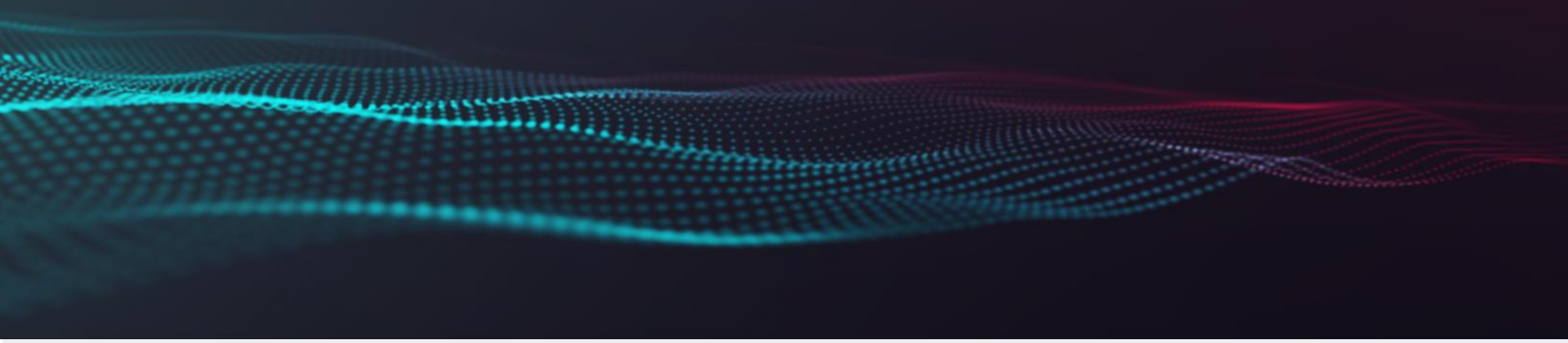
Enterprise Strategy Group | Getting to the bigger truth.™



ESG WHITE PAPER

A Breakthrough in Securing a Modern, Cloud-enabled Hybrid Workforce: Enterprise Browser

By Dave Gruber, Principal Analyst

January 2022

This ESG White Paper was commissioned by Island and is distributed under license from ESG.

Contents

Overview

With organizations leveraging more SaaS applications than ever before from a diverse collection of corporate-owned and non-corporate-owned devices used by both employees and third-party partners and contract workers, access control and sensitive data controls have become more complex than ever. New zero trust strategies seek to solve these issues. However, current security controls are flawed in their ability to effectively and efficiently provide IT, risk, and security teams the flexibility they require. New strategies are needed.

Organizations are leveraging third-party, SaaS-based applications at unprecedented levels to accelerate and manage operations, improve employee collaboration, and spin up new initiatives quickly. Concurrently, organizations are leveraging more partnerships and third-party contract resources to scale, optimize, and fill skills gaps within their workforces.

Meanwhile, the use of non-corporate-owned devices has become accepted in many organizations, with 43% of organizations reporting that they allow the use of personal devices for accessing corporate applications and data even though those devices are not fully managed with corporate software or policies.[1]

Data governance and regulatory bodies have become stricter than ever before, requiring IT, risk, and audit teams to demonstrate their ability to monitor and audit access to sensitive data and privileged operations across the many SaaS applications used by this diverse workforce.

This extended, hybrid workforce, together with the widespread use of non-corporate-owned devices, is limiting the visibility and control needed to ensure appropriate security posture and regulatory compliance. Even when managed devices are used, security teams struggle to implement consistent access and data security controls across internal and multiple SaaS applications. New strategies are needed to address these issues.

New Challenges

While these strategies are enabling organizations to grow and compete more effectively, they are challenging IT, security, and compliance teams' ability to:

- Implement fine-grained, user-access privileges that limit access to privileged capabilities in a consistent way across both internal/on-premises and the multiple SaaS applications in use.
- Prevent sensitive data leakage onto user-owned or non-corporate-owned devices.
- Audit the access/use of privileged functions and the access/usage of sensitive data.
- Leverage traditional network security controls to inspect progressively stronger encryption protocols.

[1] Source: ESG Research Report, End-user Computing Trends, to be published.

A Closer Look

SaaS and WebApp Protection

SaaS and internal Web applications have revolutionized how the modern workplace functions. The typically simple, seamless process of signing up and moving key business operations to the cloud has unlocked immense value and helped organizations avoid much of the heavy lifting they endured in the past.

Meanwhile, workers have moved outside the boundaries of office environments, opening the door for consumption of applications and sensitive data from user-owned devices in a variety of uncontrolled environments, making it almost impossible for IT, risk, and security teams to ensure effective data protection and governance.

As the use of both sanctioned and unsanctioned applications explodes, the need for constant exceptions (with different departments requiring access to different resources) is creating new layers of complexity for IT, risk, and security teams while degrading organizations' security posture and governance.

For example, a user can open up Google services, which in a traditional environment means they can open all services uniformly, since many of the URLs are the same for both private Workspaces and personal Gmail. This opens the door for data leakage, as users copy data from private to personal Google services.

Privileged Access Management and Governance

In this new SaaS-based world, IT and security teams are depending on SaaS application providers to deliver access and data security controls.

Yet SaaS applications are often designed around the most common use cases, offering limited, fine-grained roles-based access controls (RBAC) around both features and data.

Shadow IT Risks Data Leakage

32% of organizations report that employees signing up for cloud applications and services without the approval and governance from IT and security teams is one of their most significant data security challenges.[2]

IT and security teams therefore often offer over-privileged access accounts to both IT and line-of-business users to enable them to operate effectively. This creates exposure for both accidental and intentional theft of data and the potential to authorize data or services that fall outside of intended controls (i.e., business email compromise).

These same applications often lack the ability to audit the use of privileged functions and access of sensitive data, adding complexity for governance and audit teams. Forensic auditing is difficult at best, making it challenging to determine if, and when, users copy/paste data, download/save files, or simply screenshot data to user-owned or non-corporate-owned devices. While most organizations want to trust key IT and line-of-business resources, the need to "watch the watchers" still exists.

Contractor or Third-party Application Enablement

When contract resources require access to sensitive data or privileged functions, RBAC controls often fall short.

This becomes more acute during the contractor onboarding process, where setting up VPN, MDM, or even VDI can be time-consuming, causing many organizations to "fast-track" around necessary controls to accelerate onboarding. Contract resources often utilize devices owned and controlled by their employers, adding further complexity in the deployment of these controls on alternative-corporate-owned devices.

[2] Source: ESG Research Report, *The State of Data Privacy, Compliance, and Data Security*, October 2021.

Further complicating matters is the fact that, quite often, contractors might be working with a variety of clients, creating issues of cross-contamination of data across their client base.

Thin slices of capabilities are often needed, requiring additional access and data controls.

Further auditing of contractor activities (without crossing into personal activities) on user-owned or non-corporate-owned devices used by contractors can be difficult, if not impossible, for IT, risk, and security teams.

Collaboration Services

The use of consumer-oriented collaboration applications has become standard operating procedure for many.

Allowing the secure use of consumer or non-corporate apps where needed can help keep employees happy and can make teams requiring their use more productive. However, when organizations do this, they may degrade their security posture.

In-depth auditing of key interactions, policy control over data sharing, and redaction of key data that might be accidentally shared is unavailable in most cases, forcing most organizations to prohibit the use of these types of applications and tools.

Yet end-users persevere, often violating policies as they strive to increase their productivity and collaboration.

Current Approaches to Overcoming the Challenges

Expanding Browser Security

When it comes to factors that organizations consider when standardizing on a browser, improving security leads the list.[3]

When engaging with critical SaaS applications today, most organizations use general-purpose, consumer browsers, such as Chrome or Edge. While consumer-based browsers are beautiful pieces of technology, they are not built with governance in mind. They provide users complete access to the data shown on the screen, including copy/paste, printing or saving content, and taking screenshots. They provide no data governance in terms of user/app engagement and no control over what users can and can't do within an application.

Access Control

Given this longstanding browser governance problem, the industry has bolted on external technologies, including web gateways and cloud access security brokers, to manage application risk. However, most gateways offer only broad categorization and often lack fine-grained control over what you can do within an app. Cloud access security brokers can offer additional levels of control but are often limited by the capabilities of the cloud provider. Using these tools can be cumbersome and somewhat ineffective, motivating many to explore other options.

Further, advancements in SSL are making it challenging for existing security mechanisms to keep up, as TLS/SSL standard updates rightfully are becoming more difficult (and in some cases impossible) for in-line security controls to crack open and inspect.

Data Loss Protection, Compliance, and Regulations

With data regulations changing at a national and multi-national level (and varying considerably by jurisdiction), it is critical to manage regulatory risk by exerting flexible but fine-grained controls. However, finer-grained data access controls,

[3] Source: ESG Research Report, End-user Computing Trends, to be published.

beyond the basic controls that are offered by individual SaaS providers, are required by most, often resulting in overprovisioning of privileges for SaaS application users.

Adding controls for employees, contractors, or partners working on personal devices, restricting the capability to download and copy/paste sensitive data into user-owned devices, is often an impossible task.

When legacy, internally built applications are involved, IT, risk, and security teams face challenges adding the necessary controls to uphold new governance requirements, especially when AppDev teams are in limited supply or in many cases simply no longer available.

Rethinking Risk and Security Controls in a Cloud-enabled World

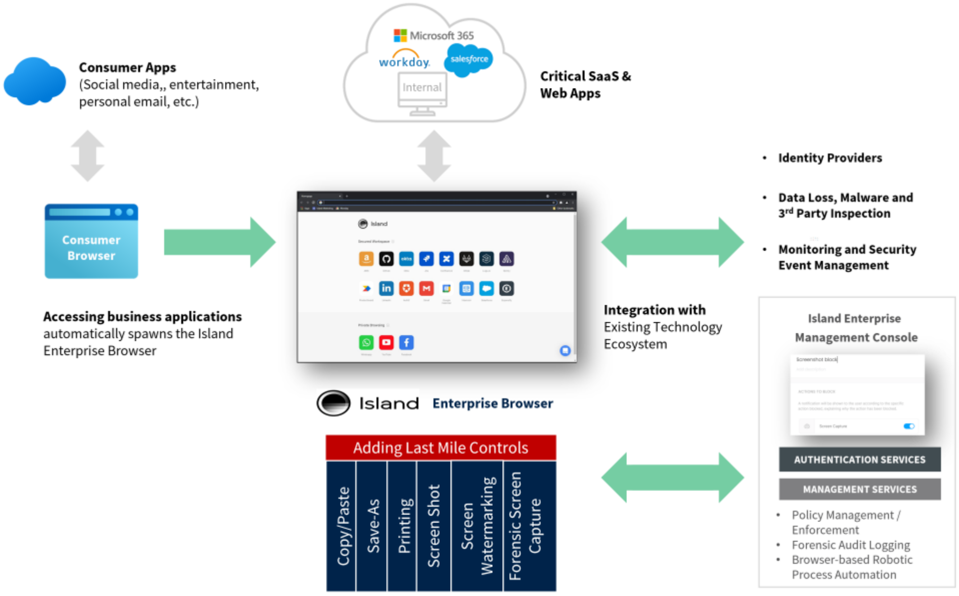
Island is a new, disruptive approach to securing a modern, cloud-enabled, hybrid workforce, providing users the freedom to leverage a multitude of SaaS, hybrid cloud, and internal web applications, while helping IT, risk, and security teams overcome many of the challenges associated with provisioning fine-grained access privileges, data leakage controls, and the fulfillment of governance and compliance requirements.

What is the Island Enterprise Browser?

Island is a new, security-enabled implementation of a web browser. It is architected using the same underlying Chromium browser capabilities utilized by both Chrome and Microsoft Edge, ensuring a consistent, almost indistinguishable u ser experience.

Island is intended to be used as a cooperative extension of an enterprise security architecture. Island can live alongside existing consumer browsers, allowing users to leverage their favorite browser for personal or non-critical work needs, but when accessing corporate applications, Island launches automatically and seamlessly (see Figure 1), applying consistent applications, services, and data controls. With core security controls embedded in the browser itself, organizations can shape how anyone works with their information from anywhere, while delivering the Chromium-based browser experience users expect.

Figure 1. Island Architecture


Microsoft 365
workday
salesforce
Internal
Consumer Apps
(Social media,, entertainment, personal email, etc.)
Critical SaaS & Web Apps
Consumer Browser
Accessing business applications automatically spawns the Island Enterprise Browser
Island Enterprise Browser
Adding Last Mile Controls
Copy/Paste
Save-As
Printing
Screen Shot
Screen Watermarking
Forensic Screen Capture
Identity Providers
Data Loss, Malware and 3rd Party Inspection
Monitoring and Security Event Management
Integration with Existing Technology Ecosystem
Island Enterprise Management Console
AUTHENTICATION SERVICES
MANAGEMENT SERVICES
Policy Management / Enforcement
Forensic Audit Logging
Browser-based Robotic Process Automation

Source: Island

Using Island, IT, risk, and security teams can make the browser behave *exactly* how they need it to, including the ability to:

- Fully control which user actions are allowed and in what use cases they are allowed.
- Audit, log, and trace any or all user activity.
- Add robotic process automation (RPA) supporting new workflows, integrations, and the addition of security controls into existing SaaS or internal web applications.

A Closer Look at What Island Delivers

Last Mile Control

Protecting sensitive data when users are leveraging web applications from unmanaged or user-owned devices is near impossible today. The ability to restrict local functions, including cut, copy, paste, and screen capture using an enterprise browser provides this critical, last-mile control, preventing the loss of sensitive information.

Further, an enterprise browser enables secure policies to be applied to private/public shared resources like Google Workspaces. Using an enterprise browser, a user can access corporate/private Google Workspaces and work fully as policies allow. Yet, when accessing personal Gmail (that a company may wish to block), policy can be implemented that limits what the user can copy/paste from a corporate/private Google Workspaces over to their personal Gmail, preventing sensitive data loss from private to personal workspaces.

Safe Browsing

Island delivers a new level of safe browsing and full visibility not offered by other security solutions. The Island Enterprise Browser allows users to freely browse the Internet while offering malware inspection, malicious category prevention, anti-exploitation, and integrated browser isolation capabilities, ensuring protection against malware infiltration, credential harvesting, and data exfiltration.

Device Posture Assessment

Island assesses the posture of the device it is installed upon and dictates the appropriate policy depending upon the device type of the logged-in user (managed, BYOD, contractor, etc.). This enables global, application-level, and even granular application usage control and precision data protection, reducing the dependency on more expensive technologies such as MDM, VPN, and VDI for many device-based needs.

Forensics/Audit

Island provides a complete forensic audit record over all browser activity with granular control over the depth of what is captured by user, device-type, application, and location. Island even captures events and insights as granular as copy/paste, screen captures, printing, saving, and custom information, which can be easily viewed as built-in dashboards and reports or exported to your current aggregation platform.

Multi-tenancy Control

Tenancy refers to a unique situation generally associated with cloud-based services: How do you block or control access to one instance of a cloud service while allowing another? Island can ensure control over *which* tenant your users are engaging.

- Are they using the company tenant for an application? If yes, then allow them to engage more freely.

- Are they using a personal tenant for that application? If so, then prevent them from uploading or pasting data into that tenant.

This assures a much greater level of governance over these situations.

Centralized Management

With Island, administrators can set granular policies based on user, device, location, app, and many other parameters, all from a single centralized management console, providing the ability to:

- Add additional layers of security and data access.
- Create new workflows and IT controls.
- Customize presentation of third-party SaaS applications without the need to involve the SaaS provider.

Browser-based Remote Process Automation

RPA is a capability that allows a company to configure software to capture and interpret applications for processing a transaction, manipulating data, triggering responses, and communicating with other digital systems. Island introduced browser-based RPA, which allows an organization to build automation scripts over the presentation layer of any web-based application. This ensures the organization can alter workflows of any application based on business need, seamlessly introduce additional security controls over an application (such as 2FA within a critical transactional area) or integrate to external systems to make use-based workflows cleaner. And while initially focused on security controls, browser-based RPA could positively impact many different use cases across IT.

The Bigger Truth

A cloud-enabled, work-from-anywhere, any-device workforce has caused IT, risk, and security teams to completely rethink the architecture and underlying technologies they use to effectively secure and govern their organizations. As the dependency on third-party applications and workers continues to become the standard of operation for most organizations, new approaches to security and governance are required.

ESG thinks that organizations should explore what Island is doing, using a new, enterprise-class browser as a disruptive approach to security and governance. Specific attention to the extended workforce is particularly interesting, as supply-chain risk continues to increase at unprecedented levels.

Enterprise Strategy Group is an IT analyst, research, validation, and strategy firm that provides market intelligence and actionable insight to the global IT community.

www.esg-global.com ✉ contact@esg-global.com ☎ 508.482.0188