Bromium®

Bromium Redefines Endpoint Security

Isolation: An innovative, new security architecture

Bromium®

Introduction

Every day, enterprises are bombarded by rapidly multiplying and morphing advanced threats—and current solutions, including antivirus, aren't capable of defeating these targeted attacks. The only surefire way to safeguard sensitive data on and off the network is to protect the endpoint itself. With Bromium's revolutionary alternative to security as usual, you're no longer fighting a losing battle.

According to Verizon's *2013 Data Breach Investigations Report*, 71% of breaches targeted user devices.

Bromium has redefined security with its game-changing approach: isolation. Instead of using outmoded detection and blocking techniques, Bromium defends the endpoint by isolating all content for each task, *including threats,* through micro-virtualization technology that leverages CPU hardware technology. Attacks can't evade Bromium's isolation technique, and malware can't affect the protected endpoint or the corporate network. Best of all, Bromium is completely transparent to the user, so that everyone can get down to business without security worries.

Bromium's innovative approach focuses on the endpoint, where it all starts, streamlining and simplifying enterprise security. Our technology dramatically reduces and even eliminates:

- Compromises on the endpoint.
- Costly remediation and re-imaging.
- The need for urgent security-related patching.
- The noise and cost of security alerts and the wasted effort of chasing false positives.

"Advanced targeted attacks are easily bypassing traditional firewalls and signature-based prevention mechanisms. All organizations should now assume that they are in a state of continuous compromise."
—Gartner 2014

In addition, you get detailed attack insights that help you protect your entire organization, and users are empowered to freely access the applications and tools they need to get their jobs done.

Traditional Security Is Behind the Times

Evasive malware

Today's complex malware evades most traditional security solutions, and it may be weeks or months before malicious malware is discovered. Meanwhile valuable information can be stolen or critical infrastructures can be disrupted. Most solutions attempt to detect and block malware using signatures, behavioral blocking, post-infection analysis, or other means. But these approaches can only detect known threats and attack techniques, not sophisticated, insidious zero-day threats, which more often than not result in serious and costly breaches.

As hackers get more creative and determined, enterprises end up spending more time and money layering on more security solutions—antivirus, application whitelisting, host intrusion prevention, web filtering, and more. Each layer tries to solve the same problem: protecting vulnerable data and applications. Each layer adds complexity and cost without solving the problem.

No matter how many millions of dollars enterprises throw at the problem, IT is constantly in fight mode. Precious time and resources are spent investigating thousands of false alerts, searching for zero-day threats, and attempting to remediate hundreds of infected endpoints while users contend with downtime.

All software is inherently vulnerable

Today's business applications offer rich feature sets that create multiple attack vectors for cybercriminals. Microsoft Windows now has more than 60 million lines of code, and Adobe Acrobat has more than 1 million. These vast attack surfaces constantly exhibit new vulnerabilities that can be exploited by cybercriminals.

Even technologies focused on securing applications like web filtering or whitelisting are largely ineffective—and they keep users from accessing the tools they need to be more productive. Whitelisting, for example, which allows employees to use only known and trusted applications, is limited because it interferes with business processes, and attackers can still exploit supposedly trustworthy applications with unknown vulnerabilities.

Users can't be locked down anymore

Aside from the increasing onslaught of security challenges that originate from the web, email, and social media, IT is faced with the growing trend toward mobility and "bring your own device" (BYOD), which are transforming the way people do business. Users demand the freedom to work from home, from branch offices, and on the road without worrying about compromise. But when they access corporate data on mobile devices using public Wi-Fi hotspots or download apps from untrusted sources, they are opening the door to hackers. In response to this, enterprises continue to add more layers of security that are generally cumbersome, ineffective, and impose restrictive policies on users.

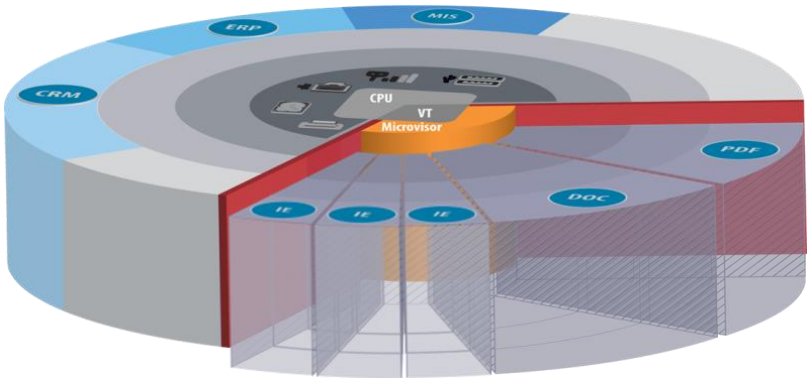
The detect-and-deflect IT treadmill

On a daily basis, IT struggles to keep up with the constant barrage of unknown threats. Even when one threat is detected and remediated, hundreds more can surface. So much of IT's valuable time is spent creating a new signature, patch, or behavior profile to detect and block the latest attack—or implementing additional security products for new vulnerabilities that show up.

Bromium: A Game-Changing Approach to Endpoint Security

The current approach to endpoint security not only has fundamental shortcomings, it's also unsustainable over the long term. Bromium has a better way. Our revolutionary hardware-isolation technology places each user task, along with the data and resources associated with it, in a hardware-isolated micro-virtual machine (micro-VM). Protected tasks have only "need-to-know" access to data, networks, and local hardware devices.

Even if malware finds its way into a micro-VM, the system still protects the enterprise network, the endpoint, and the user. Micro-VMs are created and destroyed in milliseconds, discarding malware and ensuring that the system is unaffected. All of this occurs automatically, with minimal impact on the user experience.



Bromium's unique isolation technology creates a micro-virtual machine for vulnerable operations, like web browsing and opening untrusted documents. These operations are isolated from the host operating system, eliminating the need for any type of detection or behavioral analysis—or the possibility of compromise.

Bromium vSentry: Secure by Design

Bromium vSentry® uses proprietary micro-virtualization technology to isolate content delivered via Internet browsers, documents, email, and more. Malware that may enter the micro-visor through vulnerable applications or malicious websites is unable to steal data or access either the protected system or the corporate network and is automatically discarded when the web session or document is closed by the user.

Task-level isolation

Bromium vSentry automatically and instantly isolates vulnerable user-initiated tasks, such as opening an unknown web page in a new browser tab or an email attachment from an unknown sender. It can create hundreds of micro-VMs dynamically, in real time, on an endpoint. Users are not prompted to "allow" or "deny" actions and can focus on getting the most from their system without worrying about threats.

Engineered to defeat malware

Today's software presents millions of lines of code and a seemingly infinite number of possible interactions and vulnerabilities that hackers exploit to gain control of a system. Bromium vSentry integrates directly with the Intel VT advanced hardware virtualization technology, which is built into every CPU, ensuring that malware can't break out of the vSentry micro-VM to compromise the rest of the operating system, other applications, or tasks. Bromium vSentry implements its security outside of the operating system, in the micro-virtual machine and hardware layers, which reduces the attack surface and provides a more secure platform for running tasks.

Bromium Benefits Your Business

Defeat attacks

Because we isolate every user task, we also isolate every component of every threat, no matter how advanced. Your system resources and your network are not affected by malware because it's never able to access your trusted systems.

Liberate IT
Today IT faces a constant flood of alerts from every system, challenging your best people to find the critical threats in a sea of false alerts or insignificant events. Ultimate protection means the near elimination of false positives and remediation of infected endpoints. Security-related patching of Microsoft Windows or Java is greatly reduced. Even if malware finds an open door through an application vulnerability, for example, it's instantly trapped and stopped cold.

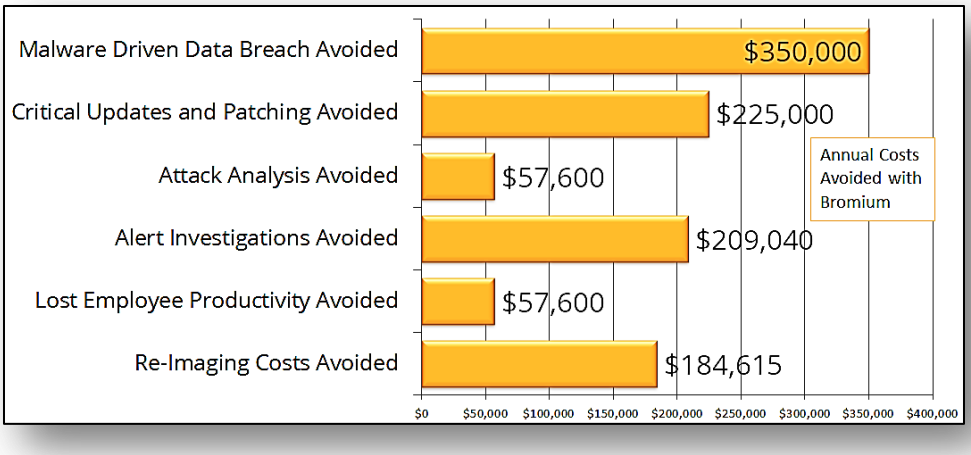
Gain practical intelligence
New advanced persistent threats and stealthy attacks are discovered every day. You can no longer hope that your company won't be compromised. With Bromium, you get unprecedented insights into all phases of every attack. It's like having a black box flight recorder for threats on the host. With Bromium's isolation technology you can safely allow threats to execute completely, giving you total awareness of the source and any external links. No other security solution can offer you full visibility direct from the endpoint where most attacks are targeted.

Empower users
Users want the flexibility to use the latest available tools, freely access the web, and work anywhere: at home, hotels, airports, or branch offices. Restrictive policies can get in their way and frustrate them. Now you can give them back their freedom so that they can do their jobs anywhere and access anything—without ever worrying about security.

The Bottom Line: Lower Operational Cost, Eliminate Compromises and Data Breaches

No technology can be justified without the ability to lower operational or capital costs. Bromium customers have identified the following areas of cost avoidance:

- Cost of patching.
- Cost of attack analysis by trained specialists.
- Cost of investigating false alerts from existing systems.
- Cost of lost employee productivity due to infection.
- Cost of re-imaging systems.



A real-life example of how Bromium offers unprecedented cost savings in key areas of IT operations.

And of course, Bromium can dramatically reduce the likelihood of a potentially catastrophic malware-driven data breach.

The Endpoint Security Solution of the Future 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 micro-virtualization technology virtually eliminates compromises on endpoints, false alerts, urgent patching, and costly remediation. And it frees up users to be more productive and creative securely, while reducing management overhead and enabling security teams to focus on more strategic tasks rather than scrambling to deflect threats.

To learn more about Bromium's game-changing security architecture, please visit www.bromium.com