daisy.

YOUR HOMEWORKING
SECURITY ESSENTIALS

To be effective, a homeworking solution needs to be fast and reliable, but most of all, it needs to be secure – to and from your devices, applications, data, and your network.

GET SERIOUS ABOUT YOUR HOME WORKERS' SECURITY...

Is your connection secure?

VPN

WWW

4G/5G

Is your data backed up?

Every home worker needs...

Corporate Network at Home

Secure access to the enterprise network, from any device, at any time, in any location for safe but convenient access to work.

Multi-factor Authentication (MFA)

Requiring two or more credentials in order to authenticate their identity will significantly improve end-user security.

Malware Protection

Threat protection for home workers needs to be the same as for those in the office to keep malicious software at bay.

System & Patch Management

Updating software and systems to fix known vulnerabilities as quickly as possible is crucial in closing down opportunities for cyber criminals.

Mobile Device Management (MDM)

Controlling sensitive information and ensuring security protocols are set up, protecting smartphones and tablets and empowering home workers.

Secure Backup

Most SaaS data is not backed up and Office 365 data is no exception, so you need to make sure that home workers' data is backed up safely wherever it resides, and able to be recovered.

...AND MAKE SURE YOUR CORPORATE NETWORK IS PROTECTED

ARE YOUR HOME WORKERS PROTECTED AS EFFECTIVELY AS THEY WERE WHEN THEY WORKED HERE?

Company headquarters

Data centre

Essential solutions for corporate security...

Cloud, Hosted and On-premise Firewalls

Filtering harmful traffic and protecting your network with next generation features is as critical as ever, but a large increase in traffic may mean you need to upscale your firewall.

Networking Solutions

As well as needing fast broadband connectivity for home workers, you will need to increase your HQ or data centre bandwidth, extend enterprise wireless capabilities to home workers and ramp up your VPN solution to cope with the new demands.

Security Information & Event Management (SIEM)

The ability to gather, analyse and manage real-time security data from all network devices is critical to detect, prevent and resolve cyber attacks – the more end-points, the more points of risk.

DDoS Protection

Protecting your publicly available infrastructure to keep core websites and portals live remains a significant requirement.

Have you got adequate provision and guidance for:

- Remote-working access management
- The use of personal devices for work and work devices for home (streaming, unauthorised downloads/applications)
- Data privacy for access and use of sensitive documents and personal information
- An outside-in approach that focuses on end-point and end-user risk management and mitigation

IS YOUR SECURITY POLICY APPROPRIATE?

CORONAVIRUS

UK PHISHING UP BY 667% FROM FEB-APR 2020*

The way we work is changing irrevocably and so is the threat landscape. Organisations will need to re-evaluate their security strategy. Daisy can help at every level...

THERE ARE 3 MAIN SECURITY LIFECYCLE STAGES THAT SHOULD FORM THE BACKBONE OF YOUR SECURITY STRATEGY...

1 DISCOVERY

UNDERSTANDING

your weakness and monitoring your environment for security threats

2 PREVENTION

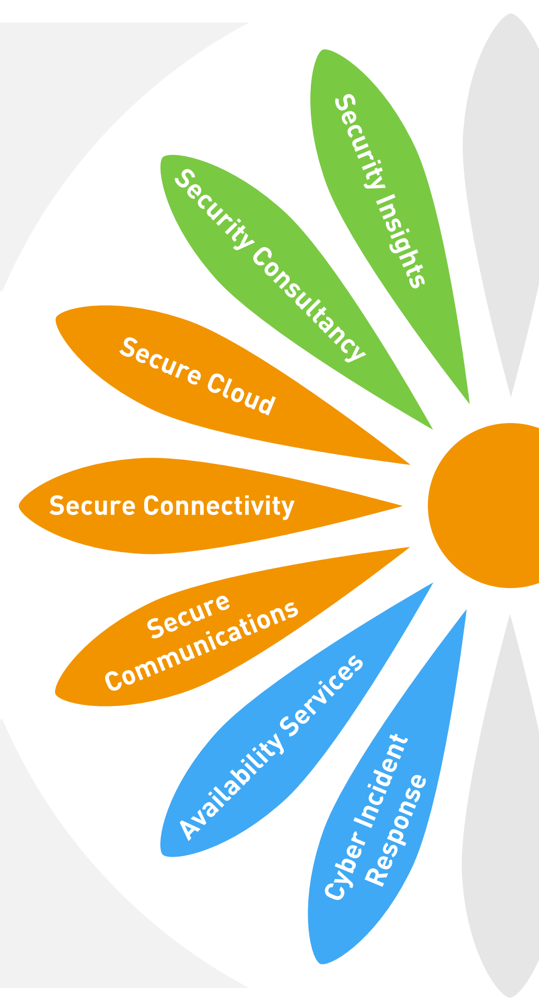
DEPLOYING

technology to prevent attacks

3 RESPONSE

RESPONDING

to cyber breaches with remediation experts and fail-back to a clean environment



*statistic courtesy of Barracuda Networks

Daisy's security operations centre (SOC), has UK government baseline security standard (BPSS) and security cleared (SC) personnel, globally recognised security accreditations and partnerships with world-leading security vendors. Our security expertise spans across our full portfolio of IT, communications and cloud solutions to deliver unrivalled peace of mind and help you succeed with strategic goals.

We're here to talk: enquiries.dcs@dcs.tech
0344 863 3000 or visit dcs.tech/safe-haven

we are daisy.
dcs.tech

228 06.20 2020 © Daisy Corporate Services Trading Limited (CRN: 2888250)