



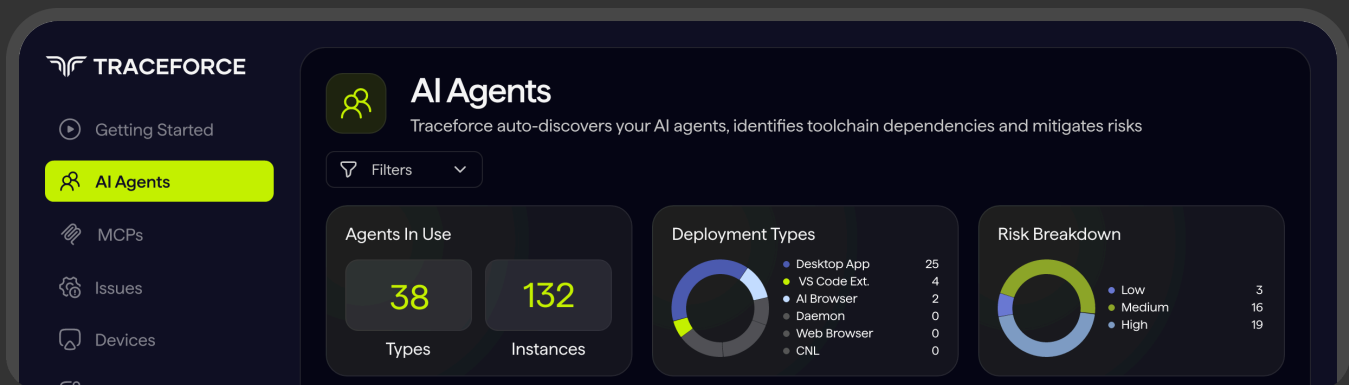
TRACEFORCE

FOR MSPs

PARTNER GUIDE

See and secure the AI running on every computer you manage.

Everything MSPs need to know about Traceforce, the free AI Risk Assessment, and making AI security part of your standard stack.



The short version

If you only read 1 page, make it this one.

- 1 AI is already on your clients' computers.**
Desktop apps, browser tools, coding assistants and AI agents that can reach files, email and business systems. Most of it arrived before anyone decided how it should be used.
- 2 Your stack wasn't built to see it.**
Your RMM, EDR, email security and the rest each watch their own layer. Traceforce adds the AI layer: what's running, who's signed in and on which account, what's going into it, and what it's allowed to do.
- 3 It's easy to start.**
It deploys through the RMM or MDM you already use, and the first results come in within about an hour.
- 4 The first 30 days are free for every client.**
Run a free AI Risk Assessment, or add Traceforce straight to your stack. Either way, there's no obligation.
- 5 PORTER builds the client meeting for you.**
A presentation in your branding with the script already written, plus a 2-part report you send afterwards.
- 6 It becomes a recurring service.**
Some findings get fixed once. Others need watching every month as new tools arrive. That's what makes it a managed service.
- 7 PORT1 is with you the whole way.**
We help you sell it, deploy it and run the client meeting.

IN THIS GUIDE

Why AI, why now	3
AI is the newest layer in your stack	4
What Traceforce is and what it finds	5
The opportunity for MSPs	7
2 ways to start	8
Your best door-opener	9
How the AI Risk Assessment works	10
PORTER and the readout	11
From findings to a managed service	15
Coverage, deployment and privacy	16
Working with PORT1	19
FAQ and glossary	20
Get started	22

Ready when you are

port1.io/traceforce

AI is already on every computer you manage

Nobody rolled it out. People picked up tools that helped them get their work done, and those tools keep getting more capable. Today AI writes emails, summarizes client files, writes code and, more and more, takes action on its own.

45%

of employees now use AI regularly on company devices, up from 15% a year earlier.

2026 Verizon DBIR

67%

of those employees use AI through personal, non-corporate accounts.

2026 Verizon DBIR

58%

of U.S. small businesses say they use generative AI.

U.S. Chamber of Commerce, 2025

3 things changed at once

AI moved onto the device

It lives in desktop apps, coding tools, browser extensions and command-line tools, well beyond a website somebody visits.

Accounts got blurry

A free personal plan and a company plan look the same on screen. The personal one may train on what's typed in, and nobody can switch it off when someone leaves.

AI started taking action

AI agents connect to files, email, code and databases through MCP servers and other connectors, often with permission to change or delete what they reach.

THE WAY WE THINK ABOUT IT

Businesses spend years putting strong doors, locks, cameras and alarms on the building. Unmanaged AI is a hole in the back wall where the data pours right out.

9 seconds

In April 2026, an AI coding agent deleted PocketOS's entire production database, backups included, in about 9 seconds. It had been told not to.

AI arrived faster than the controls around it, the way new technology usually does. It can be seen and managed like anything else in the business.

AI is the newest layer in your stack

Every tool in your standard stack earned its place the same way. A new kind of risk appeared, the tools you already had weren't built to watch it, and a new layer went in. First at a few clients, then everywhere.

A TYPICAL MSP STACK

NEW LAYER

AI security · Traceforce

Sees and controls the AI running on every computer

MFA and identity

Makes a stolen password useless

Security awareness training

Helps people spot a scam

Backup

Brings data back after the worst day

DNS filtering

Blocks dangerous sites

Email security

Stops phishing before it lands

EDR or MDR

Watches for malicious behavior on the endpoint

RMM

Keeps every computer managed and patched

What the AI layer adds

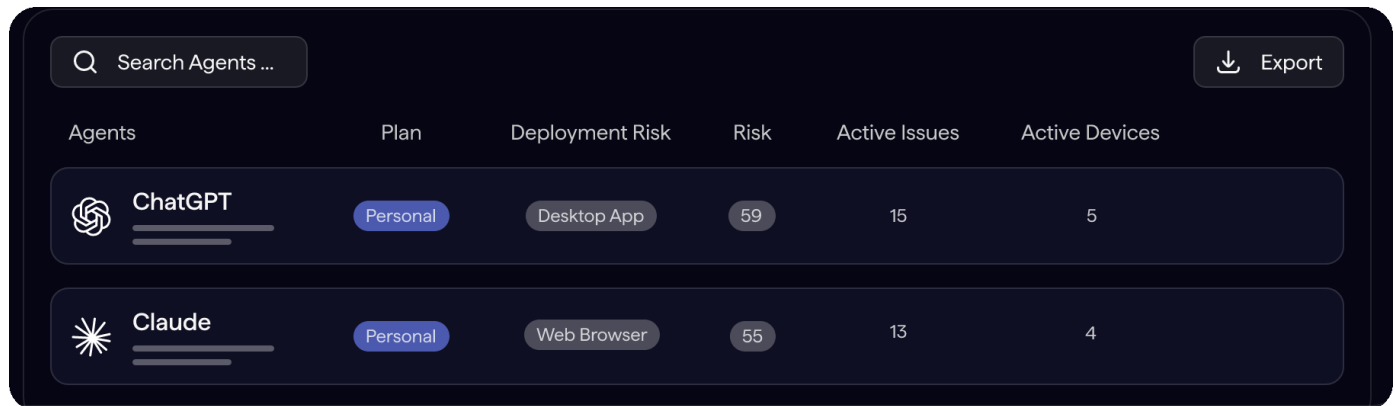
The rest of your stack watches processes, files, mail and traffic. The AI layer watches what those tools weren't built to see.

- Which AI tools are running, from desktop apps and browser tools to coding assistants and local models
- Who's signed in, and whether it's a company account, a consumer plan or a personal one
- Whether what people type is being used to train someone else's AI
- Passwords, keys and personal information going into AI conversations
- What AI agents and connectors can reach, and whether they can change or delete data
- Passwords and keys sitting in plain text in AI configuration files

AI is a new category of risk, and it's on every computer you manage. We think it belongs in your stack alongside everything else, which is why a lot of MSPs are adding Traceforce to every managed computer at every client.

What Traceforce is

Traceforce is an on-device AI security platform. It finds the AI running on each computer, scores the risk, flags what needs fixing and puts controls in place when you're ready. Traceforce for MSPs is the official Traceforce channel for MSPs and MSSPs, run by PORT1.



The screenshot shows a dark-themed interface with a search bar at the top left labeled 'Search Agents ...' and an 'Export' button at the top right. Below is a table with columns: Agents, Plan, Deployment Risk, Risk, Active Issues, and Active Devices. Two agents are listed: ChatGPT and Claude.

Agents	Plan	Deployment Risk	Risk	Active Issues	Active Devices
 ChatGPT	Personal	Desktop App	59	15	5
 Claude	Personal	Web Browser	55	13	4

Every AI tool in use, with the plan behind it, how it's deployed and its risk score.

COMPONENT 1

The agent

A lightweight agent on each Windows and Mac computer. It sees desktop AI apps, coding assistants, IDE extensions, command-line tools, local models, and the MCP servers and connectors they use.

COMPONENT 2

The browser extension

Covers AI in Chrome and Edge, where a lot of AI use happens. It sees which account someone signed in with, what plan they're on, and when sensitive information goes into a conversation.

The Atlas registry

Every AI tool and connector Traceforce finds is checked against Atlas, Traceforce's library of security ratings for more than 100 AI agents and 800 MCP servers and connectors. Each one is scored on things like how sign-in works, whether MFA is supported, what's kept and for how long, and what the tool is allowed to do. Scores run from 0 to 100 and map to the NIST 800-53 framework.

Built to sit alongside your stack

Traceforce works next to your EDR, email security and everything else you run. It fills in the AI layer, deploys through the tools you already use, and manages every client from 1 console.

What Traceforce finds

Findings fall into 3 groups, and each one is a conversation your client will want to have.

Who's using AI, and how

- Personal accounts signed into AI
- Work email on consumer plans
- AI sign-ins with no MFA

What AI is allowed to do

- AI connected into business systems
- AI that can change or delete data
- Connections with no sign-in, or secrets stored in plain text

Where information is going

- What's typed going into training
- Passwords or keys pasted into AI
- Personal and contact details going into AI tools

Issue Breakdown	Issue Description	Risk Attribute	Status	Issue Detected	Remediation
6 incidents	Personal email authentication detected	Identity Federation	Active	Sep 23, 2026 11:46 AM	Use SSO if available. Otherwise consider using company email instead of personal email.
11 incidents	Credentials detected in AI conversations	Sensitive Data Handling Detection coverage	Active	Sep 22, 2026 03:05 AM	Immediately rotate any exposed credentials, and audit access logs for unauthorized use. Remind users to never share credentials in AI conversations.
5 incidents	Training data usage is enabled	Training Data Usage	Active	Sep 23, 2026 07:31 PM	Disable training data usage.
7 incidents	MFA disabled	MFA Support	Active	Sep 23, 2026 07:31 PM	Enable MFA.

Issues found across AI tools, each with a risk rating and remediation guidance.

Issue Breakdown	Issue Description	Risk Attribute	Status	Issue Detected	Remediation
13 incidents	Secrets exposed in plain-text in MCP configurations	Secrets Exposure	Active	Sep 23, 2026 07:41 PM	Avoid putting plain-text secrets in MCP server configurations. Such secrets are visible to anyone with file access.
2 incidents	Destructive commands detected on MCP servers	Unsafe Local Commands	Active	Sep 23, 2026 07:41 PM	Remove destructive commands from the MCP.
9 incidents	Local service execution mode detected	Execution Mode	Active	Sep 16, 2026 01:46 PM	Run MCP servers in a local container rather than a local service to improve isolation.
9 incidents	Unencrypted HTTP connections detected	Connection Security	Active	Sep 16, 2026 01:46 PM	Avoid using http connections.

Issues found across MCP servers, the connections AI uses to reach files, code and systems.

Fix it once, or keep watching

Some findings are settings or accounts, and once they're fixed they stay fixed. Others are limits built into the AI tools themselves, like no admin logging or no choice about where data is stored. The work there is knowing they exist and deciding which tools are right for the business. New tools and vendor updates change both lists every month.

Your clients are asking about AI

48%

of MSPs say AI and automation is their clients' top need for 2026, ahead of security at 42% and backup at 36%.

Kaseya 2026 State of the MSP, 1,061 MSPs

13%

of MSPs say AI and automation is a meaningful revenue source for them today.

Kaseya 2026 State of the MSP, 1,061 MSPs

That gap is the opportunity. Clients want help with AI, and most MSPs haven't turned it into a service yet. Traceforce gives you something concrete to offer: visibility first, then controls, then an ongoing service.

The security conversation clients want to have

Most security conversations are about risk nobody can see, and clients buy them the way they buy insurance. AI is different. Leadership wants to know what their people are doing with it, and it lets you help them say yes to AI, safely.

A project that becomes a service

Some of what Traceforce finds gets fixed once. The rest keeps changing as people pick up new tools and vendors ship updates. Watching it, adjusting controls and reporting back is recurring work, and recurring revenue.

Built for how MSPs work

Multi-tenant from day 1. Deploys through your RMM or MDM. No minimums, no long-term contracts, month to month. And a channel team that works alongside you.

INNOVATION, SAFELY

IT has spent years being treated like a utility. AI hands MSPs a seat at the strategy table again. Your clients are counting on someone to help them adopt it safely, before they fall behind. That someone can be you.

2 ways to start

Some MSPs add Traceforce to their stack from day 1. Others start with a free assessment at a client and go from there. Both end up in the same place.

OPTION A

Add it to your stack

Deploy Traceforce to every managed computer at every client, the same as your EDR or your backup. A lot of MSPs are doing exactly this. Once you've seen what it shows you, it's hard to go back to not knowing.

- Visibility across every client from day 1
- Turn on controls as each client is ready
- Offer AI security to every client as part of what you already do

OPTION B

Start with an AI Risk Assessment

Pick a client, deploy Traceforce, let it run for 1 to 2 weeks and walk them through what it found. PORTER builds the presentation and report for you. If the client moves forward, great. Run another one.

- Costs you nothing
- Report-only, so nobody is interrupted
- 1 of the best ways to start with a new business

**30
days**
free for every client

Whichever way you start, each client's first 30 days are free, starting when the first computer checks in. It's a 1-time free period for each company, with no obligation. If a client doesn't move forward, remove Traceforce within the 30 days and there's no charge.

We think Traceforce belongs on every computer you manage. You don't have to start there.

Your best door-opener right now

71%

of MSPs say acquiring new customers is their biggest challenge.

Kaseya 2026 State of the MSP

A free AI Risk Assessment is 1 of the easiest yeses you'll get from a business you don't work with yet. Most businesses want to know what AI their people are using, and very few have ever seen it.

How it works with a prospect

- 1 Offer it**
Ask a prospect what they're doing with AI today. The answer usually leads to "why don't we run an assessment and see what's really going on?"
- 2 Run it**
Traceforce runs for 1 to 2 weeks. Nothing is blocked and nobody is interrupted.
- 3 Show them**
You walk into the meeting knowing their environment better than anyone, with a presentation built on their own data.
- 4 Earn it**
The readout ends with a clear recommendation: your managed service.

Why it lands

AI arrived ahead of the tools most businesses have. Whoever manages their IT today, this is likely something they've never seen about their own business.

Works with your clients too

It's a strong agenda item for a QBR and a natural way to introduce a new service.

Free, once per company

Every company's first 30 days are free, so each business gets 1 free assessment.

AN EASY WAY TO BRING IT UP

"Most businesses have more AI running than they realize. We're offering a free AI Risk Assessment that shows what's in use, who's signed in and what it can reach. Nothing gets blocked and nobody's interrupted. Would that be useful?"

How the AI Risk Assessment works

Most assessments go from deployment to readout in 2 to 3 weeks, well inside the client's free first 30 days.

- | | | |
|----------|---|--|
| 1 | Get set up
Day 0 | Sign up at port1.io/traceforce . The partner agreement is free with no purchase commitment, and we set up your Traceforce console. |
| 2 | Add the client
Day 0 | Create an organization for the client in your console. It takes minutes. |
| 3 | Deploy
Day 1 | Push the agent and browser extension through your RMM or MDM. The first inventory comes in within about an hour. |
| 4 | Let it run
1 to 2 weeks | Give it at least 1 week and up to 2. Everything reports to you only. Nothing is blocked and nobody is interrupted. |
| 5 | Generate the readout
Before the meeting | Connect the client in PORTER, pull the data and download the presentation and report. Read through the script and make it yours. |
| 6 | Present
About 20 minutes | Walk the client through what you found. Book 45 minutes so there's room for questions. |
| 7 | Follow up
Same day | Send the report and book the policies and controls session before you leave the room. |
| 8 | Turn it on
Ongoing | Put the agreed policies in place, fix what can be fixed, and keep watching as your managed service. |

What the client experiences

An agent and a browser extension go on their computers, and that's it. There's nothing for their people to do.

Tell staff or not?

Ask the client before you deploy. Some want their people to know, and some would rather see things as they are.

PORTER builds the readout for you

PORTER is PORT1's partner platform. It turns the Traceforce data from an assessment into a client-ready presentation and report, in your branding, in minutes.

SET UP ONCE

Your brand, your service

Add your company name, website, logo and colors in PORTER Settings, and name your service. The default is Managed AI Security, or call it whatever fits your lineup. Everything PORTER generates carries your branding, and the client only ever sees you.

WHAT YOU GET

The presentation

- 6 to 13 slides, built for about 20 minutes
- The full spoken script in the speaker notes, in plain business language
- Names the AI tools, never the people
- Recommends your own service by name
- Refers to Traceforce only as "the platform"

WHAT YOU GET

The report

- An editable Word document, sent as a PDF after the meeting
- Part 1 for leadership: a letter-style executive summary, the key numbers, what was found and what you recommend
- Part 2 for IT: every tool, connection and finding, remediation guidance, and exactly what was and wasn't collected

It's all yours to edit

Change anything you'd say differently. Once the files are downloaded, they're yours.

PORTER answers your questions too

PORTER includes an AI assistant that knows Traceforce, from deployment steps to what a specific finding means. Ask it any time.

The readout was designed to feel like a conversation with a trusted advisor. It opens with AI as an opportunity for the business, shows what's actually happening, and ends with a clear next step.

What your client sees

Here's a sample readout PORTER generated for Harbor & Pine Accounting, a fictional firm with 58 computers. The logo, the service name and every number come from your settings and the client's own data.

AI Risk Assessment

Harbor & Pine Accounting


Data as of September 17, 2026

The cover, in your branding

How is AI being used

11	computers signed into AI with a personal account
15	computers using work email on a consumer plan
20	computers where AI sign-in needs only a password, without MFA


Data as of September 17, 2026

How AI is being used

What AI is allowed to do

9 of 58	computers where AI connects into your systems
7	computers where AI can delete your data
4 of 23	connections that nobody can identify


Data as of September 17, 2026

What AI is allowed to do

Where your information is going

12	computers where what's typed goes into training
3	computers where passwords or keys went into AI
6	computers where somebody's contact details went in


Data as of September 17, 2026

Where information is going

What we'd fix first

Start here	Then
Switch off training data use on 12 computers	Agree what AI is approved for use here
Move 9 people off personal sign-ins	Add controls to prevent these risks
Stop AI from deleting data on 7 computers	Keep watching, because this changes monthly

105 items to fix in total, all of them listed in the report.


Data as of September 17, 2026

What to fix first

What we recommend

Managed AI Security, run end to end by us.

What this looks like	What happens next
We watch what AI is running here and what it's connected to.	We walk you through our recommended policies and controls.
We set the guardrails and keep them current as the tools change.	You sign off on the rules we enforce.
Nothing lands on your people to operate.	We fix what can be fixed, riskiest first.

The next step is to move forward with our Managed AI Security.


Data as of September 17, 2026

Your service, recommended by name

Sample slides from a PORTER readout. Harbor & Pine Accounting and “Your MSP” are fictional.

The report that follows the meeting

Executive summary

AI is already part of how work gets done at Harbor & Pine Accounting, and there's more of it coming. That's a good thing. AI is one of the biggest opportunities in years for a business to get more done with the people it has, and the returns are real. It also tends to arrive before anybody has decided how it should be used. People pick up tools that help them, those tools connect to other things, and the business ends up relying on something it never set up on purpose.

So we took a look. Between August 18, 2026 and September 17, 2026 we ran a read-only assessment across 58 of your computers to see which AI tools are in use, which accounts they're signed in under, and what they're connected to. Nothing was blocked or changed, and nobody's work was interrupted.

Some of what we found tells us there's work to do. Sensitive information has already gone into AI tools the business doesn't control, and once it's there it can't be pulled back. Some of what people type in is being used to train AI models the business doesn't own. Some AI is signed in on personal accounts or consumer plans, which sit outside the business, so nobody here can switch them off when someone leaves or see what's gone into them. And some AI tools can delete business data on their own, with no approval step in front of them.

Most of this comes from people trying to get their work done, which is how AI arrives in almost every business. Left alone, though, it grows. New tools arrive every month, and the ones already here change what they can do with each update. Some of the tools also have limits built in that nobody can change. And nothing is watching any of it today. The moment that costs a business is usually a client asking what happened to their information, and that's a hard moment to be without an answer.

That's why we're recommending our Managed AI Security. We'd run it for you end to end: we watch what AI is running and what it's connected to, fix what can be fixed, and keep the guardrails current as the tools change, so nothing lands on your people to operate.

Here's how we'd start. We'll bring you our recommended policies and controls, covering which AI tools are approved, what they're allowed to connect to, and what should never go into them, and we'll go through them with you and anyone on your team you'd like involved. We recommend the settings and you decide on them, so the rules we enforce match how you want the business to run. Once they're agreed, we put them in place and fix what can be fixed, starting with what carries the most risk. From there we keep watching, because this picture changes every month.

Getting ahead with AI and staying in control of your business can go together. With the right guardrails in place, you get both: a business that uses AI with confidence and stays resilient while it does. We'd like to help you get there. The next step is to move forward with our Managed AI Security, and we'll set up a session with you and your team to go through our recommended policies and controls.

Data as of September 17, 2026. Document version 1.0.

Page 3 of 25

At a glance

8	58	61	31
AI tools in use	Computers assessed	Accounts signed in to AI	Computers with a finding to act on

7 of what we found are the items we'd act on first. Every count below is out of the 58 computers we assessed.

What we found	Computers
Computers where what's typed goes into training	12
Computers signed into AI with a personal account	11
Computers where AI can delete your data	7
Computers where passwords or keys went into AI	3
Computers where AI can change your data	6
Computers where somebody's contact details went in	6
Computers using work email on a consumer plan	15

Data as of September 17, 2026. Document version 1.0.

Page 4 of 25

The report goes to the client the same day, as a PDF, after you've walked them through the findings.

Part 1 speaks to the owner

A 1-page summary in plain language, the key numbers, what was found and what you recommend.

Part 2 is for whoever handles IT

Every AI tool and connection with its risk level, every finding in full, the platform's own remediation guidance, the computers and accounts involved, and what was and wasn't collected.

It fits the client

Sections with nothing in them don't appear, so a lighter assessment gets a shorter report.

What we recommend

We'd run this for you end to end as our Managed AI Security. We watch what AI is running here and what it's connected to, we set the guardrails and keep them current as the tools change, and we handle it when something new turns up. Nothing lands on your people to operate and there's no console for anybody here to learn. What comes back to you is a read on where things stand and what we did about it.

16 of the items we found can be fixed, and they stay fixed. The other 13 are limits in the tools themselves, so those you can only decide to live with. That second list changes every time a vendor ships an update, which is the reason this is a service rather than a project. If all of it were fixable, you'd want a one-time piece of work and we'd say so.

Here's how we'd start. We bring you our recommended policies and controls, covering which AI tools are approved, what they're allowed to connect to, and what should never go into them, and we go through them with you and anyone on your team you'd like involved. We recommend the settings and you decide on them, so the rules we enforce match how you want the business to run. Then we put them in place and work through the list below, starting with what carries the most risk.

What we'd do	Computers	Findings to fix
Switch off training data use on 12 computers	12	14
Move 9 people off personal sign-ins	11	13
Stop AI from deleting data on 7 computers	7	12
Change the credentials exposed on 3 computers	3	3
Limit what AI can change on 6 computers	6	9
Agree what personal information may go into AI	6	6
Move 14 accounts onto an enterprise plan	15	16
Turn on multi-factor for 19 accounts	20	21

The next step is to move forward with our Managed AI Security, and we'll set up a session with you and your team to go through our recommended policies and controls.

Data as of September 17, 2026. Document version 1.0.

Page 8 of 25

What was and wasn't collected

Running an assessment like this on people's computers raises a fair question about what was collected. This section is the answer in writing, so it can be handed to anybody who asks rather than repeated from memory.

What people typed into AI tools was not kept. Where something sensitive was detected in a conversation, what's recorded is that it happened and where, rather than the conversation. Keeping prompt-level detail is a separate setting that has to be switched on deliberately, and it was not switched on for this assessment. Where it is turned on, what it keeps is redacted by default and it writes to storage you own rather than to the platform.

Where the assessment found something that looked like a password or an access key, the credential itself was not uploaded anywhere. It's reported as a finding so it can be changed, which is the point of finding it.

For browsing, web addresses were recorded with the parameters stripped out of them, and page contents and request headers were not collected at all.

What was collected travels encrypted and is stored encrypted, in a tenant separated from every other organization's at the database level.

What this isn't is a monitoring tool pointed at people. It looks at business AI use on company-managed computers, and the content of what anybody typed isn't part of what it keeps. What the findings describe is which tools are running, how they're set up, and what they're connected to.

Inside this report, individual computers and accounts appear in 1 section and nowhere else, so that part can be removed before the document goes any further if that's the right call for your business.

Data as of September 17, 2026. Document version 1.0.

Page 23 of 25

Executive summary, written as a letter

At a glance

What we recommend

What was and wasn't collected

Running the readout

A few things that help

- **Book 45 minutes.** The presentation runs about 20, which leaves room for questions.
- **Lead with the opportunity.** AI is good for the business. The findings are about using it on purpose.
- **Say what each number is out of.** “12 of 58 computers” lands better than “12 computers.”
- **Name the tools, never the people.** People picked up what helped them get their work done.
- **Send the report after the meeting.** Same day, as a PDF.
- **Book the next step before you leave.** The policies and controls session, with a date.

A lighter readout is still a good one

Some clients use less AI than you'd expect. That's still a useful meeting. Nothing is watching today, new tools arrive every month, and it's the right time to agree what's approved before it grows.

What clients ask

“Were you monitoring our people?”

What people typed wasn't kept, and passwords weren't uploaded. The report has a section that spells out exactly what was and wasn't collected.

“We haven't really adopted AI.”

Point to what's running on their own computers. It usually arrived without anyone deciding it should.

“Can't we just block it all?”

Blocking tends to push AI onto phones and home computers, where there's no visibility at all. 1 approved path works better.

“Doesn't our Microsoft licensing cover this?”

It covers their own Microsoft environment. Personal accounts and the other AI tools people use sit outside it.

“Can't we just write a policy?”

A policy says what's allowed, controls make it stick, and monitoring shows whether it's working. You want all 3.

“What does it cost?”

Keep pricing out of the room and send it along with the report.

From findings to a managed service

During an assessment, Traceforce only observes. When the client's ready, the same agent starts enforcing the policies you agree with them. There's nothing new to deploy.

Policy Controls

Security controls and actions for this policy

Controllable Issue Controls

7

ENFORCEABLE BY TRACEFORCE

Rule	Requirement	On Violation	Actions
Identity Federation Which email domains are permitted	Only company email permitted	Block login	
Sensitive Data Handling Whether sensitive data such as credentials and PII can be minimized Detection coverage 17	Disallow credentials and all PII	Warn user	

MONITOR & ALERT

Rule	Requirement	On Violation	Actions
MFA Support Types of multi-factor authentication the agent supports	On (MFA Required)	Report as issue	
Training Data Usage Prevent vendors from using user inputs for agent training	Off (No Training)	Report as issue	
Allowed Connector Types Types of 3rd party integrations the agent can use	No Connectors Allowed	Report as issue	
Risky Action Handling Whether the agent handles failures or high risk actions safely Detection coverage 17	Default for all categories Do not allow delete	Default Report as issue	

A Traceforce policy for general-purpose AI tools. Each control can block, warn or report.

TRACEFORCE ENFORCES

- Block sign-ins to AI tools like ChatGPT and Claude with anything other than a company account
- Warn people before passwords, keys or personal information go into supported AI tools
- Stop AI coding agents from taking risky actions, like deleting data, before they run

TRACEFORCE FLAGS, YOU FIX

- Training switched on
- MFA switched off
- Work email on consumer plans
- AI connections with write or delete access
- Passwords and keys in plain text in AI configuration files

YOU KEEP WATCHING

- Limits built into the AI tools themselves
- New AI tools as they arrive
- Changes after vendor updates

This is the part that makes it a service.

The policies and controls session

You bring recommended policies covering which AI tools are approved, what they're allowed to connect to and what should never go into them. The client decides, and you put it in place.

Roll it out like anything else

Turn policies on for a pilot group first, then everyone. Turn controls on 1 at a time, so nothing surprises anybody.

What Traceforce covers

Computers

Windows 10 and 11, and current versions of macOS on Apple Silicon and Intel.

Browsers

Chrome and Edge.

AI tools

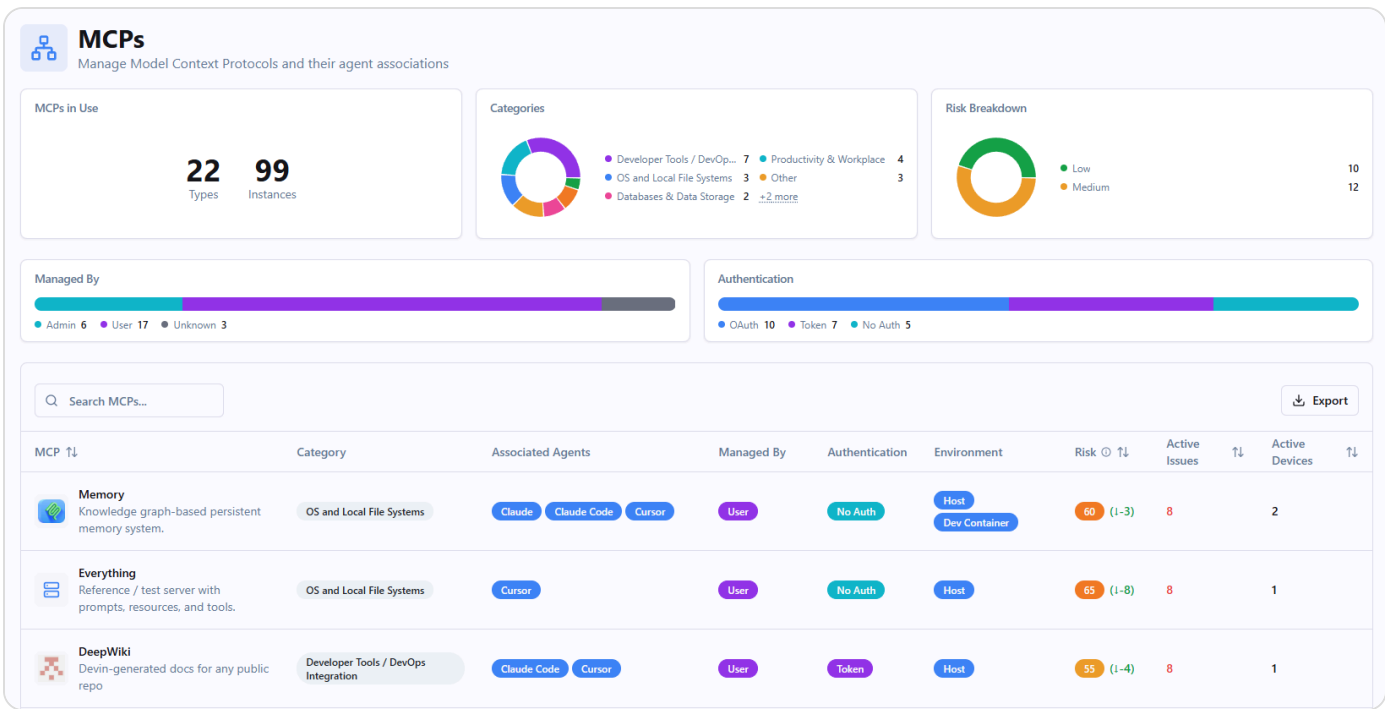
Desktop apps, browser tools, AI browsers, coding assistants, IDE extensions, command-line tools and local models. That includes ChatGPT, Claude, Gemini, Microsoft 365 Copilot, Perplexity, GitHub Copilot, Cursor, Claude Code, Windsurf, Codex, Ollama and LM Studio.

Sensitive information

Passwords, API keys and access keys, personal and financial details like Social Security and card numbers, and contact details, when they go into supported AI tools.

MCP servers and connectors

MCP is how AI plugs into files, email, code and business systems. Think of it as the USB-C cable for AI. Traceforce finds every MCP server and connector in use and checks how it signs in, whether it can read, write or delete, where it runs, whether its connection is encrypted, whether secrets are stored in plain text, and whether it can run destructive commands.



MCP servers in use, with the AI tools they connect to, how they sign in, where they run and their risk scores.

Deploying and managing it

Deploy with the tools you have

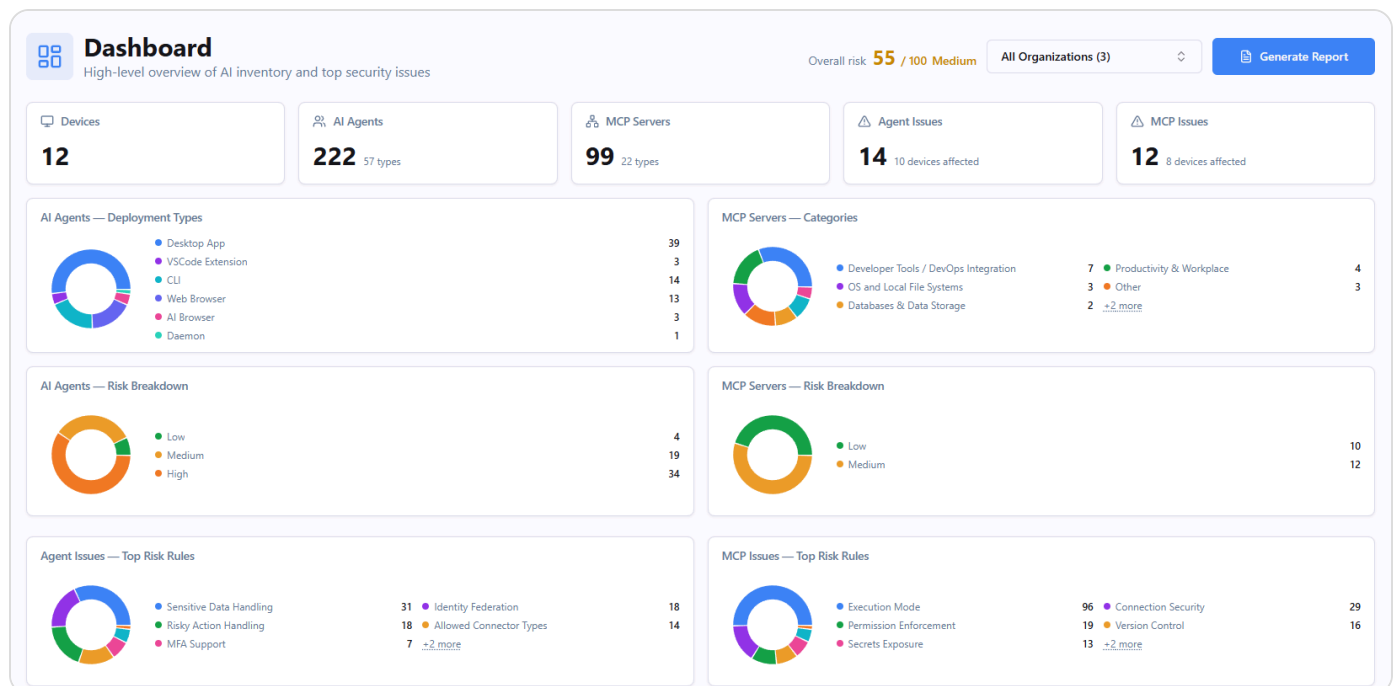
Traceforce deploys through virtually any RMM or MDM, including NinjaOne and Datto. Our step-by-step onboarding guide walks you through it, with instructions for the most popular RMMs and MDMs. If you run something else, we'll help you get it done.

- **Windows** installs through your RMM with a single script that puts the agent in place and sets up the browser extension for Chrome and Edge.
- **Mac** deploys through your MDM.
- **Results come in quickly.** The agent reports in within minutes, and the first inventory lands within about an hour.
- **Nothing for users to do.** No prompts and nothing to sign into.

1 console for every client

Each client is its own organization under your Traceforce account. Switch between them, or see all of them together on the dashboard.

- **You control access.** By default, only you can get into a client's organization.
- **Clients can have their own view.** If a client's internal IT wants access, add single sign-on for them with Entra ID, Okta or OneLogin.
- **Clean removal.** If a client decides not to move forward, the onboarding guide covers removing everything cleanly.



The Traceforce dashboard, here showing every organization together.

Privacy and security

The first question a client asks is usually what's being collected. Traceforce looks at business AI use on company-managed computers, and the answer is short.

Analysis happens on the computer.

Only metadata and findings go to the platform.

What people type isn't kept.

When sensitive information is detected, Traceforce records that it happened and where, without keeping the conversation.

Passwords stay put.

A credential found on a computer is reported so it can be changed. The credential itself is never uploaded.

Browsing is kept to a minimum.

Web addresses are recorded with their parameters stripped. Page contents and request headers aren't collected.

Logging is optional, and it's the client's.

Conversation logging is off by default. If a client wants it, it's redacted by default and writes to storage the client owns in AWS, Google Cloud or Azure.

Encrypted and isolated.

Hosted on AWS, encrypted in transit and at rest, with every organization separated at the database level.

Independently certified.

Traceforce holds SOC 2 Type II and ISO/IEC 27001:2022 certifications.

What was and wasn't collected

Running an assessment like this on people's computers raises a fair question about what was collected. This section is the answer in writing, so it can be handed to anybody who asks rather than repeated from memory.

What people typed into AI tools was not kept. Where something sensitive was detected in a conversation, what's recorded is that it happened and where, rather than the conversation.

Keeping prompt-level detail is a separate setting that has to be switched on deliberately, and it was not switched on for this assessment. Where it is turned on, what it keeps is redacted by default and it writes to storage you own rather than to the platform.

Where the assessment found something that looked like a password or an access key, the credential itself was not uploaded anywhere. It's reported as a finding so it can be changed, which is the point of finding it.

For browsing, web addresses were recorded with the parameters stripped out of them, and page contents and request headers were not collected at all.

What was collected travels encrypted and is stored encrypted, in a tenant separated from every other organization's at the database level.

What this isn't is a monitoring tool pointed at people. It looks at business AI use on company-managed computers, and the content of what anybody typed isn't part of what it keeps. What the findings describe is which tools are running, how they're set up, and what they're connected to.

Inside this report, individual computers and accounts appear in 1 section and nowhere else, so that part can be removed before the document goes any further if that's the right call for your business.

Data as of September 17, 2026. Document version 1.0.

Page 25 of 25

Every PORTER report includes this page, so the privacy answer is in writing for anyone who asks.

Client running a security review?

Bring us in. We'll help you work through the questions so you can answer them with confidence.

Working with PORT1

PORT1 is a channel-only company, founded by MSPs and built for MSPs. We run the official Traceforce channel for MSPs and MSSPs, and we work alongside you rather than handing you a portal.

We help you sell it

Talk tracks, demos, and we'll join your client meetings whenever you want us there.

We help you deploy it

Onboarding, a step-by-step deployment guide and hands-on help with your first clients.

We build the readout

PORTER turns every assessment into a presentation and report in your branding.

We answer the questions

PORTER's AI assistant knows Traceforce, and our team is a message away. We handle anything that needs Traceforce, so you only ever have 1 place to go.

We keep the terms simple

No minimums, no long-term contracts, month to month. The first 30 days are free for every client.

We only work with MSPs

PORT1 is channel-only. We only sell to MSPs and MSSPs.

INTERNAL-USE CREDIT

10%

back every month

Earn your internal use

Every month, 10% of what we bill you for your clients, across all our solutions, comes back as a credit toward your own internal use of any of our solutions. Mix and match however you like. The credit resets each month and can cover your internal-use bill completely.

HOW SUPPORT WORKS

Your clients



You



PORTER



PORT1



Traceforce

Your clients come to you. You come to us, through PORTER or support@port1.io. We take care of anything that needs Traceforce.

Frequently asked questions

Is there a minimum?

No minimums and no long-term contracts. It's month to month, and you can start with a single client.

What does an assessment cost?

Nothing. Every client's first 30 days are free, once per company, with no obligation.

What happens after the 30 days?

If the client moves forward, billing starts from there. If not, remove Traceforce within the 30 days and there's no charge.

Will it slow computers down or get in anyone's way?

The agent is lightweight. During an assessment it only observes, so nothing is blocked and nobody is interrupted.

Does it replace my EDR or DLP?

It sits alongside them. They each watch their own layer, and Traceforce covers the AI layer.

Can I run an assessment for a business I don't manage yet?

Yes, and it's 1 of the best ways to start that relationship. How you deploy it is up to you and the prospect.

Will my client see the Traceforce name?

The readout carries your brand and your service name and refers to "the platform." The agent and browser extension on their computers carry the Traceforce name.

Can my client have their own access?

Yes. Add single sign-on for their IT team and they get their own view of their organization.

How long does deployment take?

Setting up a client takes minutes, and the first inventory comes in within about an hour of deploying.

Do I need to be an AI expert to sell this?

PORTER writes the readout script in plain business language, and PORT1 will join the meeting if you'd like.

Does it work on Macs?

Yes. Traceforce covers Windows and Mac, and deploys to Macs through your MDM.

What if a client already pays for an enterprise AI plan?

Traceforce shows who's using it and who's still on a personal or consumer plan alongside it. The readout even calls out what's already set up well.

Can I use Traceforce inside my own company?

Yes. Every month you earn an internal-use credit on what you bill your clients through PORT1, and it applies to any of our solutions.

What does the client need to do?

Nothing beyond saying yes. You deploy it, and there's nothing for their people to install or sign into.

Where do I get help?

Ask PORTER any time, or email support@port1.io.

Glossary

AI agent

AI that can take action, like editing files, running commands or updating records, as well as answering questions.

AI Risk Assessment

The free, report-only assessment you run for a client with Traceforce and present with PORTER.

Atlas registry

Traceforce's library of security ratings for AI tools, MCP servers and connectors.

Browser extension

The Traceforce component that covers AI used in Chrome and Edge.

Connector

Anything that links an AI tool to another system, including MCP servers.

Consumer plan

A free or personal AI plan, as opposed to a business plan the company administers.

Controllable issue

A finding that comes from a setting or an account, so it can be fixed.

Limit

A finding that comes from how an AI tool is built. It can't be changed, only known and managed.

MCP

Model Context Protocol, the standard way AI tools connect to files, apps and data. An MCP server is 1 of those connections.

Organization

A client's own space in your Traceforce console.

PORTER

PORT1's partner platform. It builds the readout and answers your Traceforce questions.

Readout

The client meeting where you present what the assessment found.

Standard stack

The tools you deploy to every managed computer at every client.

Training data use

A setting that lets an AI vendor use what's typed in to train its models.

SOURCES

Verizon, 2026 Data Breach Investigations Report. Employee AI use on corporate devices and non-corporate accounts.

Kaseya, 2026 State of the MSP Report. Survey of 1,061 MSPs worldwide.

U.S. Chamber of Commerce, Empowering Small Business, August 2025.

PocketOS database deletion, April 2026, as reported by Fast Company and Tom's Hardware.



GET STARTED

Make AI part of your stack.

AI is a new category of risk, and it's on every computer you manage. Traceforce was built to see it and control it, and it's easy to start.

- 1 **Sign up at port1.io/traceforce.** The partner agreement is free, with no purchase commitment.
- 2 **We'll set up your console** and walk you through deploying your first client.
- 3 **Run your first AI Risk Assessment, or add Traceforce to your stack.** The first 30 days are free for every client.

Everything starts here

port1.io/traceforce

This guide describes Traceforce for MSPs and the PORT1 program as of September 2026. Features, pricing and program details can change without notice, and everything here is subject to the PORT1 Partner Agreement. For the latest, visit port1.io/traceforce.

