devoteam
Cyber Trust

Cybersecurity Trends for 2025

Making your tech journey more secure

What are the main cybersecurity trends we should pay attention to in 2025?

Introduction

As 2024 ends and 2025 approaches, it is time to reflect on the challenges faced and what the future holds for cybersecurity.

So far, this decade has brought us a bit of everything: high-risk cyberattacks, major technological failures, and even a global pandemic. With this backdrop in mind, looking ahead to 2025 involves contemplating emerging trends and preparing for what lies ahead.

The cybersecurity landscape is currently in a phase of rapid transformation, driven by several contributing factors. Political tensions have intensified, making state-sponsored cyberattacks an increasingly significant global concern. Additionally, the growing global digital interdependence amplifies the potential impact of these attacks, turning them into threats that transcend borders.

In this rapidly changing context, artificial intelligence (AI) has made significant technological advances, radically altering the threat landscape and forcing organisations to rethink their security strategies. This has led to **an increase in the use of AI and ML (machine learning) tools** to enhance threat detection and response.

In recent years, we have also witnessed a shift in tactics used by malicious actors. The growing emphasis on **identity-based approaches** has led cybersecurity professionals to reconsider concepts such as "privilege" and "identity security". The focus has shifted to limiting the impact of compromised accounts, strengthening defences against identity-based attacks.

With so much on the horizon, **it is essential for organisations to remain alert to new trends** and adjust their security strategies to tackle emerging challenges. Thus, it has become crucial to find solutions with simple and accessible approaches for all employees, enabling a shift from a reactive cybersecurity posture to a proactive one. We invite you to explore with us what will redefine the cybersecurity landscape in 2025 and potentially in the years to come.

devoteam
Cyber Trust

For 2025 we highlight some trends
in the cybersecurity ecosystem:

1.

The Realism of AI

By 2025, artificial intelligence (AI) is expected to move beyond the phase of inflated expectations and enter a stage of maturity, with organisations focusing on applications that deliver tangible value. The expansion of autonomous AI agents will be a key trend, automating operations in areas such as security and logistics, reducing manual tasks and improving response capabilities in routine activities. However, this advancement will bring new challenges, requiring stringent governance frameworks to ensure that the actions of these agents comply with organisational policies and standards, mitigating ethical and security risks. AI Governance Platforms will play an essential role in ensuring transparency and compliance in a landscape where regulatory demands vary.

The industry will adopt a pragmatic approach, prioritising the real impact of AI in high-value operational contexts, with an increased focus on security and accountability.

2.

Cybersecurity as a Service (CaaS)

Cybersecurity as a Service (CaaS) is expected to grow in popularity as companies seek more cost-effective ways to protect their digital assets. Cybersecurity as a service provides businesses with outsourced cybersecurity solutions, ranging from continuous threat monitoring to incident response. By utilising these services, even smaller companies can access advanced security tools without the need to build internal teams.

CaaS solutions will evolve to include AI-driven threat detection, automated incident response, and real-time analytics, helping businesses detect and mitigate threats more quickly. As cyberattacks become more sophisticated, partnering with specialised cybersecurity providers will offer a scalable and flexible option for many organisations.

3.

The Expansion of Zero Trust Architecture

The concept of Zero Trust Architecture (ZTA), which operates on the principle of "never trust, always verify," will see widespread adoption. As cyber threats become more advanced, organisations can no longer rely on perimeter-based security. Instead, ZTA requires continuous verification of users, devices, and applications - whether they are inside or outside the network.

The expansion of ZTA will help mitigate risks such as insider threats, lateral movement within a compromised network, and unauthorised access. With more organisations shifting to cloud environments and remote work, implementing ZTA will be critical to maintaining robust security and limiting potential breaches.

4.

The Rise of Reverse Identity Theft

In 2025, a significant increase in reverse **identity theft** is expected - a phenomenon where stolen data accumulated over the years is incorrectly combined, resulting in "digital doppelgängers" that compromise a person's true identity. This issue may arise from database vulnerabilities, where the combination of common names or incorrect information leads to wrongful claims or even identity swapping, creating opportunities for fraud or unjust accusations.

With the growing volume of personal data exposed in multiple breaches, the improper merging of data will become an increasing concern. This type of reverse identity theft could have serious consequences, from credit issues and legal disputes to the creation of fake digital profiles used for malicious purposes. Prevention will require heightened vigilance over data integrity and the implementation of stringent measures to verify individuals' true identities.

5.

Human-Centered Cybersecurity

Human error continues to be one of the biggest cybersecurity risks, with phishing attacks and weak passwords accounting for a significant portion of these risks. Therefore, organisations will need to go beyond traditional training and adopt more integrative and contextual approaches, where security awareness is constantly reinforced through realistic simulations, micro-trainings, and content tailored to the specific behaviours and roles of each employee. This approach uses technologies like AI and behavioural analysis to identify potential risks, delivering the right content at the right time. Additionally, practices such as "gamification" encourage employees to actively and voluntarily adopt secure practices.

Another trend will be the development of a **cybersecurity culture**, where security becomes a shared organisational value and a responsibility for all, not just the IT department. This means adopting simple mechanisms, like the Alert Readiness Framework, where organisations define their own alert levels based on relevant information sources, assign weights to each, and calculate their current alert level. Here, leaders and managers will play a central role in reinforcing the importance of the topic and creating an environment where secure practices are constantly promoted and rewarded. In 2025, there will be a stronger focus on human-centred cybersecurity, emphasising training and awareness programmes to reduce these vulnerabilities.

devoteam
Cyber Trust

6.

Regulatory Changes and Compliance

With the rapid evolution of cybersecurity threats, regulatory frameworks are expected to become more stringent by 2025. Governments worldwide are introducing new regulations that require organisations to improve their security practices. In the European Union, NIS 2 and DORA are the standards that will create more work for institutions and businesses, requiring robust adaptation to ensure digital resilience, protection against cyber threats, and operational continuity. While NIS 2 imposes stringent cybersecurity and risk management requirements, including supply chain protection and incident response, DORA focuses on digital operational resilience, covering IT security, incident recovery, and continuous risk monitoring, including third-party risks. Together, these guidelines force organisations to strengthen their cyber defences, implement stricter governance practices, and prepare for rapid recovery in the event of attacks—all aimed at mitigating risks and ensuring the continuity of critical services in an increasingly complex and dynamic digital environment.

In addition to NIS 2 and DORA, the AI Act, approved in 2024, will also come into effect, establishing the European Union as the global benchmark for AI regulation.

7.

Proactive and Collaborative Third-Party Risk Management

The dominant trend for Third-Party Risk Management (TPRM) in 2025, in the context of NIS 2, will be continuous monitoring and automated risk assessment across the entire supply chain. With NIS 2 expanding the responsibility of organisations for the security of third parties, we will see greater adoption of artificial intelligence and machine learning tools to monitor the security posture of suppliers and partners in real-time. This will enable quick identification of vulnerabilities or irregular behaviours that may indicate risks.

Additionally, the market is expected to shift towards integrated TPRM platforms that centralise risk data and facilitate audits and compliance with NIS 2, enabling companies to demonstrate their commitment to cybersecurity across the entire chain more efficiently. The need for rapid incident response will encourage organisations to maintain agile and transparent communication channels with suppliers, as well as establish joint response protocols in the event of incidents. Therefore, in 2025, TPRM will be increasingly proactive and collaborative, based on automation and transparency to address the challenges imposed by NIS 2.

8.

Talent Retention and Recruitment Challenges

This will remain a key issue in 2025. Talent recruitment and retention in cybersecurity face significant challenges, driven by the **growing demand for skilled professionals and the rapid evolution of digital threats**. The speed with which new technologies and types of attacks emerge requires these professionals to remain constantly updated, making the market highly competitive and retention a challenge for organisations. Moreover, the shortage of cybersecurity talent means that the most qualified professionals are often highly sought after.

Another challenge is **the psychological toll of the field**, as cybersecurity specialists deal with high pressure to protect sensitive data and respond quickly to threats. This emotional strain can lead to burnout and staff turnover. To address these challenges, many organisations will continue to invest in continuous training, benefits that promote well-being, and flexible work environments, in addition to creating a culture of support and collaboration essential to retaining talent in the long term.

devoteam
Cyber Trust

9.

Improvement of Ransomware Defence and Recovery Strategies

Ransomware attacks continue to evolve, becoming more sophisticated and difficult to defend. Companies must focus both on preventing these attacks and on creating robust recovery strategies. Regular backups, segmented networks, and the use of Endpoint Detection and Response (EDR) solutions will be key components of strong ransomware defence.

As ransomware tactics become more aggressive, such as double extortion (demanding ransom for both decryption keys and non-disclosure of stolen data), companies will also need to invest in cybersecurity insurance and response plans to minimise operational disruptions.

In the last year, the cybersecurity landscape has revealed significant challenges, driven by the sophistication of artificial intelligence (AI)-based threats, the evolution of ransomware attacks, and the need to strengthen identity trust chains. **AI has democratised hacking**, allowing even less experienced attackers to create highly complex phishing and malware campaigns, challenging traditional detection systems. Furthermore, organised groups have been analysing network infrastructures in detail, exploiting vulnerabilities, and selling access to third parties in illegal markets, exposing organisations to a substantial increase in risks.

In 2024, identity trust chains became a critical target. **Conventional methods**, such as multi-factor authentication, **proved insufficient to mitigate advanced attacks** that exploit session tokens and API keys. These incidents highlight the urgent need to implement more robust security strategies, such as continuous checks, dynamic identity management, and a Zero Trust approach, capable of reducing the attack surface and enhancing resilience.

As 2025 approaches, **it is expected that threats will evolve rapidly in terms of sophistication**, with increasingly targeted, unpredictable, and difficult-to-mitigate attacks. Techniques such as advanced automation and malware randomisation will increase the complexity of attacks, while AI will allow cybercriminals to customise large-scale campaigns and exploit vulnerabilities in supply chains and interconnected systems.
To face this scenario, organisations must adopt practices such as threat-led penetration testing (TLPT) and Red Teaming, which simulate real-world scenarios, to identify and correct gaps before they are exploited.
These practices, complemented by regular audits, incident simulations, and advanced solutions like continuous authentication and behavioural monitoring, are essential to protect critical assets and enhance security teams' preparedness.

The real differentiator in 2025 will be readiness, specifically **cybersecurity readiness**, defined by an organisation's ability to anticipate, detect, and respond effectively to threats. This integrated approach, combining technology, processes, and people, will be crucial to strengthening resilience, ensuring operational continuity, and consolidating trust in an increasingly complex and challenging digital environment.

Bibliography

https://www.forrester.com/blogs/predictions-2025-cybersecurity-risk-privacy/

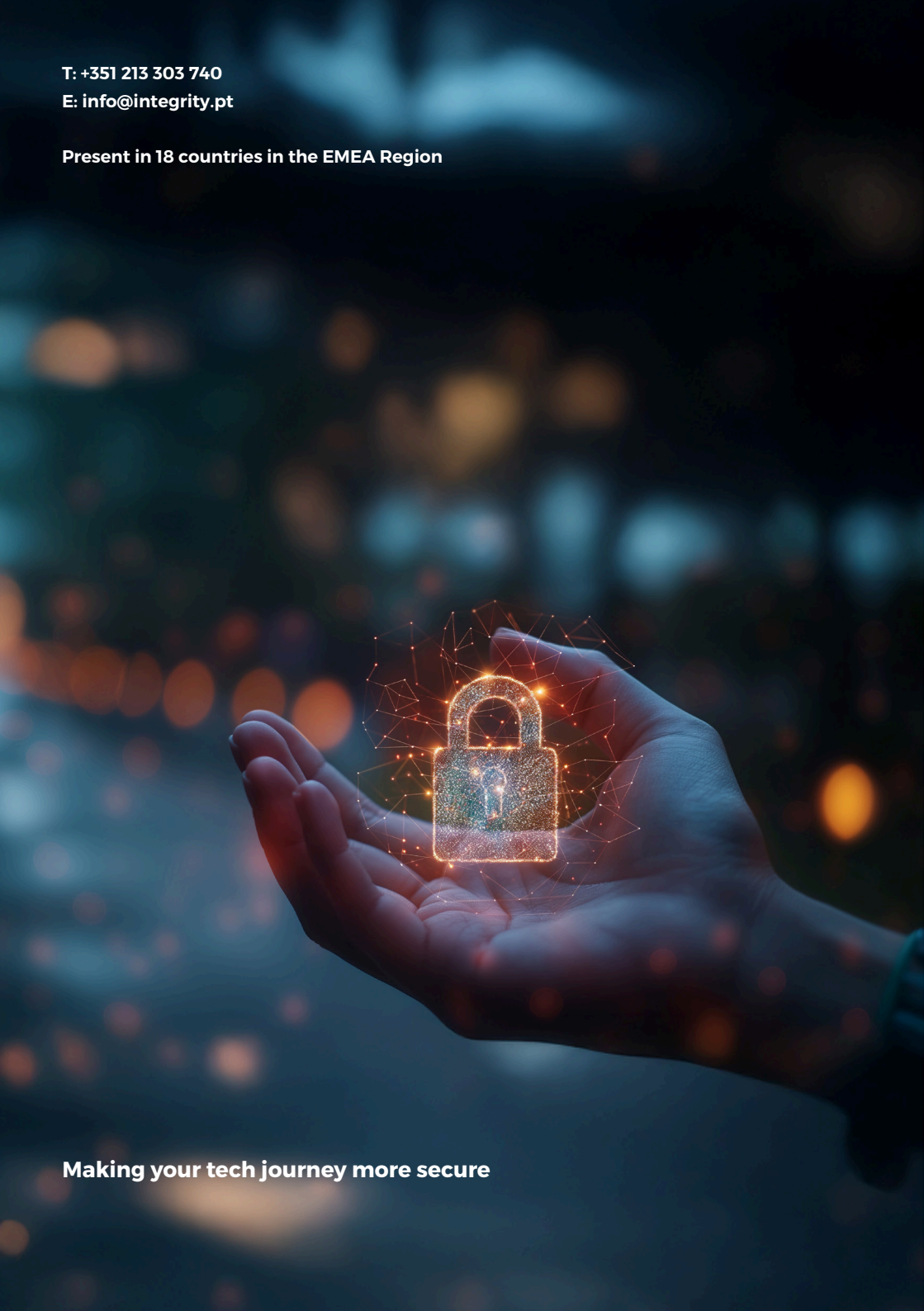
https://www.park.edu/blog/cybersecurity-trends-protecting-business-information-in-2025/

https://www.gartner.com/en/cybersecurity/topics/cybersecurity-trends

https://www.uscsinstitute.org/cybersecurity-insights/resources/top-cybersecurity-trends-to-watch-out-for-in-2025

T: +351 213 303 740
E: info@integrity.pt

Present in 18 countries in the EMEA Region



Making your tech journey more secure