Solution Brief

Key Benefits

Prevent Endpoint Attacks

Prevent attacks from targeting enterprise endpoints through web, email or USB, even off the corporate network, without signatures or cloud updates.

Reduce Security Ops Costs

Automated real-time threat intelligence for attacks targeting end users with actionable attack kill chain visualization.

Identify Compromised Assets

Leverage threat intelligence to identify compromised assets within the enterprise.

Automatically Remediate Endpoints

Automated removal of used to attack endpoints and lower IT operations costs.

Automatically Tune Perimeter Defenses

Automated configuration of perimeter defenses based on real-time intelligence of new attacks extends protection to the global organization.

The Bromium - LogRhythm Integrated Solution

The Challenge

Blocking Advanced Attacks

Preventing attacks from targeting enterprise endpoints through everyday use of web, email and removable media. Traveling users are especially at risk as they are not protected by network security.

Real-time threat intelligence

Identifying advanced attacks and compromised systems. Most threats exist undetected in corporate networks for weeks or months. Enterprises need real time threat intelligence on attacks targeting their endpoints. Security teams need to locate and analyze the attack, block it then remove it. Existing endpoint technologies provide no such real time insights to the security team.

Risk Assessment & Mitigation

Enterprises need to identify existing assets which may be compromised by attackers and remediate them. Current security and management infrastructure doesn't provide an automated mechanism to perform this analysis.

Bromium and LogRhythm – Protecting the Enterprise

The joint solution allows organizations to automatically isolate and defeat advanced malware and gather accurate, actionable threat intelligence in real-time. Bromium vSentry, installed on the endpoint, uses hardware level isolation to defeat attacks against enterprise desktops. Bromium Live Attack Visualization and Analysis (LAVA) identifies attacks without the need for signatures and provides real-time, actionable intelligence.

The solution protects the enterprise from unknown malware, which is undetectable through traditional security layers, thereby eliminating the risk of a security compromise at the endpoint from key attacks vectors – web, email and USB. Cost of remediation and incidence response for endpoint infections is drastically reduced. The solution enables the security and IT team to empower users with unrestricted access to the web, increasing productivity while drastically reducing risks.

Bromium®

About Bromium

Bromium is transforming enterprise security with its powerful new technology, microvirtualization, which was designed to protect businesses from advanced malware, while simultaneously empowering users and delivering unmatched threat intelligence to IT.

Bromium's technological innovations have earned the company numerous industry awards, including being named as a CNBC Disruptor and a Gartner Cool Vendor for 2013. Bromium's rapidly growing customer base includes leaders in the Fortune 1000 companies and the largest government agencies.

About LogRhythm

LogRhythm is the largest and fastest growing independent security intelligence company in the world. The company's patented and award-winning Security Intelligence Platform, unifying SIEM, log management, file integrity monitoring, network forensics and host forensics, empowers organizations around the globe to detect and respond to breaches and the most sophisticated cyber threats of today, faster and with greater accuracy than ever before. LogRhythm also provides unparalleled compliance automation and assurance as well as IT predictive intelligence to Global 2000 organizations, government agencies and mid-sized businesses worldwide.

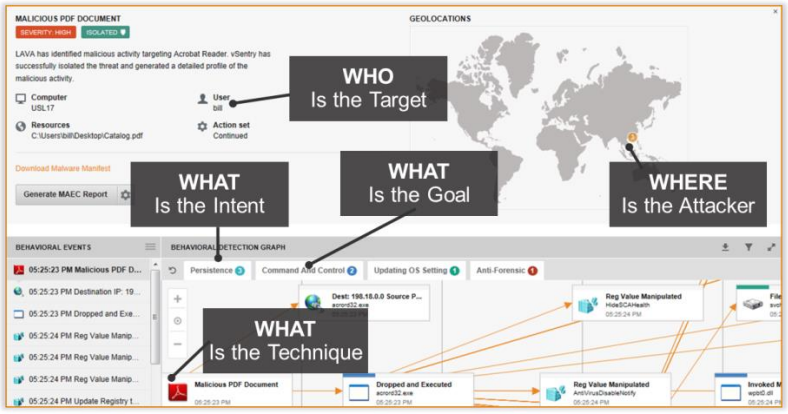
How it works

LogRhythm's Security Intelligence Platform identifies and prioritizes advanced security threats by integrating and correlating real-time threat information from Bromium LAVA with log, flow, event and other machine data collected and generated by LogRhythm from across the network environment. LogRhythm's advanced security analytics allows customers to get greater value out of their current investment by allowing them to model malware behavior based on Bromium telemetry and leverage those insights to identify other compromised hosts in their environments.

LogRhythm's Security Intelligence platform can take automated actions based on threats identified with Bromium such as:

- Adding threat intelligence to internal watch lists or black lists,
- Disabling active sessions with source IPs known to be bad
- Quarantining compromised hosts.

The combined solution helps security operations teams prioritize actions, slash response times and adjust defenses to counter today's most severe threats.



Bromium Enterprise Controller

"At a glance" visualization of attacks with automatic threat categorization. Detailed STIX/MAEC reporting, Malware Capture for detailed analysis

LogRhythm Security Intelligence Platform

Global integration and correlation of threats Automated response capabilities Advanced data visualization. Intelligent prioritization of high risk events.

Bromium HQ
20813 Stevens Creek Blvd, Suite 150
Cupertino, CA 95014
info@bromium.com

Bromium UK Ltd
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44 1223 314914

For more information refer to www.bromium.com, contact sales@bromium.com or call at 1-800-518-0845.