Liminal for MSPs solution brief

A two-page brief for MSPs on Liminal: unlimited multi-model AI, data protection before prompts reach a model, compliance, and how PORT1 helps you deliver it.

November 2026 | PORT1

Liminal is a Secure AI Workspace that keeps sensitive data out of public AI models. Your clients' people get unlimited use of the latest AI models from OpenAI, Anthropic, Google, Perplexity and xAI in one place, and PORT1 launched Liminal for MSPs, its official partnership with Liminal that brings Liminal to MSPs and MSSPs.

What do clients get with Liminal?

Clients get one approved AI workspace with the models their people want, protection for sensitive data, and controls and a full record for the business.

- **Unlimited multi-model AI.** Unlimited use of the latest models from OpenAI, Anthropic, Google, Perplexity and xAI, with no token limits, metering or per-user caps in normal use. Fair-use terms cover automated, high-volume traffic. As of October 28, 2026, that's 38 models, including Anthropic's Claude Opus 5.5.
- **Data protection.** Liminal detects sensitive data in prompts and files, protects it before it reaches a model, and restores it in the response.
- **Control.** Single sign-on with Microsoft Entra ID, Okta, Ping Identity or any SAML 2.0 identity provider, role-based access with custom roles, and policies by user, team or organization.
- **A full record.** Every interaction is logged with the original and protected prompt, the user, the model and the policies applied, with scheduled exports to AWS S3, Azure Blob Storage or Google Cloud Storage for your SIEM.
- **Insights.** Model usage, sign-ins, usage by role, topics, return on investment and where to expand, with sensitive data shown only as counts by type.
- **Connected data.** MCP connections to the systems a client chooses, included at no extra cost.
- **Assistants and Projects.** Reusable assistants with their own instructions, files and preferred model, and Projects that keep related conversations under shared context.

How does Liminal protect sensitive data?

Liminal protects sensitive data by policy before a prompt reaches a model. As of November 2026, it detects personal, health and payment card data and intellectual property with more than two dozen built-in data types, plus custom terms like client names.

Admins choose mask, redact, warn or block for each data type, per model, for the organization, teams or individuals. With masking or redaction, the value is protected on the way in, and Liminal restores the protected details for the user in the response.

How does Liminal support regulated clients?

Liminal is SOC 2 Type 2 certified through independent audit and HIPAA compliant, with business associate agreements (BAAs) available for healthcare customers.

- FERPA, COPPA and CIPA compliant, and built to support GLBA, CJIS, GDPR and CCPA compliance and GxP requirements.
- Each customer runs in its own dedicated environment, with data residency in the US (the default), the UK or the EU.
- Liminal never trains on customer data.
- Liminal holds BAAs with Anthropic, OpenAI and Google for the models it offers. Perplexity and xAI models aren't covered, so teams that handle PHI can be kept on covered models.

How do MSPs deliver Liminal?

MSPs deliver Liminal as a managed service, with a dedicated Liminal tenant for each client and a separate one for their own team.

A Liminal service can include:

- Connecting the client's identity provider for single sign-on.
- Assigning models to teams.
- Setting a policy for each type of sensitive data, including custom terms.
- Training people and building assistants for repeat work.
- Connecting the systems the client already uses.
- Sending logs to your SIEM and reviewing Insights in QBRs.

Liminal is a chat-based workspace. For the few people who need an agent tool, PORT1 recommends a hybrid: Liminal for everyone, plus the agent tool for those few, governed separately.

What does PORT1 provide?

PORT1 brings enterprise-grade security and AI solutions to MSPs and MSSPs and sells only through them. For Liminal, partners get:

- **Demos.** PORT1 runs Liminal demos and joins your client demos when you ask.
- **A sandbox.** Partners get a shared Liminal sandbox, with no client data, to learn Liminal and run client demos.
- **Licensing.** Liminal is licensed per user, and PORT1 bills you monthly in arrears for the licenses in use, month-to-month.
- **PORTER.** Partners get PORTER, PORT1's partner platform, and PORTER Chat answers Liminal product and technical questions 24x7.
- **Security review help.** Liminal's security documents and BAA requests for healthcare clients go through PORT1.

The PORT1 partner program covers billing and support.

Who uses Liminal?

Liminal's customers include Delta Dental of New Jersey/Connecticut, Northern Arizona Healthcare, Prince William County in Virginia, the Indiana Secretary of State and Southern Methodist University.

Justin Lahullier, CIO and CISO at Delta Dental of New Jersey/Connecticut, said: "5x ROI is a conservative number… we're seeing a 5x time improvement."

The full overview is at Liminal for MSPs.

Book a Liminal demo