browserling

sandboxed virtual browsers

Browserling Security Overview

Safe. Isolated. Ephemeral. Trusted.

Browserling is a secure, browser-based testing and investigation platform designed for cybersecurity teams, SOC analysts, incident responders, and digital forensics professionals. It enables safe interaction with suspicious links, files, and websites by isolating them completely from your local environment, significantly reducing the risk of malware execution, data leaks, and drive-by attacks.

Our core security principle is simple: **every session is isolated, ephemeral, and destroyed after use**. URLs, session data, and browsing content are not persistently retained, shared, or accessible by humans as part of normal service operation.

This document is provided for informational purposes only and does not create any contractual obligations, warranties, or commitments. Browserling's security obligations are governed solely by the applicable written agreement between Browserling and the customer.

How We Handle Customer-Provided URLs

- **Ephemeral Processing**: Every URL you input is opened inside a temporary, isolated virtual machine (VM).
- **No Persistent Storage**: We do not persistently store or log the URLs you test, nor do we keep copies of the web pages, session activity, or downloaded content.
- **Automatic Deletion**: Once your session ends, the entire virtual machine, including any memory, browser cache, downloaded files, and URL data, is destroyed upon session termination or shortly thereafter.
- **No Human Access**: URLs and session activity are not accessible to Browserling staff under normal operations.

1. Security Architecture

1.1 Sandboxed Virtual Browsers

- Each session runs in a dedicated, sandboxed virtual machine (VM).
- The sandboxed architecture is designed to prevent malware, exploits, and malicious scripts from escaping the VM or interacting with other sessions.

- Hypervisor-level isolation is designed to contain even kernel-level attacks.

1.2 Ephemeral Sessions

- A fresh VM is provisioned for every session.
- After the session ends, the VM is securely destroyed, including RAM, disk, browser cache, and all temporary data.
- No snapshots, disk images, or session content logs are retained.

1.3 No Local Execution

- All activity occurs in Browserling's secure infrastructure.
- No browsing activity or tested content is executed on the customer's device, significantly reducing the risk of local infection or system compromise.

1.4 Secure Networking

- All communication between your browser and Browserling is protected by end-to-end TLS 1.2+ encryption.
- TLS is enforced on all network paths, including file uploads and downloads.

2. Threat Model & Risk Mitigations

Threat	Mitigation
Malware execution	Runs only inside isolated VM. Designed to prevent escape to the host system.
Drive-by downloads	All content remains in sandbox. Content remains within the sandbox environment.
Exploit attempts	Kernel, browser, and hypervisor isolation prevent privilege escalation.
Data exfiltration / callback	Network isolation policies prevent C2 callbacks from reaching internal networks.
Phishing or credential theft	Sandbox separation ensures credentials are not linked to real environments.

These mitigations assume customers follow recommended best practices and do not intentionally input sensitive credentials or confidential data into sandboxed sessions. If enabled, files or other content may be downloaded from a sandbox at the user's request and should be treated as untrusted once outside the sandbox environment.

3. Data Protection & Privacy

3.1 Data Lifecycle

- **Input**: User provides URL, file, or command via browser.
- **Execution**: The input is processed inside an isolated VM.
- **Destruction**: Upon session termination, the VM and all associated memory, disk, and temporary storage are securely wiped upon session termination or shortly thereafter.

3.2 Metadata Retention

- We collect **minimal metadata**: timestamp, source IP, and user agent for abuse prevention, analytics, and security monitoring.
- URLs, session content, browsing history, and files are not persistently retained.

3.3 Human Access

- Session content is not accessible to Browserling personnel under normal operations.
- All sandbox operations are automated and isolated.

4. Compliance and Legal

Browserling's data handling practices are aligned with leading global privacy regulations, including:

- **GDPR (General Data Protection Regulation)** – European Union
- **CCPA / CPRA (California Consumer Privacy Act & California Privacy Rights Act)** – United States (California)

We do not sell, share, or monetize any personal information.

4.1 Data Processing & Legal Requests

- Browserling acts as a **data processor** for session data.
- Customers determine the purposes and means of processing Customer Data; Browserling processes such data solely on Customer instructions as described in the applicable agreement.
- Customers may request a **Data Processing Addendum (DPA)** for compliance documentation.
- Legal requests for data are handled in strict accordance with applicable laws and require valid process.

5. Security Best Practices & Use Cases

5.1 Recommended Workflows

- **URL Analysis**: Paste suspicious links directly into the sandbox and observe behavior without exposure.
- **Malware Detonation**: Upload potentially malicious files and safely monitor their execution.
- **Threat Intel**: Investigate phishing kits, C2 servers, and onion sites without risking your network.
- **Incident Response**: Quickly triage alerts by detonating artifacts in a contained environment.

5.2 Best Practices

- Avoid reusing credentials inside sandboxed browsers.
- Avoid uploading sensitive files inside sandboxed sessions.
- Use temporary or decoy accounts for any authentication inside the sandbox.
- Quarantine and scan any files downloaded from sandboxed sessions before opening them locally.
- Leverage multiple browser and OS combinations to identify environment-specific exploit attempts.
- Use geo-browsing and Tor access when investigating campaigns that change behavior based on location or anonymity.
- Regularly review and update internal policies on sandbox use as part of your security awareness program.
- Integrate Browserling into your SIEM/SOAR workflow for automated URL analysis.

6. Trust & Responsible Disclosure

Browserling is committed to continuous security improvement.

- Security researchers are encouraged to report vulnerabilities responsibly.
- Please contact us at security@browserling.com for disclosures.
- We aim to acknowledge reports within 48 hours and provide status updates within 7 days.

Why It Matters

Our approach is simple: treat every browsing session as temporary, isolated, and disposable. Once you close your session, session data, including URLs you input, is destroyed.

Trusted by Leading Enterprises

Leading cybersecurity teams at Fortune 100 companies, global governments, banks, stock exchanges, universities, newspapers, militaries and IT consultancies use our virtual browser technology.

Website: www.browserling.com

One-click demo: www.browserling.com/browse

Security contact: security@browserling.com

Enterprise sales: sales@browserling.com