Customer Story

Eftsure Slashes Costs and Complexity with Island

eftsure

Industry
Financial services

Solutions
SaaS, 3rd party contractors, BYOD workforce, Safe Browsing, AI, Say Yes at Work

Meet Eftsure

Eftsure is a global B2B payment fraud prevention firm based in Dallas, United States, serving SMB, enterprise and government clients across Australia, the US, France, Italy, and the UK. They maintain a whitelisted database of millions of verified supplier payment details, ensuring customers are paying into the correct vendors' details. Eftsure protects them from risks like BEC (business email compromise) and fraudulent suppliers while covering the whole end-to-end supplier or third-party vendor management process. It's a highly data-sensitive operation.

As Lead Cybersecurity Engineer at Eftsure, Jarred Gibor sits at the intersection of the company's customer contractual obligations, regulatory compliance, and business needs, all while managing security for a business built on sensitive payment data. The cybersecurity and infosec team protects the entire corporate security architecture of a company whose customers include government agencies and major enterprises across three continents.

The Challenge

Performance issues, limited visibility, and cost

When Gibor arrived at Eftsure as the org's new security chief, he quickly identified three problems with their Virtual Desktop infrastructure: performance issues, limited visibility, and cost.

"The latency with the legacy virtual machines was unbelievable," he says. "Our fraud prevention teams need to be in the forefront of catching fraud, but they were hindered by the VDI browser's slowness" — a constant lag that left the team feeling frustrated and fatigued. "We definitely had a need for speed," Gibor says.

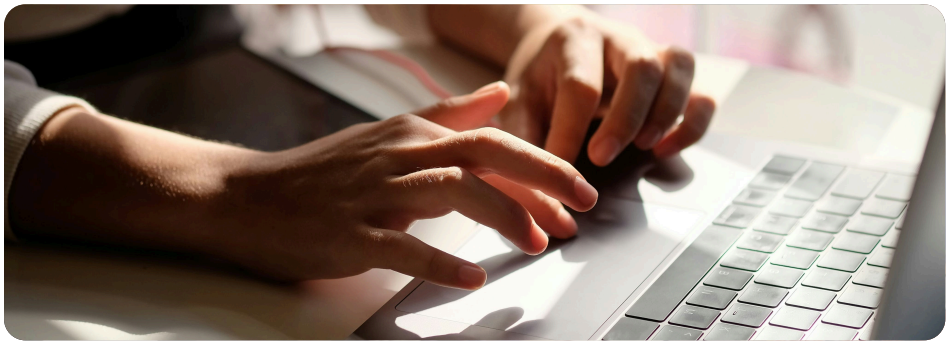
Visibility was another issue. Teams had access to sensitive customer data to verify supplier payment details and catch fraudulent transactions, and VDI provided only limited observability and oversight around data access. But another problem was even higher on the infrastructure team's priorities list: onboarding.

Onboarding new users to VDI was a constant, highly hands-on time sink for multiple teams. "The infrastructure team had to be involved because they had to provision the workspaces to the users, then set them up with the VPN to access the workspaces," Gibor says. "Then the department heads got pulled in to help troubleshoot the next phase, helping people to actually log on and figure out how things worked."

The headaches continued even after a user was finally onboarded because the VDI setup blocked auxiliary devices, including cameras and microphones. "Whenever they needed to jump on a call they had to use the local version of Microsoft Teams, which left us with zero visibility whatsoever."

Beyond the latency, visibility, and onboarding issues, the VDI infrastructure itself also carried a hefty price tag, Gibor says, requiring significant compute resources and constant maintenance from multiple teams.

> ***"It's very rare that a security team specifically onboards a tool that's security and operationally focused, and also improves the end-user experience significantly."***
>
> **Jarred Gibor,** Lead Cyber Security Engineer



The Solution

With Island I can set and forget

Gibor went looking for a way to fix these problems and found the Island Enterprise Browser.

The deployment itself took days, not weeks. "We literally packaged it up in our MDM, our mobile device management software, and distributed it to the devices and through user provisioning. Done," Gibor recalled. "And right away I began getting messages from the teams saying, 'What a game changer, we love it!'"

Island immediately gave Gibor the observability and visibility he'd been missing. "We can respond much quicker now, when incidents arise," he says, describing, for example, a possible account compromise where an Eftsure staff member clicked on a targeted and sophisticated malicious link. "Between our robust and comprehensive security solution architecture, the account compromise was blocked and remediated, and through Island I was able to actually backtrack what happened with egress and ingress traffic because of the logs that the Island browser gave," Gibor recalls. "But even more invaluable was the visibility, the ability to quickly grasp what is happening and act as quickly as possible."

Gibor also values Island's data loss prevention features: "As a data-driven company, we need the next level of data loss prevention mechanisms in place, but without limiting our users' ability to do their work. Island makes such a difference in even basic things, like preventing copy-paste outside of the browser, or downloading data. Sure, you can download as much as you want, but only into the dedicated cloud environment that we allow you to. That's massive because now we can tell our customers, hand on heart, 'Yes, we have full control over the flow and residency of data, both in transit and at rest.' and then there's no questions asked thereafter."

As for financial impact, Gibor says that moving to Island created $200,000-plus in annual savings for Eftsure. "We eliminated the cost of compute, but also the cost of resources being spent in maintenance and provisioning and associated infrastructure."

> ***"I was not expecting Island to be this low maintenance. I budgeted the time I thought I would need to maintain a tool like this, and I just don't have to!"***
>
> **Jarred Gibor,** Lead Cyber Security Engineer

So easy, even an intern can manage it

“Reducing that operational overhead was a massive win because Island for me is a little bit of a set-and-forget,” Gibor marvels. “Unless I want to specifically go in and do some investigating, there's no need for me to do anything. I trust that it's working, which is unbelievable.”

“I was not expecting Island to be this low maintenance,” he continues. “I budgeted the time I thought would be needed to maintain a tool like this, but I just don't have to, which is amazing. It's so easy that I can just hand it over to my junior or an intern for them to manage and maybe make new policies.”

But perhaps more valuable was achieving compliance by default through Island's data sovereignty capabilities. Island's flexible data hosting options — whether on-premises or in data centers worldwide — gave Eftsure the geographic control needed to meet GDPR and regulatory requirements. "It's like compliance by default, which is amazing,” Gibor says. “Island saves us a huge amount of time in terms of articulating to customers why we are compliant. They just get it."

Saying yes to AI and creativity

Eftsure does not yet enforce a blanket policy around AI usage, but Gibor feels confident that Island keeps shadow AI under control. “Island lets me understand where our risks lie, which I had limited visibility into before,” he says. “For example, the Island browser allows me to see a line a user copied from one location and pasted into ChatGPT, and then copying ChatGPT’s answer and pasting that into a third location,” he says. “I can see that end-to-end data flow.”

“But I absolutely feel safer allowing people to be fairly creative with the way that they're using AI because with Island I have parameters in place and visibility into what’s happening.”

Conclusion

With Island, Eftsure

- Eliminated over $200,000 in annual compute and maintenance costs.
- Reduced operational overhead across infrastructure, IT, and security teams.
- Gained comprehensive visibility into user activity and data flows.
- Deployed enterprise-wide through MDM in days with immediate user adoption.
- Achieved compliance-by-default for data sovereignty requirements.
- Said yes to AI use with the parameters and visibility that Island provides.

> ***"Because of the data that we're dealing with we are a compliance-driven company. Island's compliance aspect, with data sovereignty, GDPR-A regulatory checkboxes – it's like compliance by default, which is amazing."***
>
> **Jarred Gibor,** Lead Cyber Security Engineer

Results

$200,000+

Annual savings by replacing VDI with Island Browser.

Zero Latency

Elimination of 2-second delays that hindered fraud detection response times.

Set-And-Forget Operation

Low-maintenance deployment requiring minimal ongoing operational overhead.

Compliance By Default

Built-in data sovereignty satisfies data regulations like GDPR.