censornet.

THE UK MID-MARKET ON CODE RED.

The State of the UK's Cyber Security Response

Ed Macnair
CEO, Censornet

Record-breaking Cyber Attacks, with an 'Apocalyptic' Bug

The UK is a popular target for cyber-attacks. It's now the third most targeted nation by hostile states, according to **cabinet minister Steve Barclay**. It's why laws are being reviewed to boost British business' cyber resilience. It's not just hostile states on the attack; 2021 was record-breaking, with breaches and ransomware demands soaring.

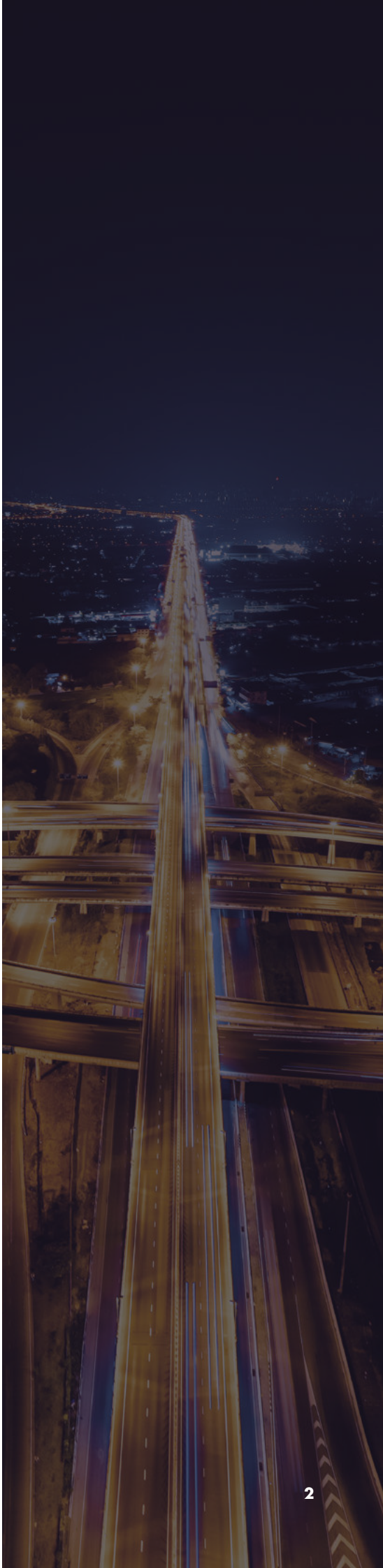
The Identity Theft Resource Centre reported 1,862 breaches in 2021 compared to 1,108 in 2020 - an increase of 68%. The wave of cyber-attacks began with four zero-day exploits in Microsoft's Exchange Server. It ended with an 'apocalyptic' vulnerability in the logging tool, Log4j, allowing criminals to attack the Java library which underpins numerous applications, websites, and servers.

Hackers are shifting from "big-game" to mid-sized targets

Many of the serious breaches came together, with record-breaking ransom demands. REvil, notoriously, asked for $70 million to end its attack on Kaseya. It's not just high-profile targets that are under attack. In February 2022, the UK's National Cyber Security Centre (NCSC) in partnership with the Federal Bureau of Investigation (FBI), **National Security Agency (NSA)** and Australian Cyber Security Centre, advised that hackers were shifting from "big-game" to mid-sized targets.

The State of the UK's Cyber Security Response

This study explores how mid-market organisations fended off attacks in 2021, and their plans for 2022. It reviews the state of the UK's cyber response with 200 IT leaders working across a range of sectors including finance, retail, technology, and manufacturing. The study reveals an unprecedented snapshot into UK mid-market cyber security readiness, highlighting the needs, wants and problems. It uncovered an uncomfortable truth - the new normal of cloud-enabled hybrid working and the devastating nature of today's threats require a step-change in cyber protection.



1. The UK's cyber security blanket

A best-of-breed approach to security exists for good reason. As new threats emerge, the desire to get the best possible protection makes perfect sense. That is, until point products became part of the problem.

> **Many mid-market firms now use an average of 24-point products to protect themselves. Over a quarter (27%) rely on more than 31 security solutions, and seven percent deploy more than 50-point products.**

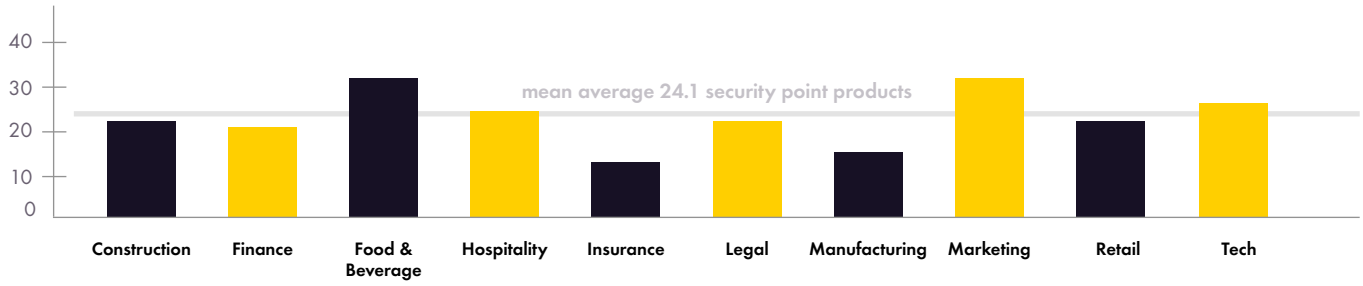
Tech and Marketing most likely to be managing 50+ point products

Those working in the technology (18%) and marketing (17%) sectors are most likely to use more than 50-point security products.

This poses several critical challenges. Firstly, it is difficult – if not impossible - to manage such a large number of point products. Most are security black boxes. Even if APIs are in place, they are often extremely limited and focused on extracting information rather than enabling security policies and rules to be modified.

Secondly, imagine a company that uses 50 security products. Each of these solutions will generate constant alerts - most of which will have to be investigated by the security team. Many will be trivial or insignificant, while a smaller number will be so serious that they could lead to a financially disastrous breach or cyberattack but risk being overlooked.

Average number of security point products



2. There is no time to investigate

On an average day, mid-market firms receive 716.4 cyber security alerts. It gives each security person an hour to investigate 35.3 security alerts. This requires time, resources, and capacity. Something that isn't easy in an industry where security practitioners are grappling with new strains of aggressive threats.

No time, Nor Capacity

It's a workload that is eroding cyber resilience and putting businesses at risk of missing critical threats.

> **One in ten (11%) said they did not have the time or capacity to investigate 50% of the alerts they receive every day.**

A similar number reported looking into even fewer threats, with 9% saying that 60% of daily threats are not investigated and the same percentage (9%) reporting that 70% of threats are not dealt with properly. Meanwhile, 42% of respondents have personally suffered the fear of missing a cybersecurity alert.

Time and capacity to investigate

45% have two or fewer people

69% of mid-sized businesses have three people or fewer in their team looking after cyber security

The challenge is compounded by businesses lacking the manpower to investigate alerts at the speed they arrive. Nearly seven in 10 (69%) mid-sized businesses have three people or fewer in their team looking after cyber security. Nearly half (45%) have two or fewer.

Unsustainable, but Unnecessary

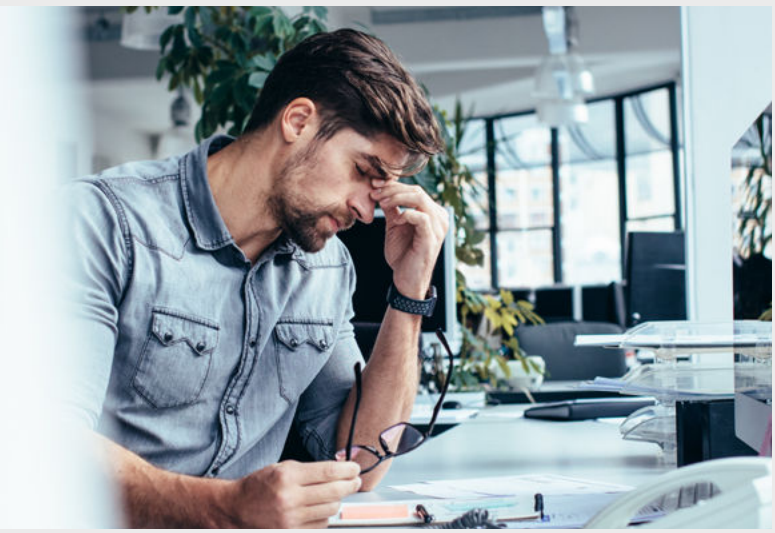
This situation is not only unsustainable, but unnecessary. Cloud security can act autonomously to easily perform routine tasks that once required human intervention. This is a step beyond automation - which can perform simple jobs in a mechanical fashion. Autonomy goes further, by responding to unknown threats and protecting organisations around the clock without needing human intervention.

3. The human cost

The sheer volume of information being generated by security tools gives businesses just 102 seconds to assess whether a threat is real, how serious it is and what action needs to be taken. For those protecting an organisation, it's difficult to stay in control.

Sleep-deprived, overwhelmed, under-pressure

Many are left feeling overwhelmed and unable to cope with the demands of the workload.



Nearly half (47%) admit to feeling overwhelmed when faced with too many cybersecurity alerts. While just under a third (31%) are unable to cope following prolonged periods of work-related stress and burn-out.

In public sector organisations, the pressure is even worse. The number of professionals feeling overwhelmed rises to nearly six in 10 (59%) and 34% feel unable to cope.

The demands of the workload leaves security professionals unable to switch-off. More than a third (38%) have received a call in the middle of the night to investigate a cyber security incident and almost one in ten (9%) say they suffered from sleep deprivation due to cyber security concerns. Typically, security teams are surviving on less sleep than recommended.

The average amount of sleep someone responsible for cyber security gets, is 5.7 hours, significantly less than the seven hours or more recommended by the NHS[1].

[1]. https://www.nhs.uk/live-well/sleep-and-tiredness/how-to-get-to-sleep/

4. The real and present danger

As many as two in three (65%) mid-market organisations suffered an outage in 2021, with half (33%) seeing systems knocked offline for more than a day. These incidents were driven in part by the unwitting insider threat: 17% of respondents reported serious attacks after employees opened suspicious or malicious emails, with that number rising to 28% for businesses turning over more than £51million.

Organisations don't just stand to time and custom:

> **30% suffered a data loss because of a cyberattack in 2021, with that figure rising to 36% for smaller businesses turning over between £1- £5 million a year.**

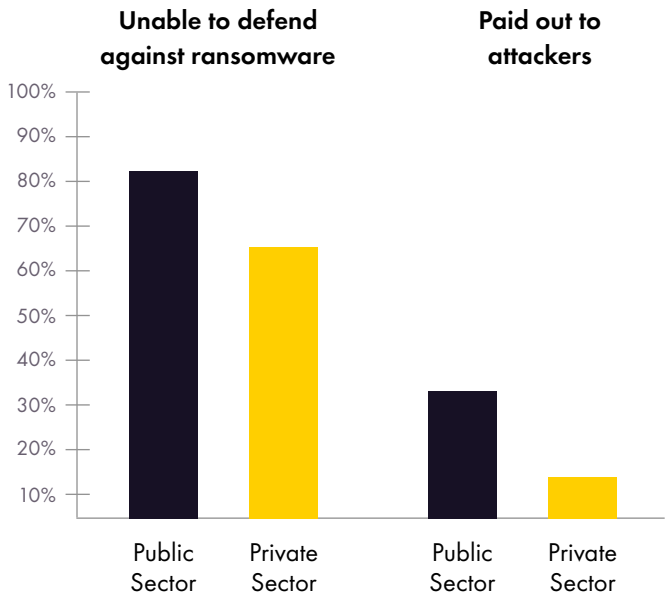
The full extent of stolen intellectual property is not always immediately apparent. It's not just the sleepless nights. Supply chains are being interrupted. In February 2022, a supplier of components to Toyota was hit by a suspected cyber attack. It forced the world's largest carmaker to close all of its factories in Japan for the entire day. The net result, it had to halt production on 13,000 vehicles.

One in five pay their ransom

A closer look at ransomware illustrates the potential severity of a security breach. In 2021, more than two thirds (69%) of midsize companies didn't feel able to protect themselves against ransomware, and with good reason.

Over the year, one in five (21%) suffered a ransomware attack and subsequently paid the ransom. The average pay-out was £144,000, with 7% of those handing over in excess of £500,000.

Public sector organisations were worse affected than their private sector counterparts. A huge 83% reported they felt unable to defend against ransomware, compared to only 65% of private sector organisations. And a third (34%) eventually paid out to attackers, compared to 14% in the private sector. The picture is all too clear: despite a wide range of point solutions on the market, organisations are still paying the price for inadequate defence, particularly in the hard-pressed public sector. When budgets and staff time are squeezed, a more intelligent approach is needed to tip the scales.



5. Not remotely covered

The global work from home mandate at the onset of the pandemic saw organisations scramble to accommodate the new modus operandi. It was the final death knell for the network perimeter, as it became universally accepted that hybrid working is here to stay. It acted as a forceful prompt for security teams to evaluate whether existing security protocols were enough to protect remote workers.

The study revealed that over half (51%) of mid-market organisations said they had not purchased cybersecurity products designed to specifically protect against threats for hybrid and remote workers. This rose to 66% for organisations employing between 250 and 2,999 people.

With many hybrid workers not specifically protected, 41% of mid-market firms reported that future proofing their cyber defences "needed development". Given that the 2020 pandemic drove a 25% rise in remote working and associated use of cloud applications, that's a major risk.

Visibility into the Expanding Cloud Attack Surface

Overall, 43% of organisations enjoy complete discovery and visibility into all cloud applications. However, companies employing between 50 and 249 employees were less likely to employ solutions offering this.

> **Twenty-seven percent of smaller companies reported deploying these tools, compared to 50% of companies employing 250-2,000 employees, and 62% of larger enterprises with between 3,000 and 5,000 employees.**

And visibility or not, only half (51%) of all businesses had complete control over the use of their cloud applications – such as the ability to block specific actions in each app.

It is fundamentally important to gain visibility of the cloud, because it is now a primary attack vector. In 2021, more data breaches involved cloud assets than on-prem assets, Verizon reported in its annual Data Breach Investigations Report. A separate report conducted by 451 Research found that 40% of organisations suffered a cloud-based data breach in the past 12 months.

Keeping an eye on the cloud is vital for tackling insider threats or even ensuring good cyber hygiene among employees. If you are not ready to protect your cloud, cybercriminals are certainly prepared to exploit this weakness.

6. Email, Web, Cloud, Identity

Criminals are hunting for opportunities to exploit any gaps in defences – launching targeted strikes in multiple different places, often all at once. Yet only four in ten (37%) were able to prevent cross-channel attacks in 2021 – for example, attacks that start via email, but continue over the web or cloud application channels.

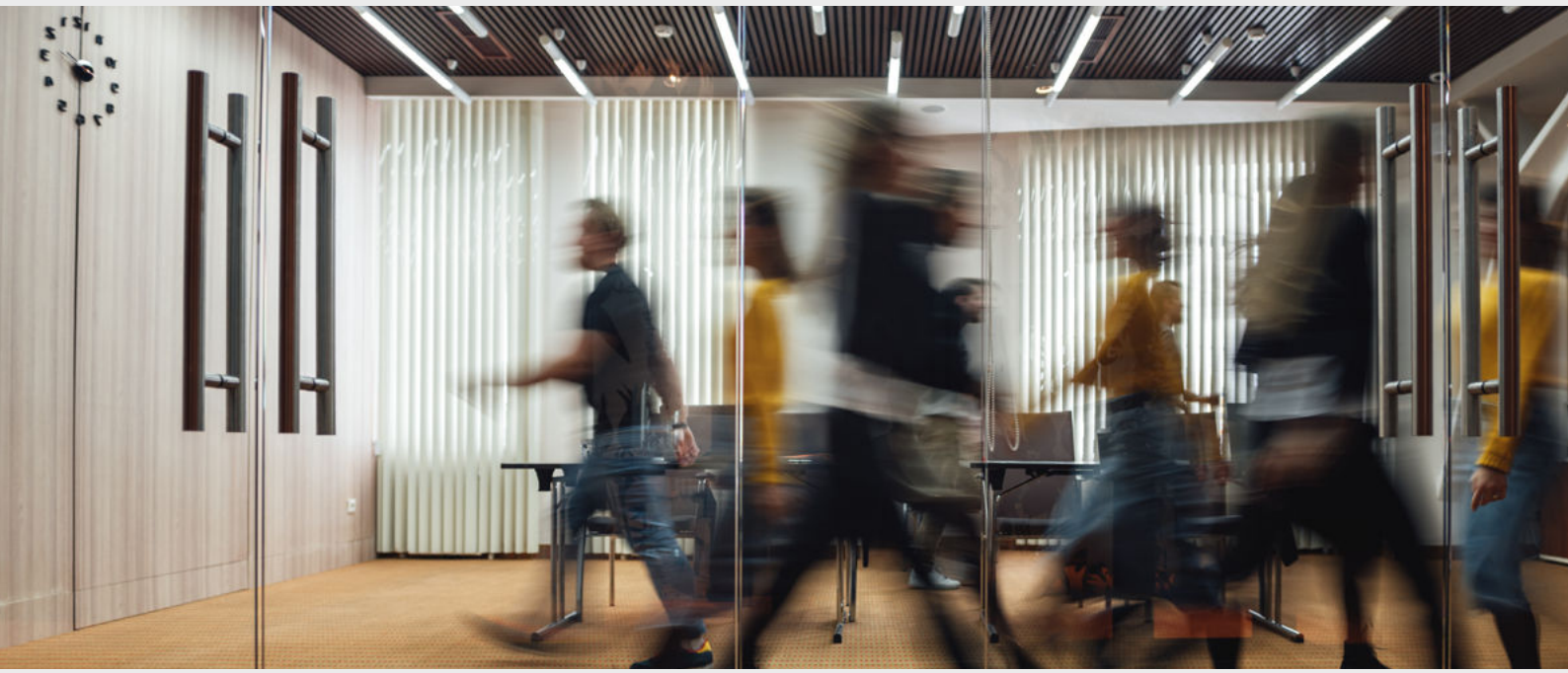
Weaknesses in email, web, cloud, and identity

It's not hard to see why. When we look at current defence capabilities, there are clear weaknesses across a range of attack vectors.

> **Just half (51%) of the UK mid-market said they were able to prevent dangerous attachments from reaching users' inboxes, and only a third (35%) had the ability to quarantine suspicious or malicious emails.**

If we turn to user identification, the picture gets worse. Only a quarter (25%) of organisations said they were able to detect when a user account was taken over.

These statistics are worrying enough in themselves, but together contribute to a bigger problem. Because if your endpoint solutions are siloed from each other, once an attack evades one defence – whether it's email, cloud, web, or identity – it's highly unlikely to be stopped by others.



7. The cybersecurity outlook for 2022

In response to these legitimate fears, organisations want to see fundamental changes in the way cybersecurity is designed and run, starting with a more integrated approach. **Gartner predicts** that 80% of enterprises will have adopted a strategy to unify web, cloud services and private application access from a single vendor's security service edge (SSE) platform by 2025.

This rings true with the security professionals surveyed: 46% percent of organisations want to see security vendors open up traditionally closed point products to enable an automated response to cyberattacks. A more coordinated approach that would allow for email, web, identity, and cloud application security systems to work in tandem, identifying and tracking attacks as they proliferate across an organisation.

The demise of cost and complexity

Organisations are also keen to see reductions in the complexity and cost of enterprise-grade security, with 37% and 34% respectively ranking these considerations as their top cybersecurity wish for 2022. Gartner's 2020 Security and IAM Adoption Trends Survey supports this and shows most organisations have, or plan to have, a vendor consolidation strategy. Of those already in the process, more than 80% had been consolidating for at least a year.

For businesses struggling to stem the tide of cyberattacks, the answer cannot be yet another pricey point product. The message is clear: they want - and need - to consolidate security with effective, reliable security systems that don't require a PhD to install and a team of hundreds to run them night and day.

The plans to invest

> It's not surprising, then, that three quarters (76%) say they have plans to invest in a cloud-based security platform **that allows their security products to autonomously share security event data to better protect their organisation.**

Autonomous, integrated cloud security is a crucial step towards effective defence that doesn't cost the earth and can keep up with evolving cross-channel attacks.

In many ways, 2022 brings more of the same for mid-market security teams: the same worries about sophisticated attack types, human error, alert fatigue, and cost control. But there is cause to be optimistic. As integration and autonomous technology becomes more effective and affordable, intelligent, enterprise-grade protection is already within reach for the mid-market.

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 December 2021. 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 Integrated Cloud Security platform integrates attack intel across email, web, and cloud to ensure cyber defences react at lightning speed. For its millions of users globally, its AI-driven, autonomous solution is smarter, faster, and safer than is humanly possible. It's supported by an award-winning team of customer support specialists. Censornet's clients include Fever Tree, Lotus Cars, Parnassia Group, Mizuno, Radius Payments, Newlife Disabled Children's Charity, National Portrait Gallery, Hallmark Hotels and Thatchers Cider. It was named Cloud Security Product of the Year (SME) at the Computing Cloud Excellence Awards 2021. For more information, please visit https://www.censornet.com