Solution Brief

HP Sure Click Enterprise

POWERED BY Bromium

ISOLATE AND PREVENT UNDETECTABLE THREATS

HP Sure Click Enterprise[1] stops even undetectable known and unkown enpoint attacks by creating micro-VMs that secure every user task, from surfing the web to opening emails and downloading attachments. Every task is completely isolated inside the micro-VM. When a task is closed, the micro-VM and any threat it contained, is disposed of without any breach.

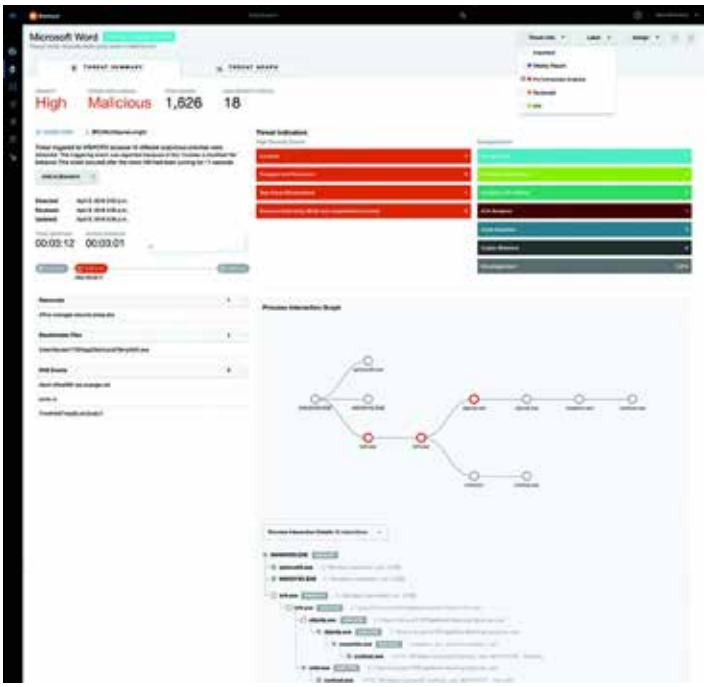
HP Sure Click Enterprise[1] is powered by unique, hardware-enforced isolation technology that uses virtualization-based security on the host to contain threats inside individual, disposable micro-virtual machines. This approach dramatically decreases attack surfaces, without any change to the way end users access their email, browsers or data.

POLICY-BASED ACCESS CONTROLS FINE-TUNE SECURITY

HP Sure Click Enterprise[1] features a robust policy engine. Administrators can configure secure web and file access by user groups, with granular controls and default policies for common use cases such as email attachments, phishing links, and web file downloads. Policies are easy to set, layered, and can be fine-tuned to address your unique security concerns and risk profiles.

THREAT INTELLIGENCE

Each Sure Click endpoint and server is part of a continuously adaptive sensor network that can be used for malware analysis and instant sharing of threat indicators. Security teams receive Threat Intelligence and complete kill-chain analyses, which helps them hunt threats, share information across the enterprise, and resolve issues fast.



Key Benefits

SAFELY ACCESS FILES FROM INBOUND SOURCES

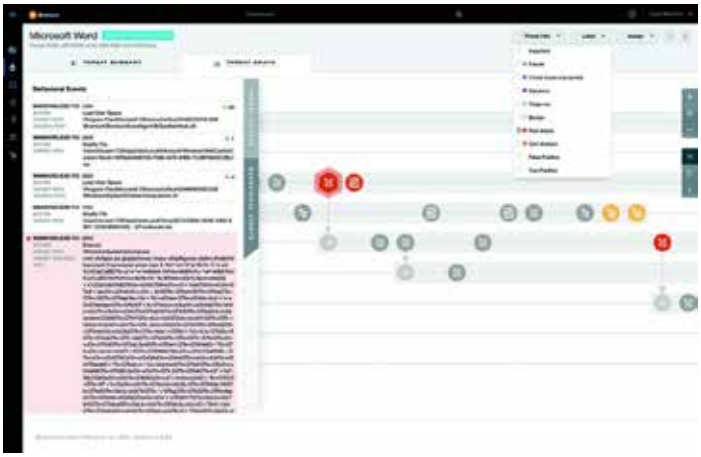
Open any file or document without risk of infection, whether downloaded from the web, received in email, or saved via portable USB drives

STOP MALWARE

Micro-VMs isolate and contain malicious activity, while malware disappears when the file or document closes

HARDEN YOUR ENTIRE DEFENSIVE INFRASTRUCTURE

Use Sure Click indicators of attack and indicators of compromise to quarantine files and search for malware lurking on servers and non-Sure Click devices using third-party tools



Key Features

IRONCLAD MALWARE PROTECTION USING HARDWARE-ENFORCED ISOLATION

Isolate incoming files and web content from the host PC and internal network using rich threat forensics from advanced behavioral analysis techniques to identify malicious activity

THREAT INTELLIGENCE

Isolated malware generates Threat Alerts for SOC analysts and sends Threat Feeds to third-party systems to help harden the defensive infrastructure

QUICKLY PROTECT KEY ATTACK VECTORS

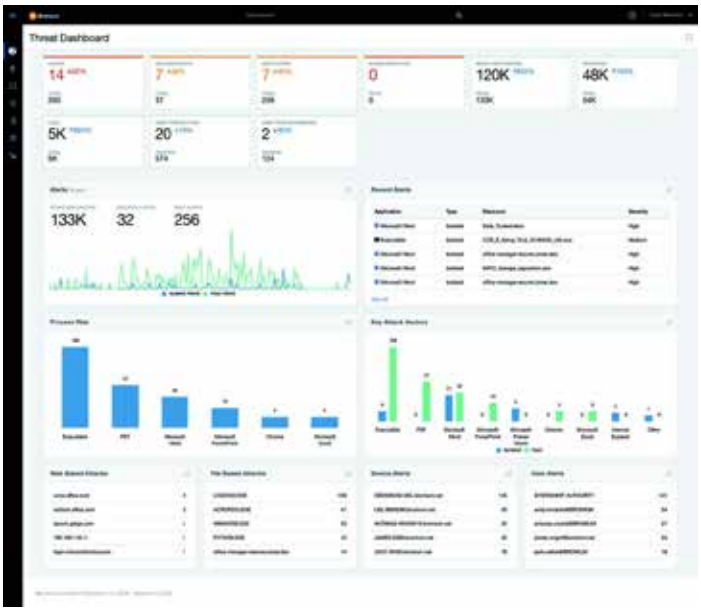
Out-of-the-box protection for key attack vectors such as email attachments, phishing links, and file downloads without wading through complex configuration settings

THREAT TRIAGE WITH CONTEXTUAL INTELLIGENCE

Workflow-based threat triage with augmented threat intelligence speed analyst identification of true positives for resolution and proactive remediation across Sure Click protected and non-Sure Click systems

ACTIONABLE DASHBOARDS, REPORTS, AND DRILLDOWNS

Easily see and share the value of Sure Click with executive summary (CISO/CIO reports, operational dashboard for the desktop team, and a threat dashboard for your security team



HP Sure Click Enterprise[1] consists of the following components:

Secure Browsing, Secure Files, and Threat Intelligence & Reporting

SECURE BROWSING

SECURE, USER-CENTRIC WEB BROWSING

Secure Browsing isolates web-borne threats and browser exploits using hardware-enforced micro-VMs, so you don't have to rely on detection or restrictive website blacklists.

Each browser tab is completely isolated from all other tabs, the host PC, and the internal network. Secure browsing takes place within a protected micro-VM, which allows for unfettered task completion in isolation from sensitive files and processes. Users experience native browsing for safe sites in Chrome, Firefox, or Edge, with automatic routing to isolated browsing for risky sites in the Sure Click Secure Browser—including suspected phishing links and uncategorized websites.

WEB THREATS, NEUTRALIZED

All website activity is sequestered within the secure micro-VM container. The micro-VM and any threats are destroyed when the browser tab is closed, leaving behind a rich Threat Report to serve as a forensic trace of all malicious activity. Web protection extends to known and unknown vulnerabilities, including zero-day browser exploits, malicious cross-site scripting, and fileless malware that exploits memory flaws or other Windows weaknesses. Crisis patching and version checking become less urgent, as Secure Browsing makes even unpatched systems safe for all users.

SECURE FILES

SECURE INBOUND FILE DOWNLOAD AND ACCESS

Secure Files uses hardware-enforced micro-virtualization to isolate malicious threats hidden within inbound files and documents, including email attachments, web downloads, and USB files.

Each file is seamlessly opened inside a protected micro-VM. The process is transparent to the user, with the files completely contained and isolated from other files and processes. Secure Files works online and offline, allowing users to securely save, modify, and rename their documents and files.

FILE AND DOCUMENT THREATS REMAIN SEQUESTERED

If a file is malicious, all activity remains isolated within the secure container, and any threats are terminated when the file is closed. This protection extends to both known and unknown vulnerabilities, including zero-day exploits, malicious macros, scripts, and advanced attack techniques that take advantage of memory kernel bugs or other Windows weaknesses.

RISKY USER ACTIVITY IS ISOLATED IN A MICRO-VM

MICRO-VMs HAVE NO ACCESS TO THE HOST, SETTINGS OR THE INTERNET

MICRO-VMs CONTAIN NO PERSONAL INFORMATION

THREAT INTELLIGENCE & REPORTING

INTELLIGENT REPORTING AND ANALYSIS

Sure Click Enterprise[1] delivers real-time alerts with complete forensic intelligence for each attack, providing real-time endpoint visibility to security teams.

The Sure Click Enterprise[1] endpoint application and central controller form a continuously adaptive sensor network for malware analysis and instant sharing of threat indicators. The HP Sure Click Enterprise central controller manages enterprise-wide policies and collects real-time attack data from end points to deliver unparalleled forensic analysis and threat telemetry data. Security teams receive real-time alerts and complete kill-chain analysis reports to help find threats faster, ensuring enterprise-wide visibility and control.

SOC teams get complete security visibility when Sure Click Enterprise is deployed across Windows endpoints and servers enterprise-wide. Real-time streaming of attack data with application flow analysis provides SOC analysts with a complete, integrated view of the attack. Thousands of low-level monitoring events are correlated in real-time at the endpointor server, eliminating the need for time-consuming manual analysis or expensive backend data centers.

The raw data is transformed into higher-level intelligence, ensuring that security teams maintain real-time awareness of the overall threat posture at all times. You'll no longer need to spend money and resources chasing false-positive alerts and on remediation, rebuilds, or emergency patching.

USE HP SURE CLICK ENTERPRISE[1] TO SECURE YOUR MOST VULNERABLE ATTACK VECTORS

EMAIL ATTACHMENTS
- Ransomware • Macro-enabled trojans
- Fileless malware • Malicious links

PHISHING LINKS
- Malicious links in email body and attachments
- Browser exploits • Fake Flash/Java updates
- Drive-by downloads • Watering-hole attacks
- Malvertising • Links in chat programs

DOWNLOADS AND EXECUTABLES
- Deliberate downloads • Fake executable updates
- Links to documents • Bad DNS / URL redirects
- Bogus drivers and utilities • Watering-hole attacks

IDENTITY PROTECTION
- Credential phishing
- Local and domain credential extraction
- Unauthorized credential reuse

UNPROTECTED NETWORKS
- Browser exploits • Fileless malware
- Drive-by downloads • Bad DNS/URL redirects
- Fake updates (Reader, Flash, Java, etc.)

UNCATEGORIZED WEBSITES
- Browser exploits • Fileless malware
- Encrypted downloads evading detection

USB MEDIA CONTENT
- Office productivity files • Multimedia files
- Executable files • document links
- Web bookmarks

ZERO MICRO-VM BREACHES
(as reported by customers)

Deploy HP Sure Click Enterprise Secure Platform to protect targeted user attack vectors or enable all capabilities for true defense-grade security

Learn more at https://www.hp.com/enterprisesecurity

1HP 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.