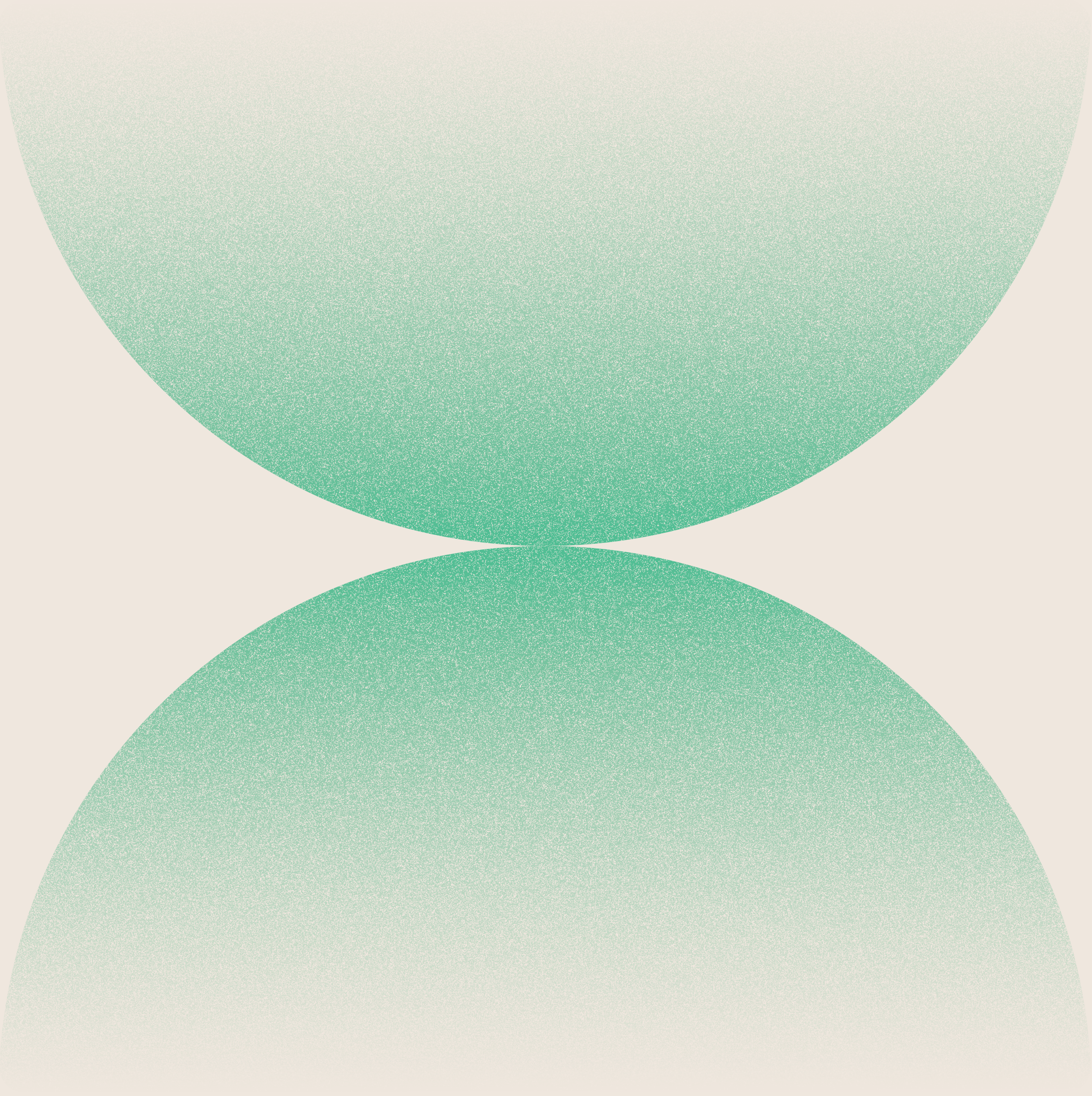
Island

Supporting Developers: **Productivity and Security in Harmony**

Solution Brief | June 2023



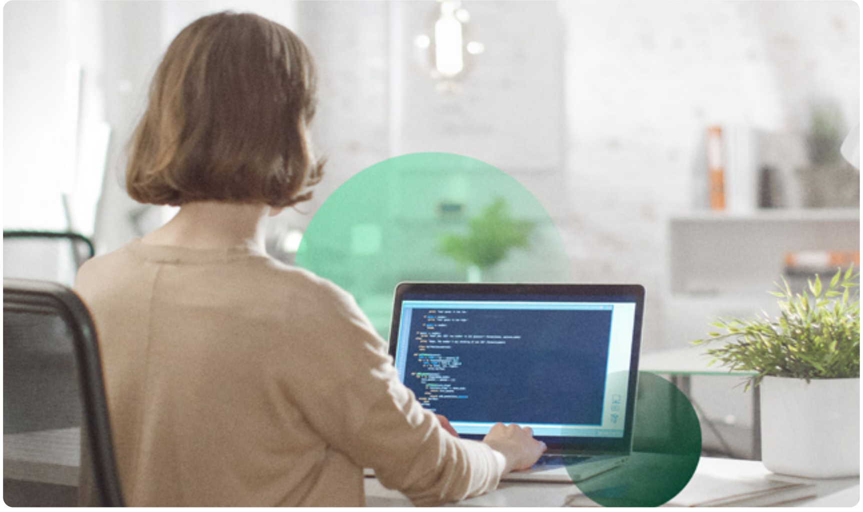
Introduction

Software developers represent a unique and mission-critical user community for many organizations. The wide range of tools and workflows required for software development, testing, and deployment require a different approach for effective IT management and security practices. Unlike most of their colleagues, developers usually require full administrator controls for their development systems so they can work efficiently. Due to the developer's necessary workflows and level of access, they are also a desirable target for malicious attackers — intercepting the software supply chain is the ultimate prize for bad actors. Security professionals and IT infrastructure teams need to take a nuanced approach to enhance productivity and security when working with developers. This paper outlines three broad categories of how an organization can support developers, whether in-house or external, and where Island, the Enterprise Browser, offers unique value.

Trusted In-House Developers

The simplest model for technology companies with a large base of in-house developers is the hands-off approach. IT teams count on a high degree of technical expertise among their developer staff where self-support and self-enablement is preferred. From selecting the device and managing the OS to patching and using development tools, the developer is responsible for it all. This model provides the least potential for friction and is often appealing for the developer persona who wants to optimize their environment to fit their exact requirements and personal preferences. In essence, this is the purest form of BYOD: the organization issues credentials to the developer and lets them do the rest.

In this model, Island is installed on-demand by the developer on any device: computer, mobile phone, or tablet. All major OS platforms are supported, so developers can use Island on the device and OS that they prefer. Island adds device posture assessment so the organization can define standards for device configurations while still allowing for individual autonomy.



Unlike many other IT or security tools, Island installs within the user-space and does not require system-level configuration changes, allowing developers to retain precise control over their endpoint environment. Island natively integrates with enterprise identity providers and Island Private Access to offer quick access to the applications and resources needed, whether they're internal or publicly accessible. A developer simply authenticates once to Island and all their tools are immediately available — with no additional agents to install or system-level configurations required. While some development tools reside outside the browser, Island can optimize engagements with many essential development tools where additional access controls and visibility are desired:

- Product and issue tracking tools (e.g., Atlassian suite)
- Code repositories (e.g., GitHub)
- Web consoles for CI/CD tooling (e.g., Jenkins)
- Cloud-based IDE (e.g., AWS Cloud9)
- Performance monitoring and analytics dashboards (e.g., Grafana)
- Administration consoles for cloud infrastructure (e.g., AWS)
- Internal backend systems (e.g., customer tenant administration consoles)

By their nature, these tools contain highly sensitive and proprietary information that deserves additional protections. With Island, organizations can apply zero trust access principles to these applications, whether they're privately hosted or SaaS applications. Robotic process automation (RPA) capabilities allows an organization to further tailor the workflows or specific features within these applications. For example, in the AWS console, Island can require an additional MFA challenge before adding a user, or enforce naming and tagging requirements when creating objects. In GitHub, Island can limit the option to create SSH keys for only certain users. By applying these RPA policies within the browser itself, there's no additional dependency on the underlying application and they can be deployed or modified in seconds.

With data protection policies, the information within each application is protected from inappropriate disclosure without interrupting the development workflow. For example, Island can prevent proprietary source code from being shared in a prompt with the consumer version of ChatGPT, while allowing for use of the Island AI assistant or other enterprise AI tools. Island also offers audit and logging of application access and engagements within the application. For critical workflows such as changes to production infrastructure, Island can both require additional authentication steps (like a step-up MFA challenge) and record the precise actions taken, including screenshots. This data can be fed to change management systems for end-to-end auditability.

This deployment model optimizes for efficiency, flexibility, and developer control. IT and Security teams get the benefit of device inventory records collected by Island along with lightweight enforcement for device posture configuration: every time Island is used to access web applications, it queries the current device configuration for attributes like OS version, disk encryption, or local firewall settings. Device posture attributes can be collected passively or used as an enforcement mechanism. For example, restricting access to sensitive applications unless the OS is up to date on patches. The developer retains control over when and how device configurations are updated, so there is no risk of an endpoint management agent interrupting their workflow or interfering with their development environment.

Managing External Contractors

For organizations who work with external developers (i.e., contractors), it's wise to apply more management controls. The organization may choose to issue the workstations with endpoint management controls and place requirements on the specific tools used for the software development lifecycle. The developers in this model typically retain local administrator access on their endpoint so they can install other development tools and optimize their environment for their specific workflow.

> In this model, Island can be easily deployed via the endpoint management platform or installed manually. Just as before, Island greatly simplifies access to company resources and development tools by integrating with the identity provider and Island Private Access. Adding browser enforcement policies for critical applications ensures that Island is used where it's needed and left as an option for other browsing. All of the controls outlined above for in-house developers can be applied in this model as well.

For an environment where endpoint management and EPP tools are used on devices where the developers are local administrators, Island's device posture queries are valuable as an audit check: since a user with administrator controls could easily disable to uninstall EPP or management agents, Island offers a control point to collect current device status and require those agents are active before accessing sensitive applications.

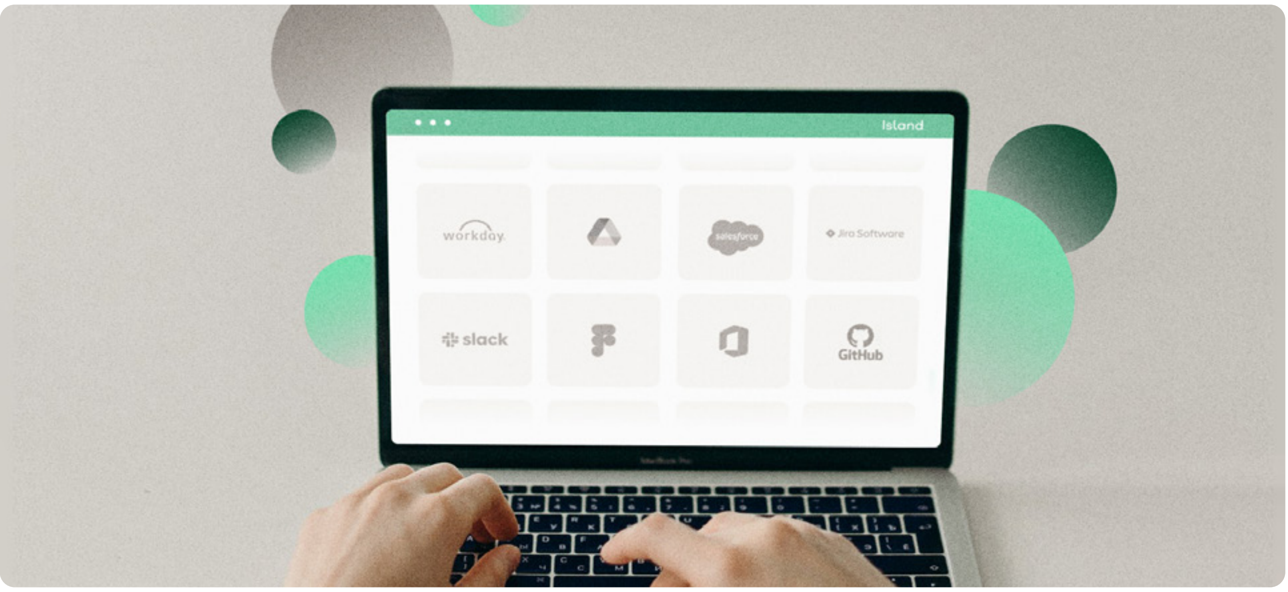
Developers in Sensitive Environments

For organizations with strict security requirements, or that operate in highly regulated environments, all end-user access — including developers — is more tightly controlled. In the prescriptive controls model, developers use endpoints that are configured and managed by their IT and Security teams, and do not hold local administrator credentials. The tools and workflows for development are prescribed and centralized to eliminate risk as much as possible.

Here, Island can be deployed as the default browser by the endpoint management system. All the advanced security controls, such as DLP, last-mile data controls, MitM protections, and tampering protections, perfectly complement a high-security development environment.
In addition to the developer-specific controls outlined above, all activity within the browser can be audited to aid incident investigations and security researchers to strengthen the enterprise security posture. This data is easily shared with analytics platforms to demonstrate compliance with change control policies.

Island Capabilities to Enhance Developer Workflows

IT and Security teams choose Island as the key technology for improving security and access controls across all web engagements. The Enterprise Browser goes beyond the security framework of a common browser to protect against external web threats, protect local data from exfiltration, and provide zero trust access controls. Last-mile controls prevent sensitive data from moving outside trusted enterprise applications and tenants. The detailed logging collection capability enhances visibility into critical web activity and interfaces with SIEM or data analytics platforms to enhance the overall enterprise security stack. All of these capabilities are centrally managed through the Island Management Console to provide global scalability and support a distributed workforce.



Going further, Island offers several key capabilities that add value directly to the developer's workflows:

- **Island Private Access** offers secure connectivity to internal web applications like code repositories or testing tools from outside the corporate network, including from a mobile device. Unlike VPN or ZTNA solutions, there's no additional agent or client to install.
- **Browser-based SSH Client** offers secure server access within Island. This can be used along with IPA to enable convenient access when developers are working remotely.
- **Browser-based RDP Client** to connect to backend systems. Like SSH, this can be used along with IPA for access from external networks. Privileged Access Management offers secure access to protected applications without disclosing actual credentials.
- **Island Password Manager** offers an enterprise-grade password and secrets manager that is available through the browser or as a standalone desktop application.
- **Robotic Process Automation** offers a mechanism to modify or enhance web applications to optimize workflows without requiring changes to the underlying source code.
- **Smart Clipboard Manager** offers multiple clipboard entries for fast retrieval, with the intelligence to protect sensitive information, along with RPA integration to pre-populate commonly used entries.
- **Profile Manager** offers developers the ability to operate Island with multiple identities to aid in testing or troubleshooting.

Conclusion

Thoughtful considerations are needed when supporting developers and their need for harmonious productivity, workflow efficiency, and security. Whether an organization takes a hands-off approach and full developer autonomy, or applies a more prescriptive approach to tools and endpoint management, IT and Security teams play an important role in enabling and securing developer workflows. Island, the Enterprise Browser, offers a unique platform to secure critical applications and data without adding friction.

Learn more about Island at Island.io.