expedient

Secure AI Gateway

Part of the Expedient AI CTRL Platform

Users are quickly building AI confidence in their personal time. Without approved AI solutions in the workplace, your employees are experimenting with public tools and creating new risks. These can include misuse leading to inaccurate or inappropriate outputs and the public exposure of sensitive information. The company is then liable for any damage or noncompliance with regulations. Nearly every business has experienced a problematic incident from their use of AI, primarily resulting in direct financial loss.[1]

78% of employees have **used unapproved AI tools**[2]

46% of workers have **uploaded sensitive company data** to public AI[3]

The average company is reporting **~$800,000 in losses** over two years from AI incidents[4]

Welcome to Business-Ready AI

Secure AI Gateway is a core service of the **Expedient AI CTRL Platform** and represents the foundational "brains" behind the solution. It enables secure, controlled, intelligent access to a variety of public models, with users being productive within days of deployment. As a cloud-based service, the Gateway delivers uncompromising capabilities along with predictable, flexible pricing options to align optimally with an organization's usage patterns and strategy.

As AI utilization matures, teams can expand to agentic AI solutions to automate and accelerate business workflows. Paired with Secure AI Gateway, you can make these high-powered workflows accessible through the same familiar chat interface.

With Secure AI Gateway, you can:

Accelerate delivery of secure AI chat to improve productivity and access to insights

Avoid the complexity and cost of managing models and infrastructure

Augment AI prompts with company documents for improved context

Prevent shadow AI, misuse of public AI tools, and exposure of sensitive data

Institute granular KPIs and track ROI for prioritized business use cases

Establish guardrails and access controls to models, data, and workflows

Key Benefits of Secure AI Gateway

Empower technical and business users alike with intuitive, intelligent AI solutions

Eliminate shadow AI with controlled, secure access to public models—that's easier to use and easier to manage

Improve AI response quality, context, and accuracy with enterprise data

Reduce demands on employees and enable self-service access to information and answers

Ensure data privacy and compliance with regulations and corporate policies

Bridge to agentic AI with chat-based interfaces

Extend existing identity and access management (IAM) policies to your AI utilization

Intelligent AI Chat

Within days, organizations can solve one of their biggest AI requirements: give your workforce the AI chat tools they need to generate insights and improve productivity. It starts with controlled access to market-leading public models, then you can increase impact by tapping into enterprise data for improved context and accuracy. A key feature of Secure AI Gateway is the smart model router, which auto-selects the optimal model based on the user's prompt. You no longer need to understand the details behind models. Using the router diversifies your model resources "under the hood" while expanding access to highly effective AI for non-technical users—minimizing complexity and maximizing output and outcomes.

Simplified Steps for Intelligent AI Chat

Choose Approach

A. Use Smart Model Router
Let Secure AI Gateway choose the best model based on inputs.

B. Choose by Function
Guide model choice based on function, such as Writing, Business, or Coding.

C. Choose Model
Use this option if you know which model you want to use.

Augment with Company Data

Optionally upload company docs in real-time to enable better enterprise context.

Data is automatically vectorized for AI compatibility.

Privacy controls are enforced.

Enter Prompt and Send Request

Model
Based on your selection, either preferred model is used, or the smart model router chooses the best-fit private or public model based on your prompts.

Data
In addition to uploaded docs, Secure AI Gateway can pair your request with the best-fit private data* to further ground answers and refine outputs.

Refine Results

Review and iterate as needed to arrive at your desired outcome.

AI response includes readout of model and data used.

* Private data, beyond documents uploaded with a prompt, can be made available by integrating your enterprise data into a private AI vector database through our engineered data connectors. Data connectors and database storage are additional services within the AI CTRL Platform.

Key Features of Secure AI Gateway

Multi-model router for model diversity while reducing complexity

Data pairing in real-time to determine which private data sets will yield the best results

Agent builder for domain specific functions and workflow automation

Built-in guidance to avoid AI-patterned writing and assure authentic tone

Policy-based, real-time protection for sensitive data and compliance

Calculated ROI based on defined KPIs to track investment value

Available integrations with IAM, SIEM, and other security platforms

Support for privately hosted models and retrieval-augmented generation (RAG) systems

Part of the AI CTRL Platform, a curated, integrated, cloud-based solution for your critical AI use cases

AI Workspaces for Simplified Agents and Automation

Secure AI Gateway gives individuals the ability quickly design highly tailored AI Workspaces—a unique capability created by uploading data and documents and defining rules and task expectations. These workspaces then act as a filter, or wrapper, around your choice of model to deliver a purpose-built, chat-based agent interface. Responses are grounded in your chosen company data, creating a single source of truth that avoids AI hallucinations. Simple automation steps can be incorporated to streamline straightforward processes or tasks. All access controls, guardrails, observability features, and ROI metrics also still apply.

Once an AI Workspace is defined, you can select it from your primary AI chat interface instead of an available learning model. Additionally, the AI Workspace can be included as an option for smart model routing. For seamless embedding, you can make an API call to an AI Workspace from another tool or web application.

With AI Workspaces, you can:

Power Your Personal Productivity

Simplify search and interactions with a body of knowledge for your own project and productivity purposes with a private AI Workspace.

Example Use Cases

- **AI Assistant:** Create an AI "teammate" to simplify engagement with a large body of knowledge built from product manuals, competitive analysis, as well as transcripts and other artifacts that can be difficult to leverage manually.
- **Product expert:** Empower your personal agent with deep product knowledge to support work efforts.
- **Template Building:** Suggest a best-practice template based on work you've done before.

Empower Others and Offload Inquiries

Internally publish your AI Workspace and create a chat-based portal that allows others across the company to get insights and answers to inquiries.

Example Use Cases

- **Support Technician or Field Engineer:** Query against product docs, knowledge bases, and tickets for real-time troubleshooting support.
- **Human Resources:** Help employees get the HR support they need, such as asking questions about their PPO plans.
- **Marketing:** Make deep, detailed research and competitive analysis easily accessible to anyone in the department.
- **Sales:** Automate workflows for accelerated, consistent RFP research and responses.

A Note About Document Stores

AI Workspaces are ideal for enabling access to tens of lengthy documents. To enable larger data stores at scale, AI CTRL Platform offers data connectors for your applications, such as SharePoint, Salesforce, ServiceNow, and more, to proactively pull enterprise data into a vector database. Data connectors and database storage are additional services within the AI CTRL Platform.

AI Workflows at Scale

As AI solutions scale, sometimes costs can get out of hand. This is especially true for agent-based AI and automated workflows where actions and resource consumption may be obscured or hidden. Teams can develop workflows and agents with low code/no code tools to operationalize AI at scale with attention to cost, accuracy, and change control as volumes grow.

AI Governance Controls

When it comes to AI, governance is essential. Secure AI Gateway provides capabilities across governance, access controls, observability, and KPIs to ensure your AI solutions are being used appropriately and users are leveraging authorized services, models, and data.

Access Controls

Integrations with single sign-on (SSO) and role-based access controls (RBAC) ensure secure and appropriate AI tool usage that is consistent with existing corporate settings. Users can also control access to their AI assets, such as AI Workspaces, using them only personally (Private), sharing with a select set of users (Groups), or sharing across the company (Public).

Data Privacy

Protect sensitive, personally identifiable information (PII) and company-confidential data to ensure compliance with industry and regional regulations as well as company privacy and AI usage policies.

API keys

Users can provision their own API keys for SSO-gated access to all Secure AI Gateway new features via API.

Secure Data

Establish a fortified entry point for AI tools, ensuring data is always protected; all uploaded data within the AI CTRL Platform resides in our private cloud environment.

Logging

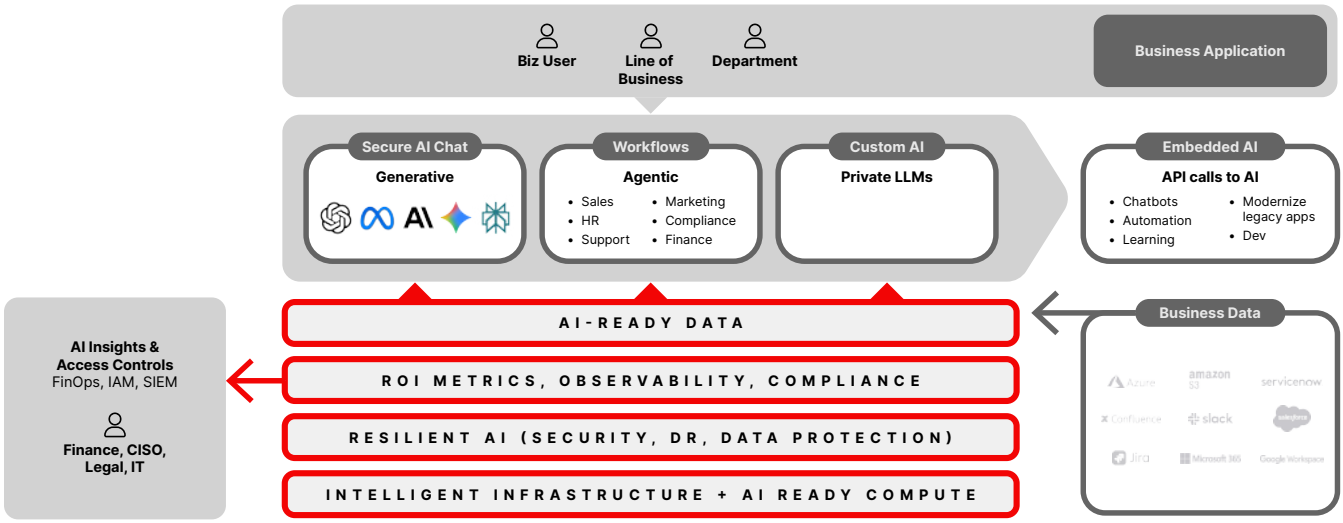
Access to centralized logging improves system oversight and provides historical use data to analyze for continuous improvements and accountability.

KPIs for ROI Tracking

Define your own customized metrics, such as time saved, to align AI usage with tangible, measured ROI every time a workflow is executed.

Secure AI Gateway Is Part of the Expedient AI CTRL Platform

Expedient AI CTRL Platform simplifies adoption with a curated, integrated solution stack that delivers immediate business value, without the risk, complexity, or runaway costs of DIY approaches. Together with Expedient, you can safely deliver robust, resilient AI services companywide while overcoming security, privacy, and complexity roadblocks.



To learn more about AI CTRL Platform and Secure AI Gateway, please visit **expedient.com/ai**

Sources:

1. Infosys, Responsible Enterprise AI in the Agentic Era, Aug 2025
2. WalkMe, an SAP company, New WalkMe Survey Shows Shadow AI Is Rampant; Training Gaps Undermine AI ROI, Aug 2025
3. KPMG, The American Trust in AI Paradox: Adoption Outpaces Governance, April 2025
4. Infosys, Responsible Enterprise AI in the Agentic Era, Aug 2025

expedient