aws

This report was produced by

FT LONGITUDE

# Finding the balance

## How to build secure foundations to scale AI innovation at speed

# Contents

# Executive summary

## Cybersecurity takes center stage as organizations race to scale their AI ambitions.

Organizations are angling their ambitions toward autonomous AI, and this is turning cybersecurity into a powerful source of business growth. But growth will only happen when organizations build their strategies on three pillars: cybersecurity, data governance, and workplace culture.

New research from AWS shows that 94% of organizations expect autonomous AI agents to be making business-critical decisions by 2030. To prepare, many are thinking about the role of cybersecurity and whether it will support or obstruct this kind of bold innovation.

About

# One in three

say that security is embedded into AI innovation processes to support safe and efficient adoption and increase trust and long-term competitiveness

# Seven in ten

want to make sure they are not trusting AI faster than they can secure it

# One in four

are confident that their organization's current security position can support autonomous AI

Confidence in cybersecurity will give organizations a strong competitive advantage, says Clarke Rodgers, Office of the CISO at AWS Security. "The organizations that can start experimenting with AI are the ones that made the security, regulatory, and data governance investments ahead of time," says Rodgers. This is because the right frameworks allow an organization to break down innovation silos and empower teams. Those teams will go on to create new products and services that are less likely to experience security blocks before the organization launches them in the market.

But the pace of AI innovation is accelerating, and the research shows that most organizations are facing challenges in how to respond. This report aims to give them some guidance.

We study organizations with strong security frameworks to understand how their solid foundation enables faster AI innovation. These security frontrunners make up just 9% of the organizations in the research, and the returns on their AI investments are more likely to be significantly outperforming expectations across the three pillars.

> "The organizations that can start experimenting with AI are the ones that made the security, regulatory, and data governance investments ahead of time"
>
> **CLARKE RODGERS**
> **Office of the CISO, AWS Security**

## Who are the security frontrunners?

Security frontrunners meet all the following criteria:

**PILLAR 1** + **PILLAR 2** + **PILLAR 3**

### CYBERSECURITY

Our AI investments performed significantly better than our expectations over the past 12 months for cybersecurity

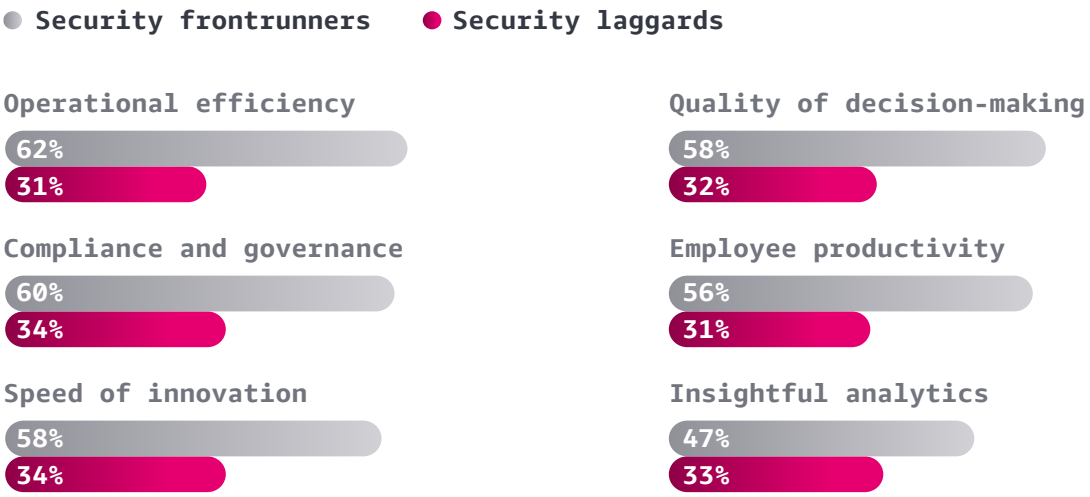
### DATA SECURITY

Our AI investments performed significantly better than our expectations over the past 12 months for data security and risk management

### WORKPLACE CULTURE

Our AI investments performed significantly better than our expectations over the past 12 months for workforce responsible use of AI

## Security frontrunners' AI investments are outperforming across all metrics




Q How did your AI investments perform compared with expectations across the following areas in the past 12 months?–(Significantly better)

Security frontrunners n=45; Security laggards n=455

The research findings at a glance:

- **Organizations are aligning security and AI to scale innovation with more confidence.** About one-third already see security as an enabler of innovation.
- **Closer collaboration between business and IT will accelerate strategic decision-making.** Security executives must educate business leaders to understand how security can help them to seize AI opportunities more quickly.
- **Leadership accountability is the most effective security measure among security frontrunners, but other organizations are not prioritizing it.** Other human elements, such as workforce training and collaboration, are inconsistent in both security leader and security laggards, which can create cultural gaps that stall progress.
- **Security frontrunners are redefining resilience.** This group sees autonomous AI as an opportunity to make security more proactive, intelligent, and integral to business resilience.

# Strong foundations: Security is the proven AI enabler

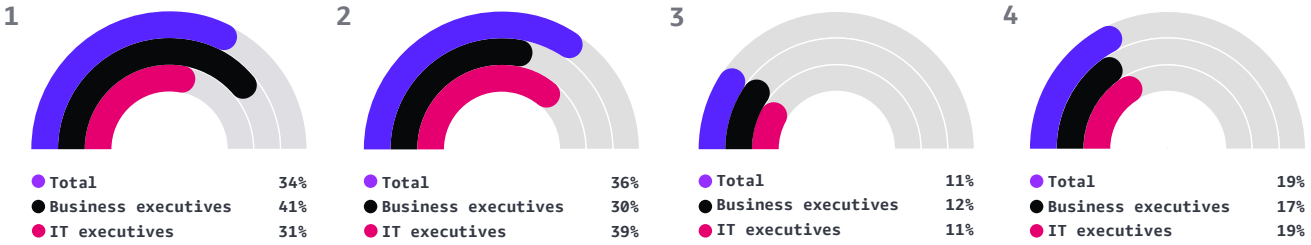
The rapid rollout of generative AI tools has shown that innovation can quickly outpace cybersecurity. Data leaks through open-source models are common, and high-profile cyber events have used AI to automate phishing, generate deepfakes, and manipulate models. Regulators are starting to respond with standards, such as the European AI Act and the US NIST AI Risk Management Framework, and the fastest-moving organizations are making security central to any innovation they pursue.

One critical early step in embedding security into AI innovation processes is to define what strong security foundations look like. A third of organizations (34%) say that security is already embedded into AI innovation processes to support safe and efficient adoption and drive trust and long-term competitiveness. A similar number say that they still need to better integrate their security and AI innovation teams, and one in five have not yet defined their approach to balancing security and AI innovation.

**34%**

of organizations say that security is already embedded into AI innovation processes to support safe and efficient adoption and drive trust and long-term competitiveness

## Organizations are working toward embedding security into AI innovation processes




1. Security is embedded to support safe AI innovation and to drive competiveness.
2. Security and AI innovation are both valued but managed separately.
3. Security takes priority, even if it slows down AI innovation.
4. Our approach is not yet clearly defined.

Q Which of the following best describes your organization's approach to balancing cybersecurity with AI innovation?

Total n=500; Business executives n=141; IT executives n=359

## Security improves when IT and business teams agree

What does a balanced approach mean in practice? Organizations' lack of progress toward optimized security could be a result of IT and business executives disagreeing on this point.

IT executives are 9 percentage points more likely than business executives to say that security and AI innovation are both valued but managed with limited coordination. Business executives, meanwhile, are 10 percentage points more likely to believe that security is already embedded into AI innovation processes and that it supports safe and efficient adoption.

Existing measures, security protocols, and attitudes can entrench silos between innovation and security. To avoid this, organizations can educate the broader business and then define what the optimum balance between security and AI innovation looks like today and into the future.

"Security and business value are co-equals," says Tom Godden, executive in residence at AWS. "You cannot sacrifice one of them for the other. Today, the CISO needs to be a business executive first and a technology executive second, otherwise they are going to miss the AI opportunity."

> "Security and business value are co-equals. You cannot sacrifice one of them for the other. Today, the CISO needs to be a business executive first and a technology executive second, otherwise they are going to miss the AI opportunity."
>
> **TOM GODDEN**
> **Executive in residence, AWS**

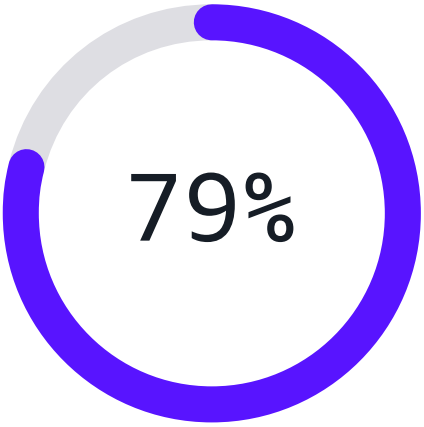
## Security frontrunners are overcoming misalignment

Security frontrunners have faced security challenges, both in terms of moving too quickly and too slowly, which has forced them to work with the business to find a better balance between security and innovation.

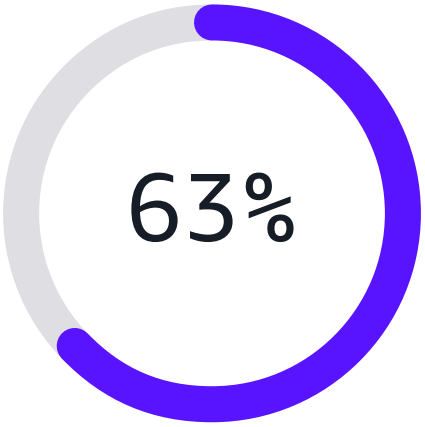
Two-thirds say that innovation has moved forward despite the organization not having the right security, and about the same number say that they have also experienced delays caused by security measures that are too stringent. Security failings relating to AI rollouts can lead to significant financial loss for the business, and proactively building security into innovation will be far less costly than retrofitting it after disruption.

### AI is less of a worry when security is embedded into innovation

"I have some concerns that we risk trusting AI systems faster than we can secure them."




of executives who say that their approach to balancing security and AI innovation has not yet been defined




of executives who say that security is embedded into AI innovation processes

It is important to be proactive and embed a strong security culture into the innovation process before it becomes a business-critical issue. This is especially important for security laggards, which are less confident than security frontrunners.

**69%**

of security laggards worry about whether they are trusting AI systems faster than they can secure them

**24%**

are very confident that their organization has the right security foundations to adopt AI innovations as they emerge

By defining clear ownership between IT and the business and embedding shared accountability for secure innovation, these organizations will be able to put the right guardrails in place.

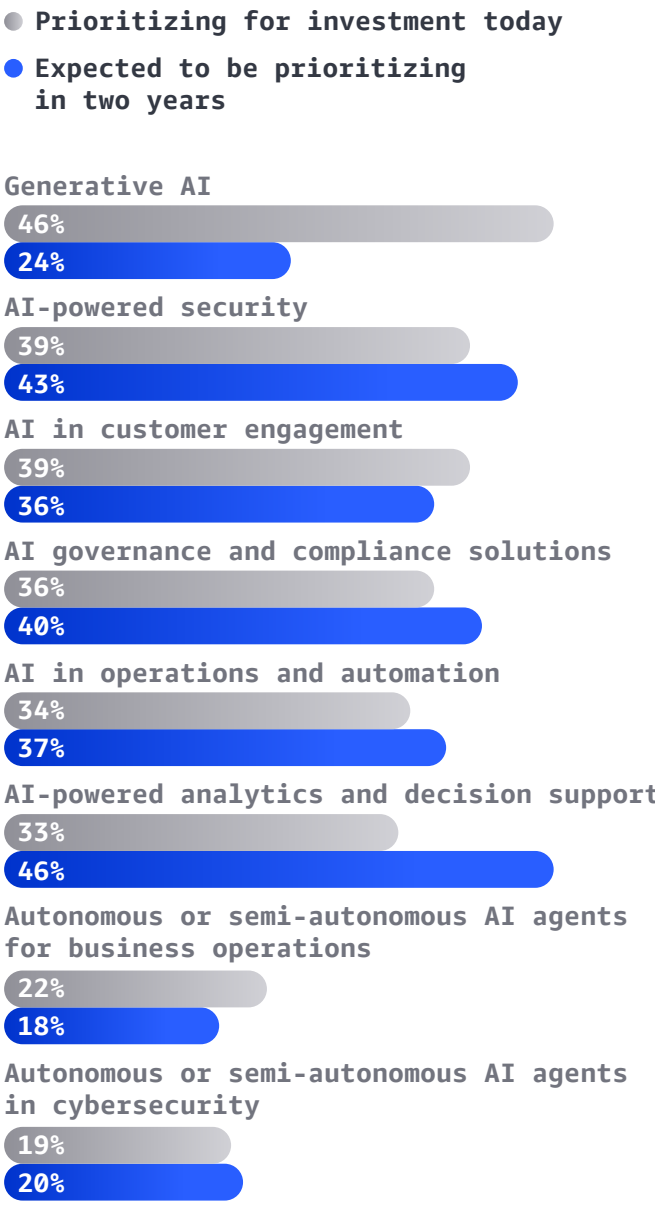
# From risk to ROI: A proactive attitude helps in achieving AI ambitions

Generative AI tools are leading to productivity gains and cost savings at the same time as executives are coming under growing pressure to do more with less. But when AI is led by business units rather than IT, experimentation can outpace governance.

Our research shows that organizations' focus for AI adoption is on productivity and automation instead of the less tangible work of building resilience, governance, and control.

Within two years, investments are expected to shift toward AI-powered analytics, with 46% expecting this to be a priority area. Considering the scale of risk exposure created by generative AI, it is concerning that AI-powered security and AI governance investments are only expected to rise modestly over the next two years.

## Generative AI is currently the top investment priority




Q Which of the following AI technologies is your organization prioritizing for investment today and which do you expect to prioritize in two years' time?

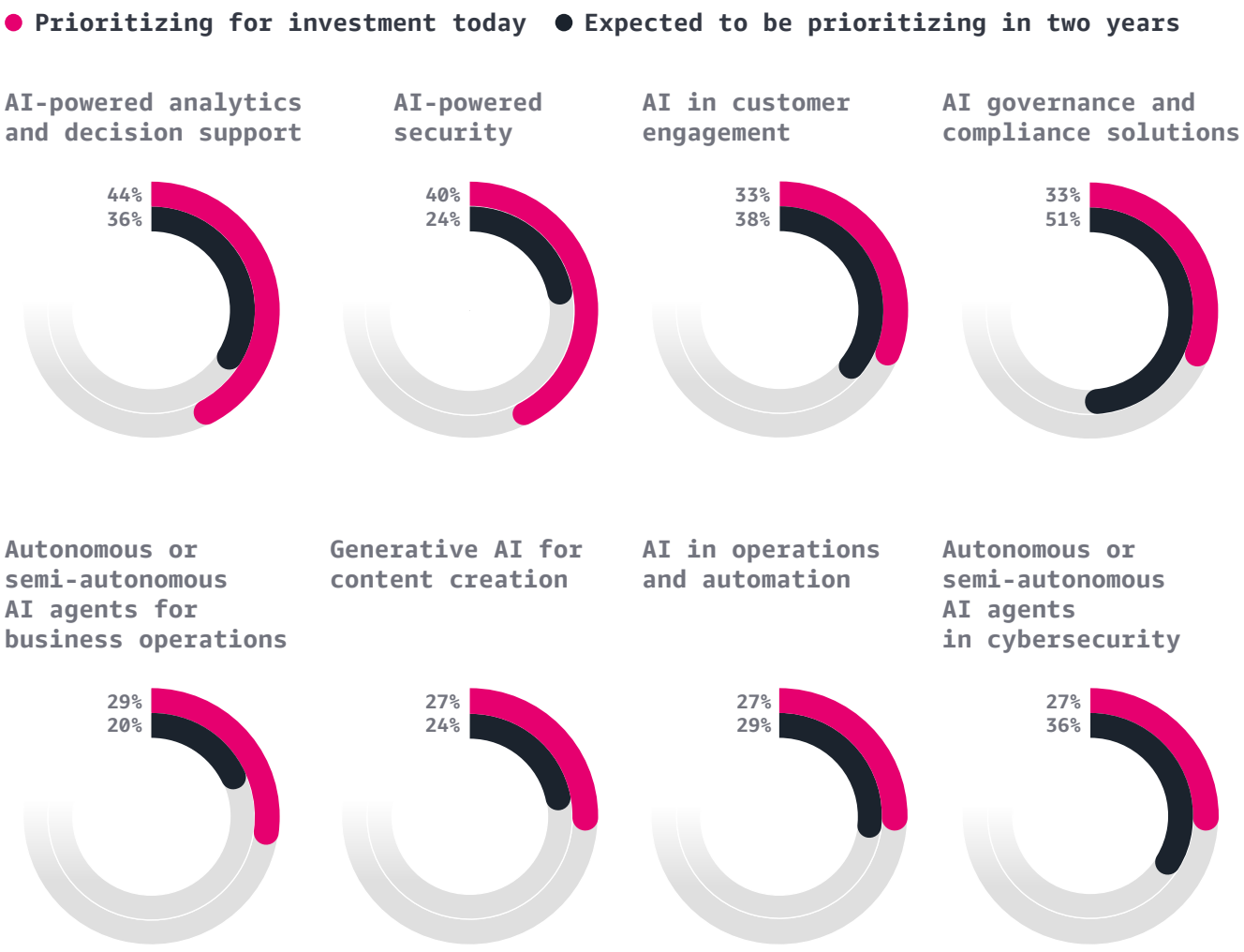
Total n=500

## Leading organizations match their AI ambitions with targeted investment in security

Security frontrunners are different: They are embedding security by design. In these organizations, investment in AI-powered security far outweighs investment in generative AI (40% are prioritizing these technologies for investment, compared with 27% of security laggards).

Within two years, 51% of security frontrunners expect to be prioritizing investment in AI governance and compliance solutions. This leads all other investment areas by 13 percentage points.

## Security frontrunners are looking ahead to better governance




Q Which of the following AI technologies is your organization prioritizing for investment today and which do you expect to prioritize in two years' time?

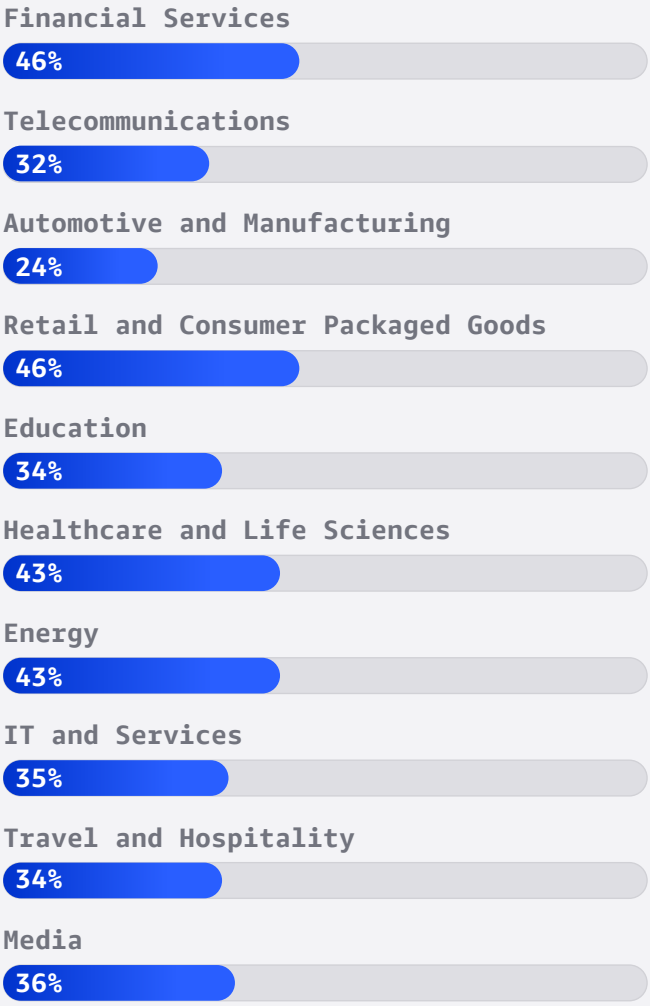
Security frontrunners n=45

## In highly regulated industries, compliance obligations are shaping AI maturity

Healthcare, energy, and financial services organizations are taking a more structured approach to scaling analytics and decision support by prioritizing governance and compliance from the start. This sequencing is building confidence in AI capabilities: Other than healthcare, organizations in these industries are most likely to be very confident that they have the right security foundations to adopt AI innovations as they emerge.

“Companies in financial services, healthcare, and life sciences, and so on, all made security investments ahead of generative AI hitting the scene because they had to comply with various regulatory standards,” explains Clarke Rodgers at AWS Security. “Security, regulatory, and data governance controls are already part of their core operating model, so they were far better placed to start experimenting.”

### "We are prioritizing AI governance and compliance solutions"




Q **Which of the following AI technologies is your organization prioritizing for investment today?**

Financial Services n=50, Telecommunications n=50, Automotive and Manufacturing n=50, Retail and CPG n=50, Education and Nonprofit n=47, Healthcare and Life Sciences n=40, Energy n=44, IT and Services n=49, Travel and Hospitality n=41, Media n=50

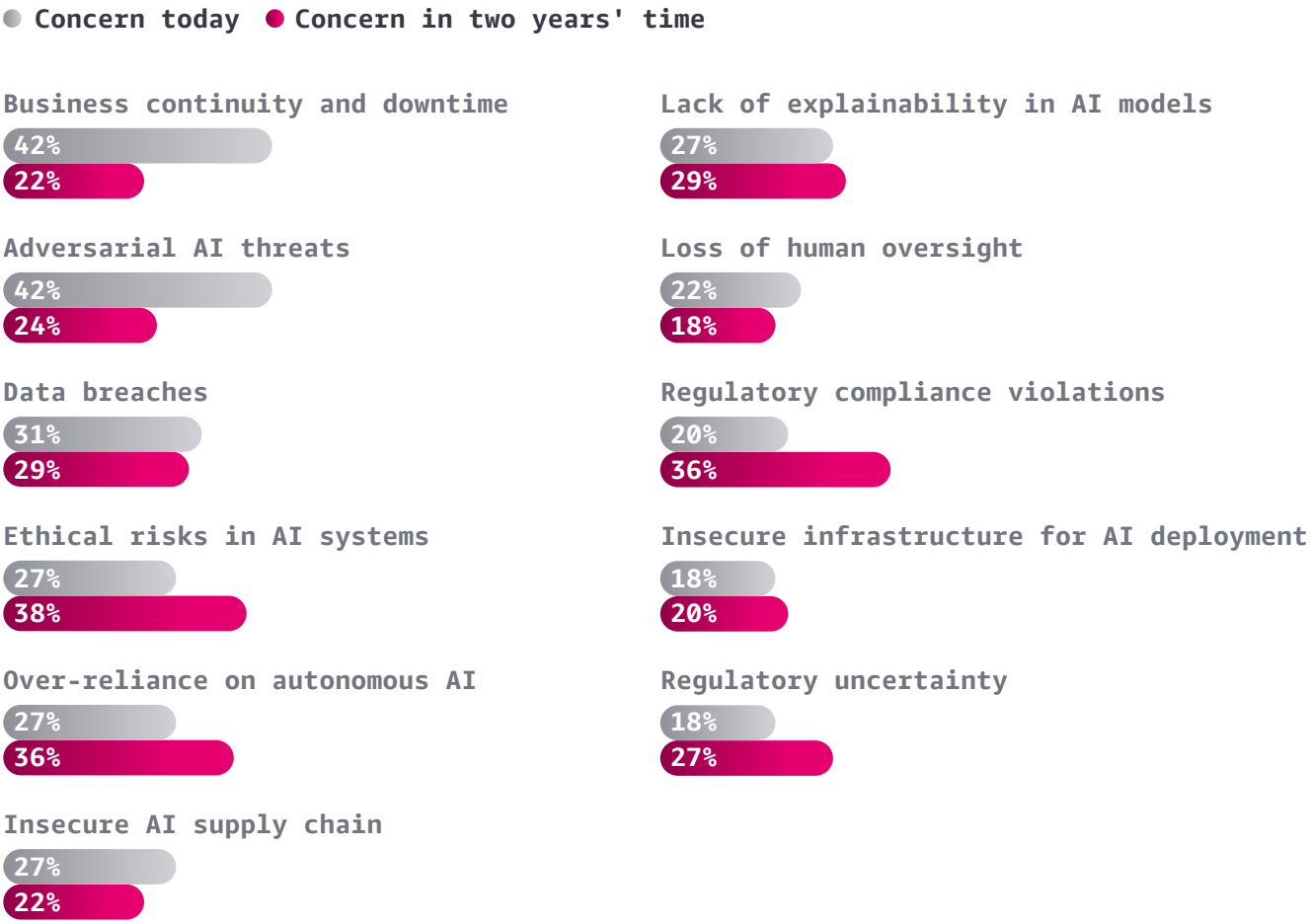
> “Security, regulatory, and data governance controls are already part of their core operating model, so they were far better placed to start experimenting.”
>
> **CLARKE RODGERS**
> **Office of the CISO, AWS Security**

## Strong foundations today enable better risk management tomorrow

By 2027, security frontrunners expect to have implemented solutions that address their immediate challenges. This will allow them to shift their focus toward issues arising from emerging AI technologies.

For example, business continuity and downtime and adversarial AI threats are security frontrunners' top concerns today (42% each), but these drop by 20 percentage points and 18 percentage points, respectively, in two years. Their future concerns are bias, fairness, and ethical risks; over-reliance on autonomous AI systems; and regulatory uncertainty around AI use.

### Security frontrunners are securing themselves by tackling threats now

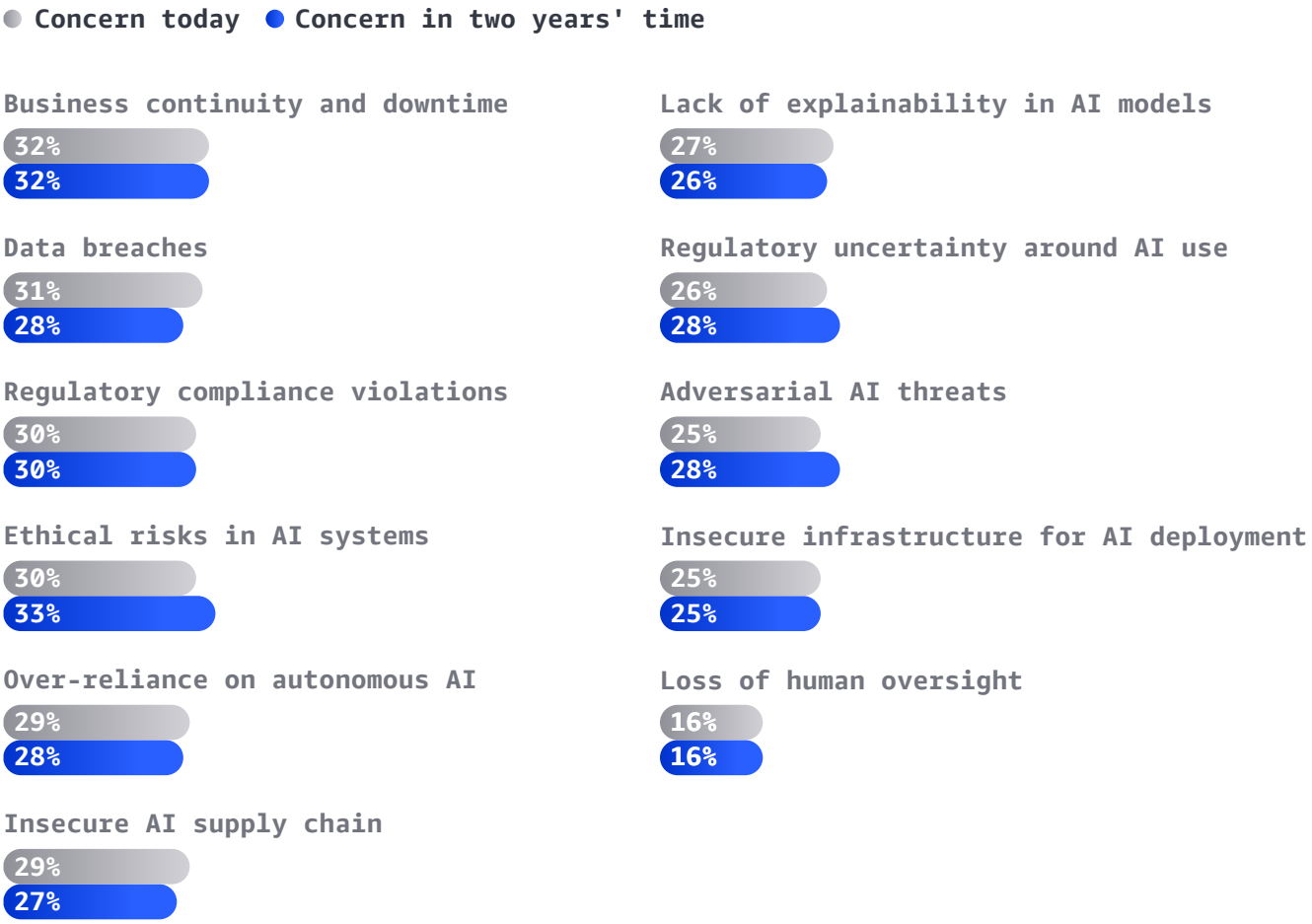



Q What are your primary cybersecurity concerns relating to AI adoption in your organization today? And in the next two years?

Security frontrunners n=45

Security laggards need to more quickly shift their focus from perimeter protection to AI model integrity, data provenance, and resilience. But when it comes to setting priorities or planning for more robust frameworks that help address the issues, security laggards are at a standstill. The top areas of focus today are resolving business continuity and downtime from AI failure, regulatory compliance failures, and data breaches (all 31%). But similar numbers expect these issues to still be a problem in two years' time–and it's a similar story across all areas. This lack of movement indicates low confidence in their ability to build resilience.

## Security laggards are at a standstill when it comes to resolving key concerns




Q What are your primary cybersecurity concerns relating to AI adoption in your organization today? And in the next two years?

Security frontrunners n=45

# Security starts at the top: Scaling AI securely depends on leadership

Human cooperation underpins the successful adoption of technical tools or strategic frameworks, and it will be critical for building an effective cybersecurity culture. When executives from across the business see security as an enabler of competitive advantage, they will find it easier to secure the necessary levels of investment.

Security frontrunners recognize this. Their three top priorities for the next 12 months are empowering the CISO (56%); investing in secure cloud, data, and infrastructure (56%); and ensuring executive leadership commitment (53%).

Security laggards, however, are jumping ahead without achieving executive alignment. Their top three priorities are investing in secure cloud, data, and infrastructure (45%); strengthening compliance and governance (42%); and developing ethical AI implementation frameworks (39%). Only 34% of business executives (compared with 40% of IT executives) in security laggards say that empowering the CISO with authority, resources, and accountability is a top-three priority.

Our data shows why leadership alignment matters. Nearly twice as many security frontrunners (42%) say that leadership accountability is their most effective AI security measure, compared with 22% of security laggards.

The next most effective AI security measures for security frontrunners are continuous monitoring and testing of AI systems (36% compared with 26% of security laggards), and automated safeguards integrated into AI workflows (33% compared with 27%). This is encouraging: it aligns with their main business concerns and shows that executive buy-in leads to a more targeted strategy.

The top three priorities for security frontrunners are:

56%
empowering the CISO

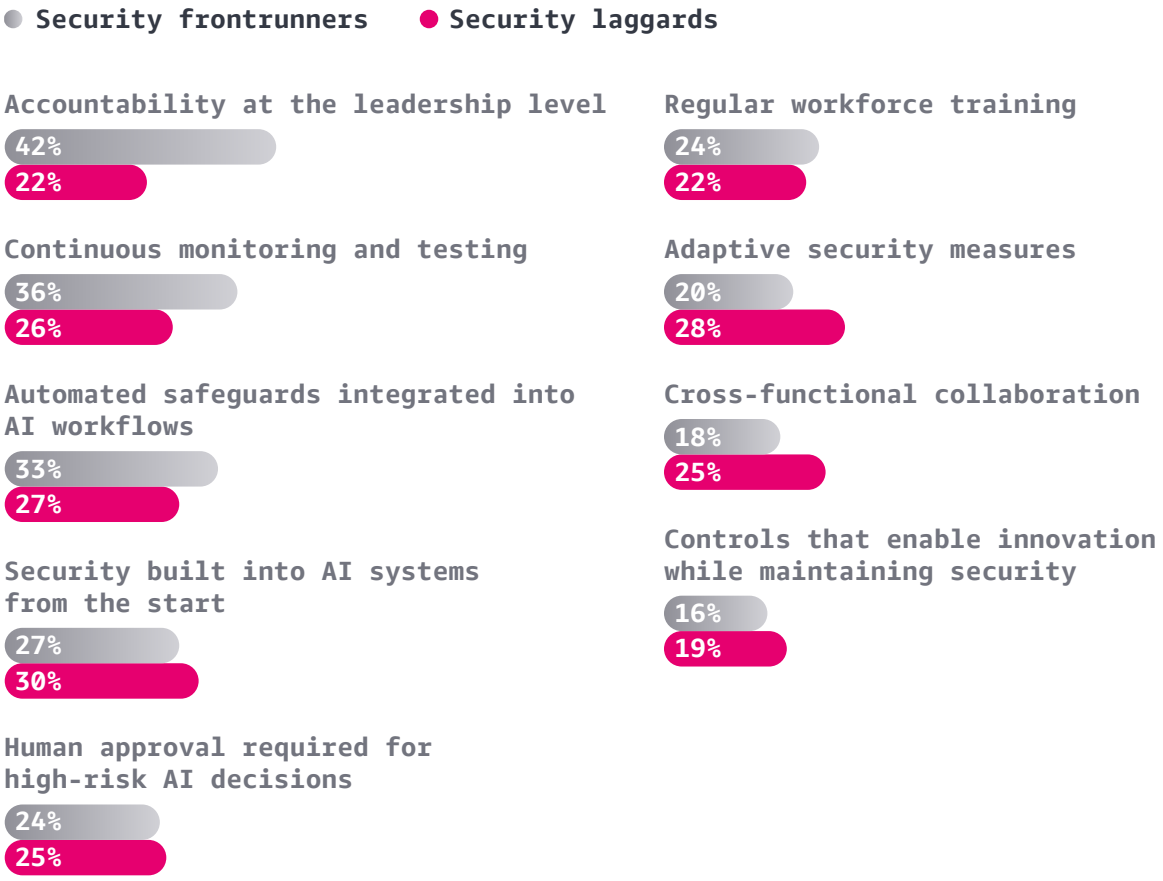
56%
investing in secure cloud, data, and infrastructure

53%
ensuring executive leadership commitment

But even the security frontrunners have work to do. Like security laggards, they need to extend their focus beyond leadership to the broader workforce. Only about one in four (24% of security frontrunners and 22% of security laggards) say that workforce training is an effective security measure, and both groups admit that they are struggling to successfully implement cross-functional collaboration and controls that enable them to innovate while maintaining security.

Clarke Rodgers from AWS Security recommends educating the workforce to see security as a competitive advantage and then empowering them with the tools to do their jobs more efficiently. "Training programs expand security reach and embed security as close to the problem as possible," says Rodgers. "For product teams, security insights can reduce friction and allow them to launch new features faster. So security allows them to be more innovative, to pivot much more quickly to business demands, and to hopefully outperform competitors."

## Security frontrunners are more positive about their leadership's accountability




Q Based on your experience, which AI security measures seem to be working well in your organization?

Security frontrunners n=45; Security laggards n=455

# Lay the groundwork now: AI agents are transforming security

"With the promise of AI and agentic AI, we are going to see security teams automate a lot more," says Clarke Rodgers from AWS Security. "Human oversight will still be needed, but we are going to see IT leaders coming to the C-suite table with ideas about how to take products or services to market more quickly because they are not worried about the basics."

This is a sentiment that comes out in our data. Half of all organizations (49%) expect autonomous AI security agents to be playing a central role in day-to-day security operations by 2027—up from 9% who say this today. And more than half (54%) plan to reduce their reliance on human security personnel as AI agents become more capable.

Our research also underlines the power of executive sponsorship in accelerating AI disruption within the enterprise. About two-thirds of early adopters—those who say autonomous AI security agents already play a central role in security operations — say they are prioritizing executive leadership commitment (63%) and that the CISO will be empowered with authority, resources, and accountability (65%).

Security frontrunners, which are more likely to have business alignment in place, are starting to implement their future vision for security operations. These organizations are most likely to say that the greatest potential lies in AI security agents' ability to free up security teams for higher-value work (42%, compared with 16% of security laggards) and provide advanced protection against AI-powered threats.

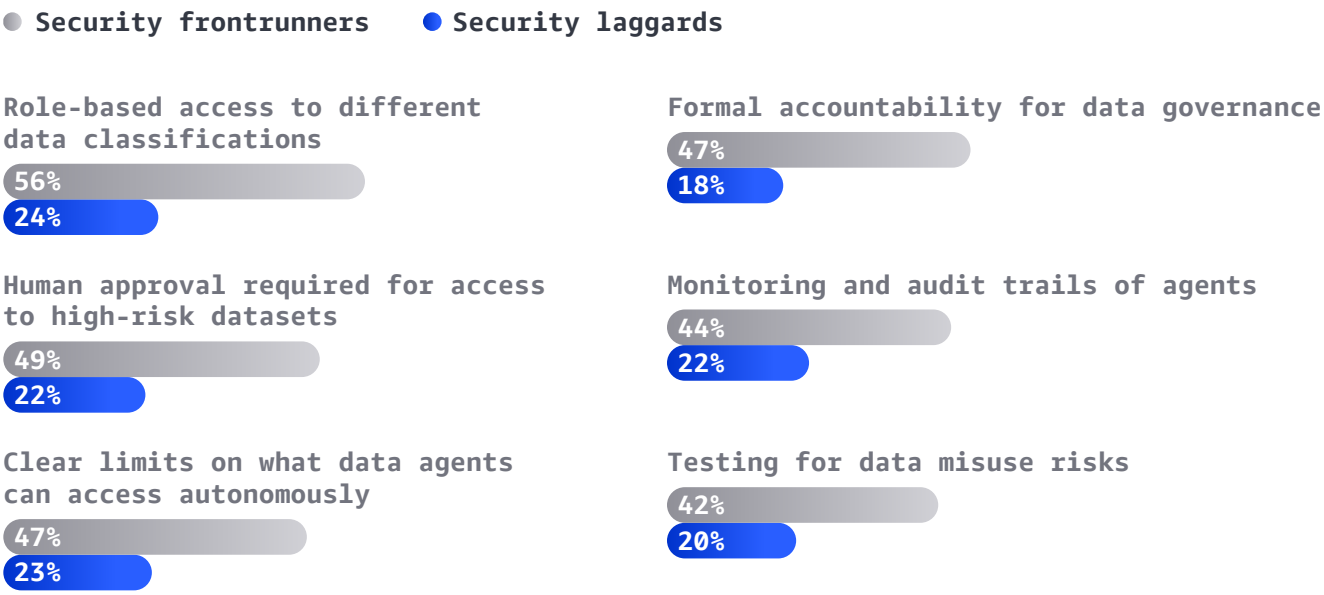
"Human oversight will still be needed, but we are going to see IT leaders coming to the C-suite table with ideas about how to take products or services to market more quickly because they are not worried about the basics."

**CLARKE RODGERS**
**Office of the CISO, AWS Security**

Allowing autonomous AI security agents to take on human tasks will demand robust data security and governance processes, according to Clarke Rodgers at AWS Security. “I would challenge any security organization if they are going to give anyone, human or non-human, unrestricted access to anything,” says Rodgers. “Even when you are completely comfortable with an agent doing a process for you, you need to have routine checks to make sure that the outcomes that you expected are still the outcomes and that the agent does not have more access to things than it should have.”

Security frontrunners show how to prepare for this new way of working: 56% say they have fully implemented role-based access to different data classifications, compared with 24% of security laggards that say this. And nearly half (47%) have already defined clear limits on what data agents can access autonomously, compared with 23% of security laggards.

## Security frontrunners provide guidance on how to prepare for autonomous AI security agents




Q To what extent has your organization put the following data governance controls in place for autonomous or semi-autonomous AI security agents?

Security frontrunners n=45; Security laggards n=455

CONCLUSION

# From innovation to impact: Security powers growth in the AI economy

The transition to autonomous AI is reshaping the risk landscape, and security is evolving in tandem with innovation. Organizations that build a security culture based on robust cybersecurity tools, leadership empowerment, and data governance are moving faster on AI adoption.

The security frontrunners in our research are treating resilience as a business growth strategy. These organizations have more freedom to experiment with AI and scale and adapt it safely because they are confident that security foundations are in place. They are setting the pace on AI, and growth is their prize.

## Five ways to compete with security leaders:

01

IT executives should align with the business to define what secure innovation looks like. This ensures that security becomes a shared strategic enabler and that future AI initiatives are developed with resilience built in from the start.

02

Identify and prioritize today's risks but plan for new ones. The security frontrunners show that organizations can tackle current concerns, such as data breaches and downtime, while preparing for new risks that come with self-directing systems.

03

Empower the CISO and hold the C-suite accountable. To fully embed change management processes, security frontrunners should evolve from technical guardians to business strategists. Equipping CISOs with clear authority, resources, and board-level accountability ensures that security and innovation advance together.

04

Strengthen data governance foundations to be ready for security transformation with autonomous AI. Robust data governance is the cornerstone of trusted AI. As autonomous systems become more capable, it is critical to establish clear rules about who (or what) can access, modify, and act on data.

05

Make security cultural. An organization cannot achieve resilience through policies alone. Building a proactive security culture means embedding awareness, shared responsibility, and continuous learning into every function. It means shifting from compliance-driven activity to a mindset where every function sees resilience as part of innovation.

# About the research

The data in this report comes from a global survey commissioned by AWS and conducted by FT Longitude in September 2025.

There were 500 respondents across Financial Services, Industrial, Media and Entertainment, Health, Automotive, Retail, Travel and Hospitality, Technology, Telecommunications, Education, and Government sectors. Respondents were based in Australia, Brazil, Canada, France, India, Japan, the UK, and the US.

In addition to this quantitative research, FT Longitude carried out two in-depth qualitative interviews with Clarke Rodgers and Tom Godden from AWS. We thank them for their insights.

This report was produced by

FT LONGITUDE