FULLCONTROL NETWORKS

Bromium

Bromium Secure Files

Today's enterprises are constantly bombarded with malicious files—ransomware, keystroke loggers, remote access Trojans, and more—all designed to hold your data hostage or steal your intellectual property or proprietary information. Attackers use multiple attack vectors—including web, email, and USB—to gain a foothold on one PC with the aim of compromising your network, spying on users, or stealing critical information.

Detection is Futile and Ineffective

The security industry is continuously playing catch-up against adversaries that overwhelm defenses by sheer file numbers and variations. Detection rates remain low and file-based breaches are getting larger and more frequent.

A New Approach

You need Bromium Secure Files, part of the Bromium Secure Platform. Bromium takes a completely different approach to file security, isolating file-borne threats and associated system and kernel exploits by way of hardware-enforced micro-virtualization. Each individual file that is opened is completely isolated from the host PC, the network, and the file system.

All file activity takes place within a protected micro-VM, transparent to the user, which allows for unfettered task completion in full isolation from sensitive files and processes. Bromium Secure Files works on its own and in conjunction with Bromium Secure Browsing and Bromium Secure Monitoring, to provide a complete protection and visibility solution.

Protection by Design Against Unknown Threats

If a file is malicious, everything it does—or attempts to do—remains sequestered within the safe container, and any threats disappear forever as soon as the file is closed. This protection extends to both known and unknown vulnerabilities, including zero-day exploits, malicious macros, scripts, and advanced attack techniques that take advantage of memory kernel bugs or other Windows design weaknesses.

Key Benefits

Safely access files from any inbound source
Open any file or document without risk of infection, whether downloaded from the Internet, received in email phishing attachments, or attached via portable USB drives

Malware is contained and rendered harmless
Micro-VMs isolate and contain malicious activity, while malware vanishes completely when the file or document closes, with all threat intelligence preserved for analysis

Simplified deployment and management
Flexible policies for individuals and groups with no file blacklists to maintain granular policy-based access controls

Bromium secure platform integration
Safely browse the web with Bromium Secure Browsing as security operations teams visualize threats and analyze malicious activity with Bromium Secure Monitoring

Key Features

Protect against malicious files
Isolates untrusted files from the host PC, tracks suspicious activity, and performs attack visualization and analysis

Ingress application and email protection
Saved and downloaded files from untrusted ingress sources—web, email, or USB—are isolated in micro-VMs when opened in their applications for secure access

Secure editing and printing
Safely interact with files in the usual ways—edit, copy, and print documents securely within isolated micro-VMs

Granular policy controls
Custom policies support file-type matching and perform background security checks before allowing file trusting

"Bromium micro-virtualization is the most significant advance in information and infrastructure security in decades."

BOB BIGMAN, FORMER CISO, CIA

"It is clear that the industry is failing in its primary goal of keeping malicious code off PCs."

GARTNER MAGIC QUADRANT
FOR ENDPOINT PROTECTION Q1, 2015

Interact with Files in the Usual Expected Ways

Even though each untrusted file opens within a secure micro-VM, users still have full access to do their jobs—they can read, edit, save, copy, and perform other file actions based on your administrative settings—safe in the knowledge that no malicious activity can ever reach the host PC, the file system, or network resources.

Full Threat Intelligence and Kill-Chain Analysis

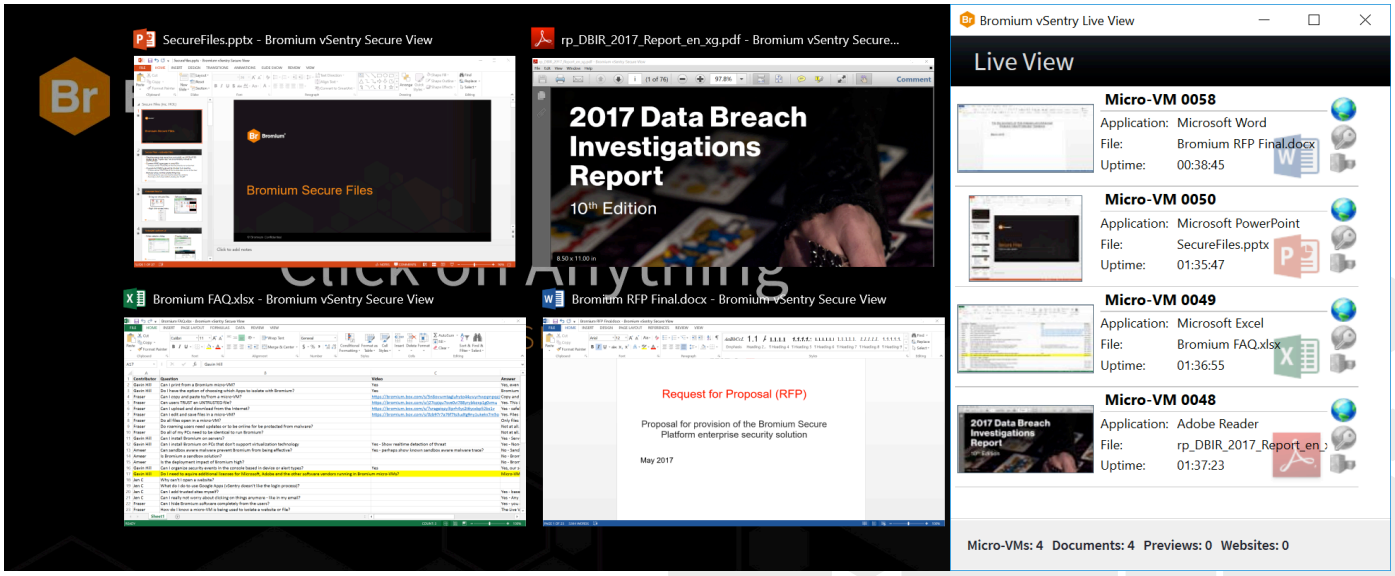
Administrators gain full threat intelligence and complete, step-by-step kill-chain analysis via the Bromium Controller's behavioral threat graph.

Policy-Based Access Enforcement

Bromium Secure Files includes a robust policy engine that permits administrators to tailor the level of file access by user, business unit or group, file source, file type, and much more. Policy control is very granular. Policies can be layered, where higher-level policies supersede lower-level policies, providing fine-tuned control appropriate to every situational context.

Flexibility for Trusted Files and Sources

For trusted files—those that have been created by the user or downloaded from trusted websites—Bromium Secure Files allows for complete access outside of the micro-VM environment your administrator's discretion.



BROMIUM SECURE FILES PROTECTS AGAINST MALWARE ON MULTIPLE FILE ATTACK VECTORS

Safely Access Files Originating from Any Source

While there is still a place for network and endpoint antimalware—to screen out known bad files—Bromium believes that users should have full access to files without worrying about triggering malware on their systems. Traditional solutions are notoriously poor at stopping zero-day threats once files slip past the filters and are opened by users on their endpoints.

Despite repeated training, users still download web files, open email attachments, and connect external USB drives with hardly a thought to security. Human behavior is deeply ingrained and difficult to change. Enterprises can be confident that all of their file-based activity will be safely contained within micro-VM containers, away from physical computers and enterprise resources. Bromium users can safely click on any files without a second thought, as Bromium Secure Files has them covered!

About Bromium

Bromium pioneered the next generation of enterprise protection by turning an enterprises 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.

Secure Files 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

Applications for Secure Files

- Microsoft Office 2010 and Above
- Adobe Acrobat 9 and Above

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®

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