Bromium®

DATA SHEET

# BROMIUM SECURE BROWSING

## Secure, User-Centric Browsing

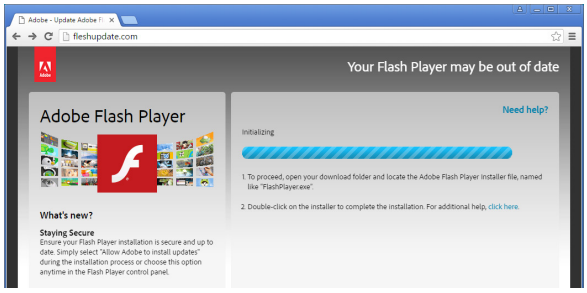
Bromium Secure Browsing isolates web-borne threats and browser exploits using hardware-enforced micro-VMs, so you don't have to rely on detection or restrictive website blacklists.

Each browser tab opens inside a unique, single-use micro-VM, isolated from all other tabs, the host PC, the internal network, sensitive files and processes. Users browse with native Chrome, Firefox, or Edge for safe sites, with risky sites automatically routed for isolated browsing in the Bromium Secure Browser, including suspected phishing links and uncategorized websites.

### Isolation stops web-borne threats

All website activity, including malicious threats, is sequestered within the secure micro-VM container. The micro-VM and any threats are destroyed when the browser tab is closed, leaving behind a rich Breachless Threat Report™ to serve as a forensic trace of all malicious activity.

Web protection extends to known and unknown vulnerabilities, including zero-day browser exploits, malicious cross-site scripting, and fileless malware that exploits memory flaws or other Windows weaknesses. Crisis patching and version checking become obsolete, as Bromium Secure Browsing makes unpatched systems even safer than patched ones that are not protected by Bromium.




*Safely isolate browser exploits and fileless malware*

### Flexibility for trusted sites and services

Bromium Secure Browsing allows for complete access outside of the micro-VM environment for trusted websites via policy—as recommended by Bromium or via your own whitelists.

Secure Browsing also protects your intranet from cross-site scripting and other vulnerabilities, allowing for network isolation against external threats while offering special protection to essential Cloud/SaaS services.

### Performance end users expect

Compared to native Windows systems that are not protected by Bromium, Bromium-protected systems have improved CPU performance, faster page file access, and increased input/output operations on Virtual Desktop Infrastructure (VDI).

Bromium's superior system resource management of background and inactive tabs is accomplished using aggressive shared memory management and automated resource scheduling from continuous learning of observed user behavior.

### Breachless Threat Intelligence™

You don't have to be breached to protect against threats. Isolated malware generates Breachless Threat Alerts™ with complete, step-by-step kill-chain analyses for SOC analysts, and sends Breachless Threat Feeds™ to external systems for automated threat hunting and information sharing.

### Secure ingress for file downloads

As part of the Bromium Secure Platform, Bromium Secure Browsing provides secure ingress from supported browsers for file downloads opened in isolation with Bromium Secure Files, on or off the network.

## Benefits

### Safely access any website

Safely open any web link and view any website without fear of website watering hole attacks, email phishing links that drop malware, or exploits that span multiple browser tabs

### Keep malware off your endpoints

Micro-VMs isolate and contain malicious activity, terminating malware when the browser tab closes, while preserving rich forensics

### Keep using your favorite browser

End users can browse with their choice of native Chrome, Firefox, or Edge for safe sites, with risky sites automatically routed for isolated browsing in the Bromium Secure Browser, including suspected phishing links and uncategorized websites.

### Ease IT strain and restrictive access controls

Eliminate the need for website blacklists, and quickly deploy flexible, granular access policies for individuals and groups

## Features

### Protect against malicious URLs and browser flaws

Bromium Secure Browsing isolates web-borne threats from the host PC and protects your endpoints from browser exploits, including zero-day browser vulnerabilities, and kernel and memory flaws

### Control over trusted websites

Protects intranet sites and cloud/SaaS services from external threats and provides flexibility to trust public URLs using web reputation

### High-performance web browsing

Supports anti-tracking and ad-blocking while improving performance over native web browsing

### Secure Browsing System Requirements

*Processor*

- Intel Core i3, i5, or i7 processors with Intel Virtualization Technology (Intel VT)
- AMD processors with Rapid Virtualization Indexing (RVI), including A4/A6/A8/A10 and Ryzen

*Memory*

- 4 GB RAM (Minimum)

*Disk*

- 6 GB Free Disk Space

*Operating System*

- Microsoft Windows 7 SP1, 32-bit or 64-bit
- Microsoft Windows 8.1 with Update 1, 64-bit
- Microsoft Windows 10 Anniversary Update, 64-bit
- Microsoft Windows 10 Creators Update, 64-bit
- Microsoft Windows 10 Fall Creators Update, 64-bit
- Microsoft Windows 10 April 2018 Update, 64-bit
- Microsoft Windows 10 October 2018 Update, 64-bit

*Secure Browsing Extension*

- Google Chrome
- Microsoft Edge
- Mozilla Firefox

*Full Browser Isolation*

- Bromium Secure Browser
- Microsoft Internet Explorer
- Mozilla Firefox

*File Download Isolation*

- Bromium Secure Browser
- Google Chrome
- Microsoft Edge
- Microsoft Internet Explorer
- Mozilla Firefox

### About Bromium

Bromium pioneered the next generation of enterprise protection by turning an enterprise's largest liability, endpoints and servers, into the best defense. Unlike detection-based techniques, Bromium automatically isolates threats and adapts to new attacks and instantly shares threat intelligence to eliminate the impact of malware.

### For more information

To learn more about Bromium's game-changing security architecture, please visit www.bromium.com.

Bromium

**Bromium, Inc.**
20883 Stevens Creek Blvd.
Suite 100
Cupertino, CA 95014
+1 408 213 5668

**Bromium UK Ltd.**
2nd Floor, Lockton House
Clarendon Road
Cambridge CB2 8FH
+44 1223 314914

**For more information**
visit Bromium.com or write to
info@bromium.com.