Deskpro

REPORT

State of AI in Support Operations: Balancing Innovation and Compliance

Why regulated industries are caught between AI momentum and compliance reality

Executive summary

Organizations want AI-powered help desk support. But compliance regulations create a barrier as most modern AI systems require sending customer data outside the organization. Regulated industries like healthcare, finance, and government rely on external data processing, creating significant challenges for adopting AI in these sectors. Security functions as both a driver of decision-making and a barrier to AI adoption.

A Deskpro survey of over 220 support and IT leaders shows that while 71% of organizations have already adopted AI for support operations, 81% rank data security as a top priority.

However, in regulated industries, only 58% currently use AI, compared to 92% of technology companies.

This creates a paradox: while businesses need AI to thrive, compliance requirements like HIPAA, SOC 2 Type II, PCI DSS, and data residency mandates demand strict data security.

Most platforms force them to choose between innovation and control.

Today's market presents a limited choice. Cloud-based AI help desk platforms deliver modern capabilities, including ticket summarization, intelligent routing, and knowledge search, but require sending customer data to external providers. Self-hosted solutions keep data under an organization's control and meet stringent security and compliance requirements, but often lack, or are limited in the use of AI features because most solutions prioritize cloud-based AI capabilities. For IT directors and compliance officers in regulated industries, this creates a genuine constraint in either direction: sacrificing data control for AI capability, or sacrificing modern AI features to maintain compliance.

This report explores how support teams are navigating these challenges, why security and compliance remain the biggest hurdle for regulated industries, and how organizations can confidently embrace secure AI help desk solutions.

The overall conclusion: Support teams that unite AI capability with security and compliance will define the next era of customer experience.

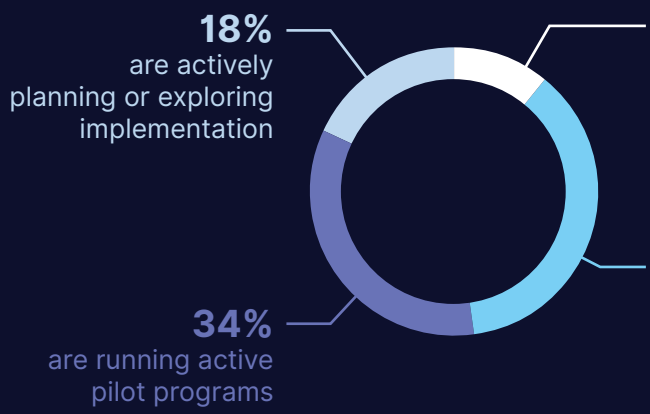
Table of contents

The AI adoption paradox: high demand, high barriers

Strong AI momentum despite security concerns

The research data shows robust AI adoption in support operations.

AI adoption in support operations is accelerating, with 71% of organizations already using AI in some capacity.



Organizations clearly aren't rejecting AI. Instead, they're waiting for solutions that allow them to deploy it securely and compliantly. For 53% currently in pilot, planning, or evaluation phases, the primary roadblock is clear: finding a solution that meets both operational needs and stringent security requirements.

Each quarter spent evaluating solutions extends reliance on manual processes, increasing agent workloads, and resolution times. For support leaders, understanding the factors driving adoption decisions is fundamental to moving from evaluation to implementation.

Data security: the foundation of AI adoption

Security as the deciding factor

For organizations in regulated industries, data security is non-negotiable. Compliance violations can result in hefty fines, operational disruptions, and reputational damage. This is why IT and Security teams play a central role in platform selection, evaluating not just features but also the vendor's security architecture and compliance readiness.

This highlights a key dynamic: organizations need AI to improve efficiency and cannot compromise data control and compliance. Vendors must demonstrate expertise in security and compliance to gain approval and build trust.

When evaluating support technology solutions, data security emerges as the paramount concern.

43%
consider security a "critical factor" and will not proceed without strong security guarantees

81%
rate security as either "critical" or "very important"

4%
view security as a minor consideration

IT and Security teams influence tech decisions

> **78% of organizations involve their IT or Security teams in the final decision-making process for support platform selection.**

This shift impacts vendor evaluation fundamentally. Support leaders can no longer recommend platforms based solely on agent productivity or AI features. Vendor security posture, deployment flexibility, and compliance certifications now carry equal weight.

Support leaders now evaluate platforms based on security credentials alongside feature capabilities. ISO 27001 certification, SOC 2 Type II and HIPAA compliance, and deployment flexibility options, whether cloud, on-premise, or hybrid, become central to the evaluation.

Compliance: the driving force behind security investments

Regulatory requirements dictate technology decisions

Industry regulations emerge as the top driver, when asked what would trigger organizations to prioritize AI security more highly.

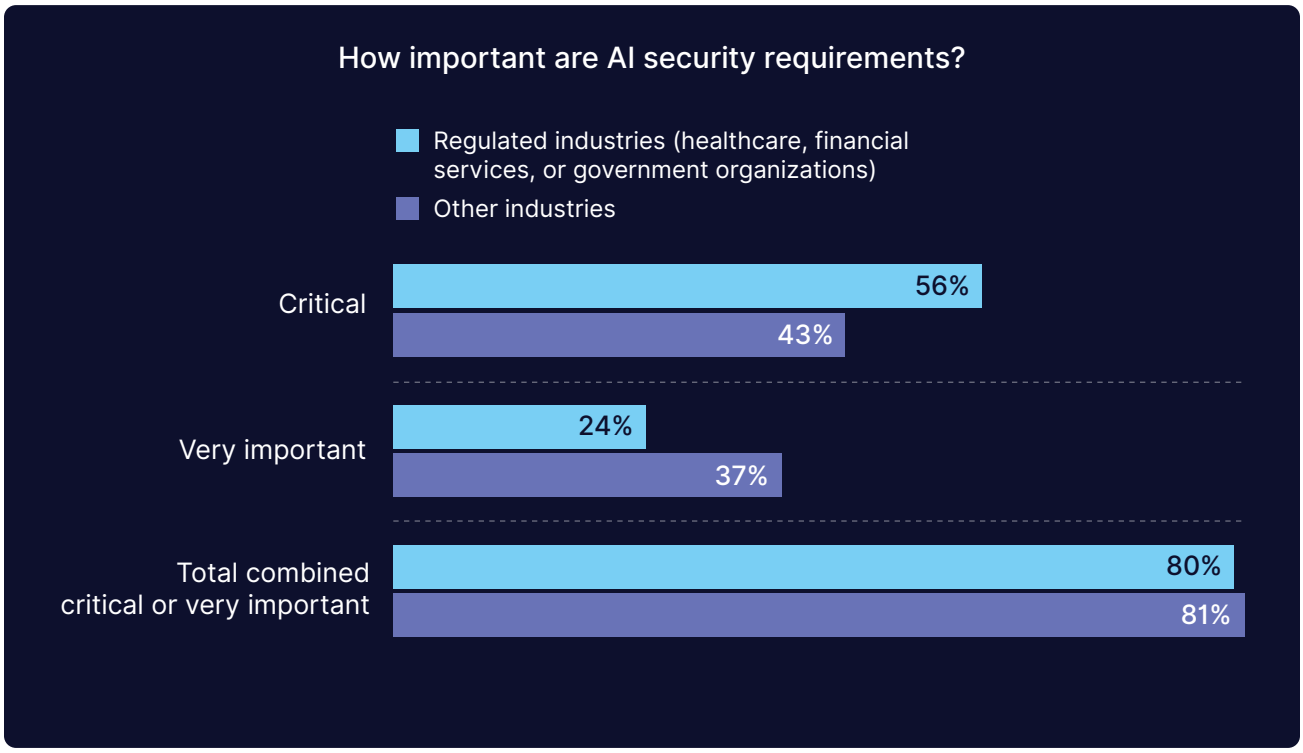
For organizations in healthcare, financial services, and government, compliance requirements are the primary driver for security investments.

These findings validate that regulated industries apply fundamentally different evaluation criteria when selecting support solutions compared to technology companies. While technology companies prioritize functional capabilities and innovation, regulated industries weight security and compliance as non-negotiable requirements. Compliance frameworks drive technology decisions across:

- Healthcare organizations managing PHI under HIPAA
- Financial services firms navigating SOC 2, PCI DSS, and regional banking regulations
- Government agencies requiring FedRAMP and data sovereignty
- Technology companies subject to GDPR, CCPA, and emerging AI regulations

Regulated industries express acute need for AI security

Among healthcare, financial services, and government organizations, security requirements are even more pronounced than in the overall population.

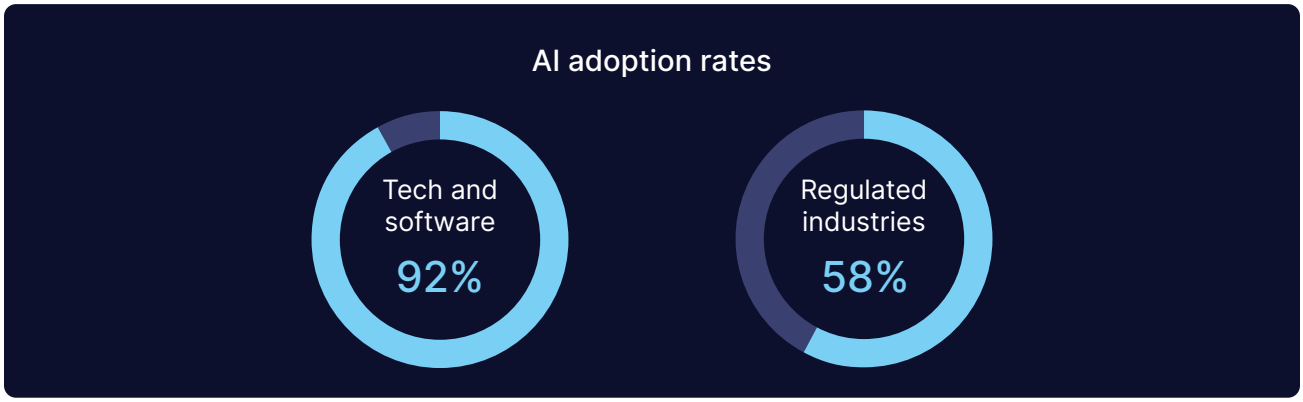


This higher “critical factor” concentration (56% versus 43% overall) quantifies why regulated industries face such different adoption constraints. Their security requirements are not merely preferences; they’re compliance mandates.

Industry AI adoption patterns show divide between technology and regulated sectors

Technology sector leads, regulated industries face barriers

Analysis by industry reveals significant differences in AI adoption rates and security approaches.



The 34-percentage-point gap between technology companies and regulated industries, driven by compliance requirements, does not reflect AI readiness or rejection of AI. It highlights a lack of market solutions that meet the stringent security and compliance demands of regulated industries.

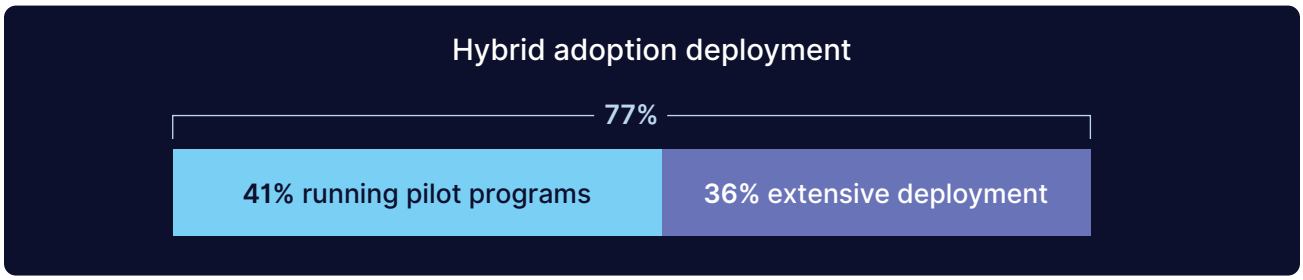
Each support function faces different challenges

Internal teams lead, external teams lag

A cross-analysis of support function types reveals distinct adoption patterns.

Hybrid support (internal + external): 77% adoption

Teams handling both internal and external support show the highest overall adoption rate at 77%. Within this group:



Internal employee support (IT help desk, HR support): 75% adoption

Internal support teams exhibit the highest adoption rate among isolated functions. This reflects lower needed concern around customer data protection and clearer security perimeters:

- Access to structured, centralized data gives teams clearer security boundaries
- Reduced customer data exposure simplifies compliance requirements
- Internal data governance is typically more straightforward

External customer support: 69% adoption

External-facing support teams report the lowest adoption rate, due to customer data complexity:

- Public exposure of customer data increases security and privacy requirements
- Multiple compliance frameworks may apply (GDPR, CCPA, HIPAA, PCI DSS)
- Data residency and sovereignty requirements create deployment constraints

The 14-percentage-point gap between internal and external support adoption shows how customer data complexity drives technology decisions. Organizations prioritize AI adoption where compliance complexity is lower.

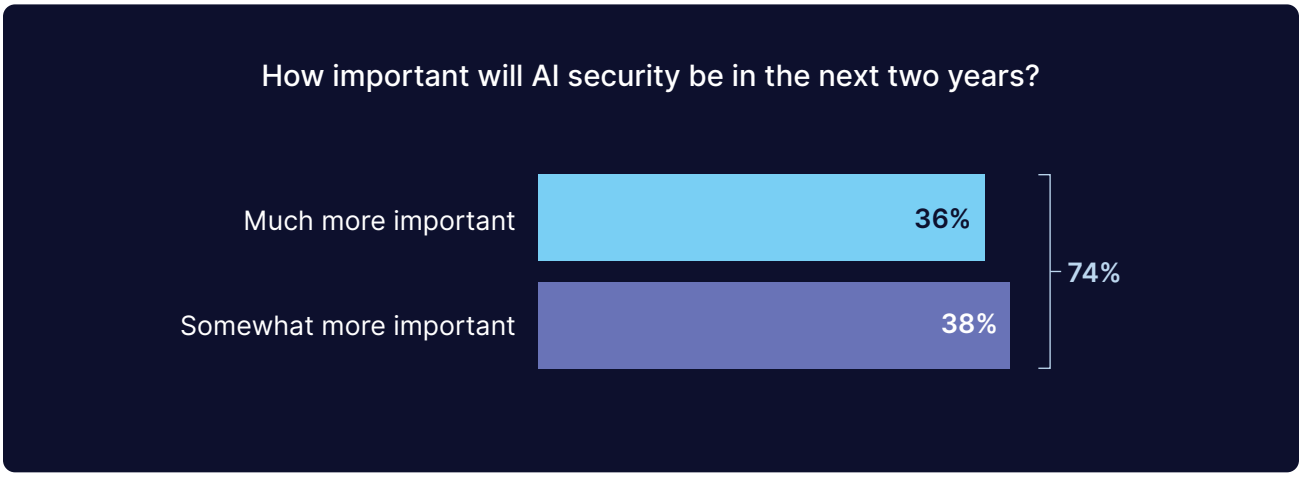
However, the deployment strategy differs significantly by industry. Technology companies in hybrid roles achieve 94% adoption with 50% extensive deployment. Regulated industries show 69% adoption but run pilots at comparable rates, indicating more cautious scaling.

This reinforces an important insight: organizations can bridge internal and external needs, but compliance-conscious organizations require different solution architectures.

Why security will define the future of AI adoption in support organizations

The intensifying focus on AI security

As AI adoption grows, so does the focus on security. Over the next two years, 74% of organizations expect to increase their investment in AI security.



Standardized security frameworks could accelerate adoption, with 58% of organizations indicating they would invest more in secure AI solutions if industry standards were widely adopted. As regulations evolve, the demand for compliant, secure platforms will only intensify.

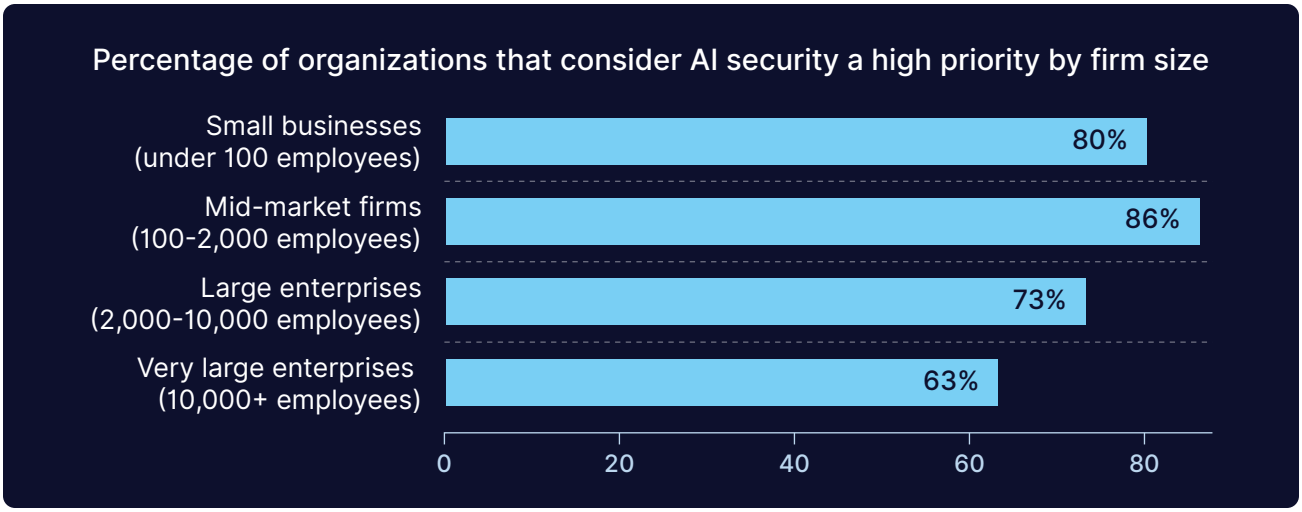
The deployment flexibility imperative

Traditional help desk solutions have taken one of two approaches: full-featured AI in SaaS clouds, or limited AI capabilities on-premise. This binary choice fails a significant segment of the market.

- 43% of organizations rate security as “critical,” highlighting organizations that will not compromise on infrastructure control
- 38% work at enterprises with 500 or more employees, managing complex infrastructure
  - These organizations typically require cloud for lower-risk functions, on-premise for regulated data, and VPC for specialized security needs

Company size influences AI security requirements

An analysis of security priorities by company size found that mid-market firms (500-2,000 employees), lacking enterprise-scale security resources but facing regulatory requirements, are most intensely focused on security. This pattern suggests that these organizations face a unique dynamic: they’ve grown beyond small-business resource constraints but operate with security capabilities that are more limited than enterprise-scale operations.



AI model selection preferences

Nearly half of organizations prefer multiple specialized models

Nearly half of organizations surveyed prefer using multiple specialized AI models for different tasks rather than standardizing on a single model:

- 43% prefer multiple specialized models for different tasks
- 32% prefer standardizing on one primary model
- 15% have not considered model selection as a factor
- 11% use whatever models come with their support platform

Organizations that prefer multiple specialized models also report the highest security priority.

> **A majority (90%) of organizations that prefer specialized models rate security as a high priority.**

This shows a significant correlation: organizations that want control over AI model selection are also the most focused on security. It reflects the need for data governance policies, compliance requirements, and control over which AI models access sensitive information.

Advanced adopters show strongest security focus

AI maturity correlates with security priority

A cross-analysis of AI adoption levels and security importance confirms a strong correlation:

- Extensive AI users: 94% rate security as critical or very important
  - 51% rate it as a “critical factor”
- Pilot program users: 82% rate security as a high priority
  - 38% rate it as a “critical factor”
- Planning stage organizations: 58% rate security as a high priority

– 21% rate it as a “critical factor”

Why this matters: As organizations gain AI experience, security becomes more critical, not less. Mature AI adopters understand that security and AI capability are inseparable. Early-stage organizations may prioritize AI features, but experience shows that a robust security architecture is essential for sustainable deployment.

The bottom line: market readiness for secure AI

1. Strong demand for AI exists. Roughly 7 in 10 respondents (71%) report adopting AI, underscoring a clear market need for intelligent support capabilities.
2. AI security is the linchpin. 81% rate security as critical or very important, with 78% of organizations involving IT or Security teams in decision-making. Security is not a secondary consideration.
3. Compliance is currently driving the market. 42% cite regulations as the primary driver of increased security investment. Compliance requirements shape technology decisions more than incident response.
4. Legacy help desk solutions are not providing adequate options. The 34-point adoption gap between technology companies and regulated industries reflects market solutions that do not accommodate compliance requirements.
5. The requirement for secure AI is intensifying. 74% of respondents expect to increase their focus on AI security over the next 2 years. Market pressure for compliant, secure solutions will only grow.

Traditional cloud-based AI help desk solutions have achieved strong adoption among organizations with low security and compliance barriers. However, they’ve created a sizable market gap for organizations with stringent security and compliance requirements. This gap represents where help desk platforms will compete going forward.

Deskpro: secure AI without compromise

The AI adoption gap for help desk software exists because today’s platforms typically force a choice: adopt modern AI capabilities with cloud deployment and accept data transfer to external systems, or maintain data control with self-hosted deployment and forgo contemporary AI features. This choice reflects architectural limitations, not market necessity. Deskpro eliminates this trade-off.

With Deskpro, your data stays under your control, whether you choose cloud, self-hosted, or hybrid deployment. Deskpro Private makes it possible to deploy AI-powered support on your terms. Run in your VPC, on-premise, or sovereign cloud while keeping all data within your security perimeter. ISO 27001 certification, SOC 2 Type II and HIPAA compliance mean you finally get advanced AI capabilities without compromising security or sovereignty. You can choose your AI model—OpenAI, Claude, Gemini, or custom—and stop choosing between innovation and control.

For IT directors, this means faster approvals with confidence in security architecture. For support teams, it means access to AI-powered tools like ticket summarization, intelligent routing, and knowledge search, all without compromising data security.

Deskpro delivers the future of AI-powered support, designed for the most demanding industries.

Methodology note

This analysis is based on a survey of 222 professionals across IT, customer support, and HR functions. Respondents were employed at organizations ranging from under 100 to over 10,000 employees, across industries including technology, healthcare, financial services, government, and others. The survey assessed AI adoption, security priorities, compliance requirements, and deployment preferences.

Survey respondent breakdown

By support function/role

- 88 Customer support/help desk
- 81 IT/systems support
- 53 Hybrid support

By company size

- 35 Under 100 employees (15.8%)
- 85 100–500 employees (38.3%)
- 49 500–2,000 employees (22.1%)
- 26 2,000–10,000 employees (11.7%)
- 27 10,000+ employees (12.2%)

By Industry

- 60 Technology & telecommunications (27.0%)
- 30 Financial services (13.5%)
- 20 Food & beverages (9.0%)
- 16 Retail & consumer durables (7.2%)
- 15 Education (6.8%)
- 15 Healthcare & pharmaceuticals (6.3%)
- 10 Business support & logistics (4.5%)
- 7 Insurance (3.2%)
- 7 Manufacturing (3.2%)
- 7 Automotive (3.2%)
- 6 Government (2.7%)
- 6 Entertainment & leisure (2.7%)
- 5 Transportation & delivery (2.3%)
- 5 Advertising & marketing (2.3%)
- 4 Construction (1.8%)
- 4 Nonprofit (1.8%)
- 5 Agriculture, real estate, utilities & energy, airlines & aerospace (0.9–0.5% each)

Deskpro

The help desk behind global leaders

Learn more about how global leaders achieve exceptional customer and employee experiences with Deskpro.

Visit **deskpro.com** to book a personalized demo.