FULLCONTROL NETWORKS

Bromium

Bromium Secure Browsing

Stop Fighting a Losing Battle

Backlisting websites by reputation is a no-win proposition, as no vendor can possibly keep up with the volume of new malicious domains, compounded by the constant stream of new browser exploits. The industry is always playing catchup, yet still falling behind. The breaches keep coming, seemingly without end.

Change the Game with a New Approach

You need Bromium Secure Browsing, part of the Bromium Secure Platform. Bromium takes a completely different approach to web security, isolating web-borne threats and browser exploits by way of hardware-enforced micro-virtualization. Each individual browser tab is completely isolated from all other tabs, the host PC, the network, and the file system. All web browsing takes place within a protected micro-VM, completely transparent to the user, which allows for unfettered task completion in full isolation from sensitive files and processes. Bromium Secure Browsing protects users of Chrome, Internet Explorer, and Firefox.

Protection by Design Against Unknown Threats

If a website is malicious, everything it does-or attempts to do-remains sequestered within the safe micro-VM container, and any threats disappear forever as soon as the browser tab is closed. This protection extends to both known and unknown vulnerabilities, including zero-day browser exploits, malicious site scripting, and file-less malware that takes advantage of memory flaws or other Windows design weaknesses. Bromium Secure Browsing makes unpatched systems even safer than patched ones that are not being protected by Bromium.

Key Benefits

Safely access websites without risk of infection
Eliminates website watering hole attacks, protects against email phishing links that drop malware, and stops exploits that span multiple browser tabs—with granular policy-based access controls and no site blacklists to maintain

Malicious sites contained & rendered harmless
Micro-VMs isolate and contain malicious activity, while malware vanishes completely when the browser tab closes, with all threat intelligence preserved for analysis

Protection for the way your users work
Choice of 3 enterprise-class web browsers so users retain the look, feel, and productivity to match their preference

Bromium secure platform integration
Safely download web files and email attachments with Bromium Secure Files, then visualize threats and analyze malicious activity with Bromium Secure Monitoring

Key Features

Protect against malicious urls and websites
Isolates web-borne threats from the host PC or server and neutralizes browser exploits, including zero-day browser vulnerabilities

Control over trusted websites
Protects intranet sites 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

Enterprise browser support
Supports Internet Explorer, Firefox, and Google Chrome web browsers in use by the vast majority of enterprises

The Internet is a dangerous place, filled with malicious websites designed to steal your intellectual property, silently download malware onto your computer, or exploit systemic weaknesses in your web browser. Attackers aim to establish a foothold on one infected machine to compromise your network and steal payment data or critical information.

"I've worked with Bromium for more than two and half of years. It allows us to browse our internet and intranet sites securely and locate any threats."

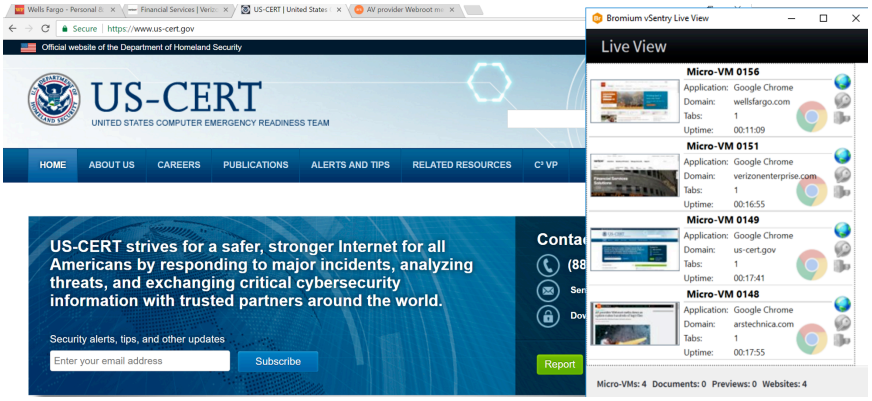
RAJU MANI, IT PROFESSIONAL,
AIRBUS DEFENCE AND SPACE

"Bromium is a great asset to protect the enterprise from the CPU layer which no other product does. We protect internet browsing, email attachments, and are looking at USB protection as well."

IT SYSTEMS ANALYST, GLOBAL 500 BANKING COMPANY

Flexibility for Trusted Sites

For trusted websites-whether recommended by Bromium or via your own whitelists-Bromium Secure Browsing allows for complete access outside of the micro-VM environment at the choice of your administrator, thereby minimizing system resources. Bromium Secure Browsing also protects your intranet for safe access over the web against cross-site scripting and other vulnerabilities, allowing for network isolation against external threats while offering special protection to Cloud/SaaS sites that are so essential to business today.



Improve Performance over Native Systems

Bromium-protected systems actually improve their resource utilization over native Windows systems that are not protected by Bromium across a range of important metrics, including: Improved CPU performance, faster page file access, and increased input/output operations on Virtual Desktop Infrastructure. Bromium's superior system resource management of background and inactive tabs is accomplished by way of automated resource scheduling from continuous learning of observed user behavior.

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

Web Browser

- Internet Explorer
- Mozilla Firefox
- Google Chrome

Empower Your Users, Don't Block Them

While web filtering still has a role in enterprise security—it can effectively restrict user access to non-business content (social media, gambling, or adult sites) and blacklist known bad sites—Bromium believes that users should have full access to the Internet for all legitimate business uses without the need to worry about malicious activity on the web or newly discovered browser exploits.

Despite increased training and awareness, users continue to click unwisely on links, whether through search or via email phishing URLs. Human behavior is deeply ingrained and very difficult to change. Rest assured that all of their browsing activity will be safely contained within micro-VM containers, away from their physical computers and any enterprise resources. Bromium users can safely click on anything without a second thought, as Bromium Secure Browsing covers the full range of web threats.

About Bromium

Bromium pioneered the next generation of enterprise protection by turning an enterprise's largest liability, endpoints and servers, into the best defense. We use a combination of our patented hardware-enforced containerization to deliver application isolation and control, and a distributed Sensor Network to protect across all major threat vectors and attack types.

Unlike detection-based techniques, Bromium automatically isolates threats and adapts to new attacks and instantly shares threat intelligence to eliminate the impact of malware. Our technological innovations have earned the company numerous industry awards. Bromium counts a rapidly growing set of Fortune 500 companies and government agencies as customers.

For more information

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

ABOUT BROMIUM

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can't stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—transforming the traditional security life cycle.

[1] TechValidate. TVID: D69-FFC-352

Bromium, Inc.
20813 Stevens Creek Blvd
Cupertino, CA 95014
info@bromium.com
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information refer to www.bromium.com
or contact mkt@bromium.com

WP.Kernel-Exploit-Trends.US-EN.1704