Cyberinc

Datasheet

Cyberinc Isla: Smart Isolation

Security and user experience are often forces tugging opposite ends. Users need access - access introduces risk, while blocking access to information impedes productivity. Security practitioners constantly pivot trying to find the right balance – giving access to some web categories and web sites while blocking off access to others. As more workers move remote, workloads move to the cloud, and access becomes core to business, achieving the right balance is imperative.

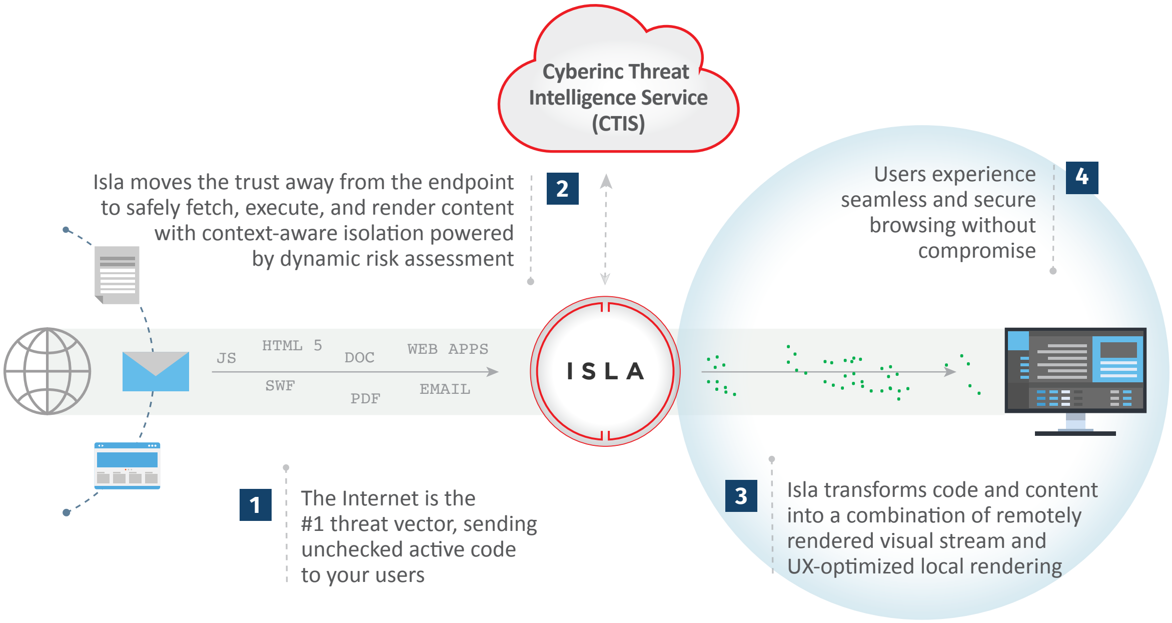
Several organizations have explored newer capabilities such as browser isolation to address these challenges (64% organizations expressed interest in these capabilities in a recent Cyberinc survey). Browser isolation, built on the principles of Zero Trust, acts by shifting the risk away from the endpoint to a remote disposable browser, transforming all internet content into harmless streams delivered to the endpoint.

Isla Smart Isolation

Organizations adopting browser isolation seek to address concerns around ensuring optimal end-user experience while identifying the key web sites or selecting web categories that should be isolated to ensure security.

As security experts well recognize, context matters. Risk isn't restricted to a site or a category – good sites sometimes deliver threats while uncategorized sites aren't always malicious. Risk also changes with user profile – users with access to key information are often more at risk than those without.

Isla Smart isolation advances the browser isolation technology, to simplify deployments and improve user experience through context-aware isolation. Smart Isolation adapts the browsing experience with dynamic risk assessment, powered by Cyberinc Threat Intelligence Service, to remotely fetch & execute web pages and safely render them according to risk levels.



Cyberinc Threat Intelligence Service (CTIS)

2 Isla moves the trust away from the endpoint to safely fetch, execute, and render content with context-aware isolation powered by dynamic risk assessment

4 Users experience seamless and secure browsing without compromise

1 The Internet is the #1 threat vector, sending unchecked active code to your users

3 Isla transforms code and content into a combination of remotely rendered visual stream and UX-optimized local rendering

Figure 1: Isla Smart Isolation

Risk-Based Rendering

Web sites represent various levels of risk - web applications sites used for business, social media sites, fake links used to steal credentials, web pages used to download malware, malicious advertisements on good pages, etc. Smart isolation fetches and executes all web pages remotely, while rendering risky elements of the page (or risky pages) remotely, and less risky elements (or pages) locally. In other words, the user experience for oft used & less risky pages will be native while ensuring security for elements that pose a risk.

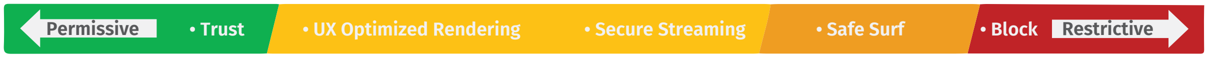


Figure 2: Risk-based Isolation

UX Optimized Rendering vs. Secure Streaming

Isla supports two different models of rendering – UX Optimized and Secure Streaming. The secure streaming model offers a higher security by performing the entire fetch-execute-and-render functions in a remote disposable browser, securely streams harmless pixels to the endpoint. The UX optimized model balances security with optimal user experience by intelligently rendering potentially harmful elements of a page (e.g. images, videos) remotely while safe elements (e.g. text) locally. It allows end users to maximize the native experience (scrolling, right-click, copy-paste, etc.) while minimizing the exposed browser footprint. When combined with Smart Isolation, the two models ensure that organizations obtain the strongest security balanced with the best end-user experience.

Powered by Cyberinc Threat Intelligence

Cyberinc Threat Intelligence Service (CTIS) is at the heart of Smart Isolation. CTIS identifies the risk-levels of a page using a combination of attributes including site reputation, recency of registration, registrar, cousin domains, etc. The risk-level of the page determines the rendering approach used with Smart Isolation – trusted, isolated, rendered as a read-only page with Safe Surf, or blocked.

Policy-based Controls

Smart Isolation disentangles the administrative challenge of security vs. usability, while simultaneously taking the burden of ensuring "click security" away from end users. Administrators can tune the risk-based controls to suit business needs or override it with URL or category-specific controls that can be at the organization, user-group or user-level.

UX Optimized Rendering vs. Secure Streaming

Simplified configuration	Simplifies the setup for browser isolation, unraveling the administrative challenge of choosing security vs. user experience.
Administrative controls	Adapt your security to suit your organizational needs with organization, user-group and user-level controls.
Optimal end user experience	Maximize end user experience with intelligent UX optimized rendering for oft used safe pages - deliver safety without compromise.
Context-aware security	Identify the risk levels of a page and a user to appropriately adjust the levels of isolation.
Quick time to value	Optimize the time to security and maximize the ROI from your isolation investment.

About Cyberinc

Cyberinc helps you experience a safer Internet by proactively stopping web, email, and document-based threats. Cyberinc's Isla platform uses cutting-edge isolation technology to neutralize threats and prevent them before they have a chance to act, simplifying the security strategy and delivering immediate protection. Cyberinc is trusted by businesses of all sizes and governments around the world.

2021.01.28.1

Contact us

☎ +1 925-242-0777

✉ info@cyberinc.com