2025 KPMG Cybersecurity Survey

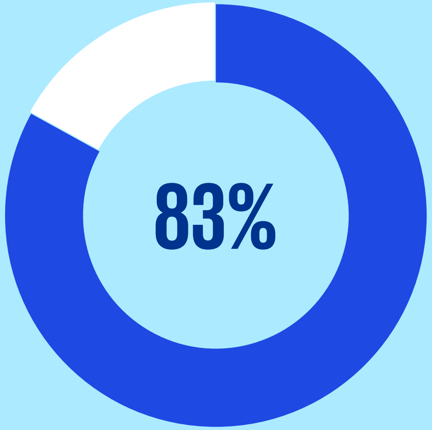
Security leaders' perspective

—

December 2025

Over the last 12 months, these are the top cybersecurity challenges...

The vast majority of security leaders witnessed a surge in cyberattacks



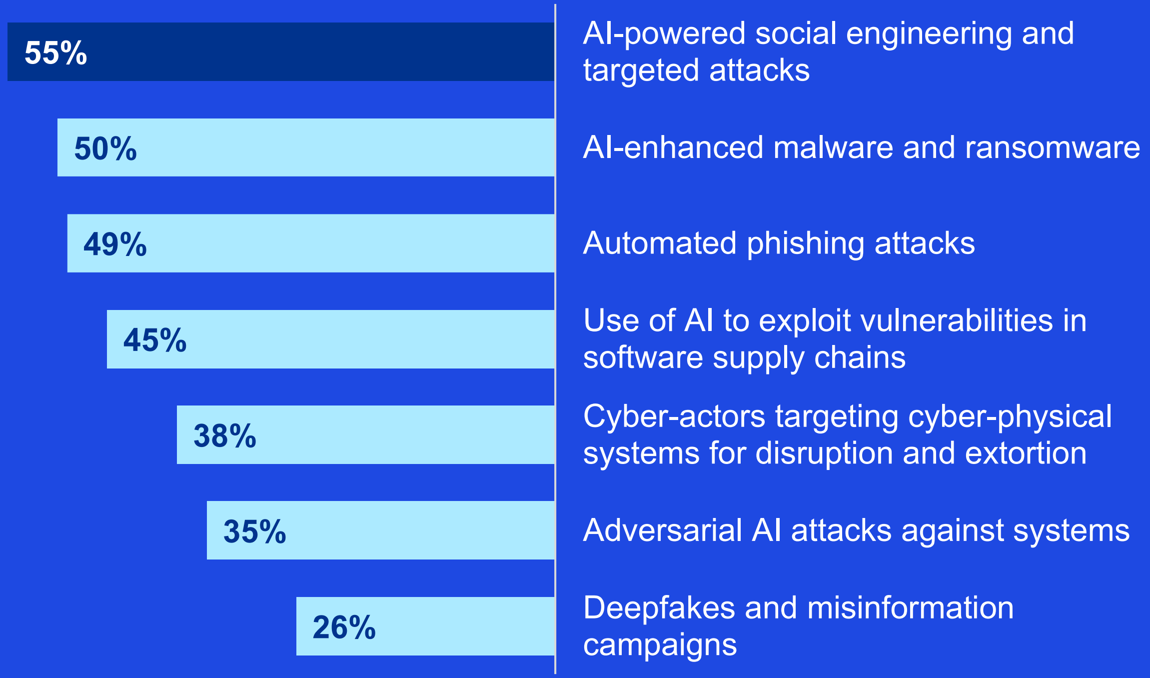
of security leaders reported a rise in cyberattacks in the last 12 months.

Phishing and DDoS attacks were the most frequent types of breaches.

Type of attack(s) (Among those who experienced an attack)	
51%	Phishing attack
49%	Denial-of-Service, Distributed Denial-of-Service
39%	Ransomware attack
33%	Malware attack
21%	Insider threats/users breaking security procedures
21%	Internet of things attack
21%	Password attack

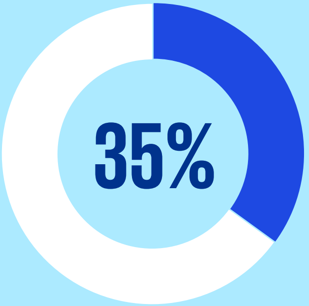
What's hindering cybersecurity? (Hint: It might be AI)

AI-driven threats, especially those involving social engineering, are top of mind.

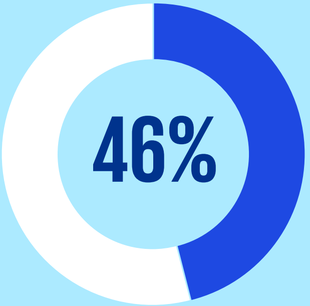


54% are also concerned about the malicious use of AI tools **by insiders**

Yet, leaders feel ill-equipped to mitigate these threats.



rated their defenses as highly effective in mitigating AI-powered social engineering attacks

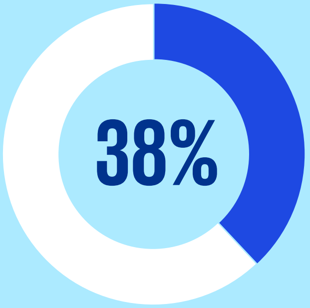


rated their defenses as highly effective in mitigating AI-enhanced malware and ransomware

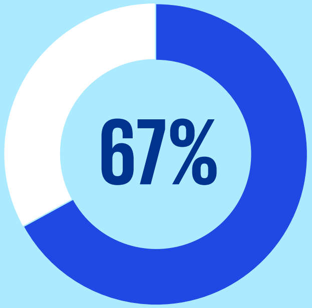
Oddly enough, AI is the top cyber threat and the best line of defense

AI-powered attacks are expected to become the top threat category

AI-powered attacks will be a major challenge within the next 2–3 years:



Of all security leaders expect AI-powered attacks to be a major challenge in the next 2–3 years



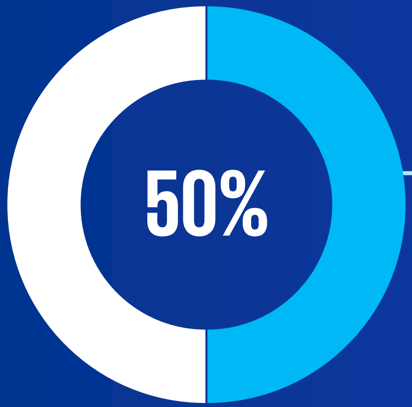
This concern is much higher among security leaders that **feel less prepared to handle cyber threats**

70% currently dedicate more than 10% of their budget to AI-related cybersecurity initiatives

AI is also seen as key to building a stronger cyber defense.

AI will have the greatest impact in proactively identifying and stopping threats, especially in:

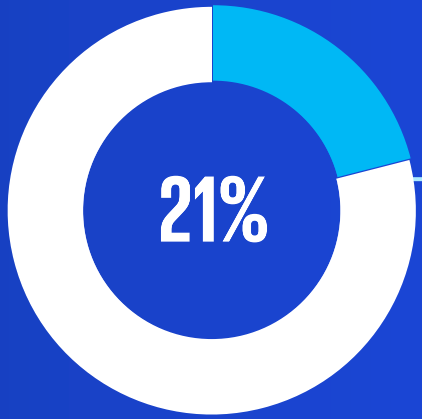
IoT threats are right behind AI as a top threat category. 1 in 5 of organizations have already experienced and IoT attack this year.



Of leaders view IoT as a significant threat to their organizations

Private and **medium-sized** companies see it as having higher threat potential

58% Private vs. 29% Public
59% Medium vs. 43% Large



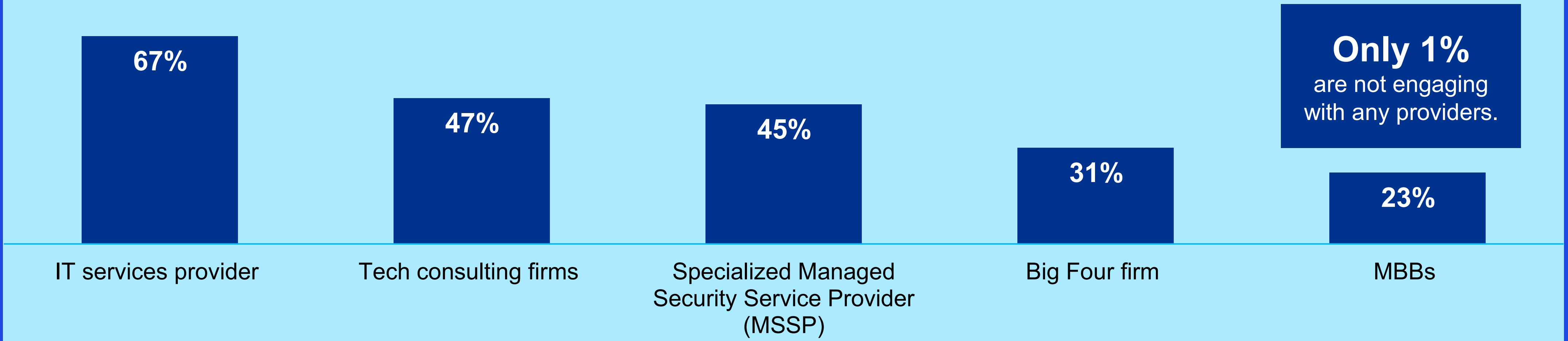
Of organizations experiences an IoT breach in the last 12 months

These attacks are more common among **private** and **medium-sized** companies

26% Private vs. 9% Public
29% Medium vs. 15% Large

To tackle AI and IoT issues, leaders are ramping up cybersecurity partners

Leaders are looking to partners for expertise, specialty offerings and acceleration



The Primary Reasons for Engaging with Cybersecurity Partners…

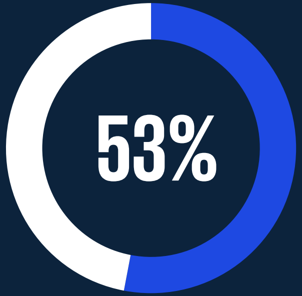
41%
Enhance cybersecurity expertise and capabilities

42%
Provide specialized security services

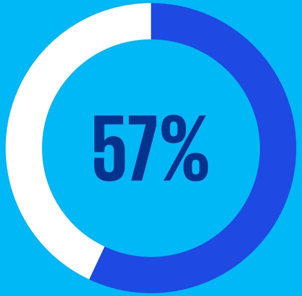
36%
Accelerate the implementation of new security technologies

To tackle AI and IoT issues, leaders are ramping up cybersecurity partners

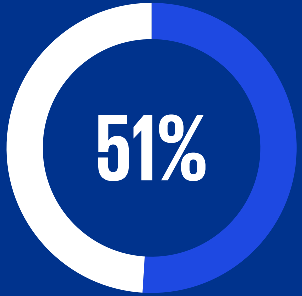
It is a big concern and a top area for investment now and in the future.



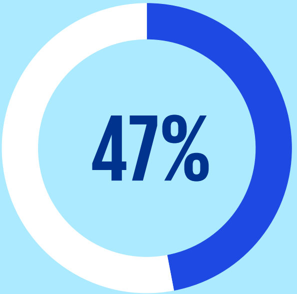
An accidental data breach is most concerning, internal, human centric threat
(right behind malicious use of AI tools – 56%)



It is the biggest obstacle for leaders when promoting responsible use of AI tools
(ahead of limited expertise & training – 47%)



It has been a top priority area for cybersecurity investment over the past 12 months
(ahead cloud security – 40%)



It is expected to get the biggest increase in cybersecurity investment over the next year 2-3 years
(just ahead of cloud security – 45%)

To combat non-human identities (e.g., bots), leaders are investing in Identity & Access Management (IAM)

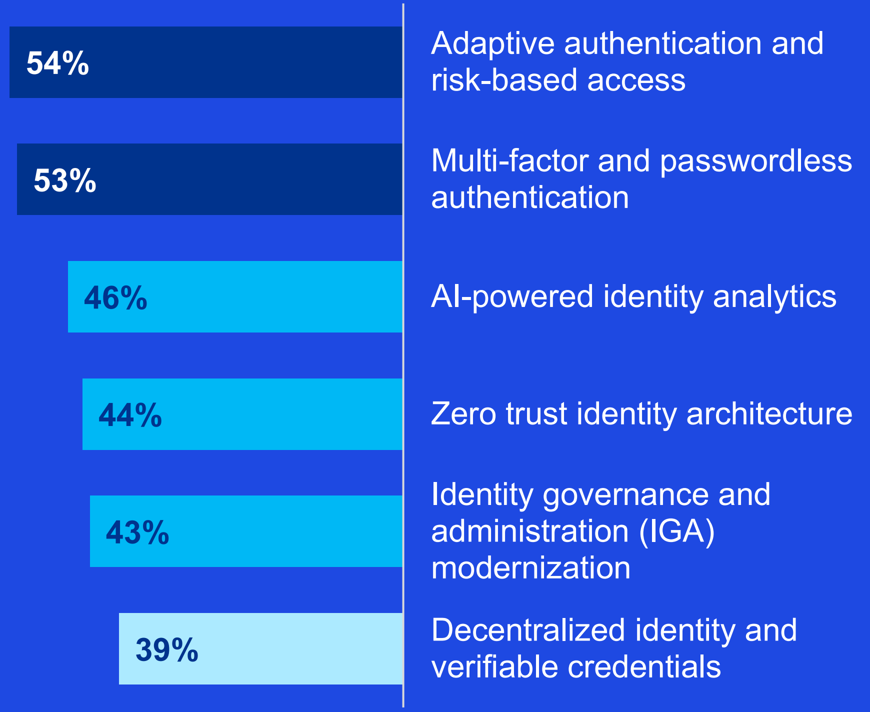
Many leaders say that non-human identities are also taking over digital workspaces

60% Of leaders say they have experienced a **very or extremely significant proliferation of non-human identities**

With this proliferation, it's not surprising that…

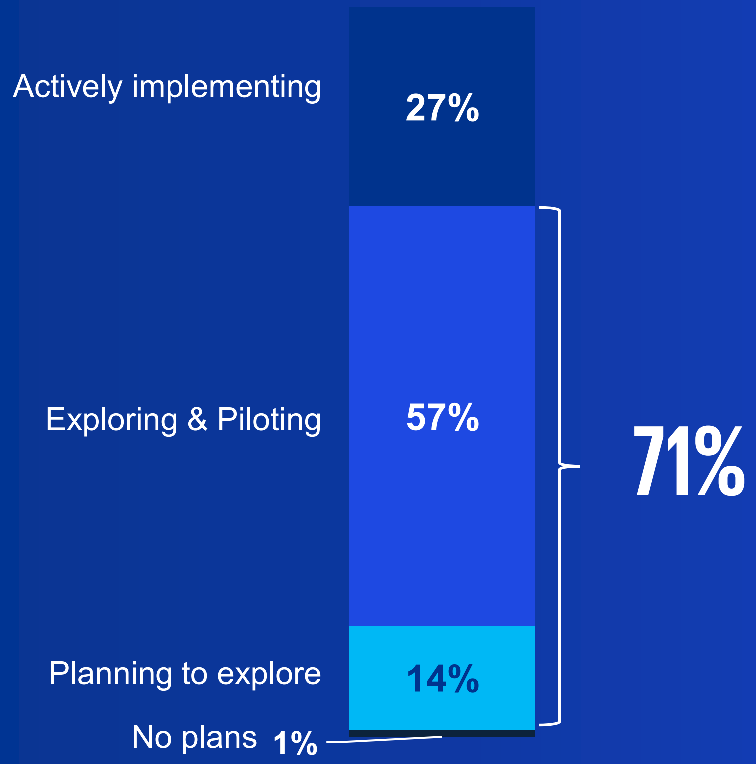
42% Of leaders are making **IAM a top budget priority in the next 2-3 years**
(right behind other top priorities of data security & privacy and cloud security)

Identity and Access Management (IAM) and digital identity investment will focus on….

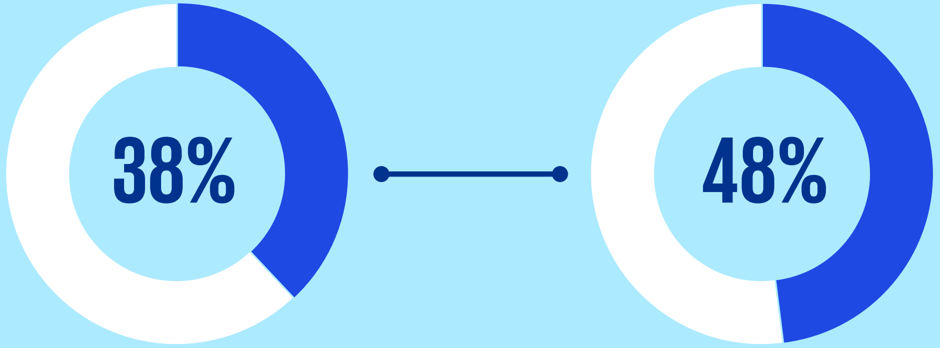


The future for cybersecurity? Defending against quantum computing threats

Most organizations (71%) are still in the exploratory stages of preparing for the quantum threat.



4 in 10 (38%) organizations view quantum computing as a high impact threat, half feel ready to address it.



Quantum computing as a high impact threat

Feel prepared to address quantum computing threat to cryptographic systems

Organizations with higher cybersecurity maturity feel more prepared

29% Less mature

65% Higher maturity

As such, leaders are ramping up cybersecurity hires.

Finding qualified security and risk team professionals is one of the top challenges for leaders.

52%

of leaders rate the lack of qualified professionals as a high-impact challenge

The biggest factors hindering optimal staffing are…

53% high cost of attracting/retaining qualified candidates

48% difficulty attracting qualified candidates in competitive market

Despite these difficulties, most organizations plan to increase their headcount.

% Change in security & risk team headcount over next 2-3 years

More than 20%	11% to 20%	1% to 10%	0%
19%	55%	25%	2%

To address these hiring challenges…

49% investing in training & upskilling existing employees

49% increasing compensation & benefits to attract and retain talent

25% leaning on partners to supplement their internal staff & fill talent gaps

Organizations are also turning to Managed Services to potentially fill talent gaps and strengthen their cyber defenses.

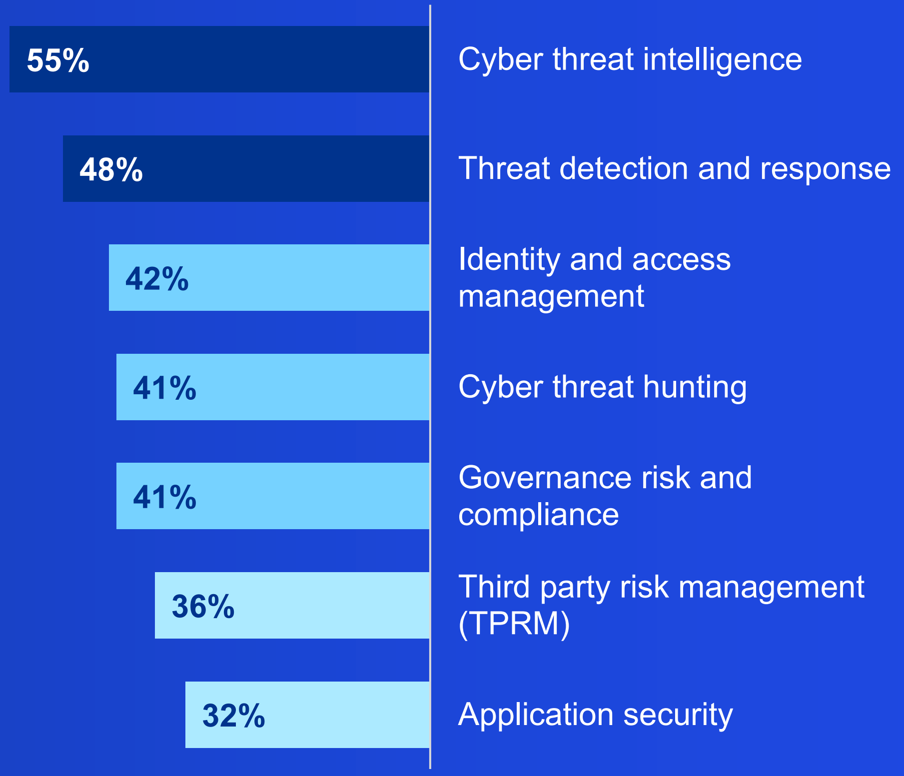
Nearly half of all organizations relied on Specialized Managed Security Services Providers (MSSPs)

45% Engaged with MSPs in the past 12 months

The primary motivation for engaging MSPs…

45%	42%	41%
Scalability, flexibility, and integration with existing infrastructure	Expertise & experience in cybersecurity	Proactive security measures & vulnerability management

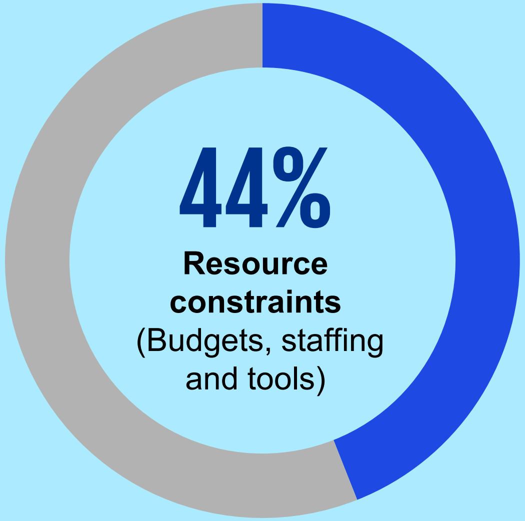
Most often for cyber threat intelligence & threat detection and response



What we're seeing in cyber spending's surge signals strong growth ahead

Resource constraints is one of the biggest barriers to remediating threats and vulnerabilities.

What are the biggest barriers to remediating threats and vulnerabilities …



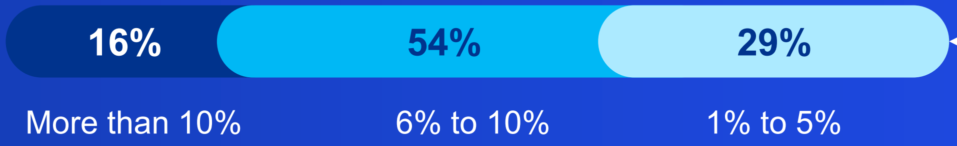
Budgets are growing steadily and are expected to continue growing over the next 2-3 years.

98%
have **increased their cybersecurity budget** in the past 12 months

99%
anticipate an increase in cybersecurity budget over the next 2-3 years

Most anticipate a 6% to 10% increase. Priorities include data security & privacy, IAM and cloud security

% Anticipated Budget Change Over the next 2-3 yrs



Objectives & Methodology

Objectives

To understand security leaders' perspectives on:

- Risk preparedness
- Evolving threat landscape (internal and external)
- Big challenges to effective threat and vulnerability management
- Risk mitigation approaches and strategies
- Future outlook
- Budget priorities
- Security partner engagement.

Survey Methodology

- **A 15-minute, online survey** among **c-suite and senior security leaders** in the U.S. fielded from September 25 to October 9, 2025.
- The sample includes **310 'security leaders'** meeting the following criteria:

Role in **Cybersecurity/Security, Risk, and Technology**
Job title: **Chief Information Security Officer (CISO), Chief Security Officer, and Chief Risk Officer (CRO), Chief Technology Risk Office (CTRO)**. See appendix for full list of titles.
Large enterprise with **at least $1B in revenue** from **public and private companies**
Organizations from a mix of industries

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**