Island
For MSPs

AI Data Protection

Stop Data from Leaking into the AI Black Hole

Shadow AI is real. End users are copying sensitive data into ChatGPT, Gemini, and dozens of other tools–without security controls, oversight, or even awareness. As an MSP, you're now responsible for securing how your clients interact with AI.

The New Risks:

- Shadow AI tools used without approval or policy
- Proprietary or regulated data pasted into public LLMs
- No visibility into what was entered or who accessed what
- Growing AI agent integrations inside SaaS apps
- Employees unknowingly leaking IP or client data to third parties

How Island for MSPs Helps You Take Control:

- **Granular AI Controls:** Block, allow, or restrict AI tools based on role, device, and data context
- **Clipboard & Input Protections:** Prevent copy/paste of sensitive data into AI chat windows
- **Watermarking & Session Audit Trails:** Capture and trace every user session, even on BYOD
- **URL & Domain Controls:** Allow only approved AI tools; block the rest
- **Dynamic DLP:** Enforce policies at the point of use, not just at the endpoint
- **Real-Time Visibility:** Know what users are doing inside AI apps without invasive endpoint software
- **Safer SaaS Integrations:** Contain risks from emerging AI features embedded in workplace apps

Give Your Clients the Confidence to Embrace AI — Without the Risk.

With Island for MSPs, you help your clients adopt generative AI safely, avoid costly data leaks, and meet growing compliance demands. No endpoint agents. No risky browser extensions. Just smart, zero-trust controls at the point of interaction.

SCAN QR CODE TO
BEGIN YOUR ISLAND JOURNEY WITH PORT1

islandmsp.com