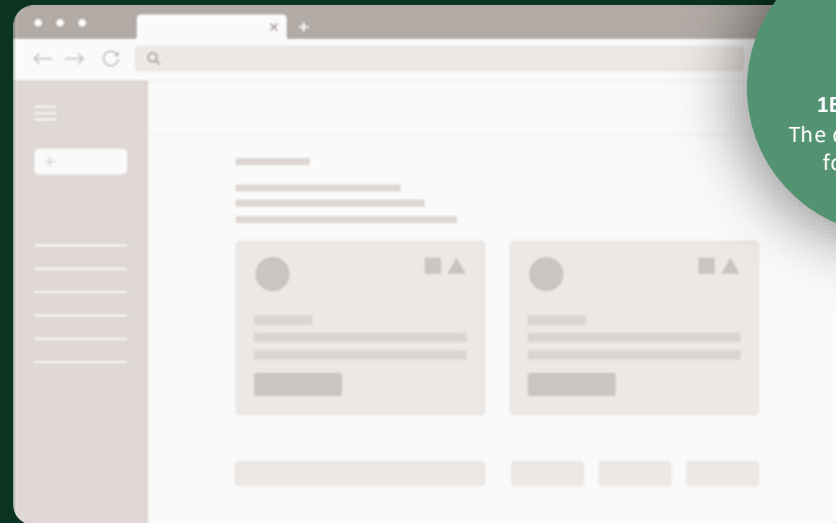




The Enterprise Browser

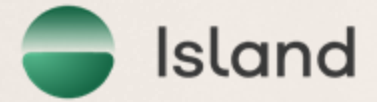
The application enterprises use most is **The Browser**



1B Global Users
The defacto standard
for consumers

Except the browser isn't an enterprise application

The Future of Enterprise Browsers



Recent research published by Gartner®

“Strategic Planning Assumptions

By 2025, enterprise browsers or extensions will be featured in 25% of web security competitive situations, up from less than 5% today.

By 2026, 25% of enterprises will be using managed browsers or extensions, up from less than 10% today.

By 2027, the enterprise browser will be a central component of most enterprise superapp strategies as productivity capabilities drive adoption.

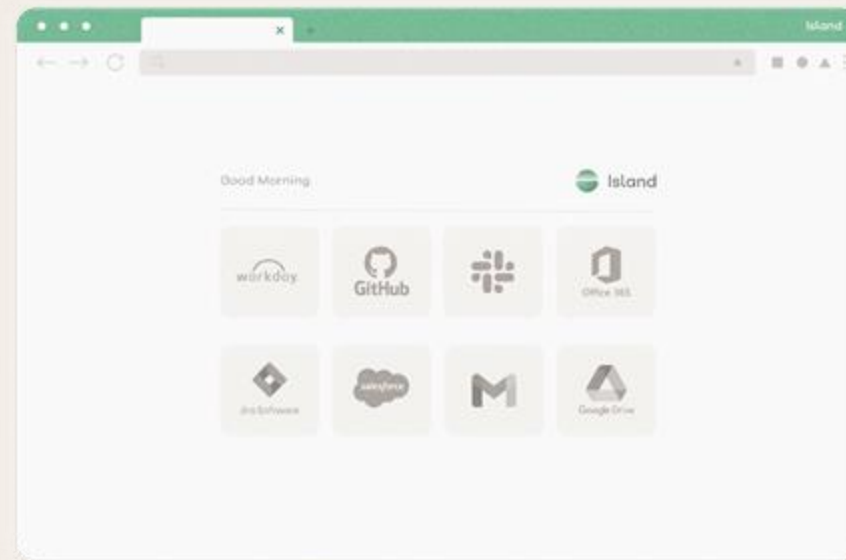
By 2030, enterprise browsers will be the core platform for delivering workforce productivity and security software on managed and unmanaged devices for a seamless hybrid work experience.”

Source: Gartner, *Emerging Tech: Security — The Future of Enterprise Browsers*, Dan Ayoub, Evgeny Mirolyubov, Max Taggett, Dave Messett, 14 April 2023

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

Introducing

The Enterprise Browser



The browser that puts the enterprise in complete control.
Delivering a level of security, visibility, and productivity
that simply wasn't possible before.

Shared Capabilities

- Last-Mile Controls
 - Cut / Copy & Paste
 - Screen Capture
 - Print/ Save
 - Download & Upload
- Browser-Based RPA
- Browser Enforcement
- Auditing, Logging & Forensics
- Device Posture (Assess & Enforcement)
- Internet Explorer Emulation
- Web Filtering
- Malware Inspection
- Secure Storage
- Security Tool Integration
- Management & Policy

Core Use-Cases



Critical SaaS & Internal Web Apps

Ensure the data interactions with SaaS and Internal Web Apps remain fundamentally secure



Contractor Security & BYOD Access

Fully govern how contractors and BYOD workers access and interact with your data



VDI Reduction

Replace an unpleasant work experience with the fluid and familiar one and users expect



Zero Trust

Deliver a simple, efficient, and completely native zero trust experience across the last mile of the user experience



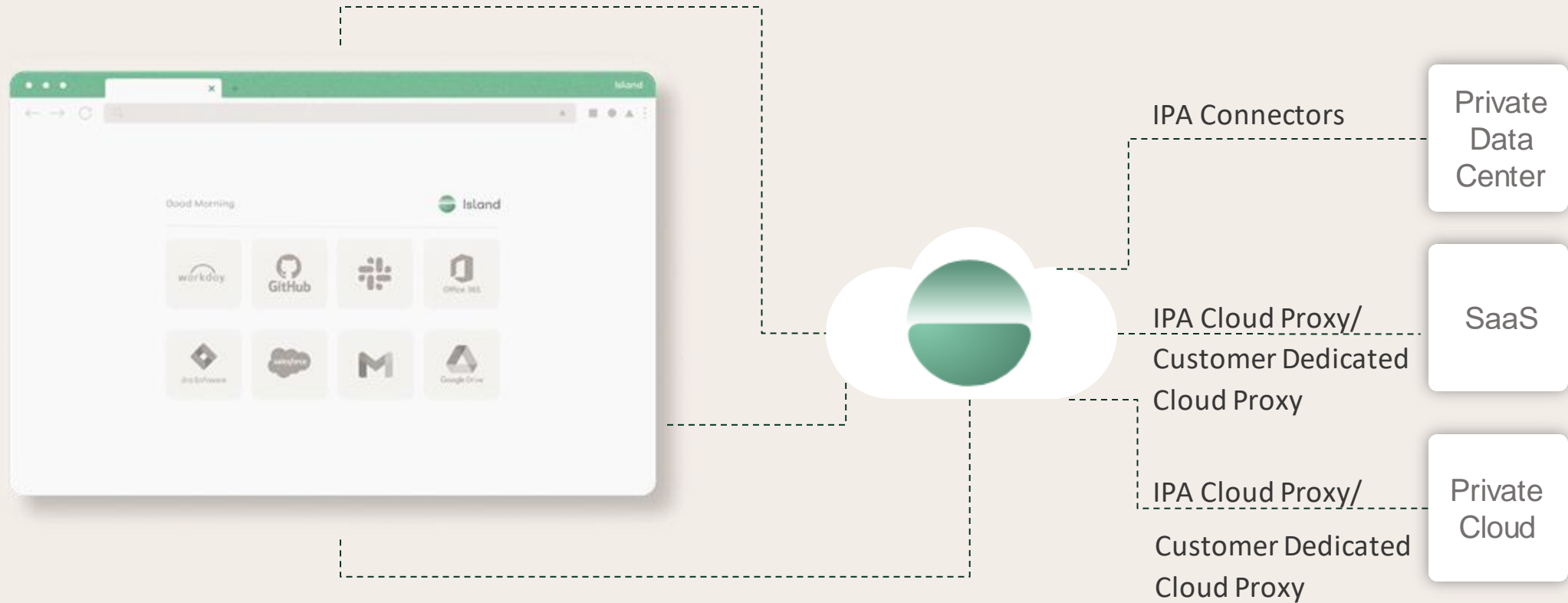
Say Yes

Say Yes to applications that challenge their security posture while ensuring no sensitive data can leak onto them

Additional Use Cases

- Govern **privileged users & critical transactions**
- Provide **native browser isolation**
- Safely **integrate M&As & joint ventures**
- Monitor & govern **call centers**
- Protect against **ransomware attacks**
- Provision **disaster recovery browser**
- Gain insight into **resigning employees' behavior**
- Securely manage **divestiture of business units**
- Eliminate unnecessary **regulatory disclosures**
- Govern **developer access & usage of source code**
- Protect **pharmaceutical & chemical formulas**
- **Geo enforcement** for roaming users
- **Prevent unauthorized access** such as impossible travel

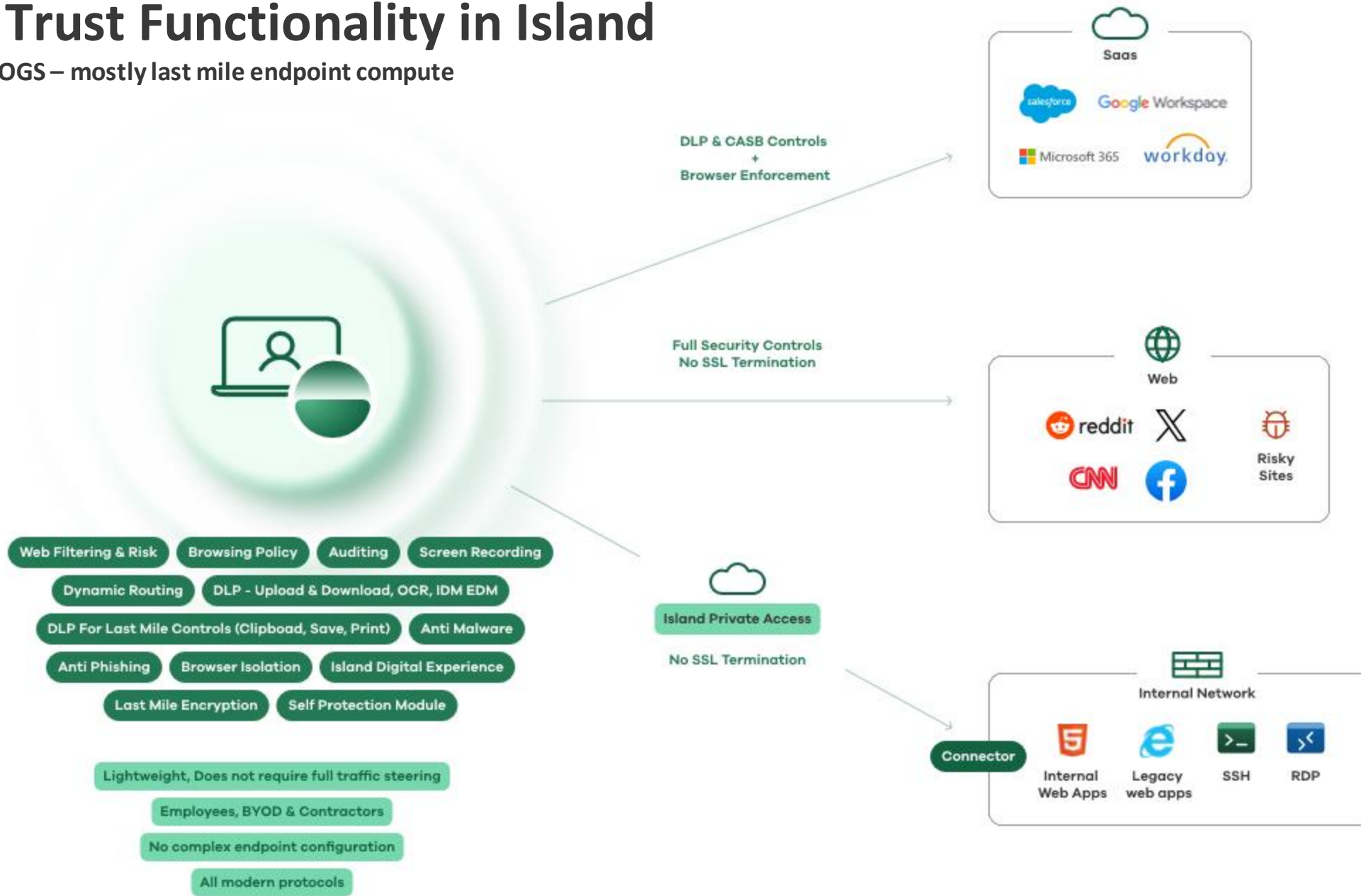
Island Private Access Solution Stack







solution is priced separately

Zero Trust Functionality in Island

Minimal COGS – mostly last mile endpoint compute



Security Capabilities Matrix - Island

Attack vector	Browser based attacks	File based attacks	Compromised environment	Data leakage
Attack type	<ul style="list-style-type: none"> Exploits (0-day, 1-day) Malware and ransomware Phishing attacks 	<ul style="list-style-type: none"> Weaponized Documents Executables Compressed & Archived Files Password protected files Files Drive-by downloads 	<ul style="list-style-type: none"> Man in the Browser Man in the Middle Malicious network Compromised device 	<ul style="list-style-type: none"> Accidental data leak Evil maid attack Sensitive data over-exposure
Capability	<ul style="list-style-type: none"> 0-day Browser Isolation (Process Isolation & OS Protections such as CFG, CET & ACG) 1-day Forced Update Dynamic anti-phishing Integrated Risk based threat intelligence and Malicious URL Filtering 	<ul style="list-style-type: none"> AV: Static, Dynamic, Hash and URL based Archive & password support CDR Secure Storage and Document Viewer/Editor 	<ul style="list-style-type: none"> SSL MITM Protection Extension Guard Cookies and Sensitive browsing data encryption Integrated Device Posture on disk an in-memory anti-tampering "Incognito mode" 	<ul style="list-style-type: none"> User actions control and audit (clipboard, print, screenshot...) Files and data DLP Force MFA for actions Idle-tab lock Sensitive data masking
Island module	 Island Security Suite	 Island Download & Upload policy	 Island Last Mile Security	 Island Last Mile Control

Policy based decisions: based on identity (OU, groups, users), device posture (managed / unmanaged, running AV), network posture (Wifi settings, public IP) Audits, alerts and SIEM integration for all capabilities



Thank you!