

Customer Story

Veeam *Secures employee end-user devices* with Island

Estimated savings of \$2 million over 3 years

Unified end-user experience

Security and visibility

Protected end-user privacy

⚡ Impact Summary

Veeam Software, the Data and AI Trust company, found securing employee end-user devices costly and complicated. Now with Island, Veeam keeps those devices secure, saves millions of dollars, and has improved visibility without violating end-user privacy.

VEEAM

Data and AI Trust company

Industry

Technology

Use Cases

VDI/DAAS

BYOD workforce

M&A

SASE/SSE

AI



Challenges

- ✓ Too many types of BYOD end-user devices to support
- ✓ No way to monitor end-user services
- ✓ Costly, hard-to-manage VPN
- ✓ Complicated security for newly acquired companies

The Challenge

Veeam operates on a powerful idea: Unlocking the value of data and AI requires trust.

Headquartered in Seattle with offices in more than 30 countries, Veeam protects over 550,000 customers worldwide, including 80% of the Fortune 500.

With 65 offices around the world, supporting and safely securing employee laptops and other devices was a major challenge. Originally, Veeam employees could use their personal devices at work. But after this created serious security and monitoring challenges, Veeam added a VPN to solve the challenges. Unfortunately, that approach raised costs and increased network load. Instead, Veeam supplied them with company-issued devices and created new policy that prohibited employees from using their personal devices.

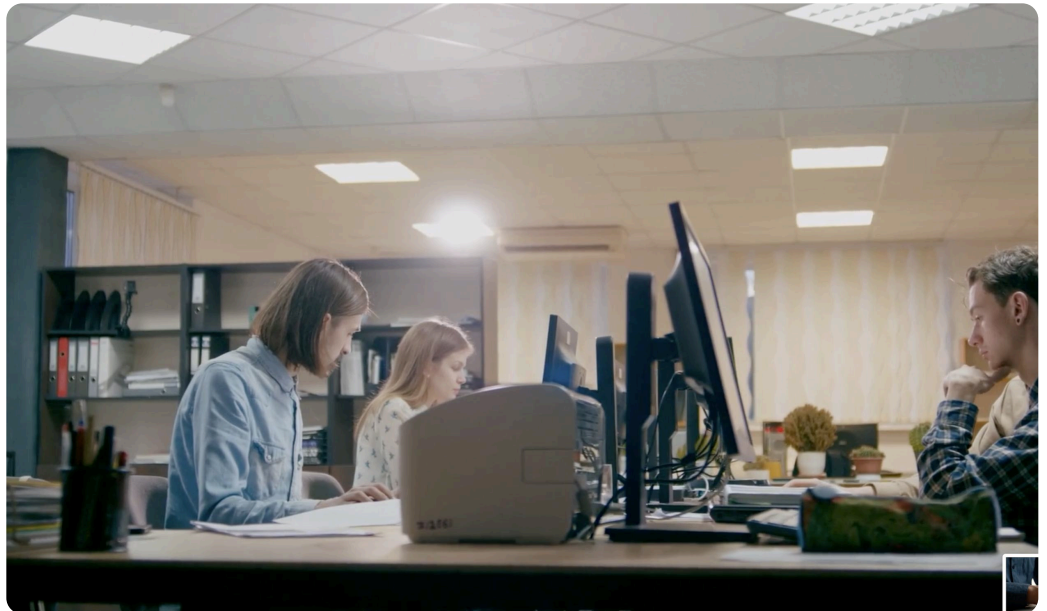
This change created new challenges. For example, when Veeam acquired another company it needed to quickly equip the acquired company's employees with managed end-user devices. In one case, Veeam would have needed to quickly ship as many as 600 devices.

Veeam also struggled with the high cost of running numerous security point solutions. In one instance, the company was surprised to learn that an enterprise password management tool it wanted carried an annual license fee as high as \$120,000.

Yet another issue: Veeam had poor visibility into the online behavior of remote employees connected via the VPN. "Once a user was logged in, they could use whatever," recounts Matt Micheletti, VP of IT Infrastructure and End-User Services at Veeam. "There was no way to monitor what service was running on which server, or why people were logging into it."

"With Island, I don't have to invade our users' privacy to enable security in places we care about. That's a really big win."

Matt Micheletti, VP of IT Infrastructure & End-User Services at Veeam



The Solution

Everything changed when Veeam discovered Island. Island didn't just solve Veeam's problem, it sidestepped the issue entirely by not relying on routing traffic through a single geographic location, data center or office. Instead, it's all on the device. The Enterprise Browser provides secure access and controls from within the browser. Managers can apply controls universally, enabling an end user to safely access data and resources anywhere, on any device.

"Switching to Island actually completely changed my philosophy around endpoint security," Micheletti says.

The rollout was quick, according to Ethan Besbris, Endpoint Management Leader at Veeam. A pilot rollout of the Island Enterprise Browser involved 6,000 users and took just one month. After that, giving Island to all remaining employees went from initial inception to full rollout in a mere five months. "It was a smooth transition for sure," Besbris says.

"Island has been a responsive and collaborative partner in a way I've never seen before."

Kyle Anderson, Solution Architect at Veeam



Results

Now, with Island, Veeam doesn't have to secure each remote device. Instead, it uses Island to delineate what's inside and outside the browser. Any user can now use any device from any location to use any application.

With Island, Veeam can also tune a user's experience and access based on their role, job profile, physical location, and device. Yet on a managed device, "Island is functionally indistinguishable from using my personal computer," says Kyle Anderson, Solution Architect at Veeam. That feature eases user adoption and simplifies management.

Adds Besbris: "Being able to get the visibility only where we need it, and without punishing users for normal day-to-day use, has been a groundbreaking experience."

Veeam also gets more value from Island than it would with competing products. When Micheletti and his team originally evaluated their options, they estimated Island would save Veeam nearly \$750,000 over three years. But that failed to account for the cost of a password manager and VDI licensing. Once the team added those in, the three-year savings estimate was closer to \$2 million. "That," Micheletti says, "was an easy sell for my boss."

Also, Veeam no longer needs to ship end-user devices to remote locations. Micheletti says, "Island was an easy solution."

Also, with Island, Micheletti and his team can monitor work-related behavior but is blocked from seeing personal use. "I can enable security in places we care about without having to invade our users' privacy," he says. "That's a really big win."

Adds Anderson: "There's a level of respect for the user that is built into the core of the Island browser. That's an enormous differentiator."

For Veeam, a company based on data and AI trust, that's a big deal.

"The Island user experience, regardless of device posture, has been overwhelmingly positive."

Ethan Besbris, Endpoint Management Leader at Veeam



Ready to simplify access and eliminate VDI complexity?

[Schedule a demo ↗](#)