Bromium®

SOLUTION BRIEF

THREAT INTELLIGENCE AND ANALYSIS

- Minimize threat alert triage time with improved malicious determination accuracy
- Gain insights into threats stopped by Bromium
- Improve your security posture with global threat sharing

Threat Intelligence and Analysis

Bromium Secure Platform provides unique insights into threats that bypass traditional detection-based enterprise security solutions. Bromium-protected endpoints are not impacted by these threats that typically arrive as email attachments, downloaded files or links that direct the user to a malicious site. Bromium isolates malware inside a virtual machine before it has a chance to infect the PC or move laterally onto the corporate network.

The Threat Intelligence and Analysis program allows customers to share their threat data with Bromium, and is open to all customers at no extra cost. The Bromium analysis team reviews the threats and provides additional insights into the malware. Sharing threat data with Bromium improves our collective understanding of the current threatscape to get ahead of attackers.

The benefits of the Threat Intelligence Sharing and Analysis program include:

- Insights into global attack trends specific to your organization and industry
- Improved accuracy of high-fidelity security alerts and triage techniques
- Better preparedness and improved security for all Bromium customers

The Value of Sharing Threat Data

When you receive a Bromium isolation alert, it is important to remember that not only is the endpoint still protected through our hardware-enforced isolation, but the valuable threat intelligence is shared through standard feeds with other security systems, helping to protect enterprise assets that are not secured by Bromium.

Deep Insights: Alerts are reviewed and triaged by our analysts to provide your organization with additional insights about most recent threats

Reporting: Bromium analysts regularly report important insights on threats that played out in isolation using multiple outreach vehicles:

- **Technical blogs**: broad coverage of the most notable recent threats.
- **Bromium Threat Insights Report** is published on a regular basis to share what we learned about unique threats that are targeting organizations all over the world
- **Personalized Threat Insights Report** (coming soon) – a new feature that gives our customers the ability to generate their own, unique reports directly from their Bromium Controller

High-Fidelity Alerts: By analyzing threat data across multiple customer verticals, Bromium can reduce false positives and generate more detailed, actionable alerts.

Join the Threat Sharing Program

Bromium threat alerts can be automatically sent to Bromium via Threat Forwarding. When your Controller receives a threat alert in response to suspicious activity on the endpoints, the threat alert and encrypted malware payload can automatically be uploaded to the Bromium Threat Intelligence Services. Once the threat is received by the Bromium Threat Intelligence Service, we use behavioral analysis to classify threats based on interactions between events contained within the threat file to determine true positive patterns.

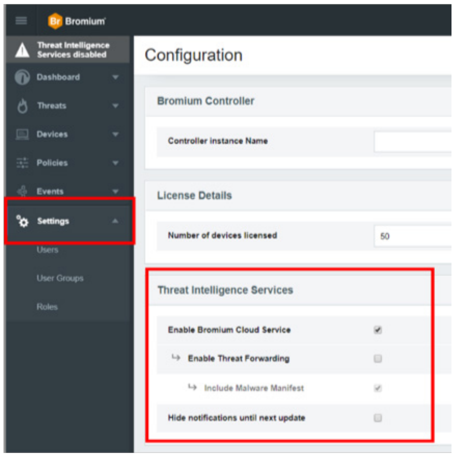
Bromium alert analysis relies heavily on data from threats that our security experts have captured and dissected, including threats that were shared with us by our customers.

The data shared with Bromium is a one-to-one copy of the threat alert that is received by your Controller, and may include the following:

- The name of the device on which the threat alert was triggered
- The filename of the suspicious file(s) that caused the threat alert to be created
- An encrypted copy of the suspicious file(s) that caused the threat alert to be created (known as the "Malware Manifest").

Neither source files nor specific threat indicators are ever shared with other Bromium customers or with third parties. Bromium will process threats in accordance with Bromum's privacy policy set forth at: https://www.bromium.com/privacy-policy/

To enable Threat Forwarding in your Bromium Controller under **Settings**, select **Enable Threat Forwarding**.



Configuration

Bromium Controller

Controller instance Name

License Details

Number of devices licensed: 50

Threat Intelligence Services

- Enable Bromium Cloud Service ☑
- ↳ Enable Threat Forwarding □
- ↳ Include Malware Manifest ☑
- Hide notifications until next update □

We look forward to expanding our community of active contributors! Together, we can improve security and make cyberspace safer for everyone.

Bromium

Bromium, Inc.
20883 Stevens Creek Blvd.
Suite 100
Cupertino, CA 95014
+1.408.213.5668

Bromium UK Ltd.
Lockton House
2nd Floor, Clarendon Road
Cambridge CB2 8FH
+44.1223.314914

For more information
visit Bromium.com or write to
info@bromium.com.