SECURITY WHITEPAPER

Isola Shield

Air-Gapped Redaction for Regulated Industries
Technical Architecture and Security Analysis

Version: 1.0

Date: January 2024

Classification: Public

Author: Isola Studio Security Team

Table of Contents

1. Executive Summary

Key Findings

- **Zero Network Transmission:** Isola Shield processes all data locally in the browser with zero network requests.
- **HIPAA Compliant:** On-device processing eliminates PHI exposure risks during media preparation.
- **GDPR Ready:** Privacy by Design — data never crosses a network boundary.
- **Verifiable Security:** Users can verify zero network traffic using browser DevTools.

Isola Shield is a browser-based redaction tool designed for regulated industries handling sensitive data. Unlike traditional cloud-based AI tools that transmit user data to remote servers for processing, Isola Shield leverages modern web technologies to perform all processing locally within the user's browser.

This whitepaper provides a comprehensive technical analysis of Isola Shield's security architecture, compliance mappings for major regulatory frameworks, threat model, and an audit checklist for security teams evaluating the platform.

> **Document Purpose**
>
> This whitepaper is intended for IT directors, security officers, compliance teams, and auditors evaluating Isola Shield for use in regulated environments including healthcare, legal, and government sectors.

2. Architecture Overview

2.1 On-Device Processing Model

Isola Shield's core architectural principle is that all data processing occurs within the user's browser. This is achieved through a combination of modern web technologies that enable high-performance computation without server-side processing.

Table 1: Processing Model Comparison

Aspect	Traditional Cloud AI	Isola Shield
Data Transmission	Files uploaded to remote servers	Zero network transmission
Processing Location	Vendor infrastructure	User's browser (local)
Data Retention	Often retained for model training	Never stored or retained
Offline Capability	Requires internet connection	Full functionality offline
Auditability	Black box — trust vendor claims	Verifiable via DevTools

2.2 WebGPU and WebAssembly

Isola Shield leverages two key technologies to enable high-performance local processing:

WebGPU

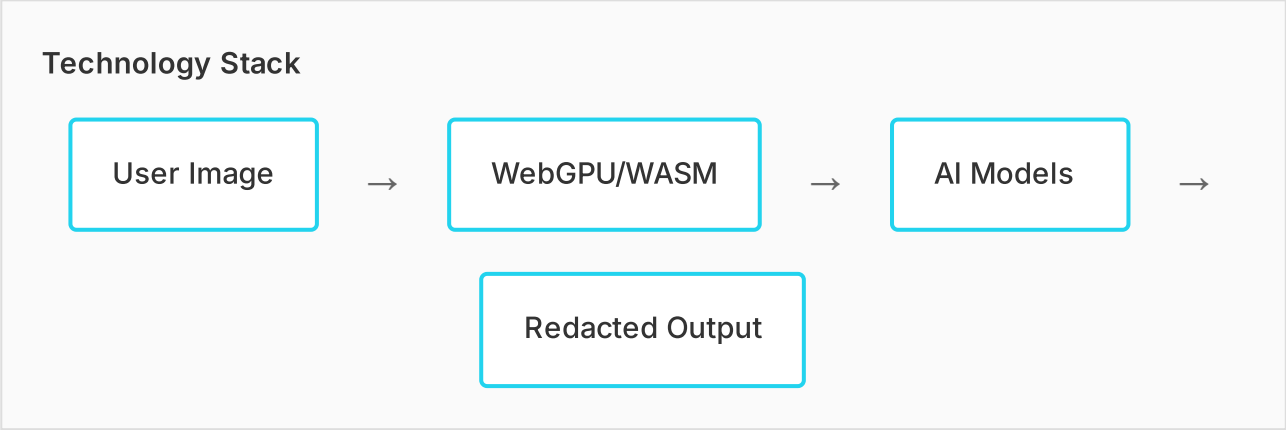
WebGPU is a modern web standard that provides low-level access to GPU hardware. It enables Isola Shield to:

- Run neural network inference at near-native speeds
- Process high-resolution images and video in real-time
- Leverage hardware acceleration for AI models

WebAssembly (WASM)

WebAssembly serves as a fallback for browsers that don't yet support WebGPU, and for certain processing tasks:

- Cross-browser compatibility
- Near-native performance for CPU-bound operations
- Secure sandboxed execution environment



2.3 Data Flow

The complete data flow within Isola Shield is as follows:

1. **Initial Load:** Application code and AI models are downloaded from the server (one-time, cacheable)
2. **File Selection:** User selects a file from their local filesystem
3. **Local Processing:** File is processed entirely within the browser's memory
4. **Output Generation:** Redacted file is generated and offered for download
5. **Memory Cleanup:** All session data is purged when the tab closes

> **Important Note**
>
> At no point in this flow is user data transmitted over the network. The Network tab in browser DevTools will show zero requests during file processing.

3. Compliance Mapping

3.1 HIPAA Compliance

The Health Insurance Portability and Accountability Act (HIPAA) establishes standards for protecting sensitive patient health information. Isola Shield addresses key HIPAA requirements:

Table 2: HIPAA Requirements Mapping

HIPAA Requirement	Isola Shield Implementation
Administrative Safeguards (§164.308)	No PHI leaves user's device; no BAA required for processing
Physical Safeguards (§164.310)	Data remains on user's hardware; no third-party data centers
Technical Safeguards (§164.312)	End-to-end local processing; no transmission encryption needed
Minimum Necessary (§164.502(b))	Only processed data exists; no copies stored

3.2 GDPR Compliance

The General Data Protection Regulation (GDPR) governs data protection in the European Union. Isola Shield's architecture aligns with GDPR principles:

- **Data Minimization (Article 5(1)(c)):** Data is processed only for the specific purpose of redaction and never retained
- **Storage Limitation (Article 5(1)(e)):** No data storage — session ends when tab closes
- **Privacy by Design (Article 25):** On-device processing is the default and only mode
- **Right to Erasure (Article 17):** No copies exist to erase — data was never stored

3.3 SOC 2 Type II

SOC 2 Type II evaluates an organization's controls over time. While Isola Shield's architecture differs from traditional SaaS platforms, it addresses the Trust Services Criteria:

Table 3: SOC 2 Trust Services Criteria

Criteria	Isola Shield Approach
Security	Browser sandbox provides isolation; no server attack surface
Availability	Works offline; no dependency on vendor infrastructure
Processing Integrity	Deterministic AI models; reproducible results
Confidentiality	Data never transmitted; no third-party access
Privacy	No data collection; no tracking; no telemetry

4. Threat Model

4.1 Security Assumptions

Isola Shield's security model is based on the following assumptions:

1. **Browser Security:** The user's browser is assumed to be uncompromised and up-to-date
2. **Hardware Security:** The user's device is assumed to be physically secure
3. **Network Security:** Initial application load occurs over HTTPS
4. **User Intent:** The user intends to redact their own data

4.2 Threat Actors

Table 4: Threat Actor Analysis

Threat Actor	Capability	Risk Level
Network Eavesdropper	Cannot intercept data — no transmission occurs	Negligible
Malicious Vendor	Cannot access data — processing is local	Negligible
Browser Malware	Could potentially access in-memory data	Low (mitigated by browser sandbox)
Physical Attacker	Could access device if unlocked	Medium (user responsibility)

4.3 Mitigation Strategies

Technical Mitigations

- **Subresource Integrity (SRI):** All loaded scripts are verified with cryptographic hashes
- **Content Security Policy (CSP):** Restricts resource loading to prevent injection attacks
- **HTTPS Only:** All initial loads occur over encrypted connections
- **Memory Isolation:** Browser's same-origin policy isolates application data

Operational Mitigations

- **No Data Retention:** Zero server-side storage eliminates data breach risks
- **No Telemetry:** No usage data, error reports, or analytics are collected
- **Transparent Operations:** Open verification via browser DevTools

5. Audit Checklist

Use this checklist when evaluating Isola Shield for your organization:

Technical Verification

- ☐ Verify zero network requests during file processing (DevTools Network tab)
- ☐ Confirm AI models load from cache on subsequent visits
- ☐ Test offline functionality by disconnecting internet
- ☐ Review Content Security Policy headers
- ☐ Verify Subresource Integrity hashes on loaded scripts

Compliance Verification

- ☐ Map Isola Shield's architecture to your compliance requirements
- ☐ Document the on-device processing model for auditors
- ☐ Verify no Business Associate Agreement (BAA) is needed for HIPAA
- ☐ Confirm data sovereignty requirements are met
- ☐ Review this whitepaper with your legal team

Security Verification

- ☐ Assess browser security posture in your environment
- ☐ Review endpoint protection on user devices
- ☐ Verify HTTPS enforcement for initial load
- ☐ Test in your air-gapped environment if applicable
- ☐ Conduct penetration testing if required by policy

Operational Verification

- ☐ Train users on proper redaction workflows
- ☐ Establish procedures for handling redacted outputs

- [ ] Document Isola Shield in your data processing inventory
- [ ] Plan for browser compatibility in your environment
- [ ] Review update and patch management procedures

6. Conclusion

Isola Shield represents a paradigm shift in how sensitive data is processed. By leveraging modern web technologies to perform all computation locally, it eliminates the fundamental risks associated with cloud-based processing: data transmission, third-party access, and vendor lock-in.

For organizations in regulated industries, Isola Shield offers:

- **Verifiable security** — Users can confirm zero network transmission
- **Simplified compliance** — No data leaves the device
- **Operational independence** — Works offline without vendor infrastructure
- **Transparent operations** — Open architecture, no black boxes

> **Contact Information**
>
> For questions about this whitepaper or Isola Shield's security architecture, contact:
>
> **Security Team:** security@getisola.com
> **General Inquiries:** contact@getisola.com

Document Version: 1.0 | **Last Updated:** January 2024