

Isla Protection for Document Based Threats



Safe Document Downloads

Isla gives administrators the ability to set policies that allow their users to safely upload and download documents. When enabled, Isla renders documents in a safe read-only mode that prevents weaponized documents from executing malicious code on the endpoint.



Credential Theft Protection

If users are taken to a spoofed website built to look like a trusted file sharing site, Isla renders the page in read-only mode, preventing users from entering and inadvertently losing their credentials.



Malware Scanning

When documents are downloaded Isla will scan the document for malware prior to delivering it to the user. This ensures safe and easy access to original content when necessary while eliminating the risk of malicious file downloads.

Document Threat Protection

Weaponized documents are one of the most common delivery vehicles for malware in phishing, spearphishing, and whaling attacks. All it takes is one user to open a weaponized document and your entire network may become vulnerable to a multitude of threats including scripts, macro viruses, trojans, keyloggers, spyware, ransomware, and rootkits.

With the Isla platform, your users are safe from document-based malware. Isla's policy-based controls allow administrators to set user, group, and organization level permissions to allow or block document downloads and uploads. Isla also transforms documents such as Excel and PowerPoint files into a safe remote rendering to keep document downloads from putting your organization at risk of compromise. Users can still download original or transformed files. Isla scans all documents as they are downloaded to ensure no malware makes it through the isolation barrier.

Additionally, as the need to share large files, collaborate on documents in real-time and the risk associated with attachments increases, more organizations are moving toward document sharing services that provide a link to download the document rather than attaching files in email. When your users click a link to access or download these document types, they are instantly protected within Isla. If a user accesses a spoofed site that appears to be a trusted document sharing site (like Google Drive or Dropbox) Isla will flag the site as suspicious and render it in read-only mode preventing the user from inputting their login credentials.

Document Security with Isla

- 1 Documents are opened remotely in the Isla Isolation Platform in a safely rendered format
- 2 Policy controls to allow administrators to control file downloads & uploads
- 3 All files are scanned for threats before delivery



Weaponized Documents

Isla enables policy-based controls and transforms documents into a safe rendering to keep document downloads from putting your organization at risk of compromise. Isla protects you from document-based threats including scripts, macro viruses, trojans, keyloggers, spyware, ransomware, and rootkits.

| Isla Document Protection | | | |
|--|--|---|--|
| Policy-based Controls | Define policies to control who can download and who can't | | |
| Document Threat Neutralization | Transform documents into a safely-rendered form protecting users from threats delivered through document downloads | | |
| Zero Day Protection | Integration with Isla and 3rd Party sandboxes for known and unknown threats | | |
| Protection from Multiple Document Threat Types | <ul style="list-style-type: none"> • Macro Viruses • Trojans | <ul style="list-style-type: none"> • Keyloggers • Spyware | <ul style="list-style-type: none"> • Ransomware • Rootkits |

Isla neutralizes all web-based threats by implementing a Zero Trust framework that isolates all incoming code, scripts, media, and other web content. Isla fetches, executes and renders all content remotely - away from your endpoint, and pixel streams the result to the endpoint, thwarting even the most complex threats and zero-day attacks. Users continue to use the web and their applications as always, but now they are safeguarded behind a layer of isolation.

Isla Benefits

- **Proactive Security** - Stop threats before they become a breach; proactively get ahead of new threats.
- **IT Productivity** - Stay ahead of attacks and focus on critical tasks instead of being burdened with alert storms.
- **Seamless User Experience** - No change to user behavior required; they use their browsers exactly as before.
- **Regulatory Compliance** - Isla helps meet PCI, HIPAA, MPAA, and other regulatory compliance requirements.
- **Broad OS & Browser Support** - Windows, Mac, and Linux-friendly security available on all major browsers.
- **User Behavior & Threat Visibility** - Isla's rich dashboard provides insight into attack vectors, targeted users, and user behavior.
- **Acceptable Use Policy Enforcement** - Enforce corporate and regulatory requirements with policy-based browsing controls and reporting.

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.

Contact us

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