

Isla Isolation Platform

Isla Isolation Platform with email and web security is a simple yet effective security solution that delivers immediate protection against threats such as phishing, ransomware, . . . without any loss of productivity to the end user.

Why Isla?

Organizations around the world face unprecedented cybersecurity challenges. As security leaders and practitioners search for innovative technologies to strengthen cybersecurity, the end user continues to remain the weakest link and accounts for nearly 70% of breaches (Cyberinc Cyber Insights 2021). When every user is remote working in a cloud-first environment, CISOs trying to decrease risk from innovative attackers face a dilemma: security or productivity? With Isla, you can have both. Isla remotely isolates all browsing sessions to shift the risk away from the endpoint, enabling you to stop bad things from happening even if you cannot stop end users from clicking web pages, email links and attachments.

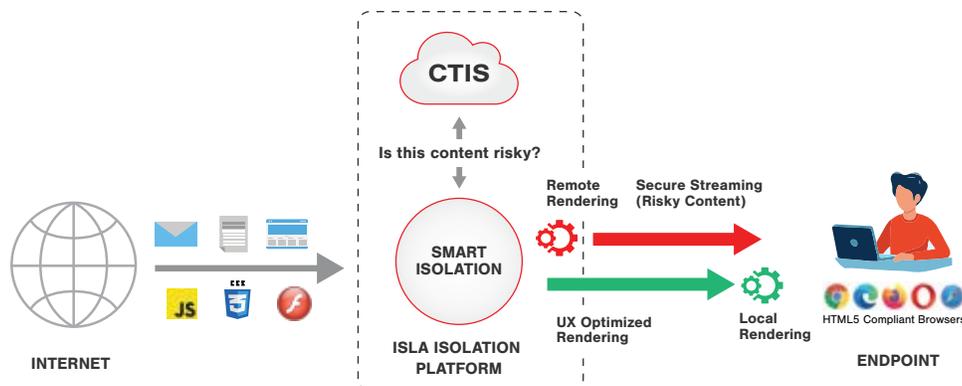
A Zero Trust Security Solution for Email and Web

Isla with a remote disposable browser shifts the risk away from the local browser enabling you to stop bad things from happening even if you cannot stop end users from clicking web pages, email links and attachments. Cyberinc Email Security closes email security gaps in Microsoft 365 by isolating links and scanning attachments to prevent email attacks via web and native Outlook clients. Isla stops email and web threats at the door.



Risk-Based Isolation

The Isla Smart Isolation technology moves trust away from the endpoint to safely fetch, execute, and render content with context-aware isolation powered by dynamic risk assessment and policy-based controls. Isla transforms code and content into a combination of remotely rendered visual stream and UX-optimized local rendering. Smart isolation renders risky elements of the page (or risky pages) remotely and less risky elements (or pages) locally. With selective isolation, instead of isolating all traffic for all users, you can isolate traffic based on the category of traffic, risk levels and user profiles to align security with the organizations risk appetite and compliance needs. With the Isla Platform, there is no compromise on experience, no compromise on security.



New Features and Benefits

Smart Isolation	Risk isn't a single dimensional problem. So why should your solution be? The new smart isolation technology, an industry first, intelligently identifies page risk to adapt isolation to risk levels of the page and page elements. Risk identification can be administratively managed and aided by the Cyberinc Threat Intelligence Service (CTIS).
Selective Isolation	Need administrative control over what traffic to isolate? Selectively isolation allows for a quick and simple deployment by offering easy administrative control over what traffic needs to be isolated. Traffic segmentation can be based on the category of traffic, risk levels and aligned with the organization's risk appetite and policies.
Email Security	Email and web represent two of the most exploited attack surfaces. Secure users' personal email access over webmail as well as corporate email access with traditional email clients, such as Outlook. Isla scans attachments and can rewrite email links to force them through an isolated environment to block phishing and credential theft attacks.
Seamless Rollout	Gain quick and seamless deployment with an agentless solution that can be deployed as a cloud-based service. Or if you prefer more control, you can choose an on-premise or hybrid deployment. Deploy Isla for all users or your most at-risk users with simple user, group and organization-level policy controls.
Integration with Security Stack	Deploy Isla standalone or with a complementary security stack such as web proxies, NGFW, SIEM, sandbox, etc. Isla maximizes your ROI from existing security technologies while also enhancing the security levels.

Benefits of Isla Isolation Platform

Security Before the Breach	Step threats before they become a breach. Proactively get ahead of an evolving threat landscape.
IT Productivity	Isla's Zero Trust model enables security and IT teams to stay ahead of attacks and focus on critical tasks instead of having to respond to burdensome alert storms.
User Behavior and Threat Visibility	Gain insight into attacks, attack vectors, targeted users and more with Isla's rich dashboard and reporting capabilities.
Acceptable Use Policy Enforcement	Enforce corporate and regulatory requirements with user and group-based policies for browsing control and rich reporting.
Deployment Simplicity	With agentless deployment and the ability to selectively isolate traffic, Isla simplifies adoption and enables administrators to scale deployment according to the risk levels.

About Cyberinc

Cyberinc prevents web, email, and document-based threats before a breach occurs, using a Zero Trust model powered by isolation-based security. The company's flagship Isla Isolation Platform simplifies enterprise security by shrinking the exposed threat surface and eliminating the risk of breach from a user's inadvertent click on a malicious link or download of a threat-containing document. Based in the San Francisco Bay Area, Cyberinc is trusted by business and government institutions around the world. More information can be found at [cyberinc.com](https://www.cyberinc.com).

Contact us

+1 925-242-0777
info@cyberinc.com