ivanti

2021 Secure Consumer Cyber Report:

How Remote Workforces are Putting Organizations at Risk of a Cyberattack

Risky consumer behavior is widening the cybersecurity gap

The 2020 pandemic not only unleashed a deadly and devastating virus around the world, but it also fundamentally disrupted every aspect of our daily lives — including where and how we work. Employees of all types and across every industry started working from home whenever possible. Although remote workforces helped to keep critical business operations moving forward, many organizations are now facing a dramatic increase in cybersecurity threats due to the influx of unsecured personal devices and risky employee behavior. After more than a year into the pandemic, what does the threat landscape look like now?

In February 2021, Ivanti released "The 2021 Secure Consumer Cyber Report," revealing the specific threats putting businesses at risk. The findings were based on a nationally representative sample of more than 2,000 people over 18 working across the US and UK in November 2020.

While organizations have been aware of the vulnerabilities posed by unmanaged, employee-owned devices and apps, this report revealed that employees are engaging in high-risk behavior even when they are given company-issued computers to use at home. For instance, one in four consumers admitted to using their work email or password to access consumer websites and applications such as food delivery apps, online shopping sites, and even dating apps.

Complicating Enterprise Security

Even if the world eventually returns to pre-COVID "normalcy," the scale of remote work is likely here to stay. Although organizations have tried to shore up security gaps among their remote workers, it's clear that they will need to do more than just provide corporate-owned hardware and software. A closer look at the report findings should give companies better insight into the challenges ahead.

1 in 4 Consumers

admit to using their work email or password to access consumer websites and applications such as food delivery apps, online shopping sites, and even dating apps.

Remote employee security habits put their companies at risk

To better understand the security level of the average work-from-home environment, the survey asked respondents about their behavior and security practices for all their devices, including IoT devices in the home.

Recycled credentials:
Almost a quarter of US and nearly one in five UK respondents said they have used their work email or password to log in to consumer websites and apps.

Personal devices for work access:
Nearly half of all US and more than one-third of UK respondents said they are allowed to use a personal device, such as a laptop, smartphone, tablet, or smart watch to access company applications and networks.

Two-factor authentication for IoT devices:
Nearly half of all US and UK respondents have not set up two-factor authentication for smart devices in their homes.

Key takeaway: Don’t neglect basic security practices at home

The lack of fundamental security safeguards across home-based IoT device leaves both remote workers and their companies more vulnerable to cyberthreats, such as the Ring hack that went viral in 2019.

Poor security habits, such as recycling passwords to access consumer websites, can put enterprises are greater risk of a breach. Organizations must enforce a clear separation between apps and websites used for work and personal business.

Enterprise security also falls short across the remote workforce

After the onset of the pandemic, we saw a dramatic rise in cybersecurity attacks against insecure personal devices and in-home IoT devices. While poor end-user security habits may be partly to blame, our survey found that enterprises can also improve security in key areas.

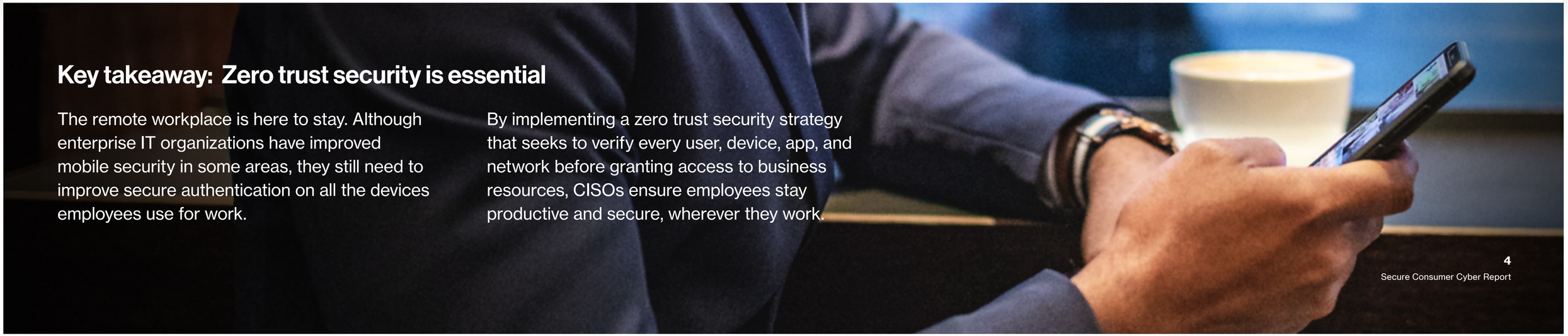
25%

Security software:
More than 25% of all respondents said they were not required to have specific security software running on their devices to access certain applications while working remotely.

Password updates:
Roughly 25% of remote workers in the US and UK said their company does not require them to update their password every six months or use a one-time password generator.

30%

Secure access tools:
Nearly 30% of all respondents across the US and UK said their organization does not require remote workers to use a secure access tool, such as a VPN.



Key takeaway: Zero trust security is essential

The remote workplace is here to stay. Although enterprise IT organizations have improved mobile security in some areas, they still need to improve secure authentication on all the devices employees use for work.

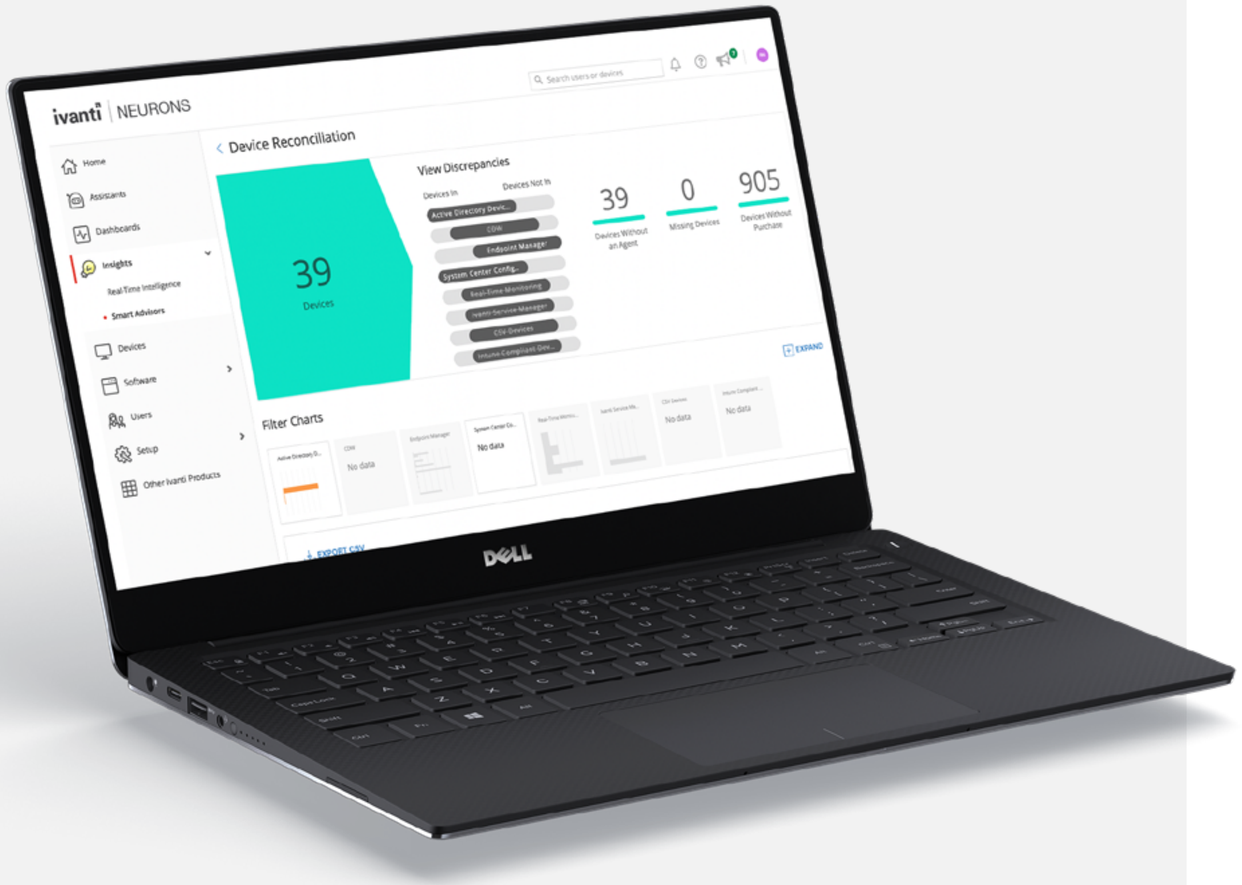
By implementing a zero trust security strategy that seeks to verify every user, device, app, and network before granting access to business resources, CISOs ensure employees stay productive and secure, wherever they work.

Secure consumers enable secure enterprises

With more people working remotely than ever before, the threat landscape has expanded faster than ever before. This is why organizations should look at key strategies for safeguarding business apps and data against lapses in IoT security and consumer awareness at home. It's clear that as more consumer devices proliferate, remote workers may struggle to activate and maintain advanced security settings — and cybercriminals know it. As a result, in addition to creating a mass threat to human health, the COVID-19 pandemic has also put our wellbeing at risk by making it easier for cybercriminals to take advantage of people and organizations who lack adequate protection.

However, there is good news:
Companies can launch Zero Trust security today

Organizations can take steps now to start implementing Zero Trust protocols across the remote workforce. With a Zero Trust model in place, companies can eliminate the risk of stolen credentials by verifying that anyone accessing corporate information, applications, or networks is a trusted entity. In addition, as remote work persists and devices continue to proliferate, Zero Trust security can make it much easier to enforce acceptable use policies, including the use of multifactor authentication, device protections, and secure network connectivity.



Methodology

The findings in the inaugural Secure Consumer Cyber Report are based on a survey conducted in November 2020. The study was designed to examine how consumer and enterprise cybersecurity habits have changed over the course of the pandemic. The survey used a nationally representative sample of 2,000 US and UK residents over the age of 18 who were working from home on a company-provided computer.

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 workplace – while delivering personalized employee experiences. In the everywhere workplace, 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.

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com