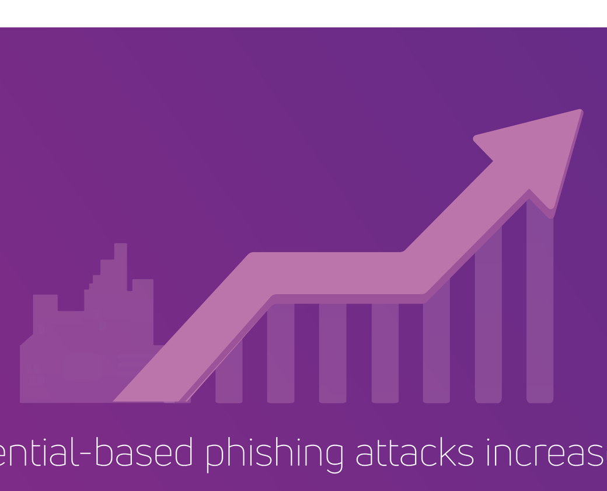
Gold Microsoft Partner Microsoft

PROTECTING YOUR REMOTE WORKERS IN AN ANYTIME ANYWHERE WORLD

AS REMOTE AND HYBRID WORK STRATEGIES CONTINUE TO PUSH ORGANISATIONS BEYOND THE TRADITIONAL SECURITY PERIMETER, VULNERABILITIES WITHIN THEIR IT SYSTEMS PRESENT MANY NEW OPPORTUNITIES FOR CYBERCRIMINALS TO EXPLOIT.



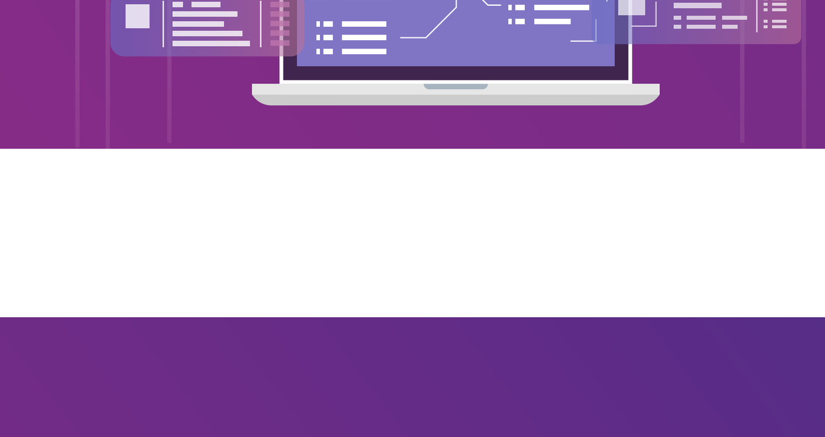
Credential-based phishing attacks increased by

667%

in 2020 as a result of the rapid shift to remote working

38%

of employees shared their concern about the risk of data breaches and doubts that their organisations' security is doing enough to protect them



Active Directory (AD) access points are frequently used to launch cyber-attacks and adequately securing these systems has become increasingly critical to organizations' security, particularly amid the shift to hybrid working

Wi-Fi Security

81%

of CIOs said their company had experienced a Wi-Fi related security incident in the **last year.**

Hacking Risks

57%

of CIOs suspect their mobile workers have **been hacked** or caused a mobile security issue in the last year.

Cafes & Coffee Shops

62%

of Wi-Fi related security incidents occured in **cafes** and **coffee shops.**

Personal Devices

94%

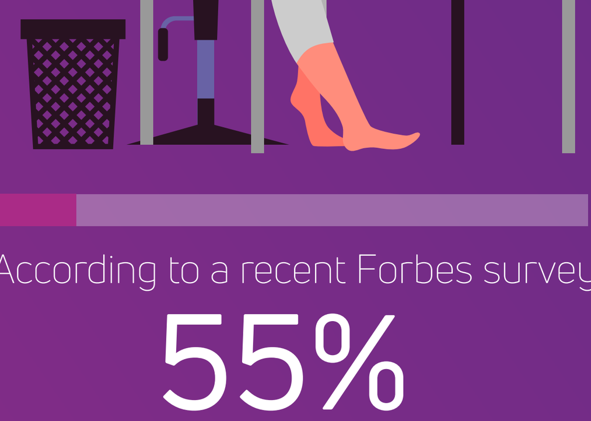
of CIOs believe the rise of BYOD has **increased** mobile security risks.

VPN Use

Only

46%

of enterprises were **confident** that mobile workers were using a VPN.



According to a recent Forbes survey,

55%

of employees prefer remote or hybrid work environments in the post-pandemic era.

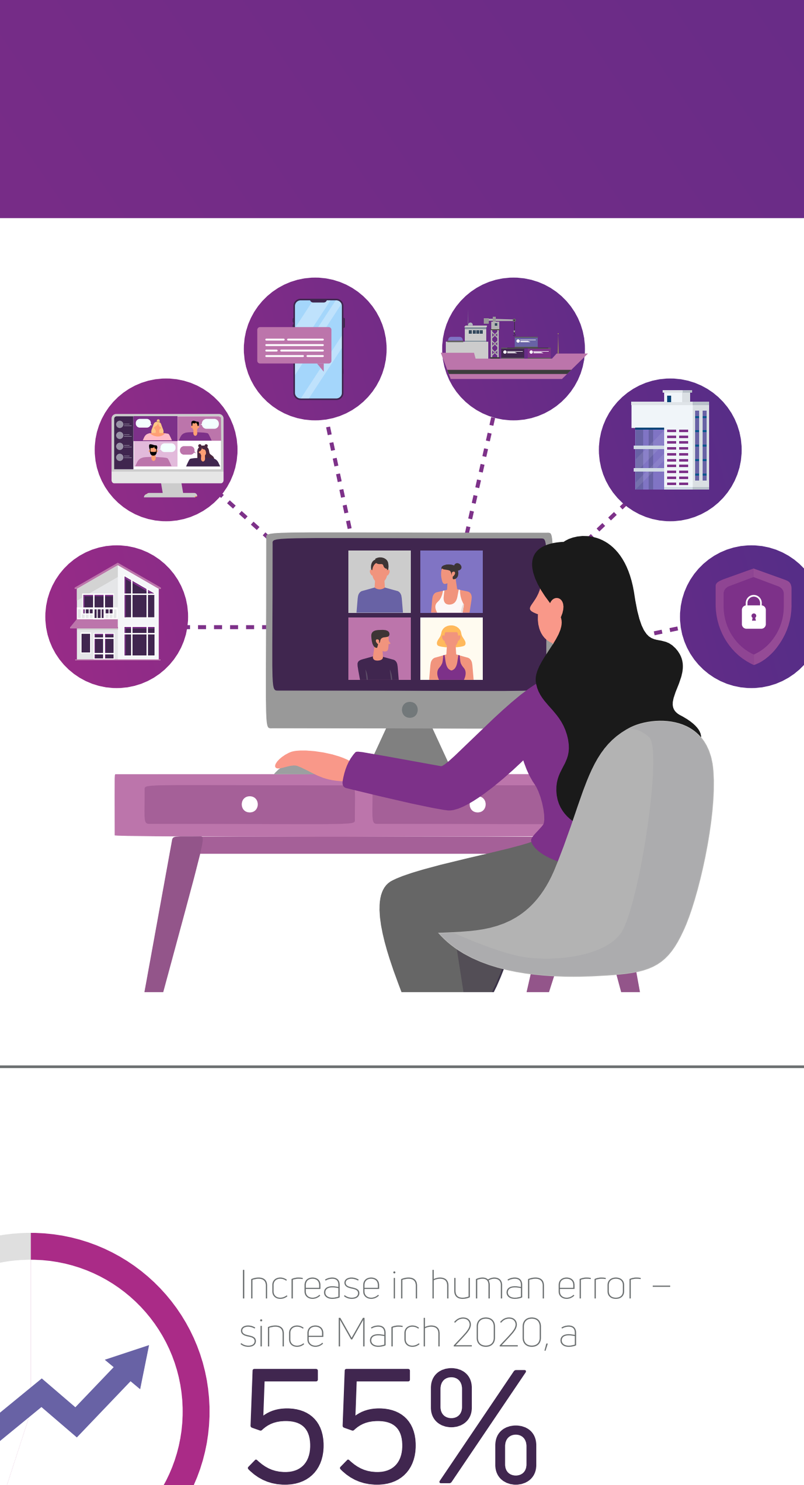
Hackers have turned their focus to cloud services with a massive

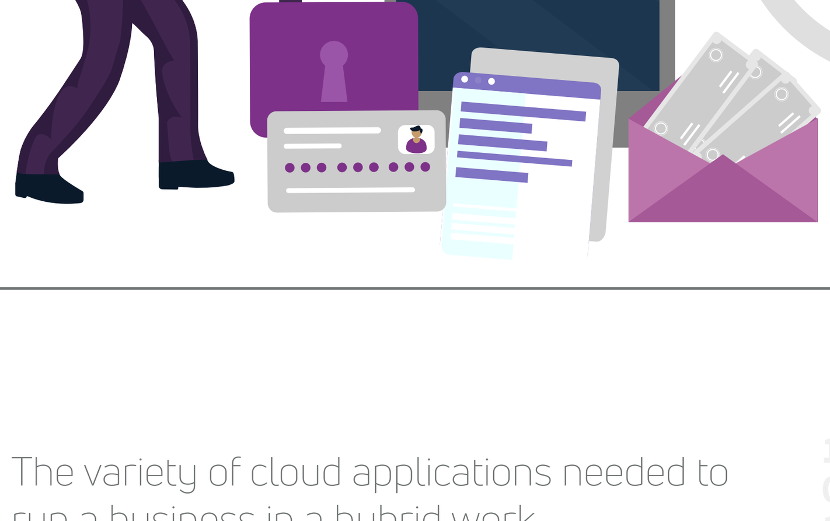
630%

increase in cloud service attacks in Q1 of 2020.

Weak home Wi-Fi security, personal laptops, unsecure mobile devices and poor security practices play a major role in increasing vulnerability.

Hybrid workspaces involve employees working from both home and the office. This means the network perimeter of a business' IT environment is much more widespread, making data protection a difficult task.



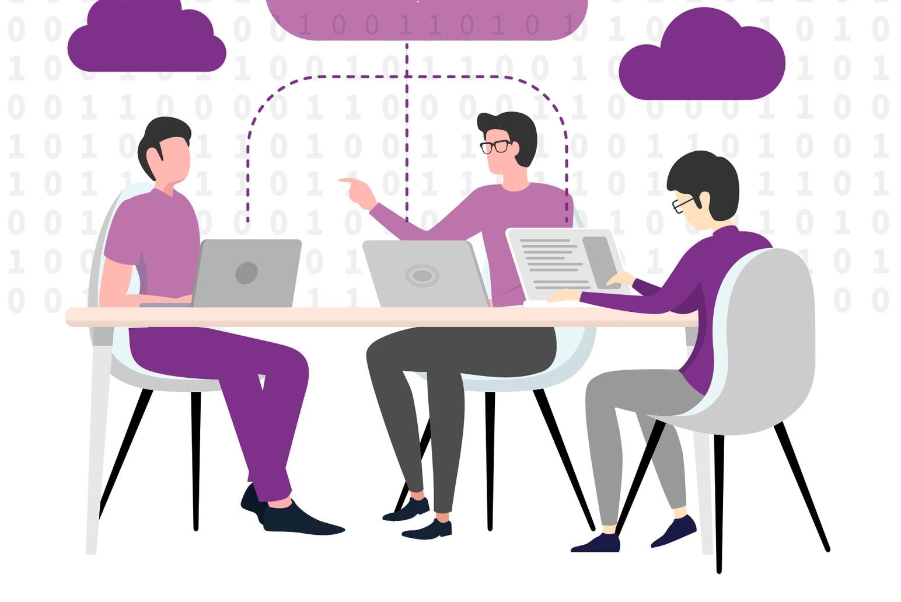


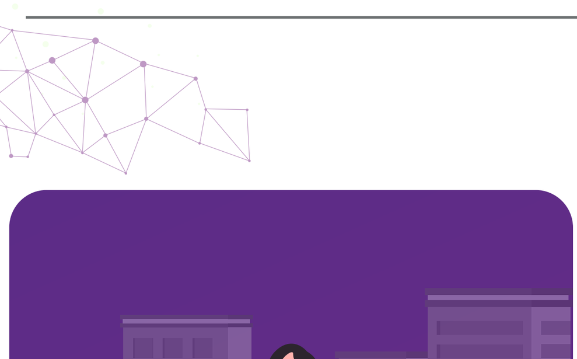
Increase in human error – since March 2020, a

55%

rise in phishing attacks.

The variety of cloud applications needed to run a business in a hybrid work environment creates new network edges. While organisations were able to quickly shift to accommodate the secure remote access needs of their workforce during the pandemic, most traditional security solutions could not keep up. It's time to focus on fortifying the network so that it can be both highly agile and highly secure.





Hybrid is the future

81%

of CISOs say their organizations have started of currently have a **hybrid work** environment in place.*

Communication is at a high

Since the pandemic we've seen email volumes grow

28%

YoY in commercial and edication.

Networks are shifting

The growing sophistication of the threat landscape, coupled with the inflection point that is hybrid, is driving a sea of change for the security industry.

Anticipate challenges

The industry is facing a

3.5 million

shortfall of security professionals, and hackers are attacking an average of **579 times a second.**

Detect threats

There is an average of

50 million

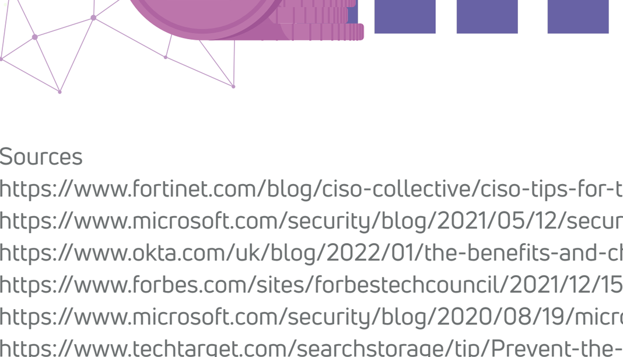
password attack attempts **daily,** yet only 18% of customers use MFA.

Microsoft® Security Essentials

Microsoft Security

There are practical steps you can take to be more secure.

Learn how at microsoft.com/security



Moving to a long-term hybrid work model requires a reassessment of budget priorities. Funds that were once earmarked for a network upgrade, for example, might need to be reallocated for cloud adoption, collaboration software, and endpoint security. Going forward, we need to think about an architecture that supports flexible work models with protection across the LAN, WAN, data center and cloud edges.

Sources
https://www.fortinet.com/blog/ciso-collective/ciso-tips-for-the-post-pandemic-hybrid-workforce
https://www.microsoft.com/security/blog/2021/05/12/securing-a-new-world-of-hybrid-work-what-to-know-and-what-to-do/
https://www.okta.com/uk/blog/2022/01/the-benefits-and-challenges-of-remote-and-hybrid-working/
https://www.forbes.com/sites/forbestechcouncil/2021/12/15/securing-the-new-hybrid-workplace-and-keeping-your-employees-protected/?sh=15684da73bef
https://www.microsoft.com/security/blog/2020/08/19/microsoft-shows-pandemic-accelerating-transformation-cyber-security/
https://www.techtarget.com/searchstorage/tip/Prevent-the-storage-and-data-security-risks-of-remote-work