PORT1

TRACEFORCE FOR MSPs

Traceforce for MSPs solution brief

A 2-page PDF on Traceforce for MSPs: the free AI Risk Assessment, what Traceforce finds and controls, PORTER, deployment, security and the 3 ways to start.

November 2026 | PORT1

Traceforce for MSPs is how MSPs and MSSPs get Traceforce through PORT1. PORT1 launched Traceforce for MSPs, its official partnership with Traceforce that brings Traceforce to MSPs and MSSPs. Traceforce manages the security posture of the AI agents and connectors your clients use across their devices, and you can start with a free AI Risk Assessment.

What does the free AI Risk Assessment show?

The AI Risk Assessment shows what AI is in use on a client's own computers: which AI tools, who's signed in and with what kind of account, what the tools are connected to, and where sensitive data is going into them.

- **No cost.** The AI Risk Assessment is free, and every client company you add gets its first 30 days of Traceforce free, with no device limit.
- **Watch only.** Traceforce runs for 1 to 2 weeks and only watches, so nothing is blocked or changed.
- **Nothing for users to install.** You deploy through your RMM or MDM.
- **A readout in your branding.** PORTER builds a PowerPoint to present, with the script in the speaker notes, and a written report.
- **Prospects too.** You can run it at a prospect, as long as you can deploy to that company's computers.

What does Traceforce find?

Traceforce runs on the device and covers AI in 3 places: in the browser, in desktop apps and in command line (CLI) agents.

- **AI tools and plans.** Each tool with its plan, from personal and free to enterprise, and its risk score.
- **Accounts.** Company accounts told apart from personal ones, using the client's email domains.
- **Connectors.** Built-in connectors and custom MCP servers, with problems like exposed secrets and unpinned versions flagged.
- **Models.** The AI models people use, including from Chrome, Edge and Electron desktop apps.
- **Sensitive data.** Detected on the device, in prompts, tool calls and attachments.

As of November 2026, Traceforce says it tracks hundreds of publicly known AI agents and thousands of publicly known connectors.

What can MSPs control?

Once a client is ready, Traceforce policies can keep AI on company accounts, warn or block on sensitive data, stop risky coding agent actions before they run, and allow only approved connectors, models and AI apps, on supported tools. Traceforce also detects and enforces against prompt injection in Claude Cowork and Claude Code. See Traceforce policies and controls.

What does PORTER add?

PORTER, PORT1's partner platform, is part of Traceforce for MSPs. It tracks every client's assessment, builds branded readouts from the client's data, gives your team PORTER Chat and schedules reports on a client's AI use once its storage is set up.

- **Readouts.** A PowerPoint with the full script in the speaker notes, plus a 2-part Word report for the client's leadership and IT.
- **PORTER Chat.** Help deploying Traceforce, preparing for client meetings, explaining findings and building learning plans for new engineers, plus drafts of emails offering the AI Risk Assessment, webinar agendas and web copy.
- **Ongoing reporting.** Once a client's storage is set up, you create and schedule reports on its AI use and spend, and PORTER emails them to your team, ready to forward to the client.
- **Your whole team.** Add as many PORTER users as you like, at no cost.

How do deployment and security work?

You deploy through your RMM or MDM. PORT1's deployment script runs from your RMM, such as NinjaOne or Datto RMM, and installs Traceforce and its browser extension on each computer. Traceforce supports Windows 10 and 11 and macOS 15 and 26.

- By default, Traceforce stores no prompts or tool calls.
- Data is encrypted in transit with TLS 1.3 and at rest with AES-256.
- Traceforce is ISO/IEC 27001 certified and has a SOC 2 Type II report, which partners can request from PORT1 under the PORT1 partner agreement or an NDA.

More detail is in Traceforce security and privacy.

How do MSPs get started?

There are 3 ways to bring Traceforce to clients: start with an AI Risk Assessment, go straight to the ongoing service, or add Traceforce to your standard stack, which PORT1 recommends for most MSPs.

- The free 30 days apply once per client company, with no obligation, and start when its first computer checks in.
- After that, PORT1 bills you monthly in arrears, per device, for the licenses in use.
- Partnering with PORT1 is free: the partner agreement is free, with no commitment, and PORT1 charges partners no fees for its work.
- PORT1 helps with your first couple of readouts, and joins readout meetings and client calls alongside you where that's useful.

Signup is online and automated, and it gives you full access to Traceforce through PORT1. Learn more at Traceforce for MSPs, follow the Traceforce Blueprint, or watch the demo video.

Start Now