

# Bromium Advanced Endpoint Security

Protect | Detect | Respond

## At a Glance

Bromium Advanced Endpoint Security uses micro-virtualization and contextual, real-time detection to protect across all major threat vectors and attack types. Enterprises can finally defeat cyber attacks and eliminate endpoint breaches.

## Key Business Benefits

### PROTECT AGAINST ZERO-DAY ATTACKS

Revolutionary micro-virtualization technology prevents known and unknown cyber attacks from compromising endpoints and your corporate network

### TRUE PREVENTION WITHOUT USER DISRUPTION

Users can safely click on anything from home, branch offices, airports and cafes—without the need for restrictive policies

### DETECT ATTEMPTED BREACHES

Behavioral detection techniques alert and monitor suspicious activity on the host system

### ELIMINATE REMEDIATION AND EMERGENCY PATCHING COSTS

Bromium-protected endpoints are self-remediating because any possibility of malware persistence is eliminated. Pivoting from the attacked system to the enterprise network is not possible

Today's enterprises are fighting a losing battle against advanced, targeted and often undetectable cyber attacks. In spite of the increased spend on more and more layered security solutions, organizations are not making headway against attackers. Enterprises are getting breached, users' productivity is hampered by side effects of security solutions, and IT is stuck on a treadmill of never-ending patching and remediation.

Bromium® Advanced Endpoint Security offers a better way to defeat cyber attacks that target the endpoint, where more than 70% of breaches originate. The first to deliver an endpoint security solution based on virtualization, Bromium offers comprehensive

next-generation endpoint protection that integrates endpoint threat isolation, threat analytics and continuous host monitoring to enable organizations to protect, detect and respond to targeted attacks, zero-day threats and attempted breaches in real time.



## Protect

Complete protection against both known and unknown threats



## Detect

Real-time detection and monitoring of threat activity



## Respond

Instant attack visualization and threat intelligence

# Bromium Advanced Endpoint Security Modules

## Only from Bromium

### POWERED BY XEN

Bromium is powered by the Xen hypervisor, the same technology that drives global computing

### BROMIUM MICROVISOR

This purpose-built, security-focused hypervisor is based on Xen and leverages advanced hardware capabilities to deliver unprecedented granularity, security and performance

### CPU-ENFORCED ISOLATION

Bromium harnesses hardware virtualization features built into today's PCs and laptops to enforce the isolation of untrusted tasks and implement the principle of least privilege between the protected system and unknown code

“Enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective and response capabilities.”

NEIL MACDONALD AND PETER FIRSTBROOK  
GARTNER, 2014

## Endpoint Protection

Complete protection against both known and unknown threats

- Leverages micro-virtualization to hardware isolate websites, email, documents, USB and executables to prevent endpoint compromises
- Protects mobile users against attacks, even when off the corporate network
- Blocks attacker access to Intranet and high-value SaaS sites
- Eliminates malware persistence through automated remediation

## Endpoint Monitoring

Real-time detection and monitoring of threat activity

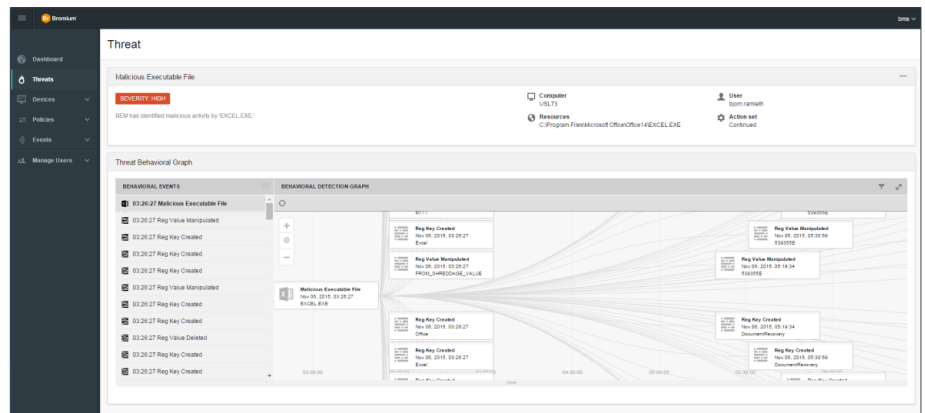
- Enables users to trust content without impacting the detection of malicious activity
- Applies behavioral rules to track anomalous activity

- Works in conjunction with Endpoint Protection to monitor activity outside the micro-VMs
- Features customizable threat modeling to flag malicious behavior appropriate for the organization

## Threat Analysis

Instant attack visualization and threat intelligence

- Delivers real-time attack forensics for malware that executes in a micro-VM or on the host OS
- Assembles and correlates across endpoints indicators of attack (IOAs) from host monitoring and indicators of compromise (IOCs) from micro-virtual machines
- Provides search capabilities to quickly identify IOAs and IOCs on endpoints
- Presents graphical view of entire attack for visualization and analysis



## Endpoint Controller

One-click deployment, policy orchestration and threat management

- Allows IT to monitor, analyze and report on dangerous security events, attack kill chains and risk profiles in real time from a centralized dashboard
- Provides full, granular policy control over all endpoint isolation and monitoring capabilities

- Accelerates deployments at scale with fully autonomous installation and update engine
- Publishes threat intelligence in real time to SIEM systems and network security tools to provide in-depth defense

“Bromium is the most significant advancement in security in decades.”

BOB BIGMAN  
FORMER CISO, CIA

“Bromium’s endpoint threat isolation revolutionizes security.”

ROLAND CLOUTIER  
CSO, ADP

## How it Works



### Protect

Bromium protects endpoints by isolating attack vectors for all untrusted content

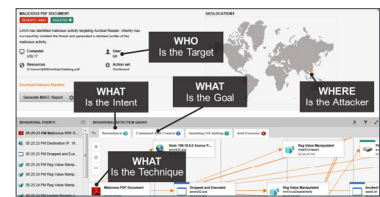
- Users have seamless experience when Web browsing, opening email attachments, opening files, etc.
- Malware is hardware-isolated by the CPU and cannot persist, pivot onto the enterprise network or access high-value data or sites



### Detect

Bromium uses micro-VM introspection to monitor execution of each untrusted task, collecting packets, files and memory changes

- Bromium monitors the host OS for any signs of malicious execution for a wide range of threatening content
- Any files that the user trusts are tracked in detail (trust but verify)



### Respond

Malware is automatically remediated when the task is closed

- Bromium assembles and correlates across endpoints IOAs from host monitoring and IOCs from micro-virtual machines
- Admins have quick search capabilities to quickly identify IOAs and IOCs on endpoints, even if offline

## System Requirements

### PROTECTED ENDPOINTS

#### Operating System

Microsoft Windows 7 (32-bit and 64-bit)  
 Microsoft Windows 8.1 (64-bit)  
 Microsoft Windows 10  
 Mac OSX

### BROMIUM ENTERPRISE CONTROLLER

#### Operating System

Microsoft Windows Server 2008, 2012

#### Data Base System

MicrosoftSQL Server 2008, 2012

#### Hardware

Intel or AMD standard architecture

## 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](http://www.bromium.com).

## The Bromium Advantage

	MICRO-VIRTUALIZATION	BEHAVIORAL BLOCKING	APPLICATION SANDBOX	WHITE LISTING	BEHAVIORAL ANALYSIS	NETWORK MALWARE ANALYSIS	ANTI VIRUS
Block known threats	●	●	●	●	○	●	●
Block unknown threats	●	◐	◐	◐	○	◐	◐
Protect mobile users	●	●	●	●	○	○	●
Protect against kernel attacks	●	○	○	○	○	●	○
Hardware-enforced protection	●	○	○	○	○	○	○
Eliminates remediation	●	◐	◐	◐	○	○	○
Unchanged user experience	●	○	○	○	●	●	○
No list maintenance or tuning	●	○	○	○	○	○	○
Visual attack analytics	●	○	◐	○	◐	◐	○
Not reliant on detection	●	○	○	○	○	○	○

● FULL SUPPORT   ◐ PARTIAL SUPPORT   ○ NO SUPPORT



**Bromium, Inc.**  
 20813 Stevens Creek Blvd  
 Cupertino, CA 95014  
[info@bromium.com](mailto: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](http://www.bromium.com) or contact [sales@bromium.com](mailto:sales@bromium.com)

Copyright ©2016 Bromium, Inc. All rights reserved.  
 DS.BAES.US-EN.1602