HP WOLF SECURITY

HP SURE CLICK

SECURITY THROUGH ISOLATION IN THE ERA OF THE HOME OFFICE

TECHNICAL WHITEPAPER

PROTECT AGAINST MALWARE

Recent security-focused advances to modern browsers have caused attackers to shift their focus to document-based attacks.

TABLE OF CONTENTS

INTRODUCTION

According to Symantec, 1 in 13 web requests lead to malware[1] by tricking the user into downloading and opening malicious documents. Over 90% of non-browser-based attacks occur from opening files from e-mail attachments, with Microsoft Word documents accounting for over 67% of all malware attacks[2]. While attacks through the browser remain a threat, a huge attack surface stretched thin by the need to support legacy applications and application frameworks (i.e., JavaScript, Flash, and Java), recent security-focused advances to modern browsers have caused attackers to shift their focus to document-based attacks.

Because more people are working from home today, they are inadvertently using unprotected home networks and accessing increasingly complex applications from vulnerable endpoints. Whereas enterprise networks frequently employ products to shield endpoints from attacks, over 80% of home office routers have been found to be vulnerable to potential cyberattacks[3]. This increases security risks for organizations, as compromised endpoints could leak sensitive data, or even carry malware into the corporate network the next time users connect physically or via VPN. Fortunately, there's a way out.

HP Sure Click[3, 4] secures commonly used document types (Microsoft Word and PDF) while delivering a safe and private Chromium™-based secure browser. HP Sure Click was originally developed through a collaboration between HP and Bromium, the pioneers of application isolation using micro-virtualization technology.

This revolutionary approach uses CPU features in HP machines to automatically isolate each supported application[5] type and each secure browser tab in a micro-virtual machine (micro-VM), protecting the endpoint from malware—even from unknown zero-day attacks that traditional, signature-based antivirus protection applications 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 is able to shrug off browser-borne attacks—malware is blocked from accessing documents, enterprise intranets, even other websites, and is automatically erased when the tab is closed, thereby eliminating costly remediation and downtime.

THE PRIMARY ATTACK SURFACE HAS CHANGED

The rapid adoption of cloud and software as a service had fueled dramatic changes in end-user computing. Internet-originated "drive-by" attacks, "man-in-the-browser", "cross-site scripting", and other web-delivered threats had become the dominant attack vectors. In response, modern browsers have been redesigned with security as a primary focus. As browser vulnerabilities have become increasingly expensive, attacks were shifted from browsers to documents, especially those delivered by e-mail, webmail, or downloaded from risky websites. Most web-based attacks are now focused on tricking the user into downloading malware-infested documents.

THE CHALLENGE

TIT 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 for access to critical content.

MOTIVES BEHIND PUBLIC ADMINISTRATION SECURITY BREACHES

- 44% Espionage
- 36% Financial
- 14% Fun (breaches)[5]

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 the new, unknown attacks. When an antivirus 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. As a result, businesses need to be able to protect against new threats that have never been seen before, including new breeds of file-less malware and malicious code that runs only in memory.

A CRISIS IN PATCHING

According to HP Security Research, Cyber Security 2016, the top 10 exploited vulnerabilities were all over a year old, and most have had patches available for months or even years. The 2017 devastating WannaCry ransomware outbreak leveraged a Server Message Block (SMB) vulnerability impacting all Windows versions dating back to Windows 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 manner6, 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 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, HP Sure Clickautomatically isolates untrusted content, protecting organizations from all conceivable attacks. Crisis patching is now relegated to the past.

MALICIOUS ATTACHMENTS ARE PERVASIVE

- The average user receives 16 malevolent e-mails per month[7].
- 66% of malware was installed via malicious e-mail attachments[8].

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 published a presentation titled "Application Isolation & Containment for Endpoint Protection." The thesis was that true security can only be achieved by reducing the ability of a compromised process to do damage. And that's precisely the approach HP Sure Click takes, noted specifically inthe presentation: leveraging the unique, multi-patented hardware-enforced process isolation and least-privileged restrictions on all tasks running within micro-virtualized environments to create high-fidelity, low-exposure endpoints.

SEPARATING THE TRUSTED FROM THE UNTRUSTED

HP Sure Click 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 e-mail. 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. This content should never be granted access to the actual host PC operation system, the file system, or the internal network. Trusted content, alternatively, can safely execute on actual physical resources. From the user's perspective, however, they 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 leveraged Bromium's unique, patented approach to micro-virtualization at the hardware level, protecting the host PC from below the Windows operating system, dramatically reducing the attack surface. Untrusted application content stays safely protected within each micro-VM. HP'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.

On HP Sure Click-protected endpoints, untrusted Microsoft Word documents, Adobe PDF files, and HP Secure Browser tabs are application-isolated from each other and from the host PC—right down at the hardware—inside of safe, disposable micro-VMs. Users can also edit and save untrusted Microsoft Word documents right inside the micro-VM, conducting 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 into the organization from which they can then 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 a HP Sure Click-protected endpoint, it executes as intended inside the safe, disposable container—it has no way of escaping 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 is unable to reach any sensitive data or process on the host, the network, or other connected devices. Malware is unable to access the intranet or perform file shares, thereby 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% are deemed to be reliable, and only 4% get investigated9. To make things 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.

HP Sure Click reduces and streamlines investigation and remediation downtime. Because HP Sure Click automatically protects endpoints 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 non-HP Sure Click-protected endpoints and other attack vectors.

THE SOLUTION

HP Sure Click leverages virtualization-based security and isolation technology to dramatically decrease attack surfaces, monitor suspicious activity, and contain threats while users are online or offline, as micro-VMs are not dependent on online access to protect your device from malware.

Secure Browsing

HP Sure Click protects organizations from web-borne threats with its Chromium-based secure browser. 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. In addition, HP Sure Click protects Word and PDF documents downloaded from Internet Explorer, Google Chrome, Mozilla Firefox, and Microsoft (new) Edge browsers by marking these downloads as untrusted, thus opening them in a secure micro-VM whenever the user needs to open them.

Secure Files

Malicious documents have gained popularity with threat actors due to 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 HP

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

Learn more at:
hp.com/wolfsecurityforbusiness

[1] Symantec, Internet Security Threat Report Volume 23, 2018
[2] Bromium (Sure Click and Sure Click Enterprise) 2019
[3] https://www.theamericanconsumer.org/wp-content/uploads/2018/09/FINAL-Wi-Fi-Router-Vulnerabilities.pdf
[4] HP Sure Click is available on select HP PCs and requires Windows 10. See https://bit.ly/2PrLT6A_SureClick for complete details.
[5] Verizon, 2018 Data Breach Report, 2018; Page 41
[6] Verizon, 2017 Data Breach Report, 2017; Page 13
[7] Symantec, Internet Security Threat Report Volume 23, 2018
[8] Verizon, 2017 Data Breach Report, 2017
[9] Ponemon Institute, 2015 Cost of Malware Containment; page 1

Learn more at hp.com/go/getupdated

HP WOLF SECURITY

4AA7-4555ENW, June 2021