HP WOLF ENTERPRISE SECURITY POWERED BY Bromium®

REDUCING ENTERPRISE CYBER COMPLEXITY WITH APPLICATION ISOLATION AND ACTIONABLE INTELLIGENCE

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Today's enterprises are fighting an ever-growing battle against advanced targeted cyberattacks that go undetected. Despite the increased spend and increased complexity of layered security solutions, organizations must redefine their endpoint security strategy, consider reducing complexity, re-evaluate business requirements, and remove user workflows from untrusted or malicious networks.

Furthermore, enterprises must ensure the integrity of their enterprise infrastructure and provide real-time threat intelligence for defensive measures over a unified platform. Enterprises are getting breached, and user systems are hampered by the resource drain from the multiplicity of security solutions, while the lack of protection and real-time threat visibility hinder enterprise requirements. Applying containment as part of a well-instrumented and agile enterprise architecture will enhance today's enterprise endpoints and provide integrity, privacy, and resilience.

HP's approach to containment offers a better way to defeat cyberattacks targeting endpoints, where more than 80% of breaches originate. HP offers application isolation and containment that integrates endpoint threat isolation, threat analytics, and threat-intelligence sharing via syslog and STIX/TAXII while supporting the MITRE ATT&CK framework and reducing complexity.

HP threat-containment technology enables an enterprise to isolate, protect, and respond to targeted attacks, zero-day threats, and attempted breaches in real time. This, in turn, enables the enterprise with enhanced cybersecurity situational awareness.

Key features of HP's containment solution include:

- Hardware-enforced application isolation and containment
- Non-signature-based protection, without the need to rely on detection
- Task-level isolation with non-persistent virtual machines
- High-fidelity alerts and full kill-chain analytics, with no commercial cloud-based analysis
- Tactical: off/limited network protection
- Integration with existing enterprise asset visibility and management infrastructure
- Legacy and modern Windows applications protection
- Runs on all PC vendor hardware platforms
- Proven in-production deployments in both US defense and civilian environments

HP has extensive experience providing containment to global defense and civilian customers:

- US government defense
- US government civilian
- US law enforcement
- UK government
- UK law enforcement
- Canadian government
- German government
- German law enforcement

This document details how the HP Sure Click Enterprise[1] application-containment solution, powered by the recently acquired Bromium technology, is an unmatched solution for meeting the application-containment requirements of the US government. This document covers:

- The HP acquisition of Bromium
- Reducing complexity while increasing visibility and management
- Protecting tactical and forward-facing devices
- Collecting rich, real-time threat data with HP Sure Click Enterprise
- Threat-intelligence sharing to support US government and joint cyber capabilities
- Enabling internet isolation with HP Sure Click Enterprise

HP INC. ACQUISITION OF BROMIUM, INC.

Bromium was founded in 2010 with a mission to restore *trust in computing*. The company's founders, Dr. Ian Pratt and Dr. Simon Crosby, had a long and deep history of innovation in virtualization and security. Inspired by the isolation principles of traditional virtualization, the Bromium team created a game-changing technology called micro-virtualization to provide powerful enterprise endpoint security by protecting end users against advanced malware using application-isolation and containment technology. The team holds 48 issued patents, and 10 patents are pending for its technology. The term *application isolation and containment*, coined by the National Security Agency in its 2016 Information Assurance Symposium, has been subsequently known simply as *containment*.

Bromium, Inc. and HP Inc. entered a formal OEM relationship in 2016. HP recognized the need to differentiate its platform security offerings by leveraging hardware-based security solutions. Beginning in 2017, HP successfully began shipping an OEM version of Bromium containment branded as HP Sure Click on millions of enterprise-class devices.

Due to the success of Sure Click, HP acquired Bromium on September 19, 2019. Subsequently, HP created a new global business unit, HP Security, with the legacy Bromium team leading the new unit. As a result of the acquisition, HP has updated the naming convention of the former Bromium Secure Platform product to align better with the HP Sure Click brand. HP is committed to supporting the Sure Click solution on any PC device, regardless of manufacturer, running Windows 10. Today, the legacy Bromium Secure Platform is known as HP Sure Click Enterprise.

HP has a 20-year track record of clear security leadership in the PC industry. In 1999, HP cofounded the Trusted Computing standards group, and in 2003 was first to install trusted platform modules (TPM) in PCs. In 2005, HP was first to introduce cryptographic signing of BIOS firmware updates, driving the industry forward by working with the National Institute of Standards and Technology (NIST) to create BIOS security standards.

In 2013, HP introduced a security-focused embedded controller to the PC platform, providing a secure computing environment separate from the main CPU that can be used to enforce critical platform-security functions. The embedded controller is used to implement HP Sure Start, enabling the BIOS and other firmware to be verified cryptographically with every boot, enabling the platform to self-heal the firmware if it has been tampered with.

HP Sure Run functionality uses the embedded controller to create a cryptographic heartbeat between the controller and the host OS, enabling security-critical host OS processes to be monitored and corrective action taken upon failure. HP Sure Recover[2] was added to the platform to enable systems to reinstall the host OS securely if it is corrupted. The OS image can be downloaded from a cryptographically signed image stored on the enterprise network or cloud, or from a special flash memory chip that is protected by the embedded controller. Thus, HP systems are uniquely able to reinstall the host OS in just a few minutes to facilitate recovery from destructive malware that has deleted critical on-disk information such as the master boot record or partition table.

In 2019, HP introduced Sure Admin,[3] an industry-leading solution to enable secure management of BIOS configuration data using public-key cryptography, enabling a much more enterprise-scalable and secure solution than the traditional BIOS password. This solution also allows both remote administration over the network and secure local user access to BIOS configuration menus.

In addition to below-the-OS security capabilities, HP has created an endpoint security stack that offers industry-leading protection of the host OS. HP Sure Click Enterprise uses the hardware virtualization capabilities of modern CPUs to isolate high-risk activities such as web browsing and opening documents from internet sources.

In 2021, HP consolidated its entire endpoint security portfolio.

REDUCING COMPLEXITY, INCREASING THREAT VISIBILITY

HP Sure Click Enterprise is built by design to provide hardware-enforced application isolation and containment, achieved through leveraging existing CPU features, including Intel VT-x/EPT and/or AMD V/RVI. As a hypervisor-based solution, HP Sure Click Enterprise is a purpose-built solution to provide application isolation and containment, supporting both thick clients and virtual desktop infrastructure (VDI). Furthermore, Bromium (HP) has worked with leading cybersecurity solutions providers for years, such as McAfee, Microsoft, and Forescout to ensure compatibility and seamless integration.

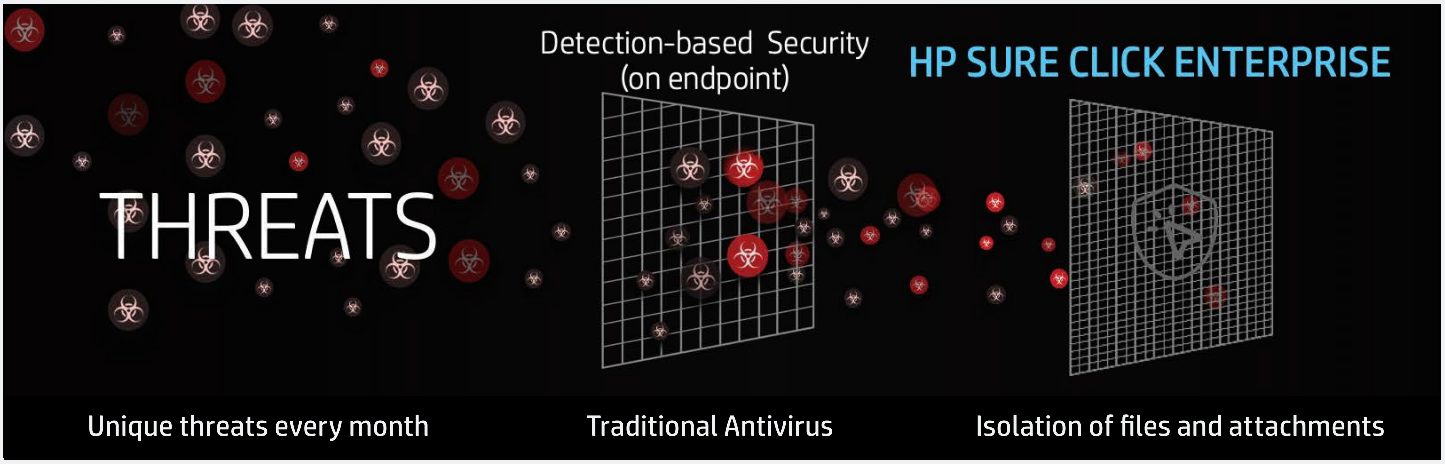
HP Sure Click Enterprise is the only containment solution to offer all of the following:

- Non-persistent micro-virtual machine containers (micro-VMs) per task
- Support of both modern and legacy OSes and applications
- Isolation and protection without a cloud connection requirement
- Full kill-chain capture and threat sharing to allow for the complete execution of an attack
- Centralized on-premises or .GOV cloud management server with AD integration
- Immediate insight into new threat vectors provided to the US government, potentially even prior to the vendor and security community, which gives the government a competitive advantage over its adversaries

APPLICATION ISOLATION AND CONTAINMENT:

HP application isolation and containment encapsulates each untrusted (inbound) file and web browser tab within a single-use disposable micro-virtual machine container (micro-VM), without relying on imperfect detection to determine malicious intent.

- Hardware-enforced isolation running on the host, leveraging CPU built-in virtualization capabilities
- Operates below the kernel, reducing attack surface down to a hardened hypervisor
- Application isolation and containment applies equally to web- and file-based threats
- Malicious threats can't reach the host OS, kernel, registry, credentials, or internal network
- False positives require no active response and are rare; potential threats have already been isolated and contained
- No impact from false negatives (missed detections), as true threats are still isolated and contained
- Eliminates user as a final cybersecurity decision-maker; allows user to perform his or her work without compromise


THREATS
Detection-based Security (on endpoint)
HP SURE CLICK ENTERPRISE
Unique threats every month
Traditional Antivirus
Isolation of files and attachments

HP SURE CLICK ENTERPRISE PROVIDES PROTECTION FOR THE FOLLOWING ATTACK VECTORS:

- Malicious email attachments (Outlook, third-party email clients, webmail)
- Malicious phishing links (Outlook, third-party email clients, Webmail, Skype, third-party chat clients)
- Malicious file downloads (http/https/FTP, etc.) – all browsers supported
- Malicious files originating from portable USB media devices, including files saved onto the host or network
- Browser exploits and fileless malware originating through the browser (IE, Chrome, FF, Edge)
- Credential theft through malicious activity in the browser
- Host protection against unknown and unsecured networks (free Wi-Fi) and malicious captive portals

PROTECTING TACTICAL AND FORWARD-FACING DEVICES

The US government supports many types of users across its global infrastructure. Requirements include standard enterprise users with devices connected to the government networks from a dedicated facility with dedicated cyber-resilience infrastructure. However, it also includes numerous devices that are connected to tactical or partner networks, or those networks supporting forward-deployed tactical users connected to low-bandwidth/high-latency or potentially hostile networks.

Protecting devices connected to remote networks is a major challenge due to network latencies and other limitations. Often, these devices are not able to connect easily to centrally managed and controlled security services, network proxies, or cloud-based browser protection solutions.

HP Sure Click Enterprise is effective for providing protection to tactical devices or devices with limited connectivity on unmanaged networks. As HP Sure Click Enterprise micro-VMs do not require any network connection to provide protection, devices running HP containment can be disconnected from central management and run for weeks or months in a hostile environment without having to “phone home” for protection.

Users on tactical devices remain fully protected using HP's containment technology while connected to any network, including malicious networks. The following activities are fully isolated while running under any network condition on the device:

- All web browsing sessions will be isolated in the micro-VM
- All files downloaded to the device or accessed via email will be isolated in the micro-VM
- All files opened from USB or removable media will be isolated in the micro-VM

An additional benefit of HP Sure Click Enterprise is that devices remain protected even when they cannot be immediately patched or updated. For example, if a new Windows kernel vulnerability is discovered, and the device is neither patched nor has its AV updated to detect the vulnerability, the HP containers will continue to protect the device fully. Any kernel or other exploits that run within the micro-VM will be unable to infect the host even though the host is unpatched and vulnerable. HP Sure Click Enterprise is the world's most advanced endpoint-application isolation and containment solution for protecting devices and users on tactical devices and networks, regardless of their connectivity or patch state.[7]

SIGNATURELESS KNOWN AND UNKNOWN ATTACK PROTECTION FIRST

HP Sure Click Enterprise's hardware-enforced isolation stops zero-day, fileless, and in-memory attacks, as well as signatureless known and unknown threats. With more than 8 billion email attachments, web pages, and downloads opened without a single reported breach,[4] no other cybersolution has been proven to isolate attacks like HP's enterprise containment solution.

THREAT VECTORS

Java
Over 5 billion
Documents and
Web pages
Protected
Zero Reported
Escapes
zoom
PDF
Adobe

MALICIOUS OUTCOMES

- Ransomware
- Spear phishing
- Macro-enabled trojans
- Malicious links
- Browser exploits
- Fileless malware
- Encrypted downloads evading detection
- Office productivity files
- Multimedia files
- Executable files
- Document links
- Fake Flash/Java updates
- Drive-by downloads
- Watering-hole attacks
- Malvertising
- Links in chat programs
- Bad DNS/URL redirects
- Intentional downloads
- Bogus drivers and utilities
- Credential phishing
- Local and domain credential extraction
- Malicious Wi-Fi hotspots

ADDITIONAL BENEFITS: COMPLEXITY REDUCTION — ENDPOINT TO THREAT ANALYST

The US government manages and operates hundreds of cybersecurity products to support its cyber needs over the largest IT and mission-supporting infrastructure of its kind. Each solution is intended to provide visibility and alerting across each agency, reporting attacks to their respective cyber teams, acting as a threat-sensor fabric. The ability to process the sheer volume of alerts requires instrumented threat aggregation and correlation tools, each then working to respond and remediate an identified attack, at scale.

Imagine the impact of processing the volume of alerts and missing the true positive due to the effort spent processing this immense volume of false positives, or worse yet, the inefficiencies of trying to solve for vulnerabilities that have yet to be identified or are without an available patch.

These realities have created an environment of unmanageable volumes of data that are stored for analysis post-attack, as well as exhaustive threat-hunt and remediation efforts and costly overhead for both incident-response teams and redundant detection-based tools, hoping one will stop or alert on what the other missed. The enterprise is often left working tirelessly to determine the full extent of an attack, post-fact, with the sensor grid becoming a complex alerting mechanism rather than agile, self-healing, self-defending threat-sensor fabric. Data destruction, exfiltration, and manipulation are first identified, and then the alerts start making sense. But there is a less complex way.

HP Sure Click Enterprise simplifies endpoint-sourced threat intelligence by first isolating a potential attack, executing the entirety of the attack in isolation, destroying the malware, and then reporting the complete threat telemetry in real-time directly to the US government. The HP Sure Click Enterprise solution forms a live-attack sensor fabric across the enterprise endpoint estate, with real-time intelligence on true-positive attacks. This reduces false-positive reporting, pinpointing the exact attack, and allowing cyber analysts and tools to focus on legitimate attacks.

With HP containment technology, the US government has provable forensic evidence of what would have been a successful breach and the binaries to process further analysis to determine source and intent, as well as the ability to automate scanning and quarantine of that exact kill chain for that department or for the entirety of the US government. This is an overall reduction in complexity from the endpoint through to the cyber analyst.

Rather than making cybersecurity pros forage through volumes of alerts, a single HP Sure Click Enterprise alert can empower the US government to know of an attack, without breach, without the adversary knowing they are in a US government environment, with live recording of the entire kill chain. The US government has access to the threat intelligence before the OS/app vendor and threat repository communities do—and before there is a patch. The government can continue delivering on its requirements and self-defend against the most advanced attacks. HP Sure Click Enterprise is effective in reducing complexity at the endpoint, the cyber fabric, as well as for the desktop and application management teams.

VISIBILITY AND MANAGEMENT

Key to a modern cyber architecture and resilience fabric is the ability to decrease complexity, increase protection, and create an integrated fabric of cyber awareness and survivability. As the government looks to modernize its cyber posture, HP Sure Click Enterprise can seamlessly integrate into visibility and asset-management infrastructure. After an attack has been isolated, the threat alert is sent to the on-prem agency- or department-managed HP controller. There, by policy, threat artifacts, hashes, and other particulars can automatically or manually be sent to existing systems. Threat telemetry can be sent to a SIEM, asset visibility and management tool (e.g., Tanium), government threat-analysis and dissemination fabric (e.g., Phantom, McAfee), etc. via SYSLOG or STIX. After the threat data is received, the US government can effectively make use of the data to act.

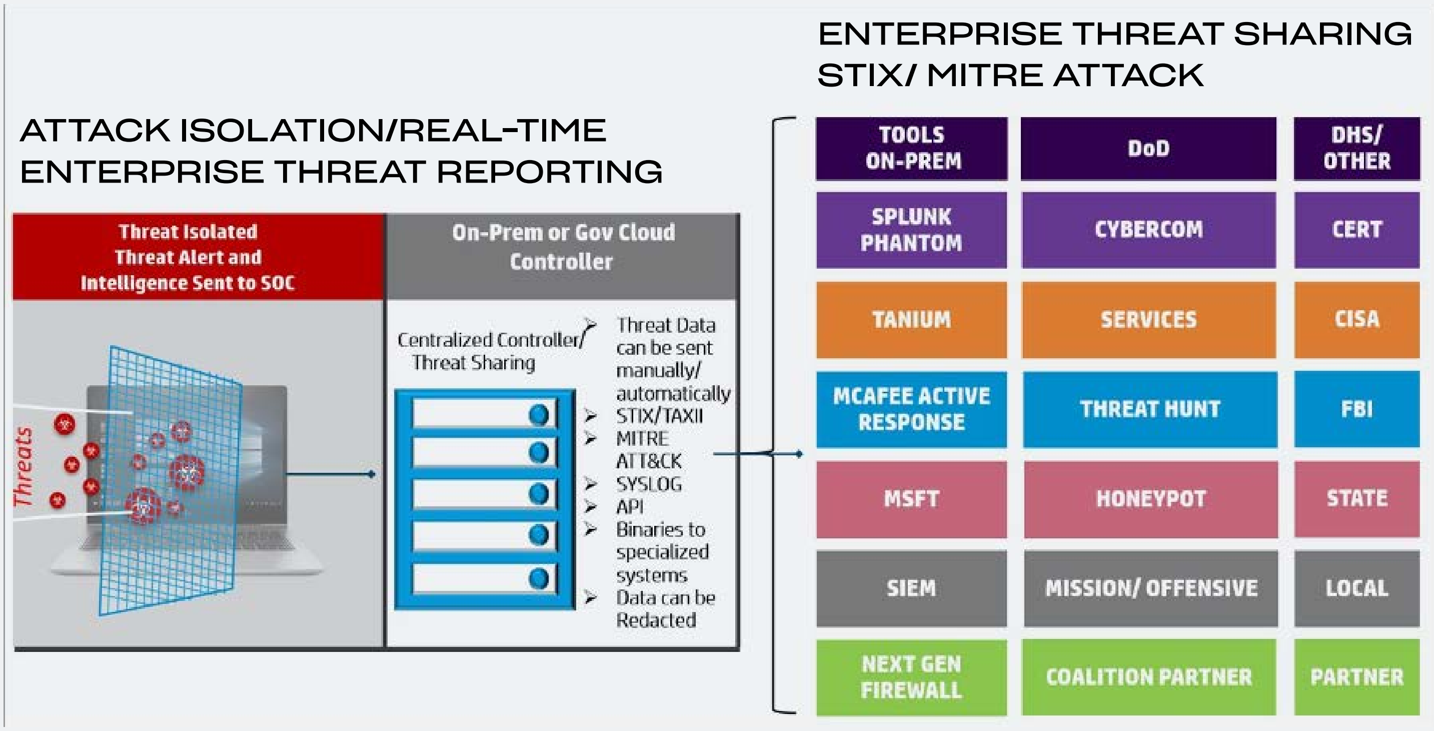
THREAT ANALYSIS

When an attack is isolated, HP Sure Click Enterprise delivers a detailed forensic trace of malicious execution in real time, allowing it to deliver the entire malware payload along with a complete forensic analysis of the kill chain. There is no need to look across several enterprise sensors to re-aggregate the malware post-fact, post-breach, or post-data exfiltration. The enterprise is protected in real time while also providing actionable threat intelligence to study the attacker's intent and serving the cyber-protection requirements of the joint commands and services.

ENTERPRISE SEARCH AND QUARANTINE/THREAT KNOWLEDGE SHARING

The HP Sure Click Enterprise system immediately delivers attack-threat forensics directly to the assigned and authorized US government enterprise centralized HP controller server. Each attack kill chain and telemetry data is assignable, via policy, either automatically or manually to a designated SIEM, asset visibility and management tool (e.g., Tanium), US government threat cloud, or any other security infrastructure component needing the real-time threat data. These existing tools, integrated into the cyber fabric, can then scan and quarantine other identified infections, update network infrastructure and their tables, or move the binaries and analysis to other US government systems requiring deeper-dive cyber analysis or measures.

HP Sure Click Enterprise containment provides real-time visibility of attacks and full integration into existing threat systems, SIEMs, threat-sharing platforms, network/perimeter compliance and visibility tools, systems-management and orchestration platforms, network cybersecurity analytics, and other solutions with simple APIs such as STIX/TAXII. The HP threat engine designed by Bromium also maps prevented attack tactics and techniques to the MITRE ATT&CK framework.



ATTACK ISOLATION/REAL-TIME ENTERPRISE THREAT REPORTING

Threat Isolated Threat Alert and Intelligence Sent to SOC

On-Prem or Gov Cloud Controller

Centralized Controller/ Threat Sharing

- Threat Data can be sent manually/ automatically
- STIX/TAXII
- MITRE ATT&CK
- SYSLOG
- API
- Binaries to specialized systems
- Data can be Redacted

ENTERPRISE THREAT SHARING STIX/ MITRE ATTACK

TOOLS ON-PREM	DoD	DHS/ OTHER
SPLUNK PHANTOM	CYBERCOM	CERT
TANIUM	SERVICES	CISA
MCAFEE ACTIVE RESPONSE	THREAT HUNT	FBI
MSFT	HONEYPOT	STATE
SIEM	MISSION/ OFFENSIVE	LOCAL
NEXT GEN FIREWALL	COALITION PARTNER	PARTNER

ENHANCING CLOUD-BASED INTERNET ISOLATION

Cloud-based internet isolation (CBII) is a technology that can route internet traffic from the end user's browser to an internet cloud-based proxy server. That proxy server renders the web page in a cloud container that is isolated from the user's device and network. The graphical output (pixels) of the remote container is the only thing transmitted back to the user's browser. This architecture protects the device from browser-based exploits.

5 ways HP Sure Click Enterprise is fully compatible with and can enhance CBII solutions:

- **HP Sure Click Enterprise browsers can connect to CBII solutions.** As an added layer of protection, HP Sure Click Enterprise can connect to CBII solutions and render web pages in a micro-VM, providing an additional layer of isolation and protection.

- **HP Sure Click Enterprise can isolate more than internet connections.** A limitation of CBII is that it cannot isolate non-internet traffic (for example, traffic from partners, traffic from other government agencies, or traffic from internal parts on the intranet). HP Sure Click Enterprise can run any website in a micro-VM and thus protect sites that CBII cannot.

- **HP Sure Click Enterprise can isolate files introduced to the host from USB and removable media.** Malicious files such as PDF, Word, Excel, PowerPoint, EXEs, images, scripts, and many other file types can be introduced onto the host from sources other than browsers connected to the internet. HP Sure Click Enterprise provides the capability to protect the device from these potentially malicious sources.

- **CBII solutions often have to whitelist or trust some well-known collaboration and file-sharing websites.** These can include sites with meeting tools such as WebEx, Skype, Zoom, Adobe Connect, etc. For these sites and tools to function for collaboration and sharing purposes, they often need to bypass the CBII. HP Sure Click Enterprise can be configured to protect these types of sites and tools by isolating and containing any files downloaded or created by these tools or websites.

- **CBII solutions provide several options for downloading files, such as flattening the file content or remote viewing of the file content.** However, there are occasions where the raw file format needs to be downloaded from the CBII browser to the desktop. HP Sure Click Enterprise can protect all file downloads that come from CBII. This provides an additional layer of protection. If a malicious file or document does bypass CBII detection algorithms and is allowed to reach the host, HP Sure Click Enterprise can still isolate and contain the file.

REMOVING HOST ACCESS TO THE INTERNET

One of the appealing configurations often associated with CBII is the ability to block direct connections from the host device to most internet sites. Preventing the host from communicating with the internet can make it more difficult for malware to reach command and control (C&C) servers.

HP Sure Click Enterprise has the built-in ability to isolate the host from the internet the same as CBII. With HP, host and network firewalls can be configured to prevent the device and all applications running on the device from communicating with the internet. HP Sure Click Enterprise can be configured to use a separate and dedicated proxy that is unknown to the host OS and applications running on it. Effectively, a device can be configured so that only HP Sure Click Enterprise micro-VMs are allowed to connect to the internet.

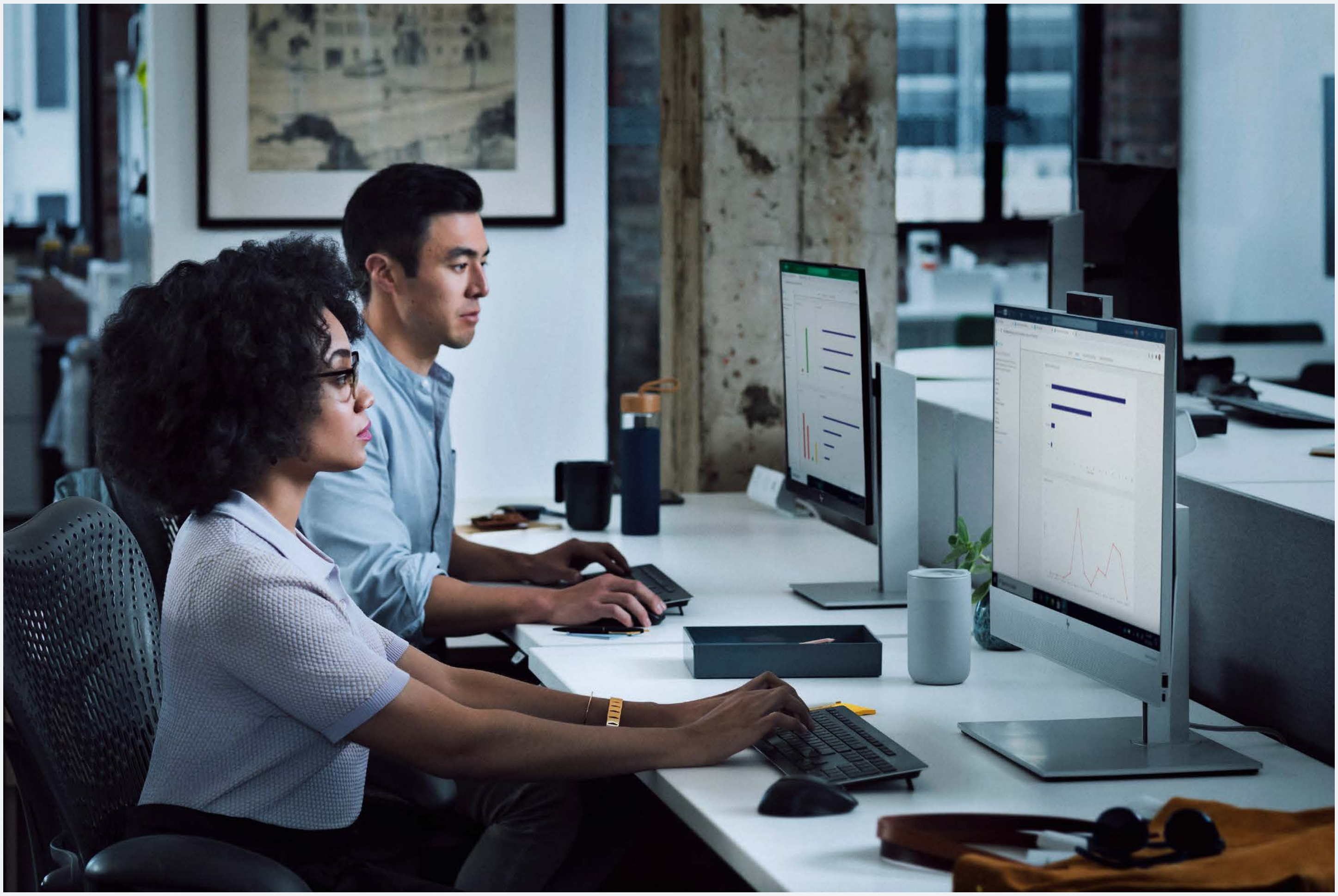
In a secure environment, it is highly desirable to monitor and control network connections from endpoint systems to identify or inhibit unexpected network flows that may be used for C&C or exfiltration by malware running on the infected host. This task is challenging for typical endpoints, as when viewed at the network level what is observed is the aggregate traffic from all applications running on the system, in particular web browsers that may be reasonably expected to make connections to a huge number of internet servers. HP Sure Click Enterprise implements a number of capabilities to help organizations better segment their network and thus identify anomalous flows.

As previously described, untrusted websites and untrusted documents are opened and rendered in isolated VMs running on the endpoint. HP Sure Click Enterprise enables all traffic from these untrusted VMs to be identified and routed independently of all other traffic from the host. Thus, it is possible to prevent untrusted VMs from communicating with hosts on the intranet (preventing lateral movement). Because the untrusted web browsing and documents isolated within VMs likely account for the vast amount of internet traffic, it then becomes possible to start more closely monitoring traffic from other applications on the host. In some deployments, customers have determined that all other applications on the endpoint are not expected to communicate with any hosts outside the intranet. Indeed, any attempt by the endpoint to do so is indicative of potential C&C or exfiltration traffic and will be blocked and investigated. This has proven to be extremely effective at identifying compromised hosts and preventing exfiltration.

A typical configuration employed by HP Sure Click Enterprise customers to implement network segregation is to deploy a special http/https proxy that is used to route all traffic from untrusted VMs, enabling applications running within untrusted VMs to talk to the internet but not the intranet. The special proxy would be unknown to other applications on the host, and they would not be able to authenticate to it. Thus, a compromised host application that attempted to talk to the internet would follow the host routing configuration and trigger a network firewall alert, providing the enterprise with immediate visibility of the potentially compromised host, while preventing the host from communicating with an attacker's C&C server.

SECURING LEGACY APPLICATIONS AND OPERATING SYSTEMS

The US government depends heavily on modern as well as legacy applications to support critical enterprise and mission systems. In the case of legacy applications, legacy systems are costly and time-consuming to upgrade and thus remain in place. However, OS and application vendors' end-of-life practices have hindered the government's ability to support legacy applications, as the vendors no longer support patching identified vulnerabilities within these systems. HP Sure Click Enterprise safeguards legacy applications that government agencies depend on, to include (but not limited to) Internet Explorer, JAVA 1.6, JAVA 1.7, and Flash, as well as Windows 10. Because of HP Sure Click Enterprise technology's use of a hypervisor, known and unknown vulnerabilities in these legacy applications are rendered irrelevant, and the enterprise can secure these applications throughout the period of continued use and while migrating to newer platforms and applications.



ARCHITECTURALLY DIFFERENT FROM OTHER CONTAINMENT SOLUTIONS

A number of solutions claim to provide containment today or will in the future. Key architectural differentiators between HP Sure Click Enterprise and these other solutions are:

Application sandboxes, running within the OS or app layer:

- Kernel mode vulnerabilities and privileged service vulnerabilities may be used to straightforwardly bypass application sandboxes
- HP Sure Click Enterprise isolates at the VM level, each VM with its own kernel and services

Some container solutions run on separate servers on the network, such as cloud-based untrusted web-browsing solutions:

- They provide internet abstraction from the enterprise host
- No enterprise integration with intranet resources. Not all internet traffic is non- enterprise, i.e., research, accounts payable, social networking, mission, etc.
- No enterprise integration with enterprise email, storage, or collaboration tools
- No enterprise integration with enterprise security infrastructure
- Limited-to-no threat intelligence possible resulting in potential loss of critical enterprise cyber threat forensics and threat intelligence
- Network configuration of internal resources to support network segmentation to untrusted internet can be complex
- HP Sure Click Enterprise isolates enterprise use of the internet and is easier to configure than cloud-based browsers while supporting protection of intranet resources as well

Hypervisor host-based security: single persistent virtual machine such as WDAG:

- Single, large virtual machine shared for all untrusted browsing for Microsoft Edge Browser (Chromium), Word, Excel, and PowerPoint only
- Single persistent VM is only shut down and reset at log-off or power-down
- With its persistent VM architecture, a compromised VM will go undetected, allowing the malware to spread to the other applications running in the VM
- Tied to enterprise licensing agreement that can be costly to the US government
- Limited-to-no threat intelligence that can be shared directly with the US government without first being sent to external cloud solution provider for analysis
- Threat analysis only if a user wants to trust the document via EDR tool that checks for known attacks leveraging their cloud analytics solution. No direct to US government analysis or zero-day analysis
- Enterprise endpoint and user telemetry may be shared with solution vendor
- No support for Windows 7 or 8.1
- No support for US government browsers: IE, Chrome, Mozilla Firefox
- No support of legacy applications
- No support for unpatched applications or OSes
- No centralized management server or reporting engine
- Relies on Active Directory Group Policy for configuration
- No local storage for cached alerts, if threat intelligence is collected
- Offline and low-bandwidth tactical environments may not have protection without connection to cloud

COMPLETE EXECUTION OF AN ATTACK WITHIN ISOLATION ENVIRONMENT

With HP Sure Click Enterprise, threats are completely isolated and, depending on the government policy that is implemented, can be allowed to execute fully and run uninterrupted in isolation so the government can fully trace the kill-chain-limiting false positives, increasing the threat intelligence collected per attack and allowing for custom templates with custom "honeypot" content inside the VM to meet other US government requirements. When the task is closed, the micro-VM is destroyed along with the threat.

The cost savings are realized at the first isolated attack. There is no longer the need to remediate, reimage, take a device off network, or evict a successful breach as HP Sure Click Enterprise is the last line of defense in the cyber-resiliency stack, isolating attacks that bypass all other defenses.

SECURITY WITHOUT DEPENDENCY ON PATCHED SYSTEMS

Patching remains a requirement for the US government; however, HP Sure Click Enterprise protects for attacks against unpatched OS and application vulnerabilities (including zero-day exploits), as well as legacy applications where patching can be near impossible. The enterprise no longer needs to commence emergency patching, an exercise that often leads to breakage of mission-critical systems.

HP Sure Click Enterprise provides isolation against large classes of unpatched vulnerabilities, giving the US government protection and visibility into unknown threats, vectors, and malware that do not yet have an available OS or app vendor patch. The threat intelligence can be leveraged and protections put in place prior to the receipt or deployment of a patch. Furthermore, the government has immediate insight into a new threat vector, perhaps prior to the vendor and security community, giving the government a competitive advantage over its adversaries.

SECURITY BOTH ON- AND OFF-NETWORK

Endpoints running HP Sure Click Enterprise isolate tasks and provide protection, regardless of location or proximity to the management back end. Whether on-premises or off-net, untrusted content is isolated from the host, and the standing policy is enforced as expected; a real-time connection to the management server is never required to provide containment. If a security event is experienced while off-net, all forensic details will be stored locally and forwarded after the endpoint re-establishes network connectivity with the management server. The malware is isolated, and the malicious file is prevented from being forwarded from the device as a further protection measure for low-bandwidth or disconnected users.

SUMMARY

Cybercriminals are more sophisticated, organized, and determined than ever. They are increasingly exploiting vulnerabilities in the changing workplace, with their sights set on the ever-growing number of endpoints and IoT devices. As overstretched IT teams struggle to keep up in the government sector, endpoint security has become increasingly critical as the first line of defense.

US government defense and civilian agencies need the ability to isolate zero-day targeted attacks and real-time forensics insight into the attack and intent, with full threat intelligence to protect the government, joint commands, and services against such an attack.

With HP Wolf Enterprise Security,[5] US government threat-sensor fabric can isolate the unknown attack, receive real-time knowledge of the attack, droppers, payloads, and intent, and then share the intelligence among its partners. Our portfolio of hardware-enforced security and endpoint-focused security services are designed to help organizations safeguard PCs, printers, and people from circling cyber predators.

HP Sure Click Enterprise provides a virtual safety net for PC users, even when unknown threats slip past other defenses. Hardware-enforced virtualization isolates high-risk content to protect user PCs, data, and credentials, rendering malware harmless, while IT gets actionable threat intelligence to help strengthen organizational security posture.

We deliver a new breed of endpoint security,[6] rooted in zero-trust principles, that is continually evolving to help the US government stay ahead of modern threats. Learn why the most security-conscious organizations in the world use HP Wolf Enterprise Security[7] to eliminate noisy, high-risk threat vectors—so their teams can stay focused on what really matters.

[1] HP Sure Click Enterprise is sold separately and requires Windows 8 or 10 and Microsoft Internet Explorer, Google Chrome, Chromium, or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint), and PDF files, when Microsoft Office or Adobe Acrobat are installed.

[2] HP Sure Recover is available on select HP PCs and requires an open network connection. You must back up important files, data, photos, videos, etc. before using HP Sure Recover to avoid loss of data.

[3] HP Sure Admin is available on select HP PCs and requires HP Manageability Integration Kit from http://www.hp.com/go/clientmanagement and HP Sure Admin Local Access Authenticator smartphone app from the Android or Apple store.

[4] Based on Active HP Sure Click users and average application usage behaviors.

[5] HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.

[6] Based on HP's internal analysis of unique and comprehensive capabilities among Application Isolation and Containment security solutions. Requires Microsoft Windows 10. Microsoft Word, Excel, or PowerPoint protection requires an Office license.

[7] HP Wolf Enterprise Security is an optional service and may include offerings such as HP Sure Click Enterprise and HP Sure Access Enterprise. HP Sure Click Enterprise requires Windows 8 or 10 and Microsoft Internet Explorer, Google Chrome, Chromium or Firefox are supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. HP Sure Access Enterprise requires Windows 10 Pro or Enterprise. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements, please visit www.hpdaas.com/requirements.

4AA8-0128ENW, June 2021