iProov

The GOOD, the BAD, and the UGLY

A global study on the threat of AI and deepfakes

Contents

1. Executive Summary

In our increasingly interconnected digital world, where interactions span across borders and occur at lightning speed, the ability to trust the identity of individuals within digital ecosystems is paramount. Whether it's employees accessing sensitive company data, customers making online transactions, or citizens interacting with government services, the consequences of misplaced trust can be devastating. Deepfakes and other AI-powered deceptions have amplified the risks, making it imperative for organizations and individuals alike to adopt robust identity verification solutions to safeguard their digital interactions and maintain the integrity of their digital ecosystems.

In the Spring of 2024, iProov, in collaboration with an independent third-party research provider, Hanover Research, conducted a study to assess the understanding of the cybersecurity community's understanding of the deepfake threat, both its current impact and future implications, as well as their level of preparedness and adoption of security measures, particularly biometric solutions, to mitigate these risks.

The results of the global survey paint a clear picture of the escalating threat of deepfakes and the rising importance of facial biometric security in response. This global survey of technology decision-makers across various industries reveals a widespread recognition of the potential damage caused by deepfakes.70% believe AI-generated attacks will significantly impact their organizations while a majority also acknowledge the crucial role AI plays in defending against such attacks.Despite this awareness, a concerning gap exists between recognition and action. While 73% of organizations are actively implementing cybersecurity solutions to address deepfakes, more than two-thirds (62%) express worry that their organizations aren't taking the threat seriously enough. This disconnect highlights the need for more proactive and robust measures to mitigate the risks posed by this rapidly evolving technology.

The survey findings underscore several key trends:

- **Deepfakes are a Top-Tier Security Concern:** Deepfakes are now tied with phishing/social engineering attacks as the third most prevalent security concern, after password breaches and ransomware. This highlights their increasing prominence in the threat landscape and the urgency for effective countermeasures.

- **Facial Biometrics are the Primary Defense:** A resounding 75% of organizations are turning to facial biometric solutions as their primary defense against deepfakes. This reflects a growing recognition of facial biometrics' ability to provide more secure and reliable identity verification compared to traditional methods like passwords or knowledge-based authentication.

- **Demand for Comprehensive Biometric Solutions:** Nearly all respondents (94%) believe that a biometric security partner should offer more than just software. There's a clear demand for comprehensive solutions that include continuous monitoring, multi-modal biometrics, and advanced liveness detection to ensure the authenticity of the person being verified.

- **Regional Nuances:** While the threat of deepfakes is global, there are regional differences in perception and preparedness. For example, APAC, European, and LATAM organizations are more likely than North American organizations to have encountered deepfakes.

Overall, the survey results underscore the urgency for organizations to adopt robust biometric security measures to safeguard against the escalating threat of deepfakes. With deepfakes becoming increasingly sophisticated and accessible, the need for solutions that can accurately distinguish between genuine individuals and malicious actors has never been greater. Biometrics, with its ability to leverage unique biological traits for identification, offers a promising path forward in this evolving security landscape.

2. Report Overview

This report was designed to get a global perspective on the following themes related to use of generative AI and biometrics in organizations:

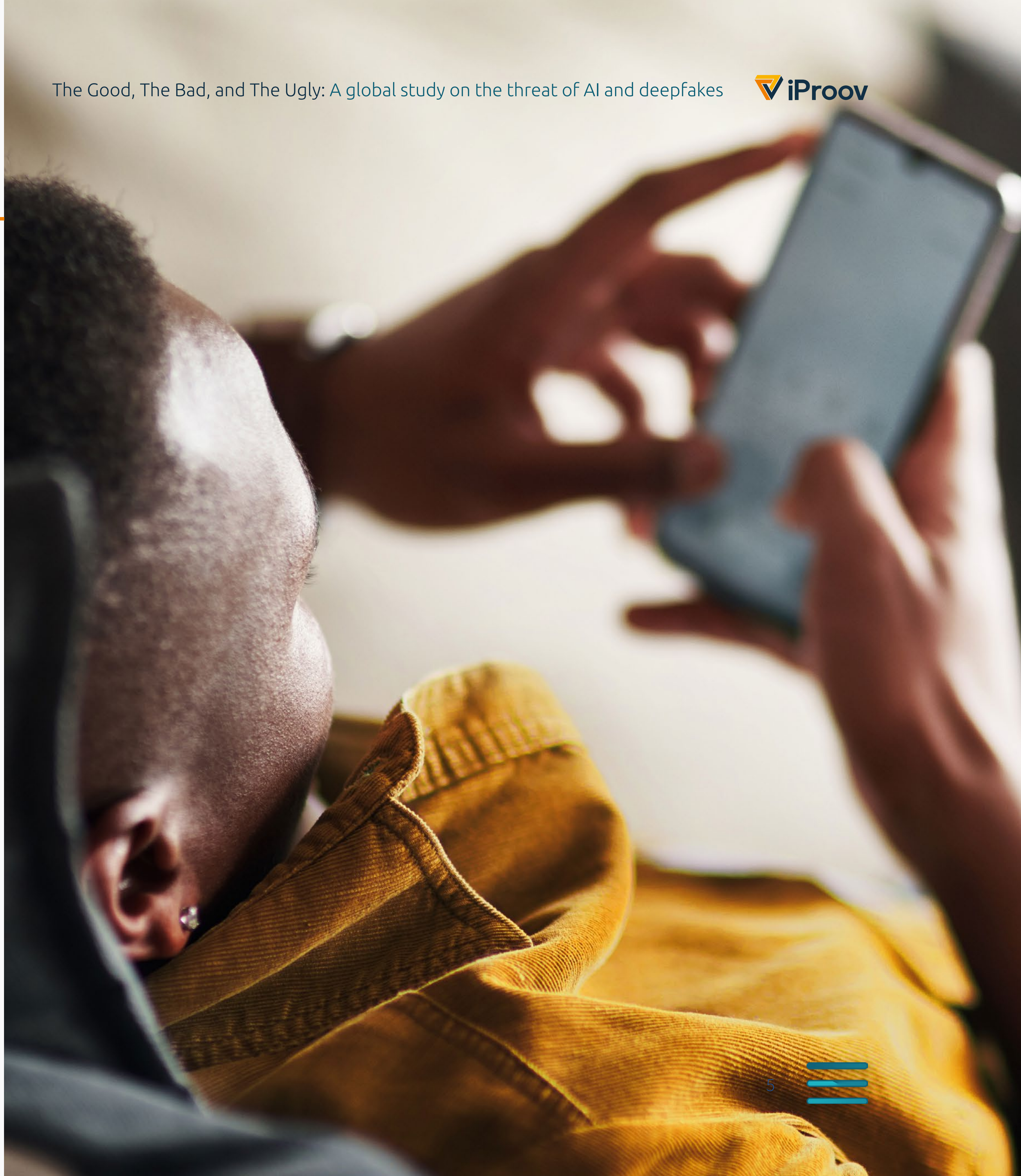
- Concern with generative AI/machine learning-enabled threats
- Methods and technologies leveraged by organizations to address the threat of deepfakes, specifically the role of science-powered biometrics
- The types of biometrics organizations are using and which they believe are "best fit" for various tasks for combatting deepfakes
- What organizations look for in a biometrics solution partner

Who Is This Report For?

This report is designed to be a resource for those tasked with decision-making for their organization's cybersecurity solutions.

When you explore the data in this report, you will see clear patterns emerge that highlight areas where cybersecurity leaders can take action.

iProov's goal is to help organizations enhance online security, safeguard user privacy, and simplify the onboarding and sign-in process for organizations worldwide through face biometric verification and authentication technologies.



3. Survey Findings

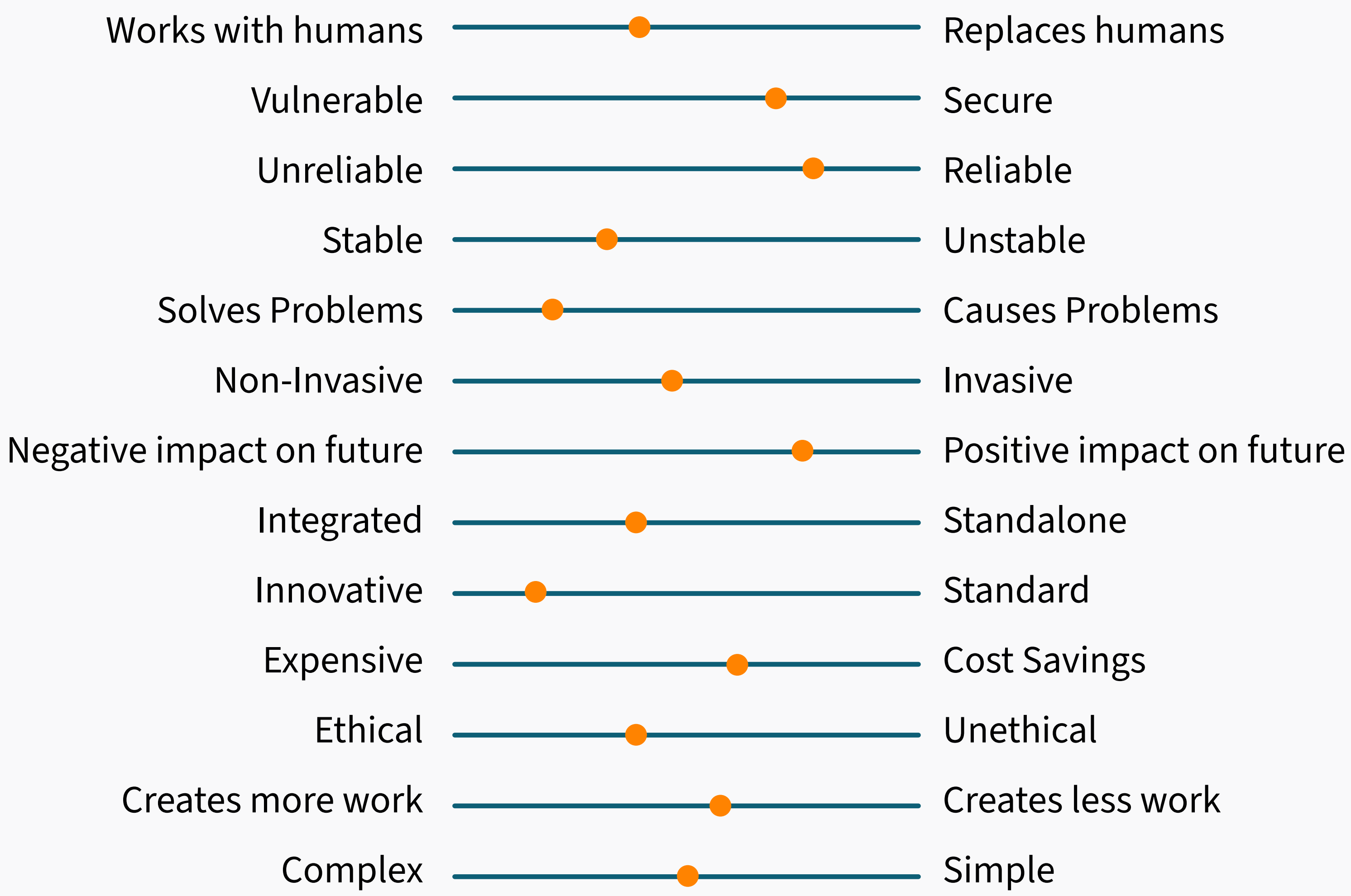
1. Generative AI and Machine Learning Evaluation

Perception of Generative AI and Machine Learning

As use of generative AI grows in business today, organizations tend to view it favorably. Generative AI is seen as a secure, reliable, stable, and innovative solution. Furthermore, generative AI works with humans to provide cost savings and solve problems, having a positive impact on the future. Organizations tend to be more split on the ethicality, invasiveness, and amount of work created. Generative AI and machine learning is double-edged, as it is both impactful in protecting against cybersecurity threats (84%) and creating threats (68%).

LATAM organizations are significantly less likely than other regions to believe generative AI and machine learning are impactful at creating cybersecurity threats (54%) and significantly more likely to say they are impactful at protecting against threats (94%).

Generative AI Attributes



Q: Do you believe the attribute on the right or left better describes generative AI? (n=500)

Impact of Generative AI/Machine Learning [Top 2]

Protecting against cybersecurity threats	84%
Creating cybersecurity threats	68%

Q: What impact do you believe generative AI and machine learning have in the following situations? (n=500)

As with any new solution, organizations have a variety of concerns with implementing generative AI. Their main concerns are vulnerabilities due to an over-reliance on generative AI (50%), misuse (50%), lack of transparency on how it is using data/ making decisions (49%), and data privacy (48%).

Concerns with Implementation of Generative AI

Over-reliance on generative AI leading to vulnerabilities	50%
Misuse (e.g., deepfakes, phishing emails)	50%
Lack of transparency on how generative AI is using data/making decisions	49%
Data privacy	48%
Compliance with regulations and standards	42%
Data breaches due to large amount of data in training sets	38%
Adversarial attacks	37%
Lack of traceability	33%
Would not have any concerns	4%

Q: What concerns would you have with the implementation of generative AI in your organization? Select all that apply. (n=500)

Cybersecurity Outcomes due to Generative AI

Increased use of generative AI and its related risks have led organizations to revise their cybersecurity programs. Two-thirds of organizations have either slightly (42%) or significantly (26%) revised their programs to include risk considerations introduced by generative AI. Furthermore, this trend will continue as one-third (30%) say they have not yet revised, but plan to in the near future. The risks created by generative AI have also prompted most organizations (83%) to increase their investment in/budget for cybersecurity programs. Additionally, most have implemented either strict (45%) or light (43%) policies on the use of these new tools.

LATAM organizations (88%) are significantly more likely to say they have revised their cybersecurity program to address generative AI risks, while European organizations are significantly more likely to have not revised yet, but plan to (39%). Notably, LATAM organizations (21%) are significantly more likely than other regions to say they do not have any policies on how generative AI tools can be used.

Impact of Generative AI/Machine Learning [Top 2 = 83%]

Slightly increased	62%
Significantly increased	21%

Q: How has your organization's investment in/budget for cybersecurity programs changed due to generative AI? (n=500)

2. Cybersecurity Implications

Threats to Cybersecurity

With the emergence of new technologies, organizations face many threats to their cybersecurity. They are most concerned with password breaches (64%), ransomware (63%), phishing/social engineering attacks (61%), and deepfakes (61%).

Concern About Deepfakes [Top 2 = 61%]

Very concerned	33%
Extremely concerned	28%

Q: How concerned are you about the following threats to your organization's cybersecurity - Deepfakes? (n=500)

Deepfake technology is defined as the use of tools, such as generative AI and machine learning, to alter the appearance and behavior of someone or generate highly realistic synthetic content to imitate human behaviors. When used maliciously, this technology can be employed to create counterfeit identities, imitate people, and gain access to secure locations. Notably, half of organizations (47%) say they have encountered a deepfake, while half (50%) have not. Although not all organizations have encountered one up to this point, nearly three-quarters (70%) believe deepfake attacks will have a high impact on their organization.

APAC (51%), European (53%), and LATAM (53%) organizations are significantly more likely than North American (34%) organizations to say they have encountered a deepfake. APAC (81%), European (72%), and North American (71%) organizations are significantly more likely than LATAM (54%) to believe deepfake attacks will have an impact on their organization.

Impact of Deepfake Attacks [Top 2 = 70%]

Moderate impact	45%
Major impact	25%

Q: How concerned are you about the following threats to your organization's cybersecurity - Deepfakes? (n=500)

With the looming presence of deepfakes, two-thirds (62%) are worried that their organization isn't taking the threat seriously enough. Regarding the use of deepfakes to commit fraud, organizations are most concerned about synthetic identities (69%), believable deepfake images/videos (64%), face swaps (62%), and voice deepfake (54%).

Organization is Not Taking Deepfakes Seriously [Top 2 = 62%]

Somewhat agree	43%
Strongly agree	19%

Q: Please indicate how much you agree or disagree with the following statement: "I am worried my organization isn't taking the threat of deepfakes seriously enough."? (n=500)

The use of deepfakes to commit identity fraud has great potential to harm an organization – they worry most about the loss of sensitive data (64%), reputation damage (61%), and financial penalties/losses (60%). Organizations believe their financial systems (59%) and IT systems (57%) are most at risk from a deepfake attack.

APAC (52%) and North American (51%) organizations are significantly more likely than LATAM organizations (37%) to say they are concerned about legal and regulatory penalties from a deepfake attack.

Consequences of Deepfakes Used for Identity Fraud

Loss of sensitive data	64%
Reputation damage	61%
Financial penalties/losses	60%
Disruption of operations	48%
Customer retention issues	47%
Legal and regulatory penalties	47%
I do not believe there would be any consequences	3%

Q: Which of the following consequences are you most worried about for your organization from the use of deepfakes to commit identity fraud? Select all that apply. (n=500)

Cybersecurity Measures

The threat of deepfakes has prompted organizations to take protective measures. **Three-quarters of organizations (73%) are implementing cybersecurity solutions/ tools to address the threat of deepfakes, most commonly biometric solutions (75%),** multifactor authentication (69%), and device-based biometrics (67%). Organizations are also educating employees on how to spot a deepfake and potential risks (63%), conducting regular audits on security measures (57%), and regularly updating systems (54%) in order to address the threats posed by deepfakes.

Solutions/Tools Used to Address Threat of Deepfakes

Biometric solution	**75%**
Multifactor authentication	**69%**
Device-based biometrics	**67%**
Deepfake detection algorithms	**47%**
Video Identification	**37%**
Digital watermarking	**33%**
Blockchain	**30%**

Q: What solutions/tools is your organization using to address the threat of deepfakes? Select all that apply. (n=366)

3. Use of Biometrics to Combat Deepfakes

Experience with Biometrics

Organizations are familiar with and utilize various forms of biometric solutions. Biometric solutions use personal characteristics (directly linked to who you are) to authenticate or identify a person. A system collects voluntarily submitted biometric characteristics unique to every person and uses these biometric characteristics to verify or identify the individual to grant access to goods or services. Organizations are most likely to currently be using fingerprint (71%) and facial (63%) biometrics. When it comes to combating deepfakes, organizations believe fingerprint (81%), iris (68%), facial (67%), and advanced behavioral (65%) are the most effective types.

Biometrics Effectiveness at Combating Deepfakes [Top 2]

Fingerprint	**81%**
Iris	**68%**
Facial	**67%**
Advanced Behavioral	**65%**
Palm	**63%**
Basic Behavioral	**50%**
Voice	**48%**

Q: How effective do you think the following types of biometrics are at combating deepfakes? (n=500)

Facial biometrics tend to be preferred to combat deepfakes for various tasks. Organizations consider facial to be the most appropriate additional mode of authentication to protect against deepfakes for account access/log-in (34%), personal details account changes (33%), and typical transactions (32%). For major/atypical transactions, iris (24%), facial (23%), and advanced behavioral (23%) are seen as most appropriate.

Biometric Solutions Partners

In order to provide value to an organization, biometric solutions partners need to offer more than just a product. **Nearly all (94%) agree a biometric security partner should be more than just a software product, they need to provide an evolving service.** It is important that biometric solutions incorporate continuous monitoring (80%), multi-modal biometrics (79%), and liveness detection (77%) to protect biometrics against deepfakes.

APAC (98%), European (96%), and LATAM (99%) organizations are significantly more likely than North America (88%) to say that a partner needs to be more than just a product and provide an evolving service.

Biometrics Partner Must Provide Evolving Service [Top 2 = 94%]

Somewhat agree	35%
Strongly agree	59%

Q: Please indicate how much you agree or disagree with the following statement: “A biometric cybersecurity partner should be more than just a software product, they need to provide an evolving service.”? (n=500)

4. Conclusion

Moving Forward

The rapid advancement of technologies, such as generative AI and machine learning, harbor the potential to introduce new vulnerabilities and risks, particularly in the form of sophisticated deepfakes. However, they also offer powerful new tools to enhance cybersecurity defenses. The results compiled in this report highlight the critical threat posed by AI-generated deepfakes, stressing the need for organizations to evolve their cybersecurity strategies proactively.

The adoption of biometric solutions stands out as an effective strategy for combating the risks associated with deepfakes. As evidenced by the practices of numerous organizations, various forms of biometrics have proven to be assets in protecting against these cyber threats. Moving forward, it is crucial for organizations to not only recognize the evolving landscape of cybersecurity threats but also to take action in updating and enhancing their cybersecurity programs.

iProov is a global technology provider and leader in delivering liveness solutions to organizations around the world via its face biometric verification and authentication technologies. iProov liveness technology is the only way to verify that an online user is the right person, a real person, and, critically, that they are authenticating right now – not an imposter or a criminal gang or a machine-driven cyber-attack. iProov enables organizations to maximize online security while protecting user privacy and making the onboarding and sign-in experience as simple as possible.

Speak to an Expert

To learn more about how biometric authentication can benefit your organization, contact us for a personalized consultation. We'll discuss your specific needs, recommend the most suitable biometric solutions, and outline a tailored implementation plan.

Embrace the future of identity verification with biometrics. Contact us today to get started.

5. Survey Methodology

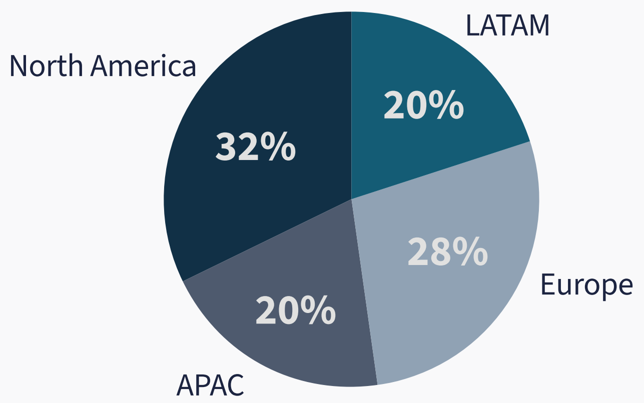
The Threat of Generative AI and Deepfakes survey on which this report is based was developed in coordination with Hanover Research.

To find the answers to these questions, potential respondents were recruited via a third-party panel and the survey was administered online in spring 2024. Following data cleaning and quality control, the final analysis included 500 respondents. Respondents were recruited globally and worked across many industries including Banking, eCommerce, Finance and Accounting, Healthcare/Medical, Hospitality, Insurance, Retail, Telecommunications, and Travel.

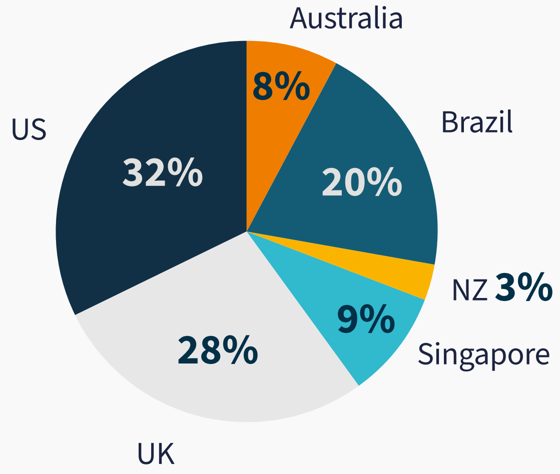
Respondent Screening Criteria

- Aged 25 years or older
- Employed full-time as a manager or higher in the United States, Brazil, United Kingdom, Australia, New Zealand, or Singapore
- Working in the Financial Services, Retail, Telecommunications, Travel, Hospitality, or Healthcare industry
- Working in IT, Operations, Network Security, Cybersecurity, Digital Experience, Risk Management, or Product Management department
- Must be the primary decision-maker or share authority in the selection and purchase of cybersecurity solutions for their organization
- Must be at least moderately familiar with biometric solutions

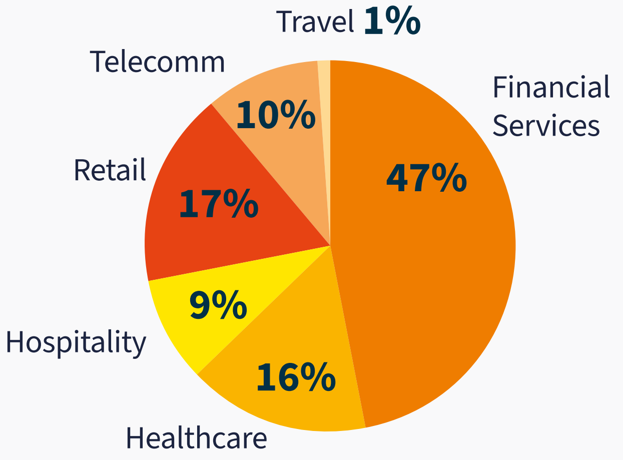
Region (n=500)



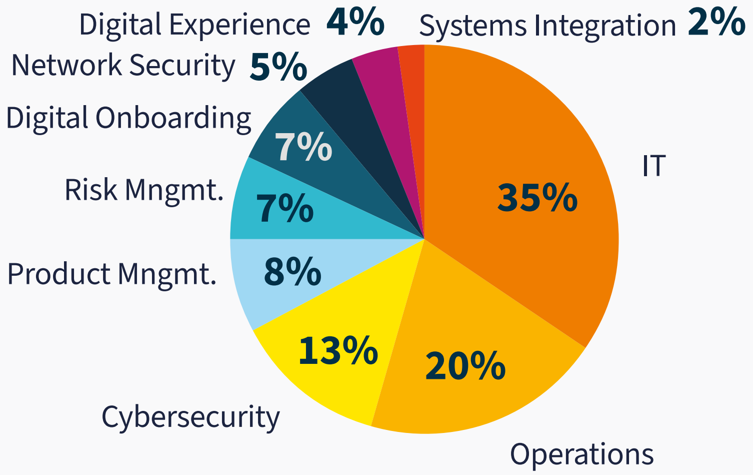
Country (n=500)



Industry (n=500)



Job Function (n=500)


Digital Experience 4%
Systems Integration 2%
Network Security 5%
IT 35%
Operations 20%
Cybersecurity 13%
Product Mngmt. 8%
Risk Mngmt. 7%
Digital Onboarding 7%