

Customer Story

Saying “yes” to AI without losing control

Raised the security bar while lowering friction

Full visibility into AI and tool use in the browser

Surgical, identity-based controls with no disruption

Near invisible rollout on a browser people know

⚡ Impact Summary

Richard Davey is cautious about AI, and his job is to help Amazon use more of it. With the Island Enterprise Browser, Amazon's security team enforces identity, sees every tool in use, and adds controls surgically. Higher security and lower friction, at last.

amazon

Industry

Technology

Team

Security

Goal

Let employees use AI and new tools safely

Use Cases

Enterprise AI

Say Yes at Work

SaaS and Web Apps

Zero Trust



Challenges

- ✓ New AI tools outrun security review
- ✓ Friction pushes users off-path
- ✓ Unapproved tool use goes unseen

The Challenge

Employees don't wait for permission to try a new AI tool. They open it, paste in whatever helps them move faster, and connect it to their work. To Richard Davey, Principal Security Engineer at Amazon, every one of those tools is a stranger's computer now holding Amazon's data, and the list of them grows every week.

He could try to shut it all down, but that wouldn't be the right answer. Richard has spent a career learning not to trust technology on faith, and he's just as wary of AI. Ask him if he trusts it and the answer comes fast: not at all. But saying no isn't the job. He isn't there to make risk disappear, he says. He's there to decide which risks are worth taking, and to keep the business moving while he does.

He also knows what happens when security gets too heavy. Richard describes a gate across a country road, open fields on either side, and the tire tracks worn into the grass where every driver simply went around it. People do the same with controls. Make them a burden and the workforce finds an easier tool you can't see, and the visibility you were counting on is gone.

“The altruistic goal in security is to raise the bar while lowering friction. In my career, I've truly achieved that maybe twice, Island is one of them.”

Richard Davey, Principal Security Engineer, Amazon



The Solution

Richard's fundamentals are plain: know who is doing what, with what, and where. With the right observability, you can weigh the real risk and place controls where they actually matter.

Most of that activity runs through the browser. It's the common interface between the workforce and the tools they reach for, approved or not. Enforce identity there and you have a foothold. Watch the interactions and you learn the real patterns. Then you can act.

The Island Enterprise Browser gives Richard all of that in one place. People keep the browser they already know, so the rollout stays close to invisible. Behind it, the security team gets identity enforcement, visibility into every tool in use, and controls it can apply surgically instead of to everyone at once. This allows them to test and learn, then tighten only where the risk warrants it.

With Island, the team can:

- Enforce identity at the point where work happens
- See which tools the workforce uses, approved or not
- Apply controls surgically, without disrupting everyone at once
- Bring credentials under control to cut account-takeover risk
- Add AI and agentic automation to services that lack it natively

The product solves more than the problem that first brought Richard to it, the way a good multi-tool does. And the engineering and sales teams stay close, turning feature requests around quickly rather than pointing at a roadmap.

“Do I trust AI? Not at all. Functionally, I’m putting my data on someone else’s computer and getting an output. We have to be purposeful about what we let it do on our behalf.”

Richard Davey, Principal Security Engineer, Amazon

Results

Most controls come with a tax. Add multi-factor authentication and you add steps. Richard has spent most of his career hunting for the rare case where security goes up and friction goes down at the same time. He says it has happened maybe twice. Island is one of them.

Richard treats AI as the current test of that balance. He uses it as a force multiplier for high-volume, low-risk work, the kind of analysis that used to swallow analysts whole. He's clear about its limits. AI will happily decide that something it sees constantly must be safe. Often it isn't. The team's job is to surface those calls to human judgment and keep a guardrail ready to drop in front of any agentic action before it does damage. The browser is where they see it happen.

None of this slows the business down. People keep working in a familiar browser while the security team gains the visibility and control it lacked before. Richard gets to say yes to AI and new tools, on his terms, with the evidence to know where the real risk sits.

Find out more: [How Amazon's Social Media Team Uses Island AI Automation to Reclaim 80 Hours a Week](#) (link to previous amazon page)

“Knowing who is doing what, with what, and where is everything you need for observability. Island lets you do all of that in the browser.”

Richard Davey, Principal Security Engineer, Amazon



Ready to improve enterprise security and usability?

[Schedule a demo](#) ↗