SOLUTION BRIEF

HP WOLF SECURITY

HP SURE CLICK ENTERPRISE

ZERO TRUST RANSOMWARE PROTECTION THAT IMPROVES USER EXPERIENCE

RANSOMWARE – WHO'S NEXT?

Ransomware is a problem that just won't go away. Despite years of experience and plenty of focus on the threat by both vendors and security staff, the successful attacks continue. A key reason for ransomware's success is that it largely relies on "social engineering": tricking employees to do something they think is benign but actually helps the attacker. Phishing is the best example but there are plenty of others. So the challenge is to stop ransomware without slashing staff productivity or expecting users to be perfect in their computer use.

HP SURE CLICK ENTERPRISE[1] – BECAUSE "CLICK HAPPENS!"

HP Sure Click Enterprise[1] (SCE) takes a totally new approach to combating ransomware. Crucially, it doesn't expect users to be perfect: HP SCE fights malware without hurting productivity or requiring people to be "Human ransomware detectors."

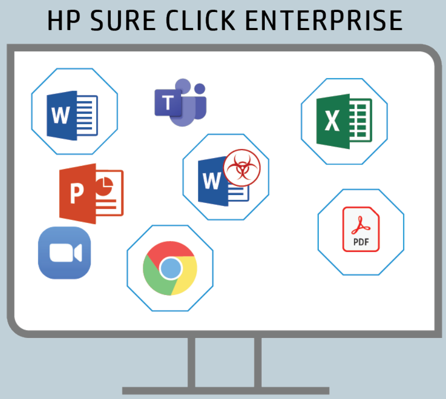
HP Sure Click Enterprise operates on the PC endpoint, isolating each potential ransomware insertion activity in a "micro-virtual machine."

Examples include:

- Opening email file attachments and downloads
- Clicking on file-less attacks via web links
- Inserting USB flash drives or other storage devices

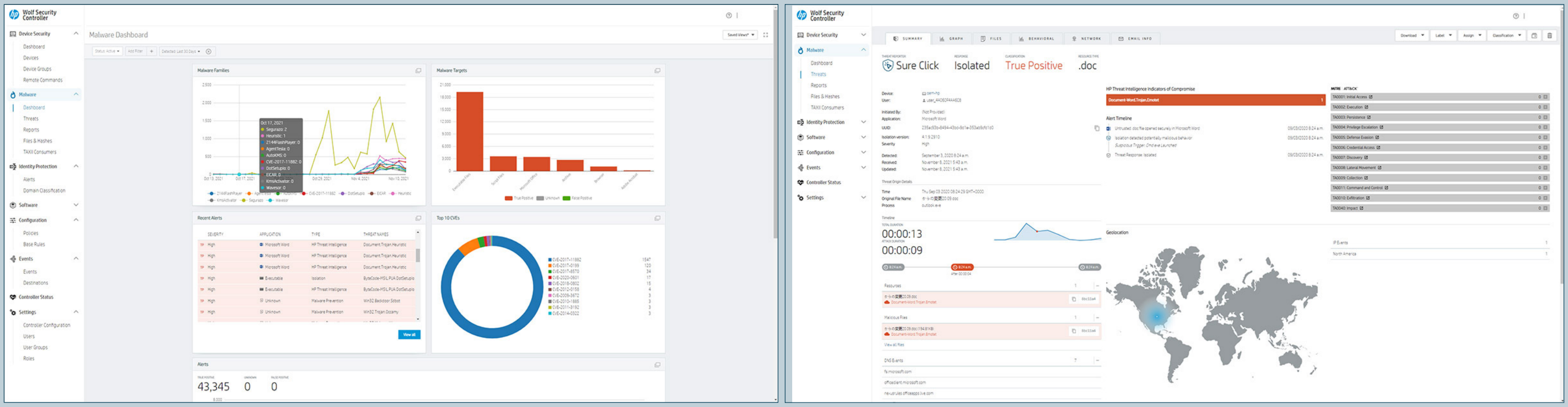
SCE uses the CPU hardware to create the isolation, so ransomware can't get around it. Malware can't encrypt files on the PC, nor can it move laterally on the network looking for other targets.

When the user ends the task, the ransomware is destroyed with it, while full forensics information is collected, and made available to security team via a central management console either on-premises or in the cloud.



Sure Click Enterprise Isolates and Contains Tasks That May Contain Ransomware

FIGHTING RANSOMWARE WHILE IMPROVING USER PRODUCTIVITY



The Wolf Controller provides both aggregated and detailed threat intelligence

HP Sure Click Enterprise[1] is effective because it doesn't depend on detecting every new attack – a hopeless task. Rather it takes a zero-trust approach: Trust nothing and verify benign operation of everything. This means it's effective on both zero-days and known threats.

Just as importantly, SCE doesn't degrade user experience. Employees don't have to modify their workflows. Unlike other solutions (e.g. sandboxing) user activity isn't held up – they can work as normal and still be protected. SCE also maintains endpoint performance, as it doesn't rely on an Internet connection or a cloud service. So it works all the time, even when totally offline such as in-flight. And finally, SCE doesn't expect staff to make a decision on what's good or bad. Security awareness training never make people "perfect security detectors". SCE eliminates this security gap, which is what ransomware has been exploiting with ease, year after year.

SUMMARY – A NEW TOOL FOR FIGHTING RANSOMWARE

Ransomware is an ongoing cyber-risk, and is constantly evolving to avoid detection. But as we've seen, HP Sure Click Enterprise fights ransomware without impacting user experience. It's also proven, having protected over 10 billion email attachments, web pages and downloads with no reported breaches. Therefore, SCE is a mandatory component of any security architecture.

[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 https://www.hp.com/us-en/security/enterprise-pc-security.html.

HP WOLF SECURITY

4AA8-0825ENW, November 2021