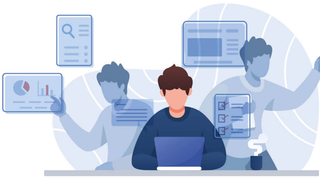
71%

of businesses state the shift to remote working increases the likelihood of a cyber breach according to Centrify

MLR Networks Ltd

57%

of CIOs are concerned that a lack of visibility and control of endpoints will make their companies more vulnerable to cyber-attacks



Remote worker behaviour creates vulnerabilities that hackers can exploit:

Clicking on suspicious links

Phishing attacks are recognised as the main cause of data breaches. Hackers systematically prey on public fear focusing on themes such as coronavirus.

Shadow IT

It's impossible to securely manage an application you're unaware of. Employees using unauthorised applications put the whole network at risk.

Accessing sensitive data through unsafe WiFi networks

Employee home networks invariably have weaker security protocols than the corporate environment. This allows hackers easier access.

Vulnerabilities from personal devices

Personal devices that are connected to the network and yet don't adhere to the IT infrastructure security policy are a big hazard.

Increased security threats

Malware

Home office networks are 3.5 times more likely to be infected by malware than corporate networks, according to BitSight.

Phishing

Google states phishing attacks have increased by 350% in the last year.

Ransomware

DataBarracks predicts ransomware attacks will be more frequent and more devastating in 2021/22.

How to secure remote workers

Duo verifies the identity of all users before granting access to corporate applications.

Umbrella provides the first line of defence against threats on the internet wherever users go.

Secure Endpoint provides the last line of defence, enabling protection, detection and response on the endpoint against known and unknown threats.

Duo Cisco Umbrella

Securing your business

Powerful, secure solutions for all your infrastructure requirements.

Contact us
0151 423 3633
sales@mlrnetworks.co.uk

www.mlrnetworks.co.uk

MLR Networks Ltd