HP WOLF SECURITY

BLURRED LINES AND BLINDSPOTS

EXECUTIVE SUMMARY AND KEY FINDINGS

Of the many effects the COVID-19 pandemic has had on business, one of the most dramatic has been the way hundreds of millions of employees around the world have been forced to work from home (WfH). Within a matter of weeks in early 2020, WfH went from an occasional employee convenience to being the only way many organizations could continue to function.

The scale of this change was extraordinary. A YouGov survey of global office workers commissioned for this report by HP shows that 82% worked from home more since the start of the pandemic. This has prompted a reassessment of WfH as having compelling economic and personal benefits. It seems likely there will be a permanent change in working patterns which organizations must adapt to to maintain competitive advantage. In fact, the findings showed that 23% of office workers globally expect to predominately WfH post pandemic, and a further 16% expect to split their time equally between home- and office-based working.

However, the danger is that organizations embrace WfH without assessing how this environment amplifies existing security threats. The volume of corporate data being accessed from home has risen substantially, including sensitive financial records, putting more information at risk. All the while, the number of endpoints – personal and employer provisioned – being used to access the corporate network from beyond the traditional network perimeter has exploded.

The data in this report highlights the limitations of the perimeter security model for securing remote workers, including the burden it places on security teams. Often, endpoint devices such as laptops, PCs, and printers are left exposed, raising the chance that security incidents become invisible until damage is done. These blindspots mean many businesses could be headed for a fall.

HP Wolf Security[1] is the company's newly integrated portfolio of hardware, software, and services designed for this new normal. In this HP Wolf Security report, we provide a multi-dimensional view of the security issues at play. We combine findings from a global YouGov online survey of 8,443 office workers who have shifted to working from home during the pandemic with a global survey of 1,100 IT decision makers (ITDMs), to gain both sides of the story. The data is further enriched with real-world threat telemetry from HP Sure Click virtual machines (VMs) – which illustrates these risks – along with analysis from leading analyst firm KuppingerCole providing the global context.

Examining the issue through these different lenses, this HP Wolf Security report will discuss:

01 **How the world has changed with the emergence of the 'new office'**, looking at the acceleration of the shift to remote working and how this has placed greater emphasis on the endpoint as a first line of defense.

02 **The impact the pandemic has had on user attitudes and behaviors**, showing that employees are taking more risks than they would in the office; potentially turning them into unwitting 'friendly foes', by increasing the risk of an unintended breach.

03 **The pressure this is putting on our cybersecurity defenders as new risks emerge,** explaining that the ever-widening range of endpoints, including IoT devices, is expanding the attack surface for attackers seeking to gain a foothold in corporate networks.

04 **Why a new breed of endpoint security, such as HP Wolf Security, is needed to defend against modern threats,** demonstrating how aligning to the principles of Zero Trust will help your organization to reduce the attack surface, mitigate risk, and better support stretched IT teams.

91%

of IT decision makers (ITDMs) believe endpoint security has become as important as network security, while the same say they spend more time on endpoint security now than they did two years ago.

76%

of office workers say that working from home during COVID-19 has blurred the lines between their personal and professional lives, with half saying they now see their work device as their own personal device and 46% admitting to using their work laptop for 'life admin'.

30%

of employees have let someone else use their work device, despite 85% of ITDMs saying they worry such behavior increases their company's risk of a security breach.

54%

of ITDMs say they have seen evidence of a higher number of phishing attacks in the last year, while 45% say they have seen evidence of compromised printers being used as an attack point in the past year.

1
THE NEW OFFICE

71% OF EMPLOYEES ARE ACCESSING MORE COMPANY DATA, MORE FREQUENTLY, FROM HOME THAN THEY DID PRE-PANDEMIC.

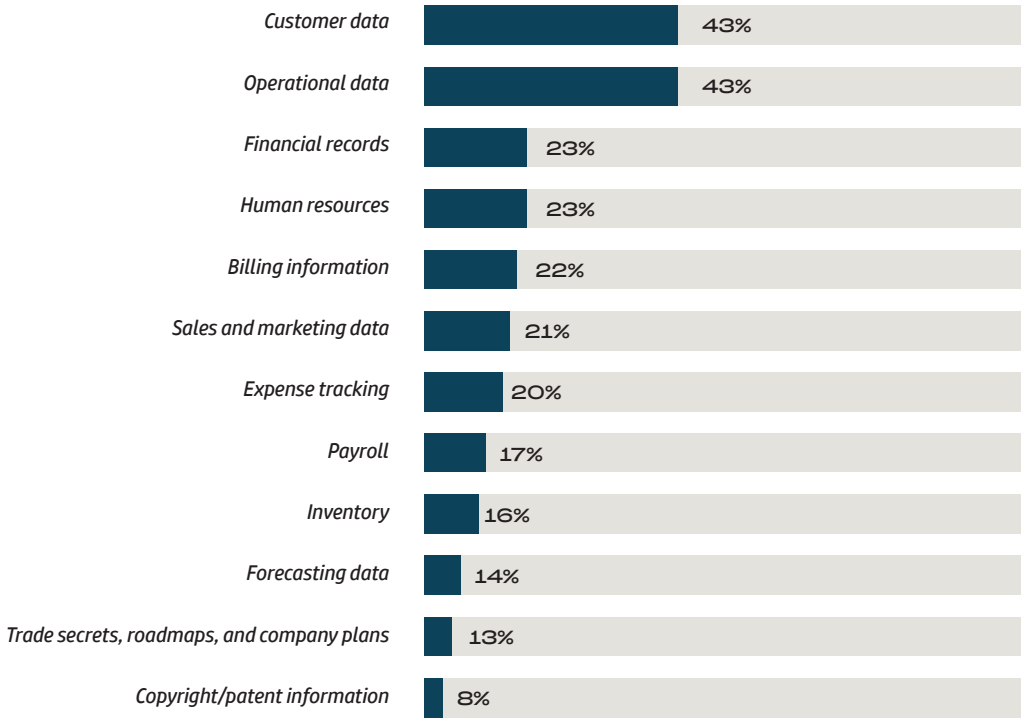
HP WOLF SECURITY VIEWPOINT:

IAN PRATT,
HEAD OF SECURITY,
PERSONAL SYSTEMS,
HP INC.:

"The traditional ways of securing access to the corporate network, applications and data are no longer fit for purpose. The perimeter has become obsolete. Over the years the workforce has become more dispersed, and SaaS adoption has risen – this means critical data is being hosted outside the enterprise firewall. 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."

BETWEEN FEBRUARY AND APRIL 2020 THERE WAS A 238% INCREASE IN GLOBAL CYBERATTACK VOLUME.

While the pandemic did not start the trend to WfH and hybrid home-office working, it has hugely accelerated it, packing what might have been a decade's worth of sedate evolution towards a more remote and mobile workforce into a few months. An inevitable outcome of this has been the increasing need for workers to access corporate data remotely. This HP Wolf Security report found that 71% of office workers surveyed are accessing more company data, more frequently, from home than they did pre-pandemic – with the most common types of data being accessed including:



Cybercriminals have been quick to capitalize on the chaos. As with the pandemic, cyberattacks appeared in waves, starting with an early phase where criminals realized organizational defenses were more vulnerable to attack than usual. According to figures from the World Economic Forum (WEF), between February and April 2020 there was a 238% increase in global cyberattack volume.

Fending off such attackers has become increasingly difficult, as distributed workers are no longer protected by the corporate firewall, with many accessing critical data via insecure connections. Of respondents in the ITDM survey, 89% are concerned that employees are not using a secure connection, such as a VPN.

SOME INDUSTRY SECTORS WERE MORE TARGETED THAN OTHERS:

50% spike in attacks on the healthcare sector between February and May, with the World Health Organization (WHO) reporting a 400% increase in cyberattacks during the same period.

Cyberattacks against education increased by 33% from 2019 to 2020.

Gaming saw a 54% rise in phishing attacks in the first months of 2020.

91% OF ITDMs SAY THEY SPEND MORE OF THEIR TIME ON ENDPOINT SECURITY THAN THEY DID TWO YEARS AGO.

As a result, the perimeter has shifted from the network to the endpoint. The survey of ITDMs revealed that 91% believe endpoint security has become as important as network security now that more employees are working from home. A further 90% of ITDMs agreed the pandemic experience of 2020 has highlighted the growing importance of strong endpoint security in defending the increasingly perimeter-less organization; 91% say they spend more of their time on endpoint security than they did two years ago.

Figure 1 - Percentage of ITDMs by country that believe endpoint security has become just as important as network security because of more work from home employees

GLOBAL	CANADA	MEXICO	USA	GERMANY	UK	JAPAN	AUSTRALIA
91%	91%	97%	92%	85%	91%	92%	92%

MORE THAN HALF (56%) OF PRINTERS ARE ACCESSIBLE VIA OFTEN-USED OPEN PRINTER PORTS THAT COULD BE HACKED.

The nature of the endpoint is constantly evolving and diversifying. According to KuppingerCole: *"The many connected devices that employees use in their working from home environment have contributed to the breakdown of the corporate IT infrastructure and network, including printers."* Home environments are now full of devices targeted by cybercriminals, such as Internet of Things (IoT) devices, which KuppingerCole noted are notorious for weak security design. This includes printers, which are often overlooked by security teams, with a 2020 study cited by KuppingerCole finding that more than half (56%) are accessible via often-used open printer ports that could be hacked.

2

THE FRIENDLY FOE DILEMMA

HP VIEWPOINT:

JOANNA BURKEY, CHIEF INFORMATION SECURITY OFFICER (CISO), HP INC.:

"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. Without all of the pre-pandemic sources of visibility of devices, including how they are being used and by who, IT and security teams are working with clouded vision."

OF THOSE THAT HAVE SHARED THEIR DEVICE, 27% SAID THEY KNOW THEY ARE NOT MEANT TO, BUT THEY FEEL THEY 'HAD NO CHOICE' DUE TO THESE BEING EXCEPTIONAL TIMES.

The shift to home working has changed the nature and scale of cybersecurity risk. In many organizations, this has not yet been fully appreciated, often because it's less visible or underestimated. An interesting facet of this has been culture change. A device used in the office lives a relatively tame existence; take the same device to the home environment and everything changes. At home, employees do things they would never do in the office, which can quickly multiply cybersecurity risks in ways that can be hard to keep tabs on.

Illustrative of this issue, this HP Wolf Security report shows that 76% of office workers surveyed say that WfH during COVID-19 has blurred the lines between their personal and professional lives, in effect merging work and home into a single environment. When asked about how this affects their use of corporate devices, 50% agree that they now think of their work laptop as a personal device.

Figure 2 - Percentage of office workers by country that say COVID-19 has led to them working from home, blurring the lines between personal and professional lives

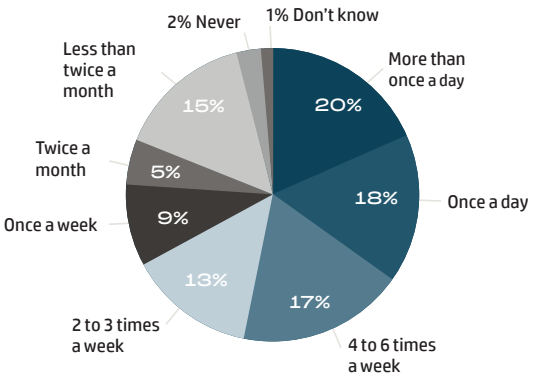
GLOBAL	CANADA	MEXICO	USA	GERMANY	UK	JAPAN	AUSTRALIA
76%	78%	84%	77%	78%	79%	62%	77%

Further to this, and potentially more concerning, 30% admit they have allowed someone other than themselves – e.g., a partner, child, or friend – to use their work laptop; often more than once a day. Of those that have shared their device, 27% say they know they are not meant to, but they feel they 'had no choice' due to these being exceptional times.

Figure 3

Region	% of office workers that say since working from home, they have started to regard their work notebook/laptop as both their work ***and*** personal notebook/laptop	% of office workers that say someone else besides themselves has used their work laptop or PC in the last year
GLOBAL	50%	30%
CANADA	63%	37%
MEXICO	79%	55%
USA	53%	31%
GERMANY	30%	16%
UK	33%	12%
JAPAN	35%	21%
AUSTRALIA	59%	34%

Figure 4 - How often, on average, work PCs or laptops are used by someone else



84% OF ITDMs ARE CONCERNED THAT EMPLOYEES USING THEIR WORK DEVICES FOR PERSONAL TASKS DURING THE PANDEMIC HAS INCREASED THEIR COMPANY'S RISK OF A SECURITY BREACH.

The effect of this ownership psychology is that employees become less wary of security risks, meaning work devices are being increasingly used for a growing range of personal tasks – 84% of ITDMs are concerned that employees using their work devices for personal tasks during the pandemic has increased their company's risk of a security breach.

When asked, ITDMs estimate that around a third (33%) of their employees are using their work computer for personal things (e.g., playing games, browsing for fun), when in reality this number is much higher. 70% of office workers surveyed admit to using their work device or letting someone else use their device for personal tasks – with 46% admitting to using their work laptop for 'life admin', a figure that rose to 61% for 25 to 34-year-olds. Four in ten office workers surveyed admit to using their work device for homework and online learning, which rises to 57% for parents of children aged 5 to 16.

Other risky behaviors weren't hard to find. Office workers surveyed (or members of their household) were found to have used work laptops for the following personal tasks:

- *Downloading from the internet: 33%*
- *Opening personal email attachments or web pages: 55%*
- *Visiting personal social media sites: 45%*
- *Making video calls: 58%*
- *Playing games: 27%*
- *Watching online streaming services: 36%*
- *Online shopping / internet browsing: 52%*

Personal email threat
During 2020, HP Sure Click and Sure Click Enterprise stopped 128 users from downloading malicious files from personal webmail services that lack enterprise email filtering, including Emotet malware and ransomware.

KuppingerCole analysis supports this, showing:

- 36% increase in global gaming playtime in 2020. Game downloads increased by up to 80%, depending on recent game releases.
- Malicious actors who exploited popular gaming platforms increased by 54% between January and April 2020, often directing users to phishing pages.

Gaming-themed threats

In 2020, Sure Click and Sure Click Enterprise telemetry saw an increase in gaming-themed malware, particularly popular titles such as Fortnite and Among Us.

- A notable example was Ryuk ransomware themed as Fortnite cheats ('FreeHacks4Fortnite.exe'). Sure Click Enterprise identified users downloading and running files from Mega, a file sharing website. Sure Click Enterprise successfully isolated the files and prevented the malware from encrypting the device.

In February 2021, Sure Click isolated samples of a stealthy JavaScript malware downloader called Gootloader

- It received very low detection rates on VirusTotal, often evading all detection engines
- Some samples masqueraded as Fortnite hacks
- Delivered in zip archives
- Final payloads were Gootkit (banking Trojan) or REvil (ransomware)

Streaming threats
According to KuppingerCole analysis, streaming services were also targeted during the pandemic, with at least 700 fraudulent websites impersonating popular streaming services being identified in a 7-day period in April 2020. Phishing scams that targeted Netflix users increased 60% over 2019. Phishing URLs that targeted Netflix increased 646% over 2019, URLs that targeted Twitch increased 337%, targeting HBO increased 525%, and targeting YouTube increased 3,064%.

69% OF OFFICE WORKERS HAVE USED THEIR PERSONAL LAPTOP OR PERSONAL PRINTER/SCANNER FOR WORK ACTIVITIES SINCE THE START OF THE PANDEMIC.

Another clear trend has been for employees to access corporate networks using personal devices. When asked, ITDMs estimate that just over half (53%) of their workers are using personal devices for work-related tasks. Again, the real figure is higher – this HP Wolf Security report shows that 69% of office workers surveyed have used their personal laptop or personal printer/scanner for work activities since the start of the pandemic. They have been using personal devices for a wide range of tasks more often in the past year, including:

- *34% use their home printer to scan and share documents with colleagues and customers*
- *21% use their home printer to save files to the network over the VPN*
- *37% use their personal PC/laptop to access work applications*
- *35% use their personal PC/laptop to save work documents*
- *27% use their mobile phone to send work documents to a home printer*
- *32% use their personal PC/laptop to access the main corporate network*

3

THE THREAT EXPLOSION

The danger of this behavioral aspect of technology is that organizations end up being subjected to risks they can no longer see. Anxiety about this is clear within HP Wolf Security's global ITDM survey, with more than a third (35%) stating that a lack of control over how corporate devices are being used and by whom is one of their biggest challenges at present. ITDMs expressed several concerns relating to new employee behavior that they felt are increasing organizational risk, including:

- 85% are concerned that employees letting others (children, partners, housemates, etc.) use their work devices has increased their company's risk of a security breach.
- 88% are concerned that employees downloading software (to do their jobs) which is not approved by IT has increased their company's risk of a security breach.
- 88% are worried that the risk of a breach has risen because employees are using personal devices for work that were not built with business security in mind.

Figure 5

Region	% of ITDMs who believe employees letting others use their work devices has increased their company's risk of a security breach	% of ITDMs who believe employees downloading software (to do their jobs) which is not approved by IT has increased their company's risk of a security breach	% of ITDMs who believe employees using personal devices for work, despite them not being built with business security in mind, has increased their company's risk of a security breach
GLOBAL	85%	88%	88%
CANADA	91%	97%	95%
MEXICO	87%	95%	93%
USA	83%	87%	89%
GERMANY	67%	72%	71%
UK	87%	89%	87%
JAPAN	94%	93%	93%
AUSTRALIA	83%	87%	89%

HP WOLF SECURITY VIEWPOINT:

ROZ HO, GLOBAL HEAD OF SOFTWARE, HP INC.:

"As companies extend corporate offices into the home environment, print security must no longer be a blindspot. The scenario of a printer being used to infect the wider corporate network is a very real potential. 45% of IT decision makers say they have seen evidence in their company of compromised printers being used as an attack point in the past year. It's time companies woke up to this problem and protected themselves against printer-based attacks."

And they are right to be concerned. Of those surveyed, 51% of ITDMs said they had seen evidence of compromised personal devices being used to access company and customer data in the past year, while 45% had seen evidence of compromised printers being used as an attack point in the past year.

Furthermore, 54% of ITDMs reported they had seen evidence in their organization of a higher number of phishing related attacks in the last year, while 56% had seen evidence of an increase in web browser-related infections, and 51% said they had found users using unpatched endpoints in the last year.

Figure 6 - Percentage of ITDMs that have seen evidence of these security breaches in the past year

Increase in phishing related infections	54%
Increase in web browser related infections	56%
Compromised devices being used to infect the wider business	44%
Compromised personal devices being used to access company and customer data	51%
Users using unpatched machines	51%
Compromised printers being used as an attack point	45%

ADAPTING TO THE NEW NORMAL

HP WOLF SECURITY REPORT FINDINGS SUMMARY:

- The pandemic has accelerated the trend for more employees to work from home (WfH), which represents a permanent change.
- The WfH environment is different in terms of security, where employees take more risks than they would in the office, such as using insecure devices, sharing devices with family and friends, and using work devices for their personal lives.
- Attackers have spotted this vulnerability and are now targeting home workers by using dedicated malware campaigns exploiting social engineering. This places a burden on already stretched IT security teams, while effectively making many WfH risks invisible.
- This has exposed the limitations of the current endpoint security approach, which is based on assumptions about trust inherited from the era of perimeter security. When a compromise happens under this model, it is often not visible until serious damage has occurred.

The big question remains: in a world where people can work from anywhere, how do we build the distributed, hybrid workforce of the future, without exposing the enterprise to an increased level of cyber risk? An employee lending their child their work laptop to download games could be considered reckless but also understandable as people try to juggle home life with work, and it is clear from the data they are not alone. This is about more than a single moment in time. While the pandemic has spurred businesses into action and accelerated the shift to WfH, the pandemic is likely to have changed the way people work forever. Organizations must quickly assess how they manage this risk in this new normal and enable workforce mobility and security at the same time.

FINAL THOUGHTS FROM HP WOLF SECURITY

A NEW APPROACH IS NEEDED

Cybercriminals are more sophisticated, organized, and determined than ever. Digital and data transformation is widening the attack surface. Despite their best efforts, overstretched IT and security teams are struggling to keep up. Against this backdrop, endpoint security is more vital than ever as the first line of defense. If an employee can be tricked into bypassing a control, ignoring a warning, or simply being careless, then it's as if that control doesn't exist. When security fails, it often fails badly, allowing attackers to gain a foothold in systems, exfiltrate data, spy, and disrupt at will. This is not new, but the advent of WfH exposes the problem on a new scale.

The extreme fix to this is to resort to the technological equivalent of lockdown. Access is restricted, layers of authentication are added in an uncoordinated way, and device usage is constrained by optimistic policies. With WfH, this quickly causes problems, hurting employee productivity and reinforcing the idea that security gets in the way.

The alternative, often championed by the industry, is 'detect to protect', looking for signatures and codes known to be bad. However, the rise in 'polymorphic' auto-generated malware – i.e., machine-generated malware – frustrates such approaches. The next generation of detection tries to address this by using machine learning to spot possible mutations, but malware developers have access to these tools; they can automatically test their code and tweak it until it evades detection, giving them confidence it will stay off the radar. Some attacks always slip through the net.

APPLYING ZERO TRUST PRINCIPLES

Re-balancing the need for security against the needs of the worker requires a completely different model of endpoint and WfH security. Built on the principles of Zero Trust, which states that nothing should be trusted implicitly, access to resources should be assessed based on context – e.g., user, device, location, and security posture. Critically, this applies not only to individual devices but to different elements on the endpoint itself, including firmware, application security, the integrity of the OS, and the account or user accessing data.

A more distributed, digital world doesn't have to mean a more vulnerable world. As the cyber world constantly evolves, so must cybersecurity. The technology of the near future will be secure by design and intelligent enough to not simply detect threats, but to contain and mitigate their impact, as well as to recover quickly in the event of a breach. Helping our customers safely navigate this dynamic digital ecosystem is what drives us at HP.

HP WOLF SECURITY – A NEW BREED OF ENDPOINT SECURITY[1]

With this front of mind, HP is introducing HP Wolf Security – our newly integrated portfolio of secure by design PCs and printers, hardware-enforced endpoint security software, and endpoint security services – to help customers navigate this challenging landscape and to defend against the plethora of new attacks and risks related to our increasingly distributed way of life. The HP Wolf Security platform builds on over 20 years of security research and innovation to offer a unified portfolio for customers focused on delivering comprehensive endpoint protection and cyber-resiliency.

Rooted in Zero Trust principles, HP Wolf Security provides defense-in-depth and enhanced protection, privacy, and threat intelligence, gathering data at the endpoint to help protect the business at large.

HP Wolf Security helps organizations to defend against both known and unknown threats – even Zero Day vulnerabilities. Combining hardware-enforced software and security features with industry-leading endpoint security services, HP Wolf Security implements layered security and enables seamless integrations with the wider security stack. As such, customers benefit from robust, built-in protection from the silicon to the cloud, from the BIOS to the browser.

For too long, the endpoint has been seen as a victim, outclassed by adversaries that could only be contained using network detection. This was always optimistic. Once a threat escapes from the endpoint, the danger it poses is hugely magnified. The right place to stop threats is exactly where they occur, in the specific layer of software that was compromised. No attack should ever be able to leave a compromised endpoint with powerful privileges.

HP Wolf Security helps to defend businesses against threats relating to remote working, and will continue to bring out new security features to help users stay ahead of evolving threats. Examples today include:

- **Defend mission-critical applications from cyber threats:** New to HP Wolf Enterprise Security is Sure Access Enterprise[2], which applies HP's unique isolation technology to ensure critical applications are completely safeguarded from any malware lurking on a user's PC. HP Sure Access creates hardware-enforced micro virtual machines (VM) that can protect key applications – forming a virtual air gap between the application and the host PC. The application and data is securely isolated from the host OS, and any malicious actors that may have breached it.

- **Render malware harmless through threat containment and isolation:** Hardware-powered micro-virtualization performs full isolation of threats delivered via the most common threat vectors – email, browser, and downloads – without impacting user experience. When a task is closed, the micro-VM – and any threat it contained – is disposed of, without any breach. So even if a user does click on something bad, the attacker has nowhere to go and nothing to steal.

- **Recover quickly from remote firmware attacks, while reducing pressure on IT:** Easily overlooked, printers and scanners and their misuse represent a growing security threat. HP Wolf Security solves this problem by allowing full visibility and management of every software layer inside printers, including the ability to upgrade firmware and self-heal should this be tampered with by malware. Instant-on security immediately configures devices to a corporate security policy when they are added to a network. HP Security Manager makes it possible to maintain more than 200 security settings for supported models.

- **Using threat telemetry to turn a traditional weakness – the endpoint – into an intelligence gathering strength:** Capture unique threat data by allowing attacks to play out in full in a safe and contained environment, helping you to better understand the threats facing your business. Use cloud-based intelligence and data gathered via endpoints to enhance threat data collection, while gaining a more rounded view of your business' security posture by automating alerts from your IoT print devices into your Security Information and Event Management (SIEM) system.

All this leads back to HP's overriding purpose: We are here to reduce the ever-growing pressure on IT and security teams as they navigate unprecedented levels of cyber risk, and to help their users and customers so they can continue to work safely from home or remotely. Go to HP Wolf Security's home page to find out more.

METHODOLOGY

The findings in this report are made up from four separate data sources:

01 A YouGov online survey of 8,443 adults in the US, the UK, Mexico, Germany, Australia, Canada, and Japan who used to be office workers, and worked from home the same amount or more than before the pandemic. Fieldwork was undertaken between 17th and 25th March 2021. The survey was carried out online.

02 A Toluna survey of 1,100 IT decision makers in the US, the UK, Mexico, Germany, Australia, Canada, and Japan. Respondents work at organizations with 50-99 employees (25%), 100-499 employees (26%), 500-999 employees (26%) and 1000+ employees (24%). Fieldwork was undertaken between 19th March and 6th April 2021. The survey was carried out online.

03 *The 2020 Cybersecurity Threat Landscape for Remote Workers as a Result of the COVID-19 Pandemic* report from KuppingerCole, conducted in March 2021. This provides context and analysis of the changing work landscape in 2020 as a result of the COVID-19 pandemic with attention to the activities and practices of companies and employees globally, as well as the activities and tendencies of malicious actors to vulnerabilities that arose because of the changing context.

04 Threat data captured within HP customer's Sure Click Virtual Machines, and analysis from the HP Threat Intelligence team.

DISCLAIMERS

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

[2] 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, please visit www.hpdaas.com/requirements.

HP WOLF SECURITY