censornet.

RED ALERT FOR CYBERSECURITY: 5 STEPS FOR DEFENCE.

Today's plan of action for mid-sized organisations

STEP 1.

Stay alert to new modes of attack

Size

The Identity Theft Resource Centre reported a record high 72% increase in breaches over the previous high-water mark - rising from 1,108 in 2020, to 3,205 in 2023. Over 90% of cyber-attacks start via email, but 65% of criminal actors then link their malware to cloud applications and the web. Not only does your organisation have to contend with increasingly sophisticated cross-channel attacks, you also need to be cognisant that every company is a viable target for hackers.

The NCSC, FBI and NSA all warn that cyber-criminals are no longer focusing their sights directly on large organisations with deep pockets. Businesses of any size can fall victim to malware-targeting, data theft, ransomware or services being knocked offline.

Speed

Mid-sized companies are being outpaced by cyber-criminals. The very same technologies that have been relied on to improve business efficiency, are now in criminal hands. Technically advanced resources, like artificial intelligence (AI) and machine learning (ML), are being used by bad actors to run automated cyber-attacks at speed and in unlimited numbers. At the same time, AI bots study targets exhaustively, probing for vulnerabilities and collecting data faster than humanly possible to form a perfectly targeted attack.

> **Half of those questioned admit that their cyber defence needs development.**

High risk, high impact

Website outages don't only lead to lost income. Breaches in customer information can severely impact the reputation of a company, and those dealing with sensitive data run the risk of falling foul of GDPR guidelines and the law. 1 in 5 businesses have experienced a negative outcome as a direct consequence of a cyber-attack.

Sophistication

Cybercriminals are becoming even more accurate and innovative. Scams designed to trick employees into handing over access to valuable data and funds are on the rise. AI and ML are empowering bad actors to create highly targeted content and evolve impersonation campaigns. ML can help hackers craft messages with a tone of voice that accurately mimics someone, and **audio and imagery in the public domain can be used to clone a voice to impersonate trustworthy individuals in calls or voicemails**.

The current threat to the everyday cyber landscape is so high that a third of UK mid-market organisations suffered an outage that knocked them offline for more than a day last year.

Ransomware is a particular threat. Unfortunately, **34% were forced to pay hackers an average of £140,000 in ransoms in 2023,** and some companies were coerced into **handing over more than £500,000.**

STEP 2.

Close any gaps in your defence

What are you protecting?

You may think your business seems less tempting to hackers compared to a large company but the mid-market possesses valuable information and supplies critical services.
In an increasingly connected economy, your organisation can represent another access point in the digital supply chain and a way to breach a wider network of businesses.

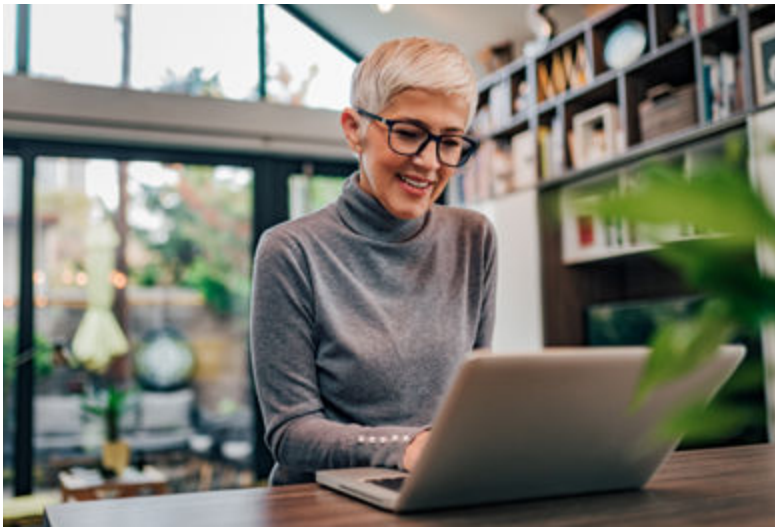
Protecting those who have access to your data and systems

The greatest asset to any organisation – its people - is typically its largest vulnerability. Some 23% of companies reported serious attacks in the last year from employees that opened suspicious or malicious emails. This number rises to 35% among businesses turning over more than £51 million.

> **48% of the mid-market said that they were unable to prevent dangerous attachments from reaching inboxes, and only a third had the ability to quarantine suspicious emails.**

Staff that work from their own devices or use older and unpatched versions of software are also prone to attack.
You need to consider where there are any potential chinks in your armour that need to be protected.

Over half of the mid-sized companies surveyed had not purchased any products specifically designed to protect hybrid and remote workers from cyber threats.



Not remotely covered

Once you have identified your more vulnerable areas, it is time to consider the security solutions that you already have in place, to ensure they rise to the challenge.

Remote and hybrid working means you need to defend your business outside traditional network perimeters. Hackers are working hard to exploit the gaps caused by your company's dispersed operations. Your remote workers need cloud-based technology designed specifically to reach them wherever they are to ensure they are protected.

STEP 3.

Streamline your current solutions

Are you weighed down by your security blanket?

Organisations have invested significantly in multiple security products in an attempt to bolster company cyber defences. Yet despite best intentions, this extensive accumulation of point products can have the opposite effect. Your solutions could be working against you.

Each product adds new layers of security, and the overlap between products creates complexity

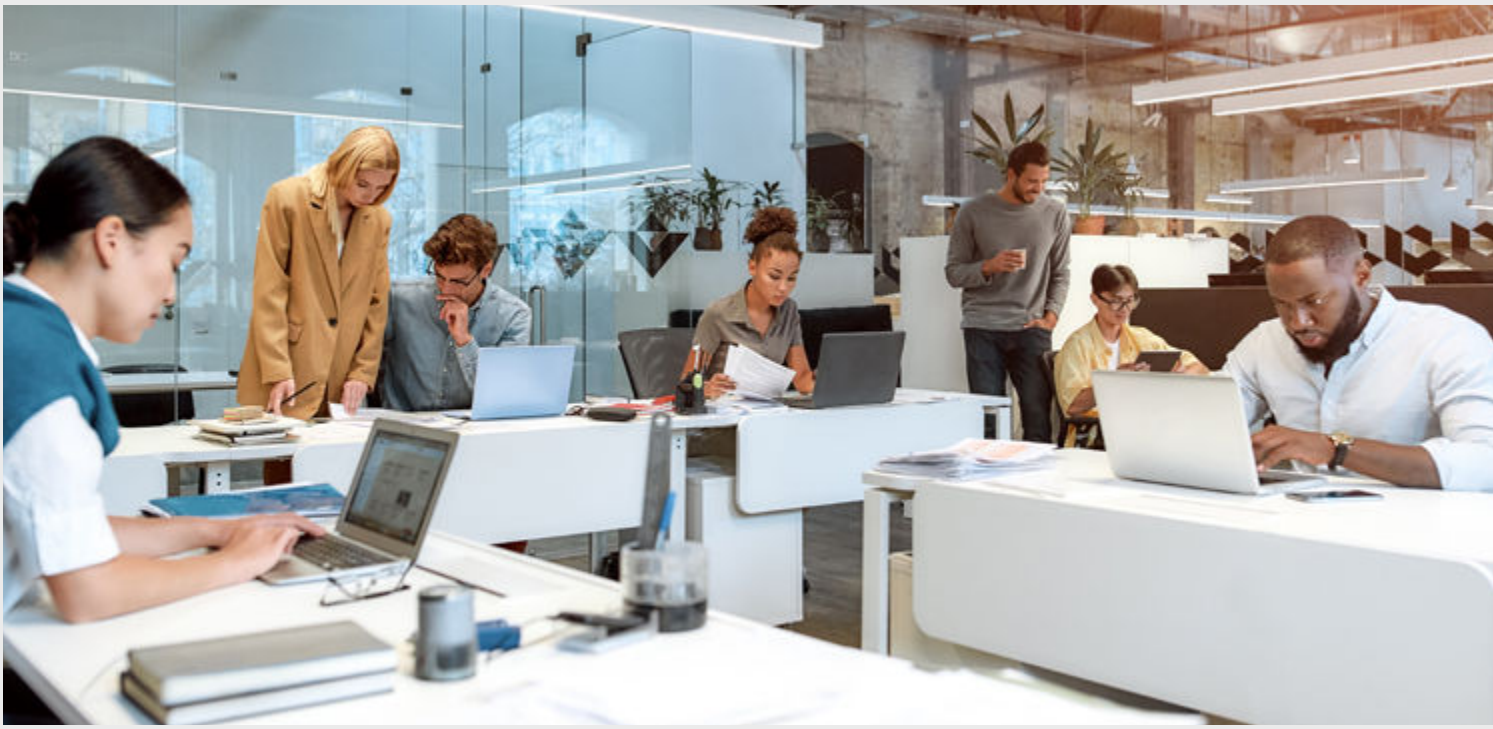
Most mid-market companies use an average of 22-point products, but this can rise to over 45 for companies in some sectors. However, multiple point products send multiple alerts, and these repeated security pings can flood your security team. More worryingly, serious warnings risk being overlooked in the deluge of information that your cybersecurity team is dealing with.

Cybersecurity software from different companies can't talk to each other

Relying on a high number of closed point products for protection means your endpoint solutions are likely to be siloed from each other. This limits visibility of attacks and creates an opportunity for threats to spread throughout your organisation and exploit the blind spots between your solutions.

Rising costs of security

If ever-increasing threat levels are reacted to individually, this can quickly lead to increasing costs for multiple technologies and larger security teams to implement them. These constantly rising costs are not sustainable in the long term. Instead, look for opportunities to close the gaps in your security and protect the major attack surface by connecting email, web, and cloud application security.



STEP 4.

Safeguard the resilience of your security workforce

Staff under high pressure

An incessant flood of alerts can overwhelm your cybersecurity professionals. The average number of point products managed in a single organisation can generate over 810 alerts per day. Most mid-sized businesses have less than three members of cyber security staff. This leaves security professionals with just 87 seconds to review each security incident and decide what is a genuine threat.

This translates into over half of security professionals feeling overwhelmed or unable to cope with the stress. It's unsurprising that 29% of cybersecurity professionals are suffering from sleep deprivation due to cybersecurity concerns...

Automate security to reduce alert overload

To increase cyber-resilience, security must work harder, keeping pace with threat alerts whilst reducing human intervention. Products need to be able to react autonomously to attacks, rather than just acting as a warning system. **Crucially, this simplifies security, whilst giving time back to overwhelmed cybersecurity professionals, who can then focus their efforts on stopping the most sophisticated attacks**.

Businesses are beginning to react to this new challenge. Gartner predicts that 80% of enterprises will have adopted a strategy to unify web, cloud services and private application access by 2025.

Red Alert:

- **43% of mid-market companies have less than 3 members in their cybersecurity team but can receive over 815 alerts on an average day**
- **14% said that they don't have time to investigate 50% of the alerts they receive every day**
- **36% are anxious about missing a cybersecurity alert**
- **38% have received an emergency call in the middle of the night**
- **The average amount of sleep for a security team is 5.58 hours.**

STEP 5.

Deploy the right autonomous solution for your company

Consider a cybersecurity solution that automatically responds to threats as it identifies them

As companies continue to grapple with closed point-products, a fundamental change in cybersecurity design and application is essential. Encouragingly, over three quarters of organisations said they plan to invest in a cloud-based security platform that allows their security products to autonomously share security event data to better protect their business.

Unifying security

New technologies, including machine learning, present an opportunity to ensure all the individual stacks in your security work in unity, talking with each other to identify and track attacks as they attempt to proliferate across your organisation.

A product that can also receive rapid updates to threats and information on new malware from other users will ensure that all possible intelligence is utilised in the defence of your company as cyber criminals' techniques continue to evolve.

Our autonomous cloud security platform integrates attack intel across email, web and cloud applications to ensure cyber defences react at lightning speed.

> **The machine learning-powered platform takes threat feeds from millions of users globally and combines them with commercially available and government threat feeds from the likes of the NSA and GCHQ.**

All these insights are automatically fed into a decision engine, that reacts autonomously to all threats.

Ultimately, the future of cybersecurity is integration and automation. Mid-size businesses need a platform that achieves this across four core areas of security – securing email, securing web, securing cloud applications, and managing authentication – which together account for approximately 93 per cent of threats in the cyber landscape.

About the Research

This report summarises the results of independent opinion research commissioned by Censornet and carried out by 3Gem. The online research surveyed 200 IT decision makers in UK based companies with under 5000 employees. The research was completed in January 2024. Respondents were split across the public and private sector and included Chief Technology Officers, Chief Information Officers, Chief Information Security Officers and IT Directors and Managers from a range of industries including finance, retail, technology, manufacturing and construction.

About Censornet

Headquartered in an innovation hub in Basingstoke, UK, Censornet gives mid-market organisations the confidence and control of enterprise-grade cyber protection. Its Autonomous Security platform integrates attack intel across email, web, and cloud applications to ensure cyber defences react at lightning speed. For its millions of users globally, Censornet synthesises a billion threats a day, to give full protection - wherever attacks start and wherever they move.

It's supported by an award-winning team of customer support specialists. Censornet's clients include Fever Tree, Lotus Cars, Parnassia Groep, Mizuno, Radius Payments, Newlife Disabled Children's Charity, National Portrait Gallery, Hallmark Hotels and Thatchers Cider. It was awarded the 'Exceptional Customer Satisfaction Award' at the 2024 Business Awards UK.

For more information, please visit **www.censornet.com**

censornet.

www.censornet.com