HYSOLATE

The Enterprise Security Paradox: Simultaneous Calls for Increased IT Freedom and More Stringent IT Security

Survey Report, June 2021

Table of Contents

HYSOLATE

Introduction and Key Findings

Introduction

The hybrid model of working is no longer a point on the horizon, it's firmly arrived, and is now an expectation for many workers. Employees demand to work from anywhere, and we should assume devices are being used for both corporate and personal activities. However, with 70% of cyberattacks starting out at the endpoint, companies need a secure way to manage the complexities involved with long-term remote working.

At Hysolate, we were deeply interested in the ongoing battle between Security and IT teams, in terms of being able to offer both security and flexibility for remote teams. Has COVID-19 changed the way that organizations manage the remote work dynamic? Have enterprises managed to find a more productive and secure way to allow employees to use their IT devices with freedom, without sacrificing security? With these questions in mind, we spoke to 200 IT and Security leaders at US and UK-based companies that range from 500 – 10,000 employees, and at which more than 50% have annual IT budgets of more than $10M. The survey was completed by independent survey firm, Global Surveyz, and the answers were collected during May 2021.

The results showed a startling change in the dynamic of today's remote enterprises. Almost all respondents had put handling remote IT challenges on the budget for 2021. IT and Security leaders alike recognize that employees need more freedoms, and more restrictions. It's time to face these demands, and challenges head on, and create a roadmap to a reality where security and productivity aren't on opposing teams.

Key findings

01 Productivity and Satisfaction Rely on IT freedom

Stakeholders in both IT and Security are aware that the lack of IT freedom is damaging employee morale and negatively impacting productivity. 87% of respondents said that if employees could perform personal activities on their work devices, their productivity would increase. Additionally, 79% of respondents said it would reduce employee frustration. IT and Security teams also recognize that with greater freedom, employees would feel more positively towards IT policies. At the moment, just 7% of users never complain about security restrictions, while the remaining 93% look for ways to bypass them.

02 Third-party Users Are Often the Largest Concern

It's not only employee IT freedom that is a problem. 87% of respondents are concerned about the access that is being provided for third party users and contractors. This number swells to 100% of respondents in the financial services sector, which handles the most sensitive data. As the use of the cloud grows, and the prevalence of a wider connected supply chain becomes the norm, enterprises need a solution that will allow for third-party and gig economy workers to securely access corporate networks.

03 Handling Remote IT is Firmly on the Agenda

These goals aren't unknown to the enterprise. Just 7% of companies don't have a budget for handling remote IT solutions in 2021. The top technologies on the roadmap are endpoint protection, (which 62% of respondents are already using, and 33% plan to onboard) and application and browser isolation technology, already used by 55% and 48% of users respectively. Browser isolation is the technology that most respondents plan to put into place, at 42% of the vote. In contrast, VDI is losing its audience, touted highly during the pandemic, but the technology that the most respondents say they have no plans to use.

Key findings

04 The Top Uses for Remote IT Budget are Aimed at Specific Risks

The top priorities for this remote IT budget are split almost equally in half. 42% of respondents are making it a priority to isolate untrusted incoming content, while 40% of respondents believe their top concern is to find a way to allow the use of non-sanctioned applications and websites. These align well with the risky activities that employees need in order to perform their jobs. 31% of employees have to install unsanctioned applications, 25% need to provide a sandbox for their developers, and 17% need to visit corporate-blocked websites. Technology that could isolate untrusted content on corporate-managed devices would check all of these boxes.

05 IT and Security Have a Shared Goal

The days of IT and Security being on opposite teams may be behind us, with both sides of the conversation speaking with a single voice. Security teams shout the loudest, with 96% demanding that we increase employee IT freedom, and yet 91% accepting that despite the urgency of allowing employees more freedom, we also need to put more IT restrictions into place because the risks are growing in number and sophistication. Following closely behind Security teams, IT agrees with these competing necessities, at 84% and 75% respectively. Today these priorities do not need to be at odds, and can complement one another with ease. Future-focused companies are recognizing that technology could fill this essential gap, moving towards isolation-based tools that will facilitate a secure and productive remote working reality.

HYSOLATE

Budgets, Priorities, and Challenges

Increasing Employees' IT Freedom is Essential

When it comes to IT restrictions, at first glance our respondents seem to be looking to make themselves an omelet without breaking any eggs. Almost all survey respondents (87%) want to increase their employees' IT freedoms from anywhere (figure 1) yet at the same time, 79% want to increase IT restrictions on employees (figure 2) and 87% are worried about opening access to third-parties and contractors (figure 3). It's clear that both IT and security are aware of the necessity of IT freedom for employees and third parties, but that it needs to be managed in a secure way.

Figure 1 Employee IT Freedom

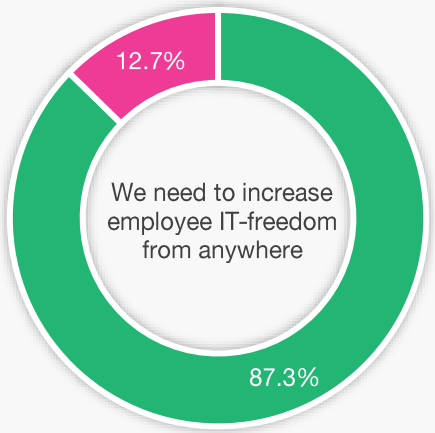
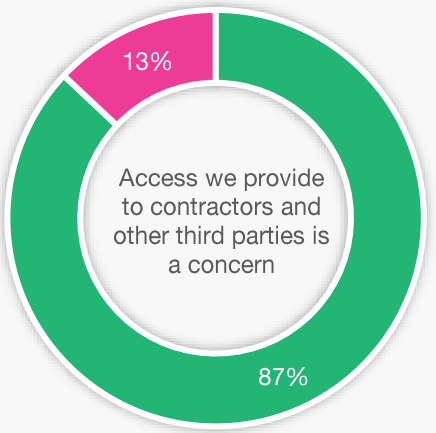


Figure 2 Restrictions for Employees

Figure 3 Access to Third-Parties



Agree Disagree

IT Restrictions – IT vs. Security

While there is an overall agreement on wanting to increase employee IT freedom from anywhere (87%, page 8), we see some differences when comparing IT to Security and between different industries.

Though one might think Security would take the lead on imposing more restrictions and less employee freedom, a different picture emerges from our results. Security is loudest when it comes to the need to provide more freedom to employees (96% in Security agree with this, compared to 84% from IT). At the same time, they also lead the way on imposing restrictions for employees and also agree that third party access is a concern (figure 4).

When compared by industry (figure 5), we see how the Retail and Financial Services sectors are worried about access for contractors and third parties, with 100% of them agreeing this is a problem (compared to 78% of Technology companies).

Figure 4 IT Restrictions – IT vs. Security

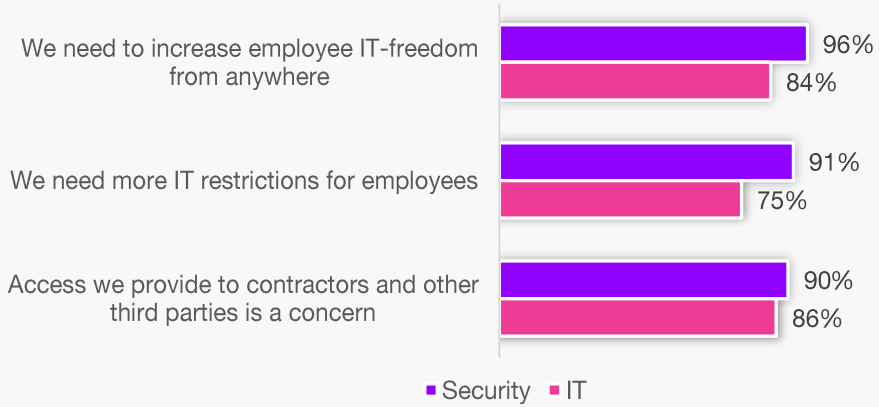
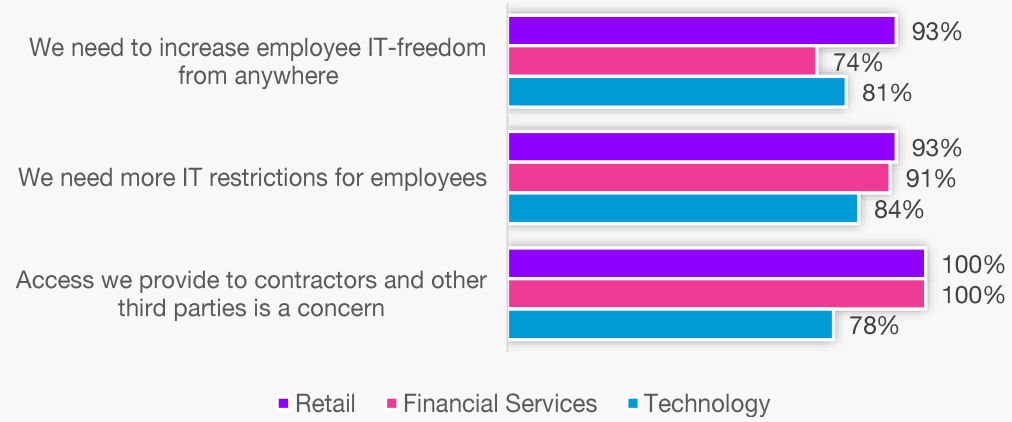


Figure 5 Need to Increase Employee IT freedom from Anywhere, by Industry



Employees Are Working Around Organization's Corporate IT Restrictions

While there is an overall positive sentiment towards opening up IT freedom for employees (pages 8, 9), employees are not waiting for freedom to come to their doorstep.

According to survey respondents, only 7% of employees are satisfied with their corporate IT restrictions, and the vast majority (93%) are working around IT restrictions (figure 6).

IT and Security are not seeing eye-to-eye on this (figure 7). Security leaders said 43% of users are in most cases working around IT restrictions, while IT believes 23% of users work around IT restrictions most of the time, a much smaller number.

Figure 6 How Employees Handle Organization's Corporate IT Restrictions

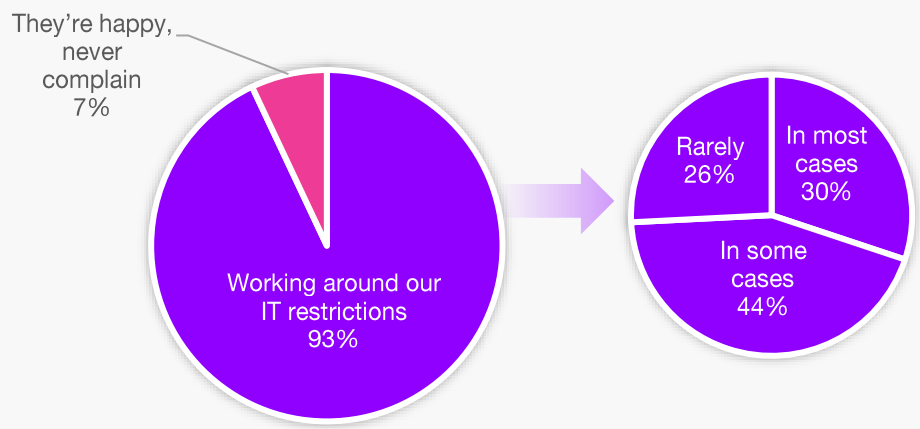
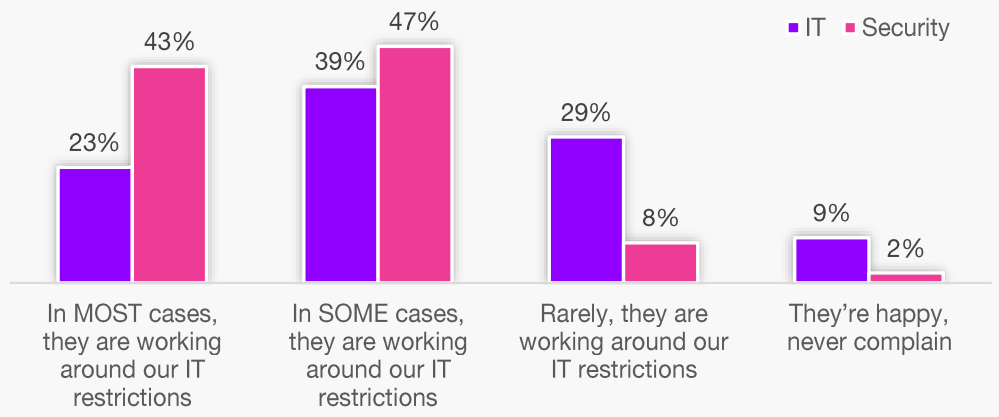


Figure 7 How Employees Handle Organization's Corporate IT Restrictions – IT vs. Security

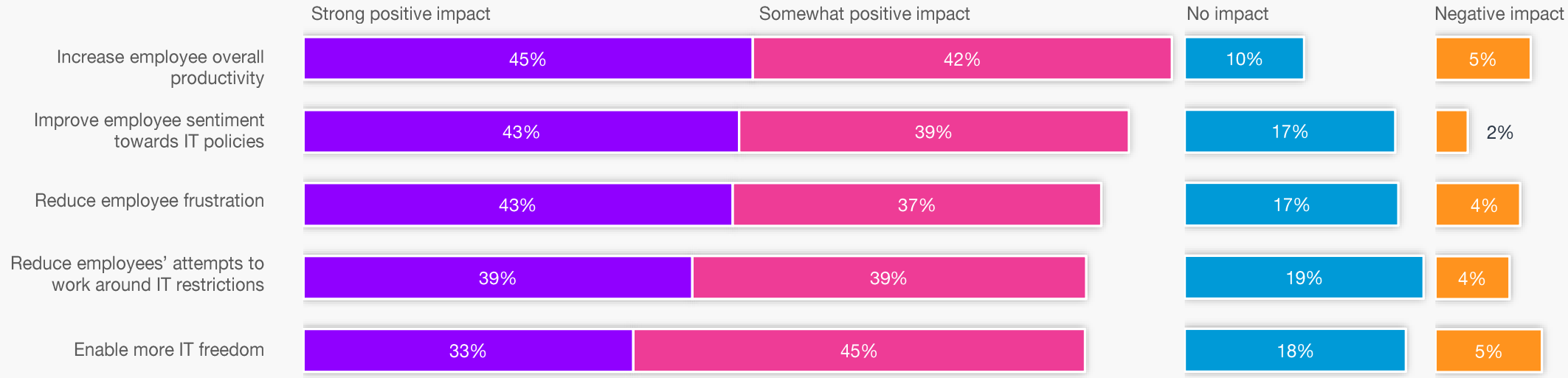


Impact of Providing IT Freedom to Users

87% of survey respondents are looking to increase employee IT freedom (page 8) We asked survey respondents what the impact is of allowing users to browse the web more freely on corporate devices. This includes behavior such as installing 3rd party apps/plugins, printing at home as well as performing personal activities.

The top three positive impacts as indicated by survey respondents were increase employee overall productivity (87%), increase employee sentiment towards IT policies (82%) and reduce employee frustration (79%).

Figure 8 Impact of Providing IT Freedom to Users



Risky IT Activities that are 'Mission Critical' for Employees

90% of employees have required IT activities as part of their job that they would call “risky”. (figure 9). The top risky activities are installing unsanctioned applications (31%), giving developers a sandbox environment (25%) and using endpoints for personal activities (17%).

The top industries, in terms of installing unsanctioned applications (figure 10) are Retail (46%), Energy & Utilities (45%) and Insurance (45%).

Figure 9 Risky IT activities Employees Need to Engage With

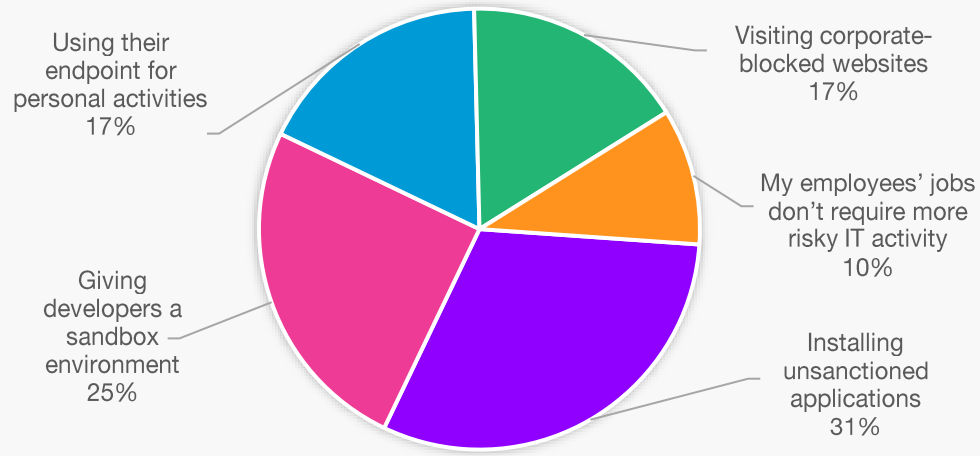
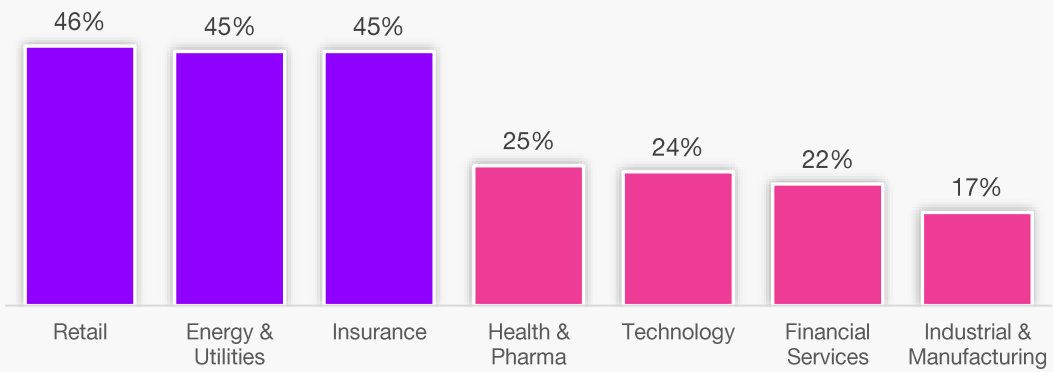


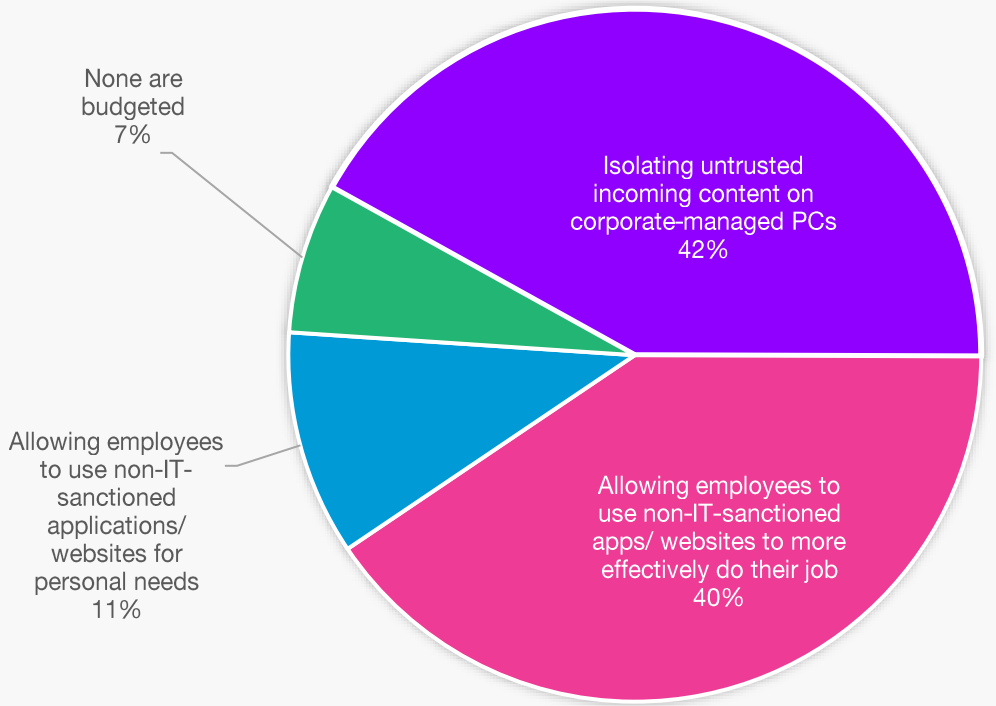
Figure 10 Installing Unsanctioned Applications by Industry



Top Remote IT Budget Priorities, 2021

93% of survey respondents have managing Remote IT as a budget item for 2021. The top budget items, split almost evenly are isolating untrusted incoming content (42%) and allowing the use of non-IT-sanctioned applications & websites that are required for their jobs (40%).

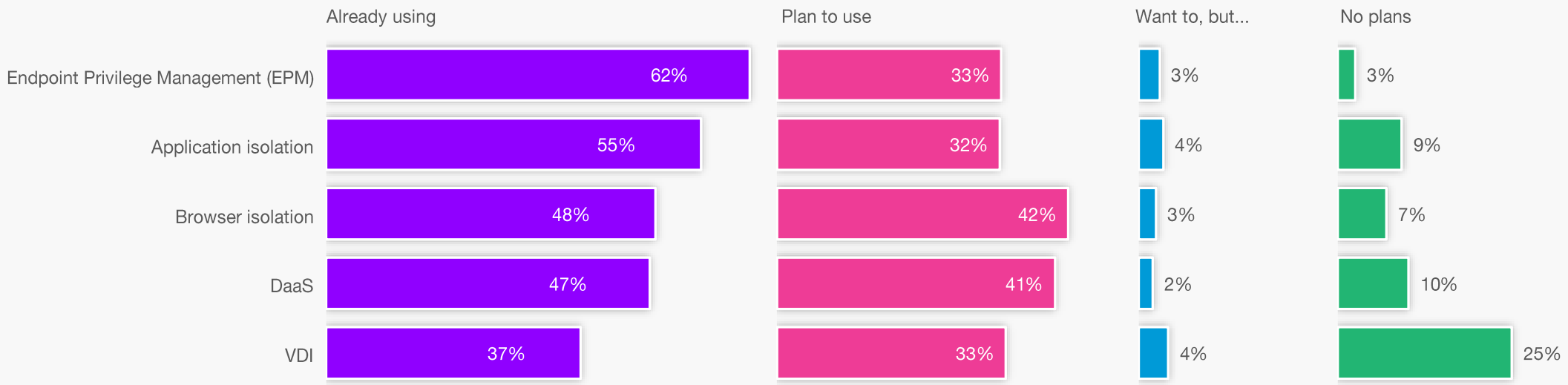
Figure 11 Remote Browser Isolation Solution – Use and Plans



Technology Map for Securing IT Ops

Looking at the technologies in use for securing IT Ops, the top three in use are EPM (62%), Application isolation (55%) and Browser isolation (48%). The top technology that companies are planning to use is Browser isolation (42%). The next isolation-based solution that companies are planning to use is Application isolation, at 32%.

Figure 12 Technology Map for Securing IT Ops



What Have We Learned?

The near-universal calls in this study from both IT and Security for moving enterprises in diametrically opposed directions toward greater IT freedom and more stringent IT restrictions concurrently demonstrate wide recognition that enterprises need a much more nuanced set of secure remote access capabilities to balance worker freedom and satisfaction with corporate security.

These results reveal an intriguing evolution in thinking from those garnered in our 2020 industry report, *The CISO's Dilemma*, in which IT and Security leaders viewed worker productivity and enterprise security as mutually exclusive objectives, either of which could be satisfied only by sacrificing the other. The collective learning accelerated by the global shift to remote work in response to the COVID-19 pandemic is pushing enterprises to rethink their approaches to enabling secure access to corporate resources from anywhere.

There was a time that solutions like virtual desktop infrastructure (VDI) were manageable for enabling secure remote access for a fraction of the enterprise's workforce. However, the clear movement today away from VDI indicates that IT and Security leaders recognize the need for a multifaceted approach to orchestrating secure remote access at scale. Enterprises need solutions that can simultaneously free workers to engage in the full breadth of their job responsibilities while making sure that the most risk-laden tasks (downloading email attachments, installing 3rd-party applications, browsing questionable websites, etc.) can be accomplished without compromising enterprise security. This report shows that isolation technologies are steadily gaining attention as a primary means for solving the Enterprise Security Paradox.

HYSOLATE

Demographics

Company Size, Job Roles Seniority and Departments

Figure 13 Company size

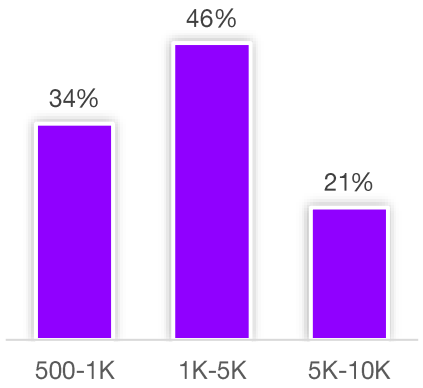


Figure 14 IT Budgets, 2021

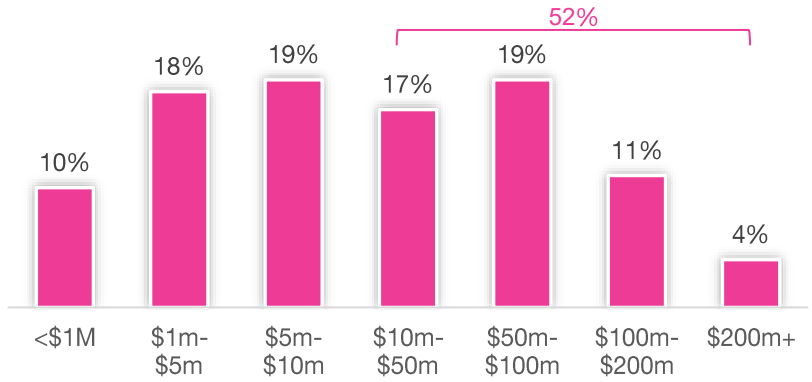


Figure 15 Department

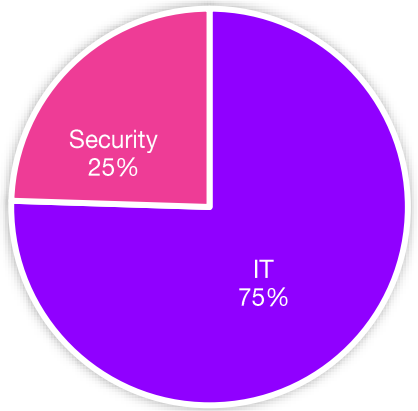


Figure 16 Job seniority

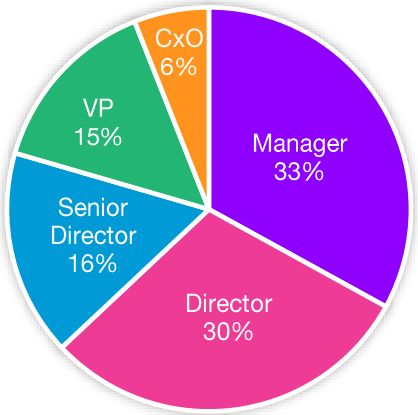
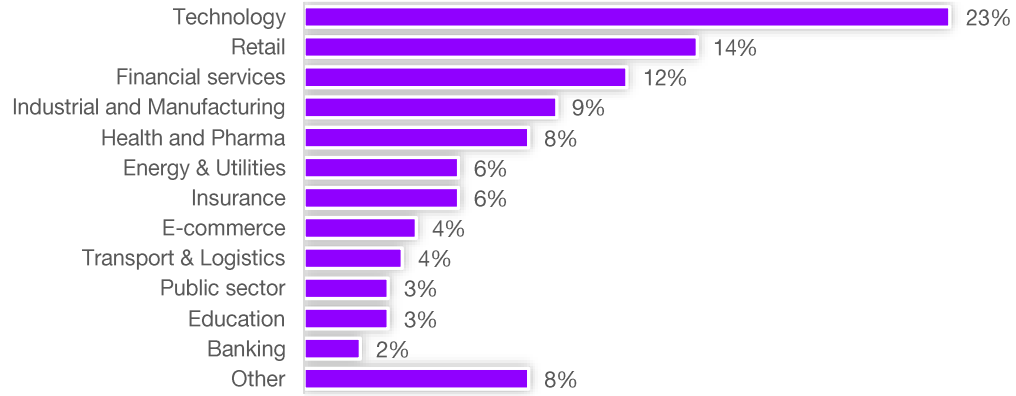


Figure 17 Industry



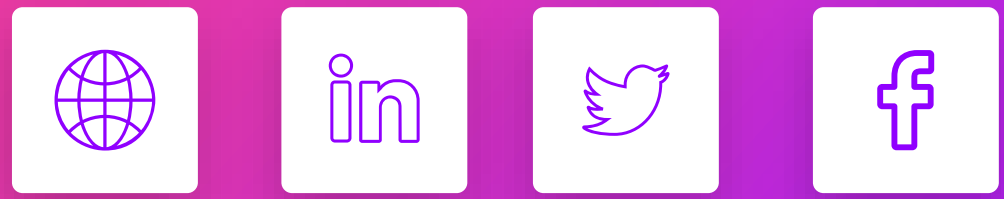
About Hysolate

Hysolate enables organizations to isolates risky or sensitive activities on users' endpoints with a local workspace that isolates applications and data. Hysolate has reinvented how an isolated virtual environment is instantly deployed on a user's device and remotely managed from the cloud. With Hysolate you can "split" the user's device into two isolated environments so users can work freely and be productive without compromising security.

Hysolate is backed by Bessemer Venture Partners, Innovation Endeavors, Team8 and Planven Capital.

Download Hysolate Free

For more information, please visit us:



Email: free@hysolate.com