Bromium®

DATA SHEET

BROMIUM SECURE MONITORING

Comprehensive Monitoring and Analysis

Bromium Secure Monitoring delivers real-time alerts with complete forensic intelligence for each attack, providing true endpoint visibility to security teams. Bromium Secure Monitoring provides complete security visibility when deployed across Windows endpoints and servers enterprise-wide.

Live streaming of attack data with application flow analysis provides SOC analysts with a complete, integrated view of the attack. Bromium 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 backend data centers. Bromium transforms raw data into higher-level intelligence, ensuring that security teams maintain situational awareness of the overall threat posture.

Secure Platform integration

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 and 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.

Reduce total cost of ownership

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

Blacklisting and automatic blocking – Stop lateral movement via behavioral-based rules and configurable blacklists with enterprise-wide IOC detection.

File quarantine – Remove malicious documents and executables from infected machines with no user disruption.

Custom monitoring rules – Simplify advanced rule configuration, including per-application exclusions and registry path aliases and allow administrators to add extra monitoring for your most valuable data assets or specific threat vectors.

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 – 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

Benefits

Complete attack visibility

Enterprise-wide visibility, directly at the point of attack, ensures that SOC teams maintain complete situational awareness of the global threat landscape

Reduce costs

No need for large backend server infrastructure for data analysis, reducing capital and operational expenditures

Comprehensive protection

Integrated threat protection and visibility with Bromium Secure Files and Bromium Secure Browsing

Features

Real-time monitoring

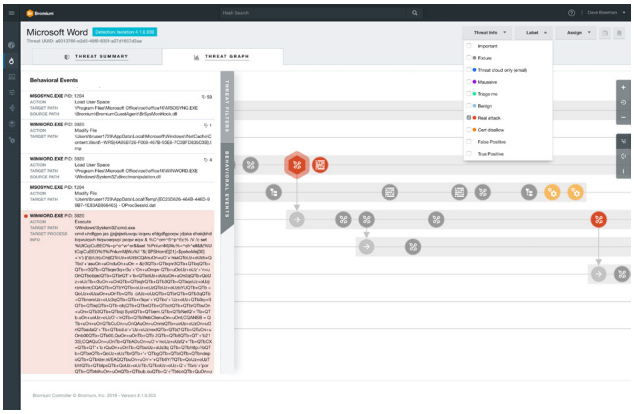
Monitoring and alerting of attacks in progress in real time with live data streaming to SOC teams

Application flow analysis

Application Flow graph correlates low-level device monitoring data for actionable threat intelligence and confidence against false negatives and false positives

Threat data auditing

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



Endpoint / Server Agent Requirements

Processor

- Intel or AMD

Memory

- 2 GB RAM (Minimum)

Disk

- 6 GB Free Disk Space

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 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.

Copyright ©2018 Bromium, Inc. All rights reserved. 06142018