PAX8 PRODUCT ONBOARDING

Island the Workspace for SMB

Complete product profile for Pax8 Marketplace listing

Product description

Island the Workspace for SMB is a single, secure browser-based platform that replaces a fragmented stack of IT security tools with one unified workspace. Built on the familiar Chromium browser, Island gives employees the fast, intuitive experience they already know — while giving IT teams the visibility, control, and data protection they need.

Island consolidates Virtual Desktop Infrastructure (VDI), Virtual Private Networks (VPN), Data Loss Prevention (DLP), web filtering, and password management into a single platform. Employees can securely access company applications and data from any device — managed or unmanaged — without the need for complex endpoint agents or costly VDI deployments.

Built-in capabilities include malware and phishing protection, Zero Trust Network Access via Island Private Access, last-mile data controls that prevent copying, downloading, and screenshotting of sensitive information, frictionless BYOD and contractor onboarding, and a Secure AI Assistant powered by Microsoft Azure OpenAI (or the model of preferance). All capabilities are managed from a single, centralized console, dramatically reducing IT overhead and cost.

Key details

Trials	
Trials available	**Yes (available through end of the month)**
Trial initiation	Initiated in the Pax8 Marketplace. Partners request the trial on behalf of their end customer directly from the Island management console.
Trial scope	Full-featured trial covering all core capabilities including Island Private Access, data protection controls, safe browsing, and the management console.

Support	
Tier 1 support	MSP provides Tier 1 support for all end-customer inquiries.
Tier 2 / Tier 3 support	Island provides Tier 2 and Tier 3 escalation support directly to from tickets entered from the Management Console.

© 2025 Island Technology, Inc. All rights reserved. · Confidential — For Pax8 Partner Use Only

Support channels	The Island management console is the source for all ticket entries from MSP only.
Documentation	Full product documentation, on-boarding guides, and knowledge base available at documentation.island.io and through the Pax8 partner portal.

Data center locations	
Primary regions	United States (US East, US West)
Secondary regions	European Union (EU West — Ireland), United Kingdom (UK South —London), Australia, Canada
Data residency	Customer data is stored in the region selected at the time of tenant provisioning. Data does not leave the selected region without customer consent.
Cloud infrastructure	Hosted on Amazon Web Services (AWS) and Microsoft Azure.

Compliance & certifications	
SOC 2 Type II	Certified. Report available under NDA upon request.
ISO 27001	Certified.
GDPR	Compliant. Data processing agreements (DPA) available.
CCPA	Compliant.
HIPAA	BAA available for healthcare customers upon request.
FedRAMP	In progress.

Integrations	
Identity providers (IdP)	Okta, Microsoft Entra ID (Azure AD), Google Workspace, Ping Identity, OneLogin, JumpCloud — SAML 2.0 and OIDC supported.
MDM / endpoint management	Microsoft Intune, Jamf, VMware Workspace ONE, CrowdStrike Falcon.
SIEM / logging	Splunk, Microsoft Sentinel, Sumo Logic, Elastic — via syslog and API.
Ticketing & ITSM	ServiceNow, Jira Service Management.

© 2025 Island Technology, Inc. All rights reserved. · Confidential — For Pax8 Partner Use Only

Secure AI	BYO Chat / AI Browser, Island Chat includes Microsoft Azure OpenAI Service (GPT-4). Customer data remains within the tenant and is not used to train external models.
Password manager	Built-in Island Password Manager. Also integrates with 1Password and CyberArk via browser extension policies available in browser or extension.
Cloud access	Microsoft 365, Google Workspace, Salesforce, AWS Console, Azure Portal and all major SaaS applications accessed via browser.

Platforms supported	
Windows	Windows 10 (version 1903+) and Windows 11. Managed and unmanaged devices.
macOS	macOS 12 Monterey and later. Managed and unmanaged devices.
iOS / iPadOS	iOS 15 and later. Supported via Island Mobile for managed devices.
Android	Android 10 and later. Supported via Island Mobile for managed devices.
Linux	Ubuntu 20.04 LTS and later. Enterprise deployments.
ChromeOS	Supported via managed ChromeOS devices with Island deployed as the default browser policy.
BYOD / unmanaged	Full support on personal, unmanaged devices across all major OS platforms. No endpoint agent required.

© 2025 Island Technology, Inc. All rights reserved. · Confidential — For Pax8 Partner Use Only

Features

Safe browsing & threat protection

Built-in malware inspection, anti-phishing engine, and URL filtering protect users from web-based threats in real time — no additional security tool required.

Data protection & last-mile controls

Granular policy controls prevent copying, pasting, downloading, printing, and screenshotting of sensitive data within any web application, regardless of device ownership.

Zero Trust Network Access (Island Private Access)

Encrypted, identity-aware tunnels deliver seamless access to private and internal applications — a complete replacement for legacy VPN, with no client agent required.

Frictionless BYOD & contractor access

Employees, contractors, and vendors self-install Island on any device in minutes. A secure, isolated workspace keeps personal and corporate data separate without MDM or endpoint agents.

Built-in password manager

Auto-generate, save, and retrieve credentials with one click. Zero-knowledge encryption keeps passwords secure and eliminates reliance on third-party password tools.

Secure AI Assistant

Microsoft Azure OpenAI-powered assistant built directly into the workspace. Employees get AI productivity tools while IT maintains full data governance — no data leaves the tenant.

© 2025 Island Technology, Inc. All rights reserved. · Confidential — For Pax8 Partner Use Only

Centralized management console

Deploy policies, manage users, configure access rules, and review activity logs from one unified console. Supports role-based access control (RBAC) for IT administrators.

Application access controls

Set conditional access policies based on identity, device posture, network, location, and application — enforced directly in the browser without additional proxies or agents.

Web filtering & content control

Block or restrict access to categories of websites by user group or policy. Real-time categorization covers millions of domains with customizable allow/block lists.

Benefits

Eliminate technology sprawl

One platform replaces VDI, VPN, DLP, web filtering, and password managers — reducing vendor count, contract complexity, and IT management overhead in a single move.

Dramatically reduce IT costs

Consolidating multiple point solutions into Island delivers significant cost savings on licensing, infrastructure, deployment, and ongoing maintenance.

Works on any device from day one

BYOD and unmanaged device support means employees and contractors are productive immediately — no device enrollment, no MDM, no complex onboarding.

Enterprise-grade security made simple

Island brings the security controls of a Fortune 500 IT team to any SMB without the need for a large security staff or complex infrastructure.

Employees love it

Built on the Chromium browser employees already know, Island requires zero behavior change. Extensions, bookmarks, and workflows carry over seamlessly.

Full visibility and auditability

Comprehensive activity logs, session monitoring, and DLP alerts give IT teams complete visibility into how data and applications are being used — without invading personal privacy.

Partner resources	Partner portal: partner.island.io · Demo: island.io/schedule-demo · Documentation: docs.island.io · Partner support: partners@island.io

© 2025 Island Technology, Inc. All rights reserved. · Confidential — For Pax8 Partner Use Only