Solution Brief

PROTECT AGAINST MALICIOUS DOCUMENT AND FILE DOWNLOADS

SAFELY DOWNLOAD AND OPEN DOCUMENTS AND EXECUTABLE FILES FROM UNKNOWN OR UNCATEGORIZED WEBSITES

DEFEND AGAINST MALICIOUS DOWNLOADS WITH VERIFIED NATIVE APPLICATION PERFORMANCE AND USABILITY

ELIMINATE RESTRICTIVE IT SECURITY POLICIES THAT LIMIT USER ACCESS TO DOWNLOADED FILES AND INHIBIT WORKFLOWS

UNDER ATTACK: MALICIOUS DOWNLOADS ORIGINATE FROM MANY SOURCES

To do their jobs, users need to be able to download files from external sources. People tend to click on shared documents quickly, averaging less than 4 minutes from the time they hit the inbox. Malicious downloads enter the organization in many ways, including:

- Web browsing
- Clicking on shared links
- Installing programs
- Initiating FTP file transfers

Malicious downloads are particularly effective because bad websites are so abundant, short-lived, and contain content that changes frequently to avoid accurate categorization, with unique and polymorphic malware that evades all traditional methods of detection. Malware distribution by file download is efficient, inexpensive, and always evolving. It can take many forms:

- **Deliberate downloads:** user initiates a document or executable file download during normal web browsing
- **Fake executable updates:** user is tricked into downloading a malicious file when visiting a website
- **Links to documents:** user receives a document link in an email or a chat program that prompts for a download of a document that contains malware
- **URL redirects:** initial link redirects the user to an alternate URL that prompts for a file download
- **Bad DNS:** if the DNS lookup record is compromised, the user may download a malicious file, even if they did nothing wrong
- **Bogus drivers and utilities:** user gets directed to an “unofficial” download site, and inadvertently installs malware
- **Watering-hole attacks:** an attacker infects a website that is commonly used by the target and replaces or redirects file downloads

HP SURE CLICK ENTERPRISE, POWERED BY BROMIUM, USES APPLICATION ISOLATION TO PROTECT ORGANIZATIONS FROM DOWNLOAD THREATS

HP Sure Click Enterprise[3] uses virtualization-based security to protect organizations from malicious downloads. HP Sure Click Enterprise application isolation opens every downloaded file in a protected micro-VM.

Using hardware-enforced isolation, each downloaded document or executable file runs in its own secure container. Malicious threats delivered via file downloads are completely isolated from the host—and from all other applications to prevent cross-contamination. When the application or file is closed, the threat is terminated along with the micro-VM. The full malware kill-chain is shared with all other HP Sure Click Enterprise devices on your network, further hardening the infrastructure and reducing the overall attack surface.

APPLICATION ISOLATION: PROTECT BEFORE YOU DETECT

Automatically Protect All Web Downloads

Securely open any downloaded document or executable file, regardless of its source (HTTP/ HTTPS, FTP, etc.).
Isolation inside the protected micro-VM lets users safely download and access their files, while preserving a familiar user experience.

Streamline IT Security and Reduce Costs

Drastically reduce triage time and stop wasting resources on false positives with HP Sure Click Enterprise's high-fidelity alerts. Eliminate reimaging, rebuilds, and emergency patching.

Share Real-time Threat Intelligence

Adaptive intelligence identifies and stops evasive attacks, shares real-time threat data across your network, and delivers full kill-chain analysis to your SOC.

Achieve Lasting Protection with Hardware-enforced Security

Only HP Sure Click Enterprise uses virtualization-based security to deliver hardware-enforced application isolation. Protect against unknown threats and polymorphic malware that easily slip past even the most advanced detection tools.

71% of websites analyzed existed for just 24 hours or less before disappearing forever, ideal for serving malicious content and evading detection.[1]

- Symantec

The median time to the first click on the attachment is 3 minutes, 45 seconds.[2]

- Verizon DBIR 2017

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

1. https://www.symantec.com/connect/blogs/one-day-wonders-here-today-gone-tomorrow
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
3. HP Sure Click Enterprise requires Windows 8 and 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.