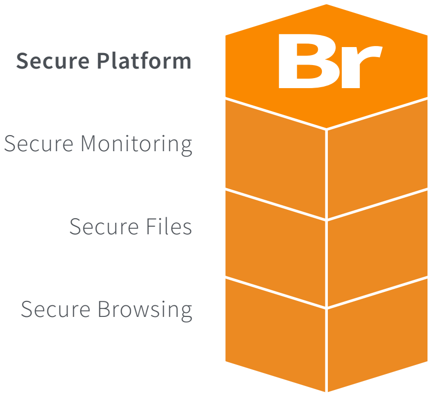
Datasheet

> *“The rise of the targeted attack is shredding what is left of the anti-malware market’s stubborn commitment to reactive protection techniques.”*
>
> GARTNER MAGIC QUADRANT
> FOR ENDPOINT PROTECTION Q1, 2015

Bromium Secure Platform

Bromium uses virtualization-based security and isolation technology to dramatically decrease attack surfaces, monitor suspicious activity, and contain threats online or offline inside of micro virtual machines in an easy to deploy and quick time-to-value platform. Each Bromium protected endpoint and server is part of a sensor network that performs threat analysis and instantly shares indicators of compromise with the rest of the network for faster time to resolution. Security Operations Center teams can access detailed forensics with full kill-chain analysis and visualization garnered from each micro-VM, for enterprise-wide visibility and control.



The Bromium Secure Platform is an advanced security solution that delivers enterprise protection and visibility with minimal user impact and low resource overhead, isolating host-based threats.

Bromium’s unique, patented hardware-enforced isolation technology leverages native virtualization-based security functions in Intel and AMD CPUs to protect against external threats for protected applications like Office documents and PDFs.

Monitoring of the user execution space detects and responds to malicious activity on the host for persistent or insider threats on endpoints and servers, delivering full visibility to SOC analysts.

The Bromium Secure Platform consists of three components: Bromium Secure Browsing, Bromium Secure Files, and Bromium Secure Monitoring.

“Bromium protects by design, allowing undetectable attacks to be automatically defeated.”

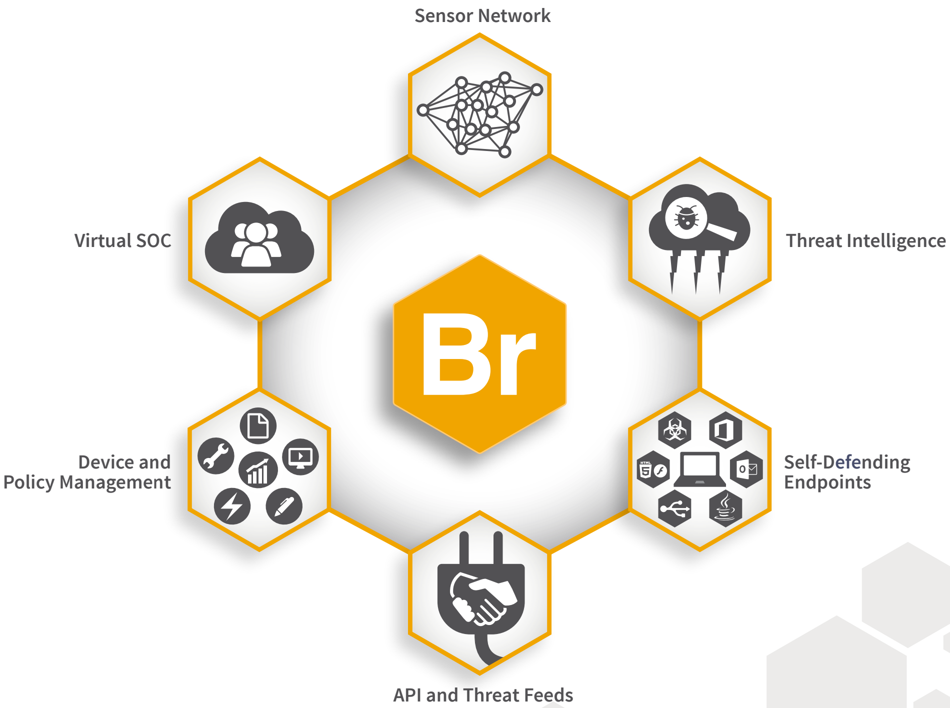
BOB BIGMAN, FORMER CISO, CIA

Bromium Secure Browsing

Bromium protects organizations from web-borne threats with Bromium Secure Browsing for Internet Explorer, Chrome, and Firefox. Each browser tab runs in its own secure container, completely isolating web threats from the host so that they have no place to go. When the browser tab is closed, the threat is terminated along with the micro-VM. The full kill chain is sent to the Bromium Threat Cloud and shared with all other protected devices via the Bromium Sensor Network.

Bromium Secure Files

Malicious documents are steadily gaining in popularity with threat actors due to their effectiveness. Ransomware is commonly delivered via malicious office documents or PDFs. Bromium Secure Files hardware-isolates each supported document from the operating system and the kernel. If a malicious document is saved via an ingress application—such as Skype, email, or USB—it is hardware-isolated in a micro-VM. When the document is closed, the threat is terminated along with the micro-VM. The full kill chain is sent to the Bromium Threat Cloud and shared with all other Bromium devices via the Bromium Sensor Network.



Bromium Secure Monitoring

Bromium Secure Monitoring helps organizations detect and respond to persistent threats already on the network by monitoring the user execution space for malicious activity. Malicious files can be quarantined and automatically removed from all network locations based on blacklist policy settings.

Within the Bromium Sensor Network, high-fidelity alerts are sent to the Bromium Threat Cloud whenever malicious behavior is found on any protected host. SOC analysts can use Bromium threat intelligence to quickly catalog and search for indicators of compromise and indicators of attack. Secure Monitoring supports endpoints and servers.

Protection and Visibility Use Cases

- Phishing emails for malware
- Drive-by download
- Watering hole attacks
- Malvertising
- Ransomware
- Macro-enabled Trojans
- File-less malware (e.g. PowerShell)
- Persistent malware
- Insider threats
- Kill-chain analysis
- Malware forensics
- Incident response
- IOC and IOA analysis
- Automated quarantine and blacklisting

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.

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