

Every App. Every Endpoint. Under Control.

Software adoption on the endpoint has been accelerating for decades. AI has pushed that pace into overdrive, introducing more software, faster, often without security review. The result is a growing attack surface and thousands of hours of manual work to investigate software and remediate risk.

Glow reimagines endpoint security with specialized AI agents that continuously discover software, assess risk, and take action across the enterprise. This dramatically reduces the endpoint attack surface by addressing risk at the point of adoption, before it becomes exposure.



Continuous AI-enriched policies

Glow's AI agents discover, assess, and act on new software as it appears, no human queue, no approval backlog. You get the full cycle of autonomy, with the control to set the boundaries.



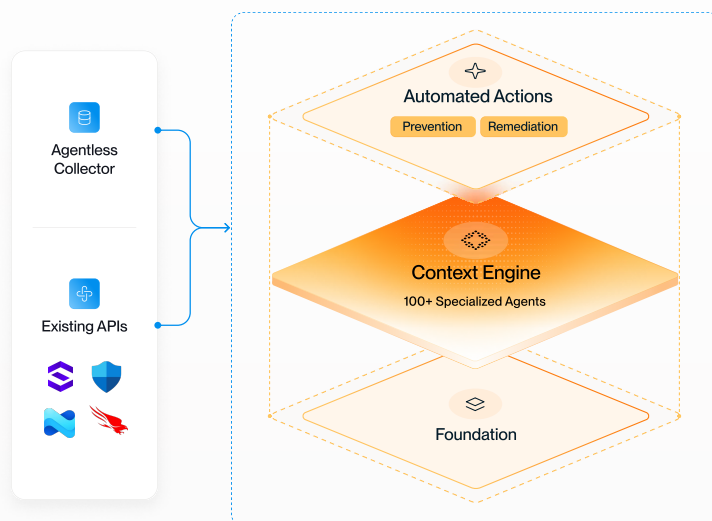
Coverage beyond traditional software

From installed applications and browser extensions to IDE plugins, packages, SaaS, and AI tools, Glow continuously surfaces what other tools miss, giving you control over what should and shouldn't run in your enterprise.



Deep organizational context and intelligence

Legacy app control is binary: something's on the list or it isn't, with the reasoning buried in an analyst's head. Glow's agents research and explain why something is risky, so every decision comes with context, not just a verdict.



Why This Matters Now

AI is accelerating how fast software accumulates on the endpoint, and most organizations have quietly normalized letting it in unchecked.

- Developers and citizen developers add non-binary software (extensions, packages, AI agents) without review
- Glow has found enterprise environments running 60,000+ pieces of software, far beyond what security analysts can keep up with
- Strict blocking isn't realistic either; it slows the business down and pushes usage further into the shadows

Manual review can't scale to this pace. Blanket blocking isn't a real option. Security teams need to leverage AI to get ahead of risk and prevent attacks.

 Act

Remove 13 unofficial and high-risk MCPs from your org

By Remediation Agent

From visibility to prevention

Visibility is only the beginning. Glow turns continuous understanding into autonomous action, helping security teams identify risk, remediate issues at scale, and enforce controls that prevent unwanted software and risk before they enter the environment.

01

Get your visibility baseline

Which tools are here? Who uses them? How & what for?



02

Remediate & set preventive policy

Remove anything unapproved, then enforce policy so it stays clean



03

Continuous runtime prevention & monitoring

Guardrails so the same issue can't recur



Get started in less than an hour.

Glow connects to your existing identity, endpoint management, and security platforms to provide immediate visibility into every piece of software running across your environment.

Once connected to Glow, you'll have:

- A complete inventory of software running across your endpoints, including extensions, packages, and AI tools other solutions miss
- Visibility into unvetted, unauthorized, or risky software already in your environment
- Autonomous policy recommendations to close gaps without adding manual review work
- A path to continuous control that scales with how fast software actually changes

Schedule your *test drive*.

“ Glow is where endpoint security is headed: less manual administration, more natural-language policy, and autonomous enforcement that actually does the work.

Eli Edelkind, CISO, Infrastructure & Tech Operations, CAVA