glow

Antares wanted to get control of Software Sprawl. *Then AI changed everything.*

The Challenge: Building a Trusted View of the Endpoint

For Antares, the original challenge wasn't AI.

The security team was focused on a problem nearly every enterprise faces: understanding what was actually running across its endpoint environment. Traditional CMDBs, endpoint managers, vulnerability scanners, and software inventories each provided part of the picture, but none delivered a trusted view of what software actually existed across the organization.

As Kyle Weckman, CISO of Antares, explained, "You can't secure what you don't know is there."

Existing tools often produced different answers, forcing security teams to manually reconcile inventories before they could even begin reducing risk. Employees were installing applications outside approved processes. Browser extensions were proliferating. Security teams were spending valuable time investigating, validating, and remediating issues. As Weckman put it, "It's chaos right now to wrangle in."

As Antares evaluated solutions, their goal was simple: gain visibility into everything running across the endpoint, clean up the environment, and build toward a future where approved software could be managed proactively instead of chasing problems after the fact.

The team often referred to the objective as "getting clean" before enforcing stronger controls.

Then AI arrived.

A New Risk Category Emerges

As AI adoption accelerated across the organization, the challenge changed dramatically. At the same time, the endpoint itself had become the new security perimeter. As employees worked, they were installing software, browser extensions, AI tools, developer packages, and other technologies directly onto their devices. AI simply accelerated a trend that was already reshaping endpoint security.

What began as software and endpoint governance quickly expanded into questions the team couldn't easily answer.

- Which AI applications were being used?
- Who was running AI coding assistants?
- Which browser extensions contained AI capabilities?
- What plugins and MCP servers were connected to AI tools?
- Were employees using personal AI accounts?
- Were credentials or sensitive configurations exposed?

The speed of AI adoption exposed a gap that traditional endpoint management tools weren't designed to solve. As Brendan Crowley, Deputy CISO at Antares, described it, "We had been struggling with AI inventory in general."

The team realized that AI wasn't a separate problem from application governance. It was the next evolution of endpoint governance.

Antares Capital

CUSTOMER
Antares Capital

HEADQUARTERS
Chicago, IL

INDUSTRY
Financial Services

From *Visibility* to *Control*

Understand the Endpoint

- Unified visibility across endpoint, MDM, and security tools
- Trusted inventory of software and browser extensions

Expand to AI

- AI applications
- Developer tools
- Browser extensions
- MCP servers

Turn Insight into Action

- Risk prioritization
- Software remediation
- Application governance
- Blocking and prevention

Build for the Future

- Foundation for application whitelisting
- AI-ready endpoint governance
- Greater confidence to enable innovation

Glow Was Already in the Right Place

Because Glow integrated with the endpoint, MDM, vulnerability management, and asset systems Antares already relied on, it didn't replace existing investments. It unified them.

By reconciling data across those platforms and adding its own endpoint intelligence, Glow gave the team a trusted, continuously validated view of what was actually running across the environment. It became a single place to understand applications, browser extensions, endpoint activity, and ultimately AI usage.

What made Glow valuable wasn't simply that it found AI tools.

It connected AI risk back to the operational workflows the security team was already building:

1. Discovery
2. Classification
3. Approval
4. Remediation
5. Blocking
6. Prevention

When Glow's AI discovery capabilities surfaced AI applications, MCP servers, plugins, personal AI accounts, and risky configurations, Antares didn't need to create a new program from scratch. They could extend the governance model they were already building.

Within early testing, the team uncovered AI risks that had previously been invisible. Bill Lee, VP of Cyber Security Architects, shared, "The number of things Glow was able to detect was very enlightening."

From Cleanup Project to AI Security Program

Today, Antares sees Glow as the foundation for both software governance and AI governance.

What began as an effort to understand what was running across the endpoint environment has become the foundation for a broader strategy built on visibility, governance, and automated control. As AI becomes embedded in applications, browser extensions, developer tools, and autonomous agents, Antares is extending the same governance model across an increasingly dynamic endpoint.

Looking ahead, Weckman believes the opportunity goes well beyond inventory.

"Before Glow, I never thought we would get to a point where we could confidently whitelist applications and block everything else."

With AI accelerating software change across every endpoint, Antares is building toward a future where software can be continuously discovered, governed, and managed automatically, giving the security team the confidence to enable innovation while maintaining control.

> "
>
> You can't secure what you don't know is there.
>
> **Kyle Weckman**
> CISO of Antares

> "
>
> The number of things Glow was able to detect was very enlightening.
>
> **Bill Lee**
> VP of Cyber Security Architects

> "
>
> Before Glow, I never thought we would get to a point where we could confidently whitelist applications and block everything else.
>
> **Kyle Weckman**
> CISO of Antares