Fluid

Hybrid working – planning for the future of work

Over the past few months, as businesses contemplate the next normal, the term 'hybrid working' has come to the fore. It's now clear that work for many people isn't going to be the same as it was pre-pandemic. Many employees want to split their time between the office and home. Businesses think it's a good idea too, with 54% of CFOs making remote work a permanent option for relevant roles.

If you're planning to continue with a mix of home and office-based working, it's essential to iron out any issues fast. For instance, are video calls being disrupted by overloaded home Wi-Fi? Are you confident that you've got security covered? If hybrid working is here to stay, your network needs to be up to the job.

So, what are the key challenges of hybrid working and how can technology help?

Providing a consistent experience from anywhere

We've all felt the frustration of battling technology when working from home. Tasks that take a few moments in the office can be derailed by connectivity issues, meaning productivity suffers and helpdesk calls increase. For your hybrid workplace to be fit for purpose, everyone needs the same effortless access to files, company systems and cloud apps, no matter where they are. This is where investing in the right technology can make all the - difference, giving people an 'in-office' experience, no matter where they are or what device they're using. 49% of CFOs say the technology investments they are making during this time will position them better for the longer term.

Defending again sophisticated threats

A comprehensive approach to network security is central to a hybrid working strategy.

78% of cybersecurity experts believe roaming or remote users are most vulnerable to attack[1]. This isn't surprising as remote workers are outside traditional perimeter security, and endpoints are a frequent target for cyber criminals, but attacks come from all angles. Email can leave you open to phishing. And ransomware is still widespread, with a new organisation falling victim every 11 seconds*.

Reducing the number of tools

IT security is already complex, but it's made worse if you're dealing with lots of different tools and processes. This increases the workload and decreases visibility. As you look to the future, it's a good point at which to retire old tools and find a smarter solution that's built for the cloud era.

Cisco Umbrella is SASE simplified for SMBs

Cisco Umbrella is a security platform that's perfect for hybrid working. It protects all your workers on any device – whether they are remote, roaming or in the office – on the network or off it. At the same time, Umbrella simplifies management for IT teams by consolidating multiple tools into a single service - secure web gateway, cloud-delivered firewall, DNS-layer security and cloud access security broker (CASB) solutions.

What does this mean in day-to-day terms?

- Malware, ransomware, phishing and botnets are blocked before a connection is established
- Your IT team gets better visibility across the network
- Actionable reporting shows trends and security risks that need attention.
- Threats can be detected and remediated faster
- Consistent policies can be applied across remote locations, quickly and easily
- Single dashboard for efficient management
- Supports direct-to-internet access to cloud applications and workloads

You can read more about our security solutions here.

Let Fluid help you get set for hybrid working

We know there's a lot to consider when it comes to revamping security across your organisation. That's why it's worth working with an experienced partner who knows how to assess your needs and apply the technology to best effect.

Why not take advantage of our Cisco umbrella and Cloud mailbox defence* 30-day free trials? Contact us to start your free trial today! (form to complete)

SOURCES

* Cisco Umbrella Global Network
* Cloud Mailbox Defense is for Microsoft 365 email users only