IDC FutureScape

A Look Into Security 2025 FutureScape Predictions

An Exclusive Look Into Four Future Technology Trends CIOs Should Consider

Table of Contents

3 About FutureScape Predictions

4 Security Predictions Overview

5 Security Predictions 1 & 2

6 Security Predictions 4 & 7

7 Conclusion/More FutureScape Content

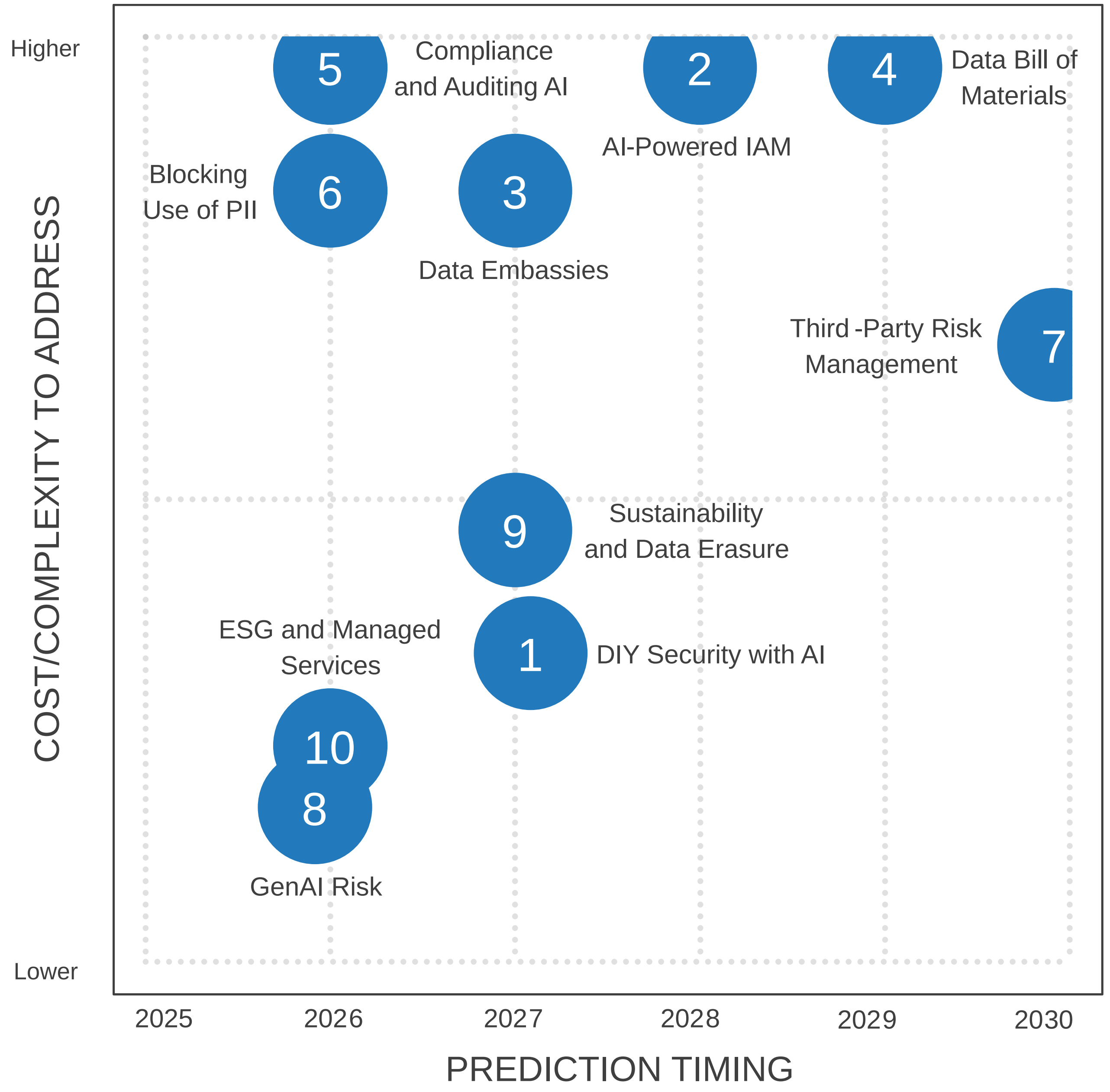
8 About IDC

About FutureScape Predictions

IDC FutureScape reports are used to shape enterprise IT strategy and planning by providing a basic framework for evaluating IT initiatives in terms of their value to business strategy now and in the foreseeable future.

IDC's FutureScapes are comprised of a set of predictions designed to identify a range of pending issues that CIOs and senior technology professionals will confront within the typical five-year business planning cycle. Each prediction is assessed on the basis of its complexity, organizational impact, and time frame to expected mainstream adoption.

IDC FutureScape: Worldwide Security 2025 Predictions



Note: Marker number refers only to the order the prediction appears in the report and does not indicate rank or importance, unless otherwise noted in the Executive Summary.

The FutureScape report delves into all 10 predictions outlined in the graphic above, but this eBook highlights four of these predictions.

FUTURESCAPE RESEARCH: [IDC FutureScape: Worldwide Security & Trust 2025 Predictions]

These predictions are the analysis of top trends shaping the future of security and trust across the globe as identified by nearly 40 IDC analysts. As organizations navigate rapid technological advancements, they also grapple with the dual challenges of harnessing the power of innovation while safeguarding data, improving privacy, and maintaining trust. These predictions highlight how organizations must navigate the complexities of emerging security threats, evolving regulatory landscapes, and growing consumer expectations around digital trust.

A core theme of these predictions is the role of artificial intelligence (AI) in reshaping the security landscape. AI will play a pivotal role in simplifying security processes and empower non-security professionals to implement protections. However, AI will not only bolster defenses; it will also fuel increasingly sophisticated cyberattacks. Companies must balance the benefits of AI-powered security tools with the risks of AI-enhanced threats, such as deepfake fraud, phishing, and autonomous malware.

In these predictions, we also address sustainable IT practices to limit the overall consumption of energy and technologies required by AI as well as ensure that data is securely erased from recycled or repurposed devices as organizations seek to limit the amount of e-waste produced.

PREDICTION 1

40% **By 2027, 40% of businesses will support DIY security for developers and line of business application owners, through AI-enabled automation of security policy generation from natural language commands.**

IT Impact

Automation is a necessary technological capability to address the concomitant risks of aggressive, rapid development practices. GenAI will provide the essential abstraction layer between users and security tooling.

Security processes often present a bottleneck in the application development process. AI assistance will bake the implementation of centrally managed security protocols into the DevOps process.

Enterprise IT organizations have invested in dozens of point products to address specialized threat vectors over the years.

Guidance

More security controls, implemented earlier and more often, will reduce security exposures significantly. The security improvements offered by a readily available, easily implemented security feature will prove to be enticing. The result will be a broad upleveling of the general security posture of IT environments and a reduction of business risk worldwide. With first generation capabilities introduced to market by 2025 and subsequent improvements rapidly taking hold, 2027 is marked as a pivotal year for the concept to achieve broad mainstream acceptance as a security best practice.

PREDICTION 2

35% **By 2027, only 35% of consumer-facing companies will use AI-powered IAM for personalized, secure user experience due to continued difficulties with process integration and cost concerns.**

IT Impact

AI-powered adaptive authentication enables IT teams to implement risk-based access controls that adjust in real-time based on user behavior, location, and device context.

Integrating AI-powered IAM solutions into legacy IT environments presents significant technical challenges. IT teams will require advanced expertise in cybersecurity, system architecture, AI/ML technologies, as well as threat modeling and AI modeling.

AI-powered IAM solutions require IT departments to handle and process vast amounts of sensitive personal data, including behavioral and contextual information.

Guidance

To navigate the complexities of AI-powered IAM adoption, organizations should begin by assessing their current IAM infrastructure to identify areas where AI can deliver value.

A well-planned integration strategy is essential to address the technical challenges and costs associated with incorporating AI-powered IAM into existing systems.

Compliance with emerging AI regulations is another critical consideration, particularly in heavily regulated regions.

Building consumer trust through transparent consent management practices is essential.

FUTURESCAPE RESEARCH: IDC FutureScape: Worldwide Security & Trust 2025 Predictions

PREDICTION 4

85% **By 2028, precipitated by AI BoM requirements, 85% of data products will include a Data BoM (Bill of Materials) detailing data collection, edits made, data cleanup, and how consent was obtained.**

IT Impact

Data BoMs will improve data transparency and inform users of how data has been changed, increasing confidence in data assets.

Effective data management can increase IT cost efficiency by identifying and eliminating duplicate datasets and underutilized data sets, in turn reducing data storage and processing spend.

Organizations who are able to implement data BoMs also support AI and ML projects through the data BoMs assurance that the correct data is available for the desired AI project and that the data is clean and ready for use.

Guidance

To implement data BoMs effectively, organizations should establish a centralized data management location or catalogue to keep data BoMs up-to-date and control and manage data assets, as well as a comprehensive data governance policy that clarifies ownership of data assets, data management approach, and purposes of data collection.

Data governance policies should also establish data quality metrics appropriate to the intent of the data. These include metrics for completeness, accuracy, timeliness, and information on how the data was collected and how consent was obtained.

PREDICTION 7

50% **By 2029, 50% of organizations will use external attack surface scan data to monitor their partner/suppliers in an effort to understand third-party risk.**

IT Impact

External scans will be another source of data about third parties interacting with an organization. There will need to be tools in place to ingest, monitor and query the data.

Organizations will need to consider the information flows that need to be in place throughout an organization because partner/supplier exposure data should not be limited to the security team.

Organizations will need to monitor themselves using ASM tools in order to understand their compliance with their own supplier agreements.

Guidance

Make use of the external scanning capabilities of attack surface management to see what an attacker sees; also, what any third-party can find out about your Internet exposed assets.

Use the same tooling to investigate your supply chain to understand if they have good proactive cybersecurity hygiene or if they leave Internet exposed assets misconfigured or unpatched for months on end.

FUTURESCAPE RESEARCH: IDC FutureScape: Worldwide Security & Trust 2025 Predictions

In Conclusion

While 2024 saw a surge in proof-of-concept (POC) projects for GenAI, many organizations are moving these projects into production without conducting comprehensive risk assessments. Companies may face significant vulnerabilities as they transition to GenAI use cases without fully evaluating their trust capabilities. This underscores the importance of a risk-based approach to AI adoption, ensuring that new technologies do not create unintended security gaps or ethical concerns. And as the world becomes more interconnected, the ability to secure data, maintain trust, and navigate the complexities of evolving technologies will be paramount for success.

This eBook was written from research and findings from the IDC research report, *IDC FutureScape: Worldwide Security & Trust 2025 Predictions*. **To learn more about predictions that technology leaders need to consider related to data privacy with ESG efforts, AI audits, privacy regulations and data transparency and governance - the full FutureScape research report explores these key topics and provides strategic guidance.**

IDC clients have access to this FutureScape research report, along with unlimited access to all IDC research produced. If you're interested in subscribing to IDC's research, click the button below.

Contact Us

INTERESTED IN MORE FUTURESCAPE CONTENT?

Unbeatable Webinar Sessions

Join us for live and on-demand sessions as we discuss what it takes to be an AI-fueled business. Hear from our analysts on predictions for AI, CIOs, Digital Business, and the IT Industry.

Unlock More IDC FutureScape Predictions eBooks

Get a sneak peak into upcoming trends and disruptions that technology leaders must prepare for with more IDC FutureScape eBooks. Understand how this year's predictions could shape your organization's strategic planning for the coming years.

Want to learn more about the IDC FutureScape predictions? Click here.

About Us

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,300 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 60 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

140 Kendrick Street
Building B
Needham, MA 02494
USA
508.872.8200

Copyright Notice