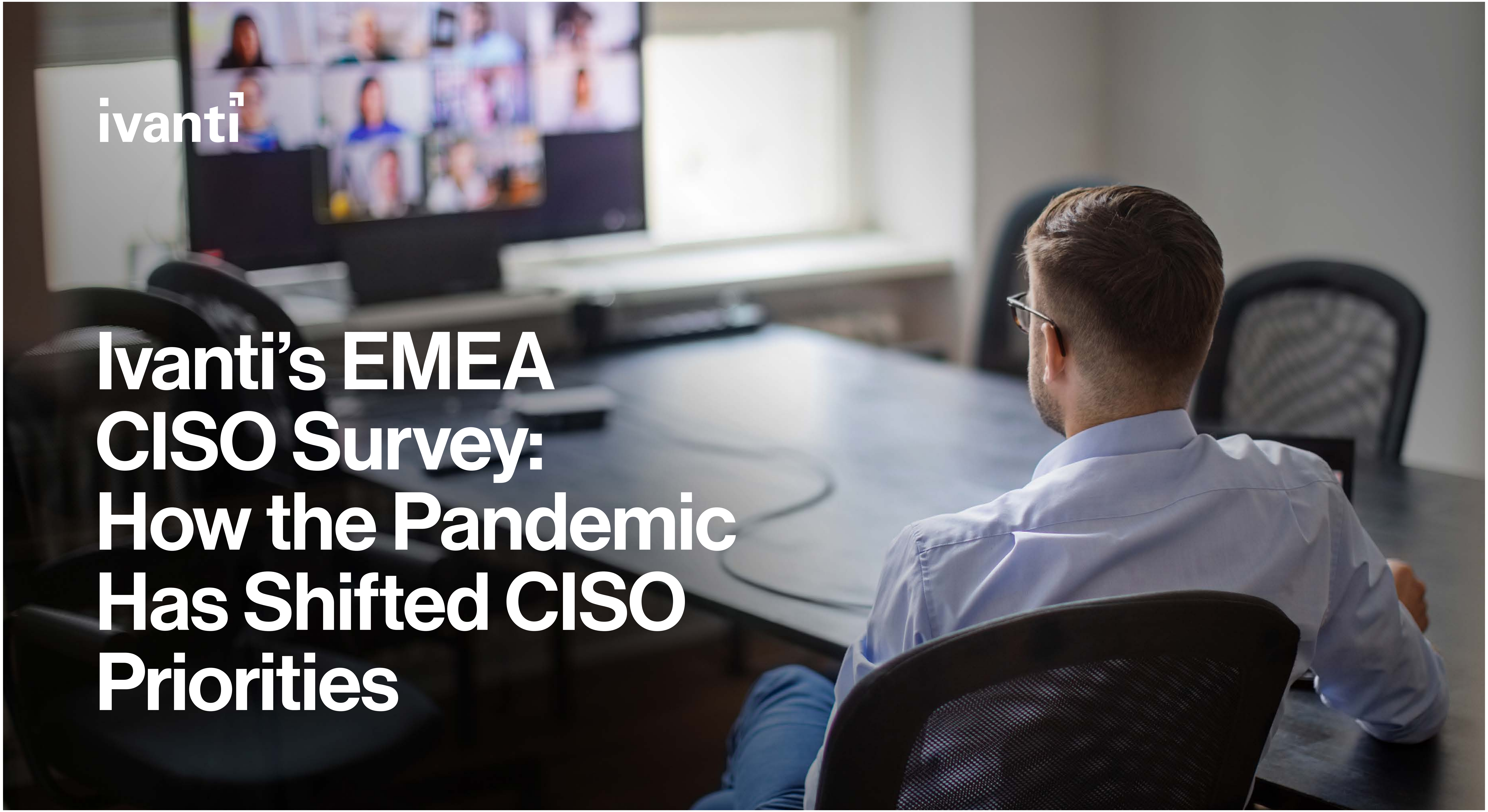


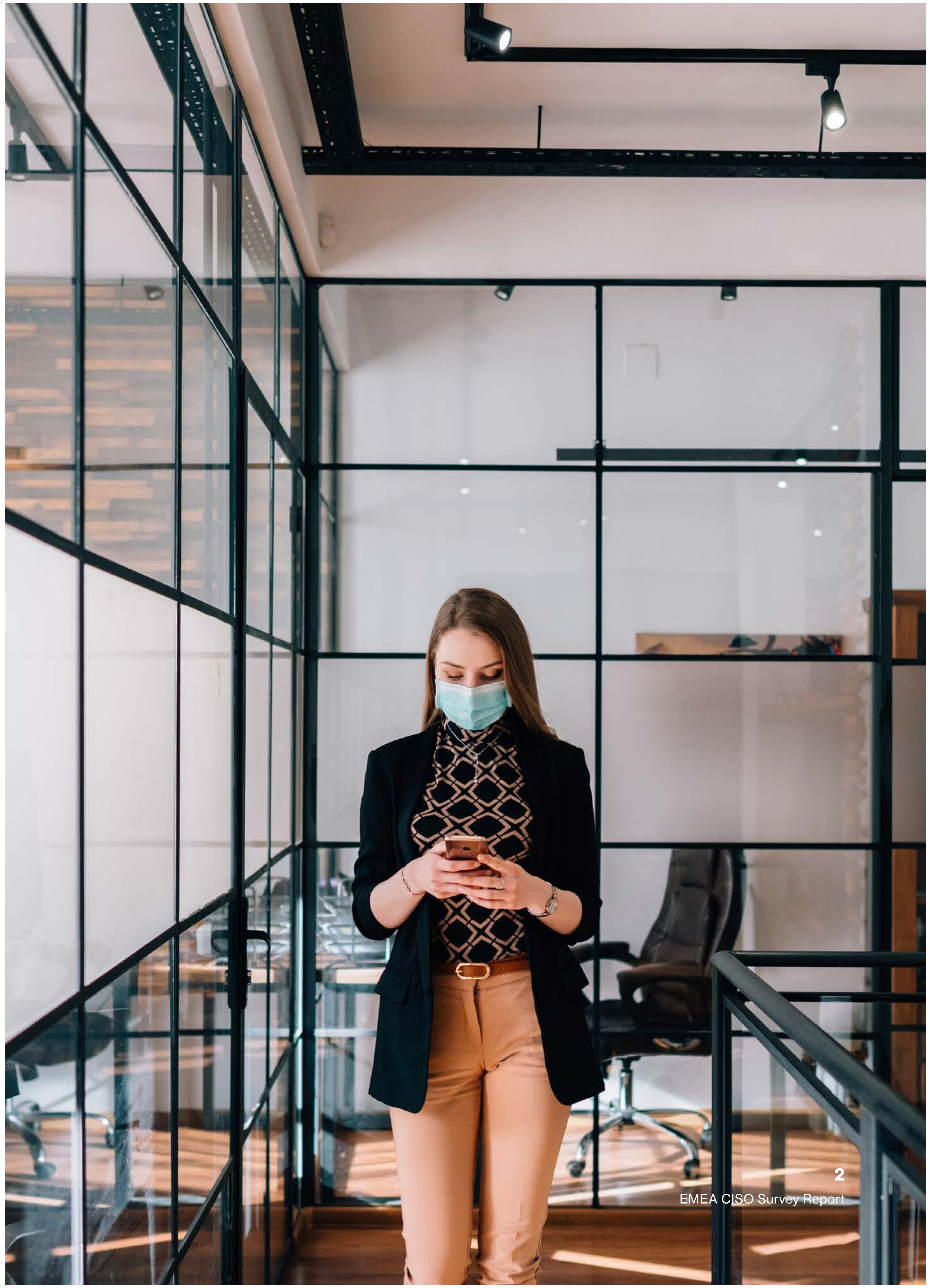
Ivanti's EMEA CISO Survey: How the Pandemic Has Shifted CISO Priorities

Introduction

The COVID-19 pandemic has forced organizations to shift to an everywhere enterprise model of working. Today, IT infrastructures are everywhere, and distributed employees need access to corporate data wherever they work, on any device. As organizations around the world consider making remote work a permanent option for their employees moving forward, we wanted to understand how the pandemic and mass shift to remote work has impacted CISOs. How has the changing IT security landscape challenged them and changed their priorities?

We commissioned independent market research agency Vanson Bourne to conduct a study examining how CISOs across EMEA have responded to the COVID-19 crisis and the new remote work environment. Between November and December 2020, 400 CISOs from large enterprise organizations in the UK, France, Germany, Benelux, Spain, and Italy were interviewed to better understand their evolving security strategies.

The survey revealed that the shift to the everywhere enterprise has forced CISOs to ensure that working from home is just as secure as working from the office. As a result, CISOs are now more focused on mitigating mobile security risks than combating enterprise network threats.



The Security Landscape Has Changed

The everywhere enterprise has changed the cybersecurity battleground for the foreseeable future. More than four-fifths (82%) of survey respondents agreed that remote work has accelerated the demise of the traditional network perimeter, which CISOs had been accustomed to defending. Mobile devices are now everywhere and have access to practically everything, which creates new security challenges for IT departments. At the same time, cybersecurity threats targeted at remote workers are reaching catastrophic new heights.

The majority (87%) of CISOs agreed that mobile devices have now become the focal point of their cybersecurity strategies, and four in five (80%) stated that passwords are no longer an effective means of protecting enterprise data, as hackers are increasingly targeting remote workers and mobile devices.

When pressed on the main IT security challenges that their organizations have faced during the pandemic, CISOs overwhelmingly agreed that they have struggled to ensure that only trusted users, devices, networks, and apps can access company data.

87%

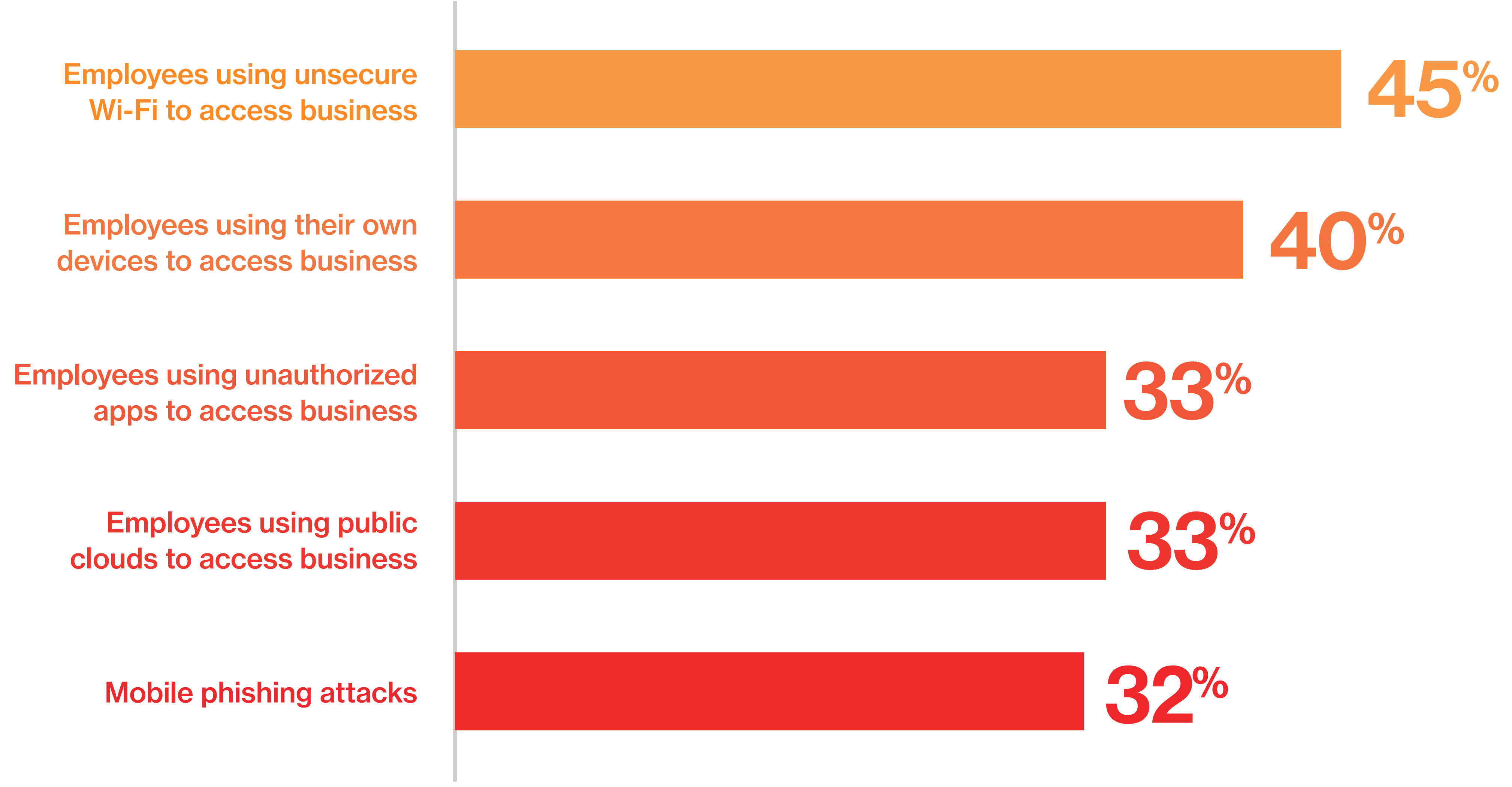
of CISOs claim that mobile devices have now become the focal point of their cybersecurity strategies.

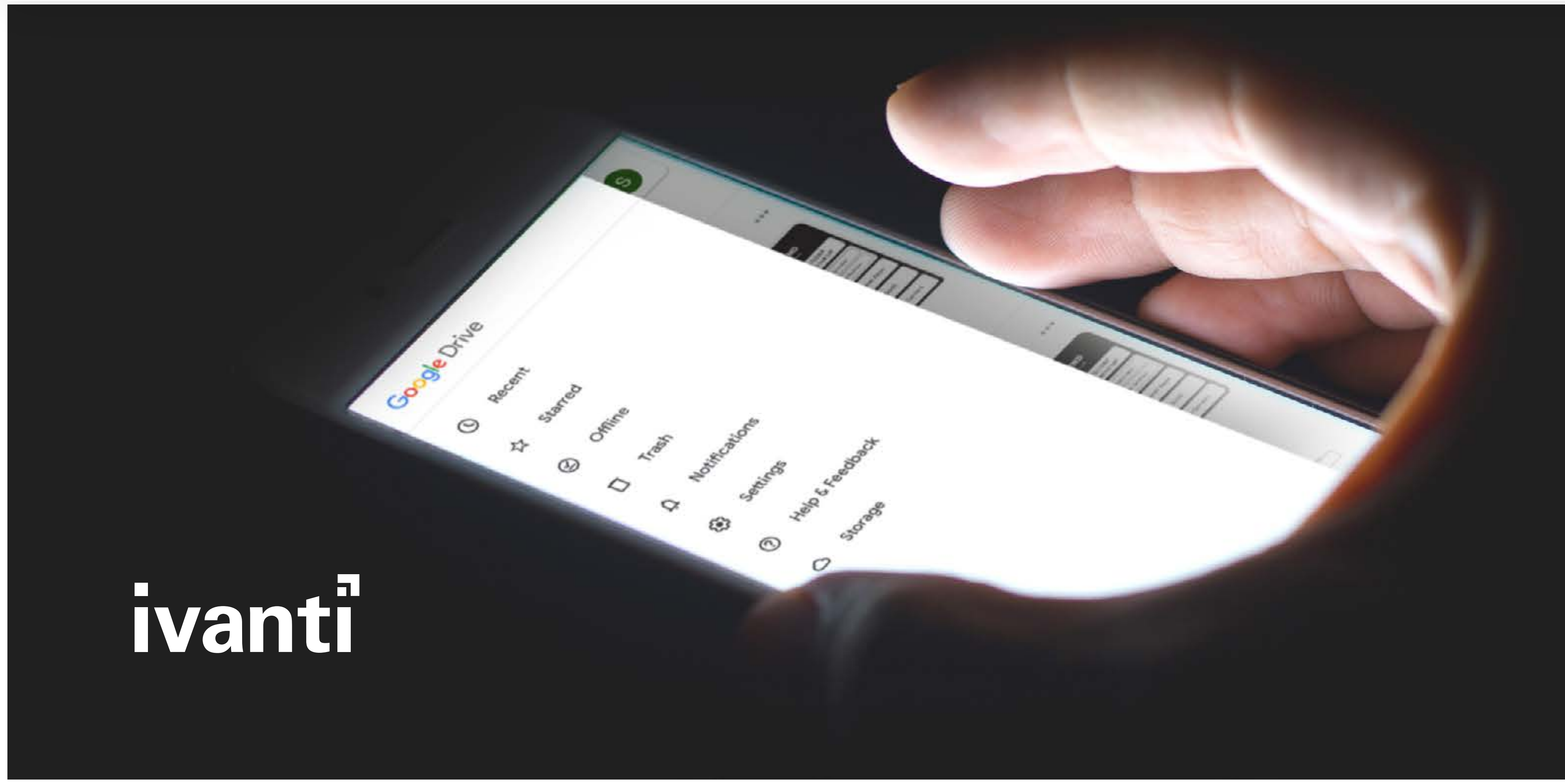
ivanti

Top IT Security Challenges Facing CISOs During the Pandemic

Almost half (45%) of respondents cited employees leveraging unsecure Wi-Fi to access business resources as a main IT security challenge. Two-fifths (40%) cited employees using their own devices to access corporate data and one-third (33%) cited employees using unauthorized apps to access corporate data as other top IT security challenges during the pandemic.

Thirty-two percent of CISOs cited phishing attacks as a major security threat. Unfortunately, hackers are taking advantage of security gaps in the everywhere enterprise by increasingly targeting mobile devices and applications with sophisticated phishing attacks. And these mobile phishing attacks are likely to succeed, as it is very hard to verify the authenticity of links on a mobile device. The mobile user interface also makes it difficult to access and view key information, while prompting users to make fast decisions.





Zero Trust

The explosion of endpoints, devices, and data required for remote work has been matched by an increase in cybersecurity threats. Securing this rapidly expanding threat landscape is a major headache for CISOs, who need to protect mobile employees without limiting access to the corporate data they need when they need it.

By implementing a zero trust security strategy that seeks to verify every user, device, app, and network before granting access to business resources, CISOs ensure employees stay productive and secure, wherever they work.

CISO Priorities are Evolving

The everywhere enterprise is undoubtedly here to stay; in fact, a recent Gartner survey found that 80% of company leaders around the world plan to let employees work remotely from now on, at least part of the time.

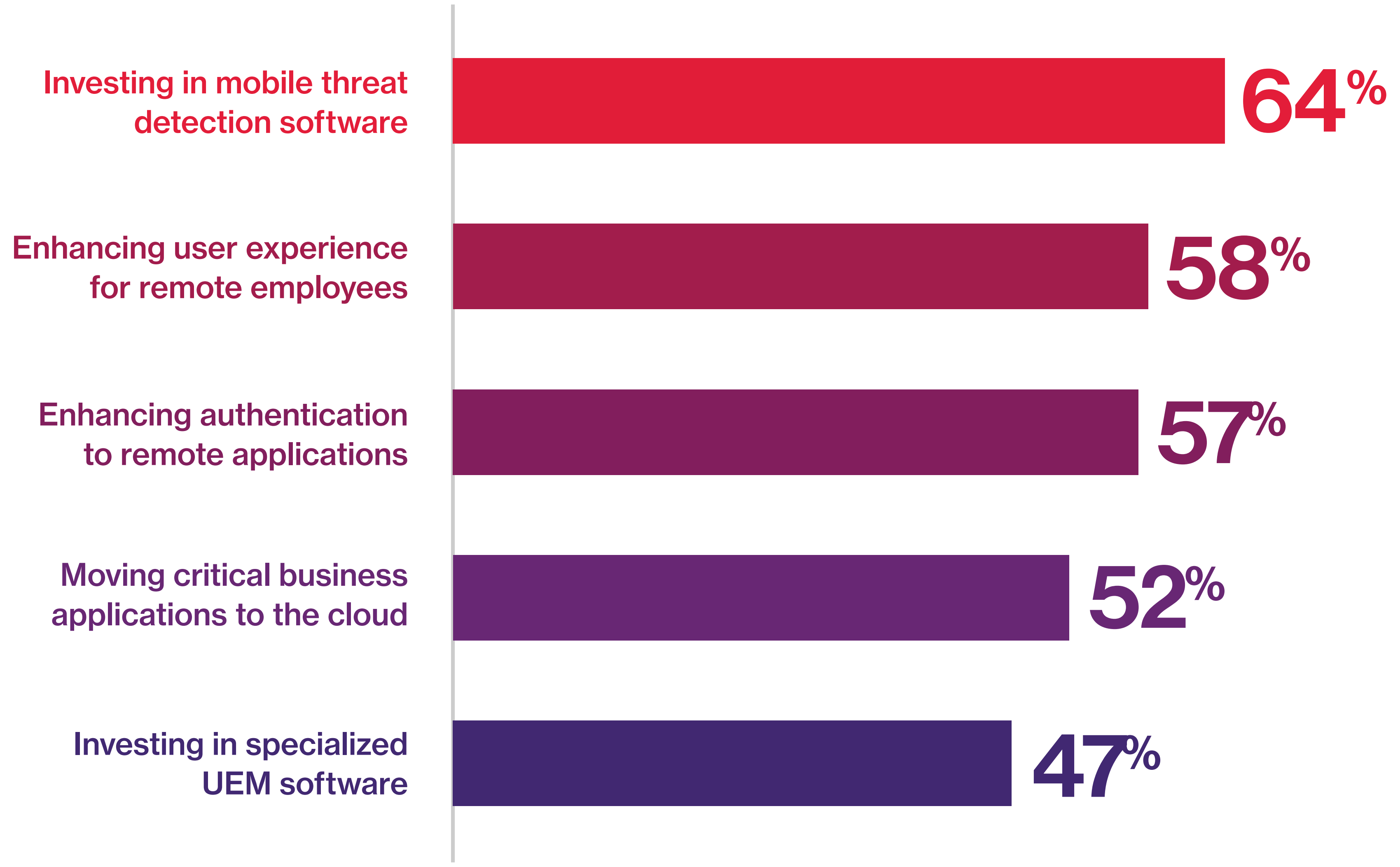
As a result, CISOs are placing greater emphasis on enabling, securing, and optimizing mobile work environments. While 93% of CISOs stated that their organizations had effective solutions in place to enable employees to work remotely at the start of the pandemic, almost all of them (92%) also agreed that they will need to put additional IT security measures in place to better enable remote workers and address the new mobile threat landscape in the year ahead.

When pressed on what these measures would specifically include, the CISOs gave a range of responses that included tightening mobile security and improving the remote work experience for employees. To support these initiatives, almost two-thirds (64%) said investing in mobile threat detection software will be a priority in 2021, while just under half (47%) said they will likely invest in specialized unified endpoint management (UEM) software in the coming year.

Meanwhile, more than half (58%) said enhancing the user experience for remote employees will be a top priority. To support this goal, (57%) said enhancing user authentication to remote applications will be essential, and just over half (52%) said moving critical business applications to the cloud will be a main objective for the year ahead.

92%

of CISOs agree they need to put additional IT security measures in place to better enable remote workers in 2021



Remote Work is Increasing IT Security Budgets

The study also sought to understand how CISOs plan to adjust and reallocate their IT security budgets to address the new threat landscape. The study found that on average in 2020, CISOs across EMEA had a total IT security budget of €64,578,254, with a large portion (41.4%) being spent on specialized UEM software to manage and secure endpoints and mitigate mobile security threats.

However, IT security budgets are expected to grow in 2021 to support the additional IT security measures needed to protect remote workforces. More than four-fifths of CISOs said their overall IT security budget is likely to increase in 2021, with more than a quarter (27%) claiming it will greatly increase.

Considering the growing number of endpoints and devices across the everywhere enterprise, 80% of CISOs said that their investments in specialized UEM software will increase during 2021. To overcome the pain of passwords, seven in ten (70%) CISOs said they also plan to increase their investment in biometric authentication technologies.

By increasing their investment in these two areas, CISOs will be able to better discover, manage and secure the devices, applications, and networks that employees need to work from home, while also delivering a seamless end user experience for employees.

80%

of CISOs will increase their investment in specialized UEM software in 2021

ivanti

Conclusion

These survey results illustrate the dramatic shift in priorities for CISOs in 2020. Remote work has accelerated the death of the traditional network perimeter and has put mobile security firmly in the spotlight. The explosion of mobile devices, apps, and users – combined with the exponential growth in cybersecurity threats – means that CISOs must now place greater emphasis on enabling, securing, and optimizing mobile work environments.

To this end, every CISO should urgently adopt a zero trust security strategy to ensure that only trusted users can access corporate data. In addition, IT should invest in automation technologies that can discover, manage, secure and service all endpoints, devices and data. Not only then will these new approaches help CISOs support a more secure remote infrastructure, they will also help IT reduce time-consuming management tasks and allocate resources to more strategic initiatives.

Methodology

Ivanti commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this report is based. A total of 400 CISOs were interviewed in the UK (85), France (85), Germany (80), Benelux (50), Spain (50), Italy (50) between November and December 2020. Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were allowed to participate.

About Ivanti

The Ivanti automation platform helps make every IT connection smarter and secure across devices, infrastructure and people. From PCs and mobile devices to virtual desktop infrastructure and the data center, Ivanti discovers, manages, secures and services IT assets from cloud to edge in the everywhere enterprise -- while delivering personalized employee experiences. In the everywhere enterprise, corporate data flows freely across devices and servers, empowering workers to be productive wherever and however they work. Ivanti is headquartered in Salt Lake City, Utah and has offices all over the world. For more information, visit www.ivanti.com and follow @GoIvanti.

About Vanson Bourne

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.

ivanti.com
1.800.982.2130
sales@ivanti.com