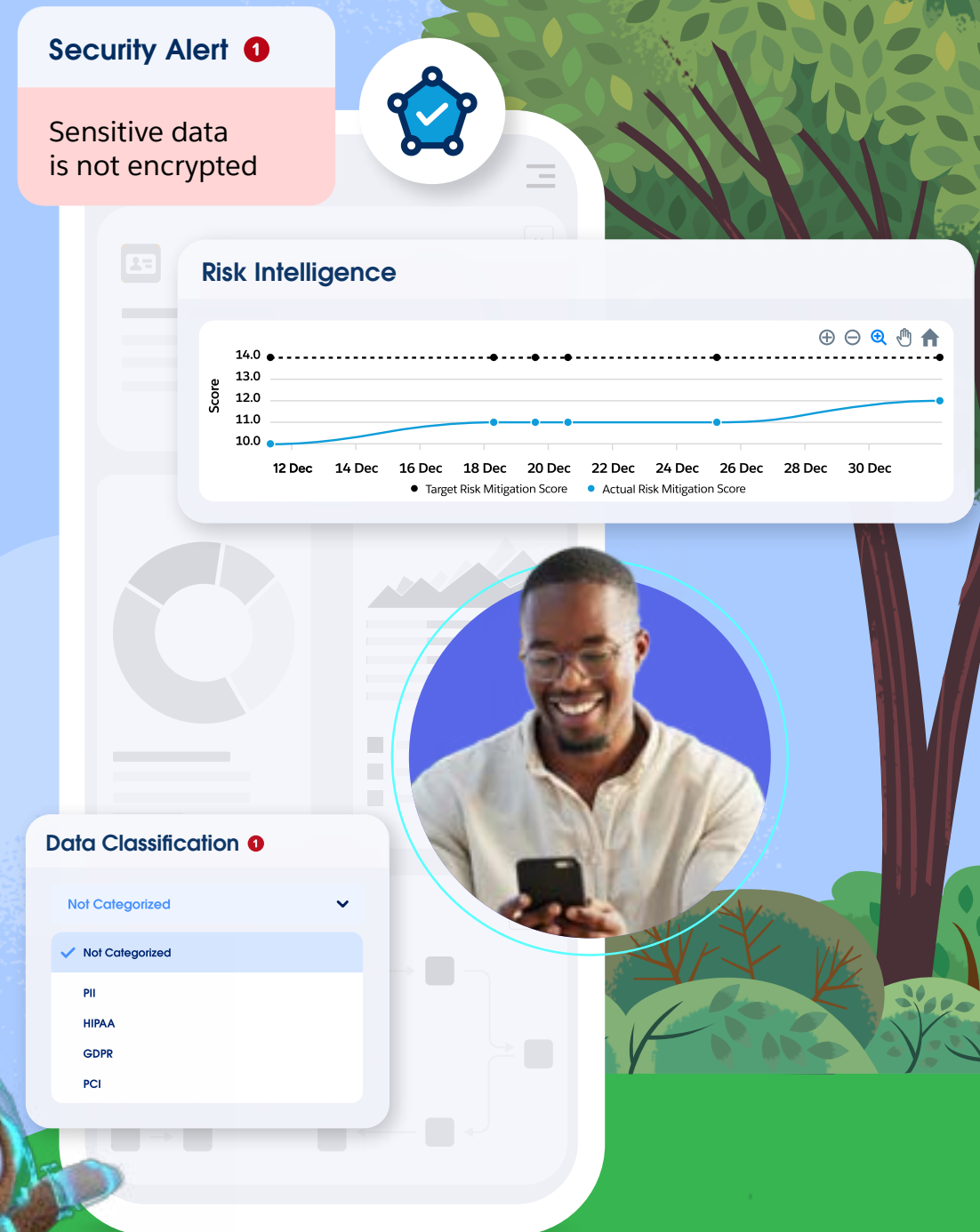




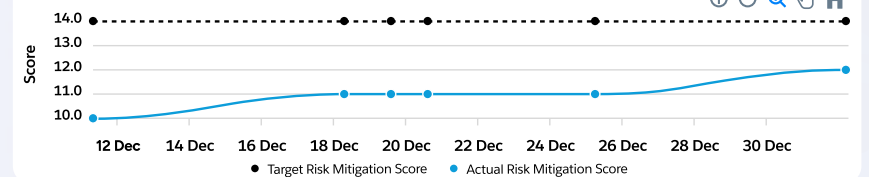
FOURTH EDITION

State of IT: Security

Insights and trends from 2,000+ security, privacy, and compliance leaders in the agentic AI era.



Risk Intelligence



Data Classification

Not Categorized

✓ Not Categorized

PII
HIPAA
GDPR
PCI

A Note From Salesforce on Security

Data security has taken center stage in today's AI landscape, and not just because threats are growing more complex. IT and security leaders are walking a tightrope – on one side, they must protect the organization from everything from ransomware to data poisoning, and on the other, they're under pressure to fuel innovation in an era where AI and automation are integral to staying competitive. Striking that balance can feel like trying to solve a puzzle while the pieces keep shifting.

What's clear is that data security isn't just a checking-the-box exercise. It's the catalyst for trust and innovation – both within your organization and with your customers. Our survey of over 4,000 IT leaders worldwide, including more than 2,000 responsible for global security, privacy, and compliance, shows that developing a strong security posture can do more than safeguard data – it enables new possibilities. We heard stories of teams using AI to spot threats earlier, automate compliance tasks, and ultimately free up employees to focus on more strategic initiatives. But we also uncovered very real challenges: regulatory complexity, uneven adoption of AI governance, and a trust deficit with customers wary of how their data is being handled.

This report captures the perspectives of your peers across industries and geographies who are wrestling with the same high-stakes challenge. We hope is that these insights inspire you to see security not just as a defensive shield but as a launchpad for innovation. Here's to protecting what matters – and creating new opportunities in the process.

























What You'll Find in This Report

Salesforce surveyed over 4,000 IT decision-makers worldwide, including more than 2,000 professionals specializing in security, privacy, or compliance, to uncover key insights on:

- **Evolving threats and growing security priorities:** Why security and compliance remain top concerns and how organizations are maturing their defenses.
- **Building customer trust in an AI-driven world:** How robust security measures can instill confidence with customers and stakeholders.
- **Leveraging AI to strengthen security postures:** Exploring how AI agents and advanced technologies enhance detection, response, and resilience.

Unless cited otherwise, data in this report is from a double-anonymous survey conducted from December 24, 2024, through February 3, 2025. This survey yielded 4,275 responses from IT decision-makers, with 2,138 focusing on security, privacy, or regulatory compliance, across North America, Latin America, Asia-Pacific, and Europe. See page 25 for full survey demographics.

Due to rounding, percentages may not always total 100%. All comparison calculations use unrounded figures.

 Australia [†]	 Belgium	 Brazil
 Canada	 Denmark [†]	 Finland [†]
 France	 Germany	 India
 Ireland	 Italy	 Japan
 Mexico	 Netherlands	 New Zealand [†]
 Norway [†]	 Portugal	 Singapore
 South Africa	 South Korea	 Spain
 Sweden [†]	 Switzerland	 United Arab Emirates
 United Kingdom	 United States	

2,138 security, privacy, and compliance decision-makers surveyed worldwide

^{† ‡} Single Sample Groups

Contents

Executive Summary 05

Chapter 1: Introduction 06

Chapter 2: Security in the Age of Agentic AI 11

Chapter 3: Governing Agentic AI 15

Chapter 4: Building Customer Trust in the Agentic AI Era 20

Salesforce's Take 23

Survey Demographics 25



Executive Summary

IT leaders today face growing complexity due to escalating cyber threats, rapid AI advancements, and evolving regulations. Organizations are increasing security investments to counter threats like ransomware and data poisoning.

Strong security practices enable innovation. Companies proactively integrating security through DevSecOps and advanced threat detection report greater confidence in adopting AI agents.

Compliance challenges continue to grow as the regulatory environment becomes more complex. Many organizations feel unprepared for the regulatory changes AI will bring, highlighting the need for clearer guidelines and proactive governance. Rising customer expectations for data transparency further underscore the importance of solid data security practices.

AI presents both opportunities and risks. While it enhances capabilities in threat detection and automation, it also introduces concerns around data privacy and bias. Navigating this effectively requires comprehensive governance, proactive risk management, and transparent AI processes.

- 1 Security budgets on the rise:** 75% of organizations anticipate budget increases to address everything from data poisoning to more advanced threat detection.
- 2 Trust is paramount:** 64% of customers feel that companies are being reckless with their data, and 61% of them believe that AI advancements make it more important than ever for companies to protect their data, underscoring the importance of organizations to prioritize data stewardship.
- 3 Compliance is complex:** 68% of security leaders say that compliance has become more difficult as the regulatory environment changes swiftly, and 43% feel underprepared for potential AI-related regulations.
- 4 AI can strengthen defenses:** While 79% of security leaders believe that AI agents will introduce new security and compliance challenges, 80% of them believe that AI agents will also introduce new security opportunities.



1

Introduction



01

Security Budgets Grow to Address Evolving Threats and Defense Tactics

As cybersecurity threats intensify, many organizations are funneling more resources into their security programs. We're seeing more sophisticated attacks – ranging from cloud breaches to data poisoning – that require advanced defensive measures to counteract. In response, most IT departments anticipate growing their budgets in the coming year, with data encryption, data backup, and identity and access management topping the list of effective tactics.

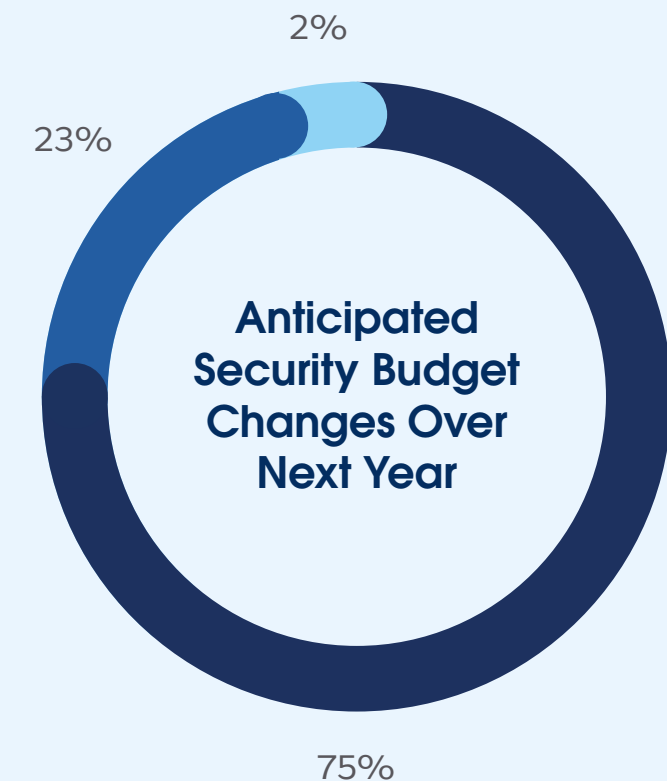
Most Concerning Security Threats

- 1 Cloud security threats
- 2 Data poisoning
- 3 Malware
- 4 Phishing
- 5 Ransomware

Most Effective Security Tactics

- 1 Data encryption
- 2 Data backup and restore protocols
- 3 Identity and access management
- 4 Zero trust strategies
- 5 Data masking

- Increase
- Stay the same
- Decrease



Strong Security Postures Enable Innovative Organizations

This surge in investment isn't solely about risk mitigation; a robust security posture enables teams to innovate with confidence. From adopting cloud-native solutions to experimenting with AI-driven tools, organizations feel safer launching new initiatives when they know their defense-in-depth strategy can keep pace with modern threats.

Balancing security and new technology implementations can be challenging, yet the most forward-thinking IT teams prove it's far from impossible. Our research shows that departments with strong security and governance practices also rank higher on measures of innovation, suggesting that structured, proactive defenses actually free teams to explore new ideas.

When security best practices, like encryption, backup protocols, and employee training, are woven into everyday processes, it becomes easier to experiment and scale without jeopardizing the integrity of systems or data.

IT Departments With Above-Average Innovation Compared to Others

+9% more likely to have above-average security and governance policies and practices

-19% less likely to have trouble balancing security and business objectives

+6% more likely to have above-average privacy policies and practices

+13% more likely to proactively train employees on security best practices

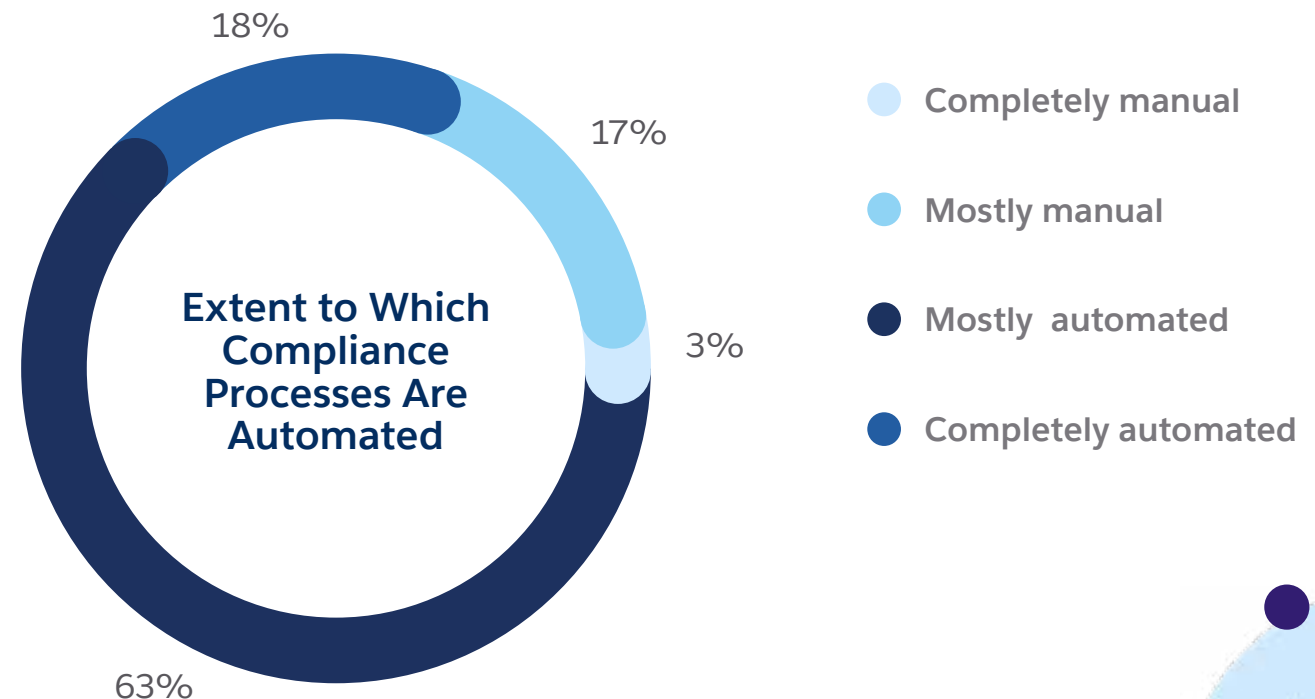
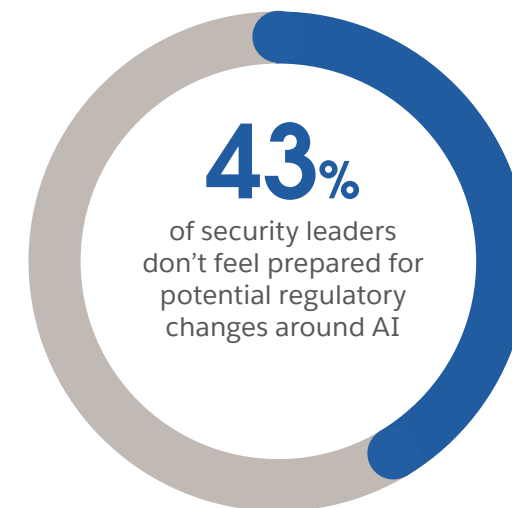
01

Compliance Becomes a More Difficult Endeavor

As organizations expand globally and new regulations emerge, compliance has grown increasingly intricate. Many security leaders say they're working harder to keep pace with requirements that vary by region or industry. Throw in the emerging rules around AI, and it's no wonder teams feel it's harder to keep up.

Compliance isn't merely about checking regulatory boxes. It also builds credibility with customers and stakeholders. While some compliance processes have become entirely automated, a significant portion still involve at least some manual effort, leaving room for error and inconsistent application across departments and geographies.

Regulatory Concerns Among Security Leaders



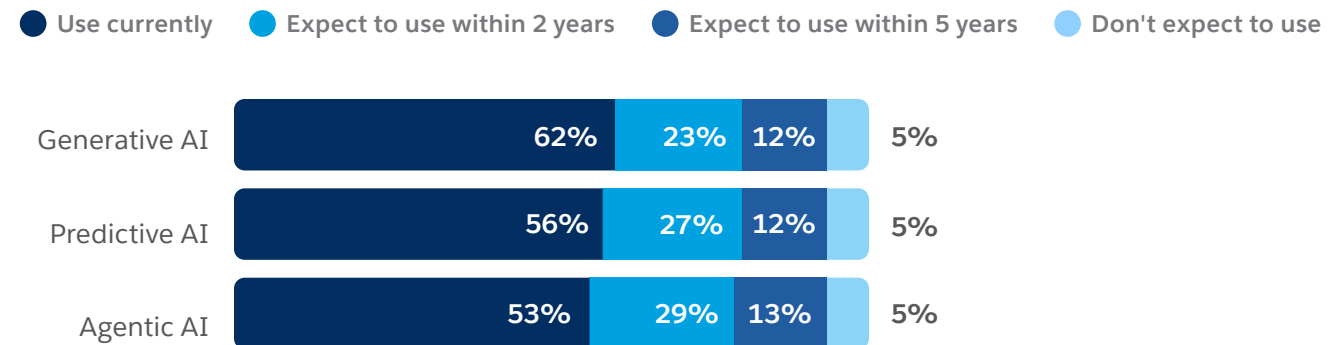
AI Brings Security Opportunities and Threats

The use of AI is already prevalent and only expected to grow in the coming years. The most recent wave of AI has brought us AI agents that can autonomously perceive, reason, and take actions to perform specific tasks, with either little or no human oversight. Security leaders acknowledge that without proper governance, AI agents may introduce new security and compliance challenges. It's no surprise then that CIOs rank security and compliance as their top AI concern – and the top criteria when selecting AI vendors.¹

However, security leaders also see AI agents offering powerful advantages and new opportunities when it comes to security and compliance. Built with the right skills, AI agents can enhance threat detection, automate vulnerability management, and support compliance efforts at scale. This dual reality calls for a two-sided strategy: leveraging AI to strengthen defenses while putting robust guardrails in place to manage its risks.

¹ Salesforce CIO Dilemma Research, October 2024.

IT Organizations' Use of The Following Types of AI²



² Percent based on all State of IT survey respondents (including developer and security decision-makers).

Security Leaders See Both Challenges and Opportunities with AI Agents



2

Security in the Age of Agentic AI



02

Teams Prepare for the AI Era's Evolving Threat Landscape

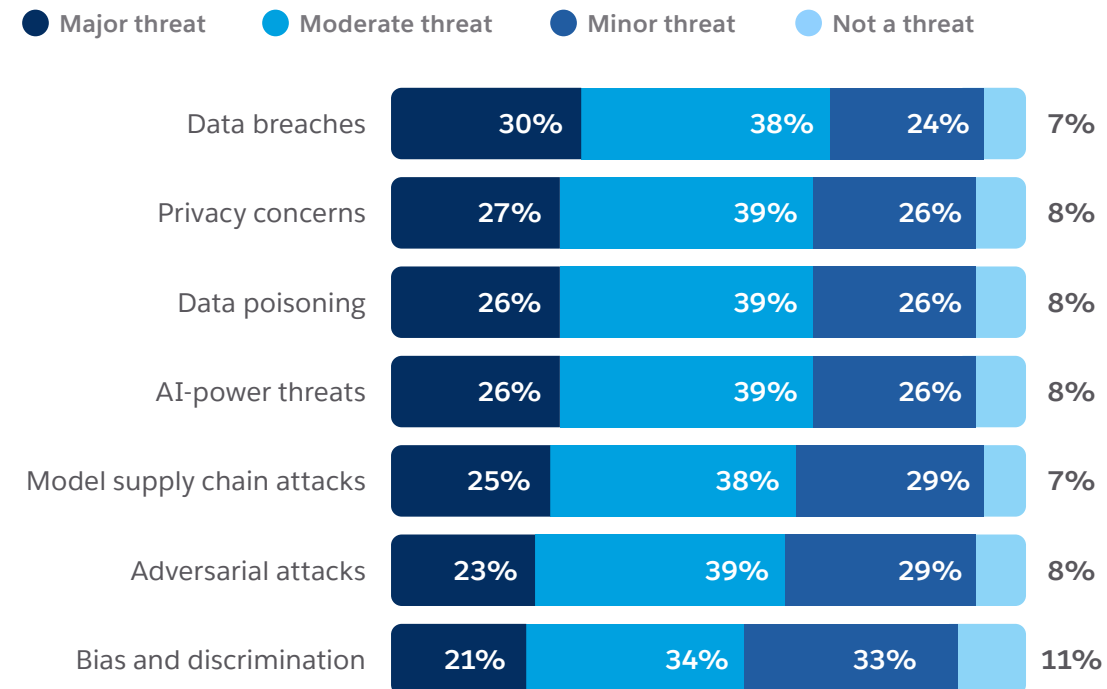
Security teams have long grappled with threats like malware and phishing, but AI has fundamentally changed the game. Cybercriminals are using AI to automate attacks at scale, while security leaders must defend an expanding perimeter that includes cloud infrastructure, remote work, and IoT devices. Most security leaders believe AI-driven cyber threats could soon outpace traditional defenses, underscoring the need for new tactics and continuous vigilance.

Effectively addressing these emerging threats requires a focus on building data resilience across the organization. This can include implementing strict access controls to limit exposure and ensure that only authorized personnel can access sensitive information. Proactive event monitoring is also a valuable tactic and can identify security threats using automation. As a last line of defense, having a backup solution in place can help organizations build resilience by ensuring users always have accurate, up-to-date data.

75% of security leaders believe AI-driven cyber threats will soon outpace traditional defenses

79% believe their security practices must transform as AI use increases

How Security Leaders View the Following Threats As AI Use Increases



How AI Agents Can Help Increase Data Security

AI agents don't need to add complexity – they can be formidable security allies. These agents can rapidly parse vast amounts of data to detect abnormal patterns, automate routine tasks like patching or compliance checks, and expedite the analysis of potential threats. Many security leaders believe that AI agents can help them scale their defense-in-depth strategy.

A few ways AI agents can strengthen security and compliance:

- **Threat detection and response:** Flagging unusual activity and coordinating incident remediation with minimal delay.
- **Model bias identification:** Continuously auditing AI models for biases and vulnerabilities, ensuring fairness and reliability.
- **Compliance automation:** Tracking policy adherence across systems, reducing manual oversight.


By offloading repetitive or high-volume tasks to agents, teams can redirect their focus toward higher-level strategy – an essential shift when threats proliferate faster than most security teams can keep up.



100%

of security leaders believe AI agents can improve at least one security concern

Top Security and Compliance Improvements Expected From AI Agents

- 1 AI model performance auditing and tracking
 - 2 Threat detection
 - 3 AI model bias identification and mitigation
 - 4 Real-time event monitoring
 - 5 Anomaly detection / behavioral analysis
- 

Spotlight: DevSecOps

Security risks aren't just confined to live environments – it's important to secure development environments as well. Vulnerabilities introduced during development can have just as big an impact on an organization's security posture, especially as they scale AI.

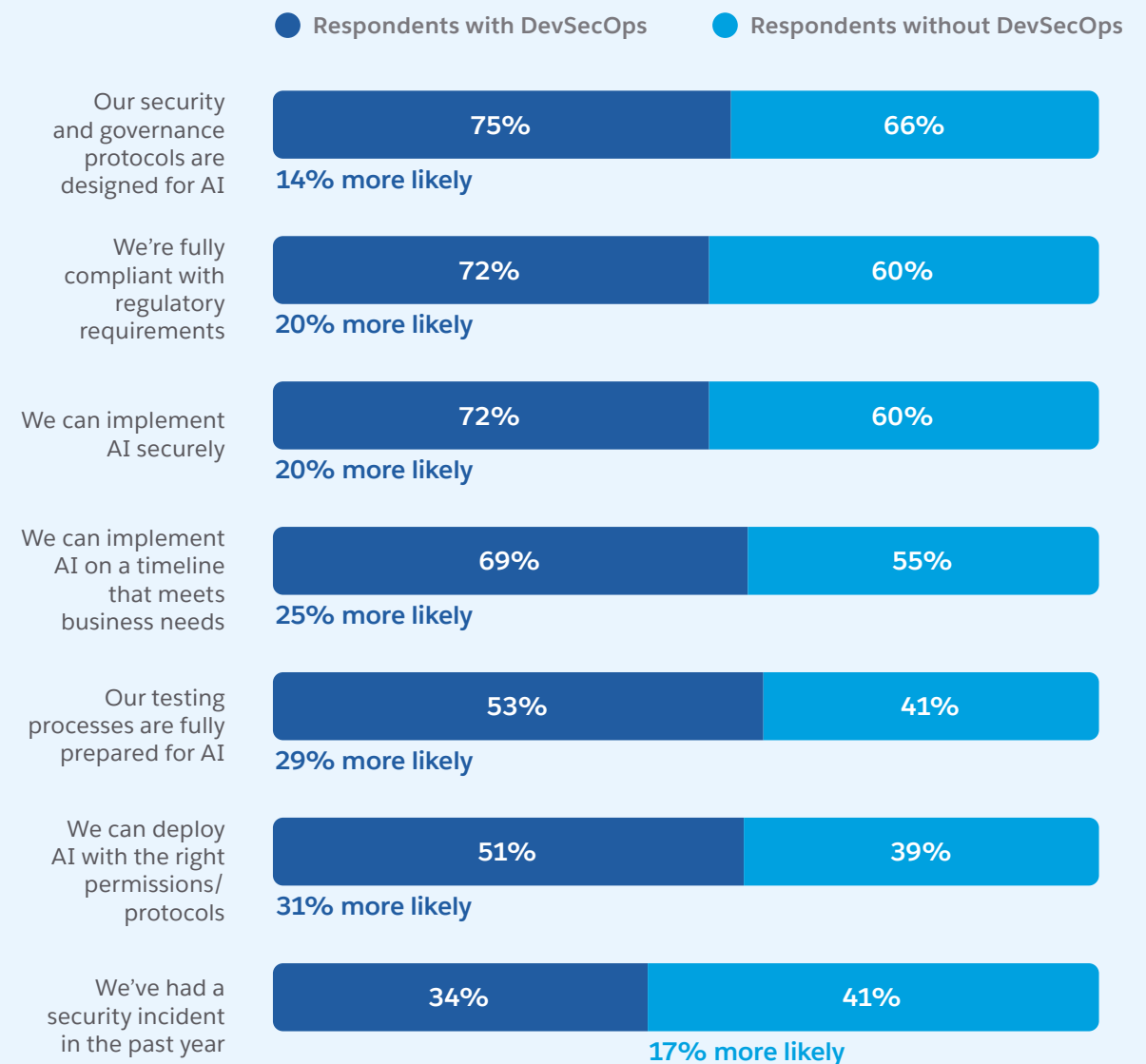
DevSecOps seamlessly integrates security into every stage of the development lifecycle. Rather than waiting to address vulnerabilities at the eleventh hour, DevSecOps embeds security scanning, compliance checks, and remediation processes from initial design through deployment.

This proactive approach is invaluable for security teams entering the AI era. Many IT leaders expect increased confidence when rolling out AI agents or advanced analytics because potential vulnerabilities are identified early and often. DevSecOps is designed to accelerate collaboration between development, security, and operations teams, with the goal of reducing patch times and last-minute surprises, while increasing overall trust in the systems that power AI-centric businesses.

85% of IT organizations follow a DevSecOps model

IT Leaders Who Agree with the Following Statements¹

Orgs with DevSecOps vs. Orgs Without



¹ Percents and calculations based on all State of IT survey respondents (including developer and security decision-makers).

3

Governing Agentic AI



03

AI Agent Compliance and Governance is a Work in Progress

Any emerging technology – from cloud computing to AI – introduces questions of governance and compliance. While many organizations have strong policies for traditional infrastructure, fewer have matured the frameworks needed for AI agents. This gap often stems from unclear regulations, siloed systems, and reliance on manual processes.

With 55% of security leaders not feeling fully confident that they can deploy AI agents with the right guardrails and 53% not fully confident that they can deploy AI agents that are in compliance with regulations and standards, this is an area where many organizations have room to improve.

Security Leaders Who Are Fully Confident in the Following

We have the quality data to underpin AI agents 48%

We can deploy AI agents with the right permissions/ access protocols 48%

We can deploy AI agents in full compliance with relevant regulations and standards 47%

We can audit AI agents to protect against bias 45%

We can deploy AI agents with the right guardrails 45%

Our employees know how to responsibly manage data used for AI agents 41%



03

Accountability for AI Governance Takes Shape Across Organizations

Who oversees AI ethics, privacy, security, and compliance in the face of shifting regulations and high-stakes outcomes? Do you have security, privacy, and compliance protocols specific to AI in place? These are critical questions facing organizations implementing AI today. While there is still room for improvement, over 70% of security leaders say they already have AI security and privacy protocols in place and 64% have clearly defined roles and responsibilities around AI development and governance.

Security Leaders Who Agree With the Following Statements

We have security and governance protocols specific to AI

72%

We have privacy protocols specific to AI

71%

We have compliance protocols specific to AI

69%

We have clear roles and responsibilities around AI development and implementation

64%

03

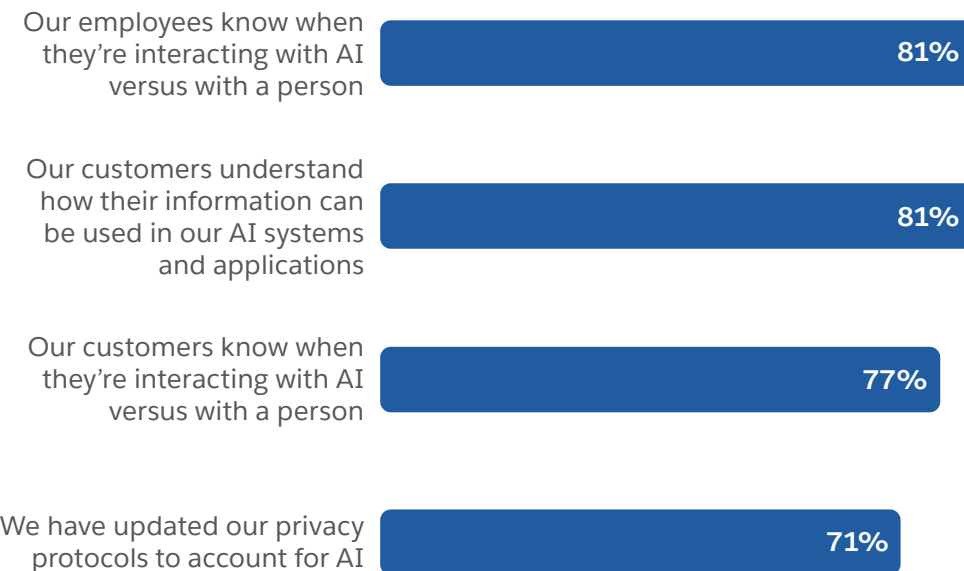
Transparency is Essential for Building Trust in AI

Customers and regulators increasingly demand to know how data is being used, especially when AI is involved. Transparency is not a “nice-to-have” – it’s the bedrock of trust. According to Salesforce research, 42% of customers say that transparency into how AI is used would increase their trust in AI. Another 31% say that explainability of AI outputs would boost their trust.¹

The good news is that this seem like an area where many organizations are doing well. Over three-fourths (77%) of security leaders believe customers are aware when they are engaging with AI versus a person, and 81% believe customers understand of customers understand how their information can be used by an organization’s AI systems and applications.

¹ Salesforce State of the AI Connected Customer, October 2024.

Security Leaders Who Agree With the Following Statements²



² Base: Respondents at organizations with AI.



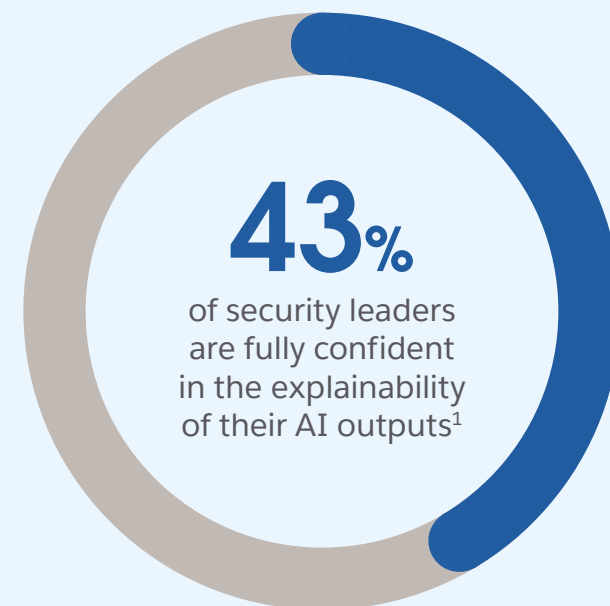
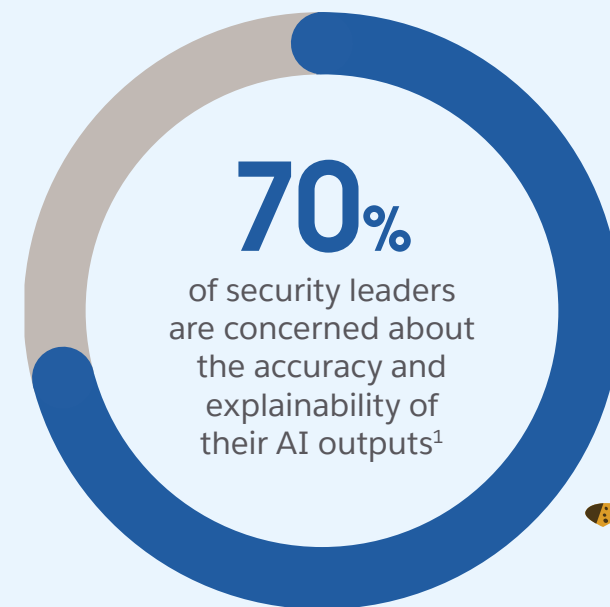
"By prioritizing security in our AI tools and applications, we're not only protecting our internal systems, but also building trust with our customers. Transparency and strong security measures give our customers the confidence that their data is handled safely, even when interacting with AI-powered solutions."

ADAM HOOPER
HEAD OF CENTRAL PLATFORMS, DPD



Explainability is a Key Concern in AI Adoption

Beyond transparency lies explainability: the ability to articulate, step-by-step, how an AI application or agent processes data and arrives at its outputs. Among organizations actively using AI, 70% of security leaders feel that AI accuracy and explainability are a concern, and less than half are fully confident that they can explain AI outputs.



¹ Base: Respondents at organizations with AI.

4

Building Customer Trust in the Agentic AI Era



04

Suspensions Around Data and AI Underscore the Trust Imperative

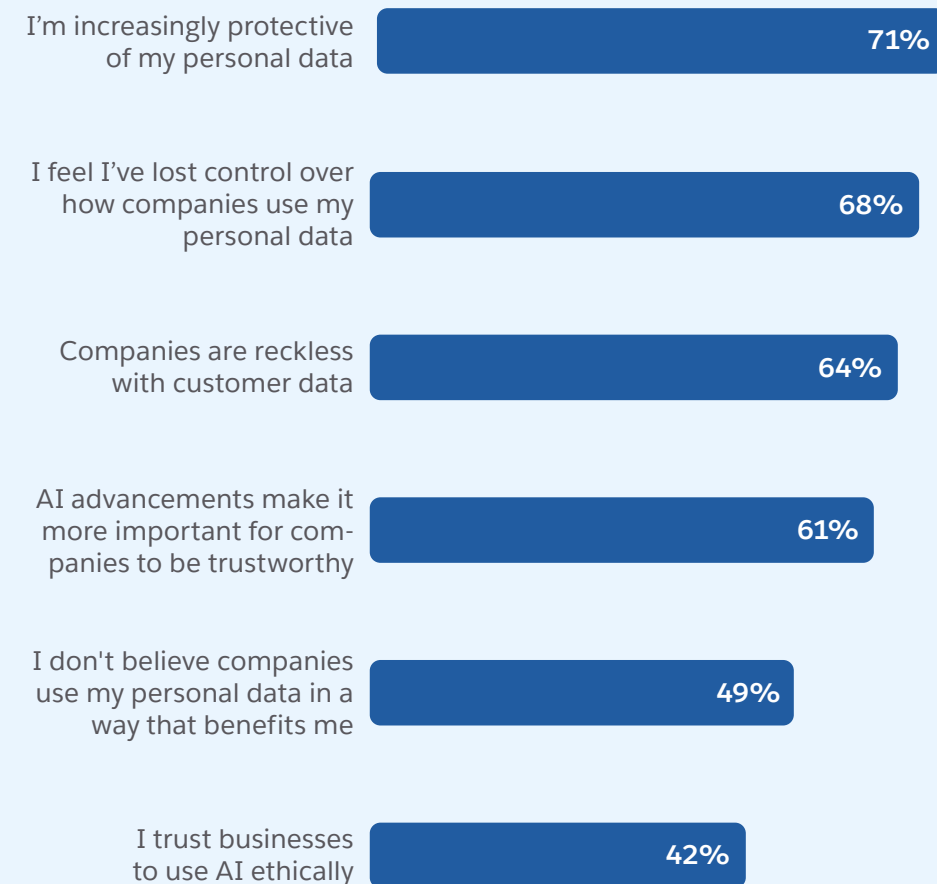
Customers increasingly question how their data is collected, stored, and used, especially when AI is involved. Customer trust in companies continues to fall. Over two-thirds of customers feel like they've lost control over how companies use their personal data, and nearly half feel like companies don't use their personal data in a way that benefits them.¹

As organizations expand the use of AI, including AI agents – along with the data that makes it work – this dynamic of trust, data, and AI between customer and companies will become more challenging.

However, there are steps that IT and security teams, who are at the forefront of AI-related trust-building efforts, can take to make this better. Customers say that as organizations are able to build protections to AI products, be transparent about AI usage, improve the accuracy of AI outputs, and take customer feedback, their trust in AI will increase.¹

71% of customers say their trust in companies is decreasing – up from 52% in 2023 and 47% in 2022¹

Customers Who Agree With the Following Statements¹



¹Salesforce State of the AI Connected Customer, October 2024.

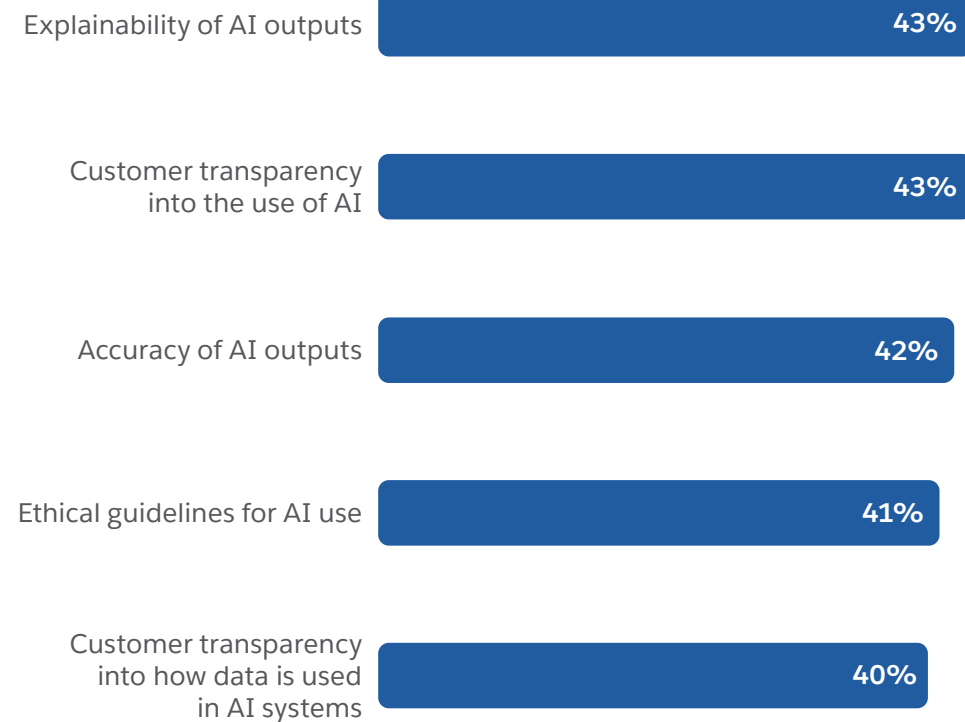
04

A Scorecard on Ethical and Transparent AI

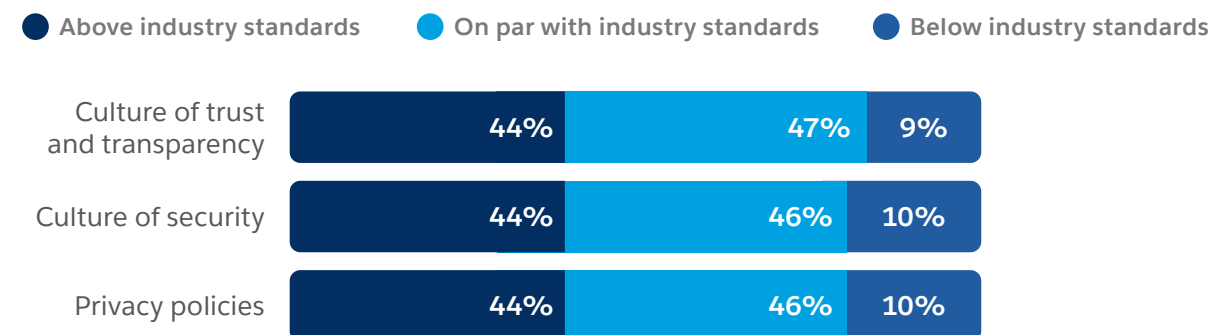
Security leaders are aligned with customers on the importance of transparent and ethical AI, but have work to do in bringing their practices and capabilities up to par. In fact, 64% of security leaders believe customers are hesitant to adopt AI services due to security or privacy concerns.

Where can organizations improve? While over 90% of security leaders feel like their organizations are on par with or above industry standards when it comes to privacy policies and their cultures around security, transparency, and trust, less than half feel like their organizations are excellent at providing explainability of AI outputs, accurate AI outputs, and transparency to customers on how their data is being used in AI systems.

Security Leaders Who Rate the Following at their Organizations as Excellent¹



Security Leaders' Self-Assessments of the Following



Salesforce's Take



Salesforce's Take

Security has evolved from a reactive function to an engine of strategic growth and innovation. As AI advances, forward-thinking IT leaders are building infrastructures that are equally adept at thwarting new threats and unlocking new possibilities. From bolstering threat detection to establishing stronger governance frameworks, the shifts occurring today will define how organizations operate and compete in the years to come.

Several trends are already shaping this future:

- 1 Ongoing regulatory complexity:** As AI regulations emerge across different regions, compliance management will be a continuous project.
- 2 Proactive AI adoption:** Companies that embrace AI agents as a security ally – rather than fear it – will discover new efficiencies and opportunities for differentiation.
- 3 Continual skill evolution:** Security roles will keep transforming, demanding new proficiencies in AI oversight, data governance, and ethical decision-making.

At this pivotal moment, aligning security objectives with broader business goals will help organizations stay resilient amid change. By focusing on trust, transparency, and robust security measures, IT leaders can turn potential vulnerabilities into competitive advantages, paving the way for a more secure, agile, and innovative future.



Survey Demographics



Survey Demographics

Country

Australia	N=64, 3%
Belgium	N=50, 2%
Brazil	N=100, 5%
Canada	N=100, 5%
France	N=100, 5%
Germany	N=100, 5%
India	N=100, 5%
Indonesia	N=75, 4%
Ireland	N=50, 2%
Israel	N=50, 2%
Italy	N=100, 5%
Japan	N=100, 5%
Mexico	N=100, 5%
Netherlands	N=100, 5%
New Zealand	N=36, 2%
Nordics (DK, FI, NO, SE)	N=100, 5%
Portugal	N=50, 2%
Singapore	N=50, 2%
South Korea	N=100, 5%
Spain	N=100, 5%
Switzerland	N=50, 2%
Thailand	N=63, 3%
United Arab Emirates	N=50, 2%
United Kingdom	N=100, 5%
United States	N=250, 12%

Industry

Architecture, engineering, and construction	N=112, 5%
Automotive	N=131, 6%
Communications	N=32, 1%
Consumer goods	N=150, 7%
Energy and utilities	N=78, 4%
Financial services	N=163, 8%
Government/public sector	N=44, 2%
Healthcare	N=100, 5%
Life sciences and biotechnology	N=92, 4%
Manufacturing	N=287, 13%
Media and entertainment	N=57, 3%
Nonprofit	N=11, 1%
Professional and business services	N=120, 6%
Retail	N=268, 13%
Supply chain and logistics	N=65, 3%
Technology	N=372, 17%
Travel and hospitality	N=56, 3%

Seniority

C-level executive	N=267, 12%
Vice president or equivalent	N=746, 35%
Director or equivalent	N=1,125, 53%

Company Size

Enterprise (>3,500 employees)	N=466, 22%
Mid-Market (200-3,500 employees) ...	N=1,358, 64%
Small and Medium (<200 employees)	N=466, 15%



Ready to Learn More?



6 Security Steps to Prepare for Agentforce

Learn how to empower your Agentforce with best-in-class security strategies.

[LEARN MORE >](#)

The Salesforce DevSecOps Guide

Learn how a strong DevSecOps strategy can help you scale efficiently, test changes safely, and deliver your Agentforce fast.

[LEARN MORE >](#)

Data Security Best Practices Guide

Learn how to adopt best practices for data security while innovating with AI.

[LEARN MORE >](#)

Learn More About Agentforce

See what sets Agentforce apart from other Agentic AI and what it can do for your organization.

[LEARN MORE >](#)



The information provided in this report is strictly for the convenience of our customers and is for general informational purposes only. Publication by Salesforce does not constitute an endorsement. Salesforce does not warrant the accuracy or completeness of any information, text, graphics, links, or other items contained within this guide. Salesforce does not guarantee you will achieve any specific results if you follow any advice in the report. It may be advisable for you to consult with a professional such as a lawyer, accountant, architect, business advisor, or professional engineer to get specific advice that applies to your specific situation.