SOLUTION BRIEF

HP WOLF SECURITY

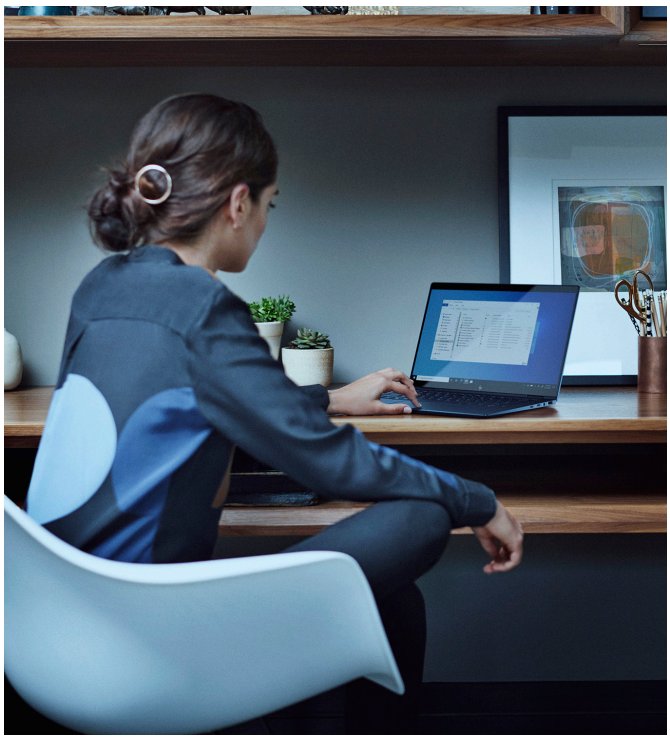
# PROTECTING AGAINST SOCIAL ENGINEERING CYBERATTACKS WITH HP SURE CLICK ENTERPRISE

## SOCIAL ENGINEERING IS USED BY THE MOST DEVASTATING CYBERATTACKS TODAY

If an attacker can convince an end user to take an action they think is legitimate and innocuous, it's quite easy to establish a beachhead on the user's PC. From there they can develop their attack. The most common Social Engineering examples include getting a user to open an email attachment or clicking on an Internet link (URL). These attacks are almost always executed on end-user devices like Windows PCs because:

- There are a lot of them in most organizations;
- That's where less-technically savvy users interact with the attacker's content;
- The sheer variety of legitimate things an employee or contractor must do provides plenty of opportunity for attackers to develop creative ways to fool their target.

With the explosive rise of remote working, the individual using the PC may actually be someone in the employee's family, even a child. Unfortunately, these attacks are cheap to launch using tools easily acquired on the DarkWeb. They also now use sophisticated AI to create advanced social engineering attacks that are very difficult for even diligent users to spot.



## CURRENT APPROACHES FAIL TO STOP SOCIAL ENGINEERING ATTACKS

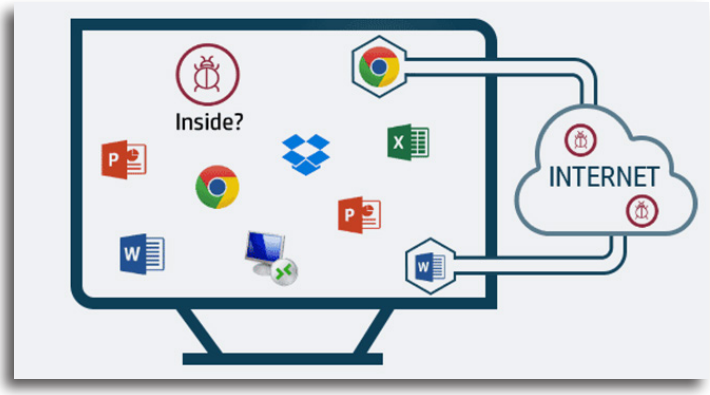
Organizations understand the threat from social engineering attacks and try a variety of approaches to stop them, but they are far from foolproof, since plenty of attacks still succeed. These are some of the most common security controls and why they fail.

| SECURITY CONTROL | DESCRIPTION | HOW IT FAILS |
|---|---|---|
| TRAINING | Educate users on what not to click on or open. | Nobody is perfect. Non-employees aren't covered. |
| ANTI-VIRUS | Identify attack and block. | Signature and simple behavior-based approaches are easily fooled. |
| EDR | Endpoint Detection & Response | Detection isn't prevention – they still get in. |

Clearly a new approach is needed – one that consistently prevents attacks, *without depending on perfect end-user behavior and without impacting their productivity.*

## HP SURE CLICK ENTERPRISE IS PROVEN PROTECTION

The approach used by HP Sure Click Enterprise (SCE)[1] is totally different, and prevents attacks from gaining a foothold on the endpoint or network, *no matter what the user does.* The idea is a simple one: SCE runs each user task (such as going to a website or opening an email attachment) in its own "virtual container", isolated from everything else on the PC. These containers prevent any malware that may be present from escaping, so it can't infect the PC or anything else on the network. Crucially, the containers are enforced by the PC's hardware, so malware can't get escape from them. When each task is completed, its container is deleted, permanently removing the malware. Best of all, Sure Click is transparent to the user:




*HP Sure Click Enterprise isolates malware, defeating Social Engineering attacks.*

- They don't have to do anything different or receive periodic training;
- They are not expected to spot attacks;
- They don't have to worry about making a mistake, hurting their productivity or infecting the whole organization.

## SUMMARY

As a leader in enterprise computing, HP recognizes the need for full-stack security across the entire PC lifecycle – from the hardware itself up to and including the applications. As remote working, hybrid cloud infrastructure and cloud-based applications have become the norm, the endpoint is the one remaining place to reliably insert security controls. **HP Sure Click Enterprise has been installed on hundreds of thousands of PCs, and has protected over 8 billion user actions without a successful compromise.** Therefore, security-conscious organizations should consider SCE as a key component of their efforts to defeat attacks based on social engineering.

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

**Learn more at [hp.com/wolfsecurityforbusiness](hp.com/wolfsecurityforbusiness).**

HP WOLF SECURITY



4AA8-0296ENW, July 2021