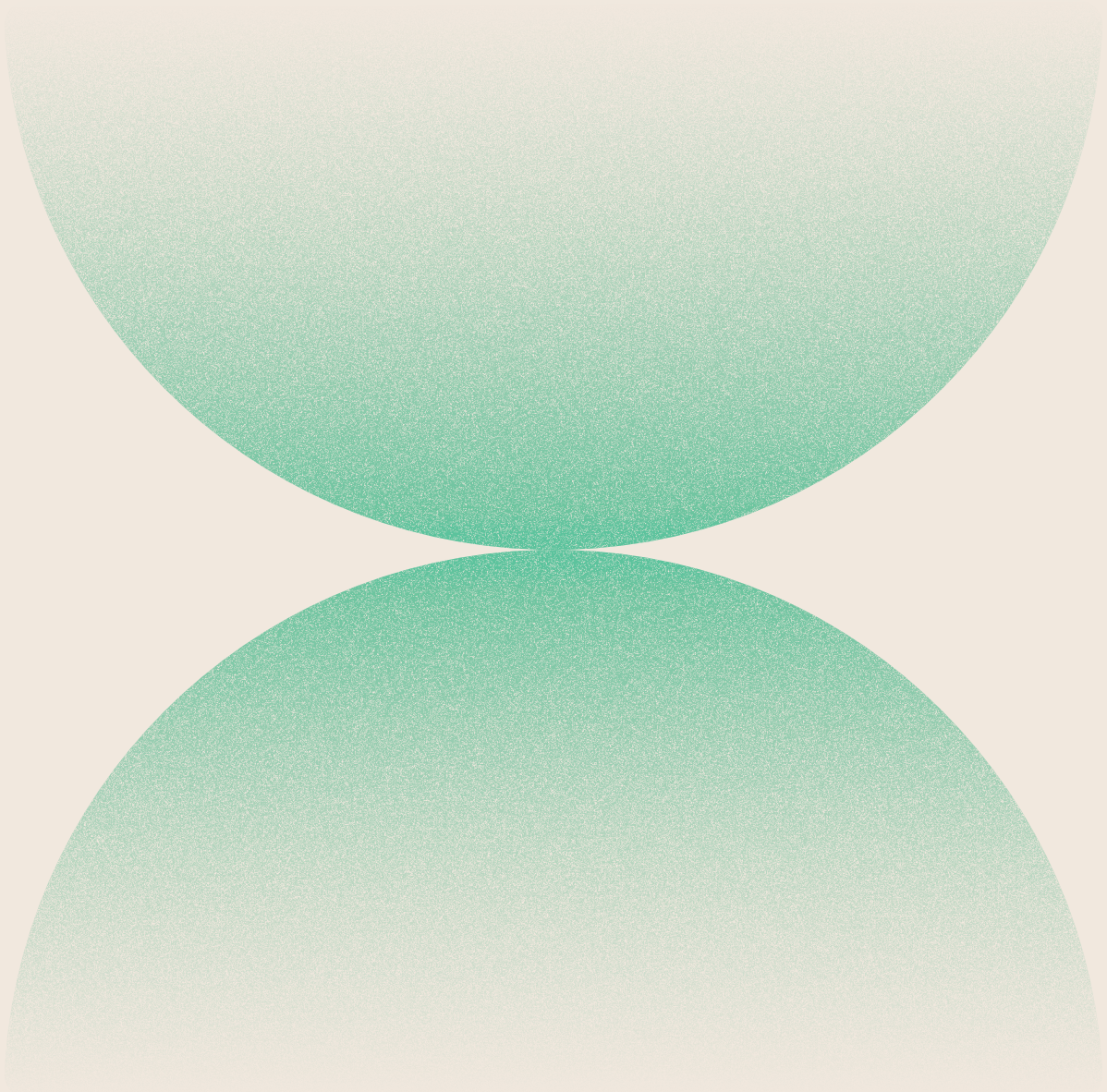
Island

Zero Trust in the Browser

Solution Brief | August 2022



Zero Trust Foundations

The zero trust security framework represents an important shift in the way we think about cybersecurity. As the name suggests, we eliminate the implicit trust between systems that is all too commonly exploited by malicious actors. Building on decades of hard-learned lessons, zero trust pushes the role of identity and authorization away from the network perimeter and onto each system or request. It assumes that compromise is inevitable and builds resilience through a distributed security architecture.

The building blocks that form the foundation of zero trust are not new: the principle of least privilege, federated identity, and multi-factor authentication are concepts that have sustained both technical and commercial success across decades. Today's challenge in adopting the zero trust methodology is primarily around integration and implementation. By its nature, a zero trust architecture requires coordination between systems at all levels of the technology stack. The goal is a robust security architecture that's low friction and easy to use.

This paper outlines the benefits of a zero trust architecture and how the Island Enterprise Browser greatly simplifies the task of implementation and integration.

Motivations for Zero Trust

The accelerating adoption of zero trust security in this decade is helped by the changing dynamics of the modern workplace. The shift from a central office model to remote or hybrid work makes the old network perimeter paradigm obsolete. At the same time, the shift away from on-prem servers to cloud and SaaS solutions continues apace. Put together, it's now common for critical business data to flow between a home network that is outside corporate control to a SaaS provider's network that is outside corporate control. The need for an evolved security paradigm is obvious.

As a sign of the category maturity and long-term strategy implications, many governments are recommending the adoption of zero trust architecture. In the United States, a 2021 Executive Order directed federal agencies to develop a plan to implement zero trust architecture, building on guidance from the National Institute of Standards and Technology (NIST). Separately, the Cybersecurity and Infrastructure Security Agency (CISA) maintains a Zero Trust Maturity Model. Other nations have issued similar guidance, such as the U.K. National Cyber Security Centre's Zero Trust Architecture Design Principles.

The benefit for governments to adopt zero trust architecture is clear: these are extremely large, complex, distributed organizations that manage huge volumes of sensitive data and are routinely targeted by malicious actors. The zero trust model is not limited to large organizations and scales remarkably well. Even at the individual level, companies like Apple and Google apply zero trust concepts to protect user accounts and prevent casual credential misuse.

Zero Trust Network Access

Within the broad umbrella of zero trust, zero trust network access (ZTNA) is a common implementation strategy. Dozens of technology vendors offer some flavor of ZTNA to protect private applications and replace legacy VPN gateways. As mentioned above, the dramatic increase in remote and hybrid work makes remote access a critical capability. Legacy VPN presents both security and operational deficiencies that need to be addressed.

Legacy VPN Deficiencies

- **Overbroad trust:** legacy VPN joins an endpoint to a private network. This connection enables remote access, but it can also be exploited by a malicious actor to move laterally.
- **Traffic congestion:** legacy VPN routes network traffic from the endpoint to a centralized VPN gateway. As more users connect to VPN, the gateway is a bottleneck that will reach saturation and degrade network performance.
- **Egress inefficiency:** traffic destined for SaaS or cloud has to pass through the legacy VPN gateway, only to be sent back out through an egress point to reach the Internet. This inefficiency adds latency and cost without any benefit.
- **All or nothing:** most legacy VPN clients will route all network traffic from the endpoint, regardless of its destination. In addition to the congestion and egress issues listed above, this raises privacy concerns for users who may be uncomfortable with sending all their network traffic through the enterprise network.

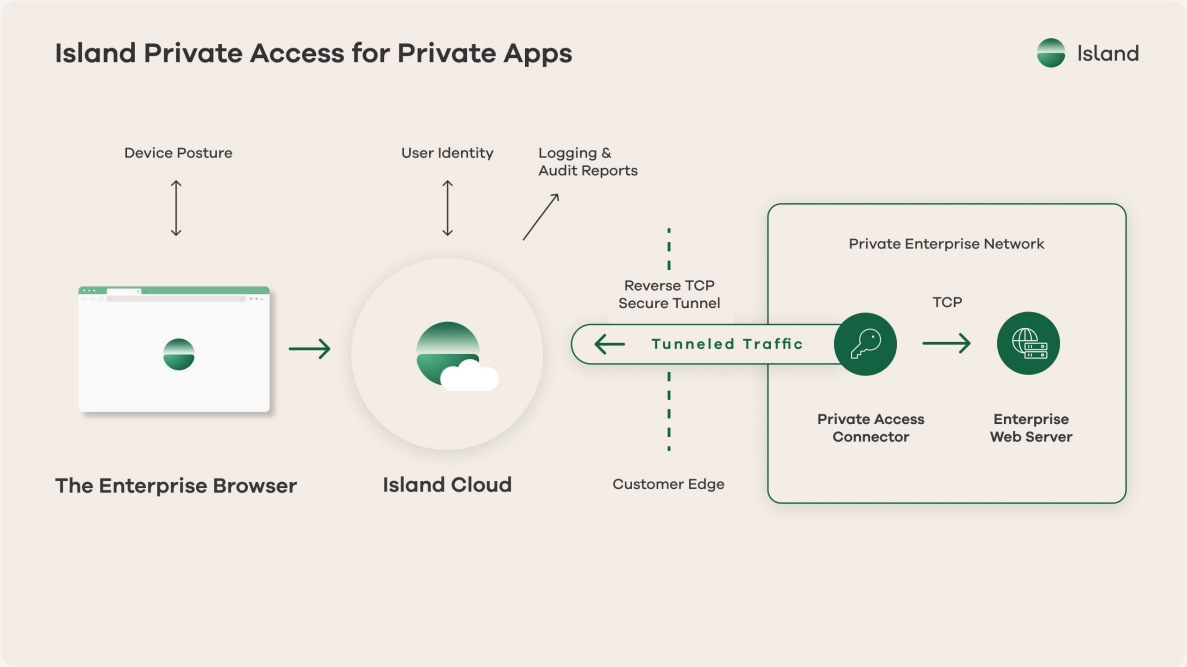
The ZTNA approach answers these concerns and offers a superior security model. (In fairness, VPN is a technology that predates ZTNA by over a decade and it served its purpose well.) With a ZTNA model, users can access private apps and resources without backhauling traffic through a gateway. Importantly, a ZTNA connection is application-specific and does not join the endpoint to the private network, as with legacy VPN. This eliminates several categories of potential exploitation and right-sizes the trust relationship.

Island Private Access

For organizations who have implemented a ZTNA solution, the Island Enterprise Browser makes an ideal complementing technology that extends the zero trust model beyond the network through the last mile.

> For organizations who are ready to implement a zero trust security model, the Enterprise Browser with Island Private Access offers the complete solution to protect all browser-based private and SaaS apps and resources.

For organizations who are ready to implement a zero trust security model, the Enterprise Browser with Island Private Access offers the complete solution to protect all browser-based private and SaaS apps and resources. Because the browser already integrates with Island Cloud for policy enforcement, extending secure access to a private network is completely transparent to the end-user. The same browser they use for secure access to SaaS and public cloud apps can be used for private apps with no additional clients or agents. Island Private Access Connectors are lightweight virtual machines that are easily deployed within a private cloud or data center to enable secure remote access. The connectors make an outbound connection from the private network to the Island Cloud, and all traffic is passed to the connectors through a reverse TCP secure tunnel. The private network stays private, with no ports open to the outside.



The Last Mile of Zero Trust

Applying the principles of zero trust architecture means considering the full end-to-end flow of information. One area that's often overlooked is the last mile – where and how users interact with sensitive apps and data.

Managing *where* users can access data is important so you can keep data off unsafe or potentially compromised devices. The most sophisticated security controls in the world are meaningless if data is freely allowed to exit the controlled environment. A lost or stolen laptop can become a serious data breach if last mile controls like data encryption and endpoint protection are ignored.

An example from the U.S. health care sector:

A hospital employee's laptop was stolen from their parked car in the hospital parking lot. The laptop was used for work purposes, but it was not managed by hospital IT so it lacked key security mitigations like disk encryption. Unfortunately, the laptop contained personal health information of over 20,000 individuals. In 2020, the hospital paid over $1 million in a settlement agreement.

Requiring the Island Enterprise Browser to access sensitive apps and resources gives the organization a control point to ensure data doesn't end up on unsafe devices. The browser continuously evaluates the configuration and security posture of the device it's running on to check for disk encryption, endpoint protection agents, or directory service registration. And since the browser can be installed on any device, including unmanaged or BYOD, this offers flexibility while ensuring good security practices.

Managing *how* users interact with sensitive data is important to ensure that sensitive data remains under control and doesn't leak outside the organization. In the context of zero trust philosophy, we are adding granularity to user authorization: we do not implicitly trust a user to copy, print, or save data outside the browser even if they are authorized to view that data. In practice, this means adding context-aware controls to govern actions like printing, saving a page, copy & paste, taking a screenshot, or sharing content over Zoom or Teams. Adding these controls for sensitive apps and data completes the last mile of a zero trust security model.

Visibility and Governance

The final layer of any robust security model is visibility and good governance. It's never sufficient to implement security controls without inspection and continuous validation. High-fidelity logging of access attempts, user activity, and security enforcement is vital. This serves both as validation for the in-place security controls and informs future governance of the evolving security policy. Just as we should not implicitly trust a device based on its network location alone, we should not implicitly trust a security policy without ongoing validation and governance. The Island Enterprise Browser stands apart in its ability to capture high-fidelity logging with full context. Unlike other approaches that require manipulating network traffic or decrypting SSL for inspection, Island observes all browser activity natively.

> The Island Enterprise Browser stands apart in its ability to capture high-fidelity logging with full context. Unlike other approaches that require manipulating network traffic or decrypting SSL for inspection, Island observes all browser activity natively.

Conclusion

Zero trust is an important shift in philosophy. It's built on decades of security research and hard-learned lessons from the trenches. As security practitioners, it's important to step back and consider the full end-to-end data flow. ZTNA is an important piece of the puzzle, but there's a real opportunity to go beyond that with last-mile controls. This insight, coupled with today's shift to web-based apps and resources, informed the design of the Island Enterprise Browser. Wherever you are on the zero trust journey, Island offers a unique approach where the web browser itself plays an active role in the security strategy.

Sometimes changing one thing changes everything.