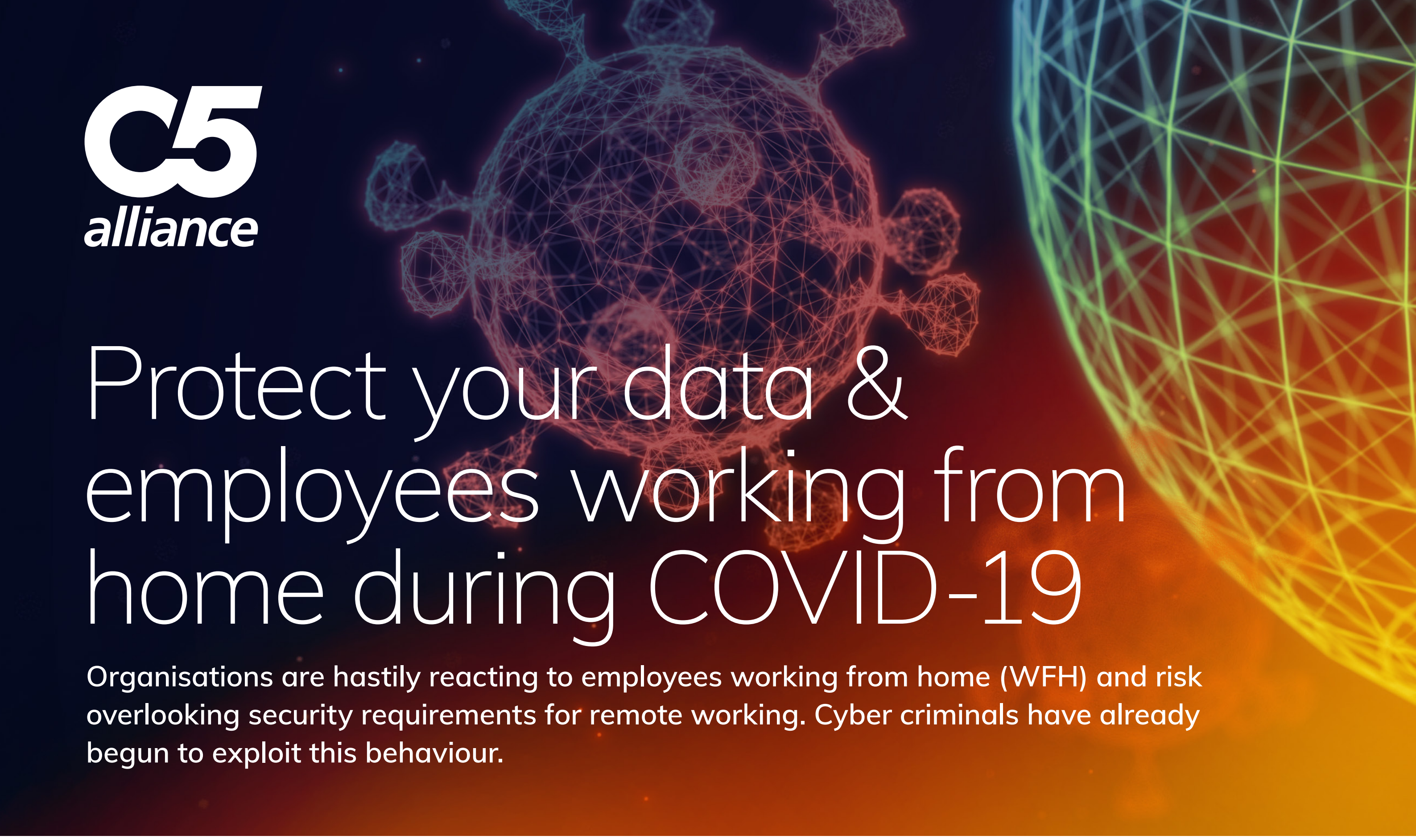


Protect your data & employees working from home during COVID-19

Organisations are hastily reacting to employees working from home (WFH) and risk overlooking security requirements for remote working. Cyber criminals have already begun to exploit this behaviour.

WFH & BYOD Vulnerabilities

Insider Threat

With remote working, there is a risk that employees may exploit their newfound freedom within which they are operating. For example, they may try to take intellectual property without being seen.

Therefore, remote access should be carefully monitored and the ability to cut and paste or access local hard drives disabled. Be aware that users can still take screenshots of sensitive information. This can also be addressed with suitable policies geared towards remote working.

Cloud Security

Cloud services provide numerous positive capabilities, especially for businesses that WFH. This solution for productivity does not always include security which should be configured, checked and monitored. Attackers are targeting Cloud services; however, the various Cloud platforms provide some excellent security features, which should be configured.

Multi Factor Authentication (MFA)

With a few exceptions, your Cloud services are potentially exposed without MFA. In addition to using a standard username and password, a MFA solution requests that workers perform an additional step after entering their credentials.

For instance, by inputting a token or code generated by an authentication app on a mobile phone – decreasing the risk of attack.

BYOD Policy

Coronavirus has meant that for many businesses, a BYOD policy is their only option in order to continue operating. Where this has to be permitted there are a number of solutions available to minimise the risk by creating sandboxes, or enclaves within the BYOD device.

Full Disk Encryption (FDE)

All remote laptops should have full disk encryption enabled to protect data at rest. This way, if devices are stolen then the contents of the hard drive are not available. This not only safeguards your intellectual property but also personal identifiable information (PII).

38%
INCREASE IN
TEAMS USERS

Usage of MS Teams has increased 38% to 44 million users due to COVID-19

~ Microsoft

1.5
MILLION
WFH IN
THE UK

In the UK approximately 1.5 million people are now working from home.

~ BBC News

How C5 can help you

Managed Patching Service

We manage Microsoft Windows 10 updates as well as a defined list of applications. Our patching service focuses on keeping laptops updated whilst also reducing security risks.

Secure Virtual Private Networks (VPN) Setup

Secure access for remote workers into your corporate environment can be configured via VPN or our Island Cloud platform in the Channel Islands.

Vulnerability assessment and security monitoring

Our cyber security monitoring service on remote devices accessing your network uses industry leading security vulnerability management tools, designed to prioritise, alert and report on security risks and threats.

Manage mobile devices

By configuring Microsoft Intune we can help you protect corporate data by monitoring and managing both corporate and bring-your-own-devices (BYODs).

Supporting your business through COVID-19

We have the largest team of IT professionals in the Channel Islands on hand to work with you through the COVID-19 crisis. Within the wider BDO Group, locally and internationally, we can provide advice to support your planning and business operations through this crisis spanning technology, risk, regulatory & compliance, project management and training.

We have drawn together all of our resources to ensure the maximum response capability to support our clients.

Advise

We can complete a variety on comprehensive health checks to understand the current state of your organisation's WFH security standing.

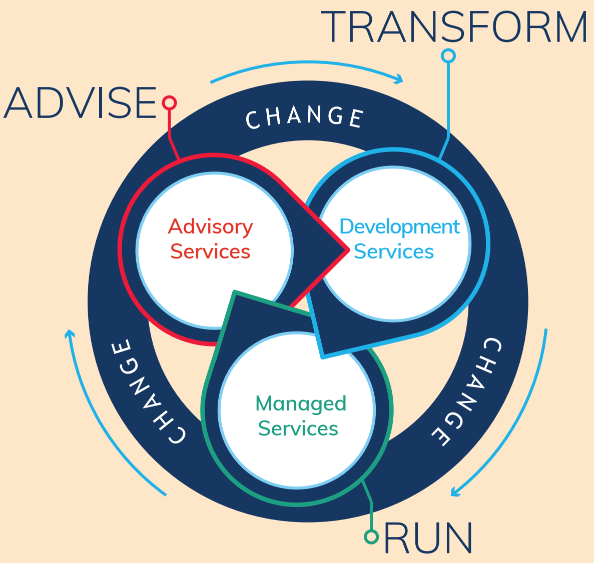
Our highly qualified consultants can recommend security solutions and can create tailored strategies to suit your WFH security needs.

Transform

Our cyber security specialists can implement the best-in-class technology to ensure your organistaion is protected while working from home.

Run

We can monitor vulnerabilities in your cyber security 24/7/365 ensuring you are continuously protected no matter where or when your workforce are active



C5 alliance

Our team is here to support your security resilience needs.
For more information please email enquiries@c5alliance.com
or call **01534 633733**

www.c5alliance.com

BDO