

Next-Generation Endpoint Security

CPU-enforced Isolation to Eliminate Breaches



The Next Generation of Endpoint Security

“Antivirus’ reign as the king of endpoint protection is nearing an end. Signature-based AV engines can no longer keep up with the explosion of malware variants.”

CHRIS SHERMAN, PRINCIPAL ANALYST, SECURITY AND RISK, FORRESTER RESEARCH

“Antivirus is dead, it only catches 45% of cyber attacks.”

BRIAN DYE, SVP OF INFORMATION SECURITY, SYMANTEC

“71% of breaches targeted user devices.”

VERIZON DATA BREACH INVESTIGATIONS REPORT

Today’s headlines shine the spotlight on one high-profile security breach after another. With over 70% of all data breaches involving malicious attacks on endpoints, enterprises all over the world are spending more, adding more layers to their security. Every day, attackers are finding new ways to evade detection and steal valuable data from vulnerable endpoints.

Traditional detection-based defenses like antivirus and sandboxes are easily evaded by today’s sophisticated threats, such as zero-day attacks, advanced persistent threats and spear phishing. Mainstream security vendors using decades-old approaches have been unable to effectively meet these challenges, forcing enterprises into a never-ending cycle of infections, false positives and constant endpoint remediation.

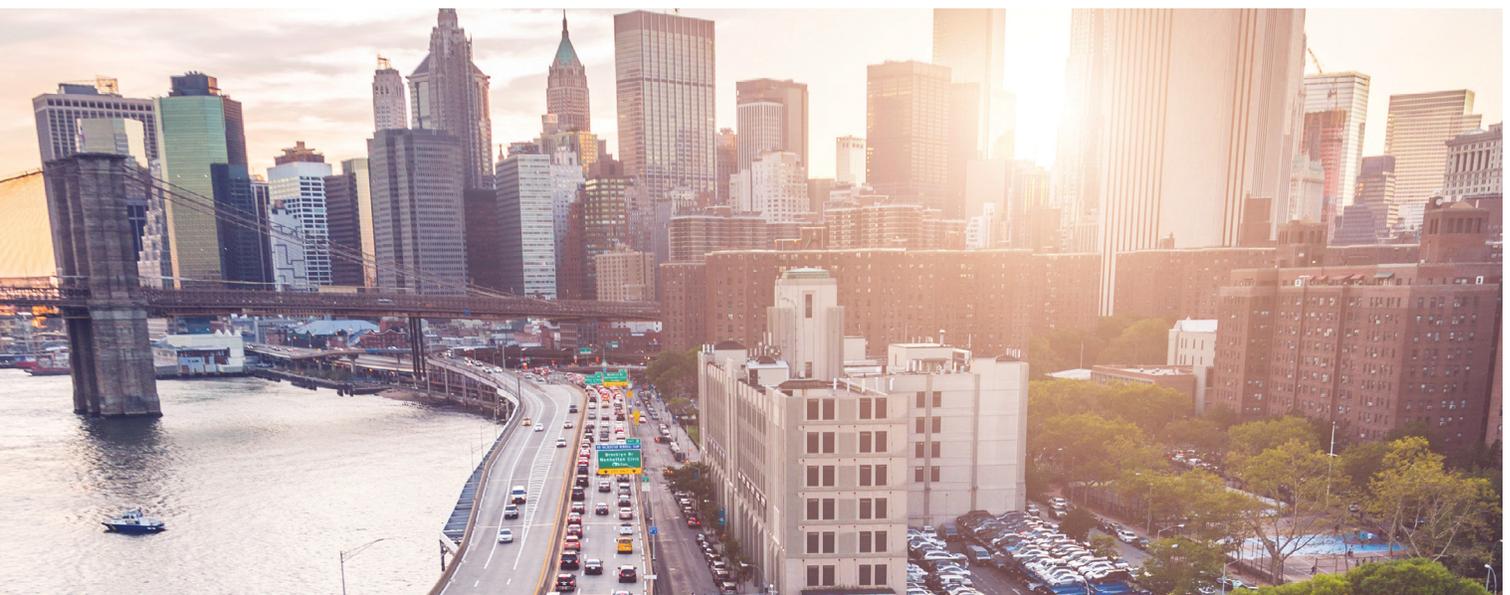
This situation has opened the door for a new approach to endpoint security,

and a new company to lead the way—Bromium.[®]

Bromium: Click on Anything Without Risk of Breach

Bromium has pioneered the next generation of endpoint security 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.



“Traditional endpoint security solutions have failed to prevent or detect breaches until it is too late, a challenge most security vendors have approached by telling their customers to assume they will be compromised. Bromium Advanced Endpoint Security represents a giant leap forward for the security industry with its ability to protect, detect and respond to advanced attacks in real time.”

FORTUNE 10 COMPANY

“Bromium’s endpoint threat isolation revolutionizes security.”

ROLAND CLOUTIER, CSO, ADP

“Bromium isolated 100% of advanced attacks in our independent testing.”

NSS LABS

The Bromium Approach: CPU-Enforced Security

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.

How We Are Unique

We prevent breaches, not detect and react to them—endpoint breaches are eliminated, dwell time is reduced to zero, and there are no false positives or need for remediation.

We protect all major threat vectors—we protect across Web, email, USB, files and executables; both known and

unknown attacks; and users on and off the corporate network.

We use CPU-enforced isolation—Bromium is far superior to a porous virtual container, vastly reducing the attack surface. Bromium has never been bypassed despite over a billion micro-VMs created to protect our customers.

Bromium Business Benefits

It’s always been an IT security dream to allow users complete freedom to click on anything, anywhere, whether on the network or on the road, in a hotel or at the airport. With Bromium, users can open any webpage or click on any attachment while at the same time preventing their endpoint from ever being compromised.

That IT security dream is now a reality. No more compromised endpoints, no more false alerts to chase down, and less frequent, untested security patches. With Bromium, IT can focus on growing the business.

HOW WE ARE UNIQUE

We have a **prevent approach** to breaches, not detect and react.

We protect across **all major threat vectors**, attack types and users.

We use **CPU-enforced isolation**, not a porous sandbox.





HOW YOUR ENTERPRISE BENEFITS



Completely secure the #1 attack surface and source of breaches... the endpoint.



Enable users to click on anything, whether in the office or on the go.



Streamline security, reduce costs and free up valuable resources.



Gain unprecedented context and visibility into the entire attack kill chain.

“With over a billion micro-VMs created, no malware has ever escaped and compromised a Bromium-protected endpoint.”

SIMON CROSBY, CO-FOUNDER & CTO,
BROMIUM

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

BOB BIGMAN, FORMER CISO, CIA

Users no longer have to worry about security or get frustrated by restrictive policies. With Bromium, you take back your right to do business securely—and without worry.

The Bottom Line

Securing the endpoint is not the only advantage of Bromium. Customers see significant operational benefits as well. Research indicates the average cost of a data breach to be over \$7.0 million. With a typical six- to nine-month payback period, it's easy to justify Bromium to business owners concerned with the bottom line.

The Next Generation of Endpoint Security Has Arrived

Bromium's revolutionary approach to endpoint protection transforms the resilience of enterprise endpoints, substantially reduces your investment in security and boosts operational efficiency. Its breakthrough Advanced Endpoint Security solution uses patented micro-virtualization technology to eliminate compromises on endpoints, false alerts, urgent patching and costly remediation. And it frees up users to be more productive and creative, while reducing management overhead, and enabling security teams to focus on more strategic tasks rather than scrambling to deflect threats.



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

Copyright ©2016 Bromium, Inc. All rights reserved.
BC.Corp.US-EN.1602