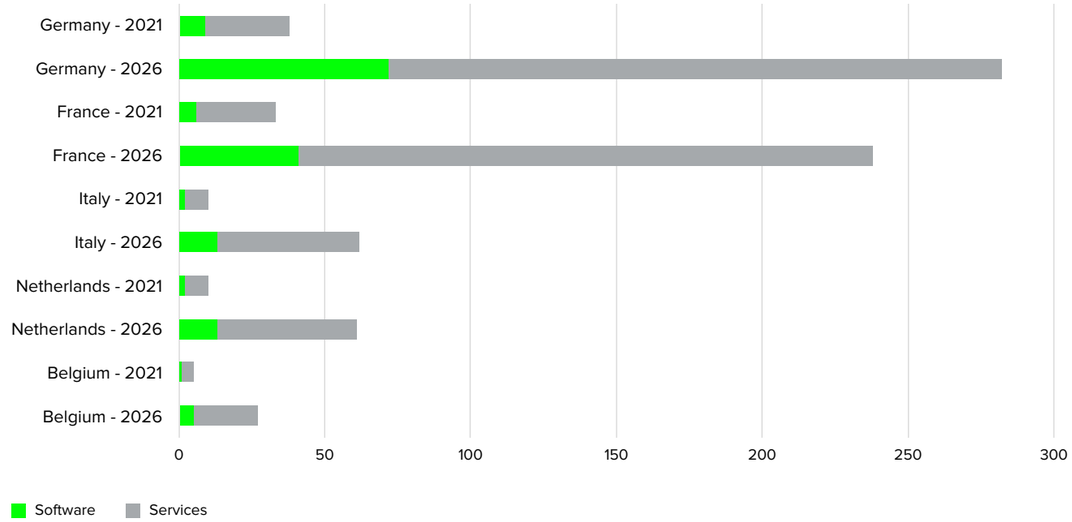
Europe-5: evolution of application security automation market (million euros)



The Europe-5 market of application security automation is forecast to grow for both the software and services segments in the next five years to a total of €669 million in 2026. The dedicated software will grow by seven times, from €20 million in 2021 to €143 million in 2026. A similar growth rate is expected for services too, forecast to increase from €76 million to €526 million.

Europe-5: comparison 2021-2026 of application security automation market, by country (million euros)

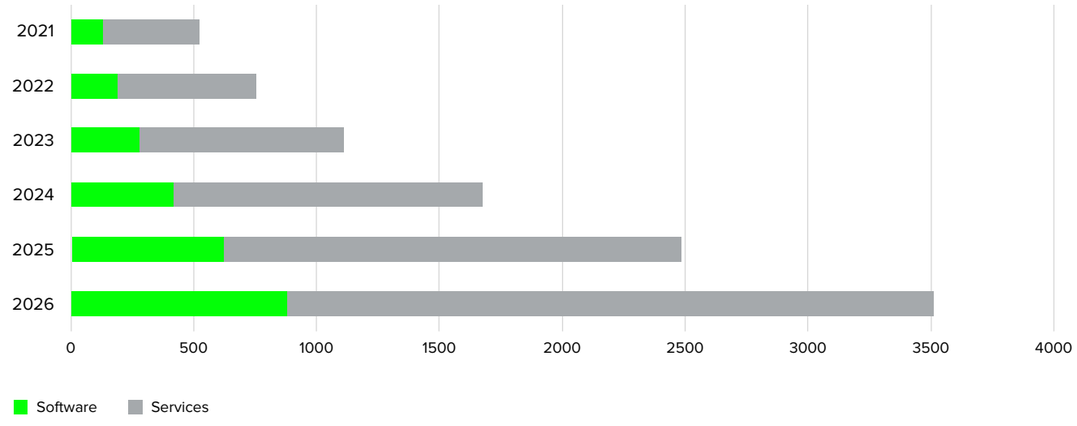
Source: Teknowlogy Group for Reply, 2022



Germany and France were the main markets in the Euro-5 cluster in 2021 and they will maintain their leadership through 2026. Their markets will grow to €282 million and €237 million, respectively. A slightly lower rate of growth is forecast for Italy, Belgium, and the Netherlands. In these countries too, however, the software segment will grow faster than the services one.

Big-5: evolution of application security automation market (million euros)

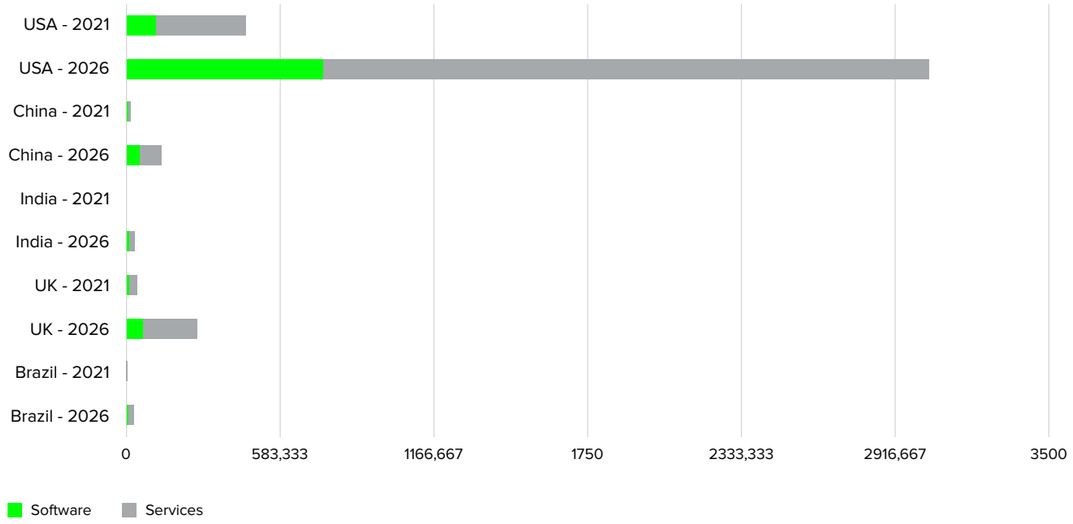
Source: Teknowlogy Group for Reply, 2022



The Big-5 cluster will also grow significantly from 2021 to 2026. The software segment is forecast from €132 million in 2021 to €881 million, while the services segment is projected from €393 million in 2021 to €2.63 billion in 2026. The size of the market is mainly attributed to the United States, which accounts for around 85% of the investments in the cluster.

Source: Teknowlogy Group for Reply, 2022

Big-5: comparison 2021-2026 of application security automation market, by country (million euros)



Both the software and services segments are forecast for growth in the USA up to 2026, respectively from €112 to €750 million and from €342 million to €2.3 billion. The UK services segment will grow to match the German market at €210 million, with a more limited software segment, forecast up to €51 million in 2026. India will register the highest rate of growth for both segments, but its market will still be pretty small in 2026, totaling only €31 million.

Automating application testing at every step

The cost of fixing vulnerabilities increases exponentially the later they are found in the development process. Manual or human talent-based application security testing expends scarce resources and can therefore only be performed for final release candidates, i.e., too late for easy and cheap fixes and practically impossible in agile environments.

The alternative is automated security testing. There are two major approaches to security test automation:

- Automation through integration – that means being able to automatically trigger security testing tasks as part of the CI/CD pipeline, preparing what is needed for their execution

- Automated tests execution – this relies on the availability of tools that, thanks to advanced capabilities (like AI), are able to autonomously execute security testing actions and, possibly, propose remediation.

Early testing typically involves scanning the code of an application for vulnerabilities, which can be done in several ways.

- Static Application Security Testing (SAST): The basic idea is that an analyzer scans the entire source code of a piece of software without executing it. The advantage of this approach is that this can be done at a very early stage, even if the entire software package is not yet executable. The extreme extension of this concept is the integration of SAST solutions with IDE tools, to provide immediate feedback to developers as soon as they code. A disadvantage is the potentially large number of false positives due to the heuristics used, which is why developers can dislike such solutions.

- Dynamic Application Security Testing (DAST): This automated test method runs the application and, through specific inputs, checks whether the software behaves as expected, deviates, or even crashes. The biggest advantage is the small number, or even the absence, of false positives. The disadvantage lies in the fact that it is virtually impossible to check the whole software and it can be complex to identify which line of code is responsible for an error.

- Feedback-based Application Security Testing (FAST): This is an improvement on DAST. The basic idea is to use current and advanced fuzzing tools to obtain precise information about the relevant code section for each input. The mutation engine's system learns from each feedback and improves the quality of the next input data set. Through continuous and feedback-driven optimization, FAST also penetrates deeper levels of code and provides better and more meaningful insights. This is currently considered the best-in-class approach.

The usage of artificial intelligence and machine learning can be a game-changer. SAST and DAST are already performed today with the help of machine learning algorithms. SAST and AI complement each other to reduce the impact of high false-positive rates using the huge amount of code analyzed. Dynamic Application Security Testing and Manual Application Security Testing are complemented with AI/ML algorithms when they are supposed to analyze dynamic applications in a known context and protect them.

Beyond code security testing, there are several other valuable security checks that show potential for advanced automation. Breach and attack simulations (BAS), automated penetration tests, and vulnerability scans are tasks that when automated can serve to relieve developers, operation staff, and security experts from repetitive standard tasks.

Traditionally, attack simulations were a form of security testing conducted manually by two teams, red and blue. The red played the role of attacker and the blue defender. BAS has allowed for this process to be conducted automatically and continuously via a combination of red and blue teaming known as "purple teaming," which seeks to find smaller subsets of vulnerabilities that could be exploited in a breach. However, this technology has not matured to include AI or ML yet and has the potential to bog down security personnel with even more alerts.

Automated penetration testing helps to accelerate security measures. It enriches the reporting process so that security reports are delivered instantly, can be re-run on-demand, cost less, and offer prioritized recommendations for remediation. Manual penetration testing is more expensive and time-consuming, as it produces lengthy reports that need to be analyzed. Interestingly, an ideal solution integrates automatic testing with human management. Automated testing boasts advantages in speed and continuity, but manual testing applies human intellect to catch business-related threats.

BAS and penetration testing perform automated attacks that assess the vulnerability and response capability of systems, but it is important to highlight that the reachability of those systems is another important factor. Companies may integrate context-aware solutions on top of or embedded in automatic penetration testing tools that can assess the potential for unauthorized access to systems or data. A security orchestrator, for example, can map the whole network (i.e., firewall, router, balancer, etc.) and highlight the exploitable vulnerabilities while also keeping in mind the reachability from the source of the attack.

The vulnerability assessment (VA) is another process that produces a lot of data, helping to identify thousands of vulnerabilities. Unfortunately, not all of them are exploitable and the sheer

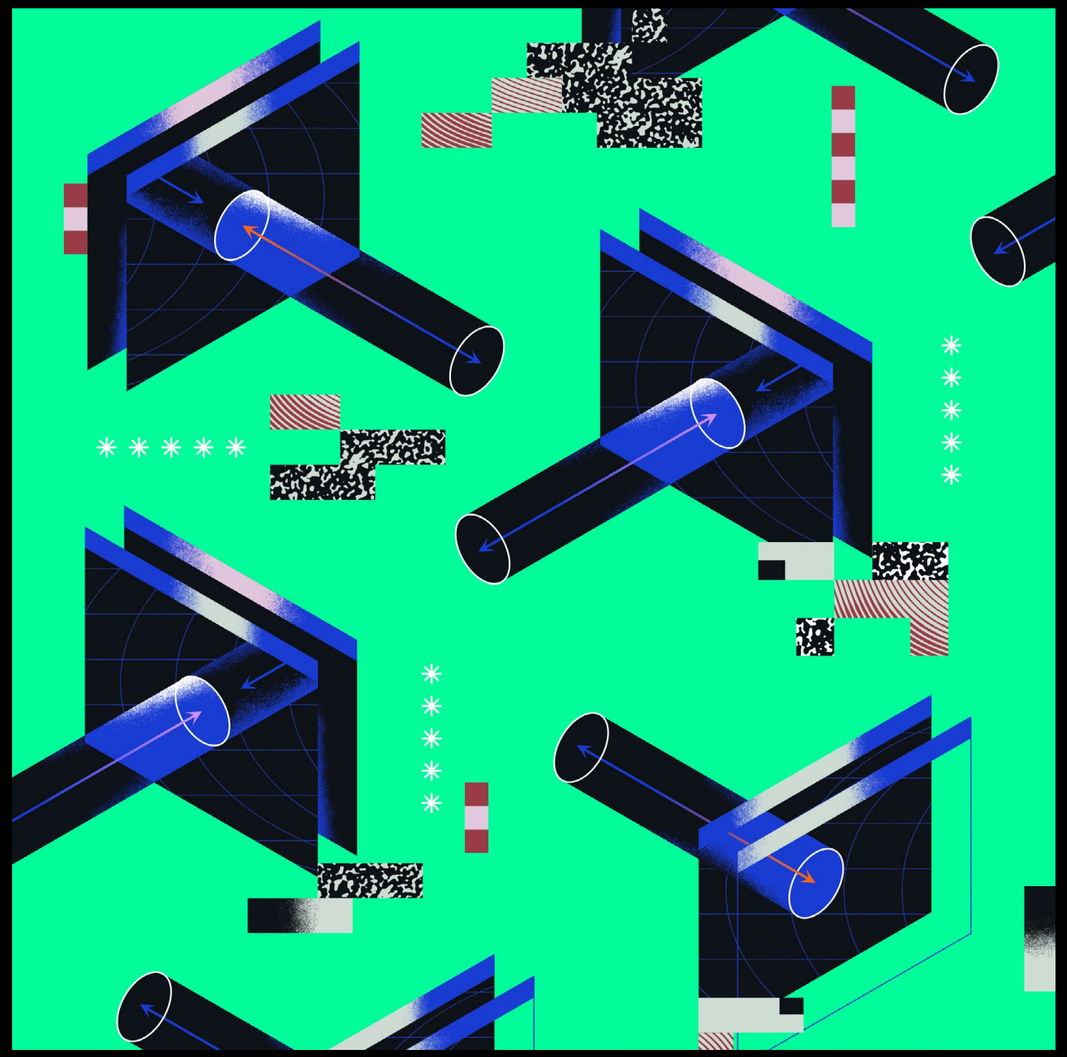
quantity can overwhelm security teams. Vulnerability prioritization technology (VPT) plugs the gaps in VA solutions by identifying and prioritizing only vulnerabilities that require aggressive treatment. VPT tools use threat intelligence, organizational asset context, and risk modeling, in addition to machine learning, to predict the likelihood of a vulnerability being exploited.

Application security automation does not end with deployment. In a DevSecOps context, application security extends through runtime. For example, due to the growing need to secure applications in the cloud, Cloud Native Application Protection Platforms (CNAPP) are now commonly used throughout the application lifecycle. Broadly speaking, a CNAPP solution aims to address workload and configuration security by using automation to scan applications both while in development and during runtime. Its main capabilities are:

- Cloud Security Posture Management (CSPM), which identifies misconfigurations in cloud resources, tracks compliance to different controls and frameworks, and remediates drifts

- Cloud Workload Protection (CWP) platforms, which secure cloud workloads, scanning for vulnerabilities, system configuration, and more

- Cloud Infrastructure Entitlements Management (CIEM), which delivers infrastructure entitlement management capabilities so organizations can enforce related governance controls.



Endpoint security and incident management

> The automation and orchestration capabilities of XDR platforms hold the potential to optimize a large portion of security operations, including monitoring, management, detection, analysis, data enrichment, correlation and response. Providing end-to-end automation capabilities that span tools, processes and workflows, security platforms help alleviate the time needed to conduct mundane, repeatable tasks so more time can be focused on strategic and value-add initiatives.
>
> Fernando Montenegro, Aaron Sherrill, and Scott Crawford, 451 Research [S&P, 2021]

EDR and XDR: a reality check

Endpoints like desktops, laptops, phones, tablets and servers can be key points of entry for cyber attackers and therefore must be thoroughly protected. Traditional endpoint security included antivirus, e-mail filtering, and firewall protections, but as attacks become more sophisticated, endpoint security must adapt. An attacker who gains access to an endpoint could gain access to the entire system, putting customer and employee data, intellectual property, and other critical enterprise assets at risk.

Endpoint Detection and Response (EDR) has been around for several years and is still one of the most relevant products on the market. Its functions include detecting, recording and responding to attacks: a clear development from traditional endpoint protections that focused only on attack prevention. EDR is well-suited for large scale networks that have too many endpoints for antivirus alone to handle. It is easily integrated alongside other security tools, malware analysis, and threat intelligence, and is now commonly used by medium-sized organizations thanks to the increasing availability of “off-the-shelf” EDR solutions.

EDR technology supports SOCs and alleviates security teams from monotonous and repetitive tasks. While it serves as the framework for many recent security tools and is considered to be a market standard, EDR is not comprehensive: due to its focus on the endpoint it cannot provide threat detection and it does not protect the network infrastructure. Furthermore, some endpoints – in particular, simpler machines like mobile phones or IoT devices – do not support EDR agents, leaving endpoints unmanaged, unmonitored, and unprotected.

Extended Detection and Response (XDR) involves collection and correlation across not just endpoints, but also networks and the cloud, offering improved visibility and better contextualization of threats. Its use of AI for event correlation produces fewer but more significant aggregated alerts, automates repetitive response activities, and supplies a centralized solution for policy configuration and security hardening.

Both XDR and EDR can be used to detect, respond, and react to threats as well as recognize emerging threats. They both offer data, alerts, automated threat responses, and assistance with threat investigation. Under XDR, much information could be aggregated onto an incident console: for example, information about access granted to a webpage containing malware, the subsequent infection, reloading of the payload, possible lateral propagation, and communication with a command-and-control system.

Another crucial difference between EDR and XDR is their implementation. EDR, specifically designed to focus on endpoints, is best employed alongside other security tools in order to protect the entire network. XDR, on the other hand, can use various tools to protect even more components of the network but must be paired with security experts who know how to utilize these tools.

While the detection of potential incidents is already highly automated, the response, including remediation like virtual patching, is in most cases still handled by human security analysts. Moreover, the increasing complexity of cyberattacks warrants an increasing complexity of the response. EDR and XDR solutions detect incidents, but when it comes to the response, companies often prefer analysts to identify the optimal solution.

One reason companies hesitate to enact automated responses is the false positive rate for threats: occasionally XDR solutions detect false positives, and most organizations want to avoid stopping valid actions by employees or customers. While false-positive rates can be minimized when companies are able to

feed comprehensive datasets into the system, this proves a challenging task. Many organizations are simply not at the proper security maturity level and lack adequate knowledge about their data and where it resides.

As such, the adoption of innovative products like XDR has been somewhat slow. The products require a suitable amount of data to function optimally, and some organizations with legacy systems and software are not ready to support the complex XDR technology. For these companies, upgrading to XDR could require first upgrading their systems and budgeting for extra time and labor, particularly during the beginning phases of installation.

The general lack of understanding of XDR, how it can be implemented into SOCs, and the prerequisites necessary to adopt such a system are all deterrents for companies who would like to develop their cybersecurity efforts. These organizations will need to prepare to face these issues as XDR ceases to be just a marketing buzzword and enters full force into the cybersecurity realm.

PAC (Teknowlogy Group)'s market forecast on EDR and XDR market

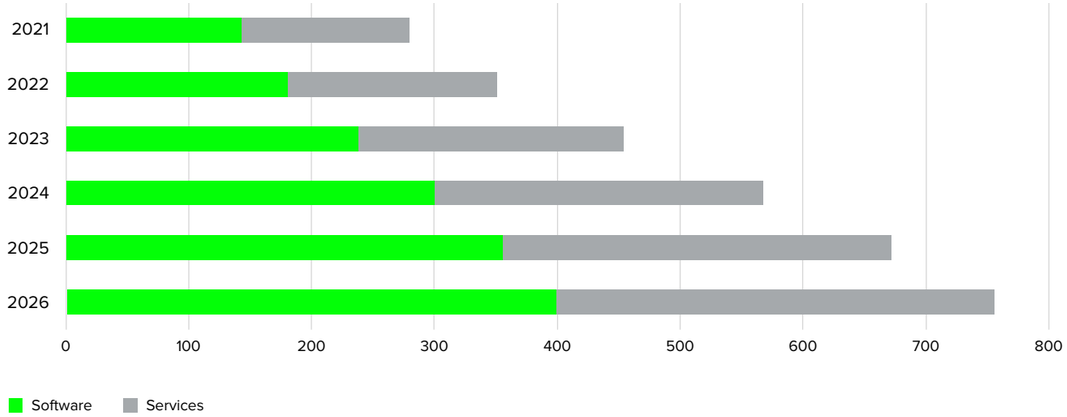
According to PAC (Teknowlogy Group), the use of EDR and XDR solutions is already a must for user organizations. Automated responses enable faster resolution times and may lower the costs of potential damage. On the other hand, trust in fully automated responses is limited.

Organizations should therefore focus on response automation monitored by humans for the time being, which basically means that the system detects incidents, recommends actions to respond to these incidents, and automatically performs these actions once a human security analyst has released them. In the future, this intermediate step of human monitoring might become unnecessary.

In collaboration with PAC, we forecast the possible evolution of the EDR and XDR solutions market in Europe-5 and Big-5 clusters, split by software and services (consulting, system integration, and managed services).

Europe-5: evolution of EDR and XDR market (million euros)

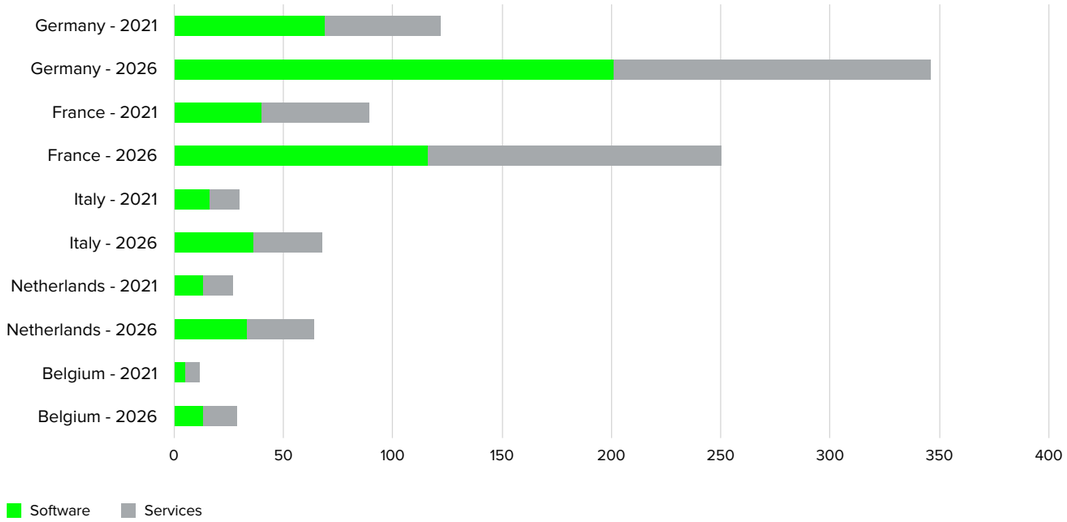
Source: Teknowlogy Group for Reply, 2022



Compared to the explosive growth rate expected for the application security automation market in the Europe-5 segment, the EDR and XDR market will grow less, despite starting with a larger initial market size. The software segment was at €143 million in 2021 and is forecast to grow up to €400 million in the next five years. The services segment was at €137 million and is projected to reach €357 million in 2026.

Source: Teknowlogy Group for Reply, 2022

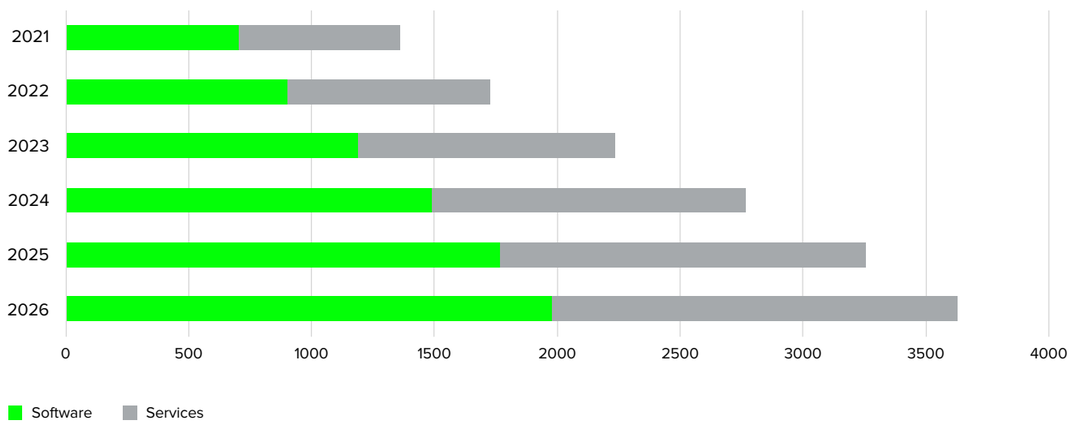
Europe-5: comparison 2021-2026 of EDR and XDR market, by country (million euros)



Both the German EDR- and XDR-related software and services segments are the largest in the Europe-5 cluster and the ones with larger forecast growth. They are expected to grow in 2026 to €200 million (almost tripling in value since 2021) and €145 million, respectively. France is already the second-largest market and it will maintain its position across both segments, followed by Italy (€68 million in 2026) and the Netherlands (€65 million).

Source: Teknowlogy Group for Reply, 2022

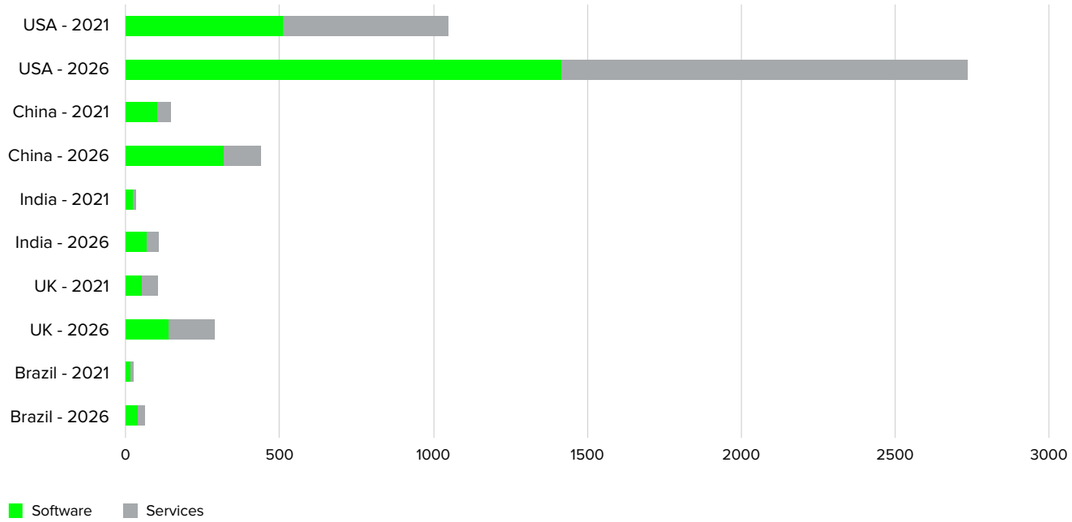
Big-5: evolution of EDR and XDR market (million euros)



In the Big-5 cluster too, the EDR/XDR software segment will be bigger and faster growing than the services one. The former totaled €700 million in 2021 and is forecast to reach €2 billion in 2026; the latter hit €660 million in 2021 and is projected to reach €1.65 billion. While the growth rate of the software segment is higher in the Big-5 cluster compared to the Europe-5 one, it is lower for the services segment.

Big-5: comparison 2021-2026 of EDR and XDR market, by country (million euros)

Source: Teknowlogy Group for Reply, 2022



The Big-5 cluster for EDR/XDR is led by the United States, where the software segment totaled €510 million in 2021 with projections to grow to €1.4 billion in 2026; the services segment was at €537 million and is projected to reach €1.3 billion. China's growth rate will be the highest in the cluster, though its total market value will reach less than €500 million in total.

Endpoint security and incident management: approaches and lessons learned

As organizations complexify their networks to include personal devices, the cloud, and IoT devices, attackers can exploit these new routes and enter the network. Additionally, as organizations attempt to track security vulnerabilities across their various endpoints, many fail to have a centralized point to store a list of all assignments and vulnerabilities. The problem is twofold: there is a need for more coordinated protection efforts across all entry points and endpoints and a need to synthesize the security data that is found when conducting these security procedures.

EDR and XDR tend to dominate in corporate discussions around endpoint and network security, but this does not mean they are the only tools on the market for such purposes. Security Incident Event Management (SIEM), for example, is one of the most popular systems for collecting and analyzing aggregated log data and discovering security events that are then dealt with by the Security Operations Center. Common sources for the data include firewalls, data loss prevention tools, antivirus software, and more. It is limited because it can only address known patterns of attack based on the logs that are provided by the company.

Based on Reply experience, many enterprises employing SIEM struggle to extract value from the increasing quantity of information collected by these solutions. They are constrained to historical data which is not quickly readable and relies on static-based triggers to detect threats. Instead, new solutions ingest this data on a big data platform and leverage AI to find alarms that would otherwise go undetected by SIEM systems.

The initial challenge with infusing AI on SIEM-based solutions is the potential production of a high rate of false positives. This is resolved by fine-tuning the algorithm and exploiting feedback from the SOC. The challenge for the management is deciding whether the big data platform is worth the cost. These systems cost more than “off-the-shelf” SIEMs and require heavy up-front labor from the SOC team.

Security Orchestration, Automation and Response (SOAR) was the next development to arrive after SIEM. It aims to automate both the process of gathering data and response actions, to accelerate remediation. SOAR incorporates data from a variety of sources, which is why it is a step up from SIEM technology. Sources for external data include threat intelligence and reports on recent attack signatures or phishing attempts. With SOAR, AI can be introduced into all of the key usage areas: threat and vulnerability management, incident response, and security operations automation.

User and entity behavioral analysis (UEBA) technology analyzes applications, networks, servers, and more, drawing on user information such as exchanges between employees or e-mails to analyze behavior and identify potential threats. Using ML algorithms, it can detect changes in behavior and sound an alert for issues like data theft, compromise of application accounts, or privilege abuse.

While today this is a separate tool, experts predict that this technology will be integrated into existing solutions such as SIEM and EDR. Additionally, while Reply’s experiences show that UEBA technology is mature and ready to use, it should be carefully integrated with proper compliance with local data privacy and work-related laws.

As organizations consider various security tools and strategies, they must take into consideration the strength of their current security measures, their long-term security plans, and potential routes for implementation that may simplify the process.

- Evaluate the security maturity level of the company before attempting to implement more complex tools and systems such as SOAR, SIEM, or XDR. These tools require effective SOCs and experienced security analysts. Certain base protections (e.g., firewall, security gateways) should be put in place before moving on to more complex security measures.

- Determine if the company will require an upgraded SOC or if it would be preferable to outsource difficult security measures to an external company. Many companies suffer from a lack of internal security talent that is capable of handling their security efforts. Managed Detection and Response (MDR) is one potential solution; it is a service that combines human talent with technology to conduct threat hunting, monitoring and response.

- Take into account that advanced endpoint protection solutions need to be employed for several years. Unlike firewall and antivirus licenses which can be re-purchased annually, these solutions are considered part of a multi-year strategy and it may not be easy to change course from one year to another.

- Remain wary of software vendors who claim to offer XDR but, in reality, are simply pairing EDR with legacy security technologies like firewalls and e-mail security gateways. Many vendors are still in development while marketing their products, resulting in “XDR” solutions that only partially meet the definition of XDR.

Companies need to be aware of the full extent of their own endpoints, particularly now that IoT devices and remote working have entered the picture. For example, companies should seek solutions to minimize the risk of “Bring your own device” (BYOD) policies. Risks include employees accidentally downloading malicious mobile applications, falling victim to phishing attacks, or simply losing their devices.

Organizations seeking to reduce these risks are usually implementing formal BYOD policies, restricting highly sensitive information to company devices only, and limiting employee access to data on a need-to-know basis. The use of Virtual Mobile Infrastructure (VMI) systems can help effectively separate company files from personal files.

Another best practice for companies is employing automatic asset discovery and inventory, which allows organizations to avoid blind spots in their system. It is important to frequently update system databases to reflect the adding, reconfiguring, or retiring of devices. In this case, AI can automatically track a company’s assets, merge duplicate data, and determine the criticality of cyber risks.

Internet of things security

> We are living in the era of big data where the necessity of applying AI/ML has been very critical to the process and analyze the collected cloud-based big data fast and accurately. However, even though AI is currently playing a bigger role in improving the traditional cybersecurity, both the cloud vulnerability and the networking of IoT devices are still major threats. Beside the security issues of cloud and IoT devices, AI is also being used by hackers and continues to be a threat to the world of cybersecurity. Moreover, most of wirelessly accessed IoT devices deployed on a public network are also under constant cyber threats.

Temechu G. Zewdie and Anteneh Girma, University of the District of Columbia [Zewdie-Girma, 2020]

The market's awareness of IoT Security has grown in recent years

IoT's interconnected format allows for each and every device in the network to be a potential weak point for an attacker. A single vulnerability could be enough to shut down an entire infrastructure and the complexity of the network massively increases the scope for attack.

By 2026, we estimate up to 80 billion networked devices on earth, with an average of almost ten devices per person living on the planet. In reality, these devices will be concentrated in a limited number of use cases and locations (i.e., a hospital might have hundreds of critical IoT devices), which poses a substantial risk from a security standpoint.

Despite quick growth, the IoT field was launched with initial low security maturity. The first vendors of IoT devices and gateways, as well as the first users of proof-of-concept installations, invested too little in security and privacy: this created issues when going live in the real world.

Since its inception, IoT has expanded to support various industries and use cases. Smart Factories and Smart Logistics, for example, are at the heart of Industry 4.0: they allow for a production environment to essentially monitor itself and proactively address problems. The resulting efficiency from predictive maintenance, increased transparency, and machine learning integration proves beneficial for lowering costs and optimizing production and distribution.

Download Reply Research "Industrial IoT: a Reality Check"

The impressive range of abilities offered by IoT regrettably prevents the creation of a standardized solution for IoT cybersecurity. As a result, further attention to the importance of IoT security in the past few years has been compelled by numerous attacks on these complex infrastructures. Over 60 million attacks on

IoT occurred just in 2021 [SonicWall, 2022]: one such attack, for example, allowed hackers access to a system of 150,000 smart security cameras located inside hospitals, companies, police departments, prisons, and schools [Bloomberg, 2021].

Companies are often deterred from adopting IoT technology because of uncertainty about fail-safe security procedures and the associated costs of implementation. Those who face major security issues may lose the trust of their stakeholders and tarnish their brand reputation, thus security cannot be ignored. Brand reputation is only one of several concerns: as IoT networks reach into fields ranging from healthcare to home to automotive industries, the risks multiply.

IoT is now employed not only by enterprises but also by private consumers. One example is the Smart Home, where users install networked and remote-controlled devices and automatable processes that can do everything from controlling the heating, lighting, and appliances to playing music or managing the home security system. Critical infrastructures are enjoying the benefits of IoT too: Smart Healthcare, for example, intelligently combines automation and data analysis to network embedded sensors for physiological data (i.e., heart rate or body temperature), actuators, or other devices that collect and transmit information.

Those who install security systems in their homes or drive semi-automated cars expect that their products are not susceptible to attacks that might endanger them or compromise their private information. In many ways, IoT security has large implications for both data privacy and personal safety; these need to be taken seriously to ensure customer trust and wellbeing.

The market's attention for IoT security is, fortunately, growing fast; yet, ensuring IoT security is anything but simple. IoT environments are more complex and less standardized, lacking well-defined best practices. Even more, different endpoints may have different security capabilities, so that smaller, more constrained devices only allow basic encryption while large servers can run countless security applications.

Automation of IoT security improves prevention and protects critical systems

IoT security is complex, so one of the most difficult challenges is viewing it holistically. Tech vendors who prefer to specialize in niche areas, such as encryption or cloud security, then lack the ability to discuss the market comprehensively. As a result, organizations make fatal errors, such as lacking proper asset inventories, focusing on detection and ignoring prevention, and underestimating cloud security by falsely assuming that its security is guaranteed by big platforms.

Architecturally, IoT is not a completely new type of infrastructure. For example, Industrial IoT usually consists of sensors and actuators, gateways, PLCs, and an edge computing unit or a SCADA system that can be connected to a data center or the cloud. Therefore, from a security point of view, standard IT measures can and should be applied. On top of that, managers should monitor and verify the reliability of devices and keep upgrading/updating them.

In fact, for IoT incident detection and response automation, the same technologies (EDR/XDR) can be used as for classic infrastructure components. For edge computing units, this is easy, as they consist of standard servers or industrial PCs. It is more complicated for small IoT gateways which use low-power controllers without a standard operating system and have limited computing power and storage. For these components, EDR/XDR is too heavy and basically unavailable; as a result, IoT gateways,

sensors, and actuators need to be encapsulated to make sure that the edge computing device or the SCADA system can be sufficiently secured.

Edge computing opened the door to a variety of IoT solutions, from digital factories to smart cities, but undoubtedly also increased the scope for potential cyberattacks by increasing the number of edge and IoT devices. In particular, edge devices that are connected to critical systems in enterprises, such as the equipment in factories, pose a risk to business operations.

Download Reply Research "From Cloud to Edge"

Therefore, one important sector of IoT security is that of trust management, which aims to assess the trustworthiness of data and devices within IoT systems. Currently, there are several trust management mechanisms that can be employed, some of which utilize automation or machine learning technology.

For example, policy-based mechanisms assess the trustworthiness of smart objects based on a set of rules that is established, then give automatic responses that can constrain the behavior of those smart objects if necessary. Machine learning-based techniques can take data from multiple IoT applications, consider various "trust features," and predict the trust level of IoT objects.

Still, most organizations remain reactive rather than proactive as they struggle to keep up with manual checking techniques that are expensive and time-consuming. But it is no longer adequate to simply remediate security issues; it is crucial to predict them. Enterprises must anticipate IoT risks, and simply having a solid security concept is not enough. Operating IoT safely requires continuous monitoring of the security infrastructure, as the success of an IoT solution largely depends on the integrity and confidentiality of the data it provides.

Reply has developed an IoT Cybersecurity Test Unit in order to help organizations develop strategic security plans. The Security Test Unit aims to assist companies in preparing for various attack techniques, such as software vulnerabilities exploitation, sabotage, IoT communication protocol hijacking, and brute force attacks. The objective of the unit is to demonstrate and test possible attacks to support organizations in reacting quickly to security issues and reduce the risk of production outages.

Read more about Reply's IoT Cybersecurity Test Unit

PAC (Teknowlogy Group)'s market forecast on IoT Security

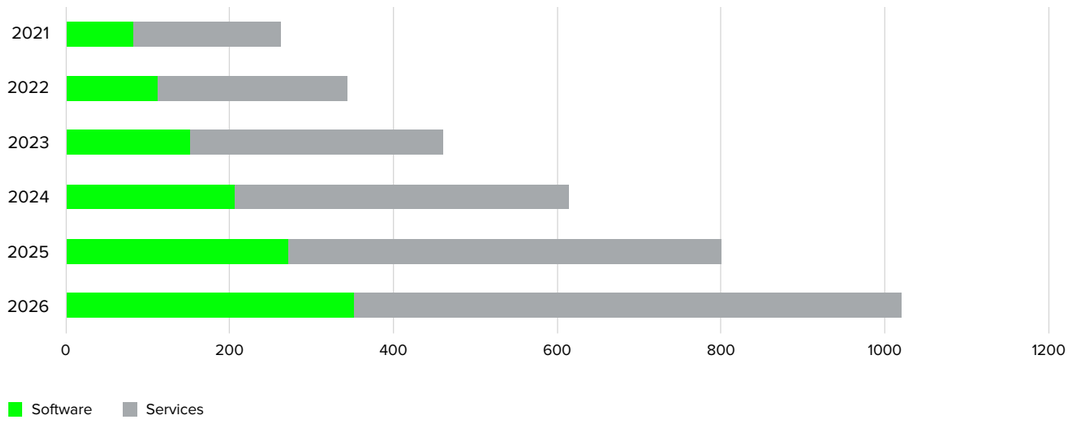
According to PAC (Teknowlogy Group), sooner or later, the boundary between IT and OT (Operational Technology) has to be weakened if IoT is to unleash its full business value. This is why IT security measures have to be applied to IoT and OT to obtain a full picture of the landscape and associated risks and detect and respond to incidents. This means SIEMs and SOCs should focus not only on IT, but should also include OT, and with that IoT.

Before deploying IoT in business-relevant areas, IoT security has to be guaranteed. The best way to achieve this is to combine IT and OT from both a system management perspective and a security perspective. This is an organizational rather than technical question, because responsibilities are often still separate and the two sides have cooperated little so far. It is also crucial to deploy technologies and solutions such as EDR/XDR, SIEMs/SOCs to the entire infrastructure, otherwise there will be gaps in the security mesh that can be exploited by attackers.

In collaboration with PAC, we forecast the possible evolution of the Internet of Things security automation market in Europe-5 and Big-5 clusters. Estimates include automated IoT endpoint security, network security, edge security, and cloud security, split by software and services (consulting, system integration, and managed services).

Source: Teknowlogy Group for Reply, 2022

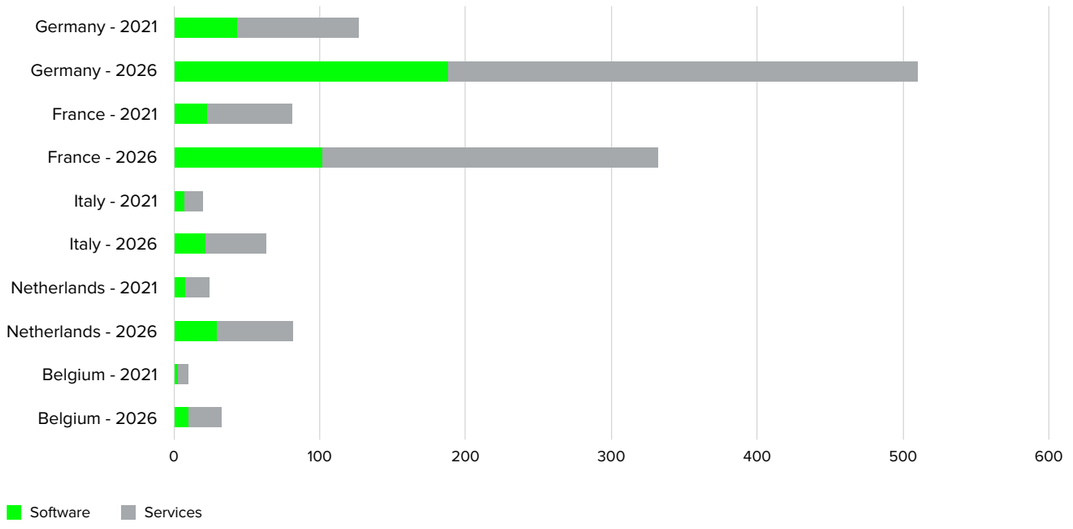
Europe-5: evolution of IoT security automation market (million euros)



The IoT security automation market will be fast-growing in the next five years in the Europe-5 cluster, eventually crossing the 1 billion euro mark. The services segment was at €180 million in 2021 and is forecast to reach up to €670 million by 2026. Even if of a smaller market value, the software segment will have a faster growth rate, increasing from €83 million in 2021 to €350 million in 2026.

Source: Teknowlogy Group for Reply, 2022

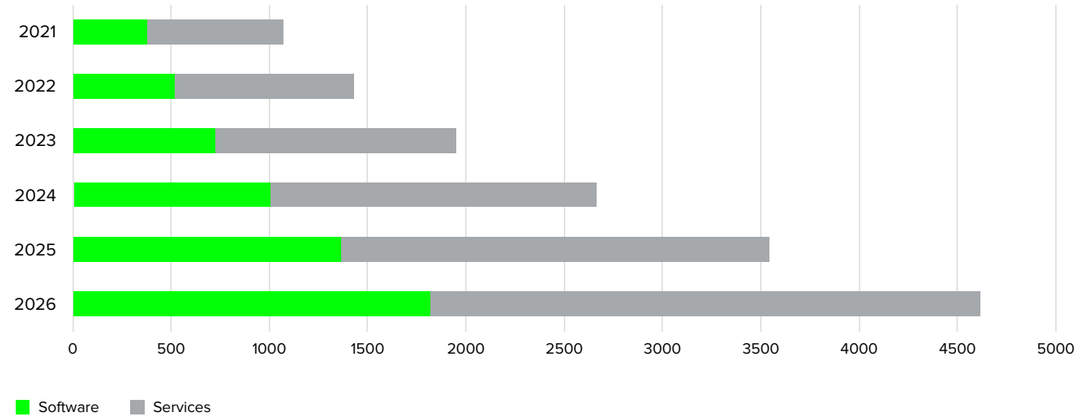
Europe-5: comparison 2021-2026 of IoT security automation market, by country (million euros)



The main IoT security automation market in the Europe-5 cluster in 2021 was Germany, driven by strong demand in the Industrial IoT context. Its software market is forecast to grow from €43 to €188 million by 2026, while the services segment is projected to go from €84 to €322 million. France is the country with the highest forecast growth rate (4x), hitting a total of €332 million.

Big-5: evolution of IoT security automation market (million euros)

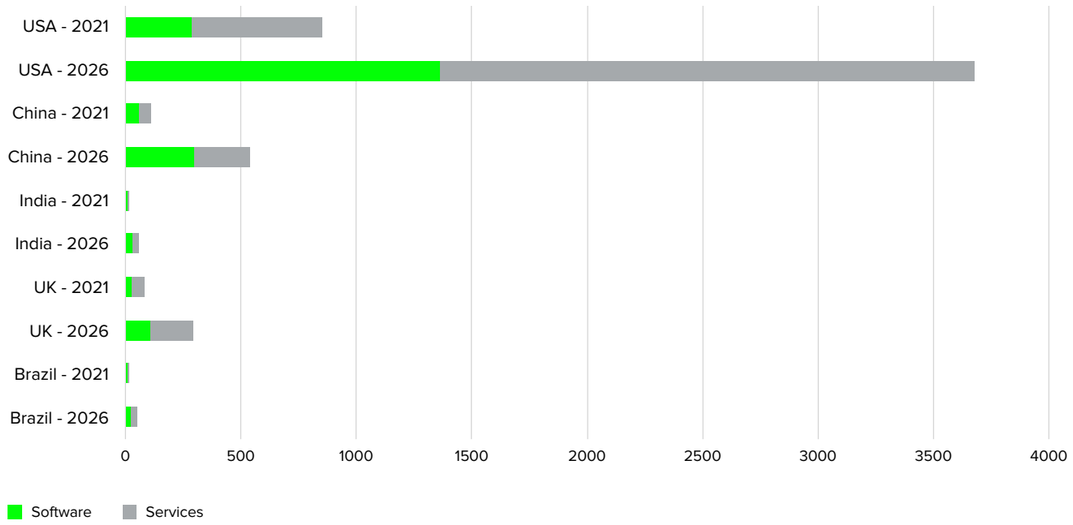
Source: Teknowlogy Group for Reply, 2022



The market of IoT security automation in the Big-5 cluster is forecast to go from €1 billion in 2021 to €4.6 billion in 2026. The growth rate for both the software and services segments is higher in Big-5 than in Europe-5 clusters: the software segment is forecast to grow from €382 million to €1.8 billion in 2026; the services segment is projected to go from €692 million to €2.8 billion.

Source: Teknowlogy Group for Reply, 2022

Big-5: comparison 2021-2026 of IoT security automation market, by country (million euros)



The United States were driving the cluster in 2021 and will maintain their leadership in 2026 thanks to consistent growth: the software segment size will almost quintuple in 2026 from 2021, while the services one will quadruple. The Chinese market will grow faster, even if its size will only reach €537 million compared to €3.7 billion in the US. Compared to these two countries, the UK, Brazil and India will present slower growth in their markets for both segments.

Data security and protection

“The commercialization of cybercrime has made it easier for criminals to exploit vulnerabilities on a massive scale,” explains Scott Sayce, Global Head of Cyber at AGCS. Previously, hackers typically targeted specific industries that dealt with personal data, such as healthcare and retail, but ransomware attacks are indiscriminate, affecting organizations across all sectors, public and private, both large and small. “In the past, a bank robber may have hit one or two banks in a week after many months of preparation. Yet, with a cyberattack, you can target thousands of businesses at once, anywhere in the world, and extract more valuable data than before. Just one gigabyte of data is approximately the equivalent of the information contained within around 5,000 books,” says Sayce.

Scott Sayce, Global Head of Cyber at Allianz Global Corporate & Specialty [Allianz, 2022]

The initial steps of good data security

Ensuring data is well-kept and safely stored is an increasingly relevant challenge for cybersecurity experts. It is easy to imagine how many different security threats arise from bad manipulation of data, cyber attackers, unfaithful employees or even just “clumsy” end-users of data. These threats can be costly and damaging to organizations. According to IBM, the average cost of a data breach rose from $3.86 million (USD) to $4.24 million (USD) [IBM, 2021]. As such, data security should be included as part of the broader security efforts in any organization.

Organizations often differentiate between two “types” of data: enterprise data (e.g., information about a company’s purchases, sales statistics, or production planning) and sensitive data (e.g., private consumer or employee information). The latter is subject to heavier compliance regulations, such as the General Data Protection Regulation (GDPR) in Europe, the General Personal Data Protection Law (LGPD) in Brazil, the Consumer Privacy Act (CCPA) in California, and other data privacy laws around the world; though, companies should strive to go beyond what is simply required for an audit or mere compliance to data privacy laws.

Meanwhile, an attack on the former may yield consequences for a business’s competitive advantage or operational functionality. This is because data breaches, which occur when attackers manage to bypass security and steal data from the system, can lead to operational downtime, unexpected costs, loss of brand reputation, and even potential legal penalties. For example, some attackers use a “double extortion” method, in which they first ask you to pay to get your data back, then ask you to pay again for them to not publish the stolen data (which could easily result in reputational damage and legal penalties).

One of the first steps in a data security plan is defining who is responsible for enterprise and sensitive data security. Data protection officers (DPO) should be appointed to ensure the company’s adherence to any requirements contingent on the geographic location of the data; in some areas, they are legally required. In addition, a company may choose to appoint a Chief data officer (CDO) to help guide privacy policies and compliance within the company. In the case of a data security incident, data breach, or audit, it is important to know who is responsible for data management.

Data discovery serves as the foundation for all other data security measures. Before data security experts can take more specific measures, such as encryption, tokenization, or data loss prevention, they need to first locate all data across the network. However, in many enterprises, the knowledge of where data is stored remains low.

This is because while database location may be easier when assessing structured data in applications such as CRM and ERP, the contents of the data may remain unknown, and it is even harder to keep track of unstructured data contained in e-mails, chat tools, videoconferencing systems, etc. Unfortunately, a large part of data generated by organizations is unstructured. While challenging, it is essential to know all data sources and adequately secure all data. Robotic Process Automation can help to support data discovery and keep corresponding inventory data up-to-date.

One of the biggest challenges to comprehensive data discovery is hybrid architecture, which requires discovery tools to locate all data both on-premises and in the cloud. Automation of these tools is imperative since new data is generated over time, cloud resources come and go, and manual search is simply not practical. These tools should be capable of scanning and inventorying all file types, structured and unstructured data, cloud repositories, and servers for sensitive data.

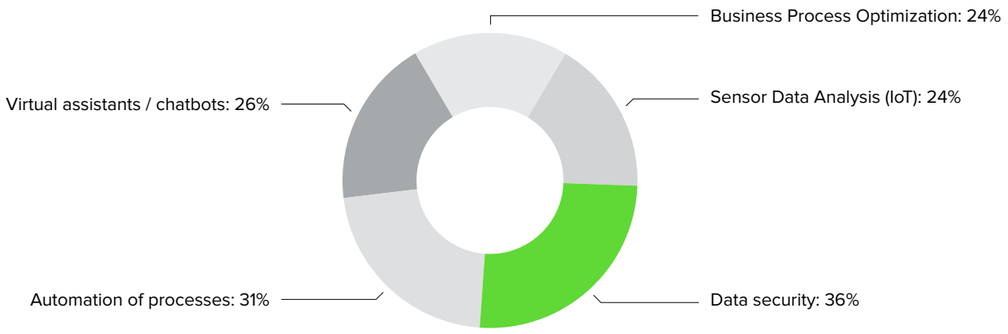
Without comprehensive data visibility, it will be very difficult for an organization to progress to more complex data protection measures. AI-enabled cybersecurity protections are only as capable as the data that is fed to them, making it an absolute imperative that security teams maximize their use of automated data discovery tools and fortify their data security teams.

Integrating AI into data security measures

AI is becoming a relevant tool for streamlining many data security procedures, from discovery to classification to remediation. It can help companies in complying with the location-based data privacy laws and play a role in decreasing the impact of data breaches. The full deployment of AI-based security automation can in fact lower the cost of a data breach from $6.7 million (USD) to $2.9 million (USD) and reduce the time it takes to identify and contain the breach [IBM, 2021].

Source: [Morning Consult, 2020]

Professionals at companies currently deploying AI report the top 5 most important ways their organization are using AI (%)



Artificial intelligence and machine learning algorithms are fed with data, so assuring that this data is completely secure is an increasingly crucial task for cybersecurity experts. This is likely one reason why over one-third of professionals at companies are reporting that the most important deployment of AI in their organization is for data security.

While RPAs are useful for automating data discovery, organizations must then classify the data that has been inventoried. Data classification is a process that organizes and tags data so that it is easily trackable, usable, and protectable. The sheer quantity of data stored by most organizations renders manual classification and periodic scans impractical and inefficient.

Automated systems improve and accelerate the process so that tasks like data tagging can be conducted via machine learning. By integrating ML into classification, organizations can train models to automatically classify data more accurately than humans. Overall, AI-enabled classification is more efficient, consistent, and continuous, and has the ability to update or re-classify data as necessary.

A recent challenge for security teams has been the expansion of data storage to more complicated networks as a result of hybrid work models brought on by the Covid-19 pandemic. Complex hybrid work models bode poorly for data security, resulting in moves toward “zero trust” approaches and micro-segmentation in an attempt to contain the range of damage caused by security breaches.

Additionally, attackers are now employing clever “marketing” strategies such as appealing to employee interests based on their personal data and browsing histories. This data, perhaps more readily available to attackers now that employees often double their personal devices as work devices, can be used to trick employees into opening phishing and malware attempts.

Automatic processes can help organizations avoid relying solely on employees to recognize when they are being targeted by these attacks. AI-enabled systems can even go a step further in recognizing phishing attempts. While automated processes can recognize signature-based threats, attackers can simply alter signatures to evade detection. AI has the capability to recognize characteristics or behaviors indicative of phishing and is therefore much more successful at preventing attempts from reaching employee inboxes in the first place.

Employee behavior around data is in general one of the most prevalent areas for modern-day data security. Organizations are expected to carefully monitor user activities with regard to data so as to prevent data exfiltration, data leaks, data loss, and insider threats.

Within an organization, access by individuals should be limited to only what they need to do their job and privileges should be adjusted or removed if an employee changes positions or leaves the company. This process is typically dictated by a company's Identity and Access Management (IAM) framework. Furthermore, IAM can incorporate AI and behavior analytical tools such as User Behavior Analytics, which analyzes human behavior, or User and Entity Behavior Analytics, which analyzes human behavior as well as device, network, and application behavior. These tools can help locate unusual or anomalous behavior that may result in insider threats.

Dynamic blocking and alerting can then implement AI to effectively identify abnormal patterns and alert security experts or block access when it detects strange behavior in the network. These tools can even leverage conditional access to corporate resources, determining when it is safe to grant access based on variable factors such as the geographic location of the user or the sensitivity of the data being accessed.

Encryption and encryption key management are two functions that also play a large role in keeping data out of unauthorized hands. Both of these processes can be automated to better protect data that is stored either on the cloud or on physical servers. Automating encryption key management in particular can reduce a significant source of major data breaches.

Occasionally, data can be retrieved by attackers even when they gain access to erased datasets. IT assets now have increased lifespans and storage capacities, resulting in the unintentional retention of sensitive business data on disk drives, mobile devices, and storage equipment. Data sanitization is a process that can remove this data without the possibility of recovery. To carry out data sanitization, organizations may choose data masking or data erasure.

Data masking is capable of preventing data loss, data exfiltration, insider threats, or account compromise by rendering stolen data useless to an attacker. Dynamic data masking can respond to automated alerts when data monitoring solutions detect abnormal behavior, and thus help prevent unauthorized access to sensitive data. Some dynamic data masking may use machine-learning algorithms, but its execution needs to be carefully monitored because poor training can impact its effectiveness.

Blocking unauthorized access to sensitive data and preventing the loss or misuse of data make up the crux of data loss prevention (DLP) software. DLP is actually a combination of several tools that perform actions like classification, identification of compliance issues, and remediation (in the form of alerts, encryption, and other protective actions).

DLP solutions aid with data identification by analyzing an organization's network and identifying sensitive information, and can then protect that data whether it is at rest, in use, or in

motion. This can mean encrypting data when sharing sensitive files or identifying anomalies as potential malicious behavior. When detecting and blocking sensitive data leaks, DLP may have to escalate requests for approval when a valid user has been blocked (i.e., for attempting to share a sensitive file).

Data security best practice involves integrating automated tools alongside manual protection procedures, such as maintaining tested backups, training employees on good security practices, and securing physical servers and devices in protected environments. Moreover, implementing detection tools does not ensure fast remediation action, so protective actions need to be considered from the beginning. Organizations must consider whether to react manually or employ various automated remediation responses such as dynamic data masking or blocking.

Data Protection should be part of the definition process of each data flow and has to be considered during the entire data lifecycle. This new model approach for data management is known as DataSecOps. Similar to DevSecOps, this approach calls for increased responsibility across data security teams and integration of data security measures in a way that is holistic and inclusive of DevOps and IT teams.

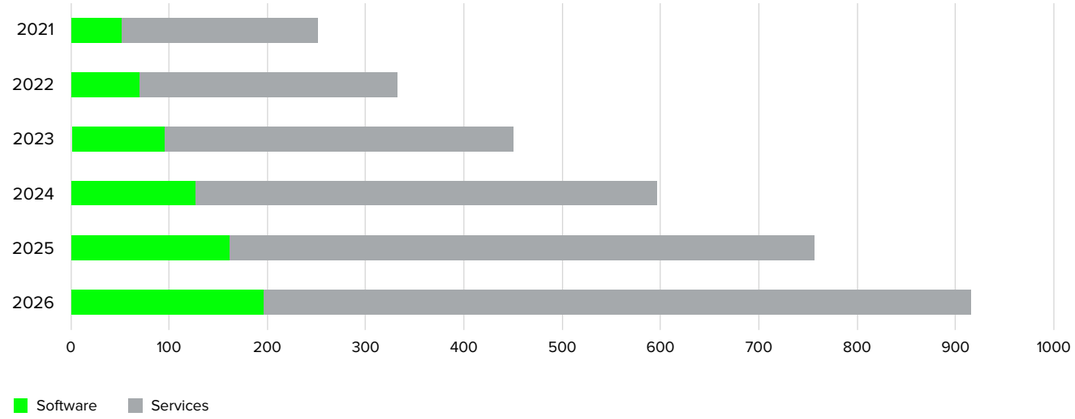
PAC (Teknowlogy Group)'s market forecast on data security automation

According to PAC (Teknowlogy Group), data security is crucial, and it starts with gaining a full picture of the data. This is why automated data discovery and automated classification are key to making sure other topics related to data security, such as encryption, adequately cover all data, and data access management guarantees GDPR-level compliance. Many organizations currently do not have these solutions in place, but with the increased use of cloud resources and a higher level of digitalization of business processes, this topic can no longer be ignored.

In collaboration with PAC, we forecast the possible evolution of the data security automation market in Europe-5 and Big-5 clusters. Estimates include automated tokenization, file integrity protection, encryption, e-Discovery, data loss prevention, data discovery and classification, split by software and services (consulting, system integration, and managed services).

Europe-5: evolution of data security automation market (million euros)

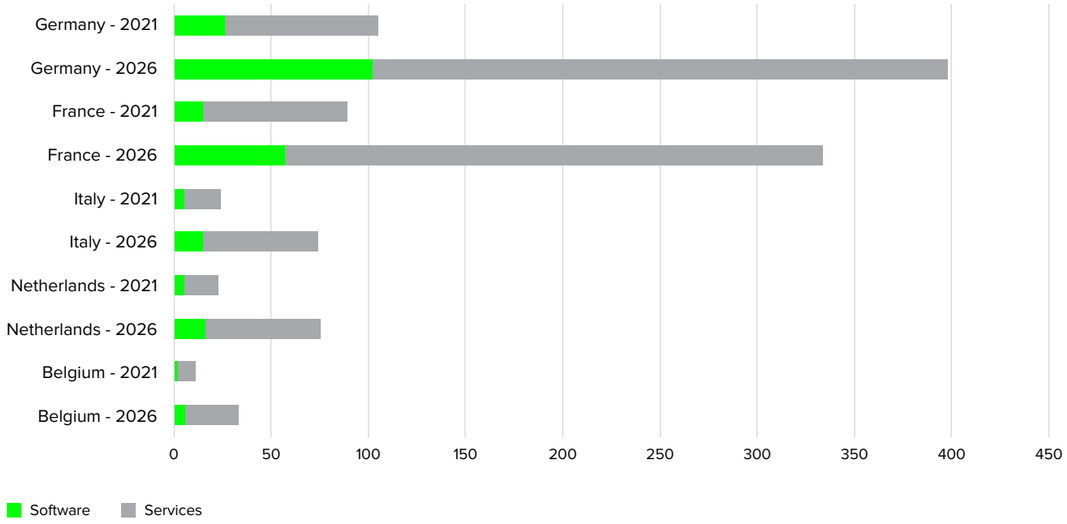
Source: Teknowlogy Group for Reply, 2022



Looking at the Europe-5 cluster, the data security automation market was at €251 million in 2021 and it will reach €915 million in 2026, with growth in both the software and services segments. The former will accelerate faster, up to €197 million by 2026; however, the latter will still amount to 73% of the market (€719 million).

Source: Teknowlogy Group for Reply, 2022

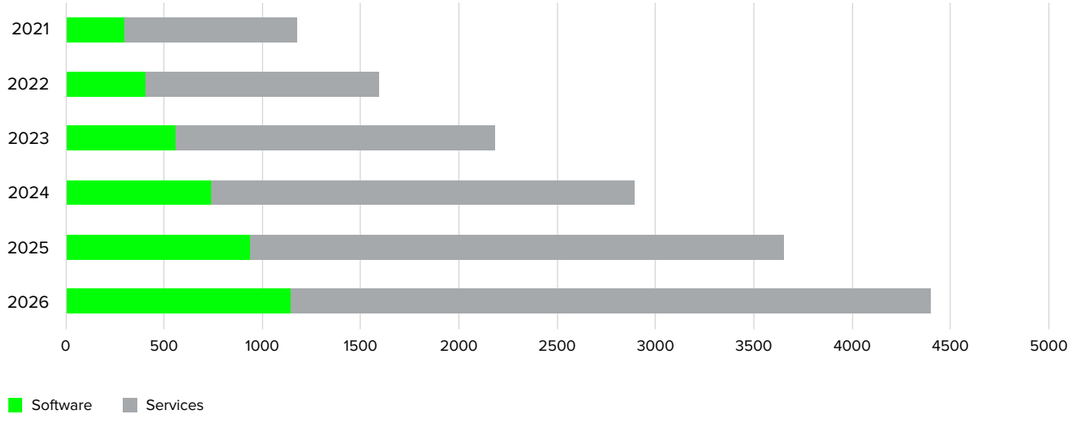
Europe-5: comparison 2021-2026 of data security automation market, by country (million euros)



The German and French data security automation markets were pretty close in 2021, with €105 and €90 million, respectively. The faster growth rate in Germany, however, will expand this margin, with projections for 2026 reaching €398 and €334 million, respectively. Italy and the Netherlands maintained similar sizes in 2021 (€23 million) and will grow similarly, reaching €75 million each.

Source: Teknowlogy Group for Reply, 2022

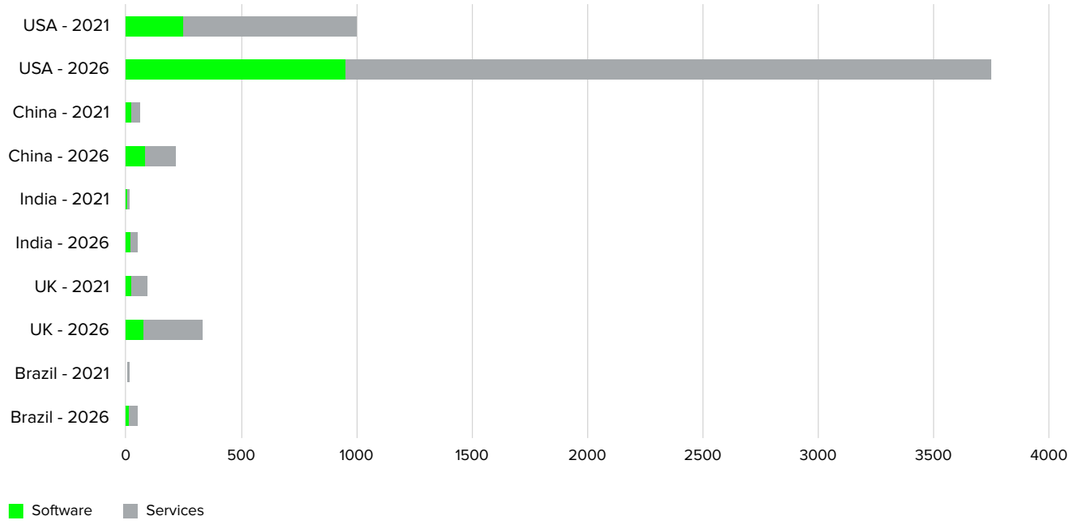
Big-5: evolution of data security automation market (million euros)



The growth rate for the data security automation market in the Big-5 cluster between 2021 and 2026 will be greater than for Europe-5. The Big-5 market will grow from €1.2 to €4.4 billion, with significant increases in both segments: the software will go from €300 million to €1.1 billion, while services will grow from €882 million to €3.2 billion.

Big-5: comparison 2021-2026 of data security automation market, by country (million euros)

Source: Teknowlogy Group for Reply, 2022



The data security automation-related software segment in the United States is forecast to grow from €92 to €333 million; the services one from €1 to €3.7 billion by 2026. The UK will be the biggest services market in the cluster after the USA, reaching €258 million by 2026. The highest growth of software will happen in China and India, where the investments will almost quadruple to a respective €81 and €19 million.

CONCLUSIONS

> **The future of cybersecurity will need to utilize AI to counter the bad guy's AI.**
>
> Kevin Krewell, Principal Analyst at TIRIAS Research [Krewell, 2020]

Cybersecurity automation is necessary to fight new threats

Present-day efforts have to recognize the increasing complexity and interconnectedness of all cybersecurity sectors and learn how to deal with it, a task that likely should have been considered far before these technologies were ever implemented. Cybersecurity is now playing catch-up with attackers who see technological innovations as vulnerabilities.

Complicating matters further, intensifying the focus on cybersecurity is often more of an investment than organizations realize. Security teams need to be robust and knowledgeable, but so do middle managers, OT, etc. Managers cannot seek the "shiny" new cybersecurity technologies that utilize AI and ML if their equipment is not fit to handle them yet. Before advancing from basics like firewall and antivirus, security teams, systems, and software often require an upgrade.

Meanwhile, every step forward in cybersecurity is a step forward for attackers as well. Several examples stem from the development of AI-based social engineering. Natural language processing, deepfakes, and AI-generated voices have all progressed in recent years and supported new methods for cyberattacks. As a result, experts have had to develop equally as powerful AI to detect fraudulent social interactions, such as deepfake detection.

Quantum computing is a field that since its inception has posed a threat to cybersecurity. While promising to transform cybersecurity through quantum-secure communications, cryptography and key distribution, it has the potential to threaten public-key cryptography. While not yet fully developed, quantum computing could someday soon be used to decrypt stolen financial and national security data. Researchers have begun pioneering solutions like impermeable algorithms in the hopes of anticipating these problems.

Cyberterrorism has perhaps been a driving force for countries to develop their security positions in recent years. Cyberterrorist attacks can have severe consequences, sometimes even deadly. One of the most common forms of attack is distributed denial of service, which can shut down the websites of crucial facilities like banks, newspapers, and government services. These attacks may also target hospitals or water supplies, having potentially lethal consequences if successful.

Cybersecurity is certainly a growing trend, but one borne out of necessity. Unlike other innovative technologies, cybersecurity is not advancing the way it is solely because of novelty or market curiosity. Cyberattacks, data breaches, and operational downtime can cripple businesses; they can topple societies. We can only expect that this topic will grow in the coming years, moving beyond basic automation to AI that continues to both create and solve cybersecurity issues.

APPENDIX

References

- [Allianz, 2022] Allianz Global Corporate & Specialty, Allianz Risk Barometer 2022
- [Bloomberg, 2021] William Turton, Hackers Breach Thousands of Security Cameras, Exposing Tesla, Jails, Hospitals, Bloomberg, 2021
- [CheckPoint, 2022] Cybersecurity Insiders, CheckPoint Cloud Security Report 2022, 2022
- [Clusit, 2022] Clusit, Rapporto Clusit 2022 sulla sicurezza ICT in Italia - Edizione di marzo 2022, 2022
- [IBM, 2021] IBM Security, Cost of a Data Breach Report 2021, 2021
- [ISC^2, 2021] ISC^2, Size of cybersecurity workforce worldwide in 2021, by country, Statista, 2021
- [Krewell, 2020] Kevin Krewell, IBM, AI And The Battle For Cybersecurity, 2020
- [Mittal et al., 2021] Kriti Mittal, Maryada Sharma, Manvi Gupta and Kavita Sheoran, DevSecOps: A Boon to the IT Industry, 4th International Conference On Innovative Computing And Communication (ICICC), 2021
- [Morgan, 2021] Steve Morgan, Cybersecurity Jobs Report: 3.5 Million Openings In 2025, Cybercrime Magazine, 2021
- [Morning Consult, 2020] Morning Consult for IBM, From Roadblock to Scale: The Global Sprint Towards AI, 2020
- [S&P, 2021] Fernando Montenegro, Aaron Sherrill, and Scott Crawford, The Rise of Extended Detection and Response, 451 Research - S&P Global Market Intelligence, 2021
- [Sensors, 2021] Ricardo Raimundo and Albérico Rosário, The Impact of Artificial Intelligence on Data System Security: A Literature Review, Sensors, 2021
- [SonicWall, 2022] SonicWall, 2022 SonicWall Cyber Threat Report, 2022
- [Statista, 2022] Statista Technology Market Outlook, Internet of Things 2022, 2022
- [Zewdie-Girma, 2020] Temechu G. Zewdie and Anteneh Girma, IoT Security and the Role of AI/ML to Combat Emerging Cyber Threats in Cloud Computing Environment, 2020

Reply Disclaimer

Mentioned trademarks and brands of customers belong to them.

This Research is for disseminative and informative purposes and it does not aim to exhaust the panorama of information available on the topic.

This Research is based on information also collected from third party sources, which Reply considers updated and accurate. However, Reply cannot guarantee the adequacy, accuracy, completeness or correctness of such information, nor can guarantee or represent that the Research is in every respect complete.

Reply therefore expressly declines any liability related to the use of the information provided, and makes no warranty of any kind concerning the information provided, including, but not limited to, warranties of merchantability or fitness for a particular purpose.

Reply also does not warrant that the quality of the information obtained by readers through this Research will meet their expectations.

The contents not specifically attributed to third parties have been developed and/or processed by Reply and Reply is the source.

Teknowlogy Group Disclaimer

Teknowlogy Group's market data mentioned in the document belong to the Teknowlogy Group. For more information, please visit http://www.sitsi.com.

Tekwnology Group's data are protected by copyright. Any reproduction or dissemination to third parties, including in part, requires the prior explicit authorization of the ordering party. The publication or dissemination of data, tables, graphics, etc. in other publications also requires prior authorization.

The contributions of the Tekwnology Group to this Research were compiled with the greatest possible care. However, no liability for their accuracy can be assumed. Analyses and evaluations reflect the state of Teknowlogy Group's knowledge in February 2022 and may change at any time. This applies in particular, but not exclusively, to statements made about the future.

PAC (Teknowlogy Group)'s contributions were produced by Pierre Audoin Consultants (PAC) - a Teknowlogy Group company. Reply had no influence over the analysis of the data and the production of the contents.

REPLY specialises in the design and implementation of solutions based on digital media and new communication channels. Through its network of highly specialised companies, Reply partners with major European corporations in the telecoms and media, industry and services, banking and insurance, and public administration sectors, to devise and develop business models built on the new paradigms of big data, cloud computing, digital media and the Internet of Things. Reply's services include: Consulting, Systems Integration and Digital Services.
www.reply.com