IDC Directions

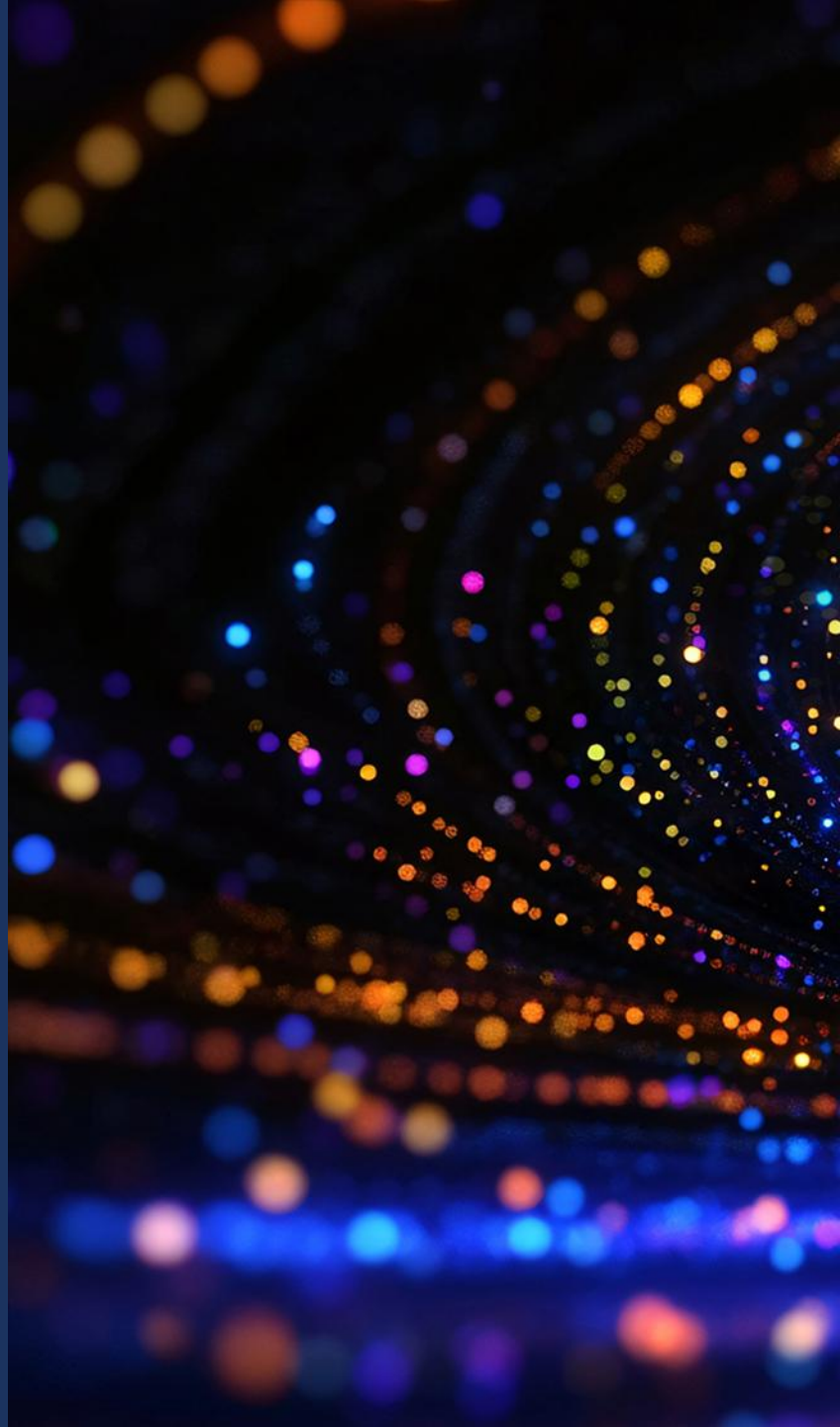
AI Security: protecting the new frontier

Frank Dickson
Group Vice President,
Security & Trust

Why are we here?

Artificial Intelligence offers the potential to deliver remarkable productivity benefits.

Those benefits come with risk;
we want to mitigate the risk.




Let’s talk about risk?

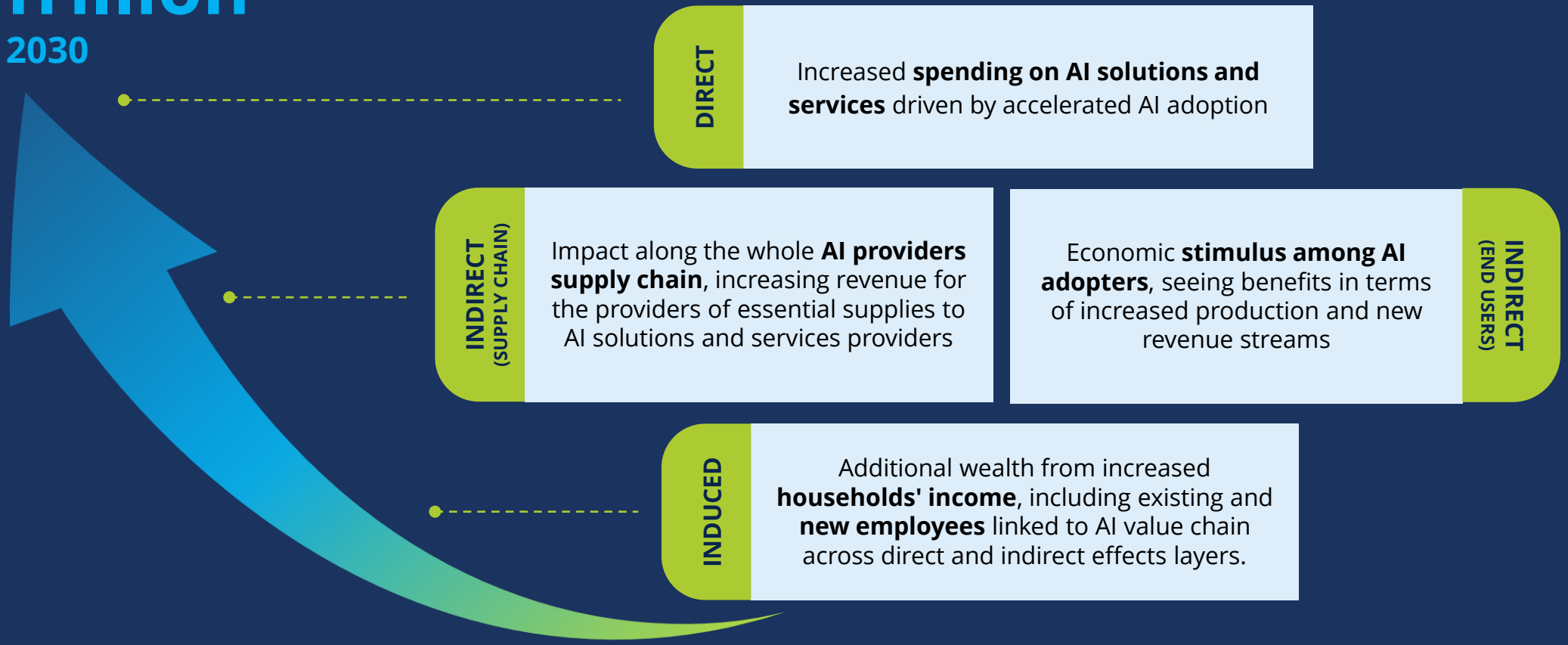
IDC's Global AI Economic Impact

AI will generate a cumulative Global Economic* Impact of

$22.3 Trillion

by 2030

This will represent 3.7% of global GDP in 2030, due to:**



* Global Economic Impact is calculated as a cumulative sum of the direct, indirect, and induced economic impact from 2024 to 2030.
** Percentage of GDP is calculated using the total economic impact of AI in 2030 and the projected worldwide GDP by IMF in 2030.
Source: IDC's Macroeconomic Center of Excellence, March 2025

2 types of risk

Constructive risk

Unnecessary risk

The key surrounds business disruption and the complexity it brings

What extent do you believe broad access to GenAI foundation models, platforms, and application technologies will disrupt your organization's competitive position or business operating model in the next 18 months?

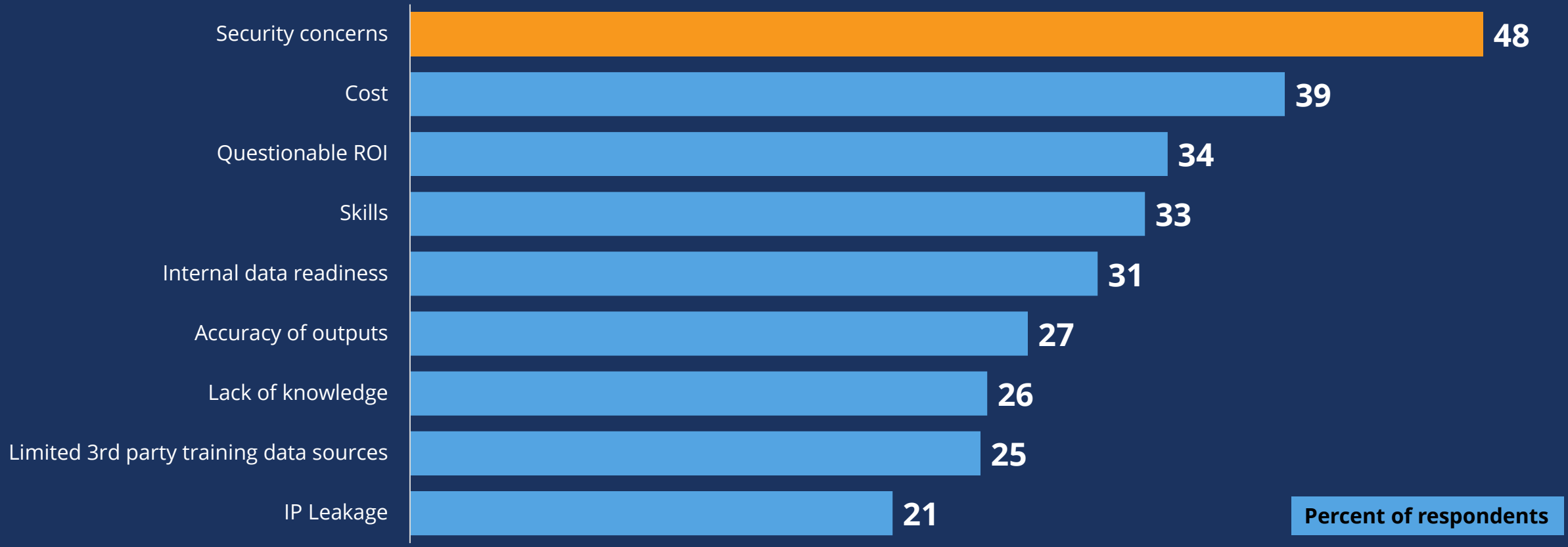



	Worldwide	North America	WE	AP
GenAI has already disrupted our business	10%	9%	9%	11%
GenAI is starting to disrupt our business now	23%	21%	20%	27%
GenAI will have a significant impact in next 18 months	37%	33%	39%	40%
GenAI will have a moderate impact in next 18 months	19%	19%	20%	
GenAI will have a minimal impact in next 18 months	11%	17%	10%	3%
Unsure/Don't Know	1%	0%	3%	0%

Source: Future Enterprise Resiliency & Spending Survey Wave 1, IDC, January 2024, N=881, NA: 361, WE: 220, AP: 300

Should you be worried about Gen AI security?

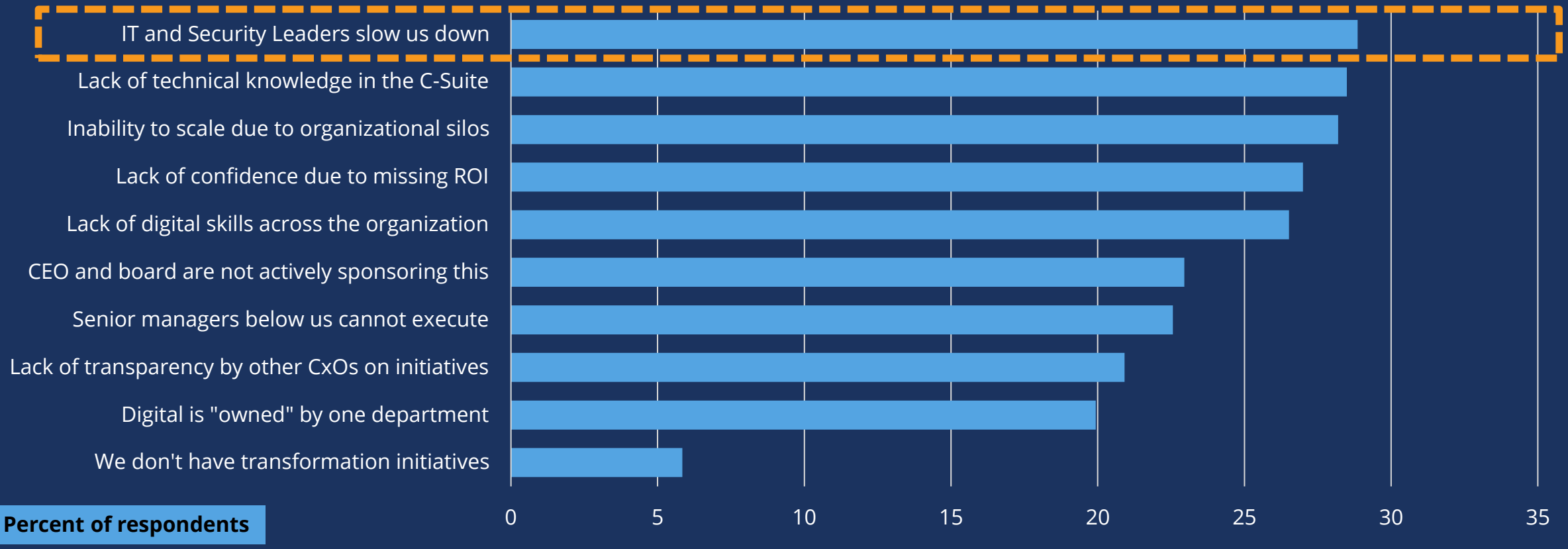
What are the most important challenges your organization is facing (or anticipate will be facing) with implementing GenAI initiatives?



Source: WW C-Suite Tech Survey, IDC, August, 2023, n = 895

Worldwide Top 5 C-Suite hurdles to digital initiatives

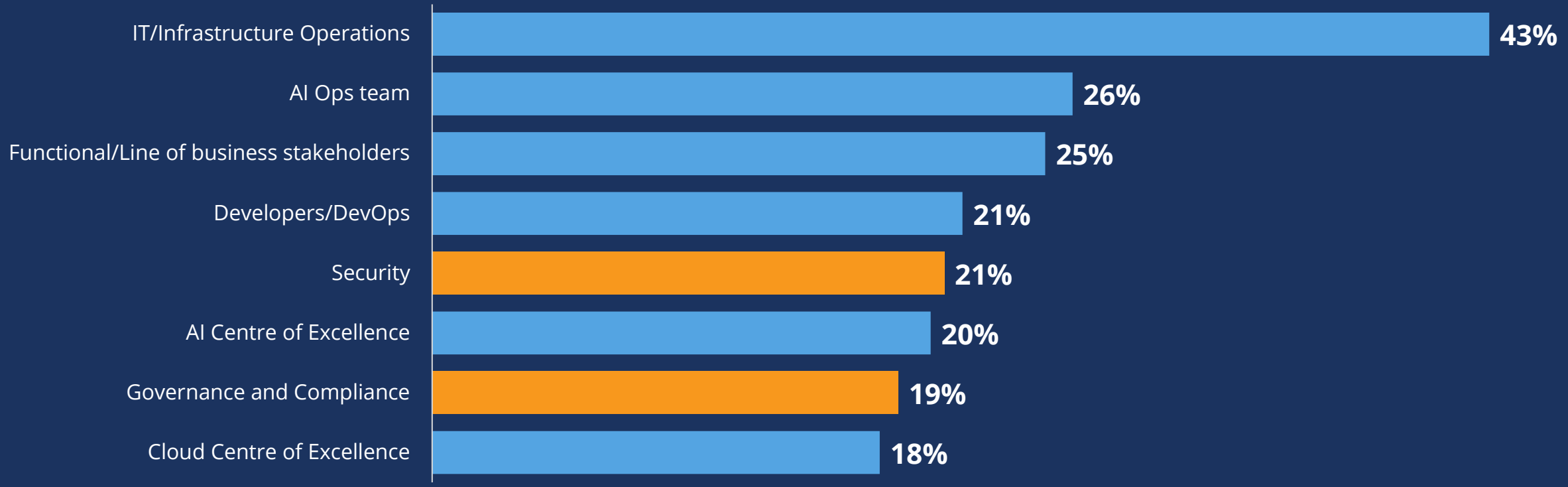
What are the most serious hurdles to completing digital initiatives in your organization?



Source: WW C-Suite Tech Survey, IDC, August 2022, n = 858

Where does security fall in considerations around AI solution deployment?

Which are the top 2 roles most involved with the data team during design, development and deployment of AI models and applications for business use cases?

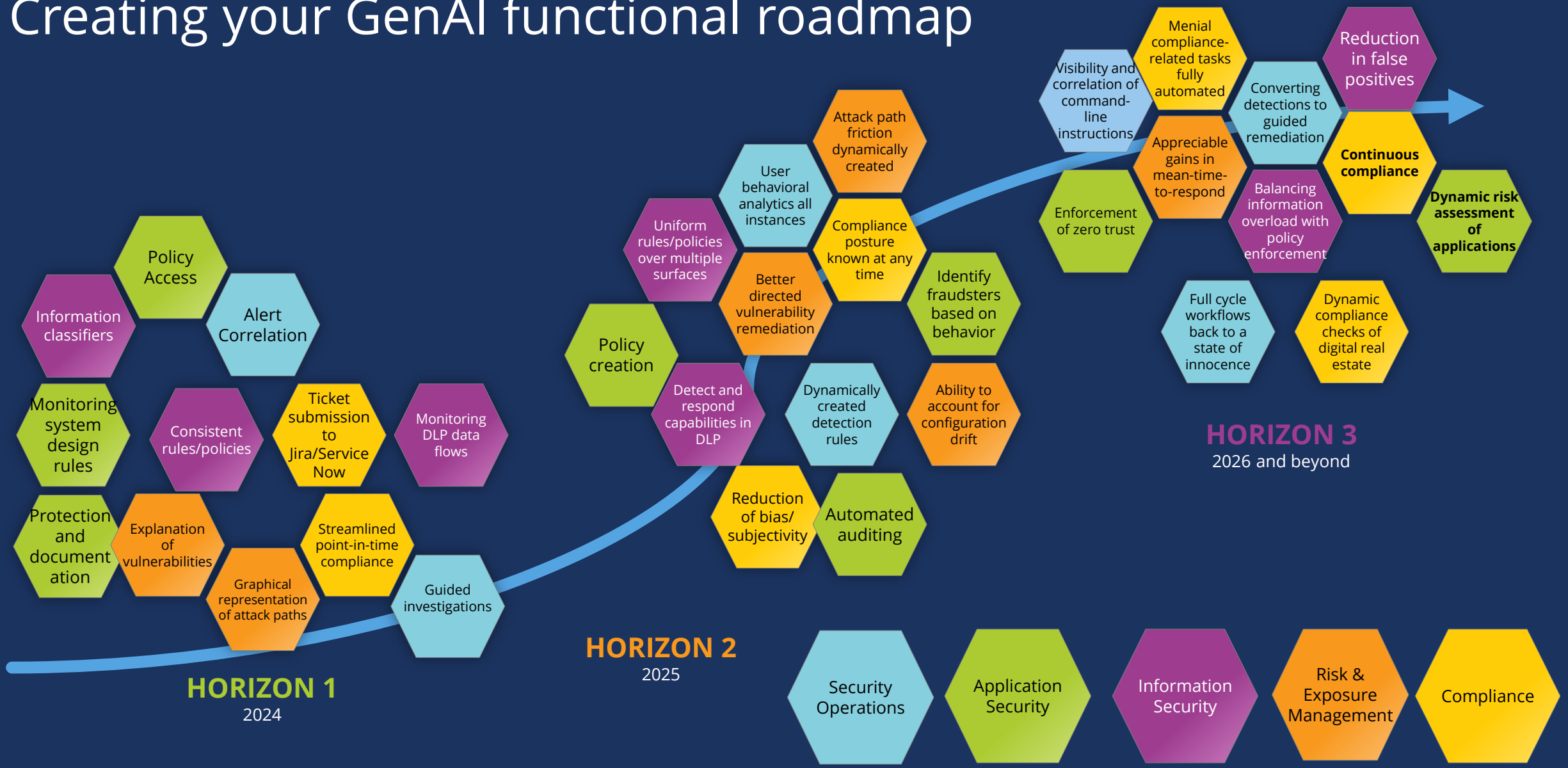


Source: Future Enterprise Resiliency & Spending Survey Wave 7, IDC, July, 2024, n=891

AI as a force for good

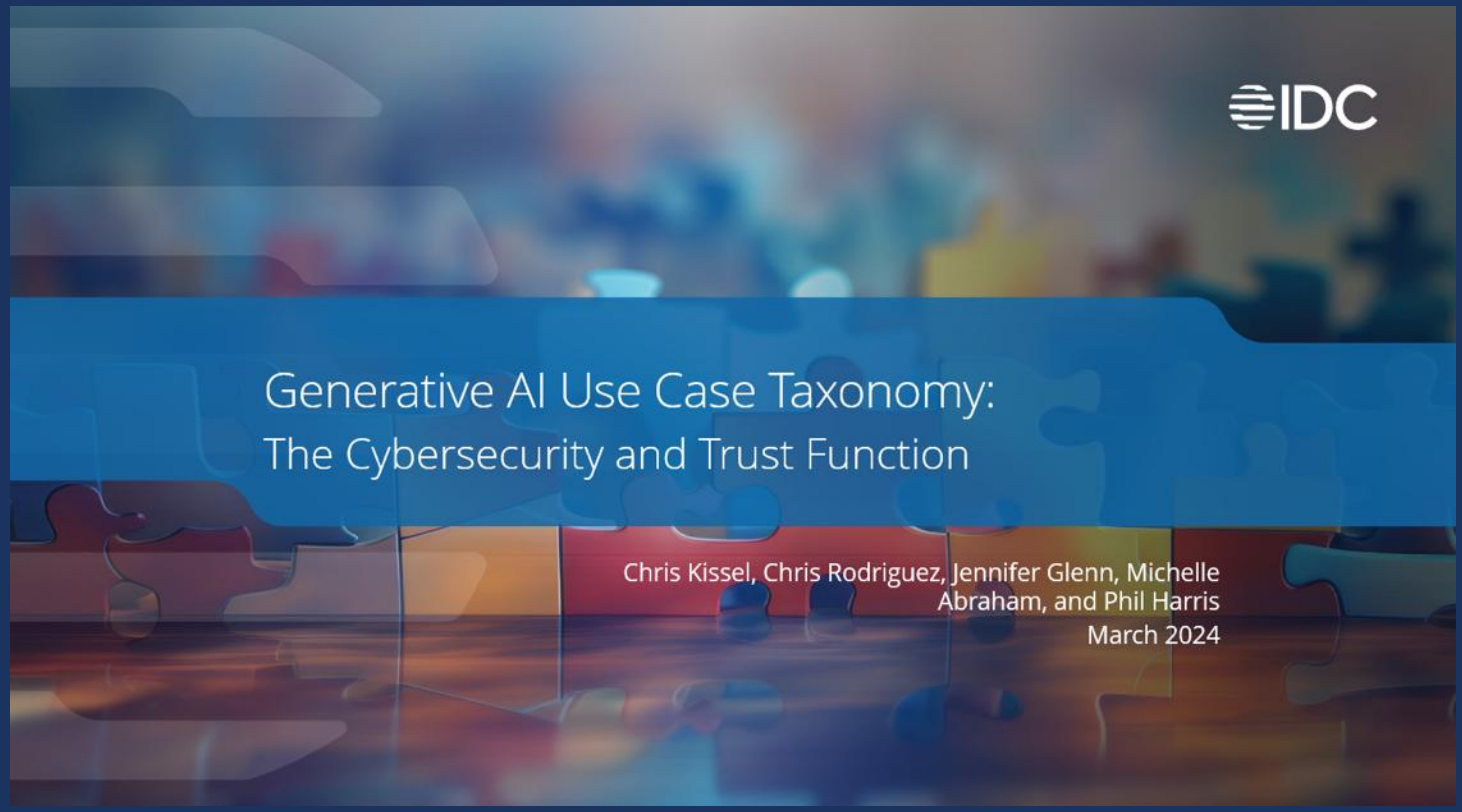
AI Ca e A P ful Fo for Cybersec ty

Creating your GenAI functional roadmap

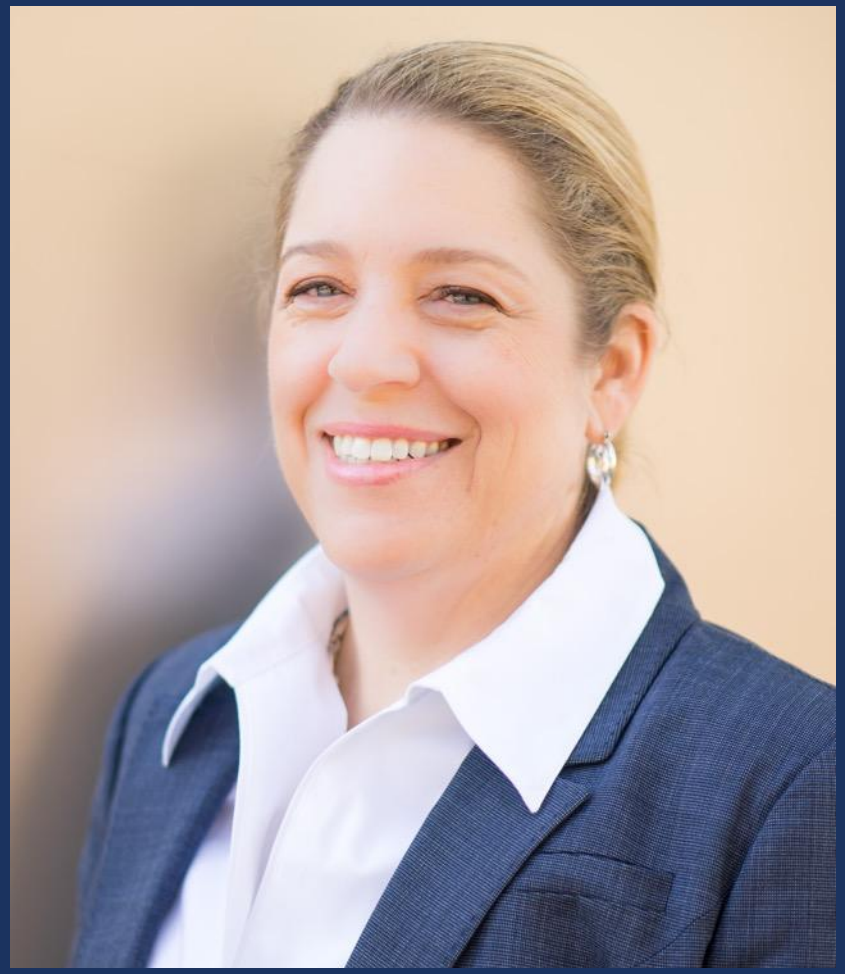


Chris Kissel, Research Vice President

Generative AI Use Case Taxonomy: The Cybersecurity and Trust Function; #US51962424



Michelle Abraham, Senior Research Director



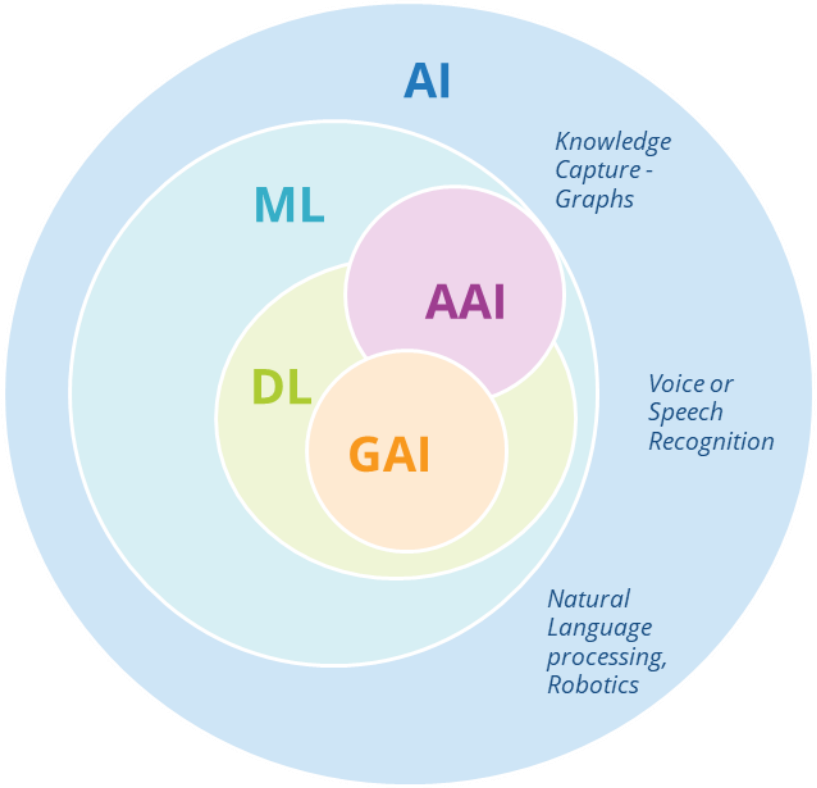
Recent Research on IDC.com

- Uses and Benefits of GenAI in Cybersecurity, Doc# US52742024
- Deployment Stage and Funding of GenAI in Cybersecurity, Doc# US52730124
- Generative AI Use Case Taxonomy: The Cybersecurity and Trust Function, Doc# US51962424
- Five More Big Questions About GenAI in Cybersecurity Answered: Volume 2, Doc #US51829324
- Five Big Cybersecurity Questions About GenAI in Cybersecurity Analytics Answered: Volume One, Doc #US51850124
- Has Our Opinion of the Impact of GenAI on Cybersecurity Changed Since Last Year?, Doc #US52393324
- RSA 2024: AI Lives; Hail to the Platform, Doc #US52188624

IDC

Protecting our organization as we Implement AI

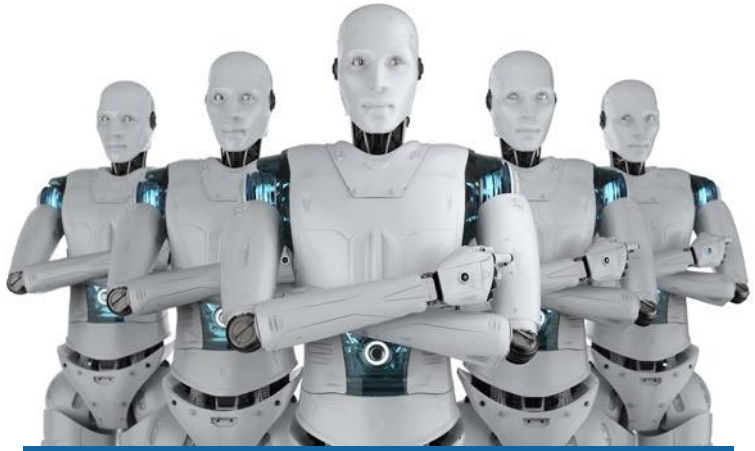
What is AI?



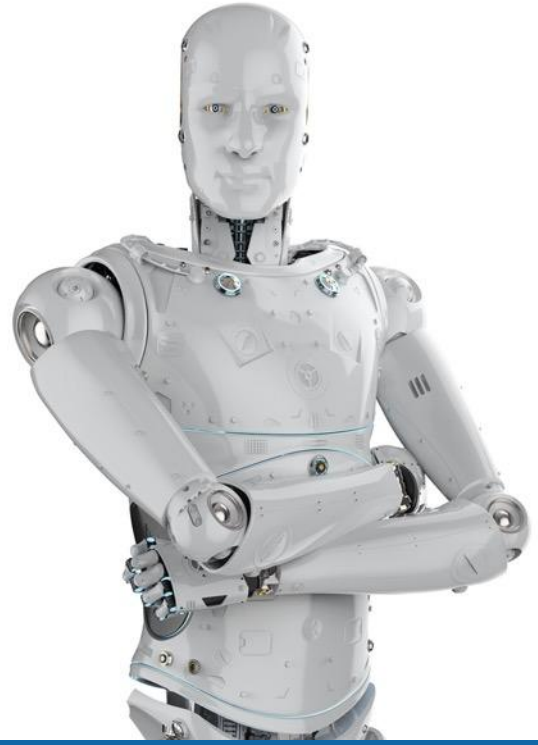
AI - Artificial Intelligence	*Techniques that help computers mimic human behavior.*
ML - Machine Learning	*Subset of AI techniques that enable computer systems to learn without programming by a human. E.g., Supervised learning, Unsupervised Learning, Reinforcement Learning.*
DL - Deep Learning	*Subset of ML techniques that makes the computational multilayer neural networks feasible. E.g., CNN, RNN, GAN.*
GAI -Generative AI	*Subset of DL techniques that enable computers to create new content using previously created content, such as text, audio, video, images and code.*
AAI - Agentic AI	*Subset of ML and DL techniques that enable computer systems to exhibit agency: set goals, make decisions and take actions through perception, reasoning and action loop.*

Source: Tech Buyer Presentation – Agentic AI Impact on Enterprises – From Tech Stack to Future of Work and Services

3 areas of CISO concerns for GenAI



Others' applications



Your applications

Your models

3 areas of CISO concerns for GenAI

Your models

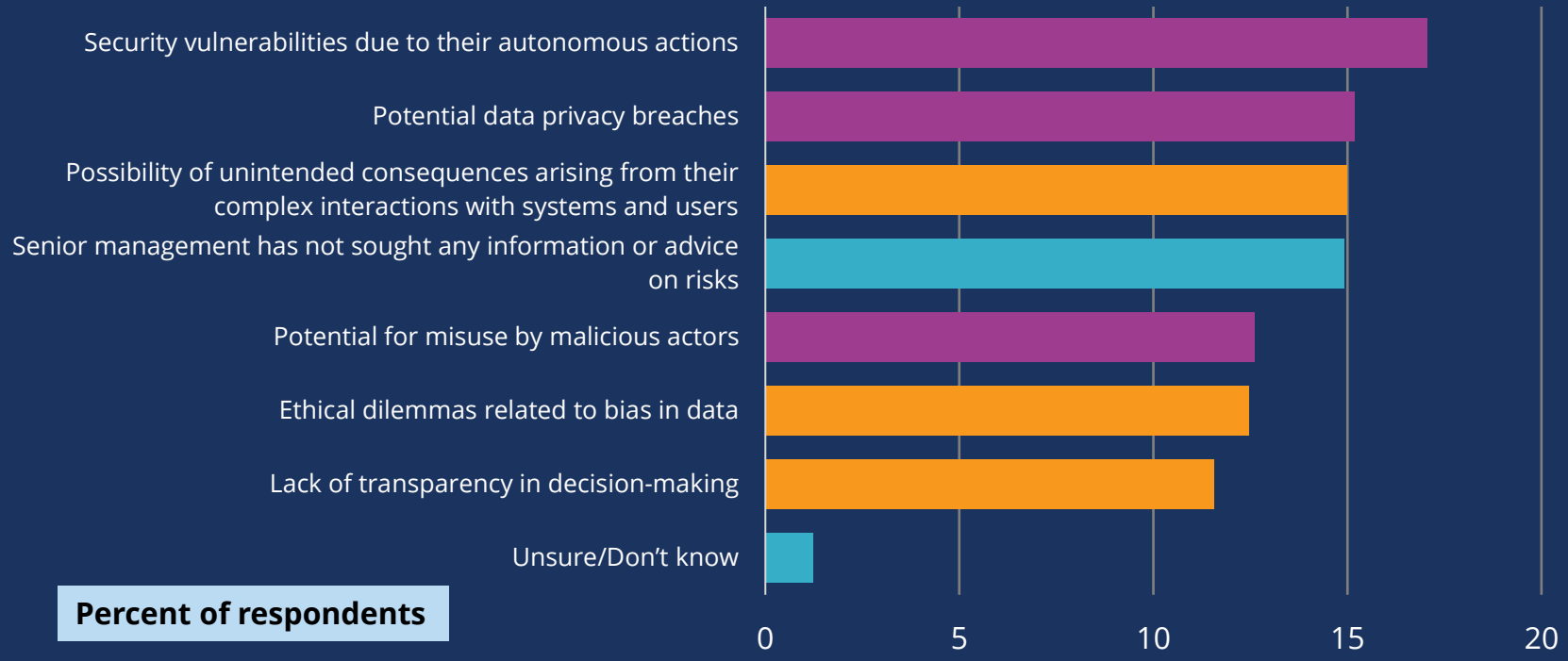
IDC Survey Spotlight

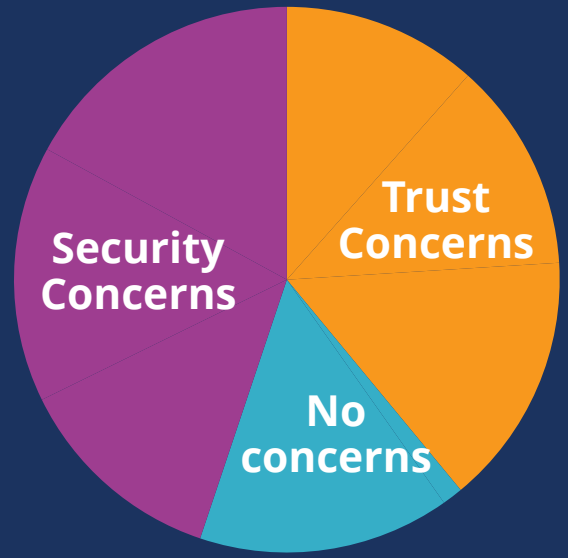
Do the security risks of Agentic AI keep senior leadership up at night?

FRANK DICKSON

MICHELLE ABRAHAM

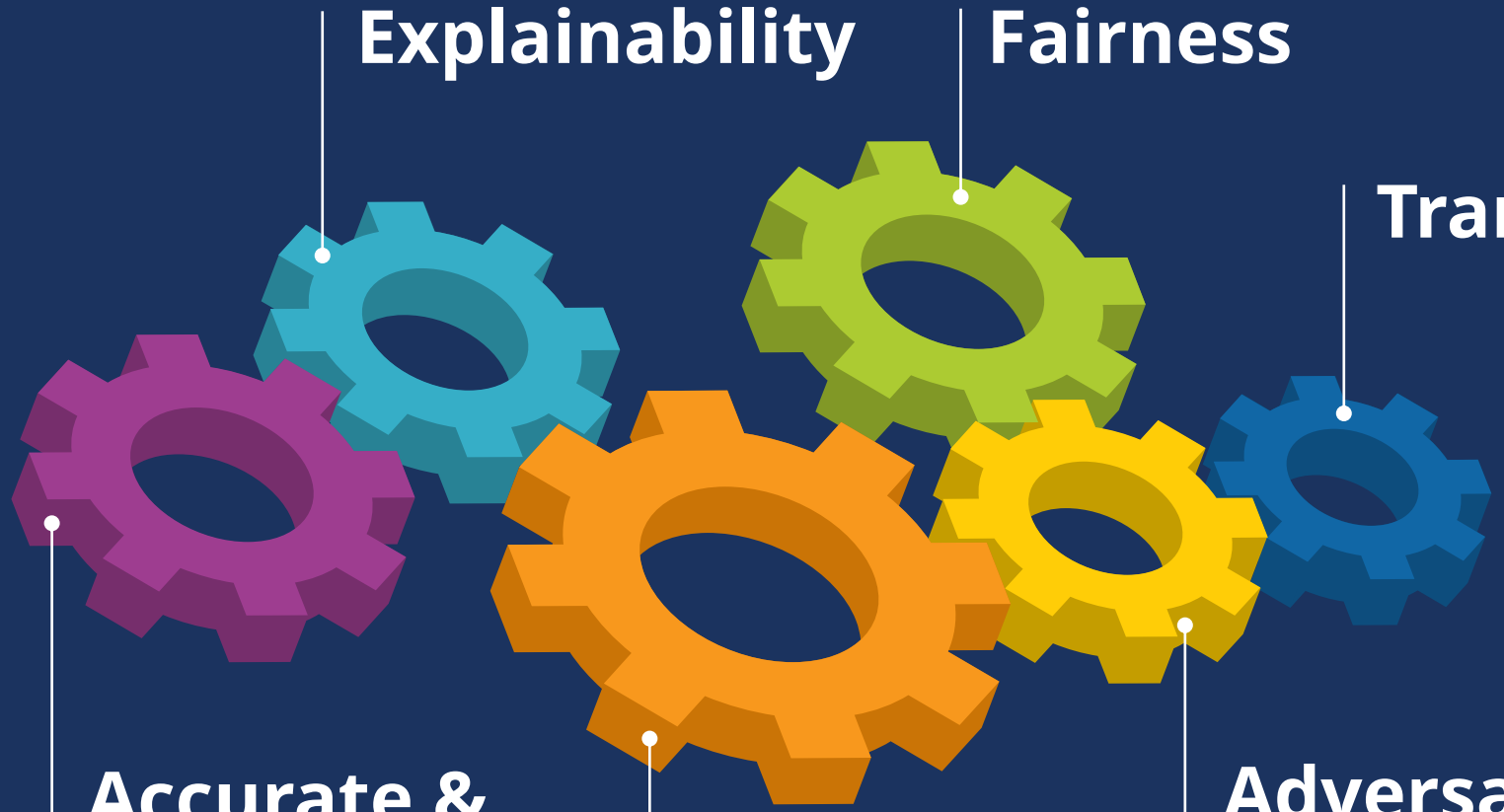
For which of the following Agentic AI-related business risks has the senior leadership most sought information or advice from IT leadership?





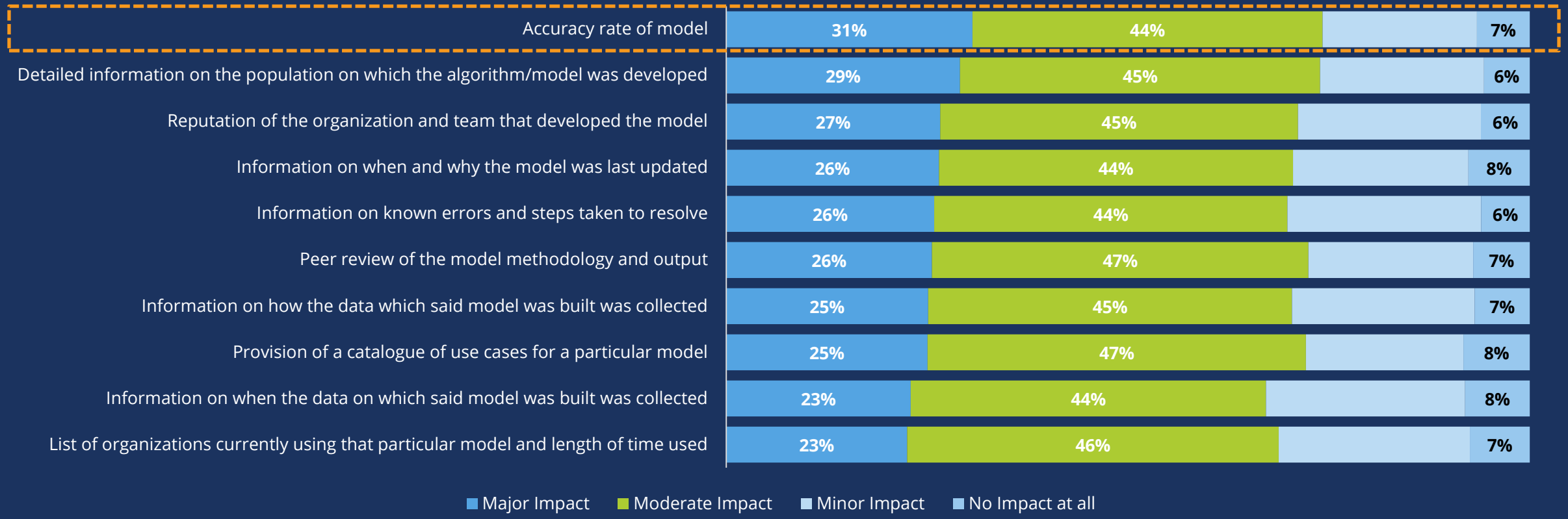
IDC #XXXXXX (Publication date)
Source: Future Enterprise Resiliency & Spending Survey Wave 11, IDC, November, 2024, n = 889

Elements of trustworthy AI



The accuracy rate of the model has the greatest impact on perceived trustworthiness of AI and automation technologies across all respondent categories

Please indicate how much each of the items below would impact your perception of the trustworthiness of AI and automation technologies.



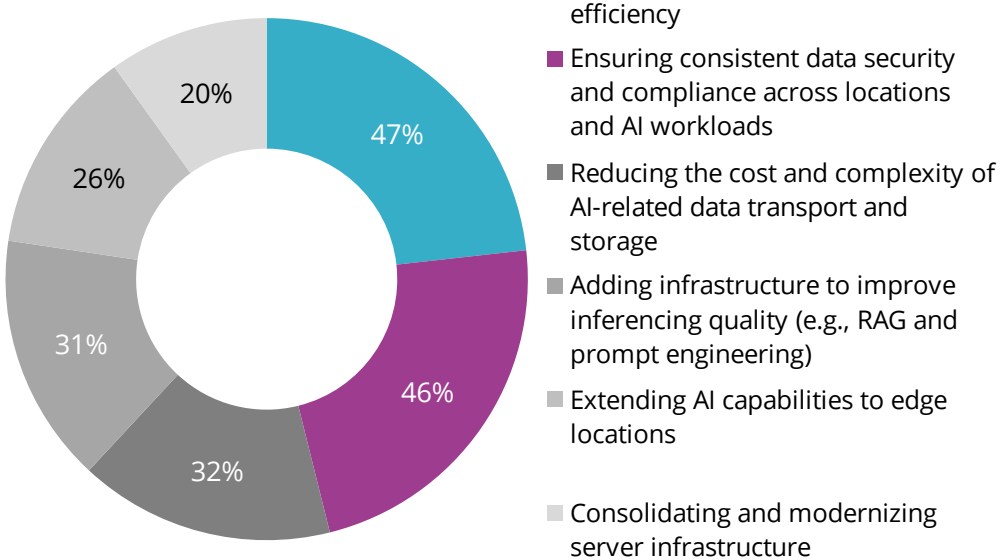
Source: Future Enterprise Resiliency & Spending Survey Wave 11, IDC, December 2023, n = 881

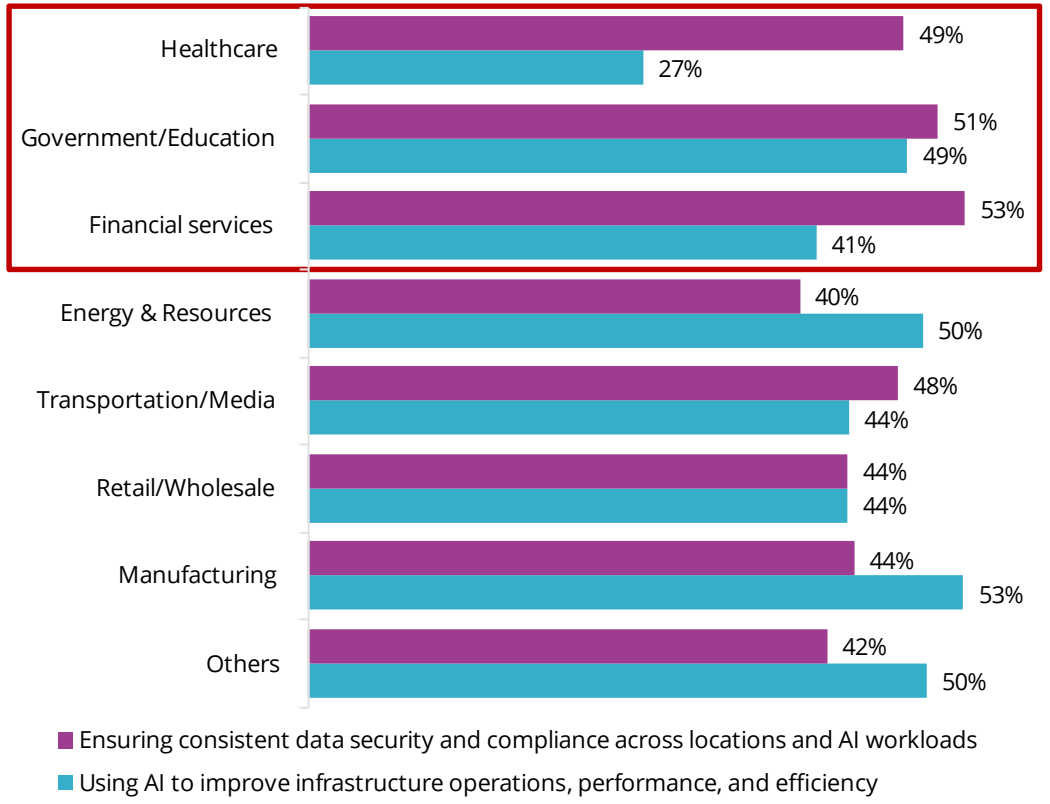
Concerns seem to vary by geography

How important is securing data for AI in heavily regulated industries?

JENNIFER GLENN

You indicated that you are prioritizing AI infrastructure readiness in 2025.
What is your most important goal for these efforts? What is your second most important goal?





IDC #US53246525 (March 2025)
Source: Future Enterprise Resiliency & Spending Survey Wave 1, IDC, February, 2025 n=424; Financial Services = 58; Government/Edu = 41; Healthcare = 33; Manufacturing = 45; Retail/Wholesale = 41; Transportation/Media = 25; Energy & Resources = 20; Others = 161

Secure at the application level as a “black box”

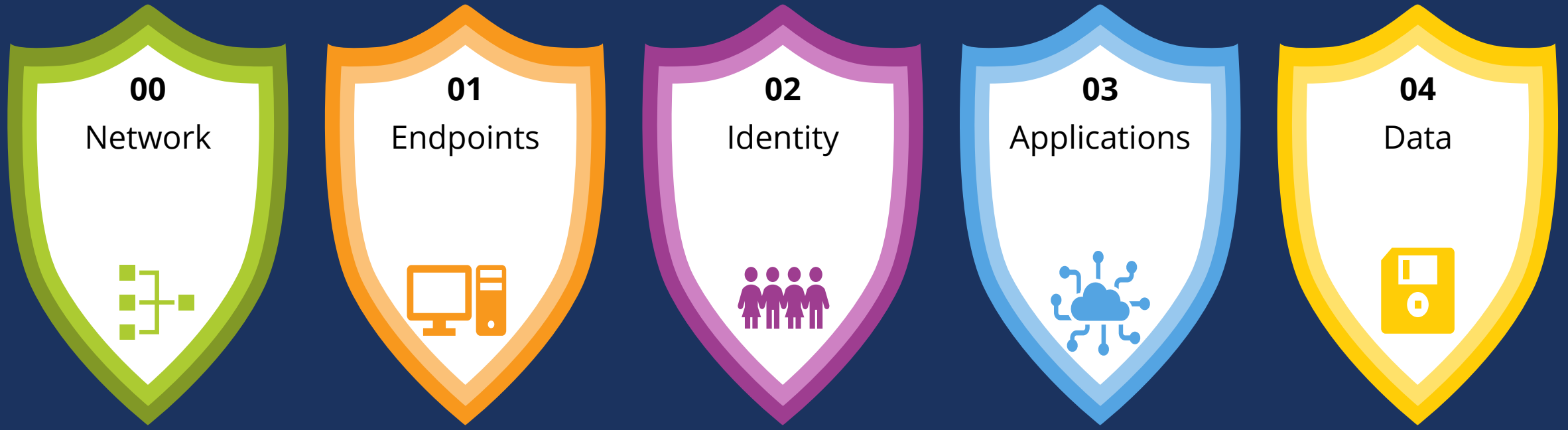
AI applications will become model cocktails

Dr. Grace Trinidad, Research Director

Will I Trust AI? Survey Research on the Impact of Accuracy, Population Data, and More on the Trustworthiness of AI Technologies Worldwide, Doc #US51944224

Reducing the risk from GenAI applications

The new four central control points of digital transformation as network- and perimeter-centric security measures become more permeable.



Network

Never goes away.

Endpoints

A dark internet will require a security presence at key termination points.

Identity

Identity becomes the new perimeter.

Applications

Layer 7 is the new Layer 3.

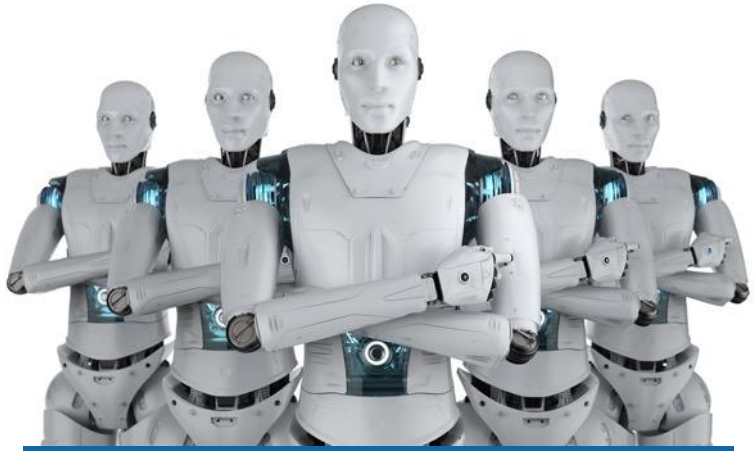
Data

Prioritizing protection while retaining sufficient usability is the new paradigm of enterprise defense.

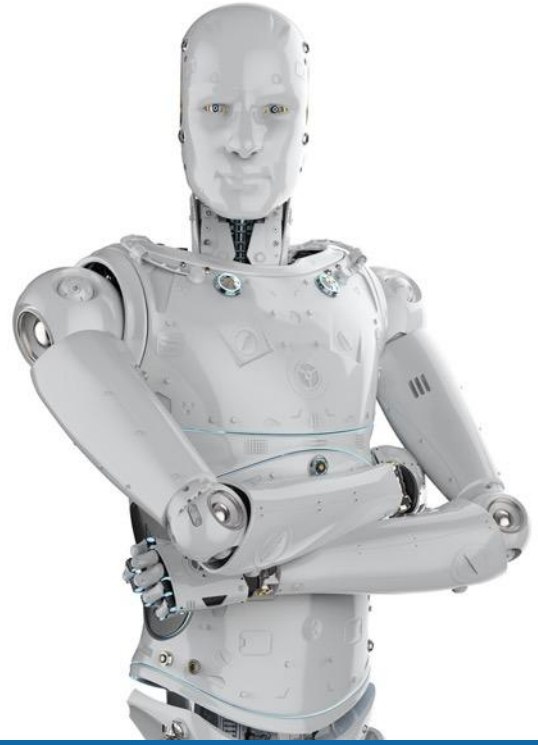
IDC

Source: March 2019, IDC #US44938819

3 areas of CISO concerns for GenAI



Others' applications



Your applications

Your models

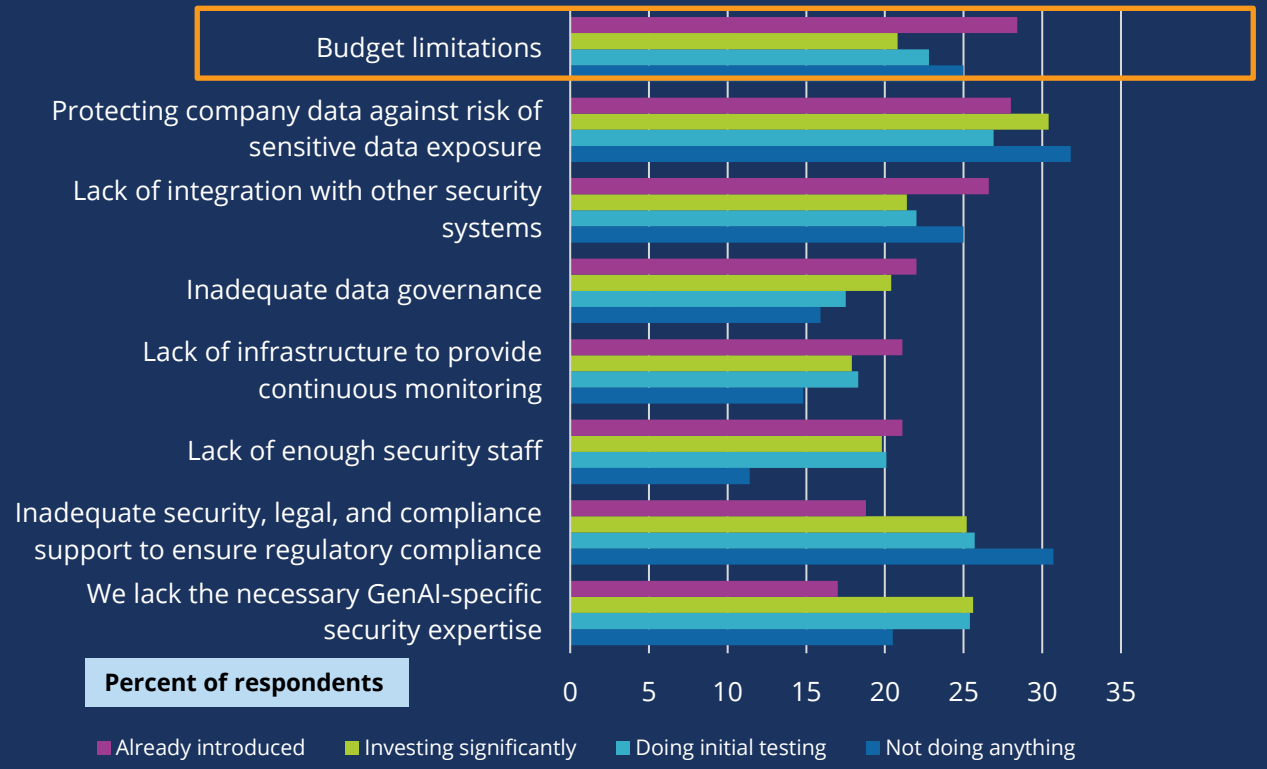
IDC Survey Spotlight

What are the problems in securing first-party versus third-party GenAI applications used in your organization?

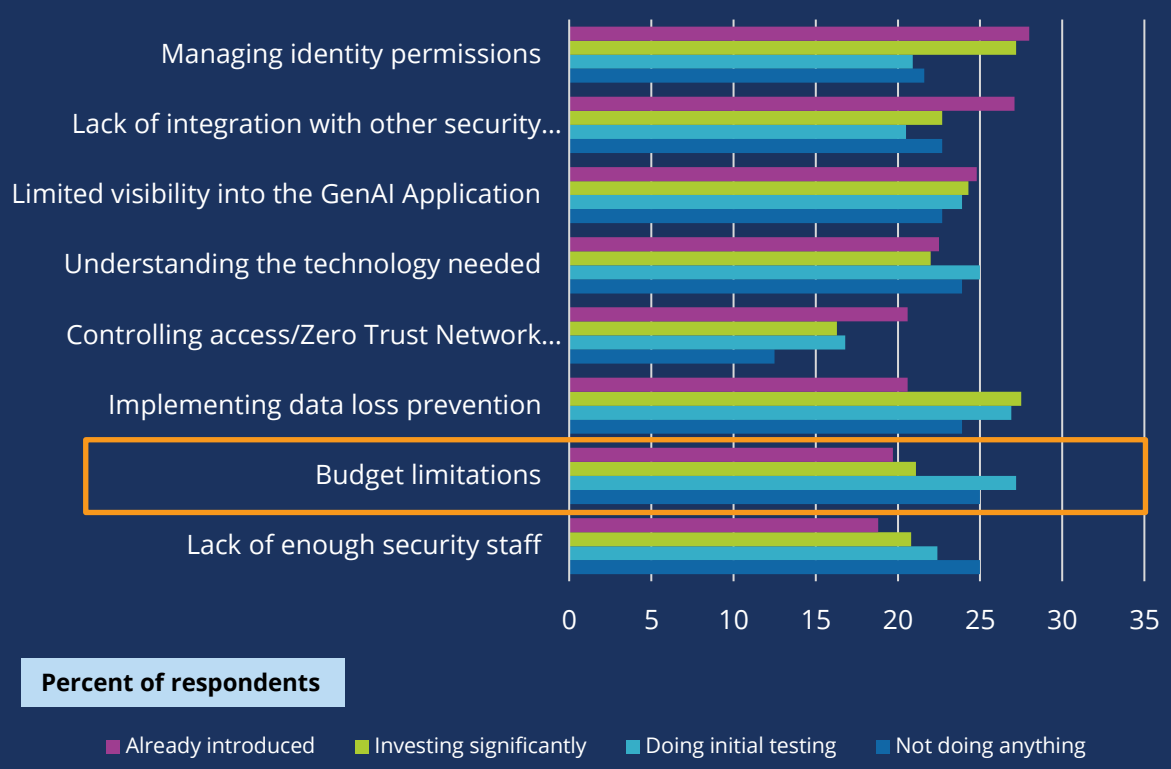
FRANK DICKSON

MICHELLE ABRAHAM

What are the two greatest challenges your organization faces in securing your *internally* developed GenAI applications?

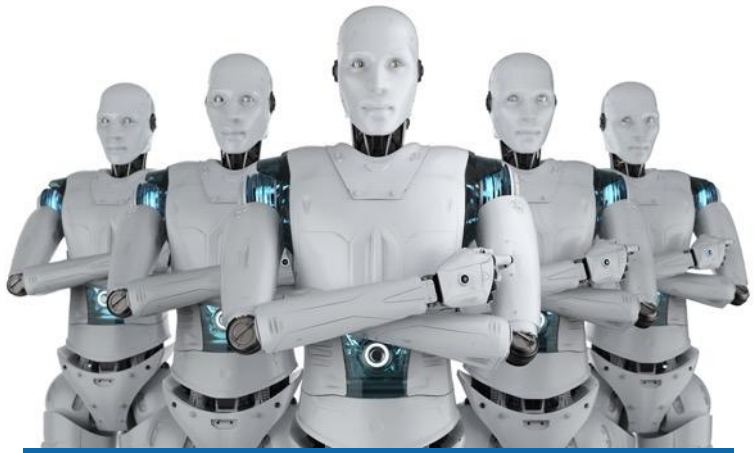


What are the two greatest challenges your organization faces in securing *third-party delivered*, GenAI-enabled applications?



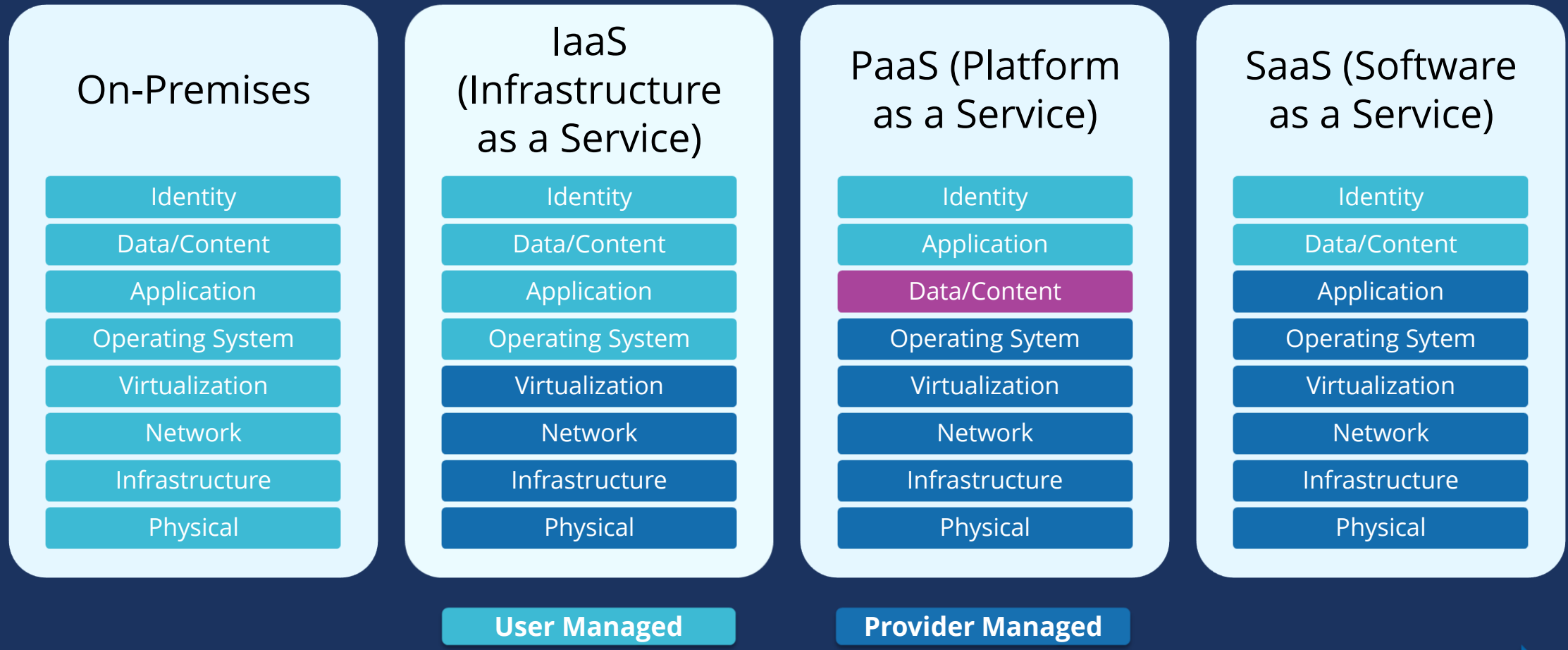
IDC #XXXXXX (Publication date)
Source: Future Enterprise Resiliency & Spending Survey Wave 9, IDC, September 2024, n = 890

3 areas of CISO concerns for GenAI

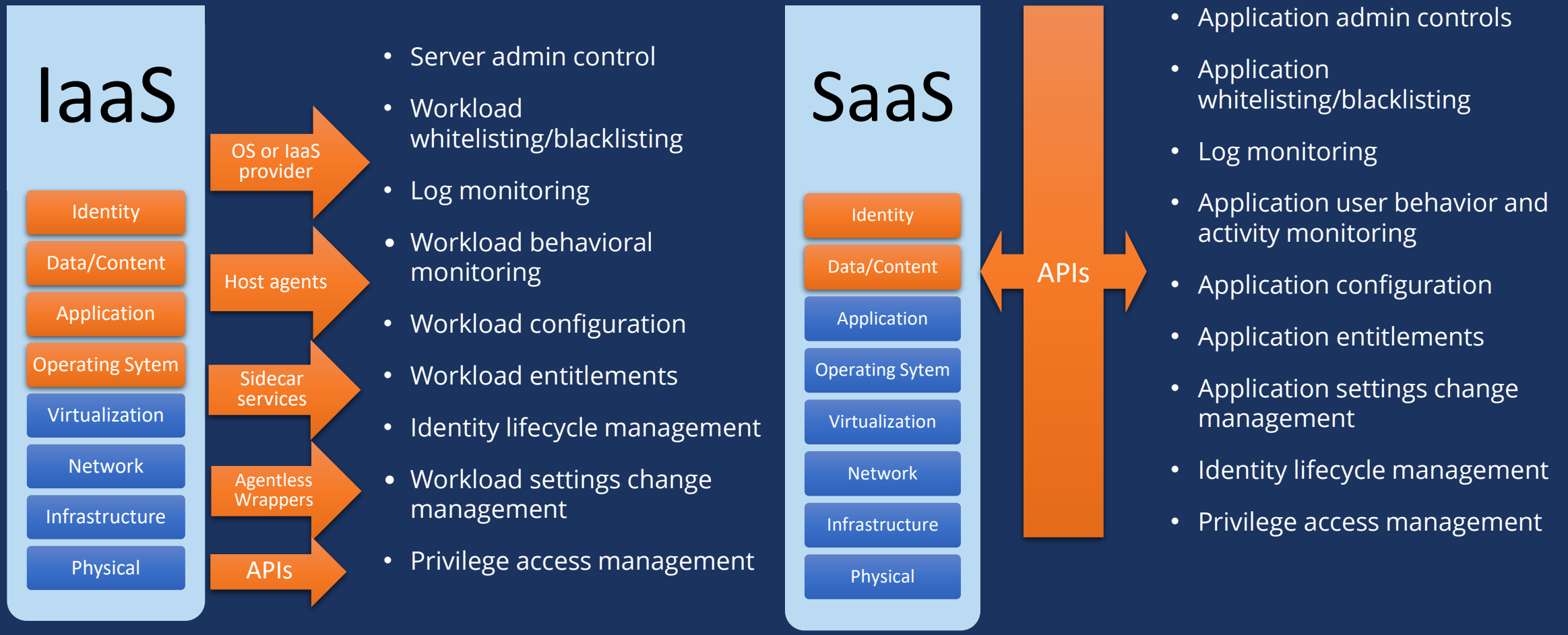


Others' applications

Shared infrastructure model



IaaS allows many ways to implement security
SaaS allows security to be only implemented via APIs



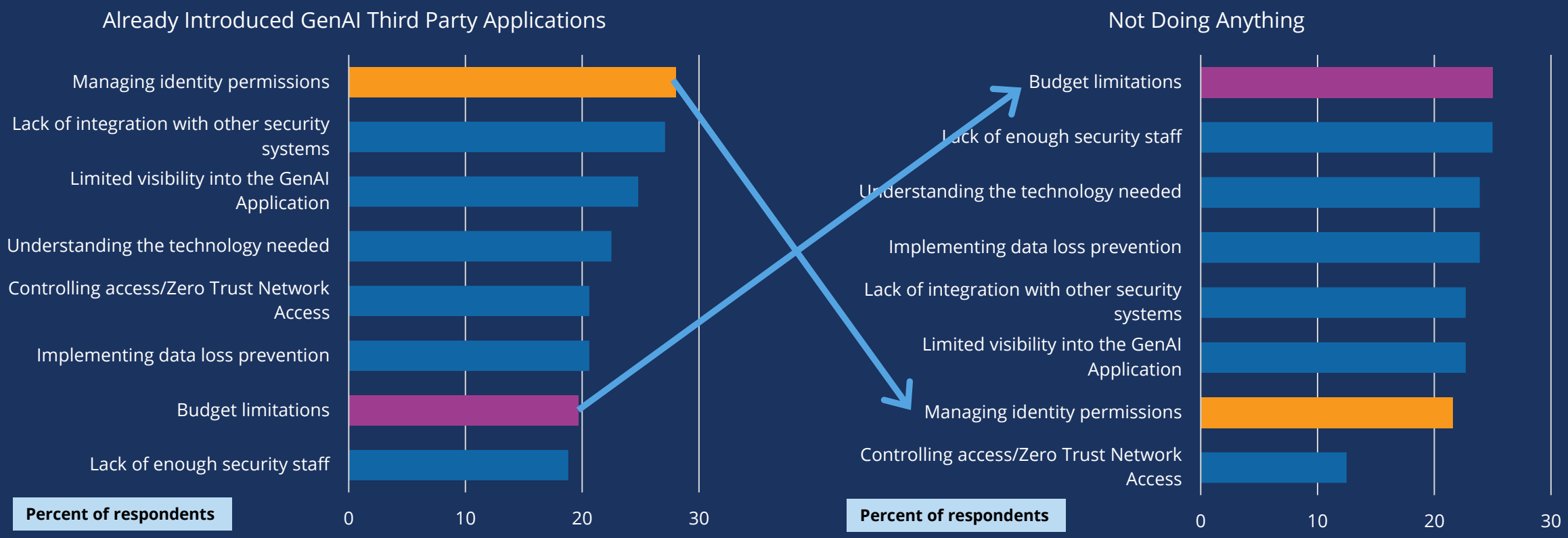
IDC Survey Spotlight

Do we really know the issues that we will face in securing third-party GenAI applications used in our organizations?


FRANK DICKSON

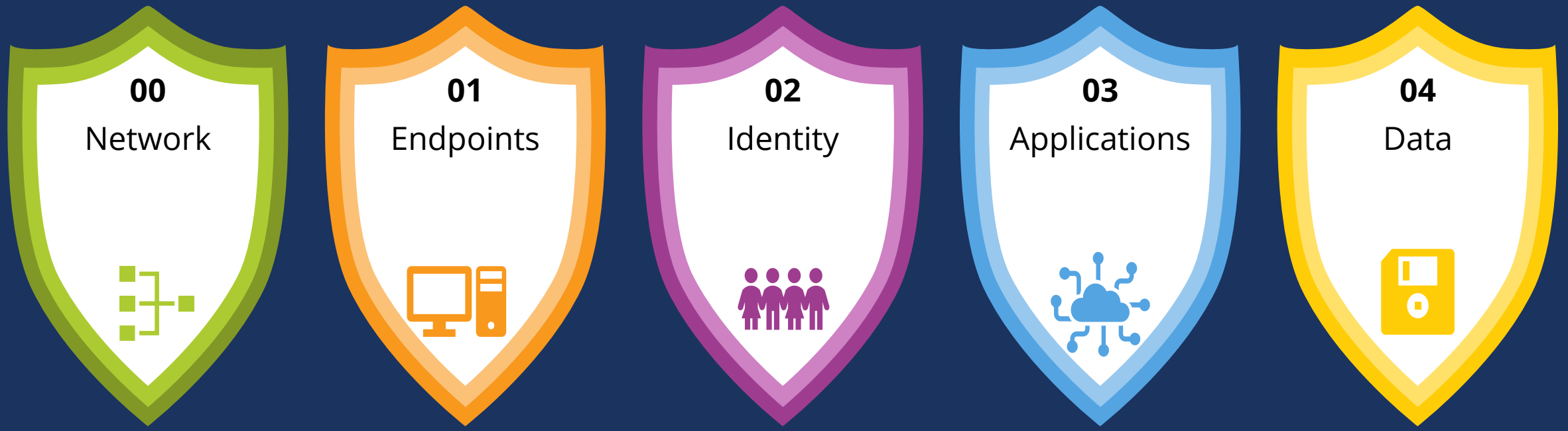

MICHELLE ABRAHAM

What are the two greatest challenges your organization faces in securing third-party delivered, GenAI-enabled applications?



IDC #XXXXXX (Publication date)
Source: Future Enterprise Resiliency & Spending Survey Wave 9, IDC, September 2024, n = 890

Control points for GenAI



Network

Secure Web Gateway

CASB

Endpoints

EDR

Identity

Authentication

Authorization

Governance

Applications

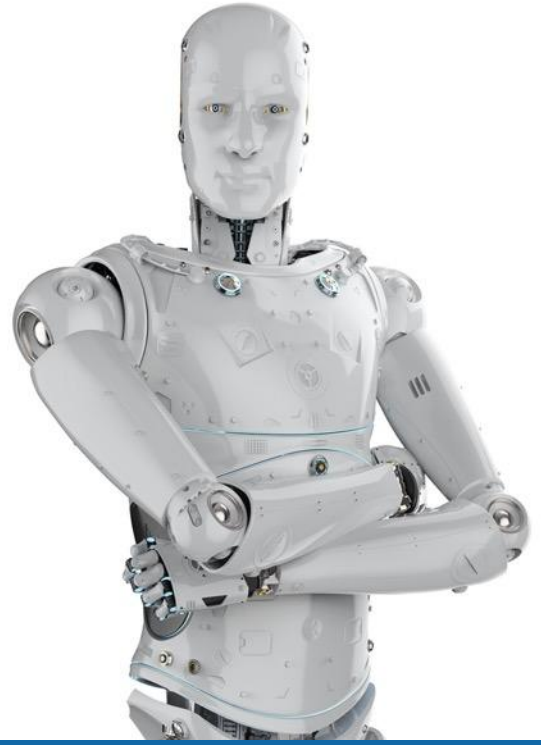
Proactive Access

Data

DLP

Source: March 2019, IDC #US44938819

3 areas of CISO concerns for GenAI



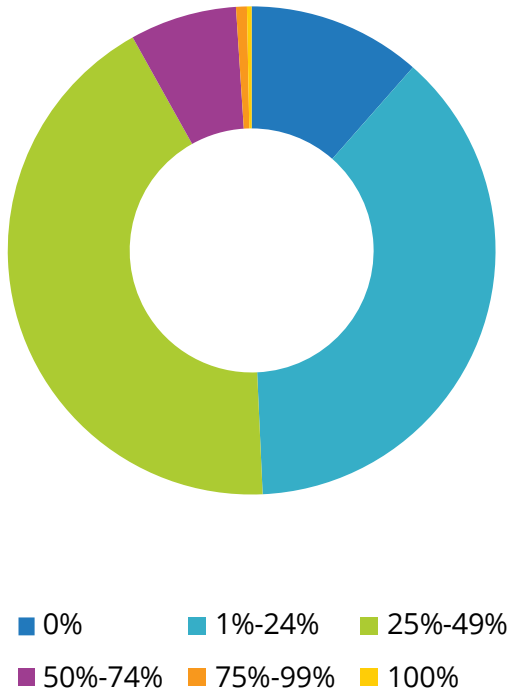
Your applications

IDC Survey Spotlight

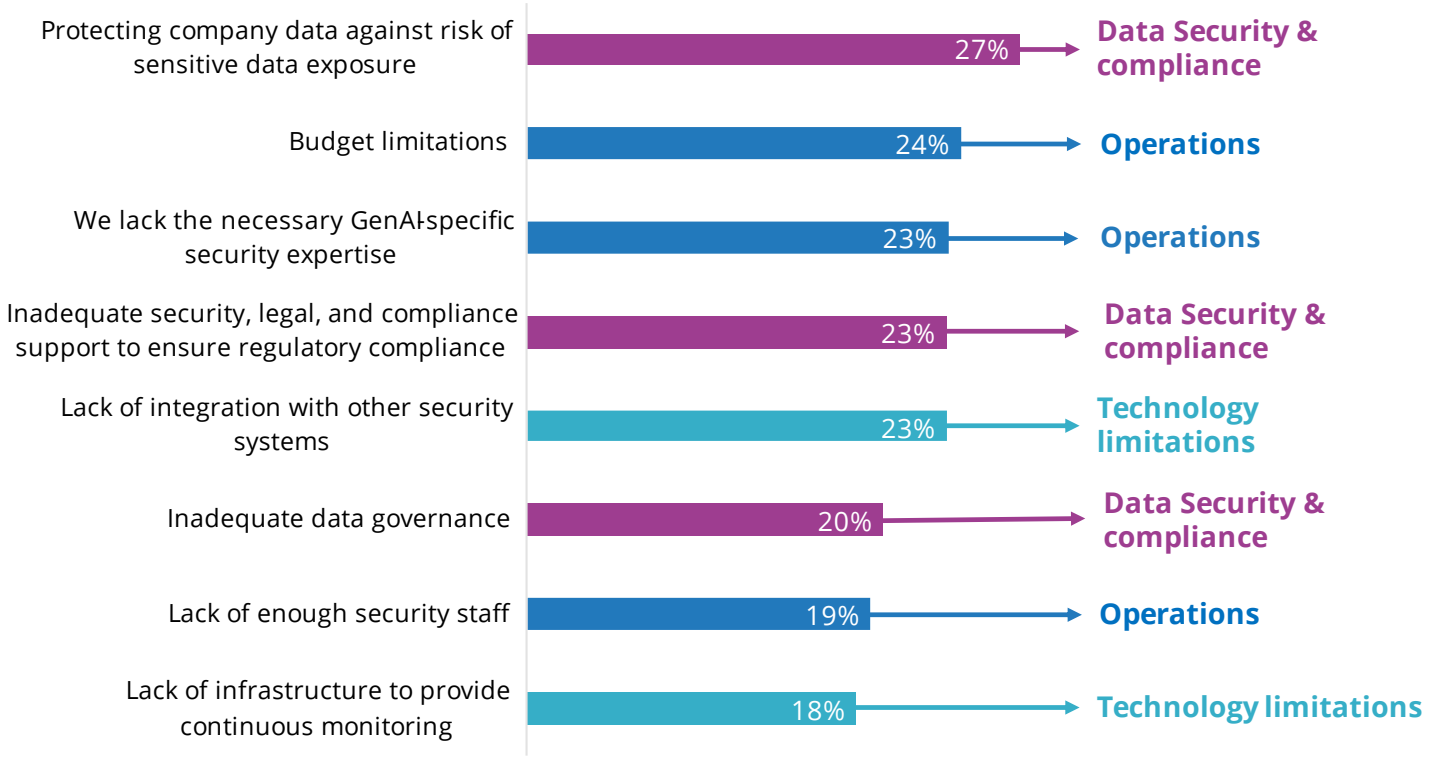
Are data security, privacy and compliance an impediment to GenAI deployments?

JENNIFER GLENN

How many custom AI apps and packaged AI apps/services were converted from POC to production in the past 12 months?



What are the two greatest challenges your organization faces in securing internally developed GenAI applications?

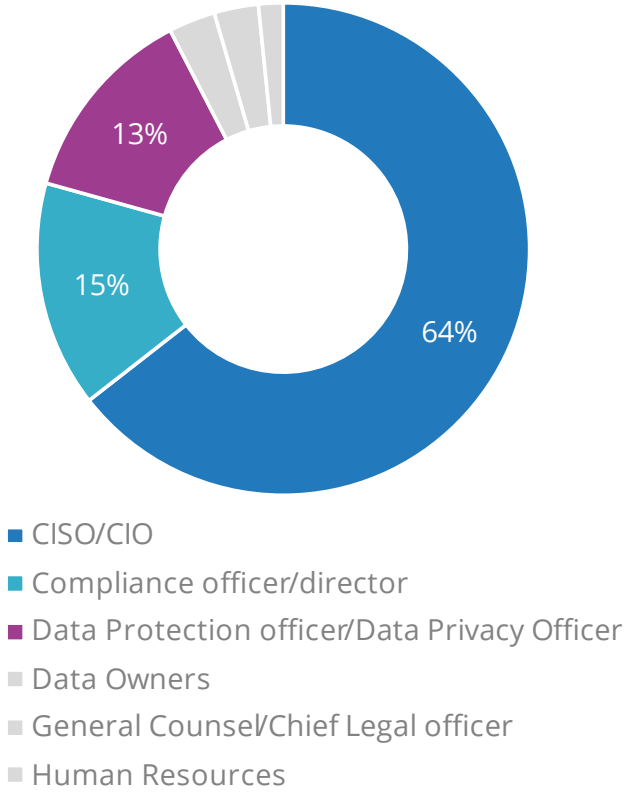


IDC #US53069825 (January 2025)
Source: Future Enterprise Resiliency & Spending Survey Wave 9, IDC, September 2024 n=890
Multiple dichotomous table – total will not sum to 100%

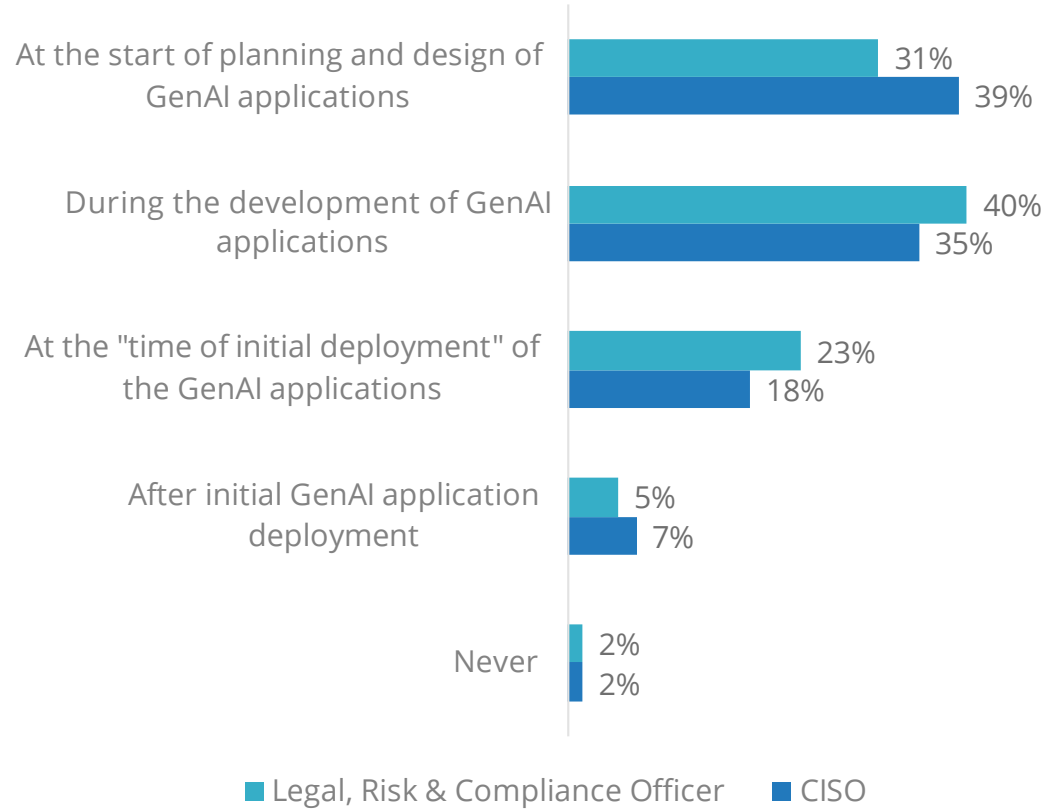
When should security and compliance teams be involved with GenAI development?

JENNIFER GLENN

Which group is primarily responsible for communicating data security and privacy risks to business leaders?

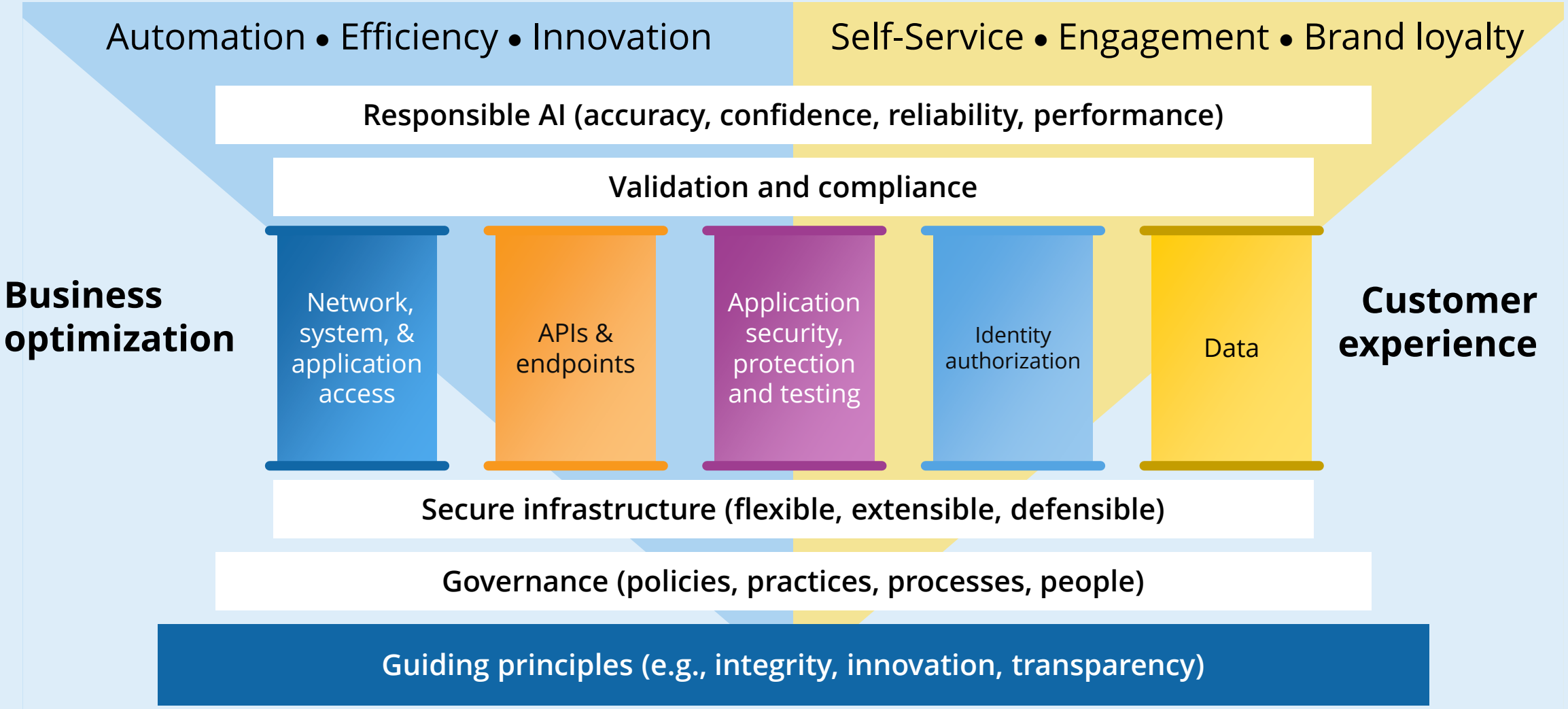


At which stage in development of your organization's GenAI applications are the CISO or Chief Legal, Chief Risk and/or Compliance Officer engaged?



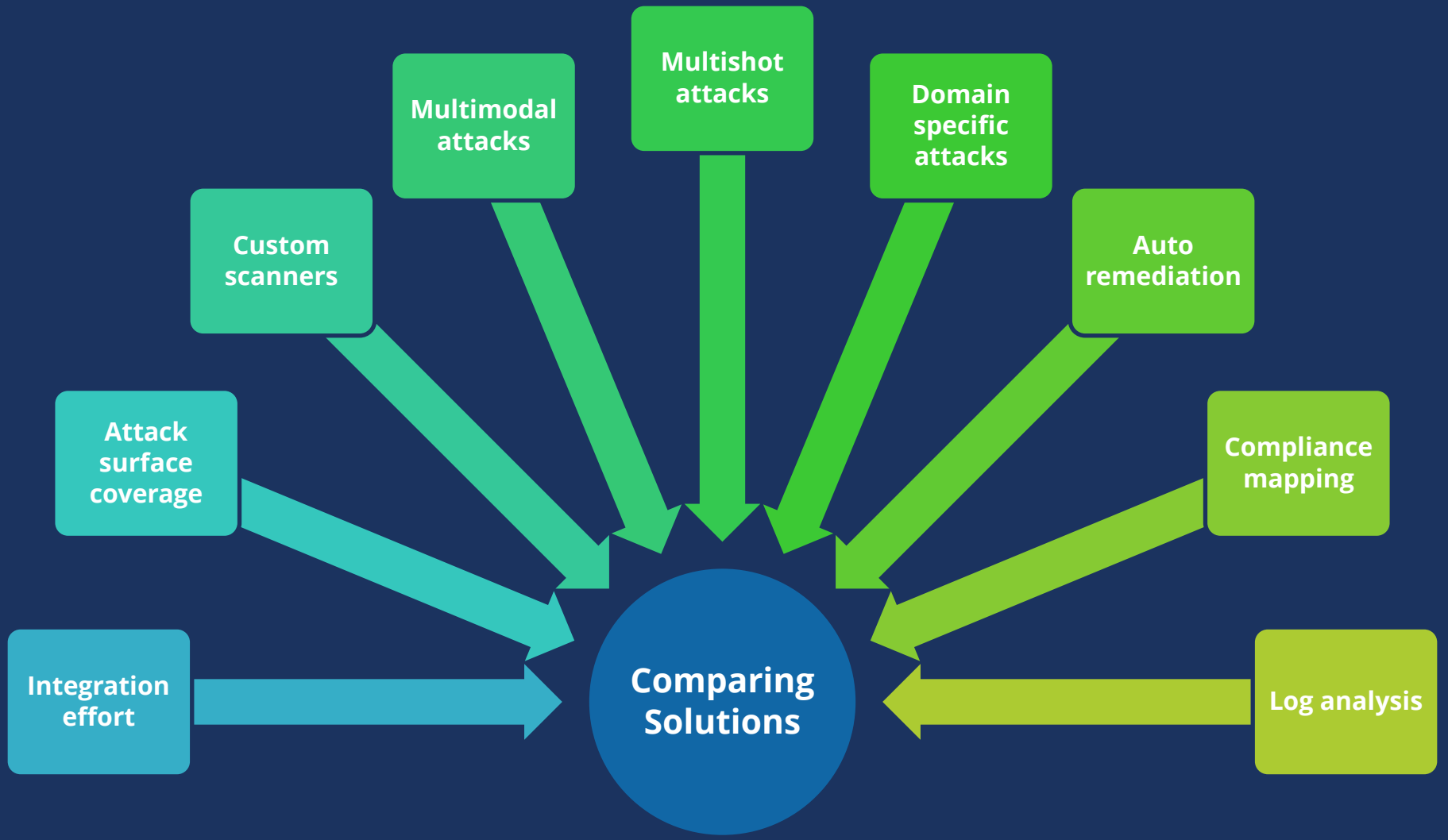
IDC #US53069925 (January 2025)
Source: Data Privacy Survey, IDC, March 2024 n=619; Future Enterprise Resiliency & Spending Survey Wave 9, IDC, September 2024 n=890

Identifying the issues associated with building out AI trust



Types of trust checks for your applications: Accuracy, security, privacy and compliance

Pen testing your AI applications




IDC
Thank you
IDC.COM
LINKEDIN.COM/COMPANY/IDC
X.COM/IDC


IDC Directions