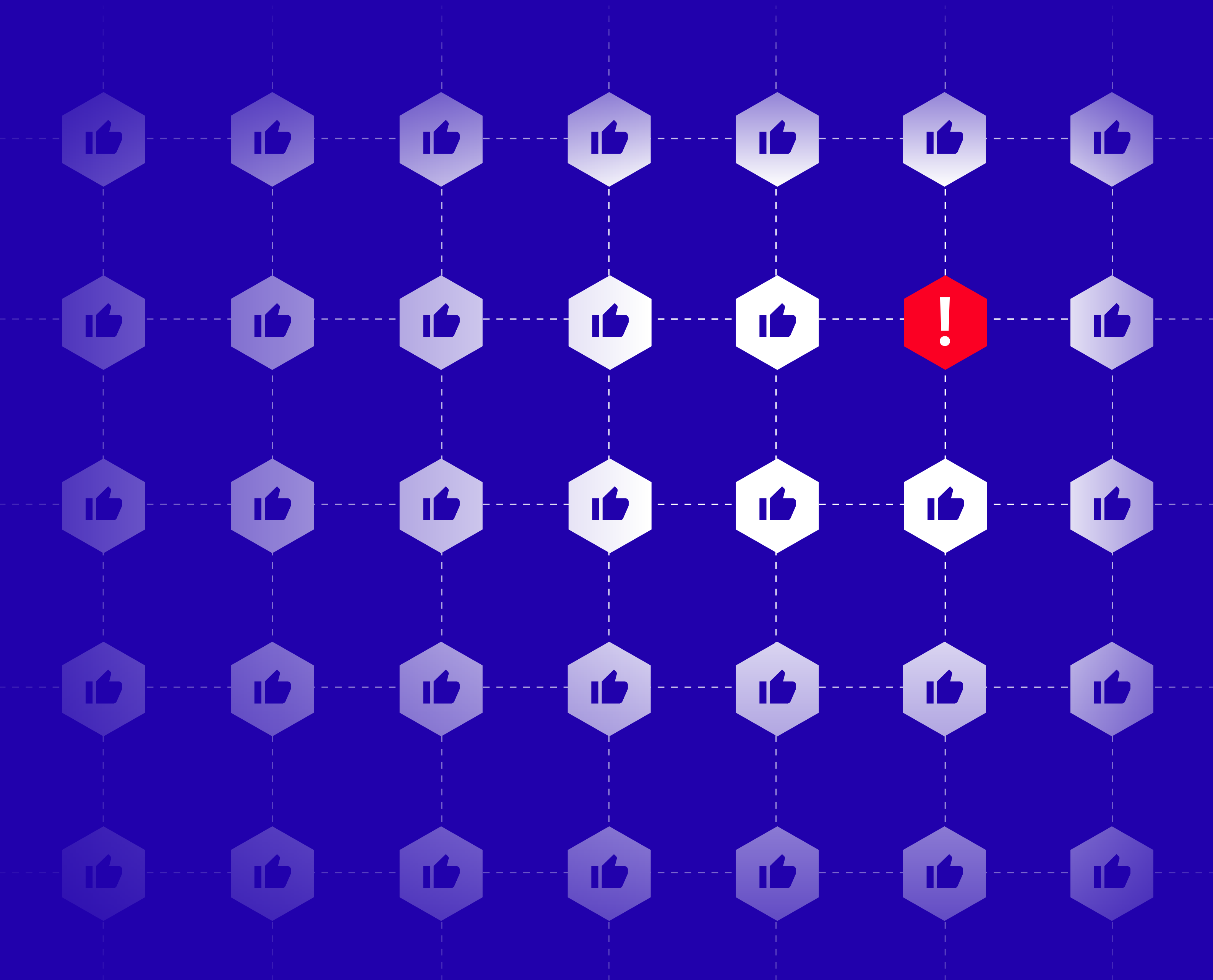
MELIUS
CyberSafe

What you don't know, *can* hurt you

Spot and stop hidden cyber security threats - before it's too late.

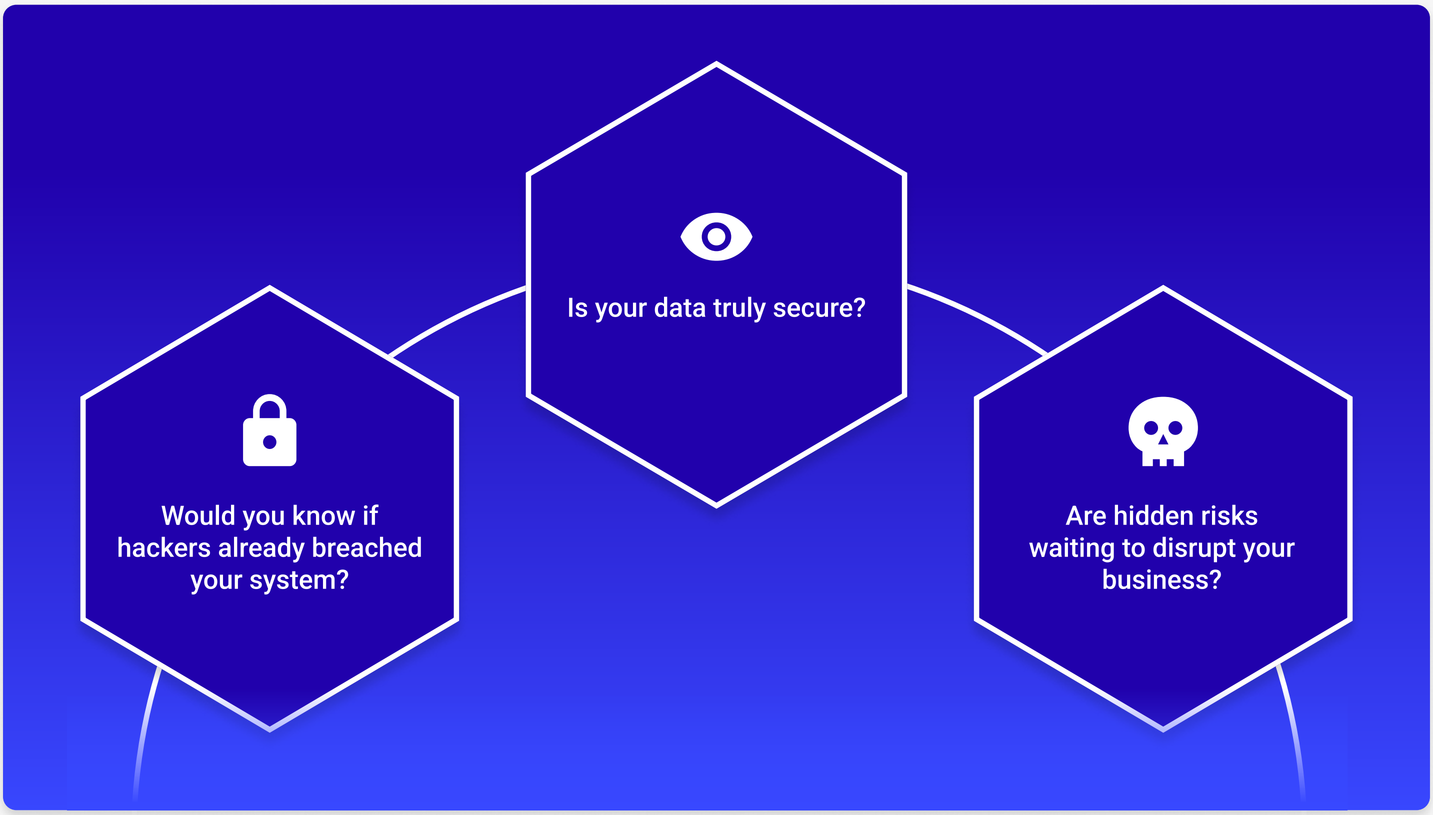


As cyber threats become more frequent, sophisticated, and harder to detect, businesses face unprecedented risks to their data and operations. Proactively identifying and neutralising hidden vulnerabilities is critical to staying secure.

What’s lurking in your digital blind spot?

Think of this quick guide as your flashlight in the dark, shining a light on the threats hiding under your business bed.

Let’s uncover the risks, bust the myths, and help you take control of your cyber security - before it’s too late.



Is your data truly secure?

Would you know if hackers already breached your system?

Are hidden risks waiting to disrupt your business?

The invisible threats

Cyber attackers often hide in plain sight, waiting for the perfect moment to strike. Here's what you're up against:

Phishing attacks

Convincing emails, fake websites, and even phone calls designed to trick employees into revealing sensitive information like passwords, financial details, or confidential company data. One click is all it takes for hackers to gain access to your systems.

Ransomware

These malicious programs lock you out of your files and demand a hefty ransom for their return. Paying up doesn't guarantee recovery, and the downtime alone can cripple operations.

Zero-day vulnerabilities

A zero-day vulnerability is a flaw in software or systems that developers don't yet know about, leaving it unpatched and vulnerable to exploitation. Attackers use these gaps to infiltrate systems, often with devastating consequences.

Outdated or unpatched systems

Skipping routine updates or ignoring software patches might seem harmless, but it's like leaving your front door unlocked. These outdated systems create an open invitation for cybercriminals to exploit known weaknesses.

Credential stuffing

Cybercriminals reuse stolen credentials from other breaches to infiltrate your systems. Without multi-factor authentication (MFA), these attacks often slip through unnoticed.

Invisible threats are not just hypothetical. These risks are real, pervasive, and potentially catastrophic if left unchecked. Recognising the dangers is the first step toward building a solid defense. What's hiding in plain sight in your business?

How safe is your business from invisible threats?

How safe is your business from invisible threats?

- How secure are your employee passwords?
- Is your data backed up and protected from ransomware?
- Would you know if a hacker accessed your system yesterday?
- When was the last time you conducted a vulnerability assessment?
- How long would it take your team to restore operations after an attack?

It’s time to sharpen your cyber defences

Preventative Measures:

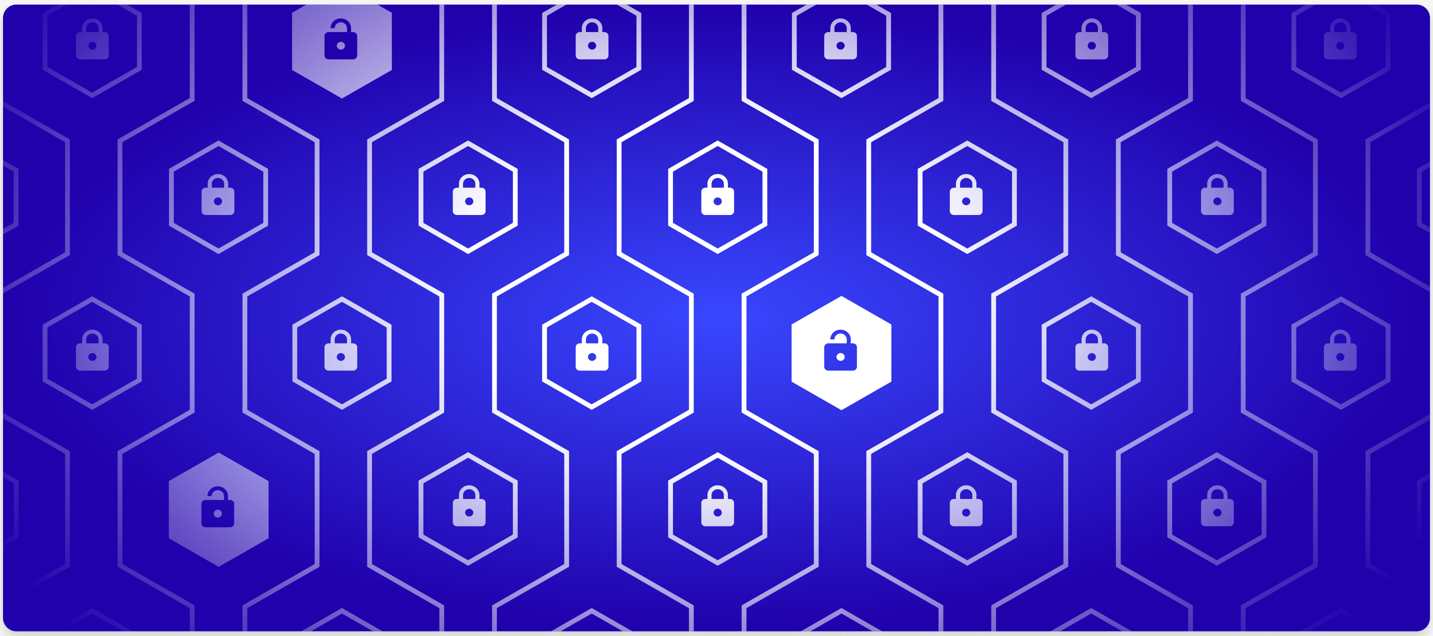
- Implement multi-factor authentication (MFA).
- Conduct employee training on phishing and other social engineering tactics.
- Regularly update and patch your systems and software to protect against vulnerabilities.
- Monitor third-party vendor security.
- Use Endpoint Detection and Response (EDR) and continuous monitoring tools.
- Use strong passwords, network segmentation, and device-level security to prevent unauthorised access.
- Develop a robust incident response plan.

In the UK government’s most recent cyber security survey, 50% of businesses reported a cyber security break or attack in the last 12 months

Myth Busters

Think your business is safe? Think again.
Let's bust some common cyber security myths.

MYTH	REALITY
My business is too small to be targeted.	43% of cyber attacks target small to medium sized businesses.
Cybersecurity is a one-time effort.	Cybersecurity requires continuous updates, monitoring, and training to keep up with evolving threats.
We haven't been hacked, so we're fine.	Many cyberattacks go unnoticed for extended periods. On average, it takes 194 days to identify and report a data breach. This means your organisation could be compromised without your knowledge for months.
Cyber Insurance will cover any losses.	While cyber insurance provides financial protection, it cannot restore lost data, fix reputational damage, or replace customers' trust.
Compliance equals security.	Compliance with standards like GDPR or ISO 27001 is a baseline, not a guarantee of robust security. Security is an ongoing process that extends beyond compliance requirements.



More than 10.5 million Suspicious Email Reporting Service (SERS) reports have been completed since April 2024, according to NCSC

What you can do

At Melius CyberSafe, we understand the unique challenges faced by businesses. Our CyberSafe platform provides a comprehensive, cost-effective solution tailored to meet these challenges head-on. Key features include:

Continuous Monitoring

- Scans and tests network integrity 365 days a year
- Checks over 200,000 known vulnerabilities daily
- Reduces breach detection time to just 1 day

Expert Penetration Testing

- CREST-accredited penetration testing services identify and exploit system vulnerabilities.
- Simulates real-world attacks to assess potential impacts on your organization.
- Helps prioritise security improvements based on identified risks.
- Combines vulnerability assessments and penetration testing for a comprehensive security view.

★★★★★

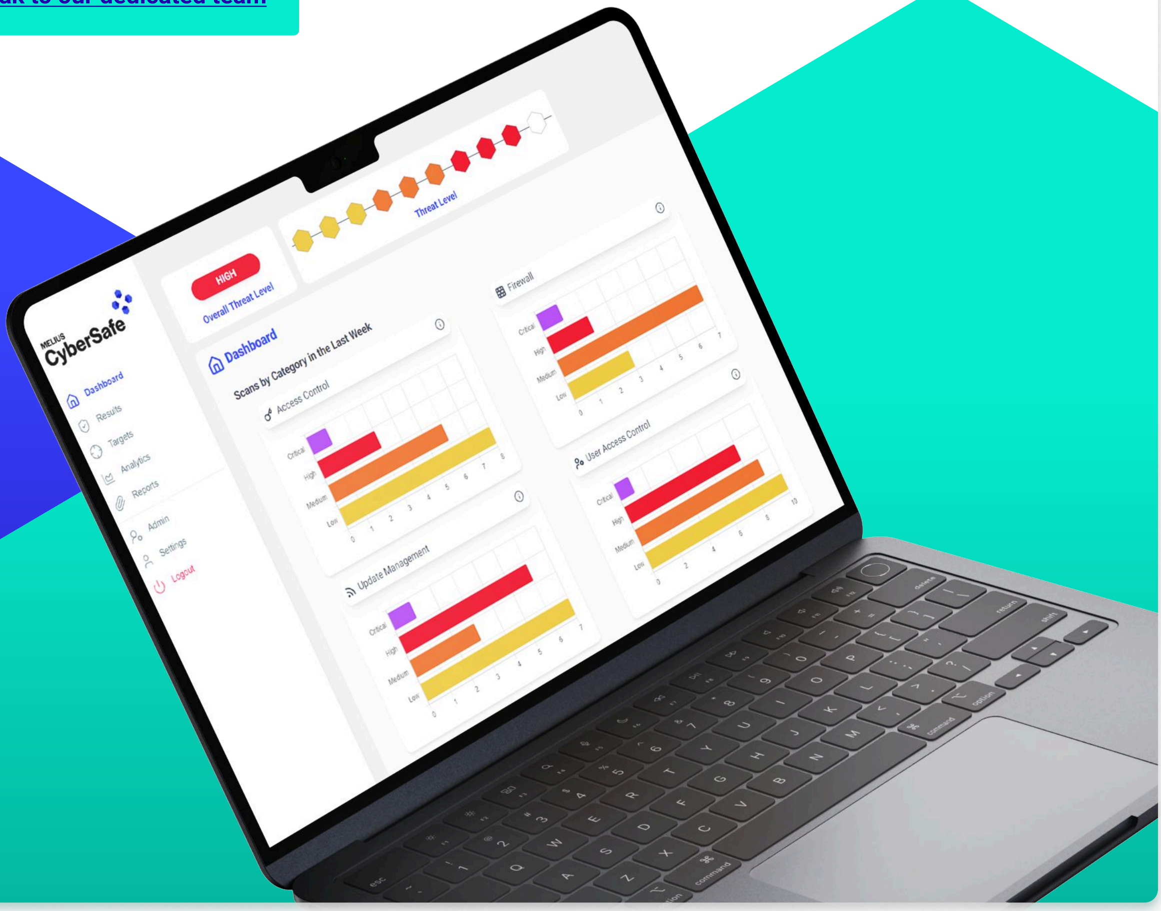
"We're very happy with CyberSafe. Having the ability to keep track of our cyber security controls in line with Cyber Essentials is great and will make re-certification quicker and easier in future - we feel we are in safe hands, our customers risk profile is paramount to us."

Stephen Adair, Partner
Broad Chare Partners

Are you prepared?

Melius CyberSafe offers a proven, scalable, and affordable solution to safeguard your organisation against evolving cyber threats. Don't wait until it's too late—contact us today.

Click here to speak to our dedicated team



About Melius CyberSafe

Melius CyberSafe is a Newcastle based cybersecurity company that helps business detect vulnerabilities in their IT systems, cloud infrastructure and web and mobile Apps. The company's CyberSafe platform automates the process of vulnerability scanning and penetration testing. Melius CyberSafe also helps businesses gain accreditation to key standards such as ISO 27001 and Cyber Essentials & Cyber Essentials Plus.

www.meliuscyber.com
Call us on: 0191 249 3003