HP WOLF SECURITY

REBELLIONS & REJECTIONS REPORT

HP WOLF SECURITY

EXECUTIVE SUMMARY AND KEY FINDINGS

HP WOLF SECURITY VIEWPOINT:

JOANNA BURKEY, CHIEF INFORMATION SECURITY OFFICER, HP INC.:

"As the old world of work that operated largely within established security perimeters gives way to a post-pandemic hybrid model of distributed working, the organizations that will come out on top will be the ones that accept and adapt to change – rather than fighting the inevitable. This won't be a pain-free process. It will require strong leadership and communication. Cybersecurity teams will need to prioritize security that is fit for purpose in the new hybrid workplace while users will need to take on more accountability for their company's security."

The global pandemic forced organizations to pivot rapidly from an office-based workforce model to one in which dynamic, hybrid working is the norm. This new way of working isn't a short-term trend. According to our HP Wolf Security Blurred Lines and Blindspots report, 23% of office workers globally expect to predominantly work from home post-pandemic, with an additional 16% expecting to split their time equally between home and the office. This will have far-reaching consequences for organizations across all economies.

During the pandemic, businesses have been forced to transform in a matter of days and have been able to do so largely using digital technologies. But what is often forgotten is that digital innovation is impossible without security. Despite their essential role in enabling the business, security teams have been left feeling rejected by rebellious employees who resent new restrictions being placed on them.

Amid the chaos of a workforce sent home to do their jobs, a second and less remarked upon pandemic was quietly unfolding – cybercrime. Evidence of this onslaught emerged from many quarters. According to an analysis from KuppingerCole, globally in 2020, endpoints connected to the internet experienced 1.5 attacks per minute.

Unfortunately, this period of cybercriminal innovation and creativity coincided with a time when businesses were in flux and having to act quickly to maintain business continuity. This created a worrying cocktail of increased cybercriminal activity, reduced visibility for security, and an increasingly distributed workforce working outside the range of IT.

Navigating a path through this new maze will be a huge challenge for security leaders. And it cannot be done in a vacuum. Users have a new set of expectations around the technology they use every day to do their jobs and are looking for a seamless experience that doesn't hinder their workflow. They expect things to work quickly and refuse to be encumbered, especially younger generations. As a result, Cybersecurity teams have been facing an uphill battle trying to secure the increasingly perimeter-less workplace and become burned out and dejected when their efforts are ignored. Building bridges between users and Cybersecurity teams will play an important part in securing the future of work.

Security leadership has never been so important, and the role of the Chief Information Security Officer (CISO) is evolving now that cybersecurity is at the top of the boardroom agenda. The most successful CISOs will tap into a broad range of skills to ensure that risk is communicated and understood so that it can be managed effectively. Key to this will be ensuring that a positive security culture is rooted into the organization and embraced by all. Security processes will be designed with usability and business continuity in mind, while Cybersecurity teams will be armed with the most advanced security tools to improve visibility and enable remote management. They will be positioned as security partners, not security enforcers.

In this second HP Wolf Security report, we gather data from a global YouGov online survey of 8,443 office workers who shifted to Working from Home (WFH) during the pandemic; a global survey of 1,100 IT decision-makers (IT teams), and analysis from leading analyst firm KuppingerCole. The report looks at the current breakdown in the relationship between workers and security teams, highlighting the need for change.

In this HP Wolf Security report, we will explore:

- **User friction giving rise to rebellion:** Our data shows a significant proportion of employees are unsure about security policies. Many see security as a hindrance and have tried to bypass security technologies and controls while WFH. This is particularly true of 18 to 24-year-olds – our future workforce – reflecting a concerning trend that must not be ignored.

- **Compromise, risk, and rejection:** The data also shows that Cybersecurity teams can see an iceberg looming ahead in the form of a data breach but feel unheard when they raise an alarm. They're under pressure to compromise security best practices to enable business continuity at a time of reduced policy compliance, less visibility, and greater cyber risk.

- **The CISOs role in building bridges across the enterprise:** Without intervention, friction and risk could escalate. Security leaders are now tasked with paving the way for a dynamic, flexible, and secure workforce. CISOs play a positive role in turning strained relationships between Cybersecurity teams and employees into partnerships that drive success. More than ever, CISOs will lean in on their negotiation, communication, and people management skills.

KEY STATS

OFFICE WORKER REBELLIONS

Apathy

39% of office workers surveyed aged 18-24 were unsure of the existing data security policies in place at their work

36% of office workers surveyed had been given training on how to protect their home network

54% of office workers surveyed aged 18-24 were more worried about deadlines than exposing the business to a data breach

Frustration

48% of office workers surveyed aged 18-24 thought security policies are a hindrance

37% of office workers surveyed said security policies and technologies are too restrictive

48% of office workers surveyed said security measures result in a lot of wasted time

Circumvention

31% of office workers surveyed aged 18-24 had tried to circumvent security

KEY STATS

IT TEAM REJECTIONS

Compromise

76% of IT teams said security took a back seat to continuity during the pandemic

91% of IT teams felt pressure to compromise security for business continuity

83% of IT teams believed home working has become a "ticking time bomb" for a network breach

Restriction

91% of IT teams updated security policies to account for WFH

78% of IT teams restricted access to websites and applications

Dejection

80% of IT teams experienced pushback from users as a result

80% of IT teams said IT security has become a "thankless task"

69% of IT teams said they're made to feel like the "bad guys" for imposing restrictions on employees

IS APATHY AND FRUSTRATION GIVING RISE TO REBELLION?

The global shift to remote working has impacted everyone – from the boardroom to the frontline, we've all had to adapt. It's been stressful but, overall, remarkable how well people have pulled together in the crisis.

And yet disruption and change can create tension and exacerbate friction. Three themes emerge strongly from YouGov's global study of office workers:

- Firstly, the degree to which home workers have been feeling disengaged and apathetic about cybersecurity; potentially due to lack of communication and training.
- Secondly, the negative effect that security policies and tools to help manage remote working risks have had on worker productivity and the friction this has created.
- Thirdly, and most worryingly, the fact that workers are circumventing security to get their work done, beyond Cybersecurity's purview.

The lack of security awareness among workers is striking, particularly among the younger generation. When asked how clearly they understood policies and guidelines for working securely from home, 39% of office workers surveyed aged 18 to 24 said they were either unclear about security policies or unaware of them altogether. This was 10% higher than the global average across all age groups (29%). Considering that this negligence leads to countless entry points for attackers which can consequently escalate into major cyber incidents, these figures are far from reassuring.

When working from home, employees face greater security risks. This puts the home network and the endpoints that populate it into greater focus. According to analysis from KuppingerCole, a breakdown in IT infrastructure and networks due to WFH initiatives are now a top worry for global risk professionals. In addition, a study from the European Union cited by KuppingerCole found that during 2020 40% of European employees experienced security issues in their WFH environments.

Figure 1 – Percentage of office workers by country that received additional user training on how to protect their home network since WFH

GLOBAL	CANADA	MEXICO	USA	GERMANY	UK	JAPAN	AUSTRALIA
36%	44%	50%	38%	27%	23%	30%	42%

HP WOLF SECURITY VIEWPOINT:

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

"The fact that workers are actively circumventing security should be a worry for any CISO – this is how breaches can be born. If security is too cumbersome and weighs people down, then people will find a way around it. Instead, security should fit as much as possible into existing working patterns and flows, with technology that is unobtrusive, secure by design, and user intuitive. Ultimately, we need to make it as easy to work securely as it is to work insecurely, and we can do this by building security into systems from the ground up."

54% OF OFFICE WORKERS AGED 18-24 WERE MORE WORRIED ABOUT DEADLINES THAN EXPOSING THE BUSINESS TO A DATA BREACH.

31% OF OFFICE WORKERS AGED 18-24 HAD TRIED TO BYPASS CORPORATE SECURITY POLICIES TO GET THEIR WORK DONE.

Despite this, 64% of office workers surveyed were given no additional training on how to protect their home network. Geographical differences were striking. The UK came bottom with only 23% of employees receiving this type of training, while Japan fared only slightly better at 30%, compared to the US (38%) and Canada (44%). Moreover, only 36% of employees received additional technical resources (e.g., secure Wi-Fi networks) to help them work securely from home.

This lack of cybersecurity engagement is contributing to a widespread feeling of apathy among workers. Overall, 36% of office workers surveyed felt that meeting deadlines is a more important concern than worrying about whether the risks they might be taking are exposing their organization to a data breach. A further 8% were unsure which should take priority, suggesting a clear level of apathy. Again, these figures are more disconcerting when looking at younger respondents: more than half (54%) of 18 to 24-year-olds think their deadlines are more important than a data breach, with 9% feeling unsure. This suggests a lack of understanding or concern about the important role security plays within their organization, or the part they can play as employees in protecting their organization from attacks.

Figure 2 – Percentage of office workers by age group that agree security tools are often more of a hindrance than a help

GLOBAL	18-24	25-34	35-44	45-54	55+
34%	48%	40%	35%	31%	23%

Another major finding was that office workers believed security policies and technologies get in the way of their day-to-day work. On average, over a third (34%) of office workers globally said they see security as a hindrance. Again, this was especially true for younger employees, with 48% of 18 to 24-year-olds and 40% of 25 to 34-year-olds making the same point.

When asked about the problem more specifically, 37% of employees thought that security policies and technologies are often too restrictive. Meanwhile, 48% agreed that seemingly essential security measures result in a lot of wasted time; especially when working from home. This rose to 64% among office workers aged 18-24. Of those that felt security wasted their time, 82% estimated they waste 2 to 6 hours a month on onerous security measures, while 18% say they wasted more than 6 hours each month.

Unsurprisingly, 16% of office workers surveyed admitted to circumventing such restrictions by trying to bypass corporate security policies to get their work done more easily. This rose to 31% among employees aged 18 to 24.

COMPROMISE, RISKS, AND REJECTION

The quick gear shift in digital transformation has saved businesses, jobs, and even lives. It has enabled organizations to not just survive but thrive. It has also ushered in an era of digital creativity, as people uncovered innovative and novel ways to build new pandemic-friendly experiences, many of which will be here to stay.

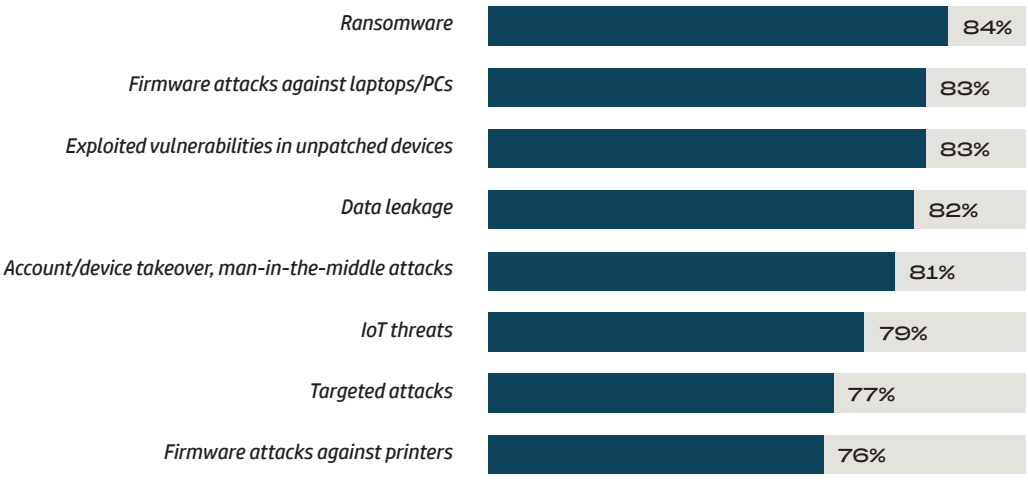
However, businesses are not the only ones that have been innovating – cybercriminals have too. Three themes emerge from Toluna's survey of IT teams:

- Firstly, the variety and scale of threats facing organizations has meant Cybersecurity teams have been working harder than ever to keep the business safe but are now feeling burned out.
- Secondly, Cybersecurity teams have had to compromise security for business continuity, with many feeling like they're in a catch-22 situation.
- Thirdly, Cybersecurity teams have had to cope with workers pushing back on their efforts to keep the business secure.

Cybersecurity teams have been faced with a rising wave of threats from increasingly effective adversaries. New policies and greater restrictions are being rejected. As a result, 83% of IT teams surveyed for this report believed home working has become a "ticking time bomb" that might lead to a corporate network breach.

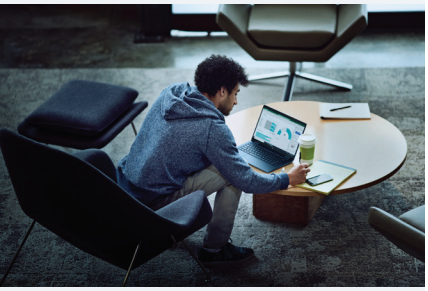
When asked about the type and significance of threats that businesses are now facing, 84% of IT teams saw ransomware as representing a significant or very significant risk. Other threats posed included: unpatched vulnerabilities and firmware attacks on laptops (83%), data leakage (82%), account/device takeover (81%), targeted attacks and man-in-the-middle attacks (79%), IoT threats (77%), and printer firmware attacks (76%).

Figure 3– Level of threat IT teams believe the following attack methods pose with people increasingly working from home on potentially insecure networks



Yet, despite the increasing level of threat, 76% of IT teams felt security had been forced to take a back seat to business continuity during the pandemic. The same percentage felt they're in a no-win situation where they're being told to lock down security while being pressured to create shortcuts to enable innovation. And almost all (91%) felt pressured to compromise security if it benefitted business continuity, including 50% who described that as "significant" pressure.

91% OF IT TEAMS FELT PRESSURE TO COMPROMISE SECURITY IF IT BENEFITTED BUSINESS CONTINUITY.



HP WOLF SECURITY VIEWPOINT:

JOANNA BURKEY, CHIEF INFORMATION SECURITY OFFICER, HP INC.:

"CISOs are dealing with an increasing volume, velocity and severity of attacks. Their teams are having to work around the clock to keep the business safe, while facilitating mass digital transformation with reduced visibility, while employees haven't quite reconciled their role in helping to secure the enterprise. Security has to become a shared responsibility across the business, with each individual understanding the important role they have to play."

69% OF IT TEAMS SAY THEY SOMETIMES FEEL LIKE THEY ARE MADE TO BE THE BAD GUY AS THEY HAVE TO BE THE ONE TO TELL USERS "NO".

Figure 4 – Percentage of IT teams by country that believe security has sometimes had to take a backseat to business continuity during the pandemic

	GLOBAL	CANADA	MEXICO	USA	GERMANY	UK	JAPAN	AUSTRALIA
YES, SIGNIFICANT PRESSURE	50%	57%	55%	43%	32%	62%	55%	48%
YES, SOME PRESSURE	41%	37%	41%	44%	49%	33%	38%	48%

Naturally, such a compromise cannot continue. The new world will need to be secure and dynamic: it cannot be an either-or situation. But retrospectively correcting past mistakes or cutting corners may not be straightforward. Now that the genie is out of the bottle, it will be impossible to put it back in. Employees will expect to continue with the same level of freedom they have enjoyed.

While security teams have understandably sought ways to minimize these risks, they have been met with resistance. 91% of IT teams have updated security policies to reflect the greater volume of home working, while 78% restricted access to websites and applications for security reasons. However, of those IT teams that imposed restrictions on user access to websites and applications, 93% said users had expressed frustration that these restrictions hamper their productivity.

More broadly, 80% of IT teams surveyed reported that they had experienced pushback from workers who do not like controls being put on them at home with surprising frequency: 18% of IT teams said they experience complaints from employees that legitimate work activity is being hampered or blocked by security policy or systems daily; for 22% this was every couple of days, with a further 27% experiencing it weekly.

Ultimately, Cybersecurity teams feel like they're fighting a losing battle. 83% of IT teams said trying to set and enforce corporate policies around cybersecurity is impossible now that the lines between personal and professional lives are so blurred. A further 80% agreed that IT security was becoming a "thankless task" because home users don't listen to advice.

Figure 5 – Remote working complicates security versus convenience dilemma

IT teams have updated security policies to reflect the increased number of remote workers	91%
IT teams currently restrict access to websites and applications for security purposes	78%
IT teams agree they are experiencing pushback from users who do not like controls being put on them at home	80%
IT teams agree creating corporate policies around cybersecurity is a thankless task	80%
IT teams agree the increase in home workers has created a ticking time bomb for a corporate network breach	83%
IT teams agree trying to set and enforce corporate policies around cybersecurity is impossible now that the lines between personal and professional lives are so blurred	83%

As a result, IT security teams felt like they're being cast as the villain of the piece; 69% of respondents said they were being made to feel like the "bad guys".

SUMMARY

HP Wolf Security Rebellions & Rejections report findings summary:

- While the idea that there is friction between employees and Cybersecurity teams is not new, these issues have been exacerbated by the pandemic, which has frayed relationships further and amplified the problem.
- A significant number of office workers are feeling disengaged and apathetic to their role in defending the business.
- Many users feel irritated, encumbered, and thus rebellious when it comes to IT security – with a worrying number stepping outside of IT security boundaries.
- This makes life harder for beleaguered security teams who have been facing increasing pressure to defend the business – with many fearing that a security breach is imminent as a result.
- IT security teams have been left feeling under-appreciated, frustrated, and misunderstood when it comes to setting boundaries for users, and their role has become an impossible and thankless task.

FINAL THOUGHTS FROM HP WOLF SECURITY

A FRESH LOOK AT SECURITY POLICIES AND RESTRICTIONS TO ENSURE THEY ARE FIT FOR PURPOSE

Security is an enabler. People embrace it in their personal lives, understanding that it would be impossible to check their bank balance, shop online, communicate, do any manner of things if there was no way of securing it. The guardrails that security provides ultimately keep people safe.

However, when it comes to their working lives, people tend to focus on what security stops them from doing, rather than what it enables them to do securely. Short-sighted as this might seem, it's also understandable. In the new hybrid working model, it has been tempting for Cybersecurity to add more restrictions on employees, as work is often conducted without the protection of corporate firewalls. However, these security policies and restrictions have been designed for times when hybrid working was the exception, not the norm, and now need to be viewed through a new lens.

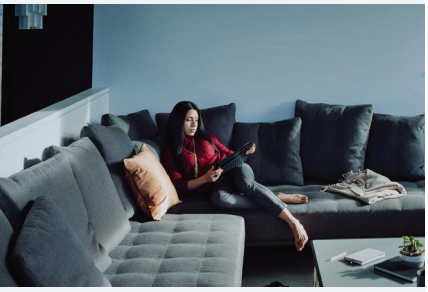
Successful CISOs are recognizing this; they are listening more to end-users and understanding how security impacts their workflows and productivity, and then re-evaluating security based on the needs of both the business and the hybrid worker.

MORE SUPPORT FOR BURNED-OUT CYBERSECURITY TEAMS

As this report shows, the pandemic has been a challenging time for security teams as cyberattacks have become more sophisticated, while the workforce has become less visible and less compliant, making it harder to defend the business.

As security teams adapt to the hybrid workplace, they are seeking out new levels of endpoint protection outside of the corporate network that also offer advanced remote management, and that are as unobtrusive as possible to avoid end-user circumvention.

Cybersecurity teams should no longer be burdened with the weight of securing the business solely on their shoulders. This responsibility must be shared in part across every employee. Until enterprises understand that cybersecurity is an end-to-end discipline, not only will they become evermore vulnerable to attack, but it will become increasingly difficult to attract or retain talent into the already vastly under-resourced cybersecurity talent pool.



HP WOLF SECURITY VIEWPOINT:

JOANNA BURKEY, CHIEF INFORMATION SECURITY OFFICER, HP INC.:

"Cybersecurity needs to be something that everyone can buy into. Cybersecurity teams need to keep the business safe, but users also need to play their part. It's like physical safety – if you have a staircase in the office, then you need to install a banister and perhaps have it carpeted instead of tiled, so people don't slip and fall. But at the same time, you're also trusting that people don't dash down the stairs three at a time and injure themselves. Cybersecurity teams can provide those guardrails, but they still need people to tread carefully. As we navigate this new era of hybrid working, I'm thinking more about how I can ensure everyone is collectively working together to keep the enterprise safe from harm."

BUILDING A MORE COLLABORATIVE SECURITY CULTURE

CISOs have been increasingly successful in driving cybersecurity higher up the boardroom agenda, emphasizing the need to include it in every aspect of corporate strategy. They now need to partner with all areas of their business to embed security into the organization's DNA.

Cybersecurity teams will need to open lines of communications with end-users. Clear, compelling communication and engaging training and education will be key to building a more collaborative security culture. Simple adjustments such as providing the rationale behind a security decision or moving away from one-way instruction to seeking user input before deploying new policies will significantly change how they are received. By building collaborative security partnerships across the workforce, cybersecurity will start to become a cultural cornerstone.

To build these bridges, CISOs will lean on a broader set of people management and communication skills that will be best found from more diverse and multi-talented teams that can inspire and promote cybersecurity and its virtues to a broader set of employees.

HP WOLF SECURITY – A NEW BREED OF ENDPOINT SECURITY

As this report shows, employees are craving user-friendly security tools and eased restrictions, while under-pressure Cybersecurity teams need to find a way to reduce the burden of security and improve visibility into user behavior and threats. Technology has a key role to play in delivering both. Helping our customers to do this in a new era of hybrid working is what drives HP.

Embedding non-intrusive security technology into the endpoint will go a long way to providing users with a better security experience while still protecting the business as needed. Endpoints, such as PCs and printers with security built-in rather than bolted on provide a more seamless end-user experience and allow for certain restrictions to be eased.

HP Wolf Security enables Cybersecurity teams to deliver user-friendly tools and help to ease restrictions, while also providing defense-in-depth and enhanced protection, privacy, and threat intelligence, gathering data at the endpoint to help protect the business at large.

Rooted in Zero Trust principles, HP Wolf Security helps to ease the burden of security. With resilient security anchored in the hardware, HP Wolf Security solutions can self-monitor and self-heal from the ground up while providing remote management capabilities to enable total visibility. This enables Cybersecurity teams to proactively mitigate the impact of threats below, in, and above the OS, while remaining transparent to the user.

HP Wolf Security combines hardware-enforced software and security features with industry-leading endpoint security services. As such, customers benefit from robust, built-in protection from the silicon to the cloud, and BIOS to browser, without restricting access to websites or preventing employees from opening email attachments. Users can go about their work uninterrupted. Examples of cutting-edge technologies that provide unobstructive protection for users today include:

- **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 attacks while reducing pressure on IT:** Easily overlooked, the misuse of printers and scanners represents 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.
- **Defend mission-critical applications from cyber threats:** HP Sure Access Enterprise[2] 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 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.
- **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.

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[1] of endpoint security. HP's portfolio of hardware-enforced security and endpoint-focused security services are designed to help organizations safeguard PCs, printers, and people from circling cyber predators. HP Wolf Security provides comprehensive endpoint protection and resiliency that starts at the hardware level and extends across software and services.

METHODOLOGY

The findings in this report are made up from two 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 March 17-25, 2021. The survey was carried out online.

02 A Toluna survey of 1,100 IT decision-makers in the UK, the US, Canada, Mexico, Germany, Australia, and Japan. Fieldwork was undertaken between March 19-April 6, 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.

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.

[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 cyber resiliency. For a list of compatible products, visit: hp.com/go/PrintersThatProtect. For more information, visit: hp.com/go/PrinterSecurityClaims.

HP WOLF SECURITY