DNSFilter



THE VISIBILITY DEFICIT SURVEY SERIES

The Cost of Shadow AI

Your budget increased, but your visibility didn't.

The Money Moved

74.5%
increased their cybersecurity budget in the past 12 months

43.0%
find out about AI tool access after it is granted, or never

40.3%
are sending their next dollar to AI security and governance

Security budgets are growing, and AI is where the new money is going. Among 400 IT and cybersecurity professionals surveyed across the US and Canada, **74.5% report a larger cybersecurity budget than they had 12 months ago,** and 18.8% grew theirs by more than 10%. **Asked where the next incremental security dollar goes, AI security and governance takes the top spot at 40.3%**, nearly a full 15 points ahead of cloud security at 25.5%.

They have reason to prioritize it. When a new AI tool requests OAuth or API access to corporate systems, 36.8% of organizations who have employees using AI tools for work let employees grant it and **notify IT after the fact**. Another 6.5% grant it **with no IT notification at all**. **That is 43% of organizations where the decision to connect an AI tool to corporate data is made by someone who does not own the risk.**

The proliferation of AI has caused organizations to move faster than they might be ready for, and while the budgets have increased the policies and governance haven't necessarily kept pace.



What the Budget Is Actually Buying

61.5%
cannot say all of their security tools are properly configured

61.8%
cannot say all of their security tools are actively monitored

46.1%
have unapproved AI tools connected to corporate systems

Before you add a tool, it is worth asking what the tools you already own are doing. **61.5% of respondents cannot say every security tool in their environment is properly configured, and 61.8% cannot say every one is actively monitored.** More than one in five say half or fewer are configured correctly. Organizations are buying new capability on top of an estate that is not fully working.

The controls meant to catch shadow AI are already in place, and already paid for. 54% say they use AI governance or monitoring controls to identify incidents involving third-party AI tools. **Yet 46.1% have had an employee connect an unapproved AI tool to their Google Workspace, Microsoft 365, or SSO environment anyway**, and 20.1% say one of those connections caused a security incident.

Governance spending is *not* the same as governance. The budget bought you a policy, but the tools are still getting connected to your environment—and you can't see them.



The Gap, Measured

15.2%
of orgs on the DNSFilter network see 10+ AI services in one afternoon

0.5%
of IT professionals say their employees use more than 10 AI tools

0.75%
of Generative AI traffic on DNSFilter is blocked

Self-reporting is where the visibility gap becomes measurable. Asked how many AI tools employees use for work, 55.3% of respondents said three to five, **and just 0.5% said more than 10.**

DNSFilter resolves DNS for tens of thousands of organizations. In August 2026, over 43,000 of them in North America generated Generative AI traffic, 3.4 billion requests in a single month. Looking at a standard business-day window, and counting distinct AI vendors rather than distinct domains, the median organization sees five. 42.8% see more than five. **15.2% see more than 10, which is 30 times the rate IT professionals reported in our survey.**

Control is the other half of the problem. Across that same traffic, 0.75% of all Generative AI requests were blocked. Allowing AI is a legitimate policy choice. Making no choice at all is not, and at under 1%, most organizations are not exercising the control their governance spending was supposed to buy.

The concern gap closes the loop. 54% of respondents are concerned their organization is incurring material AI costs that are invisible to procurement, software asset management, and security monitoring. While 58.8% of IT management are concerned. The people who approve the budget are the least worried about the part of it they cannot see. But those practitioners know something was purchased, they just have no visibility into it.



DNSFilter

You cannot budget for what you cannot see

Before the next dollar goes to AI governance, three questions are worth answering:

- Which AI services are resolving on your network today?
- Who authorized them?
- And what happens the next time one requests access to your corporate systems?

DNS-layer visibility answers all three while also protecting you from more traditional security incidents as well as providing you documentation for compliance.

See every AI service on your network.

START A FREE TRIAL OF DNSFILTER

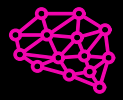


Methodology



Survey data

Between June 15 - 26, 2026, DNSFilter partnered with CensusWide to conduct a survey of 400 IT and cybersecurity professionals across the US and Canada. The roles surveyed were manager-level and above, at companies with 150–5,000 employees, across all industries.



Network data

DNSFilter resolver telemetry, Generative AI Tools category, North American resolution. Organization counts, request volume, and block rate cover August 1 through August 31, 2026. Counts of distinct AI vendors per organization were measured across two business days in August 2026, with vendors that operate under multiple domains counted once.

Get in touch

dnsfilter.com/contact
(877) 331-3412
sales@dnsfilter.com