



GUIDE

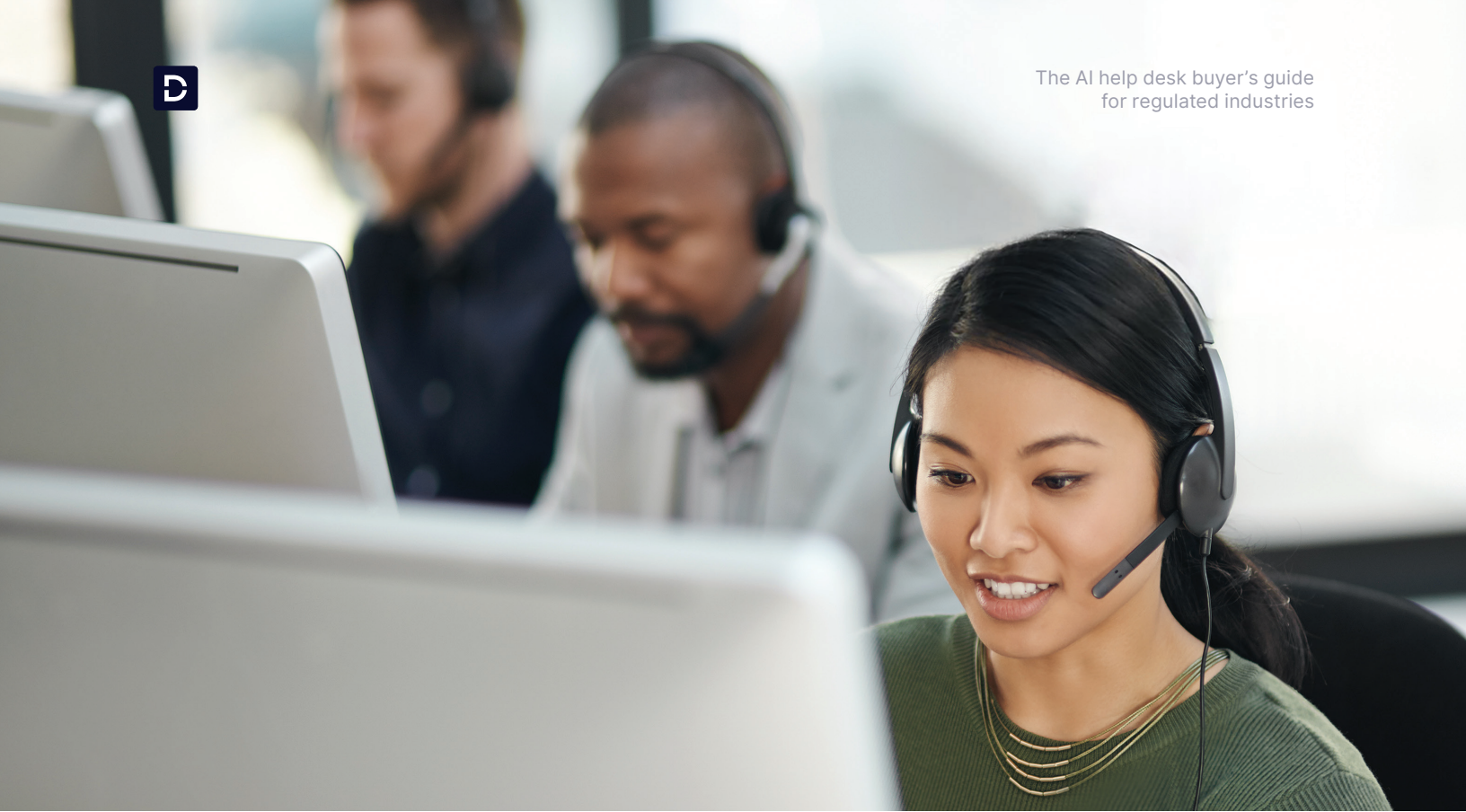
Balancing AI innovation and compliance needs:

The AI help desk buyer's guide for regulated industries



Table of contents

- 1 The balancing act: Regulatory requirements and the support experience
- 2 How do compliance requirements in regulated industries impact support teams?
- 3 How compliance requirements shape the help desk decision
- 5 4 paths to deploying your help desk in a compliance-ready environment
- 8 The next decision: AI implementation
- 9 What to look for in a help desk for regulated industries
- 11 Which leading help desk vendors meet your compliance needs?
- 12 Deskpro Private: Built for regulated environments



The balancing act: Regulatory requirements and the support experience

A support team leader at a bank has been evaluating AI-powered help desk software, looking at solutions from both a feature set and compliance perspective. She's narrowed down her shortlist to a top choice only to have her compliance team tell her that, even though the vendor has the necessary compliance certifications, the solution doesn't meet her organization's needs because it uses public AI models.

A healthcare support team has been using a SaaS help desk with AI features for several years, only to have their security team tell them they need to migrate off it because their data is unencrypted in a public cloud to allow for AI processing.

Scenarios like these are common for support teams in regulated industries and enterprises with strict data privacy, security, and compliance requirements. IT and security teams are involved in the final decision-making process for help desks in 78% of organizations, according to Deskpro's *State of AI in Support Operations* report.¹ Support leaders—especially those in industries like financial services, healthcare, aerospace and defense, and government—can't select help desk platforms based solely on their agent productivity and AI features. Vendor security posture, compliance certifications, deployment options and AI flexibility can also carry weight.

Navigating the help desk market when you have to meet strict compliance and security requirements can be genuinely complex. We've created this guide to help you understand:

- How compliance requirements for regulated industries impact the help desk evaluation process—especially when AI features are involved
- The different paths you can take to stay compliant while still using an AI-powered help desk
- What to look for (and what questions to ask) when vetting help desk vendors

¹ <https://info.content.deskpro.com/ai-support-operations-compliance-report-2025>



How do compliance requirements in regulated industries impact support teams?

Customer and internal support teams are prime candidates for AI efficiency gains. Over the past several years, we've seen organizations increasingly implement AI to power autonomous chatbots, intelligently route tickets, and provide behind-the-scenes agent assistance. Deskpro's *State of AI in Support Operations* found that 92% of technology companies and 58% of organizations in regulated industries are currently using AI in their support operations in some capacity.

That 34-point difference between AI adoption in tech companies and regulated industries is notable. There's clearly an appetite for AI across industries: support leaders know there are opportunities to automate repetitive tasks, deflect tickets, and help their agents work more efficiently. But support departments in regulated industries have a higher bar to clear when it comes to finding AI-powered solutions that meet their compliance and security requirements.

Regulated industries operate under compliance frameworks (e.g., GDPR, ISO 27001, HIPAA, SOC 2, FedRAMP, and others) that impose strict requirements on how data is stored, processed, and accessed. Any technology that handles sensitive customer or employee data is in scope for those requirements. That means data residency, access controls, vendor certifications, and deployment flexibility must be taken into account before even beginning to look at features.

AI in support software often complicates the buying process. Most modern support platforms have AI features that rely on large language models (LLMs) hosted in public clouds. When organizations expose their data to these public cloud models, they may lose control over how and where that data is stored, processed, and reused. While the major cloud providers invest heavily in cybersecurity, their security postures may not be enough to meet the compliance requirements of highly regulated industries. Using public services may also breach data protection laws that require organizations to store data on servers within specific geographic boundaries.

In the next section, we'll take a closer look at how compliance frameworks factor into help desk and AI model selection.

Examples of compliance frameworks that impact technology buying decisions:

- **GDPR** as a data privacy framework for any organization that handles personal data of EU/EEA residents
- **ISO 27001** as an international standard for information security management
- **HIPAA** for US-based healthcare organizations
- **SOC 2** for technology and service organizations that operate in the US or have US enterprise clients
- **PCI DSS**, and regional banking regulations for financial services firms
- **FedRAMP** (in the US) and data sovereignty requirements for government agencies
- **CMMC** for US defense contractors
- **India's DPDP Act, US state privacy laws, and the EU AI Act** for multinational companies



How compliance requirements shape the help desk decision

Support leaders in regulated industries must evaluate help desk platforms through two lenses: feature impact (i.e., does this solution help my team work more effectively?) and compliance (i.e., does this solution meet my organization's security and compliance requirements?).

To complicate matters further, regulated organizations often operate under multiple compliance frameworks. For example, a multinational financial services firm might simultaneously need to satisfy PCI DSS for payment card data, SOC 2 for their security controls, GDPR for EU customer data, and local banking regulations in every market they operate in. A vendor that satisfies one framework may create compliance gaps under another. Support leaders often discover these conflicts late in the evaluation process, after significant time has already been invested.

Unfortunately, many cloud-based SaaS help desks create compliance problems under multiple frameworks because the software runs on a public cloud operated by one of the hyperscalers: most commonly AWS, Microsoft Azure, or Google Cloud. Data that is processed by the software—such as support tickets, customer or employee PII, and financial records—is stored and processed in data centers chosen by the SaaS vendor and operated by the hyperscaler, which can violate data control, access, and residency requirements.

Real-world scenario: A US-based defense contractor runs an internal IT help desk to support employees across several facilities, some of which handle controlled unclassified information (CUI). To work with the Department of Defense, the contractor must comply with CMMC, which requires that any system handling CUI meet specific access control, audit, and configuration management requirements. Their current SaaS help desk has strong general security certifications, but the software runs on a shared multi-tenant cloud infrastructure, and the contractor's security team cannot verify that CUI processed through support tickets is adequately isolated from other tenants.

When they raise this with the vendor, they learn that achieving the required level of isolation would require a dedicated deployment the vendor doesn't offer. Despite years of using the platform, they have to restart their search.

When AI enters the picture: A major compliance and security challenge

Beyond the compliance challenges created by SaaS applications in general, there's also the AI piece of the puzzle. Even if you're using a help desk that runs in a private environment, its AI features may not be compliant. Help desk vendors typically power their AI features using large language models (LLMs) hosted on public cloud infrastructure, separate from the infrastructure hosting the help desk itself. So even if the help desk stores and processes data in your private environment, its AI features may be routing sensitive data outside your organization's approved boundaries for processing.

Not only does this create potential compliance and data sovereignty issues, it can also lead to security risks. While data is typically encrypted in transit, it must be decrypted at the point that it is processed by the LLM. This increases your organization's cyberattack surface and raises the risk of prompt injection: a type of attack in which bad actors insert hidden prompts into legitimate ones to get an LLM to reveal sensitive information or behave in unintended ways.



While major cloud providers invest heavily in cybersecurity measures to reduce prompt injection risks, no public cloud environment can eliminate them entirely—and organizations in regulated industries such as healthcare, finance, and government may simply be unable to accept that level of risk.

Real-world scenario: A retail bank in Germany has deployed its help desk in a private cloud environment to meet the strict data security requirements set by BaFin, Germany's financial regulatory authority. The help desk vendor releases a new AI feature that automatically summarizes customer support tickets, including cases that contain account numbers, transaction details, and other sensitive financial data. Behind the scenes, this feature sends ticket content to an LLM hosted on a public cloud server outside the bank's private environment for processing. A security audit flags this as a potential violation under both BaFin regulations and GDPR, and the bank's compliance team determines the feature cannot be used.

The cost of getting this wrong

So what does all of this mean to you in practical terms as a support leader? If you implement a help desk that doesn't meet your organization's compliance requirements, potential consequences could include:

- Cybersecurity breaches, including leaks of sensitive information
- Fines, legal violations, and increased regulatory scrutiny
- Reputational damage and loss of customer trust
- Time and resources wasted evaluating software you can't use
- Delayed rollout of your help desk, creating service disruptions
- Inability to use AI features to improve support operations

The best thing you can do is to keep compliance requirements front and center from the beginning of your help desk search. Partner with your security, legal, and compliance teams to make sure you understand the requirements your software and its AI features are subject to and determine which help desk vendors and deployment models meet your needs.

In the next section, we'll walk you through the four primary paths to maintaining compliance with a private or isolated deployment of your help desk:

- Virtual Private Cloud (VPC)
- Sovereign cloud
- Regional private cloud
- Fully private (on-premise or colocation) deployment





4 paths to deploying your help desk in a compliance-ready environment

Help desk platforms deployed in a public cloud often create compliance issues by default. If public cloud help desks are not an option for your support team, you'll need to look to vendors that offer the following deployment paths.

Virtual Private Cloud (VPC)

A virtual private cloud is a logically isolated network environment hosted within the broader public cloud infrastructure operated by a hyperscaler (e.g., AWS, Microsoft, Google). Unlike a standard multi-tenant SaaS deployment, a single-tenant deployment in a VPC gives your organization a dedicated slice of the hyperscaler's infrastructure, with controls over where your data is stored and who can access it. Many hyperscalers also offer private connectivity options (e.g., AWS PrivateLink) that allow your help desk to connect to additional hyperscaler services using company-approved encryption.

For many regulated organizations, a VPC is sufficient to meet compliance requirements. However, it's worth understanding its limits. Because a VPC runs on a hyperscaler's public cloud, the provider retains operational control over the underlying hardware—something that stricter compliance or security teams could flag as a risk. It's also worth confirming that your help desk vendor supports private endpoint connectivity for AI and that the specific AI models available through those endpoints meet your organization's requirements. Otherwise, you could find yourself unable to use your help desk's AI features.

Strengths	Limitations
✓ Lower cost and faster to deploy than fully private options	✗ Logical isolation only (infrastructure is not physically dedicated)
✓ Available in a wide range of geographic regions	✗ Hyperscaler retains operational and legal control of infrastructure
✓ Compatible with managed AI services offered by the hyperscaler, with potential for private connectivity	✗ Jurisdictional risk if hyperscaler is subject to foreign laws (e.g., US CLOUD Act)
✓ Control over data storage and access	✗ LLM processing still requires data to be unencrypted

Sovereign cloud

Sovereign clouds are typically owned by regional cloud providers and are run in data centers that are located and operated by personnel in specific sovereign countries or regions. This model is designed to keep data within the sovereign cloud's region, allowing organizations to meet sovereign standards while benefiting from the expertise and innovation of the cloud provider. Many sovereign cloud providers today also offer access to sovereign AI foundation models.

There are also some sovereign clouds that are owned by a US-based hyperscaler but designed to prevent foreign jurisdictional reach. For example, the AWS EU Sovereign Cloud operates under a parent company that is locally controlled in the EU, led by EU citizens, and subject to local laws.



Strengths	Limitations
✓ Scalability and disaster recovery managed by the cloud provider ✓ Faster to deploy than fully private options, with lower upfront costs ✓ Certified compliance with major frameworks often already in place ✓ Access to managed AI services ✓ Specialized compliance architectures available (e.g., Microsoft's Sovereign Landing Zones, AWS GovCloud)	✗ Risk of vendor lock-in (dependence on provider's proprietary AI and software ecosystems) ✗ Sovereign cloud availability varies by region ✗ AI processing may occur outside the sovereign boundary depending on the model ✗ Regional sovereign cloud providers may have less mature AI offerings and lower R&D investment than hyperscalers

Regional private cloud

An alternative approach that is adopted by some organizations, including some financial institutions and government agencies, is to deploy their help desk in a private cloud operated by a regional vendor, such as Scaleway in France or Fujitsu in Japan.

This option lets organizations tailor their cloud usage to their compliance requirements because they can choose where they want to physically store their data. However, it can be difficult to scale due to limited on-premise resources, and it requires organizations to rely on the private cloud service provider for maintenance and ongoing innovation. It also requires the private cloud vendors to make the significant investment of building their own AI infrastructure to provide AI foundation model services within the sovereign environment.

Strengths	Limitations
✓ Regional vendors operate under local laws (eliminates foreign jurisdictional risk) ✓ High degree of customization for specific industry regulations and compliance frameworks ✓ Data residency is explicit and auditable ✓ Regional vendor handles hardware upkeep and maintenance	✗ Typically more difficult to scale than VPC or sovereign cloud due to limited regional server capacity ✗ Lower R&D investment compared to hyperscalers ✗ AI service offerings may be more limited



Fully private (on-premise or colocation) deployment

For organizations that already have their own data center(s) or leverage a colocation facility, deploying your help desk on-premise may be the most straightforward path to meeting your compliance requirements, since the infrastructure has already been audited and approved by your security and legal teams.

If your organization has its own data center but is trying to reduce its maintenance load, an Enterprise Private Cloud is another on-premise option worth considering. AWS Outposts, Azure Local, and Google Distributed Cloud are examples of the hyperscaler managing a “mini-cloud” with hardware and services running directly in your own data center. This gives you the compliance benefits of on-premise deployment alongside the managed infrastructure and AI services of a hyperscaler.

To make on-premise deployment, you'll need to look for help desk vendors that offer fully self-hosted options. If you plan to use AI features in your help desk, you'll also need to determine if you can connect AI models that your security and compliance teams have already vetted. You may find your organization requires you to use an AI foundation model that can be deployed fully on-premise.

Strengths

- ✓ Strongest approach to satisfying the most demanding compliance requirements
- ✓ Option to maintain full control over data, hardware, and security perimeter
- ✓ Potential for air-gapped deployment for the most sensitive workloads
- ✓ Flexibility to connect AI models your security and compliance teams have already vetted

Limitations

- ✗ Highest upfront cost and deployment complexity
- ✗ Requires significant internal IT resources and expertise
- ✗ Organization is responsible for hardware maintenance and security (*unless using Enterprise Private Cloud*)
- ✗ Scalability is slower and more constrained than cloud-based options



The next decision: AI implementation

If your support team is planning to use any of the AI features your help desk vendor offers, you'll need to think about their approach to AI in addition to the deployment models they support. Essentially, there are two paths you can take with AI: use an AI model your vendor provides or connect to a model your organization is already using.

Vendor-provided AI

With this approach, you use the LLMs your vendor has selected to power their AI features. Popular LLMs include:

- OpenAI's GPT
- Anthropic's Claude
- Google's Gemini

If your vendor uses AI models hosted in a public cloud, this approach may not meet your compliance requirements. This is because your data is transmitted to the public cloud and must be decrypted at the point of AI processing. This may place data outside your organization's approved security perimeter, leading to compliance violations and increasing your surface area for a potential cyberattack. If that's the case, you may find that your organization won't allow you to use the AI features in your help desk—causing you to miss out on efficiency gains and improvements to the support agent experience.



Bring-your-own-AI

With a BYO-AI approach, you choose the models you want to power your help desk's AI features. Your help desk vendor connects the model via an API key you supply from the model provider.

Providing your own AI lets you select models your security team has already vetted. And, crucially for support teams in regulated industries, it allows you to use AI models that can be deployed in your private environment, a sovereign or private cloud, or a VPC. Examples of LLMs with private and sovereign deployment options include:

- Meta's LLaMA
- Mistral AI
- DeepSeek
- Qwen
- Cohere

BYO-AI isn't an option offered by every help desk provider, so it's important to ask vendors about this up front if you know it's non-negotiable for your organization.



What to look for in a help desk for regulated industries

As you start evaluating help desk vendors against your security, compliance, and data privacy requirements, there are three crucial areas to keep in mind: deployment flexibility, AI choice, and infrastructure management.

Deployment flexibility

You'll need to ensure your chosen provider offers the deployment model that works for your organizations. Many of the major SaaS help desk providers are cloud-only, or offer limited private deployment options, meaning you may not be able to use them in your organization.

Questions to ask:

- What deployment options do you offer for organizations with strict data handling requirements?
- How do your different deployment models meet my organization's specific compliance needs (e.g., HIPAA, PCI-DSS)?
- Where is my organization's data stored and processed, and can you guarantee it never leaves a specific jurisdiction?
- With your deployment models, who can access our data and what controls govern that access?

AI choice

If your chosen provider offers a deployment model that works for you, do they also let you choose an AI model that keeps you in full control of your data? If not, you may end up being blocked from using any of their AI features.

Questions to ask:

- Do your AI features work with any AI model of our choice, or are we limited to specific providers or models?
- If we bring our own AI model, can we deploy it fully on-premise or in an isolated environment?
- If we're using your AI model, does AI processing happen within the same environment as our data storage?
- Is our support data ever used to train or improve AI models?

Infrastructure management

You'll need to determine who is responsible for infrastructure management and, if you're choosing a self-hosted deployment, whether the vendor offers professional services to assist with this deployment.

Questions to ask:

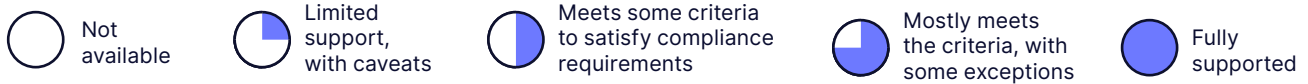
- What management models do you offer (e.g., fully managed by you, managed by a certified partner on our infrastructure, or fully managed by our team)?
- If we need help setting up or configuring a self-hosted deployment to meet our specific compliance requirements, what professional services do you offer?
- When we self-host, what is the division of responsibility between your team and ours for keeping the environment compliant?
- How are updates and security patches delivered for self-hosted deployments, and do we have control over when those updates are applied?
- What are your commitments around uptime and support response times, and do those apply equally to self-hosted and managed deployments?



Which leading help desk vendors meet your compliance needs?

There are a lot of help desk platforms on the market, but how many of them actually meet your compliance requirements? The table below breaks down the deployment models and BYO-AI offerings of some of the top providers. While this isn't an exhaustive list, we hope it's a useful starting place.

Key



Product	VPC or private cloud deployment	On-premise deployment	Data sovereignty control	AI data controls (no data retention or use of data for model training)	Bring-your-own-AI model
Zendesk			1	2	
Freshdesk			1	3	
Salesforce Service Cloud	4				5
Jira Service Management		6	7	8	9
Zoho Desk				10	11
ServiceNow	12	13			
ManageEngine					14
Deskpro Private					

1 Limited options to choose the region where "data at rest" is stored.

2 Data is retained for processing and history. "Advanced AI Add-On" is necessary to guarantee data will not be used for model training.

3 Data is retained for processing and history. Freshworks commits to not using customer data to train its AI models.

4 Salesforce Private Connect creates a private connection between Salesforce and your AWS VPC.

5 Not all Salesforce AI features work with their BYO-AI model.

6 Atlassian is sunsetting its Data Center (on-premise) version of Jira Service Management, and new licenses are no longer available.

7 Atlassian Isolated Cloud enables customers to choose their region for data hosting but is still managed by Atlassian (and subject to US jurisdiction via the US CLOUD Act).

8 Atlassian Intelligence retains data, and Atlassian has announced it will start using customer data to train its AI models starting in August 2026.

9 Option to use Atlassian-hosted LLMs only.

10 Zoho's Zia AI retains data but does not use it for model training.

11 Government Community Cloud available to approved government agencies, but no true VPC or private cloud option.

12 ServiceNow allows you to create a site-to-site VPN tunnel or use private peering to mimic a VPC experience.

13 While ServiceNow does technically maintain a self-hosted software license agreement, they typically only grant these licenses to a very small subset of customers.

14 Not truly model-agnostic. Private AI is available with Zia, ManageEngine/Zoho's proprietary model.



Deskpro Private: Built for regulated environments

Most help desk platforms take a cloud-first approach that is often at odds with the needs of support teams in regulated industries. Even when these cloud-only providers hold compliance certifications that are relevant to your industry, they may still fail to overcome certain compliance hurdles. If your organization has strict data residency or data control requirements, you may not be able to use a cloud-based help desk because it's hosted outside your approved security perimeter. And even if you choose a solution that can be deployed in a private environment, you may still be locked out of using its AI features if those features are powered by public LLMs.

With Deskpro Private, you don't have to compromise on help desk features or compliance.

Deskpro Private is an AI-powered help desk platform designed for organizations that require full control over security, data, and deployment, without sacrificing the benefits of a modern customer support platform. We built it to meet the needs of highly regulated industries and organizations that have strict data privacy and sovereignty requirements, including:

- Financial services firms
- Healthcare organizations
- Aerospace and defense contractors
- Multinational enterprises
- Government agencies

Deskpro Private lets you choose the compliance-ready deployment model that's best for your organization: in a VPC, sovereign cloud, private cloud, or on-premise in your data center or a colocation facility.

You can also connect your AI model of choice to ensure you're using an LLM that your organization has approved and that lets you maintain control of your data. Here's how it works at a high level:

1. Deploy Deskpro in your private environment.
2. Connect to LLMs such as GPT-5, Claude, Gemini, Mistral, LLaMa, or your own private models.
3. Ground Deskpro's AI features in your organization's data and knowledge, including help center articles, product documents, and resolved tickets. This enables our AI tools to generate context-aware, organization-specific outputs, and sensitive data never leaves your security perimeter.
4. Securely automate workflows and support operations with AI. Capabilities include AI-suggested responses for agents, intelligent ticket triage, ticket summarization, help center article generation, and chat.

With Deskpro Private, you get the benefits of AI and modern help desk capabilities while meeting your organization's compliance and security requirements. Your agents get more time to focus on complex issues while automating repetitive tasks. The employees, clients, partners, and customers that rely on your support get faster, more accurate responses. And your organization enhances its support operations while maintaining complete data control.

Learn more at deskpro.com/private
When you're ready, book a demo: deskpro.com/demo

Deskpro

About Deskpro

Deskpro is the developer of AI-driven help desk software that empowers organizations worldwide to deliver exceptional customer and employee experiences that translate directly into tangible ROI. Deskpro is available as a cloud SaaS service and can also be deployed in private environments (e.g. VPCs, regional private clouds, sovereign clouds, enterprise data centers). Deskpro can use any available AI foundation model to drive the productivity features and enables organizations with even the strictest security and compliance requirements to see genuine ROI from AI for Customer Service and Employee Support. Trusted by leading enterprises worldwide in banking, technology, financial services, healthcare systems, aerospace and defense, as well as government agencies, Deskpro is led by experts in enterprise software, customer experience, and customer support.

Learn more at deskpro.com.