SPARCLE · BOLT

Your team already uses AI all day. It is costing you more than you think.

Bolt is a fast everyday workspace that runs inside your boundary. Most of what your team does in it needs no AI model at all, which is why it is quicker and cheaper than the habit it replaces. When a task genuinely needs a model, Bolt is also the governed path to one: people sign in with SSO rather than holding API keys, sensitive values are replaced before the request leaves, and every decision is sealed into a record your auditor can check without us.

What it costs you today

1

Work leaves your control

Every quick paste into a cloud chatbot takes company data with it. Nobody logs it, and you cannot prove later what went where.

2

Blocking does not work

People route around a ban with a phone, a personal account, or a tool nobody has heard of yet. A block buys blindness, not control.

3

You pay a model to do arithmetic

Much of everyday AI use is formatting, converting, diffing and decoding. None of it needs a model, and all of it is billed as if it did.

What Bolt actually is

A fast everyday workspace

One keystroke, anywhere. Around 80 everyday tasks run instantly on your own machine with no model at all: decode a token, clean a CSV, diff two configs, work out a runway number, convert a timezone, redact a document.

Search across your work

Your files, mail, calendar, meetings, chats and connected systems, searched together, filtered by what you are actually allowed to see.

A memory of your own workday

What you were doing, in what order, on what. Private to you, on your machine, so picking a thread back up does not start with a hunt.

Governed AI when it is genuinely needed

The model your role permits, with sensitive values replaced before the request leaves and restored when it returns.

The part people miss

Bolt is not an AI product with governance bolted on. It is the place the work happens, and governance is a property of that place. That is why it does not get routed around: the thing being governed is the thing people want to use.

HOW IT DIFFERS

The habit, the tooling, and the alternative.

	Paste into a cloud chatbot	Buy an AI gateway or DLP proxy	Bolt
Where the work runs	Someone else's cloud	Someone else's cloud	**Your machine, or your own servers**
Cost of everyday tasks	Tokens, every time	Tokens, every time	**Nothing. Most tasks use no model at all**
Who holds provider keys	Individual employees	Central, if you buy a router	**Nobody. People sign in with SSO**
Personal data reaching the model	All of it	Usually unfiltered	**Replaced before egress, restored on return**
Files, images, archives	Unseen	Not addressed	**Extracted and inspected, archives included**
What employees actually do	Route around the policy	Reconfigure their tools	**Use something they prefer, governed by default**
What the auditor gets	Nothing	Usage and spend reports	**A sealed record they verify offline, with us unreachable**

What it changes, by role

Who	Today	With Bolt
Security	No inventory of AI use, no record of what left	One place every request passes, masked before egress and sealed after
IT and Identity	Keys issued by hand, no clean revocation	SSO and SCIM. Access and model permissions follow the person's role
Finance	One provider invoice with no attribution	Spend attributed per person, department and model, with budgets that step down instead of blocking
Everyone else	Told not to use the tools that make them faster	A faster way to work, with the safety applied for them

Why the difference is structural

A cloud proxy cannot move inspection into your network without abandoning the architecture its business is built on. A router cannot start masking without becoming a different product. A ban cannot become visibility, because the traffic it pushes away is the traffic you needed to see. Bolt starts from the other end: it is the surface where the work happens, with the inspection inside it.

Keep what you have

Bolt does not replace your DLP or your firewall. Those inspect a path they do not own, which is why AI traffic looks to them like ordinary encrypted traffic to a legitimate website. Bolt governs the content itself, where it is written. Different layer, not a rip and replace.

WHAT YOU GET

What is real today, and what is not.

We would rather you score us on this than discover it later.

Capability	State	Detail
Runs on your infrastructure, or on the employee's device	Shipping	Docker or Helm into your cloud, or a desktop app
Everyday tasks with no model involved	Shipping	Around 80 utilities, on-device
Search across files, mail, calendar, meetings and connected systems	Shipping	Filtered by the permissions you already have
SSO with SAML and OIDC, SCIM provisioning	Shipping	Your existing identity provider
An AI endpoint any standard client can point at	Shipping	Messages, model selection, streaming. Function calling, sampling parameters and embeddings are not built yet
Masking before egress, restoration on return, files and archives included	Shipping	Content is extracted first, so a container cannot hide it. Names and addresses via an optional model
Tamper-evident audit with an offline verifier	Shipping	A standalone binary re-checks the chain with nothing from us in the loop
Regional and industry rule packs	Shipping	22 regulation packs (GDPR, CCPA, DPDP, PIPL and more) plus 6 industry packs, enabled by an administrator
Managed device policy	Partial	macOS profiles and browser managed policy. Windows Group Policy is not built yet
Governing tools that cannot point at Bolt	Partial	Extension and local relay cover most. The network filter reports, it does not yet block
Central policy push with delivery confirmation	Not yet	Policy is fetched by the client, not pushed. No device registry, no delivery confirmation

How to test it honestly, in one sitting

1. Use it for a morning without touching a model: decode a token, clean a CSV, diff two configs, work out a runway number. Notice what you did not pay for.
2. Point a standard client at your own Bolt server, signing in with your identity provider. No API key is involved, and the model list is your role's, not everyone's.
3. Send a prompt with a real customer name and account number. The answer is correct, and the record shows those values were replaced before the request left. Then ask for a model your role does not permit, and read the refusal.
4. **Take the audit chain, disconnect from us entirely, and verify it on your own laptop.** Do this one first. Most vendors describe an audit trail; very few hand your auditor a program that checks it without them present.

Start here

A short pilot on one department, run in observe mode. At the end you get an inventory of which AI tools are actually in use and what classes of data were heading to them. That inventory is useful whether or not you buy anything.

Sparcle · bolt@sparcle.app · sparcle.app. Capability states reflect the shipping build at the time of writing, and are stated so you can verify them during a pilot.