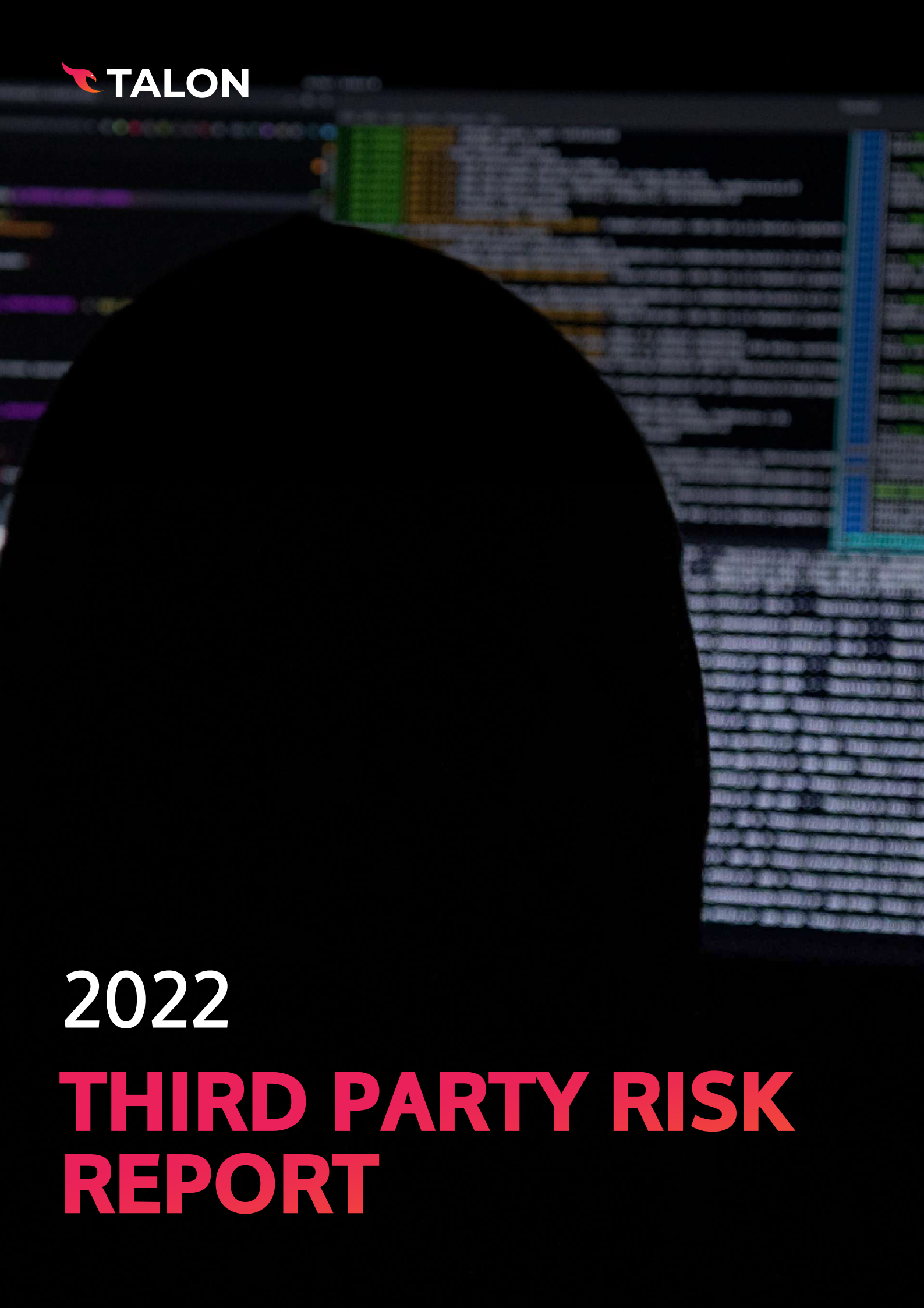


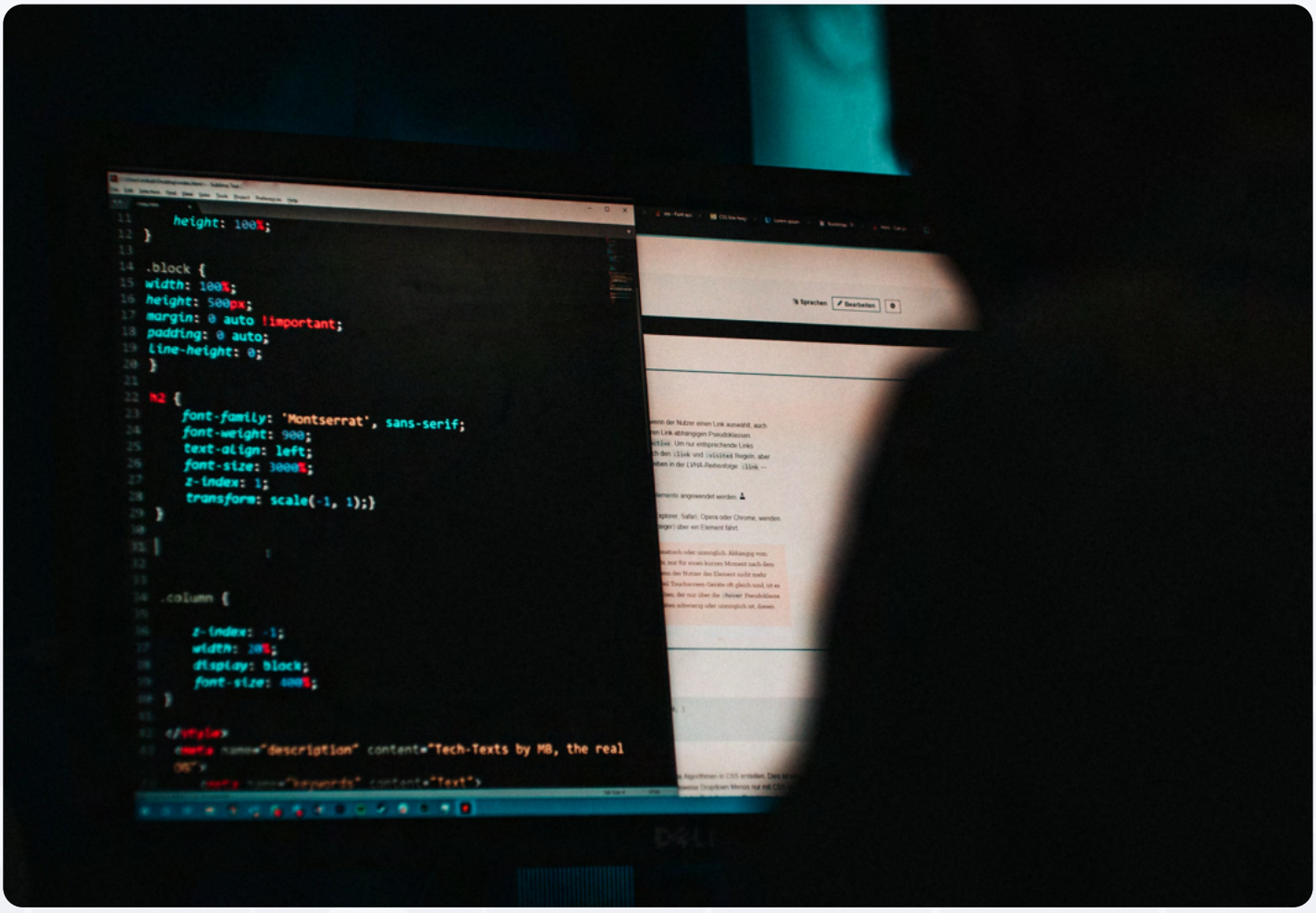
2022

THIRD PARTY RISK REPORT

TALON

Table of Contents

1. Executive Summary
2. Remote work remains prominent for third-party workers
3. 89% of third parties use personal devices for work, creating potential business risks
4. Risky behaviors carried out by contractors could leave organizations vulnerable
5. VDI / DaaS used by 45% of third-party workers, despite high costs and security concerns
6. Talon Recommendations



Executive Summary

The 2022 Talon Cyber Security Third-Party Risk Report represents the findings of a survey of 258 third-party workers, including contractors and freelancers. The results show the IT and security conditions under which they conduct business on behalf of organizations, including work models, types of devices, security technologies used, and potentially risky actions they carry out.

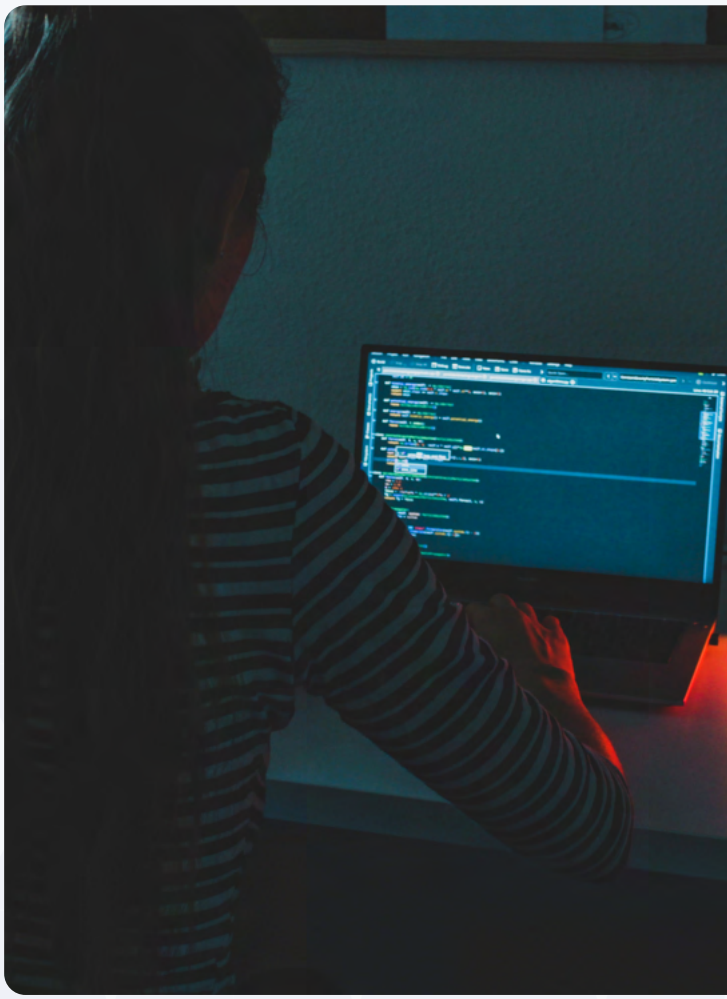
Third parties have become absolutely vital for organizations, providing flexible scalability and offering immediate bandwidth to enable businesses – adding value across a variety of functions by performing mission-critical tasks. However, as we have seen with countless recent breaches, they can create very real security risks.

According to a Ponemon report, 51% of businesses have suffered a data breach caused by a third party. To add to this, Verizon's 2022 Data Breach Investigations Report found that a whopping 82% of breaches involve a human element, where an individual carries out negligent or risky behavior, making a mistake that enables cyber criminals to access an organization's systems.

With third parties at the epicenter of many security incidents, the findings uncover how and why third parties create so much risk for organizations, creating a need to evolve security programs.

In particular, this report showcases:

- Current work models that third parties follow
- The types of devices that contractors and gig workers conduct business from
- Behaviors third parties exhibit that increase risk
- Security solutions that organizations use to secure third parties
- The extent to which security tools impact productivity
- Recommendations on how organizations can improve security for third parties

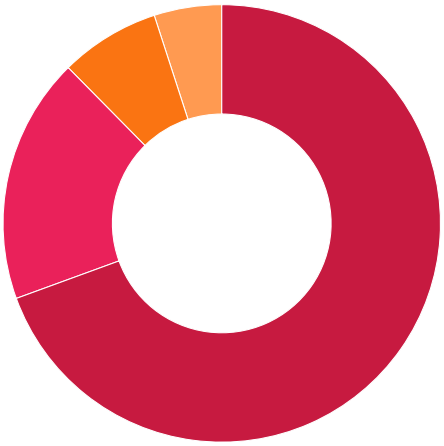


Remote work remains prominent for third-party workers

Remote work continues to be prevalent for third parties. The survey revealed that most (88%) third-party workers are remote the majority of the time. This is not surprising given that contractors and freelancers are known to work for multiple companies at one time to maximize their earning potential and fill their work weeks.

While the norm, remote and hybrid work models likely contribute to the third-party worker security issue that so many organizations are facing. In fact, a study from Tenable found that 80% of security and business leaders feel their organization is more exposed to risk as a result of remote work. A likely reason? Businesses often struggle to verify the security posture of remote devices and extend enterprise defense to distributed workers.

Considering a typical week, where do you work?



- **69.4%**
  Approximately **76-100%** remote
- **18.2%**
  Approximately **51-75%** remote, and rest of the time in a company office
- **7.4%**
  Approximately **20%-50% (1-5 days)** remote, and rest of the time in a company office
- **5%**
  Approximately **1-19%** remote, and rest of the time in a company office
- **0%**
  100% of the time in a company office

89% of third parties use personal devices for work, creating potential business risks

When thinking about third-party security, some organizations opt to ship corporate laptops to contractors to ensure secure device posture. However, the survey results indicate that this practice is losing traction in favor of more convenient alternatives.

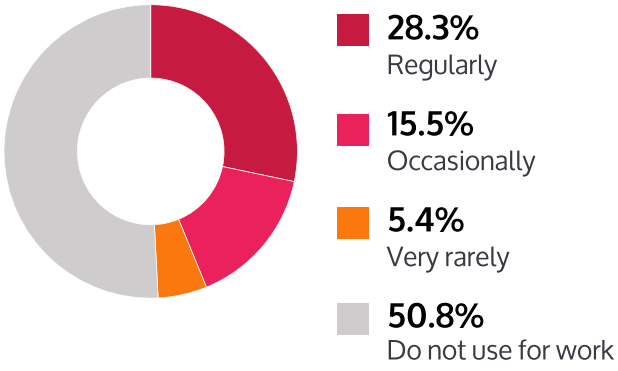
Over half of respondents indicated that they do not use company-provided or company-reimbursed machines for work, with less than 30% of third parties using such devices on a regular basis.

Personal laptops, computers, and tablets are the most used devices, as a staggering 89% of respondents said that they use them for work. This is a reality for security and IT leaders to make note of, given that personal risks can easily become business ones if a device becomes infected.

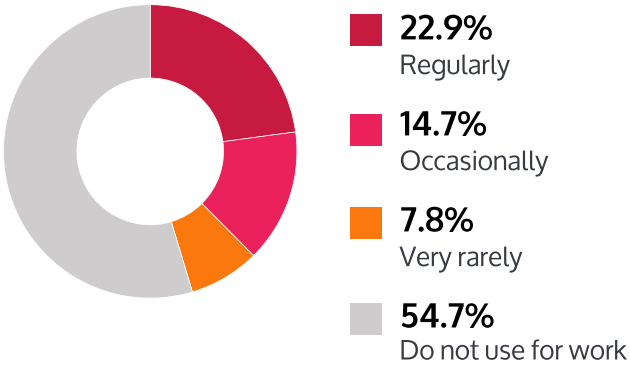
With the majority of third parties using personal devices to conduct business on behalf of organizations, it is imperative that technology leaders put processes in place to make sure they extend the organization's security posture to these unmanaged devices.

Which of the following do you use to do your work?

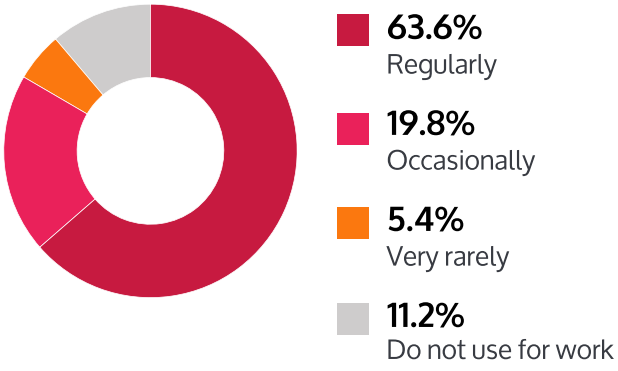
Company-provided laptop/PC/tablet



Laptop/PC/tablet you bought that company paid for



A personal laptop/PC/tablet



Risky behaviors carried out by contractors could leave organizations vulnerable

Remote and hybrid work models are no longer a "new" normal, they are simply the reality, providing unmatched flexibility and opportunity not only for workers, but companies as well. With this, the line between work and life has become increasingly blurry.

With most third parties working from unmanaged, personal devices, our results also show that the majority also carry out risky behaviors:

- **76%** browse the internet for personal needs
- **72%** indulge in online shopping
- **75%** use personal email
- **53%** play games
- **36%** allow family members to use their device

While these actions may seem harmless, it is well-known that third parties are ripe targets for attackers. Crafty cyber criminals can look to exploit these actions to launch targeted phishing attempts, execute drive-by download and other malware campaigns, and more.

In addition to risky personal tasks, it appears that password security best practices are not always followed by third-party workers. 62% have at least on occasion saved weak passwords in their web browser, and 24% have shared weak passwords with other co-workers.

As organizations continue to leverage third parties, these results suggest that proper cybersecurity training should be a part of the onboarding process for these workers. While not all personal behaviors are going to lead to a device becoming infected, they undoubtedly increase an organization's risk profile.

76.4%

browse the internet for personal needs

71.7%

indulge in online shopping

75.2%

use personal email

53.1%

play games

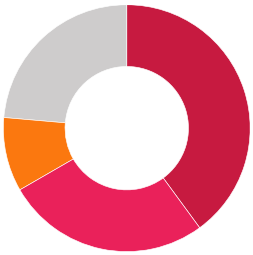
36.2%

allow family members to use their device

Have you ever done any of the following on a work laptop/PC/tablet?

Used for personal browsing

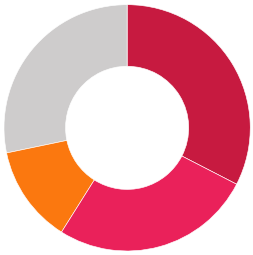
76.4% of contractors conduct personal browsing on work devices



- **39.9%** Regularly
- **26.7%** Occasionally
- **9.7%** Very rarely
- **23.6%** Do not do

Used for online shopping

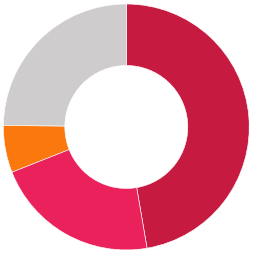
71.7% of contractors admit to doing some online shopping from device they work from



- **32.6%** Regularly
- **26.4%** Occasionally
- **12.8%** Very rarely
- **28.3%** Do not do

Used for personal email

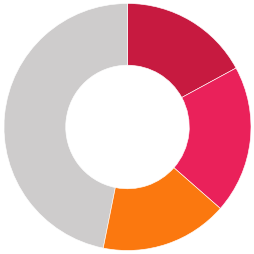
75.2% noted they sometimes use their work device for personal email



- **47.3%** Regularly
- **21.7%** Occasionally
- **6.2%** Very rarely
- **24.8%** Do not do

Played games

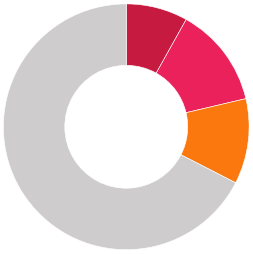
53.1% noted they have played games on their work device



- **17.1%** Regularly
- **19.4%** Occasionally
- **16.7%** Very rarely
- **46.9%** Do not do

Used by a family member

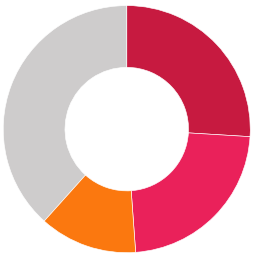
32.6% admitted they allowed a family member to use the device they work from



- **8.1%** Regularly
- **13.2%** Occasionally
- **11.2%** Very rarely
- **67.4%** Do not do

Saved one or more weak passwords in a browser

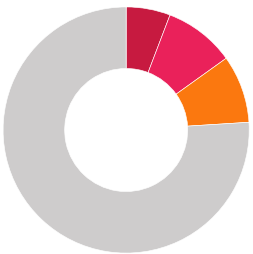
61.6% noted they have saved weak passwords in the browser on the device they work from



- **26%** Regularly
- **22.9%** Occasionally
- **12.8%** Very rarely
- **38.4%** Do not do

Shared weak passwords with other co-workers

24% have shared weak passwords with other co-workers



- **5.8%** Regularly
- **9.3%** Occasionally
- **8.9%** Very rarely
- **76%** Do not do

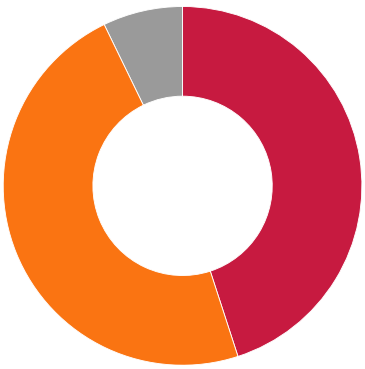
VDI / DaaS used by 45% of third-party workers, despite high costs and security concerns

In looking at what technologies third parties use to access work applications, Virtual Desktop Infrastructure (VDI) and Desktop-as-a-Service (DaaS) solutions are prominent, with 45% of respondents using these technologies.

The results indicate that many organizations are leveraging VDI and DaaS solutions to provide a secure pathway for third parties to connect back to the business. These technologies are prone to creating environments that are complex, require expensive overhead, deliver inconsistent user experiences for workers, increase security risks, and can be incredibly expensive.

As hybrid, distributed work models continue to be the norm for third-party workers, it will be interesting to see if VDI and DaaS usage decreases in favor of solutions that are better suited to secure and enable frictionless distributed work.

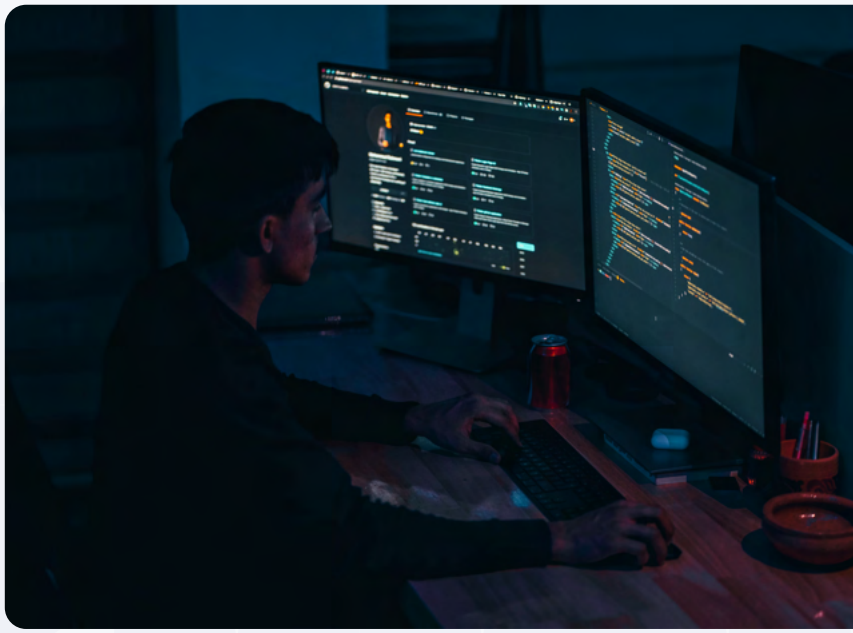
Which of the following do you currently use to access work-related applications?



45%
VDI / DaaS solution

47.8%
No VDI / DaaS solution

7.2%
I don't know



Nearly half of third-party workers have productivity impacted by security and IT tools

Remote work is coveted by so many, due to flexibility and healthy work-life balance it can provide.

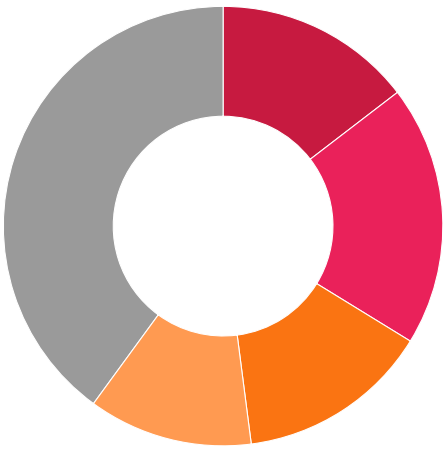
However, respondents indicate that end-user frustration is a very real thing for remote third-party workers, as 48% of respondents say that IT and security tools impact their productivity in some way.

This is not shocking, as it is well documented that security and IT tools can affect the end-user experience to some degree, despite great strides made by vendors.

Perhaps most surprisingly, 40% of third parties do not use any IT or security tools at all to enable remote work, a shocking figure when considering the number of high-profile data breaches that have resulted from such workers finding themselves in the crosshairs of attackers.

Which of the following best describes the impact of the IT and security tools you use to enable remote work on your productivity?

Only 60% of contractors use security tools to enable remote work



- **14.6%** Corporate IT and security tools materially impact my productivity
- **19.2%** Some impact on productivity
- **14.2%** Minimal impact on productivity
- **12.1%** No impact
- **40%** I don't use any IT or security tools to enable remote work

Talon Recommendations

Based on the responses received from third-party workers through this survey, Talon has several core recommendations for business and security leaders to consider:

- Extend your cybersecurity training and practices to all parties that are responsible for enabling your business, including third-party workers.
- With IT and security tools impacting productivity, invest in solutions that reduce security risk and cause little-to-no impact on the overall employee experience. Security should be an enabler for individuals and the business, not a roadblock.
- Gain visibility into the unmanaged devices used across your environment. With 89% of third parties working from personal devices, this is critical to ensure their personal risks remain isolated from your business.
- With 45% of workers using VDI and DaaS solutions to connect to the businesses they work for, security and IT leaders should evaluate the ROI of these investments.

The Bottom Line?

Third-party workers have become critical to the success of modern enterprises. As such, their habits and overall security posture should be a critical priority for security and IT teams.

The results of this survey paint a picture of a third-party worker landscape that is far from ideal for CISOs, and is something that should be addressed to the best of the ability of any modern enterprise.