Bromium Overview

Enterprise cyber resilience for those serious about security.

Updated September 2016

"The rise of the targeted attack is shredding what is left of the anti-malware market's stubborn commitment to reactive protection techniques."

Gartner

Bromium®

"Bromium eliminates malware completely, reducing the need for reimaging and patching."

VALSPAR'S CHIEF SECURITY OFFICER

"Bromium protects by design: allowing undetectable attacks to be automatically defeated."

BOB BIGMAN, FORMER CISO,
CENTRAL INTELLIGENCE AGENCY

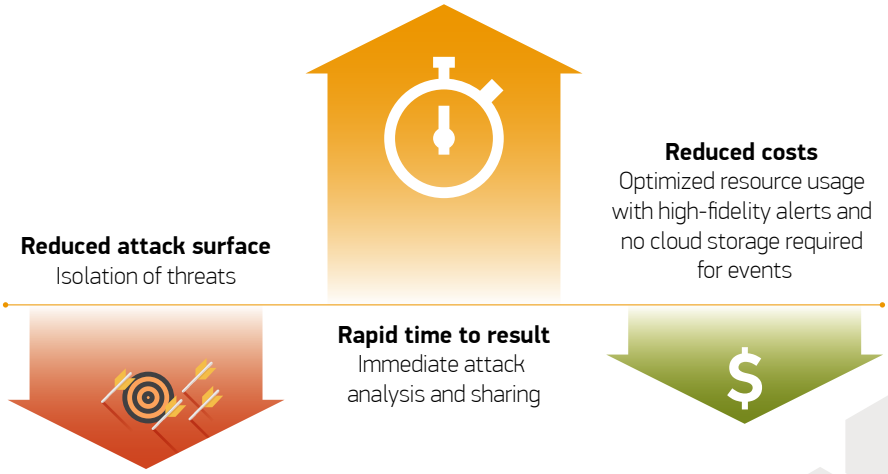
You can't afford to be patient zero. We're here to help. Even though the threatscape has evolved over the last 20 years, most security today goes about trying to protect organizations the same way they have for last two decades by relying on pre-breach detection methods.

In research published by BTIG[1], most security vendors are referred to as "clones" all doing the same thing in an attempt to address the ever-changing threatscape. They explain:

- "Detect to protect" doesn't work
- 97% of malware is unique to specific endpoints
- Machine timescale attacks are faster than humans and threats are invisible
- Average time to detect 229 days
- Your business is exposed

Why Bromium?

We help protect your data, your people and your brand. No malware escape has ever been reported by Bromium customers. Unlike most security technologies that rely on detect-to-protect methods, Bromium stops threats with virtualization-based security. By using a combination of our Sensor Network, for Endpoint Detection and Response (EDR), and patented isolation technology, we deliver high-fidelity alerts based on full kill chain analysis. We then correlate that information with all hosts to accelerate a network-wide response. And, we provide tamper-proof introspection of protected hosts.



© Bromium, Inc. 2016

How We Do It

"The Bromium approach leverages our existing investments in endpoint and network security, providing unambiguous and actionable threat intelligence that we can use to quickly and systematically enhance our overall security posture."

KEN PFEIL, CISO PIONEER INVESTMENTS

The Bromium platform uses patented virtualization-based isolation technology to dramatically decrease attack surfaces and contain threats so that hosts defend themselves when they are on or offline. Every endpoint protected by Bromium becomes a vital part of the Sensor Network. It performs threat analysis and instantly shares indicators of compromise (IOCs) with the rest of the network for faster time to resolution.

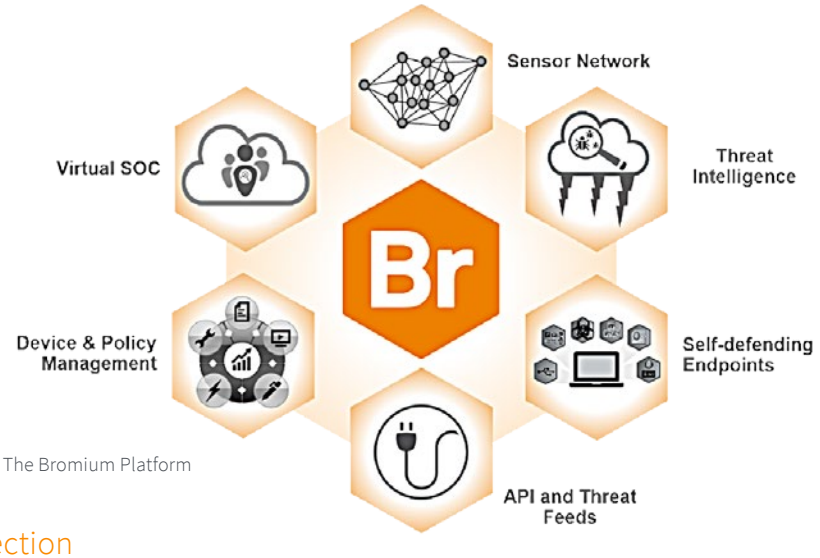


Figure 1: The Bromium Platform

Protection

- Hardware-enforced isolation stops zero-day and unknown threats without the need for signatures
- Threats are completely isolated and allowed to execute so we can fully trace the kill chain resulting in no false positives, no remediation required, and no dwell time. When the task is closed the micro-VM is destroyed along with the threat

"Bromium is game-changing technology for the enterprise."

JIM ROUTH (CISO) AETNA

"On an endpoint you can micro-virtualize applications, getting them to run individually in their own little containers, and the attacker can try to fight its way out but nothing is ever persistent."

ERIC OUELLET @ 2016 GARTNER SECURITY SUMMIT

Visibility

- Combined CPU power across all enterprise endpoints is harnessed to create a Sensor Network so that only high fidelity alerts investigated resulting in faster time to resolution and fewer alerts
- Detailed forensic trace of malicious execution is instantly available to automatically search enterprise-wide for evidence related to the detected attack to stop east-west movement

© Bromium, Inc. 2016

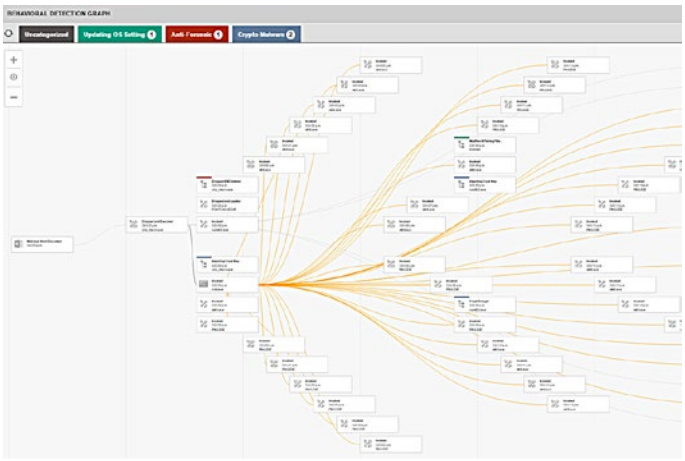


Figure 2: Kill chain trace of ransomware

Efficiency

- Stop worrying about rapid patch releases for new vulnerabilities because new threats taking advantage of the vulnerability execute in a secure enclave and cannot be used to infect the host or breach the network
- Set a regular patch schedule because emergency patching no longer needed
- IOCs are automatically hunted based on the intelligence from the Sensor Network that delivers high fidelity alerts
- Less time and fewer resources are required to triage action alerts which dramatically increases employee efficiency and requires a smaller team to respond

ABOUT BROMIUM

Bromium has pioneered the next generation of enterprise protection by turning an enterprise's largest liability, endpoints and servers, into the best defense. Just as virtualization transformed IT, we are transforming security with our unique virtualization-based isolation technology. We provide the world's most advanced security, even against the most sophisticated zero-day malware. Unlike traditional security technologies, such as antivirus or sandboxing, which rely on ineffective detection techniques, our solution automatically isolates each user-task in a lightweight micro-VM. 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.

[1]Fishbein, Joel P., Jr., Edward Parker, and Abhinav Kapur. *Cyber Security 2016 and Beyond: Playing the Game of Clones.* Report. BTIG, 2016.

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

Copyright ©2016 Bromium, Inc. All rights reserved.