Whitepaper

Making Windows Secure by Design

Bromium and Microsoft Partner to Advance Security With Micro-Virtualization

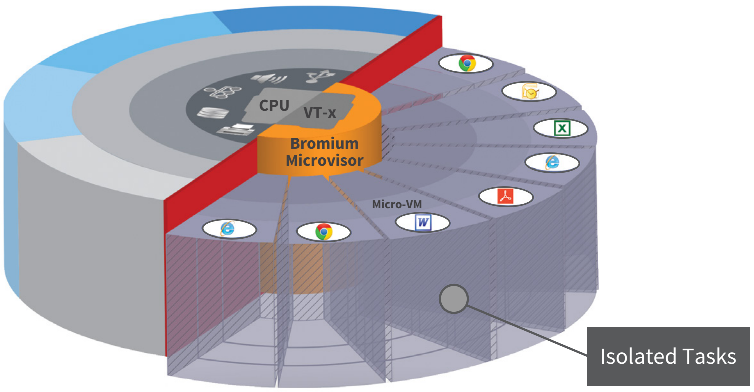
Bromium®

Introduction

Bromium has reinvented endpoint security by using a new approach to defeating breaches—micro-virtualization. Bromium hardware-isolates each Windows task that accesses untrusted content and the Web, and stops threats targeted at the endpoint. Bromium has a unique ability to observe attacks that execute in the context of a hardware-isolated micro-VM, delivering real-time visibility and attack detail to the security team, without false alerts. Bromium-protected endpoints are self-remediating and an attacker cannot access valuable data or the enterprise intranet.

Windows 10, recently announced by Microsoft, is the most secure version of Windows to date and includes many new security capabilities. One key innovation is the use of hardware-virtualization technology on the endpoint to harden the endpoint.

Bromium and Microsoft have partnered and are collaborating to ensure that Bromium products are not only compatible with Windows 10, but complement and extend the security of its in-box security features.



Why Is a New Security Approach Needed?

The threat landscape has changed. Breaches occur at an alarming pace and the #1 point of entry is the endpoint. Attempting to detect cyber attacks before they can affect a system has proven to be an impossible task. Compromises of applications and operating systems have proven to be an inevitable fact of life, so systems must provide protection of sensitive information even in the face of a technically successful attack on a system.

What Is Unique About This New Bromium and Microsoft Approach to Security?

The Bromium approach to security uses CPU-enforced micro-virtualization to defeat threats by isolating all potentially malicious data from affecting the endpoint, thereby eliminating the vectors used to attack a system. Bromium automatically records and analyzes attacks to provide advanced threat intelligence to the security operations team. Isolating ALL potentially harmful information from attacking the system ensures that no attacks are missed. Information remains secure even if malware is able to compromise the applications or operating system in the micro-VM and reveals the entire kill chain of the attack to the defenders.

Microsoft has raised the bar on security with their announced Windows 10 release. Windows 10 incorporates a host of new security features; key among them is the Virtual Security Manager (VSM).

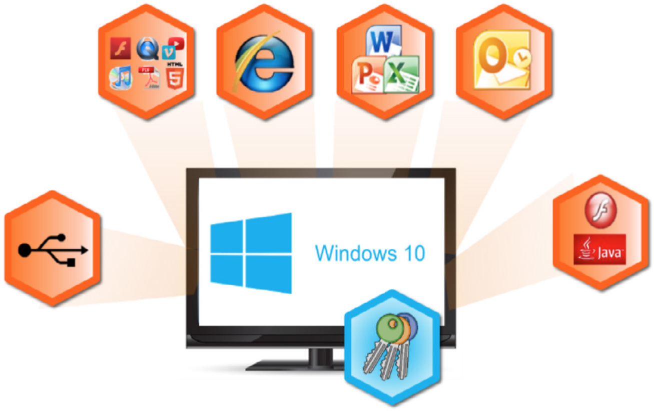
The VSM isolates key components of the Windows operating system in a hardware-enforced virtual machine ensuring that critical data like authentication information is protected even if the endpoint operating system is completely compromised.

Both of these solutions are unique in that they do not need to detect a threat in advance to protect critical information from exposure. Both are unique in that they harness the power of advanced features contained with the CPU chipsets to ensure that attackers can't escape their isolated environment. Until now Bromium has been the only vendor to use these CPU hardware features to defeat attacks and prevent breaches. When taken together, the resulting solution will be the most secure endpoint available in the world today.

How Will Cybersecurity in General Benefit From This Partnership?

Bromium has been protecting Windows 7 and Windows 8 systems deployed in some of the most highly targeted enterprises for more than two years. Three of the top five banks in North America, two of the top five financial institutes and numerous agencies in the US government rely on Bromium to protect them from cyber attacks.

BROMIUM ELIMINATES THREAT VECTORS BY ISOLATING RISKY USER TASKS



Windows 10 isolates valuable user credentials from compromise

The new partnership will extend the benefits of hardware-enforced, virtual isolation across the entire endpoint attack surface with Windows 10. Microsoft VSM will radically improve the integrity of the Windows operating system while Bromium eliminates the attack vectors that are the critical conduit for the malware needed to initiate a breach.

Working together, these complementary technologies, and the unified approach to security through isolation, will usher in a new era in security.

How Will Bromium Customers Benefit From This Partnership?

Partnering and collaborating with Microsoft enables Bromium to provide a seamless deployment on Windows operating system while extending and enhancing Windows 10 security. Additionally, customers who purchase Bromium now for Windows 7 or Windows 8 endpoints will be assured their investment is a sound investment as they migrate to Windows 10.

How Will Microsoft Customers Benefit From This Partnership?

Microsoft customers will benefit by having the most secure endpoint environment in the world. Future collaboration between Microsoft and Bromium will continue to raise the bar for attackers and enable customers to focus on getting the most from their IT assets while receiving real-time, actionable threat intelligence that can be used to lower the overall risk profile of the organization.

For more information

For more information, contact your Bromium sales representative or Bromium channel partner. Visit us at www.bromium.com.

ABOUT BROMIUM

Bromium has transformed endpoint security with its revolutionary isolation technology to defeat cyber attacks. Unlike antivirus or other detection-based defenses, which can't stop modern attacks, Bromium uses micro-virtualization to keep users secure while delivering significant cost savings by reducing and even eliminating false alerts, urgent patching, and remediation—transforming the traditional security life cycle.

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 sales@bromium.com