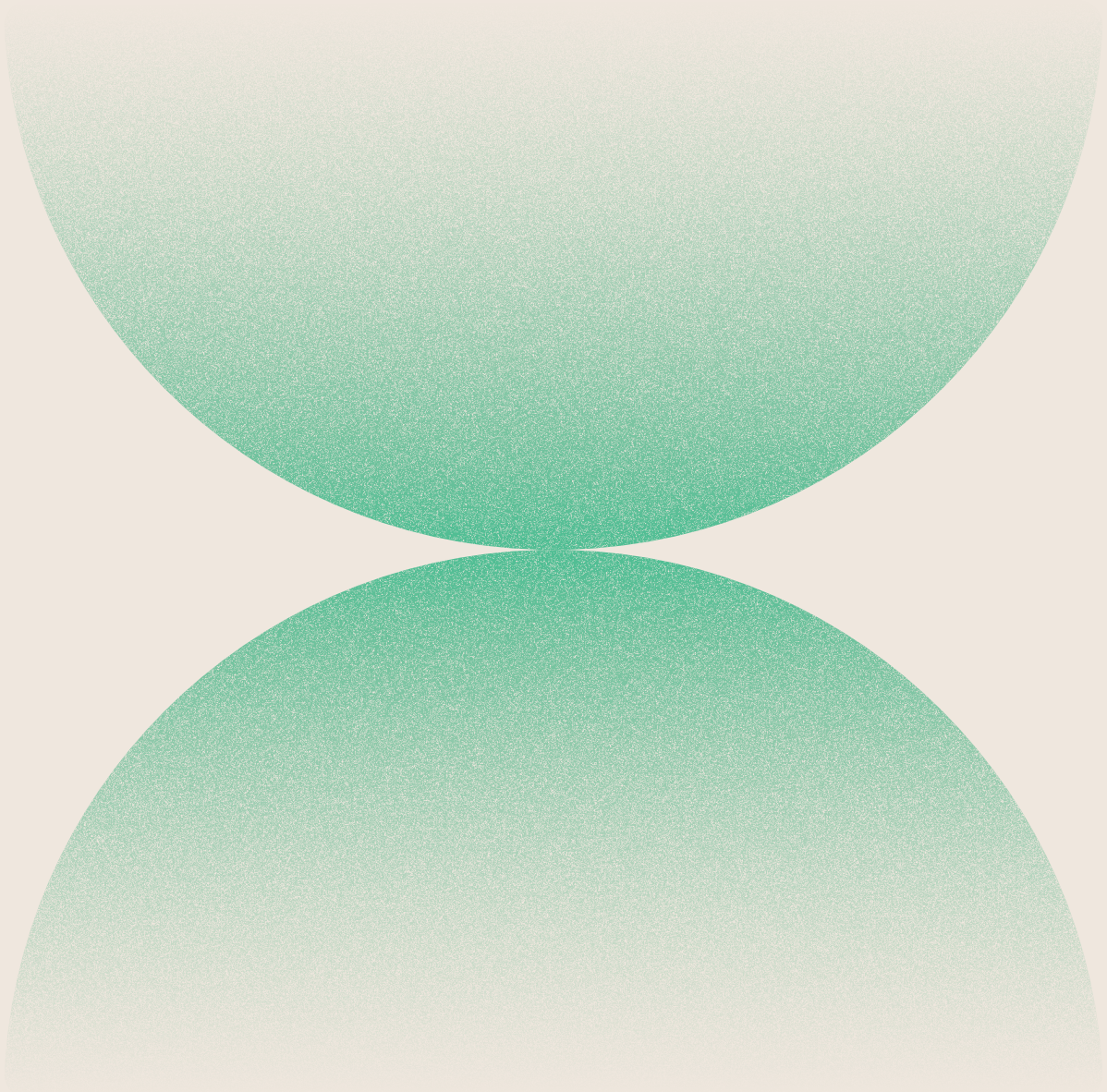
Island

The Island Enterprise Browser: **A Comprehensive Solution for a Viable BYOD Policy**

Solution Brief | May 2023



Introduction

Organizations have long struggled with implementing effective BYOD policies due to concerns over data leakage, user privacy, device identification, and regulatory compliance. Traditional solutions such as MDM, VDI, and VPN are often complex to manage and cumbersome for end-users to enroll a new device. Many BYOD programs have failed to reach widespread adoption due to the classic Goldilocks problem: a light touch approach is more appealing for end-users, but leaves data and devices largely unprotected. The more intensive management controls that expand data protection do so at a cost to user privacy, convenience, and ultimately user acceptance.

> **The Island Enterprise Browser offers a viable path that's just-right for both IT & Security staff and the end-users they aim to protect. Island's integrated BYOD capabilities offer a novel approach to managing BYOD policies by leveraging policy-based governance and last-mile controls, without taking control of the device itself and the personal data in holds.**

Challenges with Traditional BYOD Solutions

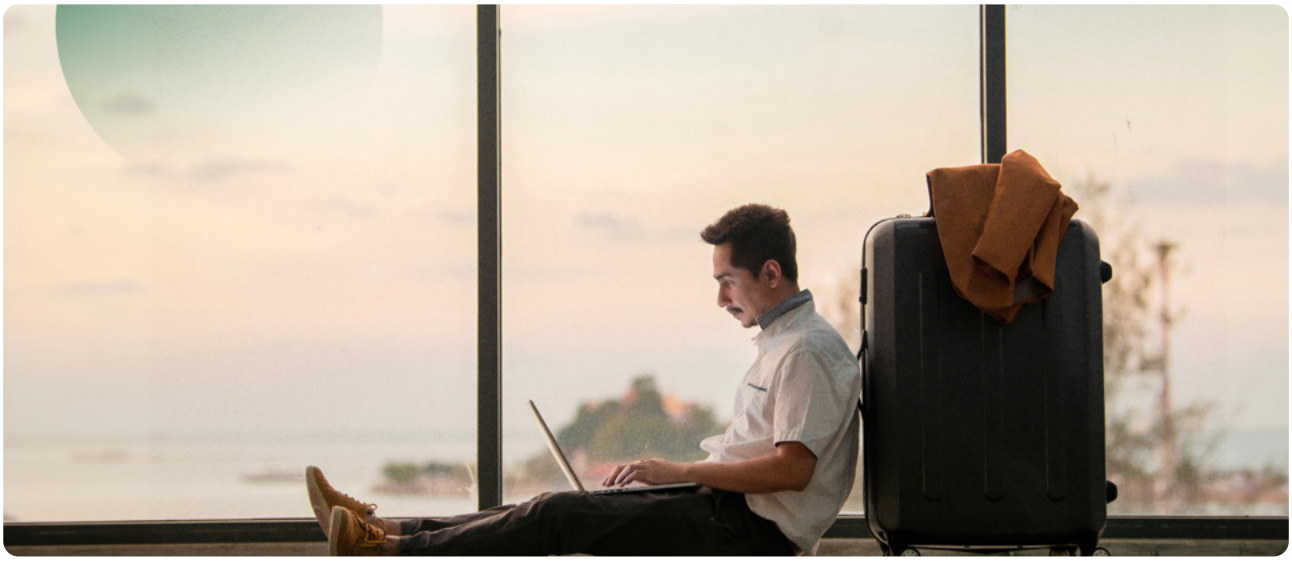
The challenges associated with traditional BYOD solutions can be categorized into three main areas: the mechanics of BYOD access, protecting application data against leakage, and ensuring user privacy and anonymity. Deploying and managing BYOD access with traditional solutions is a complex and cumbersome process. Implementing VPN clients, for instance, requires significant overhead and often results in backhauling all traffic through a VPN concentrator, which degrades network performance. Further, this is counter to the goals of many organizations not wishing to have unmanaged devices connected to their internal networks. MDM technologies, while useful for managing devices, are extremely limited in managing actions or data within applications. Further, MDM can be quite invasive on a personal device: granting IT the ability to redirect network traffic for inspection or remotely wipe a personal device is a hard pill to

swallow for the average employee. And finally, VDI adds significant cost and operational overhead, particularly when used only for delivering web applications.

In addition, existing policies often focus on user identity rather than device posture, which limits dexterity in policy enforcement. Effective policy decisions require a clear distinction between managed devices and BYOD, with granular inspection of the current device posture. For example, it's wise to consider the current OS patch level and disk encryption status before making an access decision for sensitive applications and content.

One of the main concerns for organizations implementing a BYOD policy is the potential for untraceable application data leakage. Traditional data loss prevention solutions are often unable to assert themselves on unmanaged devices. Further, these solutions may be limited in protecting data from being copied, downloaded, or even shared through screenshots. The same sharing features that make apps quite convenient also open the door to easy data exfiltration. Setting aside intentional data leakage, residual data left behind on unmanaged devices from downloads cannot be easily controlled — if identified at all. This inability to distinguish between work and personal personas on the same device leads to cross-contamination of personal and company data.

Maintaining user privacy and anonymity in a BYOD environment is also crucial, but it can be difficult to achieve with traditional solutions. Traffic backhauling sends personal user data through corporate inspection and logging, which results in privacy issues and non-compliance with data sovereignty regulations. Even mundane details like the list of installed apps on a mobile device could reveal personal details about a user that they want to keep private. Moreover, corporate data in the wrong regions can cause regulatory and privacy concerns, and organizations must ensure that they can safely store and revoke data according to their legal obligations. The tradeoffs on both sides of BYOD and privacy can be quite daunting.



The Island Enterprise Browser: A Comprehensive Solution for BYOD Management

Island, the Enterprise Browser with built-in BYOD capabilities, offers a more streamlined and effective approach for BYOD programs. By installing the Island Browser and logging in with corporate credentials, users can easily access and use corporate applications without compromising security or privacy.

Island simplifies the provisioning process for BYOD through easy browser installation and enterprise login via the existing single-sign-on provider, which significantly reduces the complexity overhead associated with VPN, VDI, and MDM. For the user, it's no different than installing a web browser — a task that virtually all users are familiar with. Yet behind the scenes, Island decreases risk by identifying device characteristics like OS patch level, encryption status, geolocation, and application destination, to govern access and in-app usage based on these criteria. Data leakage from app interactions is stopped with last-mile controls that prevent risky data actions such as copy and paste to unwanted destinations, screenshots of sensitive data, or saving downloads to a personal device. User workflows and productivity are maintained by seamlessly redirecting downloads to a secure storage (typically the organization's Google Drive or OneDrive).

Island also ensures user privacy by separating personal and work interactions. Users can choose the personal browser of choice for personal use, while redirecting all work applications to open through Island. By segregating personal and corporate personas, Island audits only corporate-specific actions and maintains compliance with data sovereignty and regulatory requirements. This strikes the perfect balance between securing the corporate resources and the user's privacy in a BYOD world.

Conclusion

The Island Enterprise Browser offers a comprehensive and viable solution for implementing and managing BYOD policies. By addressing the challenges associated with traditional BYOD solutions and providing additional value in terms of security and privacy, Island offers a seamless and efficient approach to BYOD management. Its capabilities, such as simplified provisioning, data leakage control, and user privacy, make Island a viable option for organizations seeking to reap the benefits of BYOD without compromising security or compliance.

> As a result, Island enables organizations to balance the needs of their employees for flexibility and personal device usage with the critical requirement to protect corporate data and maintain regulatory compliance. In short, Island achieves the just-right approach to BYOD management, offering organizations a viable, robust and user-friendly solution to address the challenges and complexities of traditional BYOD implementation.