HP WOLF SECURITY

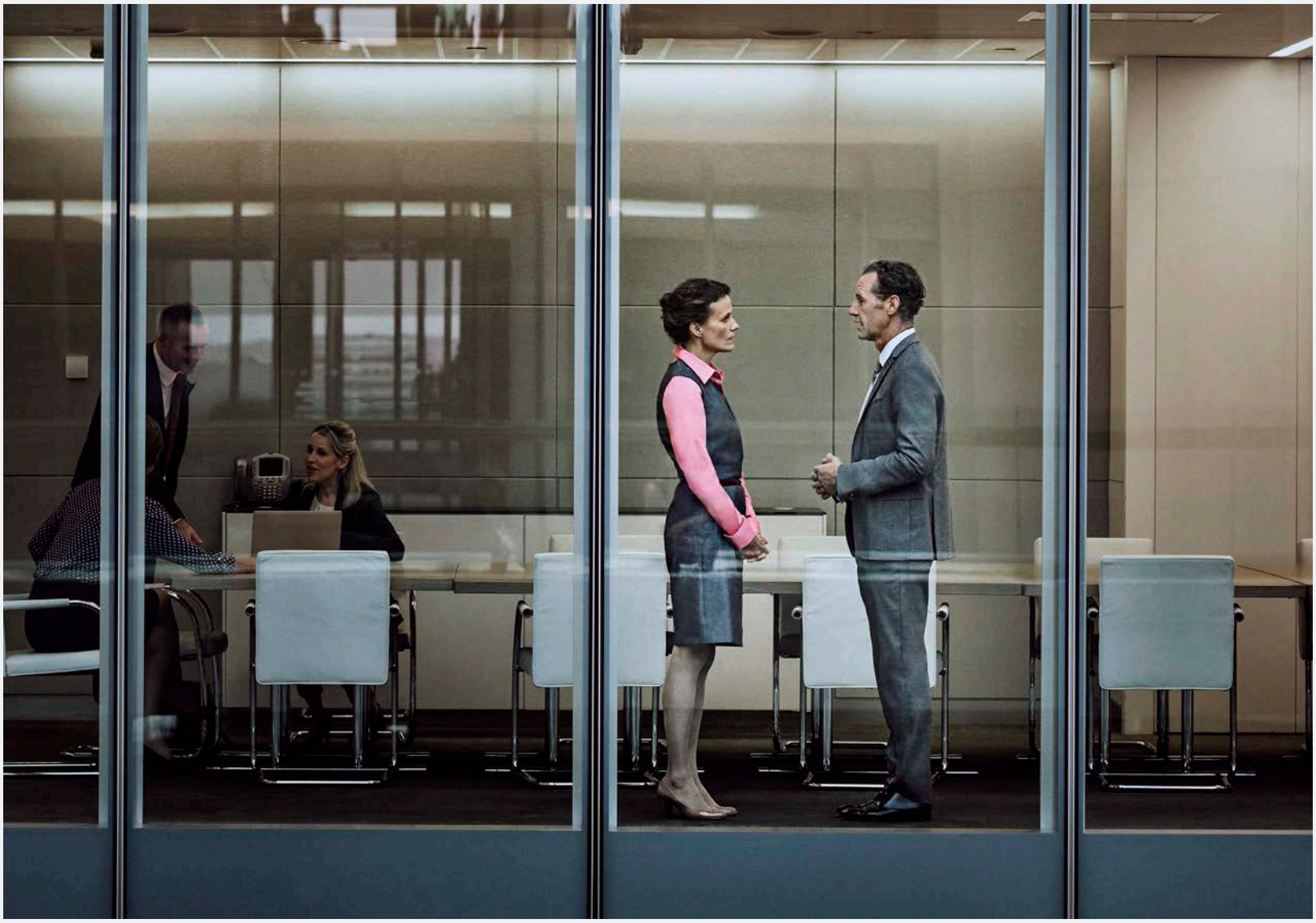
ZERO TRUST WITH HP WOLF ENTERPRISE SECURITY[1]

BECAUSE CLICK HAPPENS

The concept of zero trust was coined a decade ago and has steadily and legitimately evolved to enter the modern enterprise IT security architecture. In this document, HP presents an overview of zero trust and discusses how HP furthers this concept for PC endpoints.

TABLE OF CONTENTS

BACKGROUND



Zero trust is a crucial tool in the ongoing fight against cyber threats. The principle of zero trust is, as the terms implies, to trust nothing at face value and to verify everything that can be. It leverages user and device identities, firmware and software configuration, and broader contextual information in order to make security and access decisions.

This white paper describes in simple terms how HP uniquely delivers zero trust in an effective, yet operationally efficient manner for endpoint devices.

HP WOLF ENTERPRISE SECURITY[1]

ZERO TRUST APPLIED AT THE SOURCE

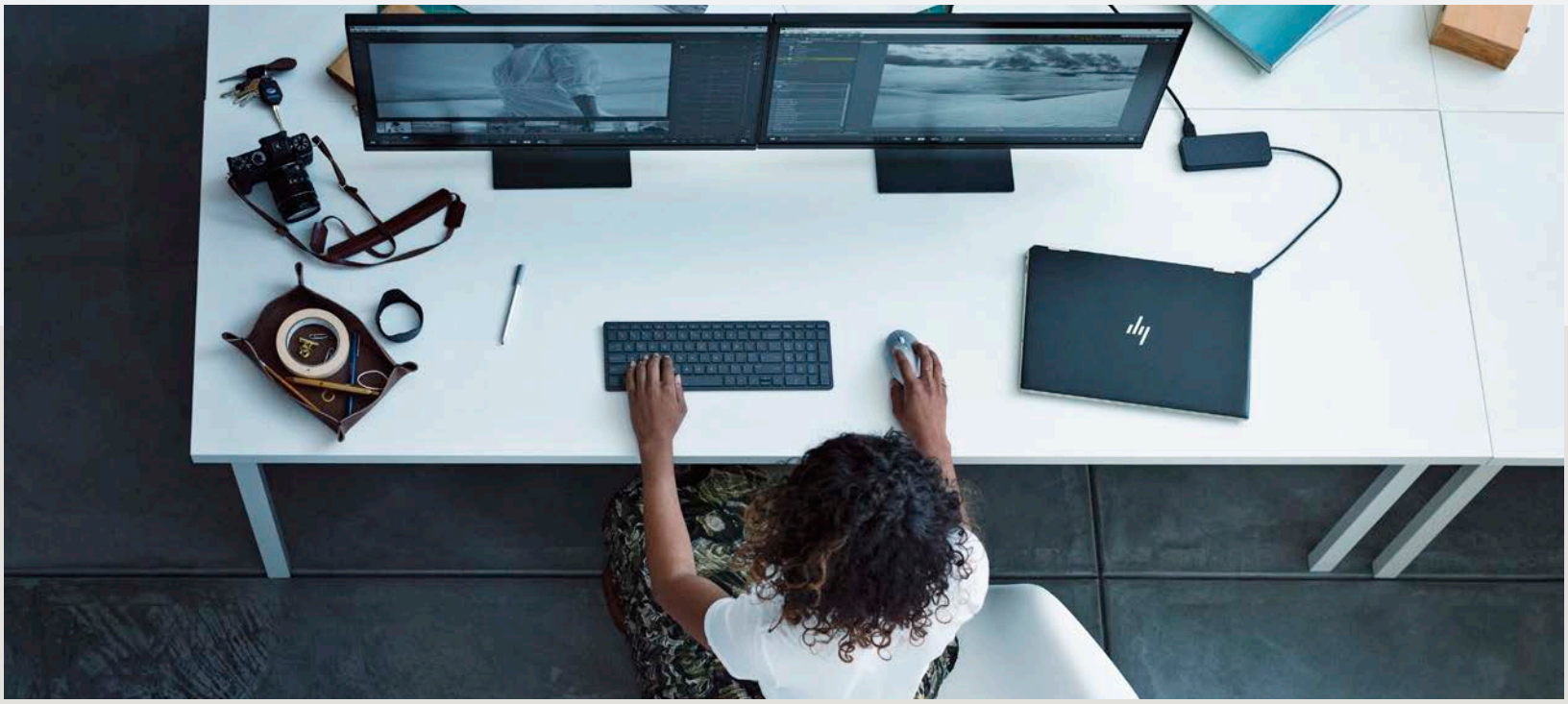
The HP approach to zero trust is built on the concept that it should be implemented as close to the source of attacks as possible. Just as ripples in a pond are much smaller closer to their source, constraining a threat very close to its point of origin is much easier than doing it elsewhere. The more quickly we can constrain an attacker's freedom of movement, the less damage they can do. Because most attacks start on end-user PCs, it's important to extend the zero-trust concept into the endpoints.

But what constitutes an attacker? It is well-documented that most attackers get in by exploiting user behavior. The most common examples are tricking people to click on bad web links or open email attachments that contain malware via phishing.

This makes it clear that the attackers are actually an organization's own employees; they just don't know it. Cybersecurity training programs for employees can help, but given that the adversary needs to succeed only once to get in, such programs cannot completely eliminate the risk.

Our approach to solve this challenge is simple: We apply zero trust on every potentially risky activity on your employees' computers. We focus on the highest-risk actions:

- Opening attachments in email (Microsoft Office documents, PDF files)
- Web browsing and clikcing web links in chat clients
- Opening files on USB devices



HP Sure Click Enterprise,[2] the flagship offering in HP's Wolf Enterprise Security[1] portfolio and the key element of our zero-trust strategy, applies zero-trust principles to endpoint security to stop even undetectable threats. Using defense-grade, hardware-enforced isolation and containment technology, Sure Click Enterprise[2] helps organizations stay ahead of modern threats that can slip past other defenses.

Sure Click Enterprise[2] places each user task (e.g. opening an email attachment) into an isolated, hardware-enforced micro virtual machine (micro-VM). This action prevents malware from escaping the task it arrived in, so it can't infect the user's computer or anything else on the network. And when the process is completed, the micro-VM is destroyed, along with the malware.

Best of all, user productivity is unaffected, as users don't have to do anything different to trigger the threat containment feature. They are free to read, edit, save and print documents as usual without being disrupted by restrictive security policies or workflows.

HP takes the zero-trust concept one step further by leveraging the advanced security capabilities built into all modern PC hardware. Sure Click Enteprise[2] uses the security hardware assist in today's Intel and AMD CPUs to create the micro-VMs and establish per-task micro-segmentation. Endpoint security software that lacks hardware enforcement is always susceptible to being defeated through compromise of the operating system or underlying infrastructure.

HP, however, applies zero trust to the entire stack, creating a threat-prevention model that is far harder to subvert. IT also gets actionable threat intelligence to help strengthen organizational security posture.

HP Wolf Security applies zero-trust principles to deliver defense-in-depth across our HP Wolf Security portfolio, helping enhance resiliency, limit exposure, and minimize damage caused by a cyberattack.

ZERO TRUST INVERTED

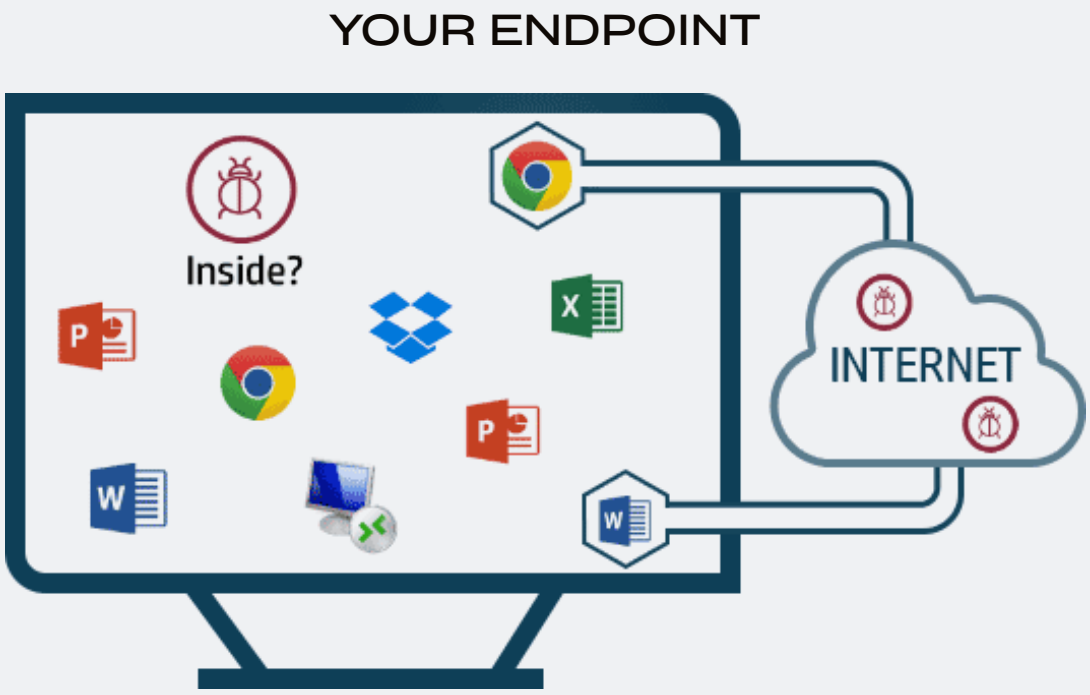
PROTECTING HIGH-VALUE APPLICATIONS AND DATA WITH HP SURE ACCESS ENTERPRISE[3]

The core zero-trust principle is not to trust data requests from unverified users or devices. But in addition to this use case, HP also supports flipping this idea on its head and protecting the known good from everything else.

A good example is IT administration activity. An IT administrator working from home and using a VPN into the data center to perform her job using superuser credentials is the perfect target for attackers. If they can find a way to install malware on her laptop, they can farm admin-level credentials, directly access sensitive assets, establish a strong foothold in the environment, and worse.

HP Sure Access Enterprise[3] protects such high-value targets through HP's application isolation capability. It places applications such as IT administration activity into a secure, hardware-assisted virtual container that can't be touched by any other process on the computer.

So even if an attacker finds a way in and compromises the PC, they still can't access the sensitive information they're after. And just like with Sure Click Enterprise,[2] protection is achieved without any impact to user productivity.



Application Isolation secures high-value protected applications from the rest of the environment.

HP WOLF ENTERPRISE SECURITY[1]

A UNIQUE APPROACH TO ENDPOINT ZERO TRUST

HP's zero-trust approach uniquely combines efficiency with effectiveness. Unlike alternative solutions, neither Sure Click Enterprise[2] nor Sure Access Enterprise[3] requires constant updates to stay relevant, both are equally effective at defeating zero-day attacks, and neither needs to be customized based on application usage.

HP zero-trust threat prevention vastly reduces the pressure on SOCs and incident response, because it eliminates most malware before it can infect even a single device. That translates into fewer alerts, less device remediation, and higher user productivity. It also means that less time and money needs to be spent on detection and response, because there's simply much less to detect.

EFFICIENCY	EFFECTIVENESS
True prevention, not just detection	Zero Trust applied at the source
Simple policies to manage	Hardware Assist: Uses security capabilities in all modern CPUs
Low false positives	Threat Containment and Application Isolation in one
Easy integration with SOC processes	Equally effective for zero-day and pervasive exploits
	Real-time threat intelligence capture

SUMMARY

ZERO TRUST FOR HYBRID WORKING AND HYBRID CLOUD

Zero Trust isn't a new concept, but it's extremely relevant in today's environment of hybrid working, where many people are not in the office.

HP's approach to Zero Trust applies threat prevention at the source: the unknowing user who opens the door to an attacker through seemingly innocuous activity.

By putting the protection on the endpoint, you don't need to worry if the user is remote or in the office, nor do you care if the data they access is in your data center or in the cloud.Hackers are stopped right on the user's computer, in a way that eliminates the need to remediate their PC. That means it's effective, can operate at scale, and reduces the costs of risk management in the modern enterprise.

Learn more at:
www.hp.com/enterprisesecurity

[1] HP Wolf Enterprise Security requires Windows 10. HP Sure Click Enterprise supports Microsoft Internet Explorer, Edge, Google Chrome, Chromium and Firefox browsers and isolates attachments from Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat are installed. HP Protected App currently supports RDP sessions, Citrix® ICA sessions, and a Chromium-based browser.

[2] HP Sure Click Enterprise requires Windows 10 and Microsoft Internet Explorer, Edge, 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.

[3] HP Sure Access Enterprise requires Windows 10 Pro or Enterprise. HP services are governed by the applicable HP terms and conditions of service provided or indicated to Customer at the time of purchase. Customer may have additional statutory rights according to applicable local laws, and such rights are not in any way affected by the HP terms and conditions of service or the HP Limited Warranty provided with your HP Product. For full system requirements https://support.bromium.com/s/article/System-Requirements-for-Bromium-Isolation-and-Monitoring.

Sign up for updates: hp.com/go/getupdated

Update to c07583975, May 2021