

# PROTECTING THE MID-MARKET AGAINST RANSOMWARE

The UK National Cyber Security Centre recognises ransomware as 'the biggest cyber threat facing the United Kingdom' - and mid-market organisations are firmly in their sights.

The top 10 tips to **protect your organisation** from ransomware - before it's too late.



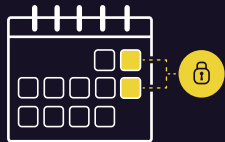
## Protect. Your. **Emails.**

Nine out of ten attacks start via email - and human error is still an often-fatal flaw in your defences.



## Protect **primary infection vectors**

Cross-channel attacks are the norm. Attackers are exploiting stolen RDPs, software vulnerabilities, and ID weaknesses.



## Don't neglect the **weekend**

Ransomware tactics are diversifying. Attacks are landing on weekends or holidays, when fewer IT security staff will be on duty.



## Enable **MFA everywhere**

Multi-factor authentication is essential in the fight against ransomware: a simple but effective way to limit avenues of entry.



## **Segment your networks**

Apply multiple individual security protocols to limit ransomware's spread and maximise the chance to track, isolate, and stop it.



## **Block attacks in real-time**

Use all contextual information to automatically take action against security compromises as they happen.



## Use **behavioural analytics**

The more granular your data, the better. Understand what constitutes normal activity and flag anything unusual for review.



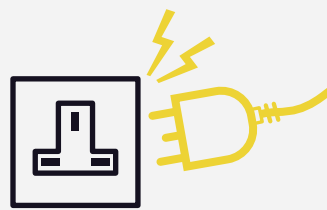
## Run regular **phishing simulation**

Never underestimate the insider threat. Regular simulations are a good way to keep employees sharp - particularly live tests.



## **Patch, patch, patch**

As the Log4j vulnerability demonstrated all too well, a simple unpatched software vulnerability can have catastrophic effects



## **If all else fails - pull the plug!**

Identify how ransomware is propagating - then isolate it! Yank the network cable out, turn off the WiFi - and stop it moving further.