Whitepaper

# Bromium & Microsoft Security Partnership

## Using Endpoint CPU Virtualization to Transform Enterprise Security

Updated September 2016

Microsoft

Br Bromium®

# Introduction

Microsoft and Bromium have partnered to secure Windows 10 using endpoint CPU virtualization to protect the endpoint and to enable automatic detection and response to targeted attacks.

The approach uses virtualization to seamlessly enforce isolation of user tasks and critical Windows Services to make the endpoint more secure "by design".

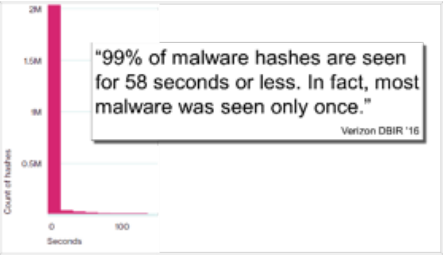
- Microsoft uses Virtualization-Based-Security (VBS) within Windows 10 to protect key OS services and prevent theft of critical data in the event that the operating system is breached.
- Bromium extends the benefits of CPU virtualization to isolate targeted applications. This protects Windows endpoints from attacks that target vulnerable applications, enables the endpoint to automatically remediate attacks, and facilitates tamper-proof endpoint monitoring.

**"Windows 10 Credential and Device Guard features and its use of use of virtualization based security represent the step change the industry has been looking for when it comes to end point security. Bromium's use of Virtualization-Based-Security to isolate the app layer from the rest of the system is exactly the right approach and complements everything we're doing."**

ROB LEFFERTS - PARTNER DIRECTOR OSG, MICROSOFT

Microsoft

# The Threat Landscape



“99% of malware hashes are seen for 58 seconds or less. In fact, most malware was seen only once.”

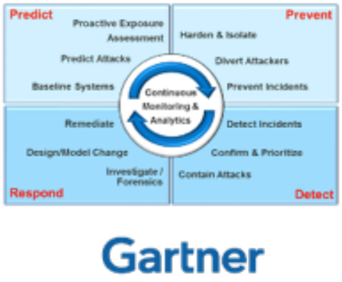
Verizon DBIR '16

In its 2016 Data Breach Investigations Report Verizon noted substantial growth in targeted attacks.  Over 90% of enterprise breaches start with a “click”: Attachments, downloads, malvertising, Java, the web, media, USB and executables punch holes in the perimeter.  IT teams struggle to keep up with patching, but malware developers are agile.  Verizon reported that over 72% of breaches resulted from malware taking advantage of a vulnerability for which a patch had been available for over a year.  Most newly disclosed vulnerabilities are attacked within a month.

Conventional “detect to protect” tools fail – at the network perimeter and the endpoint – because 99% of malware morphs into new, undetectable variants in under a minute, making signatures useless.  And the recent thousand-fold increase in crypto-malware signals a shift from manual breaches with stealthy infiltration and data theft, to machine-timescale breaches that bring an organization to its knees before the first alert.

# Responding to Targeted Attacks

How should an organization respond to attacks crafted to bypass anti-malware products? Research firm Gartner Inc. notes that there is a high chance that all organizations have already been breached, and recommends that customers evaluate Endpoint Detection and Response (EDR) tools to detect and respond to a breach in progress, and Isolation to block and detect unknown attacks.



“Consider isolation / containment solutions as an addition to EPP to ***protect*** endpoints that engage with potentially malicious content or sites, i.e. *every client that accesses the web*.  Prefer solutions with ***strong monitoring*** capabilities in the isolation environment.”

“Gartner recommends EDR for advanced threat ***detection and response***. The ideal solution will surface all information of a detected incident and put that in context for the SOC use of visualization”

# Strategic Shift: Virtualization-Based-Security

In a fundamental architectural shift toward greater resilience "by design", Microsoft and Bromium partnered to bring the isolation benefits of hardware virtualization that are familiar to data center and cloud users to Windows endpoints.

The technique relies on the use of endpoint CPU features for virtualization to isolate and protect critical Windows services, and to isolate applications that process untrusted content and that may therefore be exposed to attack and compromise.  This technique is called micro-virtualization because its goal is to use virtualization at a granular level to seamlessly extend the benefits of hardware security to the OS and its applications without relying on traditional VM abstractions.

Microsoft

Bromium

Device Guard uses micro-virtualization to hardware-isolate two Windows Services

- Credential Guard isolates credential hashes to reduce pass-the-hash attacks
- Hypervisor enforced Code Integrity enforces white-listing for applications and the OS kernel

Windows Defender Application Guard will isolate the Edge browser (in RS2)

Bromium uses micro-virtualization to protect all Windows endpoints from attacks that target any vulnerable applications, and to automate the complex "detect-protect-respond" cycle.  Microsoft uses the technology to protect critical Windows 10 system services and the Edge browser, on new PCs.

### Windows 10 Virtualization-Based-Security

Microsoft and Bromium have partnered to bring the benefits of Virtualization-Based-Security (VBS) to Windows 10 in Device Guard (DG).

VBS requires a Windows 10 enterprise license, and has hardware device feature dependencies including UEFI-based Secure Boot. VBS uses the Microsoft hypervisor Hyper-V, which has been extended through the Bromium partnership to support new use cases on the endpoint.

Device Guard uses micro-virtualization to hardware-isolate two Windows Services

- Credential Guard isolates credential hashes to reduce pass-the-hash attacks
- Hypervisor enforced Code Integrity enforces white-listing for applications and the OS kernel

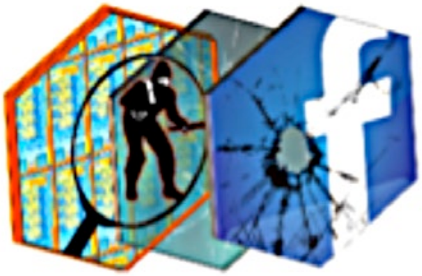
Windows Defender Application Guard will isolate the Edge browser (in RS2)

Today, Microsoft uses VBS to protect critical services within Windows 10:

- Windows 10 Hypervisor-protected Code Integrity (HVCI) protects the operating system by ensuring that only securely designed ( "http://www.microsoft.com/en-us/sdl/default.aspx" SDL compliant) code can execute in the Windows kernel.
- Windows 10 Credential Guard (CG) protects credentials and derived credentials managed by the Local Authority Subsystem Service (LSASS) that manages authentication and authentication secrets such as the NTLM hash. Hardware isolation helps to prevent "pass the hash" attacks that use stolen credentials to penetrate the enterprise network.

Microsoft has also announced that in the Windows 10 release, codenamed "Redstone 2" that will ship in 2017, will extend the benefits of VBS hardware virtualization to the Edge browser. This feature, called Windows Defender Application Guard (WDAG) aims to protect the device from attacks that compromise Edge.

## Bromium Micro-virtualization

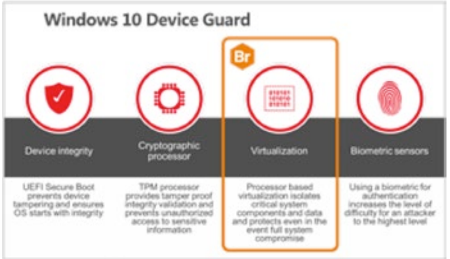


Since VBS is Windows 10 specific and can be used only on new PCs with UEFI Secure Boot, many customers won't be able to move without making hardware changes. Bromium micro-virtualization delivers today.

We provide the security benefits of endpoint CPU virtualization to all vulnerable applications on all Windows 7, 8 and 10 endpoints and we aren't UEFI dependent. And while the Microsoft security plan focuses on Edge, Bromium will extend that coverage beyond their browser. Bromium uses micro-virtualization to hardware-isolate execution of user-initiated applications that access untrusted content – the web, files, media and executables. This is particularly useful when users depend on un-patched, legacy applications.

The Bromium Microvisor is a tiny security-focused hypervisor that requires only endpoint CPU features for hardware virtualization (Intel VT-X/AMD-V) and can be used to massively enhance the security of legacy, BIOS booted Windows endpoints and BIOS-based endpoints upgraded to Windows 10. The Bromium Microvisor also seamlessly extends VBS on new Windows 10 PCs.

Windows 10

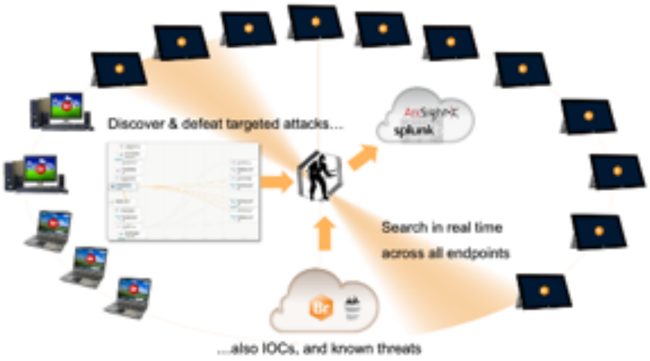

Windows 10 Device Guard
Br
Device integrity
UEFI Secure Boot prevents device tampering and ensures OS starts with integrity
Cryptographic processor
TPM processor provides tamper proof integrity validation and prevents unauthorized access to sensitive information
Virtualization
Processor based virtualization isolates critical system components and data and protects even in the event full system compromise
Biometric sensors
Using a biometric for authentication increases the level of difficulty for an attacker to the highest level

The Bromium solution protects all Windows endpoints from malicious documents, executables, attachments, downloads, and sites and empowers security teams to automate the expensive and time-consuming protect-detect-respond cycle.

- Micro-virtualization seamlessly hardware-isolates execution of each user task that accesses the web, attachments, documents and files in a tiny micro-VM - protecting the endpoint from compromise from any external vector, and automatically remediating attacks. Isolated malware cannot access high-value information, credentials or the enterprise network or sites. Bromium records detailed, false-positive free forensic intelligence for each attack, and the endpoint self-remediates by automatically discarding each micro-VM, eliminating persistence.
- Each endpoint also becomes a tamper-proof monitor in a distributed breach detection system: The endpoint uses the protected vantage point of the Microvisor to monitor all execution of the OS and its applications (including isolated apps in micro-VMs) to detect malicious execution, and shares its intelligence with the security team in real-time to accelerate enterprise-wide response. The monitor is protected using micro-virtualization to prevent it from being disabled by malware.

## Endpoints Collaborate to Accelerate Response

An endpoint that is attacked sends detailed forensic details for the attack to the Bromium Enterprise Controller which correlates them in real-time to accelerate enterprise-wide response. The endpoint automatically discards the micro-VM, remediating the attack. Bromium automatically searches all endpoints for attack indicators obtained from the endpoint to help security personnel to quickly find, remotely isolate, investigate and remediate a compromised endpoint.remotely isolate, investigate and remediate a compromised endpoint.


Discover & defeat targeted attacks...
ArcSight
splunk
Search in real time
across all endpoints
Br
...also IOCs, and known threats

| Microsoft is a trademark of the Microsoft group of companies

## Bromium Accelerates Deployment of Windows 10

Adopting Windows 10 should be the most important infrastructure security initiative for every organization.  It offers many security enhancements over Windows 7/8 and introduces a powerful suite of hardware-assisted security technologies in Device Guard that help to ensure a secure boot, protect the OS kernel, isolate credentials in CG, and enable biometric authentication.

Device Guard is device feature dependent. In particular, VBS requires Windows 10 Secure Boot, which is supported on all new PCs but is not available on older, BIOS-booted Windows endpoints that are upgraded to Windows 10. As a result, organizations will be unlikely to achieve enterprise-wide adoption of VBS in the near term.  Fortunately most deployed enterprise PCs support hardware virtualization (Intel VT-x/AMD-V), which is the only hardware requirement for micro-virtualization. As a result, Bromium can deliver many benefits of hardware enforced protection to legacy Windows endpoints - whether UEFI or BIOS based. Bromium gives customers the benefits of hardware-isolation for vulnerable applications, on any Windows endpoint.

## Summary

Windows 10 offers powerful new features that enhance endpoint resilience against a broad range of threats and its use of virtualization based security has enabled it to offer the highest level assurances that it has offered to date. Adoption of Windows 10 should be a priority for every enterprise.

Bromium micro-virtualization is a complementary security technology that complements the in-box Windows 10 security features and leverages the same virtualization-based hardware protection. Combined, the solutions make Windows endpoints massively more secure by design. In addition, Bromium uses micro-VM introspection to deliver powerful real-time insights into the nature of each attack, eliminating false alerts, and providing detailed forensic information that allows security teams to immediately respond enterprise-wide to prevent a breach.

To learn more about Bromium visit www.bromium.com

To learn more about Microsoft Windows 10, visit www.microsoft.com/en-us/windows/features

Br Bromium®

**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