HP WOLF SECURITY

The New Way to Secure the Hybrid Workforce

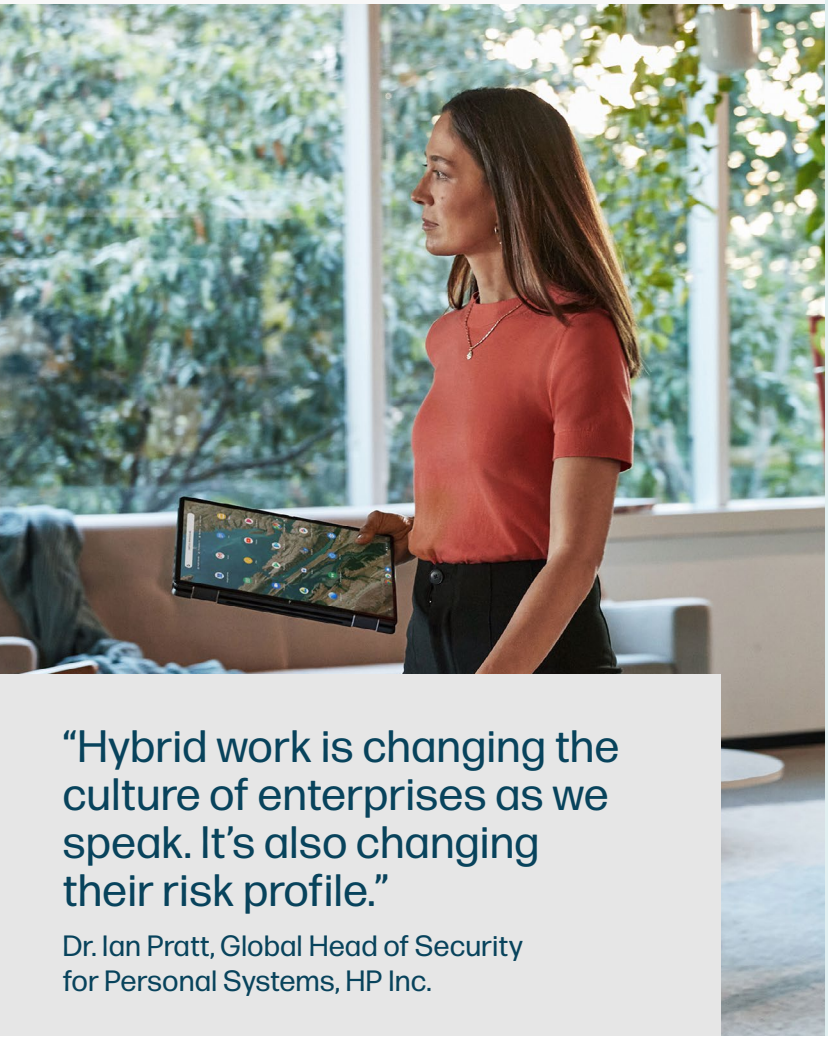
AN HP WOLF SECURITY REPORT

Executive Summary

Hybrid work is a fact of life for businesses today, and maintaining security is an ever-evolving process.

To understand how leaders perceive the risk landscape for hybrid work and the ways they are addressing the challenges, we surveyed 168 security leaders at enterprises with more than 2,500 employees. Among these organizations, hybrid employees make up 40% of the workforce on average.[i]

The steps required to keep hybrid workers safe are changing all the time. Security leaders know that new approaches are needed to maintain protection against today's cyber risks.



"Hybrid work is changing the culture of enterprises as we speak. It's also changing their risk profile."

Dr. Ian Pratt, Global Head of Security for Personal Systems, HP Inc.

Securing Hybrid Employees – Four Key Takeaways

1. PROTECT THE ENDPOINT

The hybrid enterprise no longer has a security perimeter, and end-user devices continue to be the biggest source of cybersecurity risks. Security leaders should focus their defensive efforts on endpoints, ensuring they can predict, mitigate, detect, and remediate threats at device level before these become a network problem.

2. ISOLATE RISKY ACTIVITIES

With less direct control of how employees connect to corporate systems, security leaders are looking to isolate risky behaviors rather than block them outright. If this isolation doesn't affect user productivity, it's a win-win, and this approach is becoming more common across enterprises.

3. SEEK TRUSTED PARTNERS

Security leaders have an ever-increasing workload, and most in our survey have help from external partners. A significant proportion of these use managed service providers specifically to protect hybrid workers.

4. APPLY ZERO TRUST

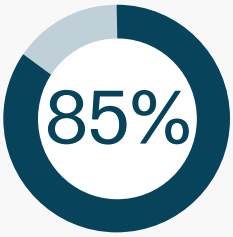
With employees, devices, and resources increasingly sitting outside the corporate network, security leaders should consider a zero-trust approach for their hybrid workforce. This means no "safe" network-based activities or known devices, and authentication and authorization used for protection everywhere.

Strategies Deployed to Protect Hybrid Workers

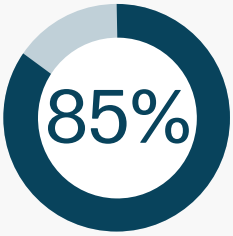
Section 01

The workforce is changing fast. This translates directly into strategic changes, targeted investment, and new defensive technologies to protect hybrid employees.

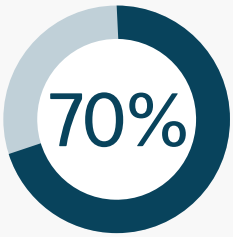
1. Adapting Defense Strategies



of security leaders in our survey have made changes to their overall cybersecurity strategy to accommodate hybrid employees.[i]



say they deploy a different set of tools and policies for these users.[i]



say that when hybrid employees are remote, they limit access to the corporate network to minimize the risk of a breach.[i]

2. Investing in Targeted Security Improvements

Enterprises are prioritizing investments accordingly to support these changes.

of respondents say they have increased their cybersecurity budget to support hybrid employees.[i]

expect their budget in 2023 to increase.[i]

The increased emphasis on hybrid security comes as boards wake up to today's risk landscape, says Justine Bone, a member of the HP Security Advisory Board.

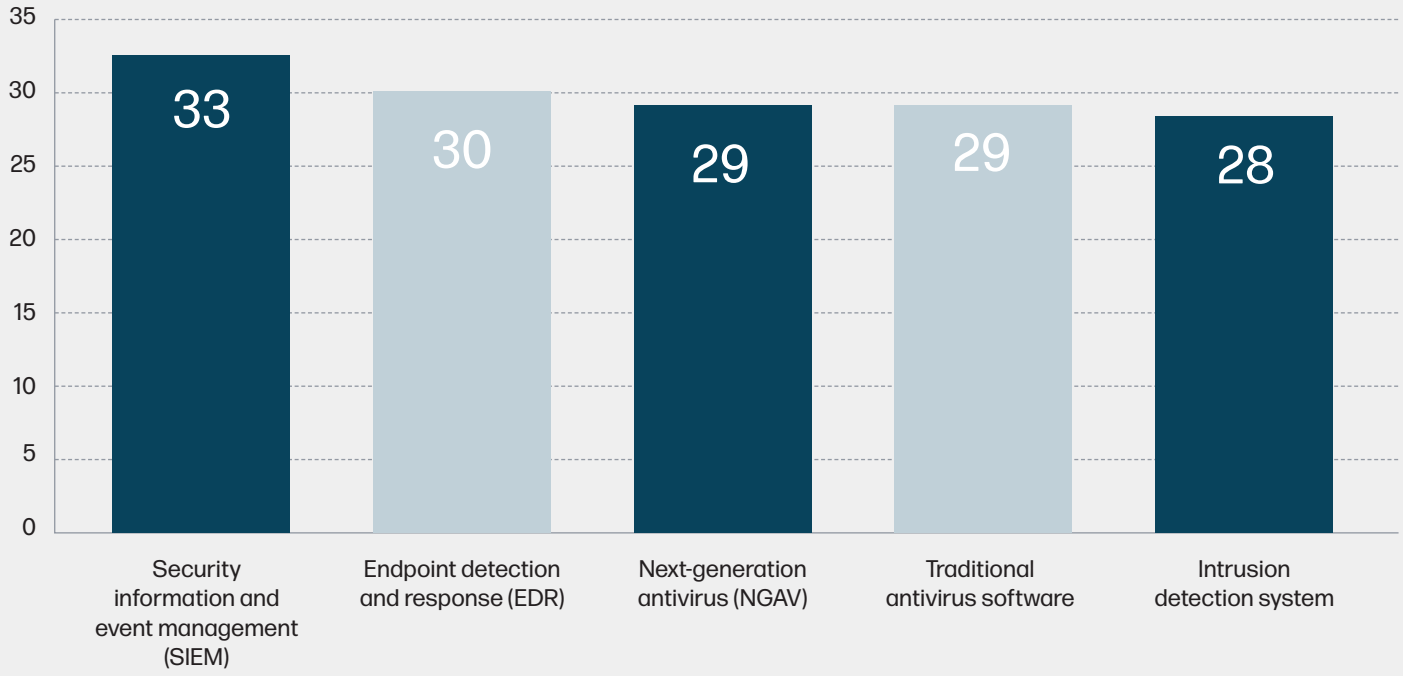
> "I think that increasingly visible incidents – like ransomware attacks – have raised awareness at senior leadership levels. This trickles out to budget planning and reassures security leaders about their ability to protect organizations."
>
> Justine Bone, HP Security Advisory Board member

Although budgets may be increasing, pinpointing the areas where investment makes the most sense is essential. "It's important to be intentional about where to invest," says Joanna Burkey, Chief Information Security Officer at HP Inc. "Good governance is about more than just compliance – it's about appropriately handling your company's resources, including budgets. There is an ocean of security issues to boil, so understanding which areas expose the company to the most risk will be essential."

3. Shifting Towards Endpoint Protection

Given the above, there is a subtle but noticeable shift in large enterprises' strategies for protecting hybrid workers. Cybersecurity technologies are moving away from the network and towards the endpoint as more employees and devices connect from outside the traditional corporate perimeter.

SECURITY TOOLS DEPLOYED OR EMPHASIZED TO PROTECT HYBRID WORKERS[i]



As well as seeking a boost in overall security operations (SecOps) capability with security information and event management (SIEM), enterprises are placing new focus on endpoint detection and response (EDR) and next-generation antivirus solutions (NGAV).

4. Embracing Zero Trust

Security leaders are seeing the benefits of their current security positions, with 75% confident about their ability to protect hybrid employees from threats.[i] They also acknowledge that there is room for improvement: 35% say there are urgent gaps in their security posture for hybrid workers, for example.[i] To address this, many are choosing a zero-trust approach, whereby they do not assume that activities are "safe" because they are happening on known devices or parts of the corporate network. Under the zero-trust model, authentication and authorization are used to protect resources — services, files, and accounts — rather than network segments, as was traditional.[ii]

5. Working with Managed Security Services Providers (MSSPs)

While deploying the right cybersecurity tools contributes to keeping hybrid workers safe, many security leaders also trust and rely on third parties to provide some of that protection.

More than two-thirds (67%) currently work with an MSSP, and another 28% are considering it. Nearly half (49%) of security leaders using an MSSP said they do so specifically to help protect their hybrid workers.[i]

Bone encourages enterprises to consider how an MSSP could boost existing internal capabilities. "MSSPs allow a company to share responsibility," she says. "This is especially useful when cybersecurity talent is hard to find or when a company is just not structured to embed cybersecurity capabilities internally."

"Endpoint-focused technologies are growing in importance for hybrid organizations because companies are embracing zero-trust models. This is one of the hottest topics for our customers.

One of our largest customers is considering 'getting rid of their corporate network' altogether. Increasingly, we see less focus on limiting network access, and more focus on new architectures that enable security and freedom for hybrid workers."

Alex Thatcher, Senior Director of Cloud Clients at HP Inc.

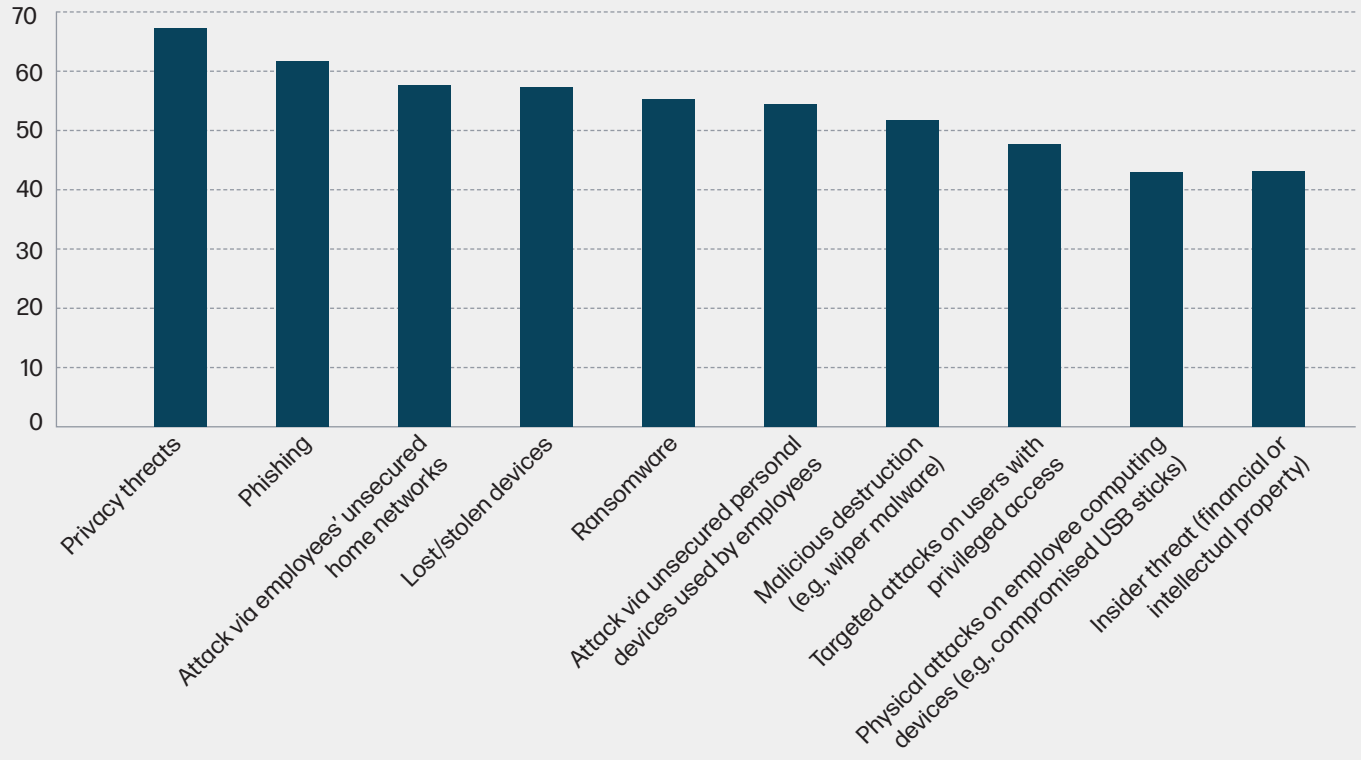
Identification of Current Threats

Section 02

As organizations shift to a work-from-everywhere model, security leaders are acutely aware of how this affects business risk. They have identified a wide range of external threats and are taking action to address them.

In our research, these leaders show a keen awareness of cybersecurity threats overall, with nine of their top 10 relating to employee endpoint devices.

CURRENT LEVEL OF CONCERN ABOUT SECURITY THREATS[i]



Privacy breaches are also a major concern, particularly inadvertent leaks by employees or the company and shortfalls in compliance. In fact, these are the threats that leaders are most concerned about, ahead of others such as ransomware and business email compromise.

Here again, modern devices with built-in security features offer part of the solution. Deploying them among the hybrid workforce reassures security leaders that breaches will be prevented, detected, and contained at the endpoint. They also help to prevent privacy breaches – data leaking outside the corporate environment – and assist companies in their zero-trust efforts.

"Those organizations that can master endpoint protection will be the most resilient in the hybrid era," says Dr. Ian Pratt, Global Head of Security for Personal Systems at HP Inc. "Not only does better endpoint security protect users, but it also gives IT teams better levels of trust and better oversight and management of a distributed workforce."

Equipping the Hybrid Enterprise for What's Next

When asked about the next 12 months, respondents identified several risks related to hybrid workers' endpoints:

36% are concerned about attacks via employees' unsecured home networks.[i]

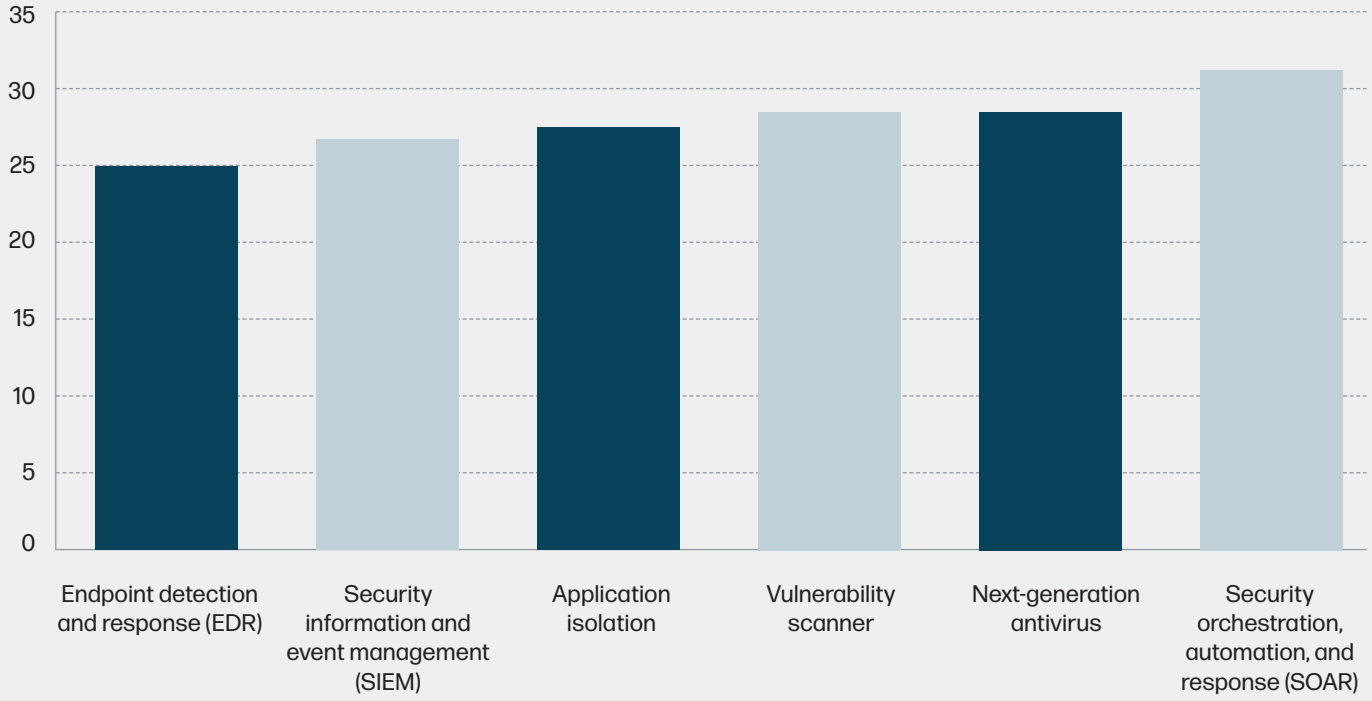
30% are concerned about attacks via unsecured personal devices used by employees.[i]

30% are concerned about physical attacks on employee computing devices (e.g., compromised USB sticks).[i]

The above issues are not new. Many leaders were grappling with them even before mass hybrid working took off, but not all will have found solutions that provide robust protection without getting in the way of employees' workflows. Built-in security offers a solution here, and enterprises are starting to see the value in solutions that have security features at the hardware, firmware, operating system, and application layers.

Indeed, security leaders are looking to double down on their investment in endpoint-focused security and tools to oversee a distributed workforce. These will help them as they roll out zero trust across the organization. Over the next 12 months, the top technologies that they plan to deploy include a mix of SecOps tools and endpoint protection.

TECHNOLOGIES THAT SECURITY LEADERS PLAN TO DEPLOY IN THE NEXT 12 MONTHS[i]



Bone adds that device-based security is a critical first step for any hybrid security strategy. "'Secure by default' has become an expectation, which means that devices must come with built-in security features that don't impact useability," she says. "And the complexities of a hybrid workforce — and hybrid security teams themselves — are driving deployment of SIEM and SOAR, which provide the oversight and control that organizations are demanding."

Isolation technology, in particular, appears to be an important part of most organizations' hybrid protection strategy. They see value in segregating tasks and applications from other elements of their infrastructure so that potential infections cannot spread.

- 79% agree that "isolation technology is key in order to protect devices during hybrid work."[i]
- 30% of security leaders use application isolation currently to handle unknown and potentially harmful documents and links.[i]
- A further 28% intend to deploy it in the next 12 months, making it the third most popular tool to deploy in the near future.[i]

"Today's micro-virtualization technology means that potentially risky tasks like opening email attachments or clicking unknown links can be carried out in isolated containers within a device," says Pratt. "Previously only military or government organizations would have used it, but it's become accessible to more organizations and is transparent to the end user."

Glossary: Protecting Hybrid Workers

The following technologies emerged in our research as either growing in popularity or being highly requested as topics for discussion among security leaders.

ENDPOINT

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

ZERO TRUST

In the past, enterprises based security policies on trusted devices, networks, and locations, all of which were company owned. Hybrid working and the cloud have brought in a new zero-trust era, based on authenticating and authorizing access to resources wherever they reside, from whichever location or device the request came from.

MANAGED SECURITY SERVICES PROVIDER (MSSP)

Organizations that provide external expertise and resources to assist an enterprise's security function. MSSPs often provide services that are difficult to deliver in-house, like 24/7 monitoring or remote assistance for out-of-office workers.

ENDPOINT DETECTION AND RESPONSE (EDR)

This technology monitors 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 services while restricting access to unauthorized or malicious users.

NEXT-GEN ANTIVIRUS (NGAV)

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.

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

The Final Word

The fact that hybrid work has become the norm so quickly shows the potential for even the biggest enterprises to adapt to change. Indeed, by making these changes, organizations have emerged stronger and more resilient.

JOANNA BURKEY
Chief Information Security Officer at HP Inc.

Security leaders clearly recognize the challenges, have successfully overcome many of them, and are looking to further strengthen their defenses. As the hybrid workforce continues to evolve, so will the threats that attackers deploy against them. If the defenders want to maintain, and ideally improve, their protection, they can't afford to stand still.

Knowing exactly where to prioritize investment and take action is down to the individual company, its appetite for risk, and its current market position. But the findings in this report offer some indication of where hybrid security is headed.

The endpoint remains a focal point for protection because it's also a focal point for attacks. We therefore encourage security leaders to put the endpoint front and center in their hybrid security strategy.

Isolation technology can help mitigate the threats to knowledge workers by reducing the impact of the attacks that most commonly target them. And a zero-trust approach makes sense for any business whose employees and resources increasingly sit outside its own network. Finally, many enterprises may find an MSSP can help improve their resiliency.

As the workforce evolves, so does business risk. Targeted investments in key areas can help security leaders stay ahead of changes and protect their organizations.

Report contributors

JOANNA BURKEY
Chief Information Security Officer at HP Inc.

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

ALEX THATCHER
Senior Director of Cloud Clients at HP Inc.

JUSTINE BONE
HP Security Advisory Board member

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 168 security decision-makers at enterprises with more than 2,500 employees. The research took place across the US, UK, France, Germany, and Japan in July to August 2022.

All security leaders oversee or manage a cybersecurity operations team.

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] National Institute of Standards and Technology, Zero Trust Architecture (2020). [Online]. Available at: https://www.nist.gov/publications/zero-trust-architecture

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.