HYSOLATE

Survey Report • October 2020

The CISO's Dilemma:

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

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

87%

of CISOs surveyed believe that their companies have now embraced remote work as a permanent workflow.

78%

believe that somewhere between one-quarter and three-quarters of their workforce will operate remotely indefinitely.

The vast majority of large enterprises are going to need to be able to support a distributed and possibly fluid workflow with some workers on-site and others working from home.

Legacy remote access solutions such as VDI, DaaS and VPN are not up to the surge in demand for secure remote access to corporate assets.

Virtual desktop infrastructure (VDI), desktop-as-a-service (DaaS), and virtual private networks (VPN), among others, leave much to be desired in the eyes of CISOs and are not well suited to handle the new demands of the Remote-First era.

24%

of survey respondents utilize VPN.

- **61%** of companies relying on VPN also employ split tunneling to reduce the organization's VPN loads and traffic backhauling.
- Of those that use split tunneling, two-thirds express doubt in the security of the split tunneling approach.

36%

deploy VDI or DaaS.

- Of those CISOs that utilize VDI or DaaS, only **18%** say their employees are happy with their company's VDI or DaaS solution.
- **76%** of CISOs feel that their return on investment in VDI or DaaS has been medium to low.

CISOs are split on whether to favor worker productivity or corporate security when scaling Remote-First policies.

CISOs have long grappled with a vexing problem: Where to draw the line between enterprise endpoint security and worker productivity with their corporate access policies? The sudden and rapid response to COVID-19 reveals companies moving in very different directions.

39%

have left their security policies the same.

26%

of CISOs surveyed 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.

Restrictions on worker access to external resources remains the prevailing approach.

Commingling of corporate assets and non-corporate digital properties is under scrutiny.

62%

of respondents said their companies restrict access to certain websites on corporate devices.

71%

report not allowing third-party applications to be installed on corporate endpoints.

Half

of CISOs believe that allowing employees to install third-party apps and browse the web freely would increase productivity.

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.

Five most

sought-after third-party apps

Zoom WhatsApp Facebook Slack Microsoft Teams

Bring-your-own-PC (BYOPC) policies further complicate organizations' approaches to secure remote access.

Even though enabling remote work on non-corporate and personal endpoints can accelerate the transition to Remote-First while also lowering CapEx outlays for workstations and OpEx costs for administration, BYOPC is not universally embraced.

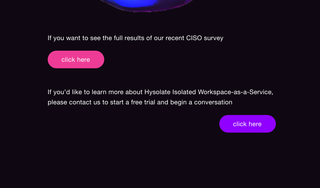
22%

do not allow access to corporate networks or applications from a non-corporate device.

The new Remote-First era opens the door for a new approach to secure remote access.

If the abrupt arrival of the Remote-First era has done anything positive, it has shone a spotlight on the inadequacies of legacy remote access solutions. Remote-First demands 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 set at the table, each has an equal share of voice, and each has its priorities fulfilled.

This is where we come in. We are Hysolate, and we are introducing the first Isolated Workspace-as-a-Service (IWaaS) solution, 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.



If you want to see the full results of our recent CISO survey

click here

If you'd like to learn more about Hysolate Isolated Workspace-as-a-Service, please contact us to start a free trial and begin a conversation

click here