Case Study

HP Sure Click Enterprise

# Top Financial Services Provider Ditches Detection for Isolation

Reissued May 2020 by HP Inc.

## Case Study Capsule

- Top financial services provider gives up on detection
- Updates security strategy by shelving venerable endpoint detection to focus on a modern security stack
- Shifts focus to protecting vulnerable applications at the source rather than examining every incoming file
- Recognizes the unpredictable security future lies in application isolation and control with network monitoring

*"True security can only be achieved by reducing the ability of a compromised process to do damage to thehost"*

NATIONAL SECURITY AGENCY (NSA) AND THE CENTRAL SECURITY SERVICE (CSS)

## Detection is Obsolete, So Realign Your Defenses to Match Today'sThreats

As the threatscape continuously evolves, a perpetual arms race between cybercriminals and cybersecurity vendors escalates unabated. Attackers innovate—providing a window of exposure—and defenders react to close resulting security gaps as quickly as possible. Yet these holes persist, with new ones continuously being identified and exploited. The Bromium advantage is that we hardware-isolate major threat vectors so that even if we fail to detect malicious activity inside a micro-VM, the enterprise is still protected. Detection- based solutions, including those that use sophisticated machine learning algorithms, still result a breach if a single threat goes undetected.

*"Micro-virtualizationis a great model. It's the way forward."*

GARTNER

Enterprise organizations have long given up on protection, shifting focus to detection and remediation in an effort to reduce the overall impact to the organization. Most concur with former FBI director, James Comey; "There are two kinds of big companies, those who've been hacked and those who don't know they've been hacked." A modern enterprise security architecture is needed to address the ever-changing threat landscape.

> *"The only way to escape the continual 'cat and mouse game' is to approach the problem differently, fundamentally redefining the approach."*
>
> **IDC**

A Bromium customer with multi-billion USD annual revenue, who processes a significant fraction of the world's electronic payment volume, is giving up on detection, recognizing that the future of security lies in more proactive techniques. Their enterprise is targeted by malicious documents on a continuous basis worldwide. Detection rates are stagnating in high-90 percent range—despite years of efforts and a vast security team devoted to incident response—yet too many threats continue to slip past their defenses and execute on production endpoints.

HP Sure Click Enterprise is their last line of defense. Furthermore, on multiple occasions, this customer has provided the forensic data from the targeted attacks—isolated by Bromium—to their NGAV vendor for them to update their detection-based machine learning models. Yet every few days, different variants of the same malware again slipped through the NGAV solution, only to be defeated once again by Bromium application isolation. Now every time the SOC team receives a new security alert from Bromium, they can perform detailed forensic analysis— with IOCs and IOAs automatically cataloged by Bromium—without any need for remediation due to application isolation and control. This "breachless threat intelligence" is a tectonic shift from the "react and respond" mode of traditional breaches.

## Why Application Isolation and Control?

At the root of the cybersecurity problem, true vulnerability lies in the applications, not in the files and web content that manifest their malicious behavior through those applications. Therefore, if you protect the applications themselves, you secure the enterprise against whatever variations the attackers send your way.

With application isolation and control:

> *"Bromium is our last line of defense."*
>
> **- TOP FINANCIAL SERVICES PROVIDER**

- False-positive detections no longer require the expenditure of scarce resources to track down
- False negatives (missed detections) still cause no harm because the threats are isolated
- Endpoint remediation and reimaging due to malware infections become practically non-existent
- Security patching for applications and operating systems can be planned, eliminating crisis patching

> *"Bromium micro-virtualization* ***is the most significant*** *advance in information and infrastructure security in decades. Bromium protects by design, allowing undetectable attacks to be automatically defeated."*
>
> **BOB BIGMAN, FORMER CISO, CIA**

Isolation through micro-virtualization creates an impenetrable dome of protection against all known and unknown threats, whereas detection requires "hitting a bullet with another bullet" every single time without fail, with the attackers having the upper hand by weight of sheer numbers and first-mover innovation. Detection demands perfection, which is mathematically impossible to achieve. In a constantly changing threatscape with a structural advantage to the attackers, detection-based defenders are always playing from behind.

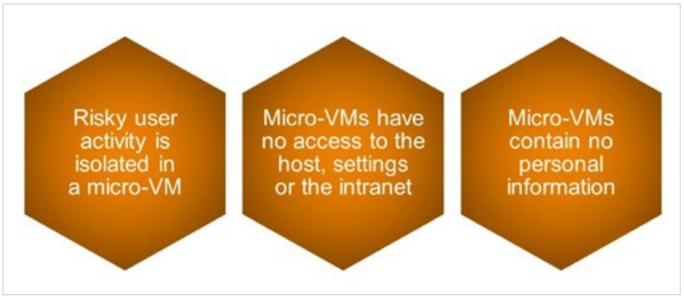
*Application isolation and control essentially "future-proofs" your defenses against unpredictable changes in the threatscape.*

## Why Bromium?

Bromium micro-virtualization provides many uniquely powerful benefits that simply cannot be matched by traditional detect-to-protect solutions, including traditional anti-virus and next-generation anti-malware defenses.

With Bromium application isolation and control, malicious content:

- Can't reach the host operatingsystem
- Can't read/write to the registry or the file system
- Can't escalate privileges or achievepersistence
- Can't access the intranet or spread laterally
- Can't exploit the kernel or escape the container


Risky user activity is isolated in a micro-VM
Micro-VMs have no access to the host, settings or the intranet
Micro-VMs contain no personal information

Security benefits of micro-VMs: Micro-virtual machines provide an impenetrable blanket of protection against an ever-changing threatscape.

Isolate the vulnerable application attack vectors to secure the enterprise without detection.

## Why Now?

The threatscape is immense and ever-changing. By some estimates, upwards of 500,000 new malware variants are released into the wild each day, with tens of thousands of new auto-generated malicious websites standing up on a daily basis as well. How can detection possibly contend with such an asymmetrical disadvantage in such an immense problem space? It can't, and enterprises and governments are steadily coming to that same realization.

What if you could reduce the problem space down to just the vulnerable applications through which the vast panoply of threats seeks to compromise your endpoints and reach into your enterprise? Protect the key application attack vectors and you neutralize all the threat variants that seek to exploit application vulnerabilities, without relying on a flawed detection model.

No more missed detections, no more false-positive fire drill responses, no more endpoint remediation or reimaging, no more crisis patching, and no more cat-and-mouse games.

*HP has partnered with Bromium to build on the secure solutions found in the world's most secure PCs. HP Sure Click Enterprise uses Bromium-powered virtualization-based security methods, such as hardware- enforced micro-virtualization, and does not require detection or emulation to offer protection against web-borne attacks.*

Protect your future with HP Sure Click Enterprise.

Reissued May 2020 by HP Inc.

For more information refer to visit
www.hp.com/proactive-security.