HP Sure Click

Secure Browsing for the Era of the Mobile Worker

Introduction

According to research from Symantec, 1 in 13 web requests leads to malware.[1] The browser has become the new enterprise perimeter, a huge attack surface stretched thin by the need to support legacy applications and application frameworks such as JavaScript, Flash, and Java that have been exploited in the past.

In today's environment, users are mobile, use unprotected networks, and access increasingly complex applications from vulnerable endpoints that cannot be secured by traditional antivirus technologies. Fortunately, there's a way out.

HP Sure Click[2] secures commonly used browsers (Internet® Explorer and Chrome™), while delivering a fast, safe, and private browsing experience. HP Sure Click was developed through the collaboration of HP and Bromium, the pioneers of application isolation using patented micro-virtualization technology.

This revolutionary approach uses CPU features in HP PCs to automatically isolate each browser tab inside a micro-virtual machine (VM), protecting the endpoint from malware—even from unknown zero-day attacks that traditional, signature-based antivirus software might miss. This granular, task-by-task isolation protects users as they work and play, delivering unparalleled security and privacy within a fast, familiar, and responsive user experience.

With HP Sure Click, the endpoint device can shrug off browser-borne attacks. Malware is blocked from accessing documents, enterprise intranets, or even other websites, and it is automatically erased when the tab is closed, thereby eliminating costly remediation and downtime.

The wild, wild web versus the browser

The rapid adoption of cloud computing and software-as-a-service is fueled by dramatic changes in end-user computing. Users are increasingly accessing consumer and enterprise applications on the go, on untrusted networks, and often from their own personal devices. We have entered an era of mobile workers connected to the cloud, decreasing the relevance of traditional network protections and leaving IT security teams in the dark. Internet-originated "drive-by" attacks, "man-in-the-browser," "cross-site scripting," and other web-delivered threats have become dominant attack vectors. Even reputable sites have delivered malware spread by compromised advertising networks.

The challenge

IT security teams face a daunting series of challenges in securing their networks against modern malware intrusions, including advanced persistent threats (APTs), advanced targeted attacks (ATAs), polymorphic malware, and file-less intrusions. Private, corporate, and public-sector networks and infrastructures can become prime targets for attacks led by organized criminals, political agitators, and other hackers eager to access critical content, whether for espionage purposes, to cause public embarrassment, or to reap financial gain.

[1] Symantec, Internet Security Threat Report Volume 23, 2018

[2] HP Sure Click is available on most HP computers and supports Microsoft® Internet Explorer, Google Chrome™, and Chromium™. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files in read-only mode, when Microsoft Office or Adobe Acrobat is installed.

4AA7-4555ENW, November 2018

The legacy approach is not up to the task

Detection-based security solutions protect against the vast majority of known attacks but struggle to resolve new, unknown attacks. When antivirus software relies on matching against signatures, heuristics, behaviors, or other attributes that have previously been identified, novel threats will always be a risk. Even next-generation antivirus software does not enable detection-based solutions to match the rapid innovation of exploits and techniques; businesses need to be able to protect against threats that haven't been seen before, including new breeds of file-less malware and malicious code that runs only in memory.

MOTIVES BEHIND PUBLIC ADMINISTRATION SECURITY BREACHES[3]

44% Espionage
36% Financial
14% Fun (breaches)

A crisis in patching

According to an Hewlett Packard Enterprise Security Research study titled *HPE Cyber Risk Report 2016*, the top 10 exploited vulnerabilities were all over a year old, and most have had patches available for months or even years. Take, for example, the devastating WannaCry ransomware outbreak in 2017, which leveraged a Server Message Block (SMB) vulnerability impacting all Windows versions dating back XP. Microsoft had already made a patch available—but many devices remained unpatched, with devastating consequences.

Verizon research indicates that only 33% of public sector systems are patched in a timely manner,[4] leaving critical systems—their valuable data and intellectual property—vulnerable to countless old and new exploits (Verizon's measure for "timely" patch cycles averages 12 weeks, even as Microsoft and other vendors offer monthly patches).

A new approach is urgently needed

HP Sure Click embraces application isolation at its core, utilizing hardware-enforced isolation to protect the enterprise from the inevitability of user errors, unpatched machines, and highly susceptible Internet-facing or partner-accessible devices. We've taken the ineffective practice of "bolted-on," detect-to-protect security and fundamentally shifted it to a "built-in" protection model enforced right down at the chipset. HP Sure Click protects by design, without relying on external detection of the unknown or the judgment of users to keep their organizations safe. Instead, it automatically isolates untrusted content in the browser, protecting organizations from conventional, advanced, targeted, file-less attacks, zero-day exploits, and more! Crisis patching can be relegated to the past.

Security via application isolation

At the Information Assurance Symposium (IAS) 2016, the National Security Agency (NSA) and the Central Security Service (CSS) of the United States jointly published a presentation titled "Application Isolation & Containment for Endpoint Protection." Their premise was that true security can be achieved only by *reducing the ability of a compromised process to do damage*. That's precisely the approach HP Sure Click takes through hardware-enforced process isolation and least-privilege restrictions on all tasks running within micro-virtualized environments. This creates high-fidelity, low-exposure endpoints.

Separating the trusted from the untrusted

Bromium's technology views the world in terms of trusted or untrusted content. Untrusted content typically originates from outside the organization and enters via various ingress vectors including web and email. Trusted content largely originates from known internal sources or from files that an organization's own users create and distribute themselves. The two types must be treated differently.

Untrusted content might contain anything at all—previously seen or unseen, detected or undetected—and should *always* be regarded as potentially malicious. It should never be granted access to the actual host PC operation system, the file system, or the internal network. Trusted content,

[3] Verizon, 2018 Data Breach Report, 2018; Page 41
[4] Verizon, 2017 Data Breach Report, 2017; Page 13

4AA7-4555ENW, November 2018

alternatively, can safely execute on actual physical resources. The user, however, should never see any difference in application appearance, behavior, or workflow.

Application isolation in micro-Virtual Machines

The power of application isolation is simple and straightforward—to remove the opportunity for an unknown threat to cause harm—but the execution is quite difficult. That's why HP has worked with Bromium to leverage their unique, patented approach to micro-virtualization at the hardware level, protecting the host PC from below the Windows operating system kernel, dramatically reducing the attack surface. Untrusted application content stays safely protected within each micro-VM. Bromium's one-of-a-kind approach provides protection-by-design against zero-day threats based on exploits in applications, browsers, and the kernel, a trifecta that traditional and next-generation defensive solutions can't come close to matching.

MALICIOUS ATTACHMENTS ARE PERVASIVE

The average user receives **16** malevolent emails per month.[5]

66% of malware was installed via malicious email attachments.[6]

On HP Sure Click–protected endpoints, common Office documents in read-only mode, such as Word, Excel, and PowerPoint, in addition to Adobe PDF files, are application-isolated from each other and from the host PC—right down at the hardware level. They reside inside safe, disposable micro-VMs, so users can smoothly conduct their business without workflow disruptions, knowing that their systems are secure.

Stops initial infection and self-remediates

HP Sure Click protects against the dangerous patient-zero infection within the enterprise: the initial compromised endpoint from which attackers seek to gain a foothold in the organization so they can conduct reconnaissance from lateral movement and privilege escalation.

In addition to preventing malware infections at the endpoint, HP Sure Click endpoints self-remediate when the user closes the application window or browser tab, preventing costly and time-consuming manual remediation. Malware simply disappears forever when the micro-VM is closed, never impacting the host PC or taking root within the organization.

Prevents infection spread

When malware runs on an isolated micro-VM on an HP Sure Click–protected endpoint, it executes as intended inside the safe, disposable container, with no way to escape into the host PC or other network devices. Not only is the initial target PC protected, so are all other network-connected devices that interact with the targeted host. Malicious code has nowhere to go and can't reach any sensitive data or processes on the host, the network, or other connected devices. Malware can't access the intranet or file shares, preventing lateral movement and expansion.

Lowers costs of investigation and remediation

Ponemon Institute research shows that organizations receive almost 17,000 weekly malware alerts, but only 19 percent are deemed to be reliable, and only 4 percent are investigated.[7] Making matters worse, two-thirds of the time spent by security staff responding to malware alerts is wasted because of faulty or incomplete intelligence. Detection is clearly broken—it's costly, time consuming, ineffective, and faulty in its premise and its execution. There is a better way.

With HP Sure Click, investigation and remediation are vastly streamlined and reduced. Since HP Sure Click protects endpoints automatically and self-remediates every time users close the micro-VMs containing malicious documents or web pages, the organization's actual remediation efforts can be reduced to the remaining endpoints not protected by HP Sure Click and other attack vectors.

[5] Symantec, Internet Security Threat Report Volume 23, 2018
[6] Verizon, 2017 Data Breach Report, 2017
[7] Ponemon Institute, 2015 Cost of Malware Containment; page 1

4AA7-4555ENW, November 2018

The solution

HP Sure Click leverages Bromium's virtualization-based security and isolation technology to dramatically decrease attack surfaces, monitor suspicious activity, and contain threats whether users are online or offline, because micro-virtual machines are not dependent on online access to protect your device from malware.

Secure browsing
HP Sure Click protects organizations from web-borne threats for Internet Explorer and Chrome. Each protected browser tab runs in its own secure container, completely isolating web threats from the host so that they have no place to go. When the browser tab is closed, the threat is terminated along with the micro-VM.

Secure files
Malicious documents are steadily gaining in popularity with threat actors because of their effectiveness. Ransomware is commonly delivered via malicious office documents or PDFs. HP Sure Click hardware-isolates each supported document from the operating system and the kernel. If a malicious document is saved via an ingress application—such as web download, email or Skype—it is hardware-isolated in a micro-VM. When the document is closed, the threat is terminated along with the micro-VM.

About Bromium

Bromium is the leader in application isolation, pioneering virtualization-based security to protect brands, data, and people. Using patented hardware-enforced containerization, application isolation automatically isolates threats, providing the last line of defense in the new security stack. Inside an isolated application container, malware can be allowed to fully execute because the threat has nowhere to go and nothing to steal. Unlike detection-based techniques, Bromium instantly shares threat intelligence to eliminate the impact and adapts to new attacks using behavioral analysis. Fortune 500 companies across every industry and government agencies worldwide trust Bromium application isolation.

Learn more at
www.bromium.com

About HP

HP Inc. creates technology that makes life better for everyone, everywhere. Through a portfolio of printers, PCs, mobile devices, solutions, and services, HP engineers experiences that amaze.

Learn more at
hp.com/go/computersecurity

4AA7-4555ENW, November 2018