

# Horizon

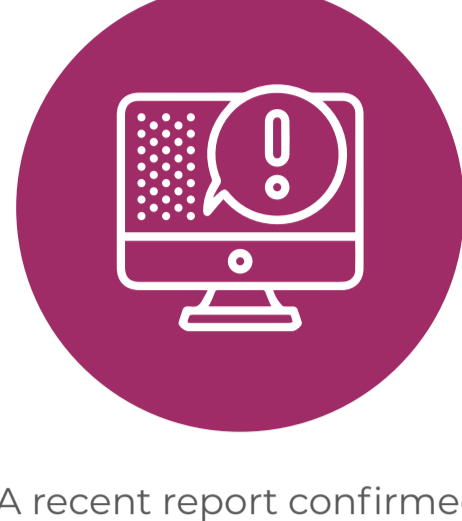
# Remote Working

## demands a more practical approach to Cyber security

Companies around the world have been hit hard by COVID-19, forcing them to send staff members home to work remotely.



**More home working significantly increases the number of Cyber security events**



A recent report confirmed that at least 1/3 of IT decision-makers admitted to suffering a data breach due to remote working.



50% of organisations could not guarantee that their company data was completely secure when accessed by workers from home.



More widespread use of cloud collaboration tools can lead to greater data integrity risks.

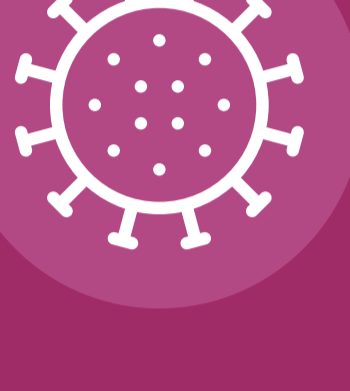
## We're faced with a growing crisis



At the end of Q1 2020 attacks reached peaks of 145 threats for every 1,000 endpoints, compared to just 30-37 at the start of Q1.



Hackers have become more active since January this year, with an increase in hacking incidents of 15-20% witnessed every month.



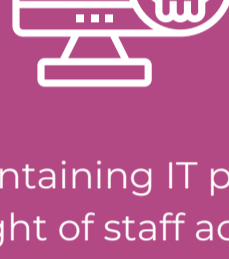
Hacking threats that use terms like "COVID-19" or "Coronavirus" in order to play on people's fears and anxieties to steal valuable information are also on the rise.



Hackers are setting up malicious websites, claiming to be reputable information sources for all things COVID-19 to steal sensitive personal and financial information from unsuspecting individuals.



Supply chain compromises are often used to increase the success of phishing attacks.



Maintaining IT policy oversight of staff activity in the cloud and with remote working is difficult.



Moving to the cloud means your network perimeter is now the entire internet

## What's the Solution?



Small, medium, large companies or public sector departments, can benefit from Horizon's intelligent, yet simple loss-prevention solution.

Horizon has been developed by those with a unique understanding of Cyber criminal motivations, intentions and techniques.

## Protect your Remote Workers and Organisation from Cyber Threats

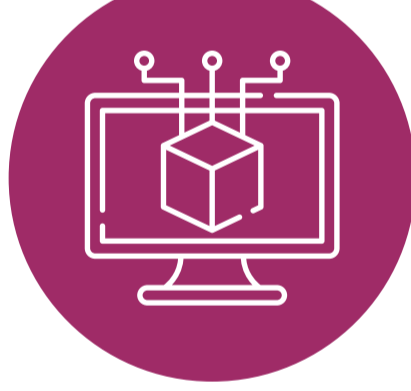
### Secure them with Horizon



Developed to work with cloud-based services such as Microsoft 365, Google G Suite.



Provides timely insights and profiling of user account activity.



Delivers alerts based on suspicious activity and detects on IT policy breaches.



Provides immediate alerts if the system identifies potential unauthorised access to your e-mails.



Detects post-intrusion activity.



Supported by preventative credential assurance tools.

Horizon was designed by leading former UK Government Cyber-attack specialist, supported by an innovative team of leading software engineers.



The Horizon CTO was at the forefront of the UK's active and defensive Cyber operations.



The UK National Cyber Security Centre is recognised as a lead agency for countering Cyber Crime.



The UK Government and the Cyber industry work in close partnership to mitigate ongoing Cyber attacks.

- Designed to be effective against the most common risks facing corporate networks particularly in a cloud-based environment with extensive remote working.
- Developed to work along side any existing malware tools Horizon sits outside the network with no requirement to install software or hardware and does not access your company information.
- Horizon visualises only the issues that need addressing in a clear, simple and easy-to-use interface developed for non-Cyber experts, with drill-down functionality and 24/7 support.

Contact us now at [horizon@cwddynamics.com](mailto:horizon@cwddynamics.com) + 44 (0) 1202 804 140 to get started.

