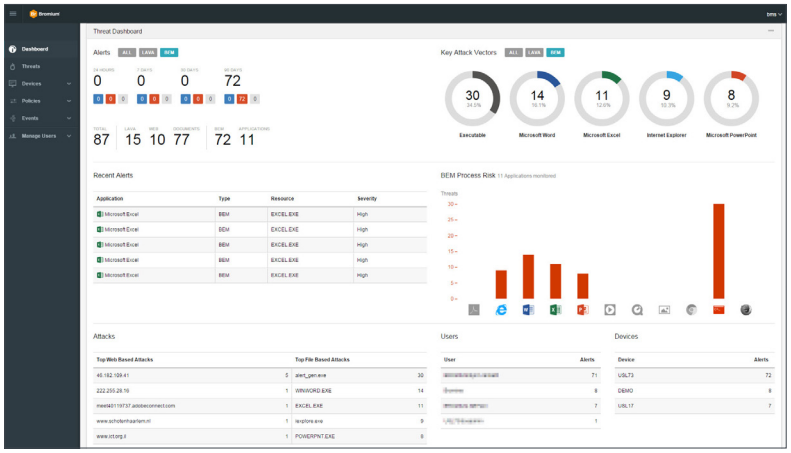
Bromium Endpoint Monitoring

Real-Time Detection and Monitoring of Threat Activity

Security teams need real-time visibility of the endpoint to ensure the overall security of the enterprise. Bromium Endpoint Monitoring, a component of Bromium Advanced Endpoint Security delivers real-time alerts with comprehensive forensic intelligence for each attack. Bromium Endpoint Monitoring delivers key features to the enterprise that wants to turn the tables on attackers and eliminate breaches.

Comprehensive monitoring and analysis

- Bromium Endpoint Monitoring is a lightweight monitoring agent that can be deployed on all endpoints and servers in enterprises with diverse hardware and software configurations, providing complete visibility into endpoint security status.
- Real-time streaming of attack data with Application Flow analysis provides SOC analysts with a complete, integrated view of the attack tying together thousands of low-level monitoring events in real time thereby eliminating the need for time-consuming manual analysis.



Key Benefits

COMPLETE ATTACK VISIBILITY

Bromium Endpoint Monitoring offers complete visibility across the enterprise, directly at the point of attack ensuring the security team maintains complete situational awareness of the global threat environment within the organization at all times

COMPREHENSIVE PROTECTION

In combination with Bromium Endpoint Protection, Bromium Endpoint Monitoring provides advanced, complete, integrated endpoint security

REDUCED TCO

Bromium Endpoint Monitoring doesn't require large backend server infrastructure for data analysis reducing significant Capex and Opex spend

Key Features

REAL TIME MONITORING

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

APPLICATION FLOW ANALYSIS

Correlates the low-level monitoring data collected from the device to create an Application Flow graph for actionable threat intelligence and reduced false negatives and false positives

THREAT DATA AUDITING

Provides the ability to audit or query historical threat data collected by Bromium or third-party systems to enable post-attack discovery of new indicators of attack

Bromium®

Supported Platforms

ENDPOINT HARDWARE

Intel or AMD
2GB RAM

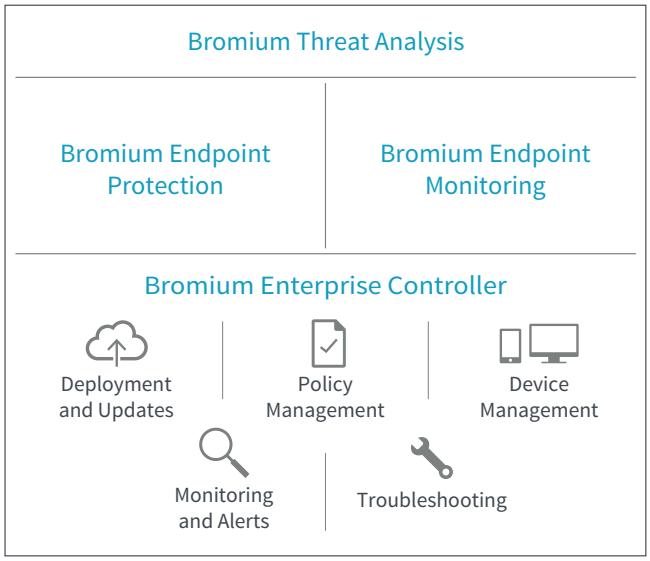
OPERATING SYSTEM

Microsoft Windows 7, 8.1, 10

About Bromium

Bromium has pioneered the next generation of endpoint protection that eliminates breaches. Just as virtualization transformed IT, Bromium is transforming security with its unique micro-virtualization technology. Bromium provides the world's most advanced endpoint security, even against the most sophisticated zero-day malware. Unlike traditional security technologies, such as antivirus or virtual containers, which rely on ineffective detection techniques, Bromium's solution automatically isolates each user-task in a lightweight, CPU-enforced micro-VM. This enables users to click on anything without risk of compromise, protecting the enterprise. Bromium's technological innovations have earned the company numerous industry awards. Bromium counts a rapidly growing set of Fortune 500 companies and government agencies as customers. Visit us at www.bromium.com.

- A wealth of tools transform raw data into higher-level intelligence ensuring that the security team maintains real-time awareness of the global threat posture of the organization at all times.
- Bromium Endpoint Monitoring fully integrates with Bromium Endpoint Protection to provide unmatched protection and visibility both inside and outside the micro-VM.
- Bromium Endpoint Monitoring allows customization of the threat model where large enterprises or government agencies can specify custom rules to flag malicious behavior. This threat model is applied in real time to the Application Flow to identify malware.
- Bromium Endpoint Monitoring doesn't require customers to set up large backend server infrastructure for data analysis. Bromium Endpoint Monitoring eliminates significant capex and opex spend by performing detection and analysis on the endpoint itself.
- Advanced Threat Intelligence export capabilities 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 integration with existing cyber defense and enforcement solutions.
- Monitor both physical and virtual systems with full support for VDI and server farms from VMware and Citrix.



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 go to www.bromium.com
or contact sales@bromium.com

DS.BromiumEndpointMonitoring.US-EN.1602