redaccess

2023 State of Hybrid Work and Browsing Security

Survey Report

March 2023

Table of Contents

Introduction and Key Findings

Introduction & Methodology

Introduction

The widespread adoption of remote and hybrid work has caused significant disruption to the world of cybersecurity. The rapid dissolution of the enterprise perimeter has left organizations the world over struggling to shore up their defenses at precisely the same time that economic headwinds are pushing them to increase efficiency and maximize productivity. These seemingly disparate mandates have created an environment in which Chief Information Security Officers are feeling increasingly uncertain about their organizational security. The rising tide of browsing-based threats, combined with growing dissatisfaction with legacy solutions, has placed the world of web security at an inflection point. In this survey, we will share insights into the types of threats that are worrying CISOs the most and the types of solutions and strategies they plan to implement to address them. We will also gain insight into the top security concerns associated with hybrid work and will explore the extent to which CISOs are satisfied or dissatisfied with their existing security programs and the characteristics they consider most important when selecting new solutions.

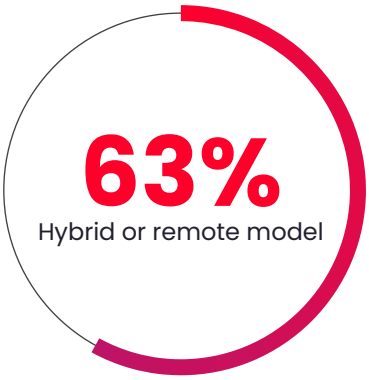
Methodology

In order to better understand the ways in which security professionals are navigating the troubled waters of remote work, Red Access has commissioned a survey of 300 Chief Information Security Officers (CISOs). This report was administered online by Global Surveyz Research, a global research firm. This report is based on the responses of 300 CISOs from the U.S. (200) and U.K. (100), from companies with 5,000 or more employees. Companies represent a wide range of industries, including Banking, Energy, Pharmaceuticals, Technology, and others. The respondents were recruited through a global B2B research panel, invited via email to complete the survey, with all responses collected during the month of January 2023. The answers to the majority of the non-numerical questions were randomized in order to prevent order bias in the answers.

Key Findings

1 Hybrid Work is Here to Stay

Nearly two thirds of respondents (63%) said that, in three years' time, most employees at their companies would work in either a hybrid model (both in the office and remotely/from home) or entirely remotely. This finding is consistent with other recent surveys of business decision makers, which have found that hybrid work remains and will continue to be the dominant way of working for the knowledge workers of the world.

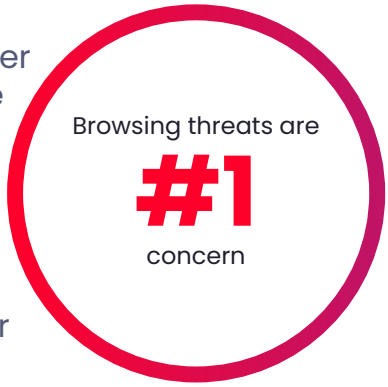


2 Most CISOs See Hybrid Work as Having a Negative Impact on Security Posture

When asked whether the hybrid and remote workforce has a negative impact on their organizations' security posture, the overwhelming majority of CISOs (72%) agreed on the negative effect. And for 29% of respondents, this negative impact of the hybrid/remote workforce is significant (rated as either a "high" or "very high negative impact"). Taken together with the finding that most anticipate hybrid and remote work to remain the norm at their organizations, it becomes clear that this is a real and persistent issue most CISOs face today and will continue to grapple with in the foreseeable future.

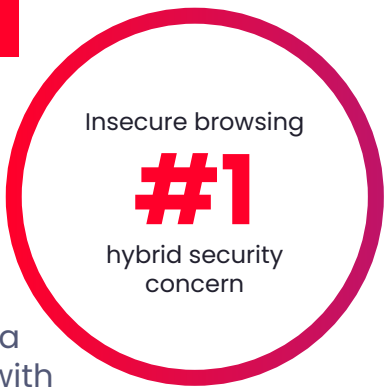
3 Browsing Threats are the #1 Concern Across Organizations

When asked to select the top three most significant cyber threats to their organizations, CISOs pointed to a wide range of issues, but "Browsing Threats" topped the list, with nearly half (43%) of CISOs ranking it as a top concern. Other commonly-cited concerns at the top of the list include cloud vulnerabilities (41%) and third-party exposure (38%). Interestingly, concerns around browsing-based threats were consistent across organizations, regardless of hybrid or in-office work models.



4 Insecure Browsing Tops The List of Hybrid Security Concerns

When asked to select the top three hybrid/remote security concerns that put organizations at risk, "Insecure Browsing" led the pack with nearly half (44%) of respondents citing it as a top concern. Insecure browsing shared its spot as the top concern with "Poor endpoint security" (44%), followed closely by the "Use of personal devices" (41%) — all seeming to suggest a growing preoccupation with heightened risk associated with distributed end-users.



5 Legacy Solutions Leave CISOs at Hybrid Organizations Feeling Unsecured

When we asked CISOs whether their current cybersecurity program was capable of protecting their hybrid and remote employees' browsing activities, we found that the level of confidence was clearly divided by office policies. 82% of CISOs working at organizations where most employees work in-office feel that their current cybersecurity program is sufficient for securing the browsing activities of their hybrid workforce. However, when looking exclusively at those CISOs from primarily hybrid organizations, that percentage plummets to just 43%. And for those who anticipate their organizations being primarily remote, the figure drops to just 33%.

6 Seamless User Experience is of Critical Importance When Selecting Hybrid Security Solutions

CISOs' priorities around hybrid security solutions aren't the same as they once were. In line with the idea that distributed teams require greater flexibility in security solutions, 73% of CISOs say that, when selecting a new security solution, it is either "extremely important" or "very important" that it enables a seamless end-user experience on any device.

Detailed Report Findings

Section 1

Hybrid Work, "Browserization" Redefine the Security Landscape

1 Expected Work Environment Three Years From Now

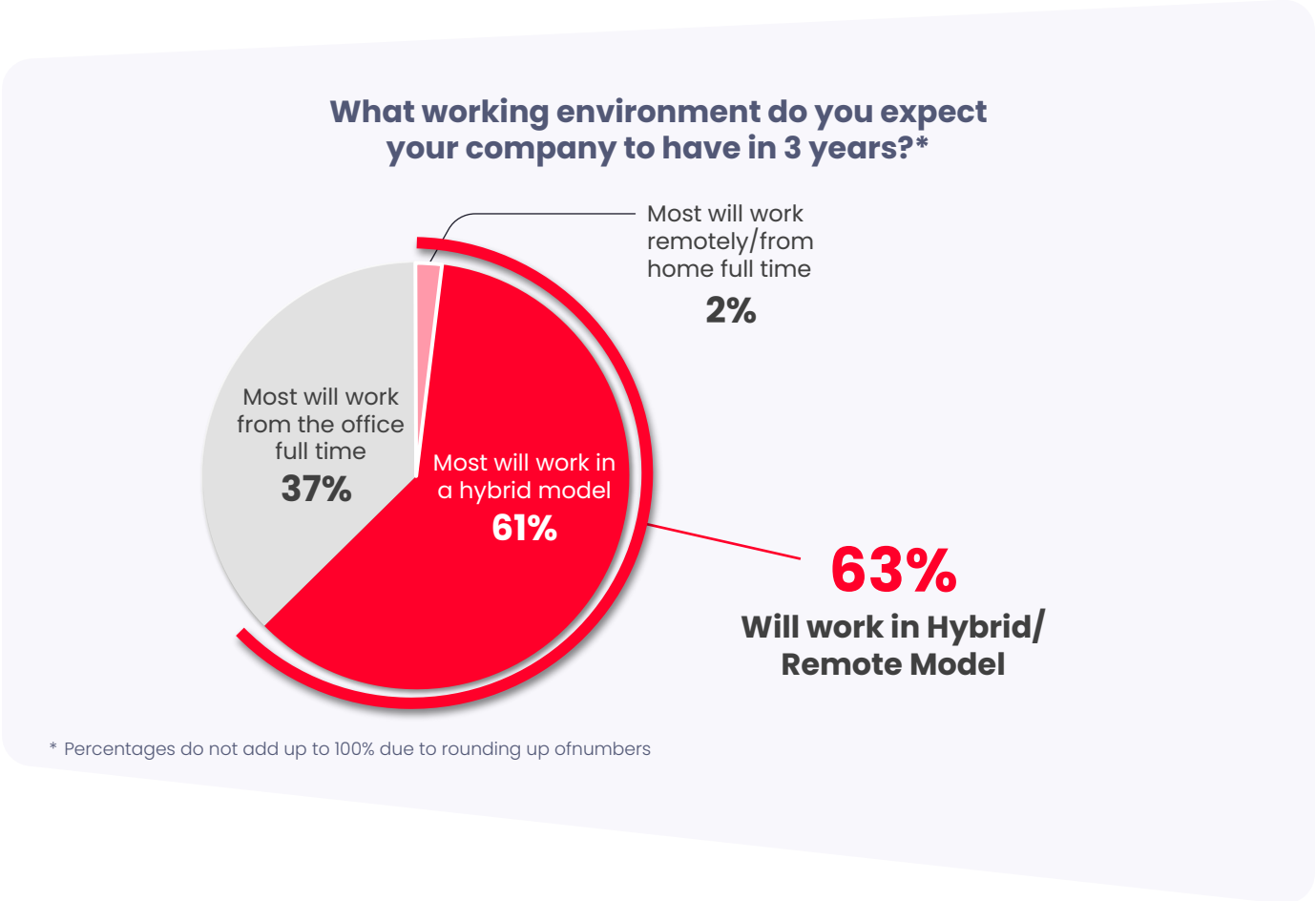
A clear majority of CISOs anticipate hybrid work to remain the norm for the foreseeable future.

When asked what they anticipate their companies' office policies to look like in three years' time, 63% of CISOs said they anticipate most employees to work in either a hybrid model (i.e. both in the office and remotely) or entirely remotely.

Meanwhile, just 37% of respondents said they anticipated most employees at their organizations working in the office full time in the next three years.

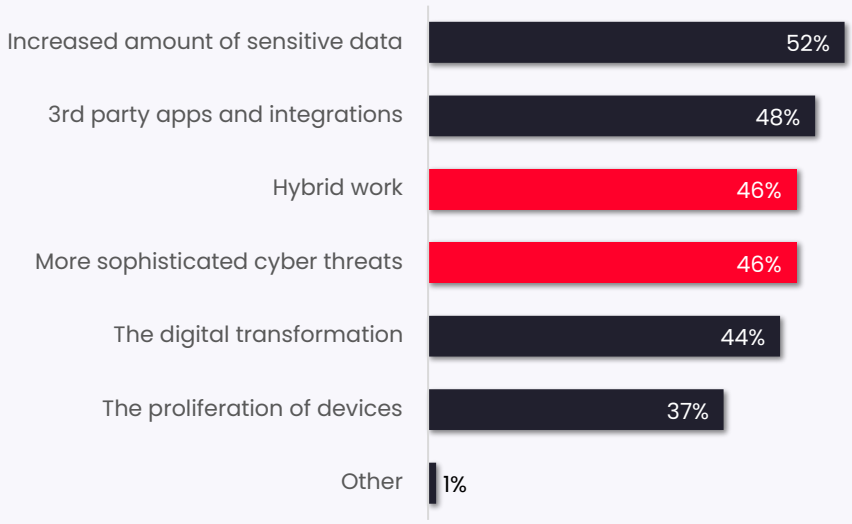
These findings are consistent with other recent surveys[1] of business decision makers, in which the overwhelming majority of respondents report expecting hybrid work to remain the norm at their organization for the foreseeable future.

Taken together, these findings leave little room for doubt that hybrid work is here to stay — prompting CISOs to face an uphill battle to maintain their organization's security in the absence of a traditional defense perimeter.



1. C-Suite Outlook 2023: On the Edge: Driving Growth and Mitigating Risk Amid Extreme Volatility (conference-board.org)

2 Factors That Compromise Organizations' Security Posture



* Question allowed more than one answer and as a result, percentages will add up to more than 100%

Hybrid work and advanced threats climb the ranks of factors deleterious to security posture.

The leading factors compromising today's enterprise have seen a dramatic reshuffling since the COVID-19 pandemic. Security teams must now address a litany of challenges ranging from the proliferation of sensitive data to the mounting risk associated with our interconnected digital ecosystem — all at the very same time that cyber threats are increasing in sophistication and distributed workforces are complicating defense efforts.

Hybrid work is now clearly seen as a cybersecurity imperative, on par with the likes of data sensitivity and the increasing sophistication of modern attacks.

When asked, "which of these factors strongly compromise your organization's security posture", nearly half (46%) of CISOs agreed that "Hybrid work" and "More sophisticated cyber threats" were having severe negative effects. These were surpassed only by "Increased amount of sensitive data" (52%) and "3rd-party apps and integrations" (48%), and by a narrow margin.

3 Biggest Cyber Threats to Organizations

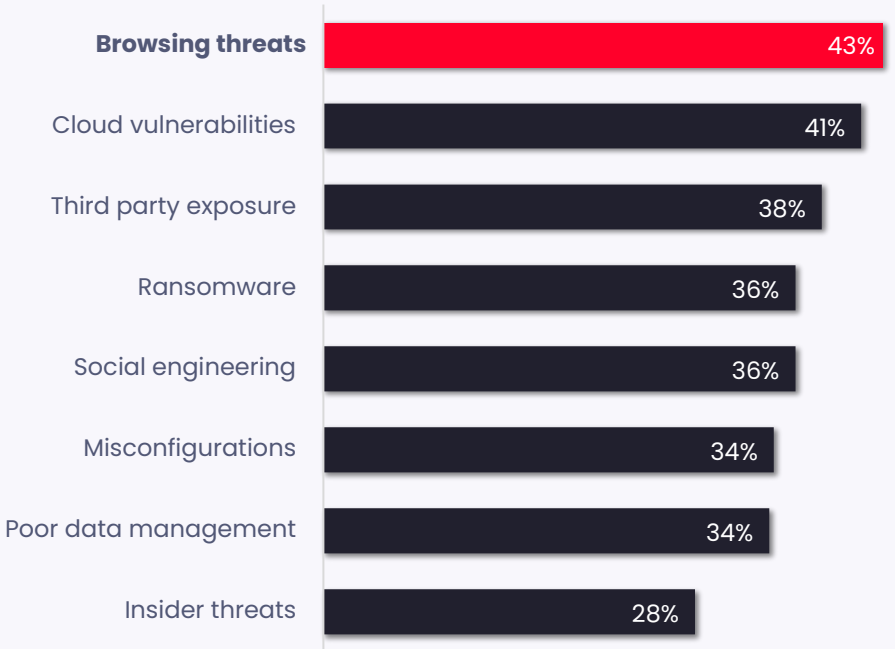
Browsing-based threats are CISOs' #1 concern across organizations.

Web browsing has become the modern knowledge worker's primary gateway to the digital world. As the key operating layer on which most of our day-to-day work is run, its significance as an attack surface has also skyrocketed.

When asked to select the top three biggest cybersecurity threats to their organization, "Browsing threats" emerged as #1, with 43% of CISOs citing it as a top concern. This was followed closely by "Cloud vulnerabilities" at 41% and "Third-party exposure" at 38%.

These findings reflect a step change in the types of threats that CISOs are most concerned about today, with browsing-based threats assuming a newfound centrality in today's threat landscape.

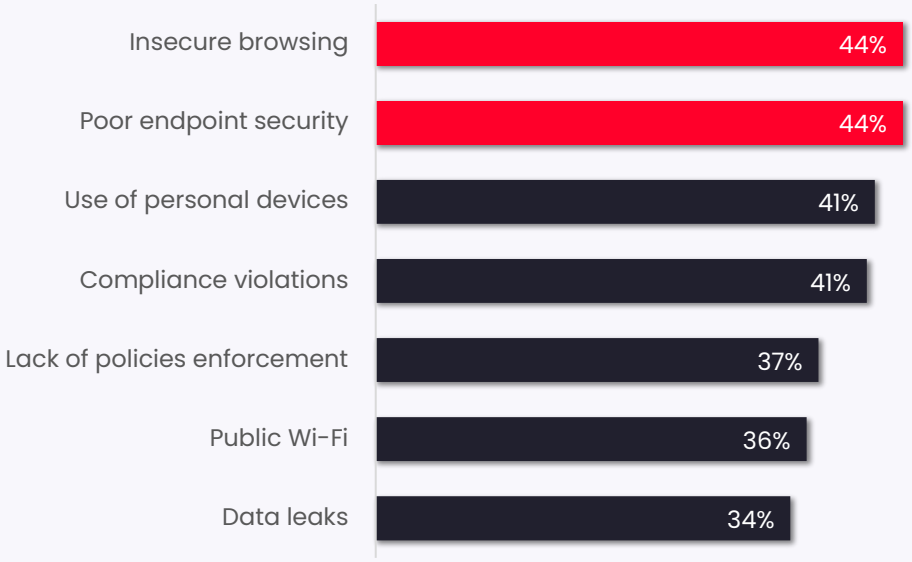
What are the biggest cyber threats to your organization?*



* Question allowed more than one answer and as a result, percentages will add up to more than 100%

4 Top Security Concerns for Hybrid and Remote Work

What are the top hybrid/remote work security concerns that put your organization at the most risk?*



* Question allowed more than one answer and as a result, percentages will add up to more than 100%

CISOs rank insecure browsing as the #1 security concern for hybrid and remote work.

For remote and hybrid employees especially, browsing is at the center of nearly everything they do at work. As such, it has become an increasingly attractive target to threat actors seeking sensitive information and/or access to networks and devices.

When asked to select the top three hybrid/remote security concerns that put organizations at risk, "Insecure browsing" and "Poor endpoint security" led the pack with nearly half (44%) of respondents citing each as a top concern. These were followed closely by the "Use of personal devices" at 41%.

Taken together, these leading hybrid/remote concerns suggest CISOs have grown increasingly concerned with the heightened risks associated with a distributed workforce and the role of end-users in such an environment.

5 2023 Cybersecurity Budget: Amount Planned for Browsing Security Solutions

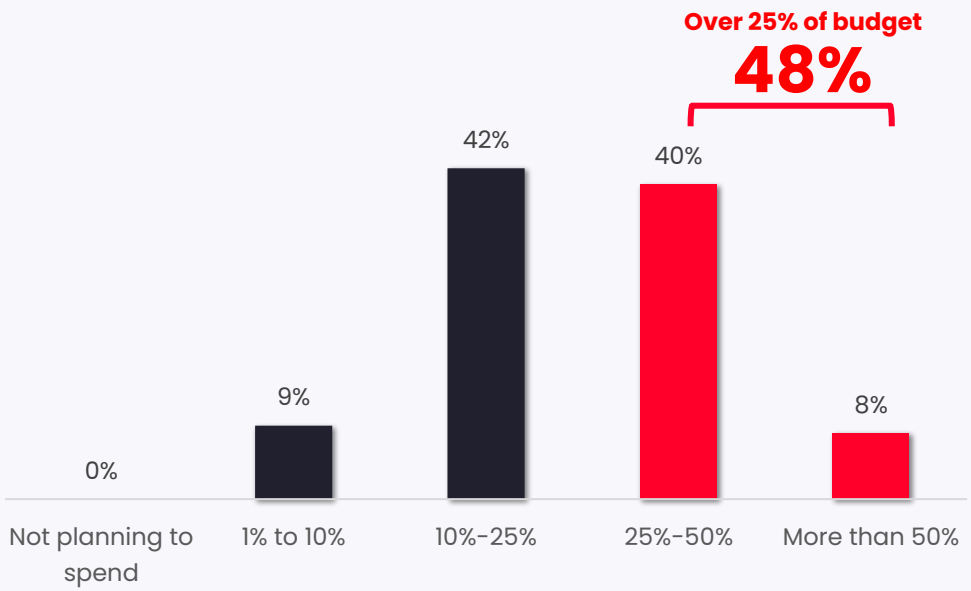
Nearly half (48%) of CISOs plan to spend 25% or more of their 2023 cybersecurity budget on browsing security.

As recently as a year or two ago, the idea of dedicating a quarter or more of one's annual cybersecurity budget to secure browsing solutions would have been almost unimaginable.

Today, with browsing playing such a central role in the average enterprise environment, CISOs are channeling more and more of their resources into securing this attack surface — and with good cause. In fact, a non-trivial percentage of respondents (8%) said they plan on devoting over half of their entire 2023 budget to browsing security.

Taken together, these findings leave little doubt as to not only the primacy of browsing security as a priority, but also the perceived cost and complexity of the problem. It is clear that CISOs today see browsing security as a pressing issue that will require considerable resources to adequately address.

What % of your overall 2023 cybersecurity budget do you plan to spend on browsing security solutions?*



* Percentages do not add up to 100% due to rounding up of numbers

Section 2

Hybrid Work – Leading Threats and the Toll on Security Posture

6 Impact of Hybrid/Remote Workforce on Organizations' Security Posture

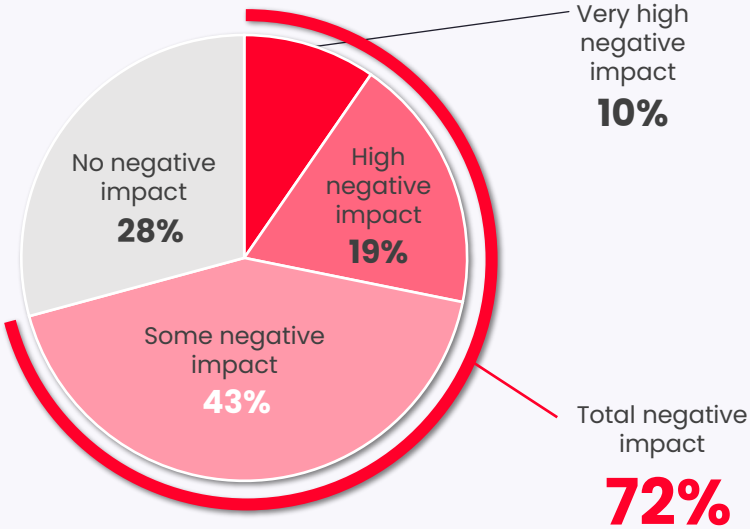
72% of CISOs agree that the hybrid/remote workforce has a negative impact on their organization's security posture.

When asked whether the hybrid/remote workforce poses a negative impact on organizations' security posture, a whopping 72% of respondents felt it presented at least some negative impact. 29% of respondents felt that hybrid/remote work had a "high" or "very high negative impact" on organizations' security posture; while 43% felt it had some negative impact.

This sentiment is what lies at the heart of many of today's most pressing cybersecurity concerns. The rapid dissolution of the traditional security perimeter has left the overwhelming majority of CISOs feeling decidedly less secure. Combine this with the fact that the vast majority anticipates hybrid and remote work to remain the norm at their organizations for the foreseeable future, and it becomes clear that most CISOs today feel their work is cut out for them.

The next logical question, then, is "how do CISOs plan to mitigate these negative effects moving forward?"

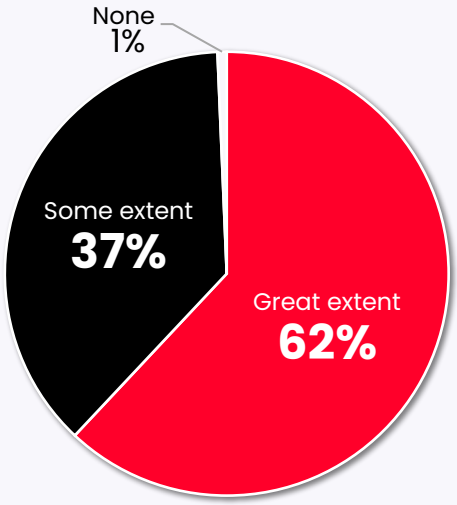
To what extent is your hybrid/remote workforce impacting your organization's security posture?*



* Percentages do not add up to 100% due to rounding

7 Perceived Risk Caused by Insecure Browsing by Remote/Hybrid Workers

To what extent is insecure browsing by your remote/hybrid employees posing cyber risk to your organization?



Nearly all CISOs (99%) agree that insecure browsing by remote/hybrid employees poses at least some cyber risk.

When asked "To what extent is insecure browsing by your remote/hybrid employees posing cyber risk to your organization", nearly all respondents (99.37%) agreed that it posed at least some risk. A clear majority of respondents (62%) felt that insecure browsing by remote/hybrid employees negatively impacted their security posture to "a great" or "very great extent".

A vanishingly small cohort of respondents (<1%) said that insecure browsing by remote and hybrid employees did not pose any cyber risk to their organization.

Given that a clear majority of CISOs today feel that insecure browsing by distributed employees not only poses risk, but poses significant risk, it is safe to assume that there is a pressing need for novel solutions to mitigate this phenomenon.

8 Most Concerning Work Applications Used by Hybrid/Remote Employees

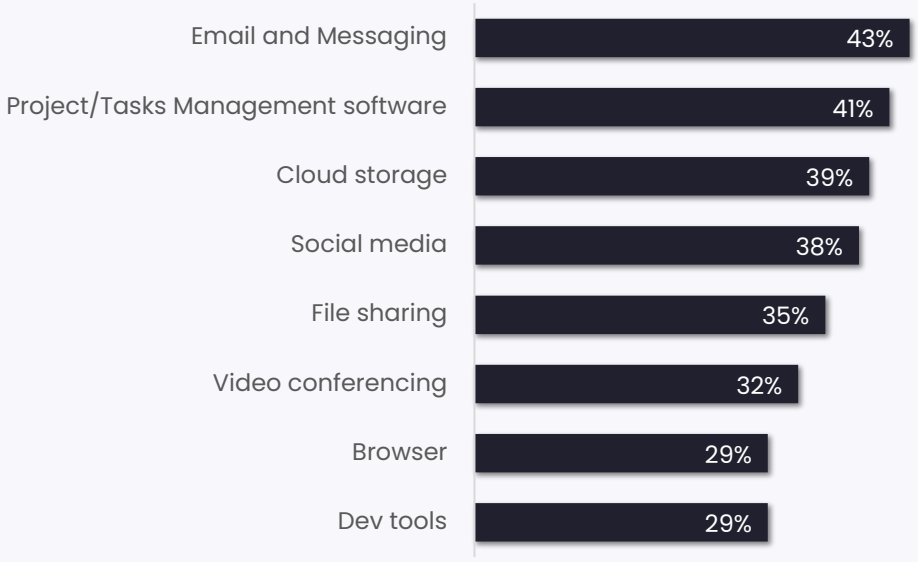
Productivity tools expand the browsing attack surface

When asked which work applications used by hybrid/remote employees were the most concerning from a security perspective, we saw a fairly equal distribution across a wide range of tools.

CISOs see the most security-concerning work applications used by hybrid/remote employees to include email and messaging (43%), project/tasks management software (41%), cloud storage (39%), and social media (38%).

Taken together, the most concerning applications are related to productivity, and perhaps more importantly, enable web connections. Ultimately, the web browser is one of many applications that enable "browsing" in a broader sense. A growing number of desktop applications feature embedded browsers themselves, and many others allow for web connections in other ways. What we find is that CISOs have serious concerns around a wide range of productivity tools, that by virtue of things like remote file access, chat protocols, and in-app browsing capabilities, bring the web browsing attack surface beyond the boundaries of web browsers themselves.

Which work applications used by hybrid / remote employees are you most concerned about from a security perspective?



Section 3

Browsing Defenses – Current Solution Realities

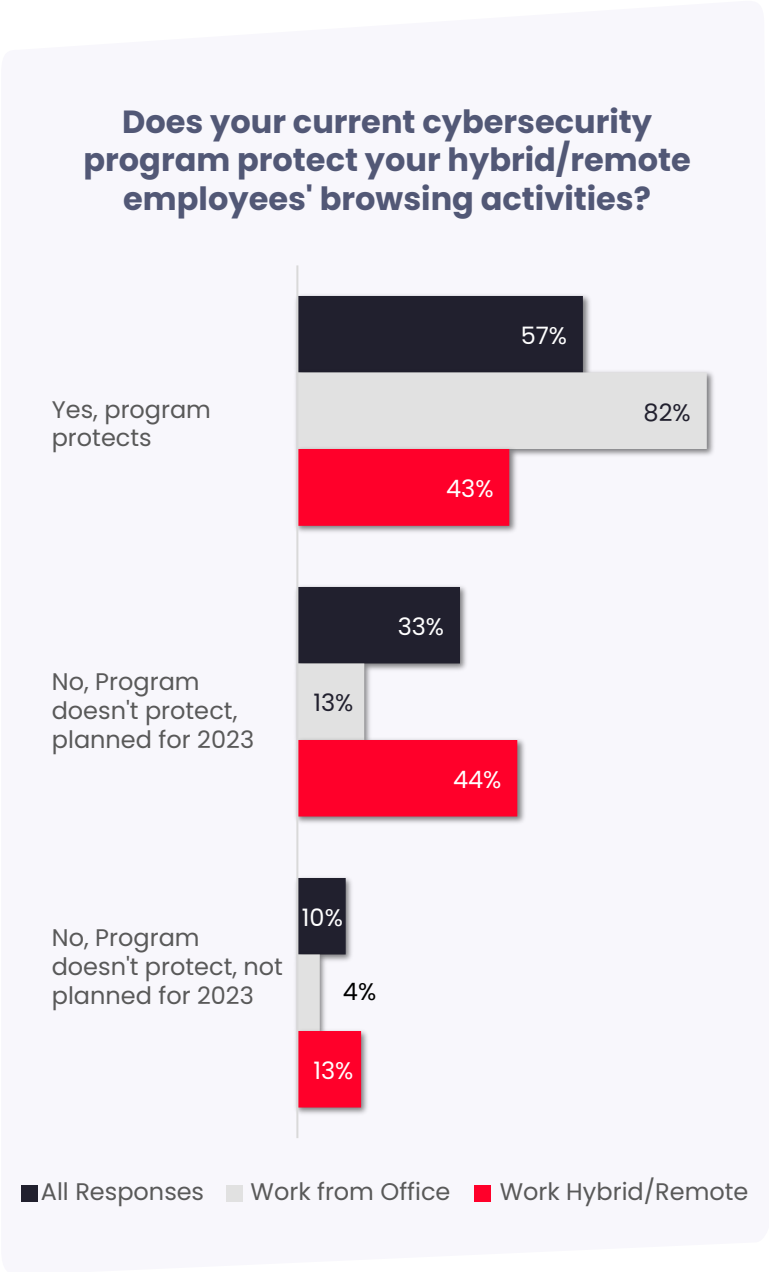
9 Current Program's Protection of Hybrid/Remote Employees' Browsing Activities

More than half of CISOs with hybrid/ remote workforces don't have adequate tools to protect their employees' browsing activities.

When we asked CISOs whether their current cybersecurity program adequately protected the browsing activities of their hybrid and remote employees, we saw a stark contrast between those that anticipate working mostly in-office and those that anticipate working in primarily hybrid or remote settings.

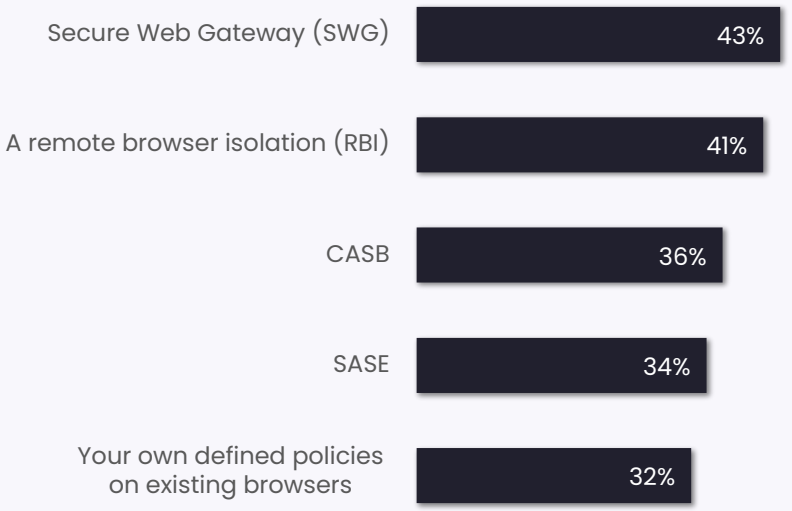
Interestingly, those that anticipated most of their employees to continue working in-office (82%) were more likely to say that their current cybersecurity program protects their hybrid/remote employees' browsing behavior. However, when we look at those who anticipate most employees to work in a hybrid or remote setting in three years' time, that figure falls by nearly half to just 43%.

The data suggests that, as the number of remote and hybrid employees increases, the less adequate these prevailing legacy solutions appear to be at browsing security. Next, we'll look at these solutions more closely and dissect where they come up short.



10 Current Solutions in Use for Protection Against Browsing-Based Threats

Which of the following technologies are you using to protect your organization from browsing-based threats?



Although Secure Web Gateways (SWGs) and Remote Browser Isolation (RBI) top the list of technologies currently in use to protect against browsing-based threats, there doesn't appear to be an agreed-upon standard.

SWGs are used by 43% of security teams today, while RBI follows closely behind with a 41% adoption rate. Cloud-access Security Brokers (CASB) and Secure Access Service Edge (SASE) tools are used by 36% and 34% of respondents, respectively.

32% of CISOs resort to implementing and using their own defined security policies on existing browsers to help guard against browsing-based threats, although these safeguards are decidedly limited in their ability to prevent and protect against most attacks.

Taken together, the data suggest that there is no consensus or agreed-upon standard for securing hybrid/remote workers' browsing activities, and no set path for protecting them against the growing scourge of browser-based threats. Let's look at why this is the case.

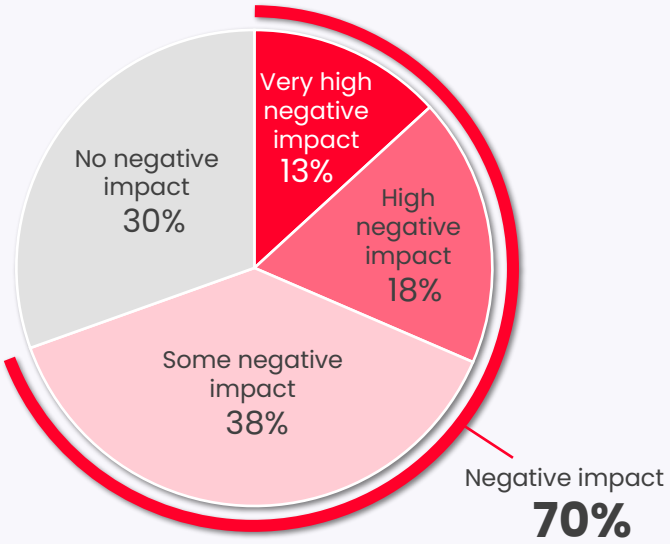
11 SWG & RBI Solutions Fall Short of Protecting Hybrid/ Remote Employees' Browsing Activities

While there is no consensus on which current tools are powerful enough to protect hybrid and remote workers' browsing activities, there appears to be a clear sense that both SWGs and RBI come up short.

Firstly, we found that 70% of organizations using either SWG or RBI felt that the hybrid workforce has a negative impact on their organization's cybersecurity posture.

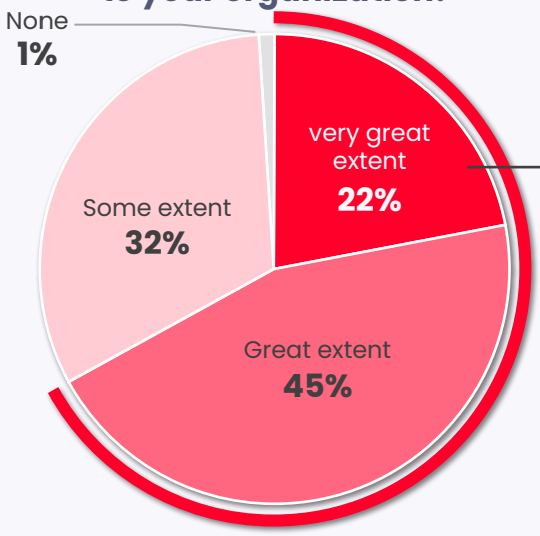
Furthermore, 99% of CISOs using either SWG or RBI solution see their hybrid/remote workforce as posing cyber risks, with the vast majority (67%) saying the risk posed was significant.

To what extent is your hybrid/remote workforce impacting your organization's security posture?



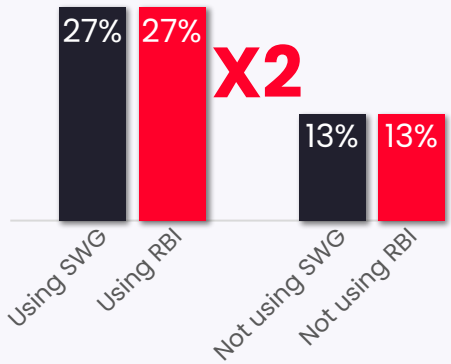
Answers from CISOs of organizations using either SWG or RBI

To what extent is insecure browsing by your hybrid/remote employees posing cyber risks to your organization?



Answers from CISOs of organizations using either SWG or RBI

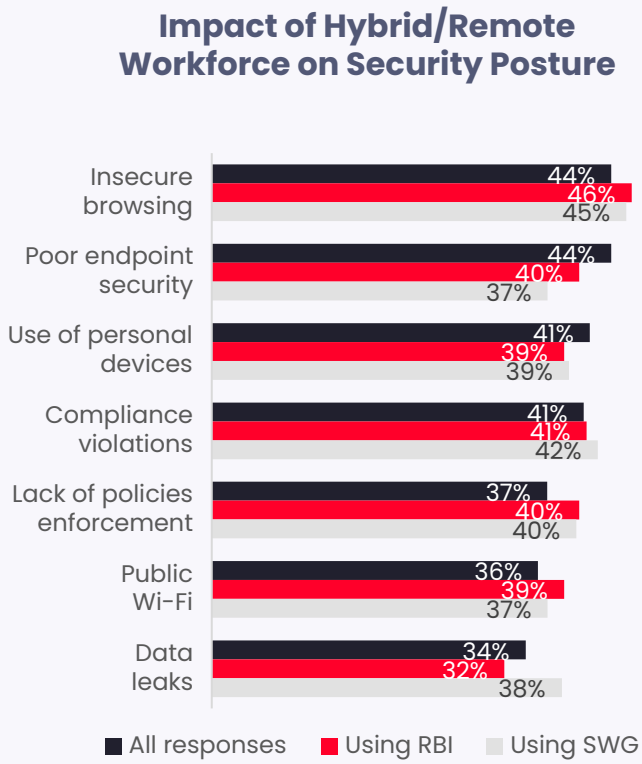
Those already using SWG or RBI were more than twice as likely to say that insecure browsing poses cyber risk to "a very great extent" than those without.



12 SWG & RBI Solutions Fall Short of Protecting Hybrid/ Remote Employees' Browsing Activities

As a matter of fact, insecure browsing tops the list of hybrid security concerns at a higher rate both for CISOs who have deployed SWG (45%) and for CISOs who have deployed RBI (46%) than it does for respondents overall (44%).

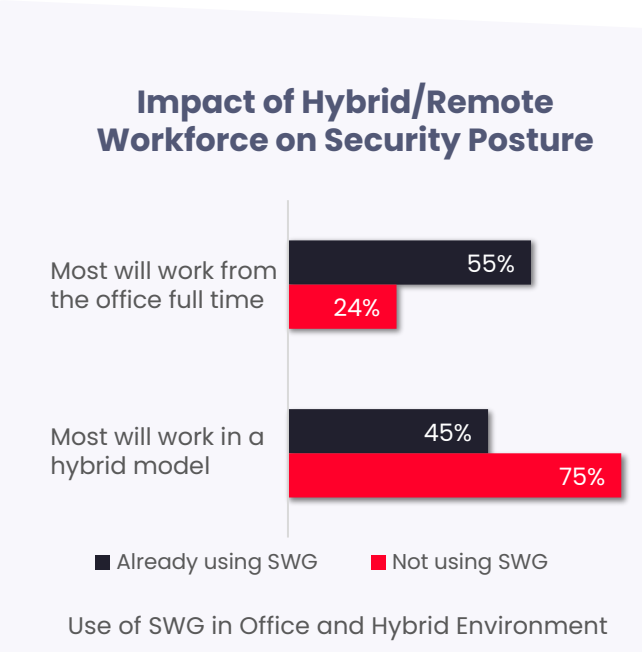
Taken together, it would seem that despite widespread adoption of these security solutions, the issue of remote and hybrid employee web browsing remains a considerable security risk for the vast majority of organizations.



SWG Spotlight:

When we looked exclusively at SWGs, we found that the rates of adoption are significantly lower at organizations in which most employees will be working in a remote or hybrid environment in three years' time (47%) than they are at organizations at which employees will be working primarily in-office (55%). Indeed, we found that 75% of CISOs not using SWG anticipate most employees working in a hybrid or remote model in three years' time.

These findings suggest that SWGs are seen primarily as solutions for in-office security, and that they are likely to be lacking in their ability to secure remote and hybrid work.



Section 4

Selection Criteria for Hybrid Security Solutions & Top Reasons for Not Having One

13 Top Criteria for Selecting Security Solutions

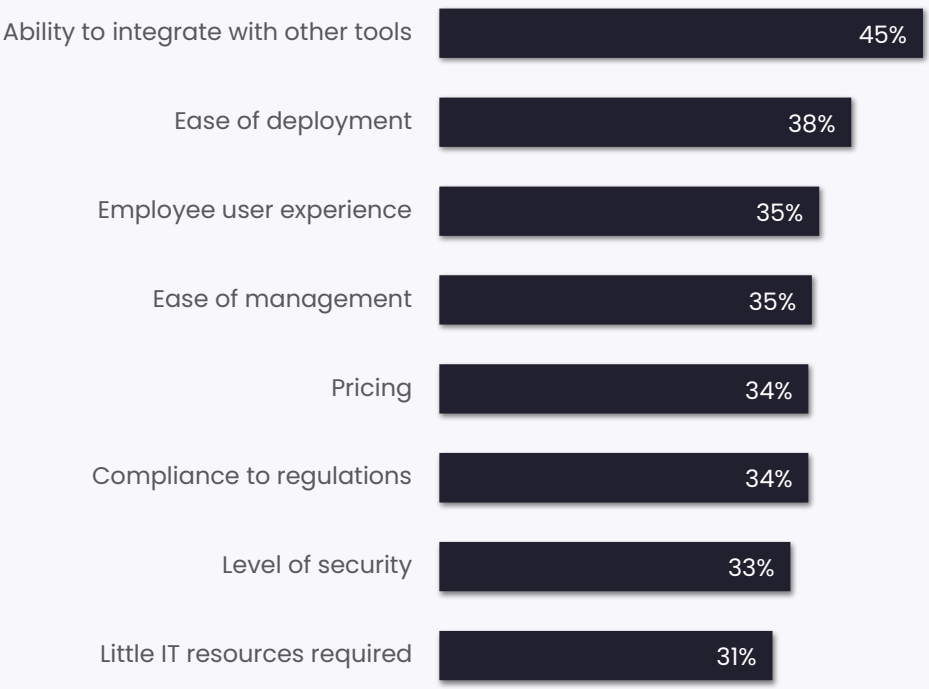
CISOs' priorities are changing — integration with other tools and flexibility in both deployment and user experience are seen as more important than pricing, compliance, and even protection.

When asked to select their most important criteria for selecting a new security solution or product, we found that "Ability to integrate with other tools" (45%), "Ease of deployment" (38%), "Employee user experience (35%), and "Ease of management" (35%) topped the list as the most important criteria.

Interestingly, these "convenience and flexibility" considerations surpassed such traditional, "bottom-line" considerations as "pricing", "compliance", and even "level of security".

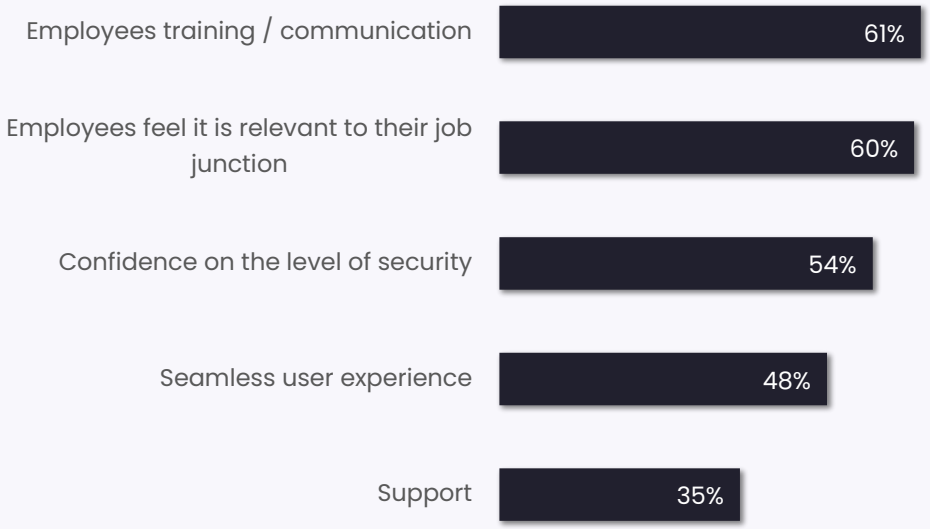
It seems that in today's cluttered and complex security landscape, ease of integration, simplicity, and ease of use (for both end users and administrators) are top-of-mind priorities for CISOs when considering adding new solutions to the stack.

In general, what are the most important criteria for you, as a CISO,when you select a security solution/product to deploy in your organization?



14 Top Criteria for Successful Adoption by Hybrid/Remote Employees

When you deploy a new security solution in your organization, what do you believe are the most important criteria to your hybrid/remote employees for its successful adoption?



The push to keep distributed teams productive shifts CISOs' priorities away from traditional concerns like customer support.

We asked CISOs, "When you deploy a new security solution in your organization, what do you believe are the most important criteria to your hybrid/remote employees for its successful adoption?"

Topping the list of considerations were "Employee training/communication" (61%) and "Employees feel it is relevant to their job function" (60%).

Both of these responses reflect a need for organizations to identify solutions that are good fits for their employees. With the rise of shadow IT upending many organizations' security initiatives, it's paramount that organizations get the buy-in from their employees and find solutions that are seen as complementary to their employees' work, as opposed to adversarial.

15 Importance of Maintaining a Seamless User Experience

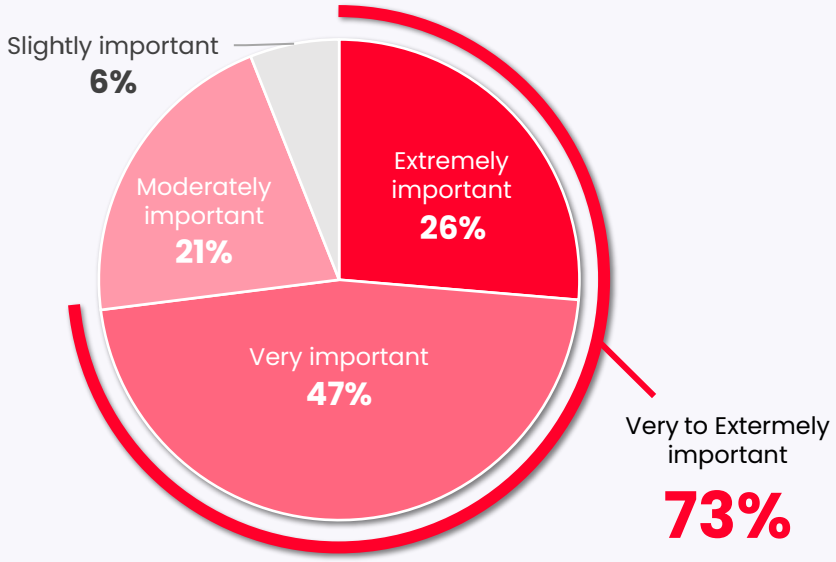
73% of CISOs agree a seamless user experience is critical for hybrid security solutions.

When examining various selection criteria for hybrid security, respondents clearly expressed that seamless user experience is a critical quality for these solutions to have.

When asked "when you select a new security solution, how important is it to you to create a seamless user experience for your hybrid/remote employees, on any device" 73% of CISOs responded that it was either "very" or "extremely important". Just 6% felt it was "slightly important" and no one felt that seamless UX was of no importance.

As remote and hybrid work become the norm, it's clear that CISOs are keen on adopting solutions that are as flexible as the work itself. To ensure security without compromising productivity or performance, today's CISOs place significant value on creating a seamless end-user experience.

When you select a new security solution, how important is it to you to create a seamless employee user experience for your hybrid/remote employees, on any device?



1. C-Suite Outlook 2023: On the Edge: Driving Growth and Mitigating Risk Amid Extreme Volatility (conference-board.org)

16 Reasons for Not Implementing a Program to Protect Employees' Browsing Activities

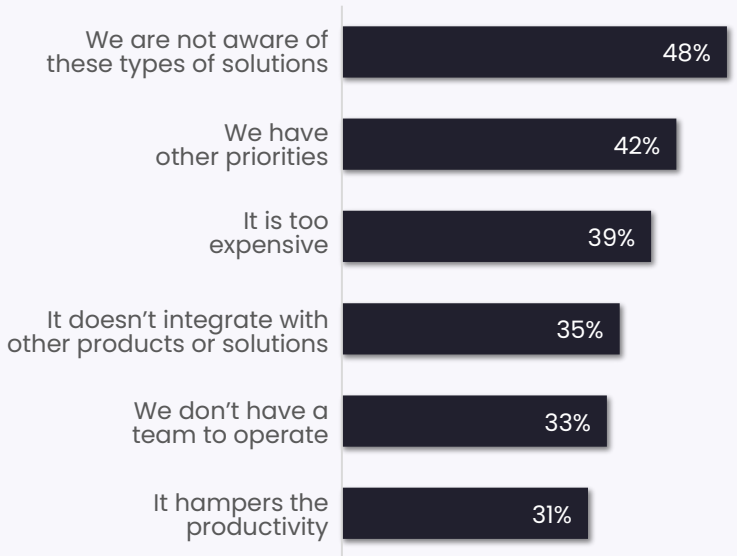
Lack of awareness: The top reason preventing CISOs from implementing a cybersecurity program to protect their employees' behavior is lack of awareness of such solutions.

Nearly half of CISOs (48%) said that the reason they had not implemented a cybersecurity program to protect employees' browsing activities was that they simply were not aware these types of solutions were available.

This is likely the main source of the apparent disconnect between surveyed CISOs' clear concern around the risk posed by browsing-based threats and the relative lack of confidence around their ability to address said threats.

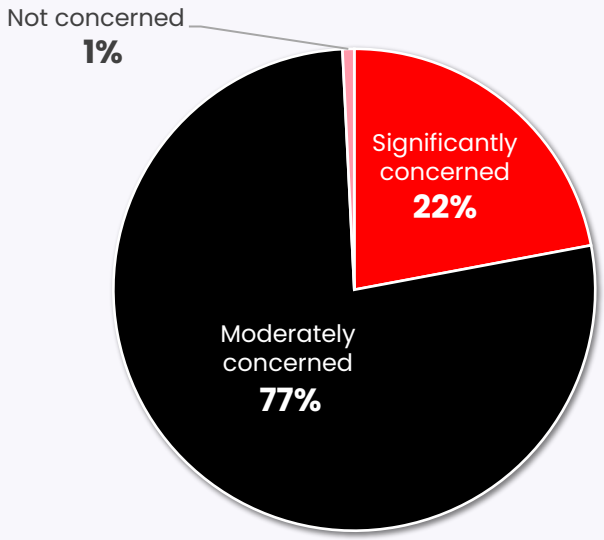
Other considerations that made the list were "We have other priorities" (42%) and "It is too expensive" (39%). Clearly, new hybrid/remote cybersecurity solutions need to easily fit into the myriad of initiatives cyber teams need to address today and they have to be affordable to enable wider access and more robust protection.

What are the main reasons you are not implementing a cybersecurity program that protects your hybrid/remote employees' browser activities?



17 Reasons for Not Implementing a Program to Protect Employees' Browsing Activities

Does your concern about a potential drop in productivity prevent you from deploying a cybersecurity program that protects your hybrid/remote employees' browsing activities?



Concern About a Potential Drop in Productivity: Virtually All CISOs (99%) are concerned about a potential drop in productivity when deploying a cybersecurity program for remote employees.

Meanwhile, nearly a quarter of respondents (22%) said they were "significantly concerned" with such a program's potential impacts on productivity. The majority (77%) reported their concern was "moderate", and just 1% said they were not concerned.

This reinforces the notion that CISOs, in their attempts to protect remote and hybrid workforces, are faced with a strong, contradictory pull to avoid any disruption to workplace productivity.

Conclusion

At the heart of this survey report we find one of the most fundamental challenges plaguing today's cybersecurity decision-makers — the disconnect between hybrid work and organizational security. Although hybrid and remote work are undoubtedly here to stay, this "new normal" poses significant security risks to the vast majority of organizations. What's more, we've found that — although legacy solutions like Secure Web Gateways (SWGs) and Remote Browser Isolation (RBI) have seen fairly widespread adoption — the vast majority of CISOs report feeling their distributed teams remain insecure.

And this remains especially true of web browsing. Thanks to the proliferation of web-enabled SaaS applications and the web browser's newfound role as the "operating system" on which we run remote work, CISOs appear increasingly concerned with web browsing as an unsecured and expanding attack surface.

Moving forward, it's imperative that organizations invest in solutions designed to protect this expanding attack surface, by incorporating a layer of dedicated browsing defense. However, this survey has made clear that for such a solution to be accepted by today's CISOs, it must be easy to deploy, easy to manage, and not hamper productivity, or otherwise disrupt the end-user experience.

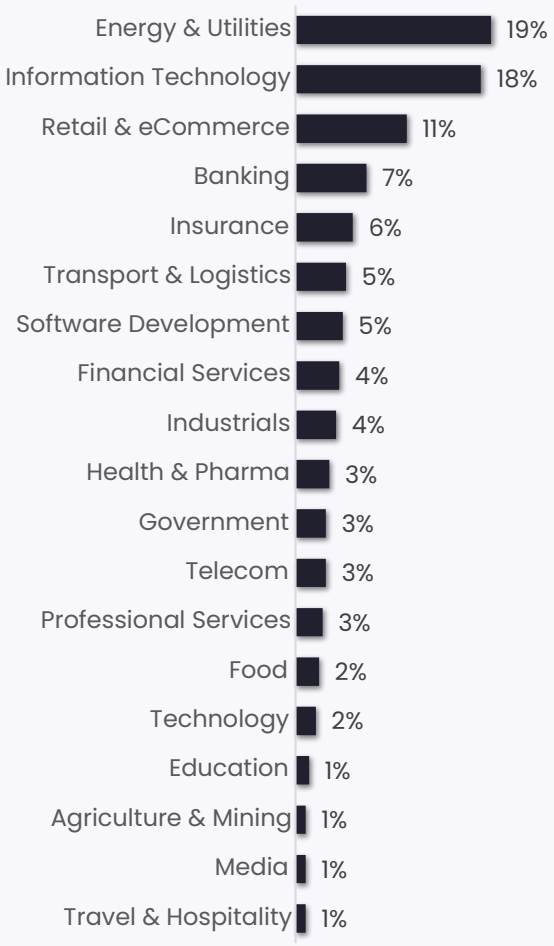
Thankfully, there are solutions out there capable of protecting your organization against this rising tide of increasingly-sophisticated browsing-based threats. What's more, these solutions are able to guarantee comprehensive protection without compromising productivity or saddling administrators with cumbersome endpoint agents. Thankfully, there's a solution capable of securing every web session, across any browser, application, or device.

Thankfully, there's Red Access.

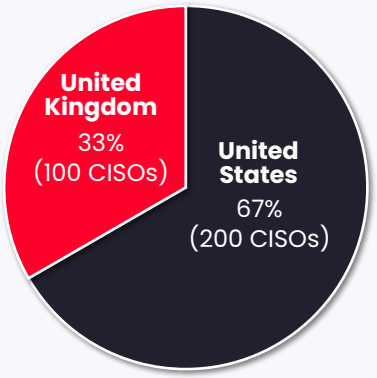
To learn more about Red Access, visit http://redaccess.io and start your free trial today.

Demographics

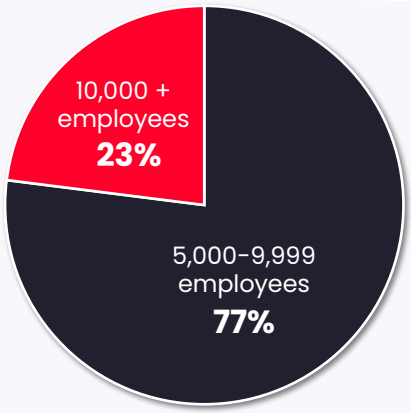
18 Country, Company Size, Department, Annual Revenue



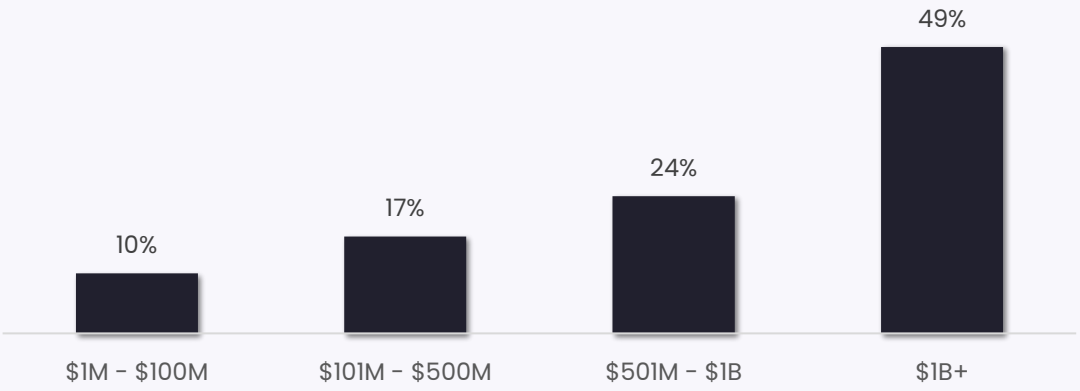
Industry



Country



Company Size



Annual Revenue

redaccess

Securing the Hybrid Workplace with Agentless Browsing Security

Brought to you by Red Access

Browsing is at the core of hybrid work and has become a main target for attackers. Red Access secures the hybrid workplace with the first agentless browsing security platform, introducing a non-disruptive way to protect devices and browsing sessions in and outside of the office. Red Access helps companies secure all the browsing activities of their employees on any browser, web app, device and cloud services, enabling them to enjoy a seamless user experience and easy management without hampering productivity and without the need to install a browser or an extension. Red Access was founded by leading experts from the Israeli Cyber Community and is headquartered in Tel Aviv. Red Access investors include Elron Ventures and Ten Eleven Ventures.

To learn more, please visit: https://redaccess.io

redaccess.io | in | | | info@redaccess.io