Solution Brief

# STOP MALICIOUS EMAIL ATTACHMENTS

SAFELY OPEN ANY EMAIL ATTACHMENT FROM OUTLOOK OR WEBMAIL, EVEN IF IT CONTAINS MALWARE

ELIMINATE RESTRICTIVE IT SECURITY POLICIES THAT LIMIT ACCESS TO EMAIL ATTACHMENTS

IMPROVE USER PRODUCTIVITY BY EMPOWERING EMPLOYEES TO OPEN EMAIL ATTACHMENTS

## EMPLOYEES MUST OPEN EMAIL ATTACHMENTS TO DO THEIR JOBS

Employees routinely work with email attachments—reading resumes, processing invoices, receiving delivery notifications, sharing financial statements, or collaborating on legal agreements with outside parties—and they often open them because they look safe. Cybercriminals are well aware of this vulnerability and they exploit it.

Today's ransomware is commonly delivered via weaponized Microsoft Office documents or PDFs that are sent through email. Cybercriminals do this because it works: ransomware related damages were estimated to exceed $5 billion in 2017[1]. Legitimate applications—many expressly whitelisted including the Microsoft Office Suite—can also be exploited to bypass layered defenses and gain an organizational foothold from a single compromised host.

Despite promising advancements in malware detection, steady improvements in secure email gateways, and an increase in user awareness training, malicious email attachments are still making it past all defenses, leading to data breach, loss, and even destruction.

Today's sophisticated, email-borne malware simply overwhelms traditional detect-to-protect defenses.

**The numbers are in:**

- 99% of malware now has polymorphic capabilities[2]
- 97% of malicious files are completely unique to each endpoint[3]
- 23% increase in the cost of these attacks in 2017[4]

## MALWARE DELIVERED VIA EMAIL IS CHEAP, EFFICIENT, AND CONSTANTLY EVOLVING

**Here's what's working for cybercriminals today:**

- **Ransomware:** Encrypts the data on a victim's PC with a symmetric key, forcing the victim to pay the ransom or reimage the machine. It is prevalent and primarily delivered via malicious documents.
- **Macro-enabled trojans:** Drop malicious binaries onto the host which then establishes communication with remote command-and-control servers for additional instructions and download additional malicious code.
- **Fileless malware:** Abuses tools such as PowerShell to execute commands without dropping any files on the host.
- **Malicious links:** Hiding in benign email attachments, these malicious links easily slip through layered defenses and result in a drive-by download or a browser exploit.

## HP SURE CLICK ENTERPRISE, POWERED BY BROMIUM, USES APPLICATION ISOLATION TO CAPTURE MALWARE HIDDEN IN EMAIL ATTACHMENTS

Using virtualization-based security, HP Sure Click Enterprise opens email attachments—such as Microsoft Office documents and PDFs—in an isolated micro-VM. Malware can launch and run but it never has access to the endpoint or the network. Malware is essentially trapped inside the micro-VM container, and is disposed of when the user closes the email attachment.

Enabling malware to execute fully changes help desk culture: end-users take pride in reporting a malware capture instead of complaining about IT security constraints.

## APPLICATION ISOLATION: PROTECT BEFORE DETECTION

### Contain Email Attachments

Open every email attachment in an isolated micro-VM. If malware is served, it is contained and cannot access the host and the network is not at risk.

### 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.

**Two-thirds of successful network penetrations come from malicious email attachments.**

- Verizon DBIR 2017[2]

**47% of malware is new or zero-day, capable of avoiding existing layered defenses.**

- WatchGuard[5]

**"This is a great product and is very effective in securing our enterprise."**

- IT Systems Analyst
Global 500 Banking Company[6]

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


1. https://cybersecurityventures.com/ransomware-damage-report-2017-5-billion/
2. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
3. http://webroot-cms-cdn.s3.amazonaws.com/7814/5617/2382/Webroot-2016-Threat-Brief.pdf
4. https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
5. https://www.helpnetsecurity.com/2017/09/29/credential-theft/
6. TechValidate. https://www.techvalidate.com/tvid/813-0A2-81D
7. 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.