Bromium

Bromium Secure Monitoring

Security teams need real-time endpoint visibility to ensure overall enterprise security. Bromium Secure Monitoring, part of the Bromium Secure Platform, delivers real-time alerts with complete forensic intelligence for each attack. It delivers key features to the enterprise that turn the tables on attackers and eliminate breaches.

Key Benefits

Complete attack visibility

Enterprise-wide visibility, directly at the point of attack, ensuring that the security team maintains complete situational awareness of the global threat environment

Comprehensive protection

Complete, integrated threat protection and visibility with Bromium Secure Files and Bromium Secure Browsing

Reduced total cost of ownership

No need for large backend server infrastructure for data analysis, reducing significant CapEx and OpEx spending

Key Features

Real time monitoring

Monitoring and alerting of attacks in progress in real time with live data streaming

Application flow analysis

Correlates low-level device monitoring data to create an Application Flow graph for actionable threat intelligence and confidence against false negatives and false positives

Threat data auditing

Audit / Query historical threat data from Bromium or third-party systems for post-attack discovery of new IOCs / IOAs

"Containerization dramatically reduces the footprint that an attacker can leverage to try and take advantage of a vulnerability within your environment."

ERIC OUELLET, GARTNER ANALYST,
AT THE 2016 GARTNER SECURITY SUMMIT

Comprehensive Monitoring and Analysis

Bromium Secure Monitoring can be deployed on all endpoints and servers in enterprises with diverse hardware and software configurations, providing complete visibility into the organization's security status.

Real-time streaming of attack data with Application Flow analysis provides SOC analysts with a complete, integrated view of the attack. The Bromium agent correlates thousands of low-level monitoring events in real time at the endpoint or server, eliminating the need for time-consuming manual analysis or expensive back-end data centers. It provides tools to transform raw data into higher-level intelligence, ensuring that security teams maintain real-time awareness of the overall threat posture at all times.

Secure Platform Integration and Customization

Bromium Secure Monitoring integrates with Bromium Secure Files and Bromium Secure Browsing for unmatched protection and visibility.

Administrators can customize the threat model, allowing enterprises or government agencies to specify custom rules to flag malicious behavior. This threat model is applied in real time to the Application Flow to identify active malware.

"I absolutely would recommend Bromium, because it is one of the few security products on the market that you can rely on to be effective 100% of the time."

PAUL HERSHBERGER,
DIRECTOR SECURITY RISK AND COMPLIANCE, MOSAIC

Reduced Total Cost of Ownership

The solution does not require a large backend server infrastructure for data analysis, eliminating significant CapEx & OpEx spending by performing detection and analysis on the endpoint itself.

Blacklisting and Automatic Blocking – Enterprise wide IOC detection stops lateral movement via behavioral-based rules & configurable blacklists.

File Quarantine – Removes malicious binaries from infected machines with no user disruption.

Custom Monitoring Rules – Advanced rule configuration, including per-application exclusions and registry path aliases, is easy and allows you to add extra monitoring for your most valuable data assets or the specific threat vectors attacking you.

Advanced Threat Intelligence – Export formats include pre-configured STIX or MAEC reports for standardized data interchange with third-party stakeholders, MD5 signatures of file-based malware droppers, and complete command-and-control channel details for SIEM/SOC integration.

Remote Enterprise Monitoring – Administrators can monitor both physical and virtual systems with full support for VDI and server farms from VMware and Citrix.

Detect and Monitor Malicious Activity on Hosts

- Real time detection of threats
- Attack visualization and analysis

Search for Indicators of Attack and Compromise

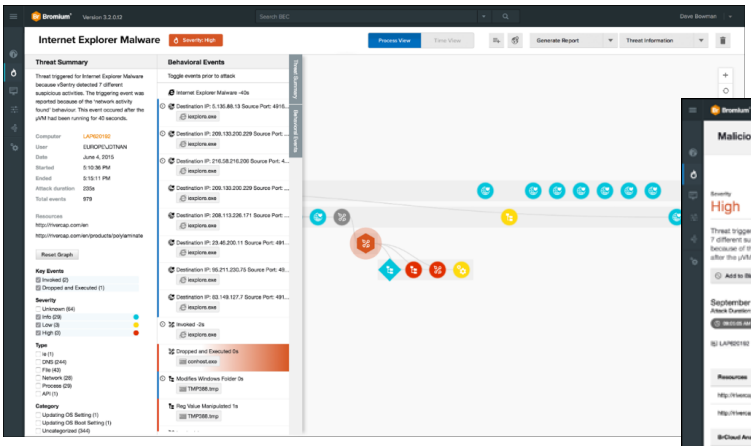
- Enterprise-wide across fixed and mobile PCs
- Covers offline and online endpoints

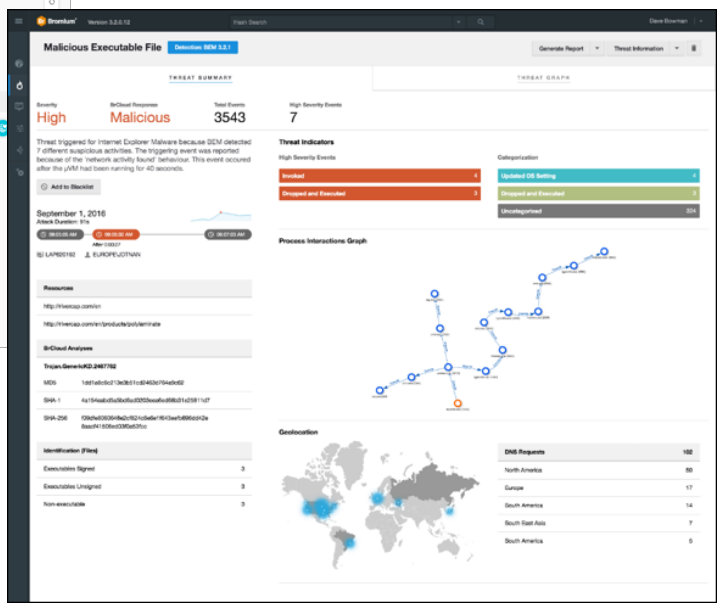
Enterprise Wide Visibility

- Monitors Windows endpoints and servers
- Includes legacy operating systems & hardware

Low TCO and Easy to Deploy

- No hardware dependency, uses existing assets
- Monitoring only, non-intrusive to end users





Endpoint/Server Agent Requirements

Processor

- Intel or AMD

Memory

- 2 GB RAM (Minimum)

Disk

- 6 GB Free Disk Space

Operating System

- Microsoft Windows 7, 8 or 10

Bromium Controller Requirements

Operating System

- Windows Server 2008 R2 SP1
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

Database

- SQL Server 2008 R2 or Later

Web Browser

- Internet Explorer 10 or Later
- Mozilla Firefox
- Google Chrome
- Microsoft Edge

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®

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