

The CISO's Dilemma:

**How Chief Information Security Officers Are
Balancing Enterprise Endpoint Security and
Worker Productivity in Response to COVID-19**

Survey Report • October 2020

Executive Summary

Hysolate and Team8 recently undertook a joint study of Chief Information Security Officers (CISOs) at Fortune 2000 companies to capture the CISO perspective on how the new remote-first reality and COVID-19 have reshaped organizations' approaches to IT security and worker productivity. The responses ranged from confirming what we have seen as being anecdotally true to revealing deep and surprising divisions in how different companies are responding in the face of real business continuity challenges posed by the pandemic.

Our study yielded four key findings

(plus one additional not-so-key finding situated at the end of this report):

1 **COVID-19 has accelerated the arrival of the Remote-First era**

Work-from-home is here to stay, and companies need to figure out how to thrive in the new reality.

2 **Corporate security? Or worker productivity? Remote-first has exacerbated the CISO's dilemma**

CISOs are split on whether to favor worker productivity or corporate security when enacting remote-first policies.

3 **Bring-Your-Own-PC (BYOPC) policies further confuse organizations' approaches to remote secure access**

There is no singular leading approach to enabling access to corporate assets via non-corporate endpoints.

4 **The world is ready for a new and better approach to the remote-first era**

CISOs know that today's remote access solutions leave little to be desired from the perspectives of user experience, corporate security and operational efficiency.

The COVID-19 pandemic has exposed a weakness in traditional approaches and tools that were conceived and designed for a time before the new remote-first era. Legacy remote work solutions have established worker productivity and corporate security as competing priorities in a zero-sum game.

The new remote-first era demands a fundamentally new approach to enabling remote work that is secure, regardless of the endpoint a worker chooses to use, and that delivers an efficient and satisfying user experience.

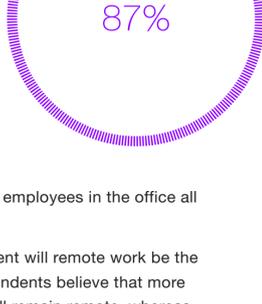
Detailed Findings & Analysis

1

COVID-19 has accelerated the arrival of the Remote-First era

This is the one that we all thought we knew already, but it's good to have the data to back it up. For months now people from all industries have been saying remote work is here to stay; it's not a fad; it's the new normal.

The preponderance of CISOs (87%) surveyed believe that their companies have now embraced remote work as a permanent workflow. [Q1](#)



13%

Just 13% believe they will go back to all employees in the office all the time.

For the rest, the question is, to what extent will remote work be the new reality? Fewer than one in ten respondents believe that more than three-quarters of their workforce will remain remote, whereas 78% believe that somewhere between one-quarter and three-quarters of their workforce will operate remotely indefinitely.

2

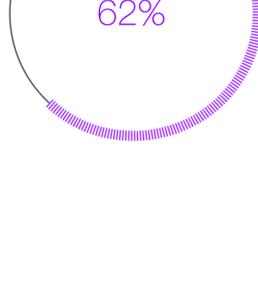
Corporate security? Or worker productivity? Remote-first has exacerbated the CISO's dilemma.

Given the traditional tool sets available to promote distributed workflows and remote work policies, CISOs have long grappled with a vexing problem: Where should they draw the line between productivity and security with their corporate access and security policies?

Limitations on Web Browsing?

Web browsing is a key issue influencing the corporate security versus worker productivity question. When asked about latitude to browse the Internet freely, 62% of respondents said their companies restrict access to certain websites on corporate devices. [Q2](#)

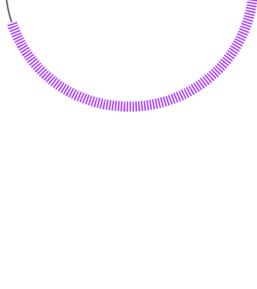
There are any number of websites that receive large volumes of traffic but that don't have any relevance to workers doing their jobs. However, challenges arise when companies limit access to websites that workers legitimately need to be able to visit in the course of a typical workday.



Restrictions on Third-Party Applications?

More than 70% of CISOs report not allowing third-party applications to be installed on corporate devices. [Q3](#)

WhatsApp, Facebook, Slack, Microsoft Teams and Zoom occupy the top slots on the list of applications that employees seek to install. While some may be better suited for personal time, it's clear that employees are looking for ways to make their days more efficient. And with the shift to remote work further blurring the lines delineating work-life balance, it is understandable that employees want access to the most popular applications and websites on the same devices they primarily use to do their jobs.



The CISO's Dilemma

Here's where we start to see splintering within our survey results. The new remote-first stance companies have been forced to assume in the wake of COVID-19 has deepened the CISO's dilemma: Is it more important to structure less stringent security policies to promote worker productivity? Or is it more important to sacrifice user experience in favor of maximizing corporate security? How should they formulate endpoint security and corporate access policies to best address the massive shift to remote work?

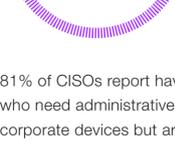
The transition to remote-first has produced mixed responses among CISOs: [Q6](#)



It's clear that the majority of companies (more than 60%) felt that they weren't ready for the changes that the proliferation of the pandemic forced. What remains unclear is whether the other 39% who have made no changes are standing pat because they are comfortable with their company's security posture or because they don't know what changes to make.



Half of CISOs believe that allowing employees to install third-party apps would increase the web freely and browse productivity. [Q5](#)



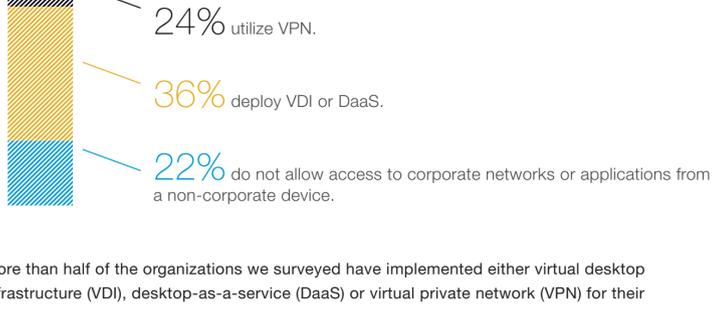
81% of CISOs report having workers who need administrative rights on their corporate devices but are reluctant to grant those permissions due to security concerns. [Q4](#)

3

Bring-Your-Own-PC (BYOPC) policies further confuse organizations' approaches to remote access.

The issue of accessing corporate assets from non-corporate-managed endpoints introduces another layer of complexity for CISOs who are navigating the shift to remote-first. As with the mixed approach to corporate access and security policies, we see that companies are utilizing a variety of strategies in addressing the access-via-BYOPC question.

There's no single standard methodology for enabling remote work on non-corporate and personal endpoints: [Q7](#)



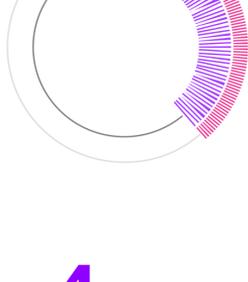
More than half of the organizations we surveyed have implemented either virtual desktop infrastructure (VDI), desktop-as-a-service (DaaS) or virtual private network (VPN) for their BYOPC security. While these are the most common solutions available, they are also known to be cumbersome both from the user perspective and from the administrative perspective. This, too, is true for zero-trust architecture, which was the secure remote access choice of very few of our survey respondents.

It is important to note that even in the current remote-first environment, more than one in five companies do not permit workers to use non-corporate endpoints to connect to company assets.

This is significant, especially when we consider the advantages that a robust BYOPC program can offer:

- Alleviates the pressure on IT organizations to procure and provision endpoints in the event of a spike in demand
- Reduces CapEx by avoiding significant procurement costs
- Improves user experience by letting end users work on a device of their choosing
- Affords end users the freedom to tap into peripherals available in their remote environments

Some organizations utilize split tunneling — accessing dissimilar security domains concurrently on the same device — to reduce the organization's VPN loads and traffic backhauling. [Q8](#) This approach is not without its detractors, however.



39% of respondents say their companies do not implement split tunneling.

Of the 61% that do, two-thirds of CISOs express doubt in the security of a split tunneling approach.

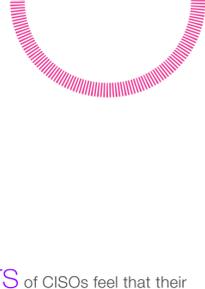
4

The world is ready for a new and better approach to the remote-first era.

The most common means for connecting workers to corporate networks and applications leave much to be desired in the eyes of survey respondents. More than 75% of CISOs report utilizing VDI or DaaS as a means to connect workers to corporate assets, but not many think their workers are happy with these solutions: [Q9](#)

Only 18% — less than one in five — say their employees are happy with their company's VDI or DaaS solution.

The other 82% are either neutral or unhappy with their company's VDI or DaaS solution.



ROI for VDI or DaaS is another sore spot for CISOs. [Q10](#)



The Big Ah-Ha!



Before the pandemic, most enterprises designed their risk appetites around the assumption that remote working was the exception, rather than the norm. When that scenario was flipped, risks such as always-on VPNs and bring-your-own-device, which were previously a lower priority for security leaders, suddenly became top of mind. This forced security teams to rapidly reassess their enterprise's risk landscape and deploy new solutions and policies accordingly.”

Jonathan Care
Senior Research Director
Virtual Gartner Security & Risk Management Summit

Decisions made around enhancing security invariably affected worker productivity. But this tradeoff exists only because companies have been dealing with traditional approaches to providing secure remote access to corporate assets. Traditional VPN, DaaS and VDI solutions aren't making the cut anymore. They're often extremely expensive to implement, and the ROI is typically too low—especially when you factor in the cost of reduced productivity and employee frustration. Not only that, but the lack of flexibility causes friction between IT and security teams and forces leaders to choose between security and productivity—as though it's reasonable to have to sacrifice one in the name of the other.

The new remote-first era calls for a new approach to corporate security and worker productivity that doesn't position these imperatives as competing priorities. There's a clarion call for a new solution that can maximize both productivity and security so that IT, security and the workforce each has a seat at the table, each has an equal share of voice, and each has its priorities fulfilled.

Introducing Hysolate

Isolated Workspace-as-a- Service

Hysolate is introducing the first Isolated Workspace-as-a-Service (IWaaS), which makes it easy to strongly isolate corporate assets, both on corporate-managed devices and on non-corporate devices. Corporate data is encapsulated on the device in an isolated environment and cannot be exfiltrated. The virtual and isolated environments deployed on users' endpoints are fully and centrally managed remotely with a robust and fine-grained set of networking, clipboard and data security policies such as access control, application management and insights across the entire workforce.

Platform Benefits

- Provides strong VM-based isolation
- Enables deployment at scale in minutes
- Does not require installation and management of an additional OS
- Eliminates VDI and DaaS data center costs
- Enables the user to enjoy a native-like user experience

Get started

And before we go...

We all know that on the best of days the CISO doesn't have it easy. But now in the COVID-19 era, the pressure is on, and many CISOs lose sleep at night worrying about all the complexities that comprise today's business continuity challenges. To help our survey respondents understand that they aren't alone in this, we asked one final question: [Q11](#) › What do you consume more of since COVID-19?



20% said Wine



32% said Coffee



8% said Whiskey

And would it surprise you to learn that

40% said All of the Above?

We hear you, and we're here for you. Reach out and we'll be happy to share a virtual beverage with you while we demonstrate how Hysolate IWaaS is the right new approach for conquering the new remote-first world.

Appendix:

Survey Questions and Interpreted Results

- Q1** What percentage of employees in your organization do you expect to return on-site when deemed safe (back to pre-covid levels)?
- Just 13% believe they will go back to 100% in-office. For the rest, the question is, to what extent will remote work be the new reality?
 - Fewer than one in ten respondents believe that more than 75% of their workforce will remain remote.
 - 78% believe that somewhere between one-quarter and three-quarters of their workforce will operate remotely indefinitely.
 - That means for the vast majority of CISOs, they're going to need to be able to support a distributed and possibly fluid workflow with some workers on-site and others working from home.
- Q2** Do you currently restrict employees from browsing certain websites (e.g. access personal email) on their corporate devices?
- 62% of companies restrict access to certain websites on corporate devices.
- Q3** What are the top 3-5 applications that your employees want to install on their corporate devices and are prohibited from doing so?
- With WhatsApp, Facebook and Slack at the top of the list, it's clear that employees are seeking ways to make their day more efficient.
- Q4** Do you have certain employees (e.g. developers) that require administrative rights on their corporate devices but you are reluctant to provide this due to security concerns?
- 81% of CISOs report having workers who need administrative rights on their corporate devices but are reluctant to grant those permissions due to security concerns.
- Q5** Do you think that employee productivity would improve by giving them the ability to browse the web with less restrictions and install third-party apps?
- 49% of CISOs believe that allowing employees to install third-party apps and browse the web freely would increase productivity.
- Q6** Has COVID-19 and so many employees working remotely caused you to rethink your endpoint security and corporate access policies?
- 26% have introduced more stringent endpoint security and corporate access measures since the arrival of the pandemic.
 - 35% have relaxed their security policies in order to foster greater productivity among remote workers.
 - 39% have left their security policies the same.
- Q7** How do employees or contractors access your corporate network or applications remotely from a non-corporate device?
- 24% utilize VPN.
 - 5% use zero-trust architecture.
 - 13% utilize multi-factor authentication.
 - 36% deploy VDI or DaaS.
 - 22% do not allow access to corporate networks or applications from a non-corporate device.
- Q8** Is VPN split tunneling a security concern for you?
- 39% do not implement split tunneling.
 - Of the 61% that do, two-thirds of CISOs express doubt in the security of a split-tunneling approach.
- Q9** How would you rate the user experience on your VDI/DaaS solutions also considering peak usage periods?
- More than 75% of CISOs report utilizing VDI or DaaS as a means to connect workers to corporate assets, but not many think their workers are happy with these solutions.
 - Only 18% — less than one in five — say their employees are happy with their company's VDI or DaaS solution.
 - The other 82% are either neutral or unhappy with their company's VDI or DaaS solution.
- Q10** How would you rate the return on investment from your VDI/DaaS solutions?
- More than three-quarters of CISOs feel that their return on investment in VDI or DaaS has been medium to low.
 - Only 24% report high ROI for their VDI or DaaS solution.
- Q11** What do you consume more of since COVID-19?
- Wine — 20%
 - Coffee — 32%
 - Whiskey — 8%
 - All of the above — 40%