CSO
FROM IDG

SPONSORED CONTENT

BECAUSE CLICK HAPPENS:

THE NEED FOR ENDPOINT SECURITY ROOTED IN ZERO TRUST

"The traditional ways of securing access to the corporate network, applications, and data are no longer fit for purpose," says Ian Pratt, Head of Security for Personal Systems at HP Inc.

HP WOLF SECURITY

Even as employees return to the office following pandemic-imposed lockdowns, they're demanding more flexibility. And employers are discovering the benefits of hybrid work environments, including reduced costs due to a smaller real estate footprint.

But the world of hybrid work comes with a major security concern: a proliferation of distributed endpoints.

Spurred in part by all those newly vulnerable laptops and even printers used for work outside the protective umbrella of corporate IT networks, companies have seen a spike in cyberattacks.

"THE TRADITIONAL WAYS OF SECURING ACCESS TO THE CORPORATE NETWORK, APPLICATIONS, AND DATA ARE NO LONGER FIT FOR PURPOSE," SAYS IAN PRATT, HEAD OF SECURITY FOR PERSONAL SYSTEMS AT HP INC. "CRITICAL DATA IS BEING HOSTED OUTSIDE THE ENTERPRISE FIREWALL."

Which is why 91% of the global IT decision-makers participating in a 2021 survey now consider endpoint security to be just as critical as network security.

Securing hybrid work environments has become a critical need for businesses of all kinds, and getting there requires a zero-trust approach to endpoint security. Among the benefits of such an approach: stopping attacks on an organization at their point of entry, before they can spread. This may mean, for example, isolating an attack on an end user's personal computer.

Here's how to make it work for your organization.

ZERO TRUST: TODAY'S IT IMPERATIVE

Beyond the operation of endpoint devices outside of corporate networks, research shows that user behavior also exposes them in the hybrid work context.

76% Workers who say working remotely blurs the lines between home and professional life

46% Workers who admit they use a work laptop for "life admin"

30% Employees who say they've let another person use their company device

20% Users who let someone else use a work computer multiple times a day

Source: HP Wolf Security, "Blurred Lines and Blindspots," 2021

As cybercriminals increasingly exploit vulnerabilities in the hybrid workplace, they've set their sights on the ever-growing number of endpoints such as work-from-home devices. That's why endpoint security is now a critical first line of defense. And the most effective defense begins with a zero-trust approach to endpoint security.

"THE TIME HAS COME FOR ORGANIZATIONS TO START PROTECTING AGAINST THE UNKNOWN, WHICH MEANS UTILIZING ZERO TRUST, BUT IN A WAY THAT IS TRANSPARENT TO THE USER," PRATT SAYS.

Zero trust means assuming that no hardware, software, or log-in is secure. It means verifying everything. It works by leveraging user and device identities, firmware and software configuration, and broader contextual information to make security and access decisions.

ZERO TRUST FOR ENDPOINT SECURITY

Applying a zero-trust approach to endpoints means stopping even undetectable threats. It means applying hardware-enforced isolation technology such as micro virtual machines to isolate malware.

A zero-trust approach protects end users and their organizations from high-risk actions such as:

- Opening email attachments, which can trigger ransomware and other malware to launch
- Web browsing, which can fool users into clicking malicious links
- Opening files on USB devices that can contain malware

Importantly, containment technology makes it possible for users to open any email attachment without restriction. Containment works in the background, with no need for restrictive IT policies for attachments.

"WITH EMPLOYEES WORKING REMOTELY, THE LINES BETWEEN WORK AND PERSONAL EQUIPMENT ARE BLURRED AND EVERYDAY ACTIONS—SUCH AS OPENING AN ATTACHMENT—CAN HAVE SERIOUS CONSEQUENCES," SAYS JOANNA BURKEY, CHIEF INFORMATION SECURITY OFFICER AT HP INC.

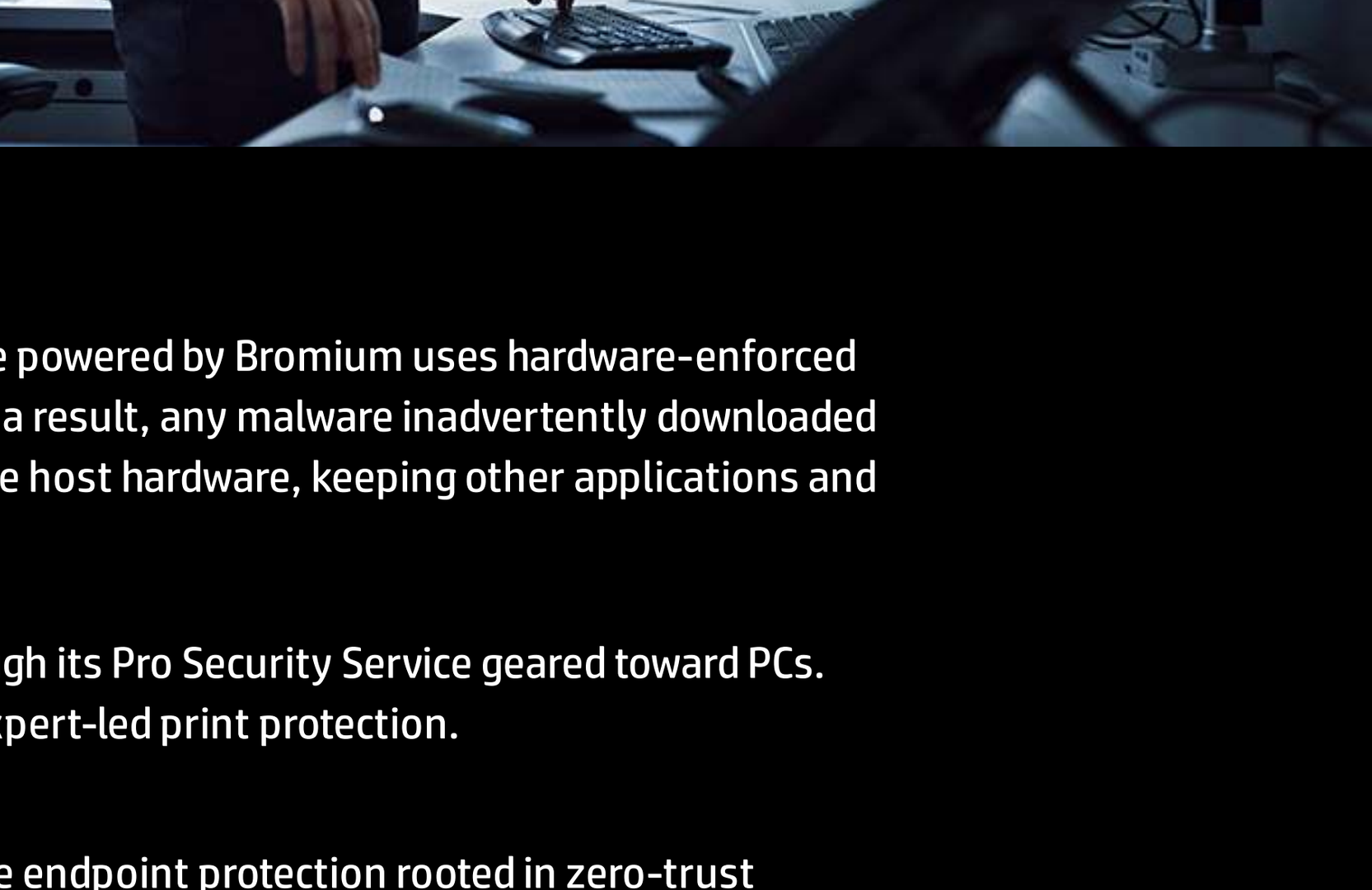
What's needed is a way to enable users to do their work without interference but keep their endpoints safe in the background. HP Wolf Security can provide such seamless protection.

ENDPOINT DEFENSE WITH HP WOLF SECURITY

With Wolf Security, HP builds on more than 20 years of endpoint security innovation, helping organizations respond to the urgent need for a new kind of endpoint security that can protect the remote workforce without hampering productivity.

"The leading technology of the future will be secure by design and intelligent enough to not simply detect threats but to contain and mitigate their impact and to recover quickly in the event of a breach, which could happen at any time, to any one of us," explains Pratt.

HP Wolf Security provides PC hardware security, print hardware security, PC security services, and enterprise security services and solutions.



For example, HP Wolf Security's Sure Click Enterprise powered by Bromium uses hardware-enforced isolation to open downloads in a virtual machine. As a result, any malware inadvertently downloaded with an attachment runs entirely separately from the host hardware, keeping other applications and data safe.

HP Wolf Security also offers threat monitoring through its Pro Security Service geared toward PCs. And its separate Managed Print Services[1] provides expert-led print protection.

Altogether, HP Wolf Security provides comprehensive endpoint protection rooted in zero-trust principles, starting at the hardware level and extending across software and services. It harnesses state-of-the-art technologies to reduce pressure on IT.

HP WOLF SECURITY DELIVERS COMPREHENSIVE PROTECTION BY:

- Shrinking the addressable attack surface through virtualization
- Enabling remote recovery from firmware attacks via self-healing firmware
- Enhancing threat data collection through cloud-based intelligence[2]
- Providing high-fidelity alerts thanks to in-memory breach detection[2]

"WITHOUT ALL OF THE PREPANDEMIC SOURCES OF VISIBILITY OF DEVICES, INCLUDING HOW THEY ARE BEING USED AND BY WHOM, IT AND SECURITY TEAMS ARE WORKING WITH CLOUDED VISION," SAYS BURKEY.

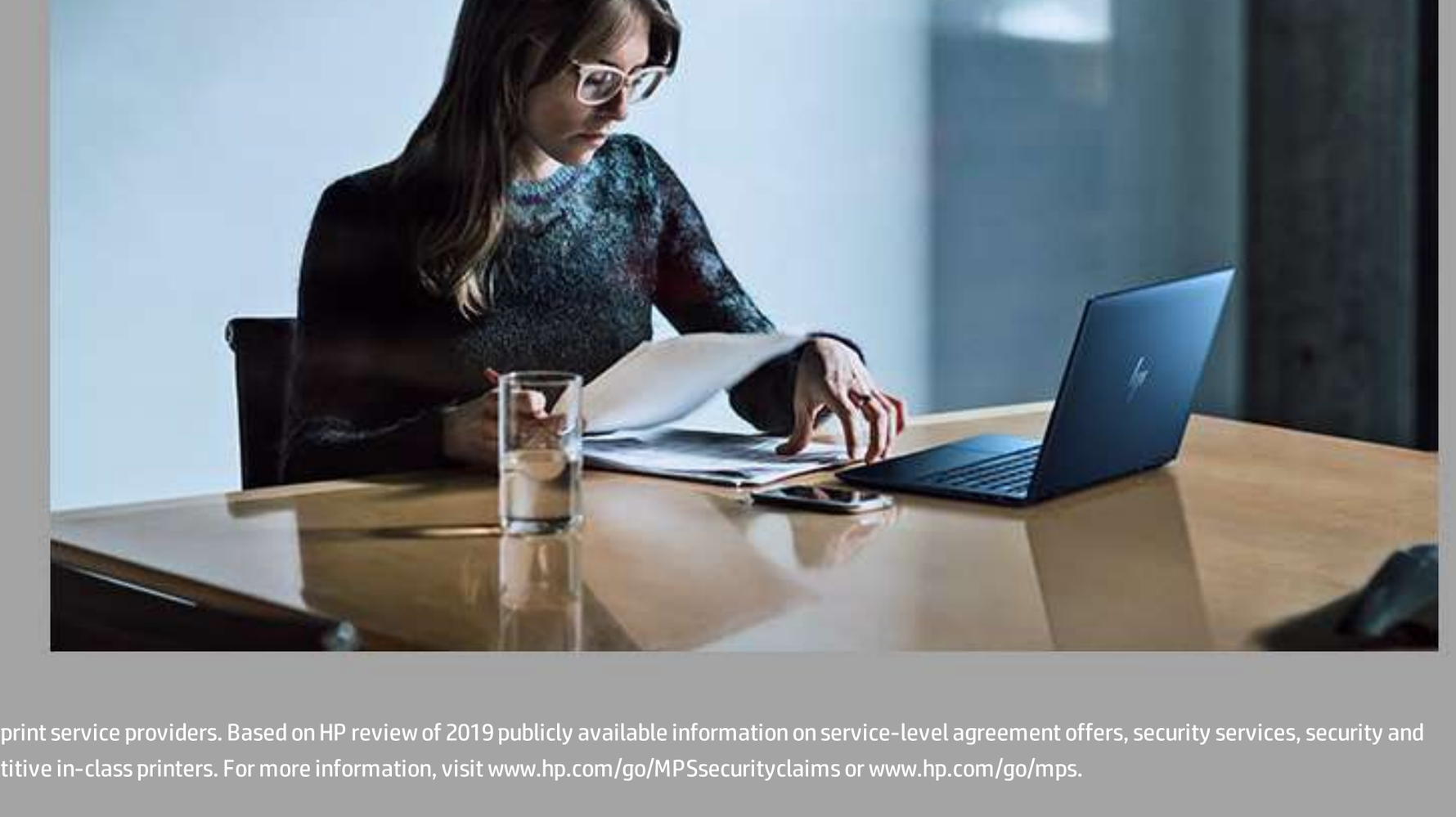
Today's hybrid work world requires a new approach to endpoint security that can secure laptops and other work devices as employees use them at home.

LEARN HOW SOME OF THE MOST SECURITY-CONSCIOUS ORGANIZATIONS IN THE WORLD SECURE THEIR ENDPOINTS BY USING ZERO-TRUST PRINCIPLES AT HP WOLF SECURITY.

LEARN HOW

ABOUT HP WOLF SECURITY

From the maker of the world's most secure PCs[3] and printers[4], HP Wolf Security is a new breed[5] of endpoint security. HP's portfolio of hardware-enforced security and endpoint-focused security services is designed to help organizations safeguard PCs, printers, and people from circling cyberpredators. HP Wolf Security provides comprehensive endpoint protection and resilience that starts at the hardware level and extends across software and services.



[1] Includes device, data, and document security capabilities by leading managed print service providers. Based on HP review of 2019 publicly available information on service-level agreement offers, security services, security and management software, and device-embedded security features of their competitive in-class printers. For more information, visit www.hp.com/go/MPSsecurityclaims or www.hp.com/go/mps.

[2] HP Sure Click Enterprise is sold separately and requires Windows 8 or 10; and Microsoft Internet Explorer, Google Chrome, Chromium, or Firefox is supported. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files, when Microsoft Office or Adobe Acrobat is installed.

[3] Based on HP's unique and comprehensive security capabilities at no additional cost among vendors on HP Elite PCs with Windows and 8th Gen and higher Intel® processors or AMD Ryzen™ 4000 processors and higher; HP ProDesk 600 G6 with Intel® 10th Gen and higher processors; and HP ProBook 600 with AMD Ryzen™ 4000 or Intel® 11th Gen processors and higher.

[4] HP's most advanced embedded security features are available on HP Enterprise and HP Managed devices with HP FutureSmart firmware 4.5 or above. Claim based on HP review of 2021 published features of competitive in-class printers. Only HP offers a combination of security features to automatically detect, stop, and recover from attacks with a self-healing reboot, in alignment with NIST SP 800-193 guidelines for device cyberresilience. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/PrinterSecurityClaims.

[5] HP Security is now HP Wolf Security. Security features vary by platform, please see product data sheet for details.