HP WOLF SECURITY

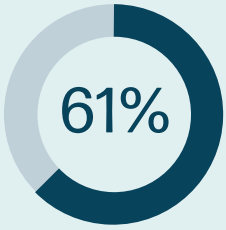
# A New Era: Securing the Hybrid Workforce

AN HP WOLF SECURITY REPORT

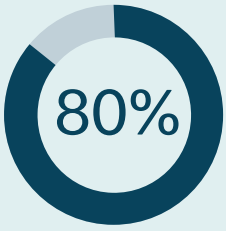
# Executive Summary

Now that most organizations have a blueprint for hybrid in place, it's time to take stock of how far we have come, evaluate the challenges, and address the opportunities that lie ahead.

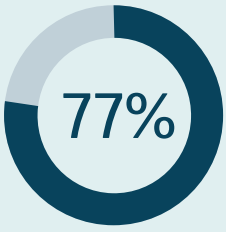
According to 984 IT leaders we surveyed across the US, UK, France, Germany, and Japan:




say it will get even harder to protect their hybrid employees in the next year.[i]




have made changes to their overall cybersecurity strategy to accommodate hybrid workers.[i]




agree that cyberattacks will accelerate, as will the number of endpoints for hybrid employees.[i]

Read on as we dive into the data and discuss what IT leaders need to do next. We hope this report helps you and your teams understand the new requirements of the hybrid workforce and take decisive action.

# Working Towards Better Hybrid Security

## Section 01

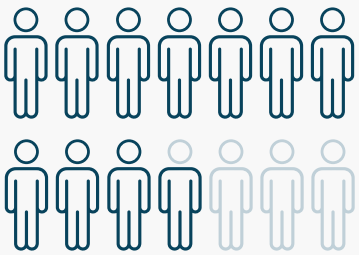
### Improving security for hybrid employees starts with a full understanding of the risks – both internal and external. Overwhelmingly, these relate to out-of-office workers and their devices.

Respondents to the survey recognize that there are gaps in their security posture. In fact, IT leaders are more likely to see gaps for their hybrid workforce (82%) compared to their always-in-the-office workforce (73%).[i]

In the survey, two broad challenges emerged that IT leaders are consistently looking to address:

#### 1. THE PROLIFERATION OF DEVICES AND SOFTWARE

**77%**

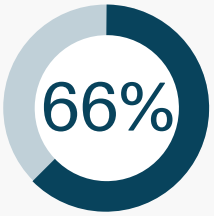


agree that cyberattacks will accelerate, as will the number of endpoints.[i]

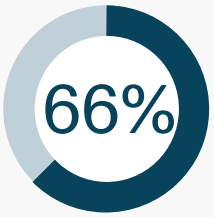
**7 in 10**

agree that hybrid work increases the risk of employees losing their work devices or having them stolen.[i]

#### 2. HAVING WORKERS OUTSIDE THE CORPORATE NETWORK




agree that the greatest cybersecurity weakness is the potential for hybrid employees to be compromised.[i]




say it is challenging to update their threat detection measures (e.g., EDR and SIEM tools) to reflect the behavior of hybrid employees.[i]

Leaders have accepted the reality of hybrid work as it relates to devices and user locations, even if they don't yet have all the answers. They know that endpoints can be vulnerable to attacks, and they know that hybrid workers outside the corporate network may present a weak point that attackers can exploit.

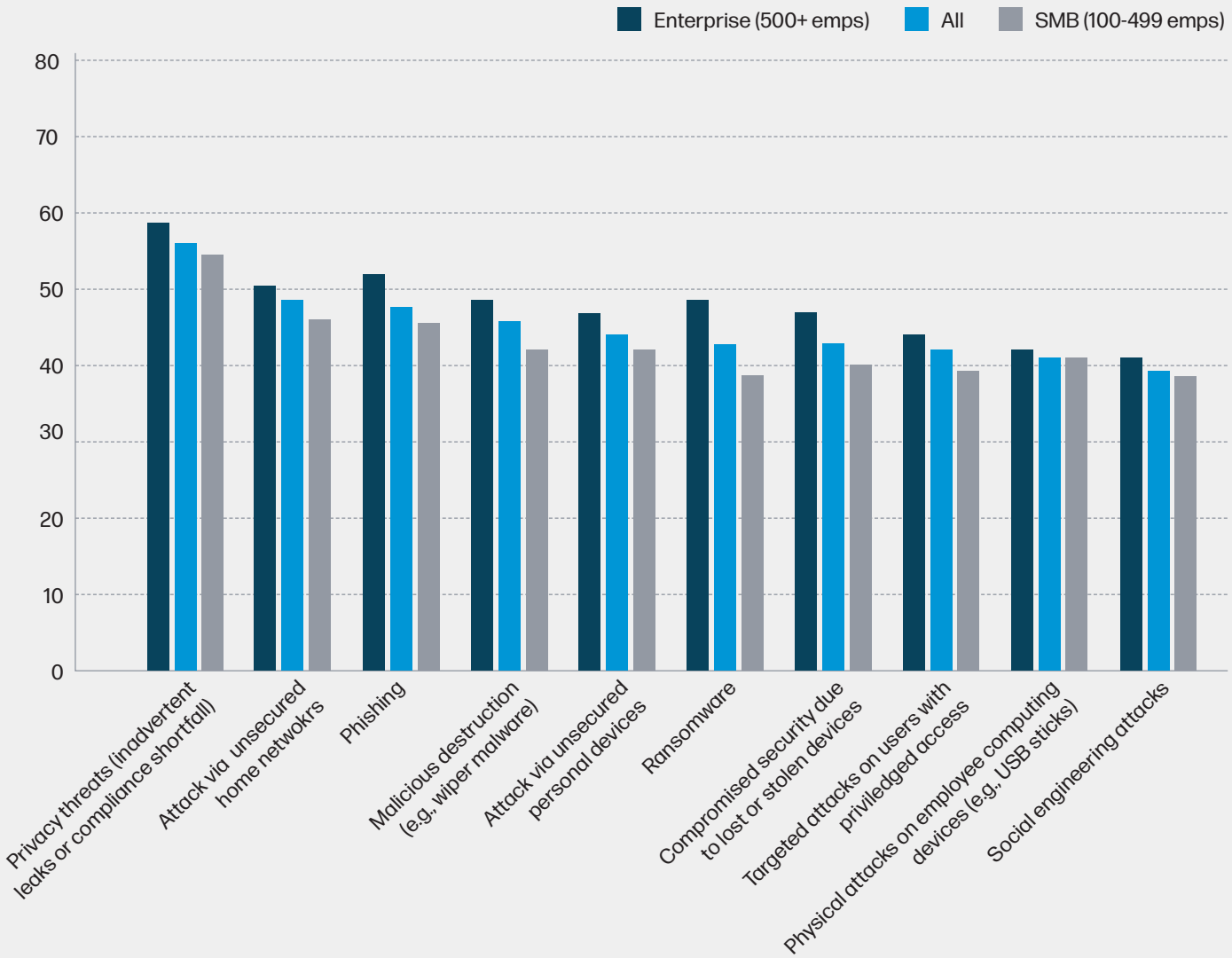
> "Educating hybrid workers about risks and responsibilities is vital, as is endpoint security. Technologies like micro-virtualization are a great example. This segregates potentially risky tasks – like opening links or attachments – from the rest of the system and ensures that attackers cannot access sensitive data."
>
> Dr. Ian Pratt, Global Head of Security for Personal Systems, HP Inc.

# Diverse Threats, One Common Target

As well as acknowledging organizational challenges, leaders recognize a broad range of external security threats. And almost all the most pressing ones target employee devices in some way.

When thinking about security overall, the threats most frequently chosen as a cause for concern were as follows, with nine of the top 10 endpoint related.

## TOP 10 SECURITY THREATS RESPONDENTS ARE CURRENTLY CONCERNED ABOUT[i]



# The Importance of the Endpoint

It is clear that IT leaders consider current endpoint threats to be a continuing – and indeed growing – risk. The same endpoint-focused threats that leaders are currently concerned about also rank highly among the threats that they expect to grow for their hybrid workers in the next 12 months. The most frequently cited are phishing (33%), ransomware (28%), and attacks via employees' unsecured home networks (27%).[i]

Given that the focus for attacks has shifted away from the physical office and towards the end user – wherever they happen to be – any defensive solutions should focus here as well. In the second part of this report, we explore the tools that organizations are choosing to address their hybrid security needs.

> "Zero trust is one of the hottest topics for our clients. One large financial customer wants to 'get rid of their corporate network' altogether. So we see less focus on limiting network access, and more focus on new architectures that enable security and freedom for hybrid workers."
>
> Alex Thatcher, Director of Cloud Clients, HP Inc

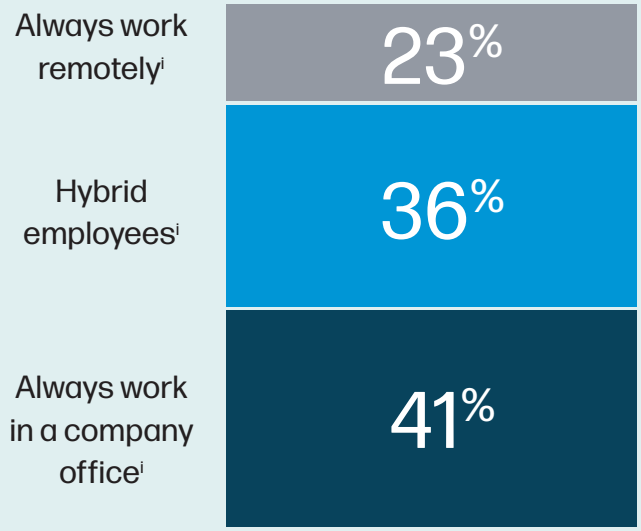
# Protecting Hybrid Workers at the Point of Attack

## Section 02

### IT teams already support a successful hybrid workforce. But what technologies are they deploying to protect them against tomorrow's hybrid threats?

Over the past three years, IT teams have stepped up to become the enablers of a productive, secure, distributed workforce. Hybrid work is now a permanent part of many organizations, and employees are enthusiastic about the potential that it brings. However, the hardest work may still lie ahead.

AVERAGE ESTIMATED WORKFORCE SPLIT (PC USERS)




**85%** of employees are happy working in the office, but also want to work from home at least twice a week[ii]

**67%** say that they never imagined they could be so productive at home[iii]

# Actions Taken

After the success of the enablement phase of hybrid work, the focus for IT is to dedicate more resources and deploy different tactics to protect their growing hybrid workforces.

- 82% say they have already increased their cybersecurity budget for hybrid workers.[i]
- 71% expect more money for security overall in 2023.[i]
- 81% have deployed a different set of tools and policies to protect hybrid employees.[iv]
- 80% have made changes to their overall cybersecurity strategy to accommodate hybrid employees.[iv]
- 70% limit remote workers' access to the corporate network to minimize the risk of a breach.[iv]

This investment in protection is already paying off. Compared to last year, 77% of IT leaders agree that their hybrid employees are doing a better job of protecting themselves against security threats.[i]

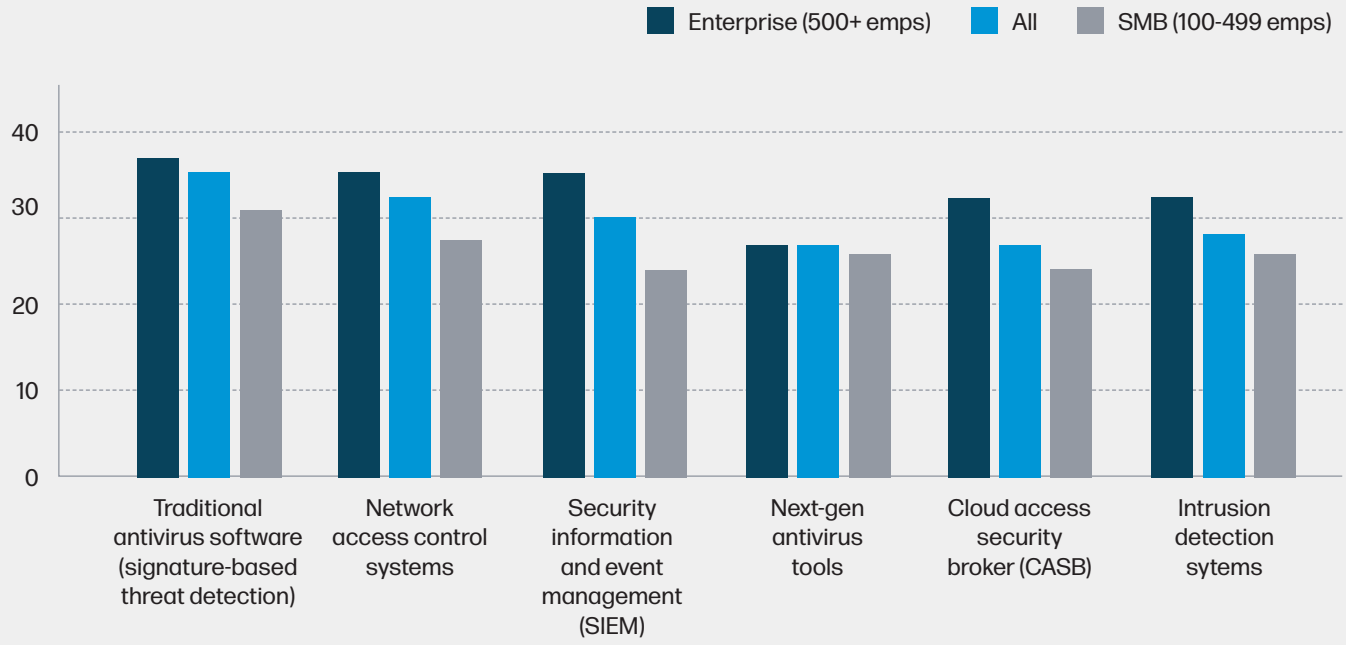
But given the challenges that IT leaders readily acknowledge, many are taking further steps to protect their hybrid employees.

# Deploying the Right Tools

Technology is the key enabler in hybrid work, and it also plays a central role as an attack vector and defensive tactic. As the workforce becomes more distributed, protecting the endpoint (where most attacks happen) should be the primary defensive tactic.

This is being recognised by IT leaders. Two-thirds (66%) of them see the potential for hybrid workers to be compromised as their greatest security weakness, so it's no surprise to see so many taking action to prevent and remediate potential breaches via the endpoint.

USE OF CYBERSECURITY TOOLS AMONG ORGANIZATIONS OF DIFFERENT SIZES[i]



# Technology to Protect Hybrid Workers

The following technologies are growing in popularity among security teams. Research indicated that IT teams were keen to learn more about them and/or intended to deploy them in the future.

ENDPOINT

A network-connected remote computing device, typically used for user or environmental interaction (e.g. a PC, printer, smartphone, or IoT device).

ENDPOINT DETECTION AND RESPONSE (EDR)

This technology monitors the system activity on user's devices — including PCs, laptops, and mobiles — and triggers alerts when it detects suspicious behavior. EDR solutions can also take action to contain the threat and help IT teams respond appropriately.

CLOUD ACCESS SECURITY BROKER (CASB)

Cloud services are a vital part of today's hybrid organization, and CASBs make it easier for IT teams to manage and control access to cloud resources. They simplify employee access to the services they need while restricting access to unauthorized or malicious users.

APPLICATION ISOLATION

Application isolation protects endpoints from known and unknown threats by isolating high-risk activities inside temporary virtual containers. For example, it is effective at protecting users who inadvertently try to access malicious content in email attachments, web links, and browser downloads.

NEXT-GEN ANTIVIRUS

Traditional antivirus software relies on signatures to detect and quarantine known malware. Next-generation antivirus uses AI and machine learning to identify anomalous behavior on endpoints to stop threats.

FILE INTEGRITY MONITORING (FIM)

FIM scans an organization's critical files, systems, databases, and applications to check whether they have been altered, which may be a sign of attack. If it detects an unexpected modification, it alerts IT teams so they can investigate.

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

SIEM solutions allow security teams to collect data from various sources and analyze it for security threats. Having a detailed log of information and events can also help with security management (understanding where to allocate resources) and demonstrating compliance.

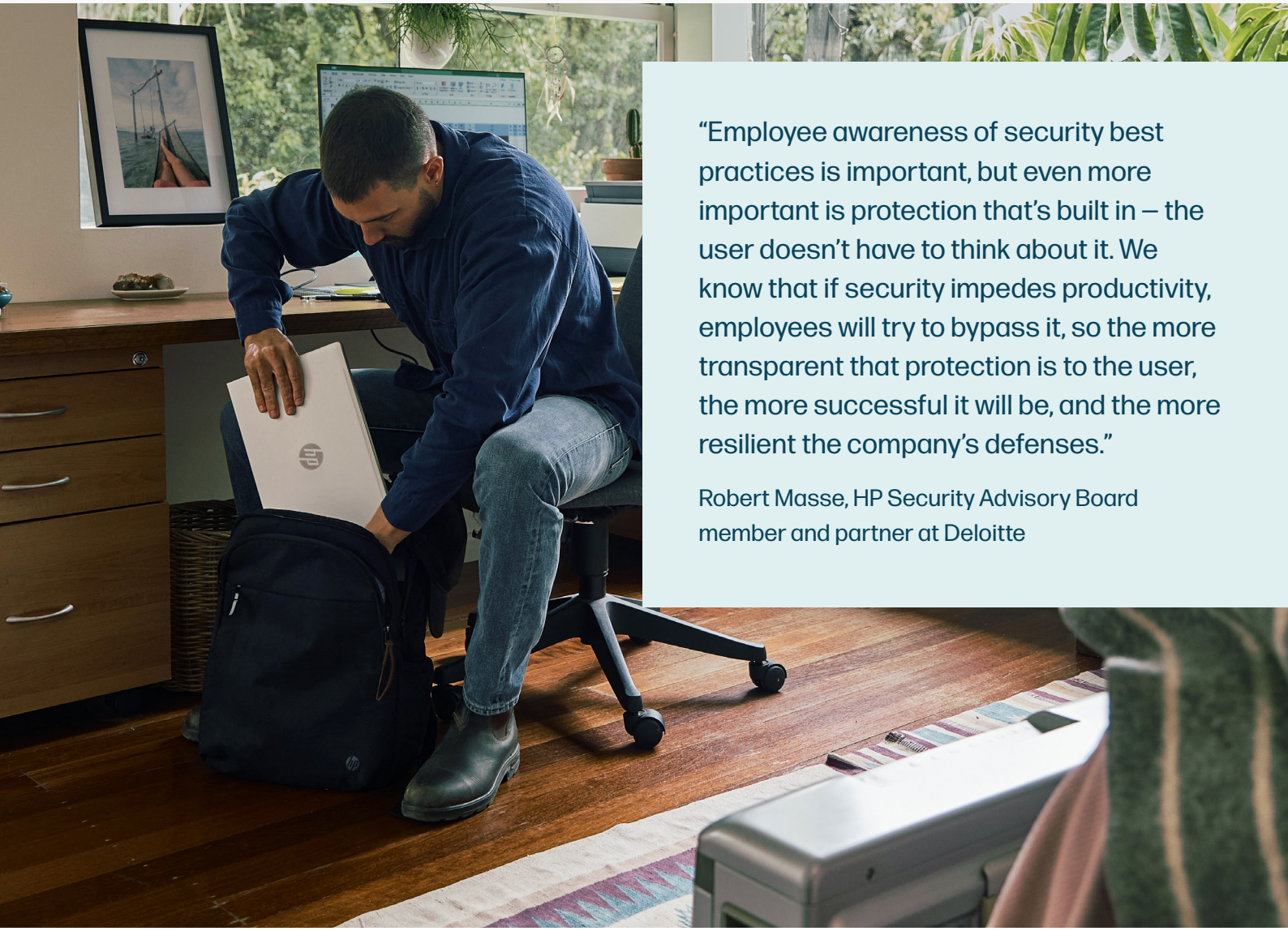
While most of the technologies on the previous page are already well-known and widely deployed, isolation technology in particular came up several times in the research as a significant part of respondents' hybrid worker defenses.

These tools improve an organization's resilience by segregating devices, applications, or specific tasks (such as browsing, email, or word processing) from other parts of the IT infrastructure. And they are growing in importance for IT leaders.

Currently, 23% use application isolation to handle unknown and potentially harmful documents and links. But 32% intend to deploy isolation technology in the next 12 months, and 76% consider it key in protecting devices during hybrid work.[i]

## "Silent" Solutions Show Promise

Research shows that employees can reject security measures if they get in their way, so any protection that IT teams put in place should be as transparent as possible to the end user. According to our research, 37% of office workers surveyed say security policies and technologies are too restrictive, and 48% think security measures result in a lot of wasted time.[v]



"Employee awareness of security best practices is important, but even more important is protection that's built in — the user doesn't have to think about it. We know that if security impedes productivity, employees will try to bypass it, so the more transparent that protection is to the user, the more successful it will be, and the more resilient the company's defenses."

Robert Masse, HP Security Advisory Board member and partner at Deloitte

## Report contributors

ALEX THATCHER,
Director of Cloud
Clients at HP Inc.

DR. IAN PRATT
Global Head of Security for
Personal Systems at HP Inc.

ROBERT MASSE
HP Security Advisory Board
member and partner at Deloitte

## About HP Wolf Security

HP Wolf Security is part of HP's portfolio of hardware-enforced security and endpoint-focused security services. It is 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. Visit hp.com/wolf.

## Methodology

[i] HP surveyed 984 IT leaders in hybrid organizations of 100 to 2,499 employees, across five markets (the US, UK, France, Germany, and Japan), in July to August 2022.

Eighty percent of respondents are Director level or above (VP and C-suite). All are decision-makers for endpoints, network, cloud, or privacy management, and they all oversee a cybersecurity operations team or IT hardware and software within their organization.

Hybrid organizations are defined as having a range of employees who either work in the office, work remotely, or a mixture of both.

## References

[ii] HP, UK and US, Survey of end-users, n=200, July 2021.

[iii] HP, US and UK, n=537 end-users in US and UK, Sept 2020.

[iv] Based on % of respondents that "strongly agree" or "agree" with statements about protecting hybrid workers.

[v] HP Wolf Security. (2021). HP Wolf Security Rebellions & Rejections Report. [Online]. Available online: https://press.hp.com/content/dam/sites/garage-press/press/press-kits/2021/hp-wolf-security-rebellions-and-rejections/hp-wolf-security-report-rr-final.pdf

HP Wolf Security for Business requires Windows 10 or 11 Pro or higher, includes various HP security features and is available on HP Pro, Elite, RPOS and Workstation products. See product details for included security features.