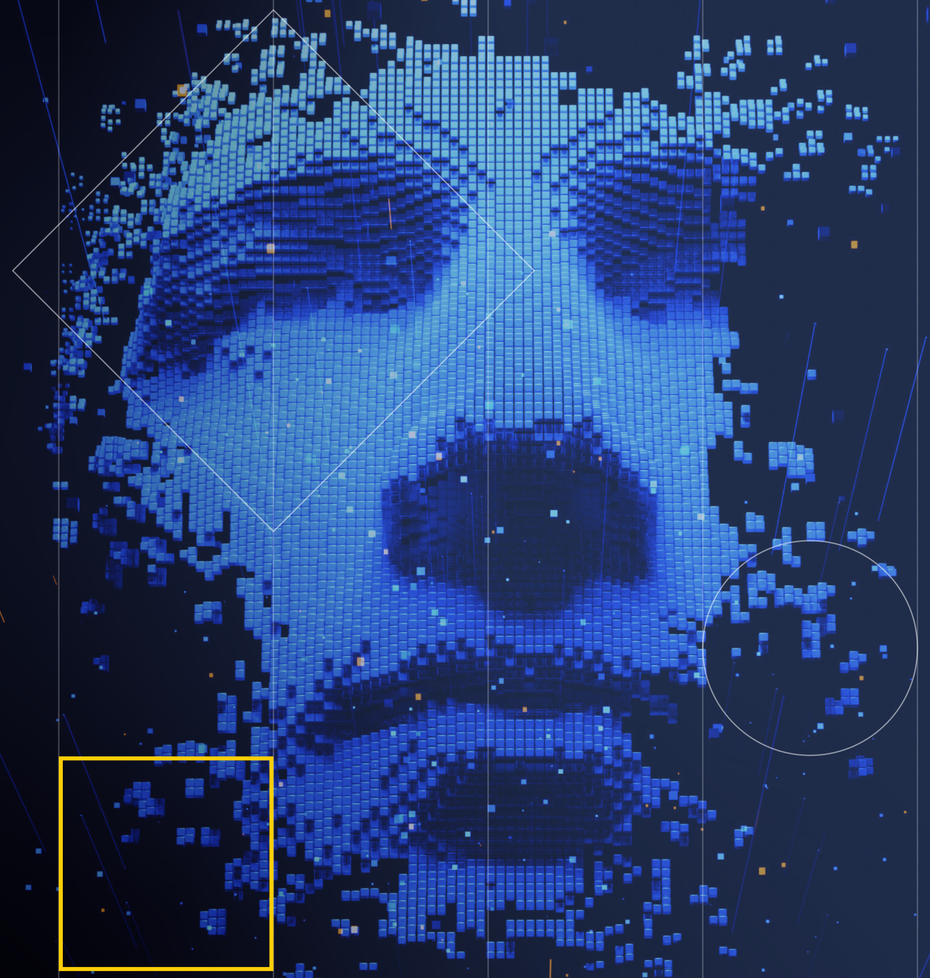


censornet.

State of AI in Cybersecurity

Is AI the answer to cybersecurity threat overload?

As AI becomes more sophisticated, traditional cybersecurity systems may struggle to fight AI threats.

And with over half (53%) of global IT decision makers concerned about ChatGPT's ability to help hackers craft more believable and legitimate sounding phishing emails[1], it's no wonder AI is at the top of the cybersecurity agenda. In fact, (84%) of IT decision-makers plan to invest in AI-driven cybersecurity in the next two years and almost half (48%) plan to invest before the end of 2023.[2]

Whilst this intention for investment is partly driven by a desire to protect against new and evolving threats, there is also another aspect at play. 35% of UK SMEs have two or fewer people in their cybersecurity team.[3] And with this comes huge risk. One in five cybersecurity pros are losing sleep over concerns – up from 9% on 2022, contributing to lack of concentration and inability to focus. In fact, according to Gartner, lack of talent, or human failure, will be responsible for over half of significant cyber security incidents.

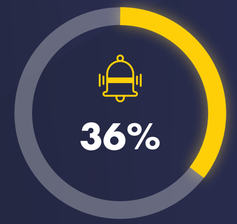
> **AI isn't the silver bullet to everyone's cybersecurity worries. While generative AI has moved AI to the front of everyone's minds, artificial intelligence, and more specifically machine learning has been a feature of cybersecurity for a while, delivering a huge amount of value for security teams and improving security for their organisations. From stopping cross channel attacks to automatically preventing data exfiltration attempts.**

Richard Walters, CTO, Censornet

1, 2 BlackBerry Limited Research (February 2nd 2023)
3 Censornet research, 2023

6 in 10 cyber alerts go undetected

SMEs receive 597 security alerts each day



feel overwhelmed when faced with too many cyber security alerts

Down 11% from 2022 PRIVATE **34%** / PUBLIC **36%**

Only 2 mins available to check each security alert

Cybersecurity professionals check 26 security alerts per hour on average, that's only 2 minutes of attention on each alert

1 in 5 losing sleep over security concerns

fear missing an alert that will allow a threat to enter the business

PRIVATE **34%** / PUBLIC **39%**

Attention spread too thin across multiple security products

censornet.

So where does AI fit in today?

SMEs are feeling overwhelmed by the sheer number and speed of cybersecurity alerts. Intelligent automation and integration are the keys to regaining control. As machine learning and AI capabilities continue to evolve, solutions are emerging with the ability to autonomously sift and prioritise alerts, even without preloaded playbooks.

The industry is investing heavily in AI-led security. OpenAI, the creator of ChatGPT and Dall-e, has announced a $1 million cybersecurity grant program to enhance and measure the impact of AI-driven cybersecurity technologies.[4] Forrester's forecast reveals cybersecurity is the fastest-growing AI software category, with significant investments being made in real-time monitoring and response in order to mitigate growing cybersecurity threats.[5]

> **The democratization of AI is a game-changer in the world of cyber-attacks. Now more than ever, bad actors can easily manipulate the power of AI to automate and advance attacks. Generative AI is helping hackers create highly persuasive content for phishing, or business email compromise (BEC) attacks. It's also much easier to create convincing deepfakes in manipulated videos and images.**
>
> **The pressing question that all cybersecurity teams need to ask is how to adapt to these changes. Whilst AI- powered tools are a core part of the solution, the human element cannot be ignored. Training, education and embedding a culture of security awareness throughout the organisation are equally as important as any AI-powered tool in protecting against the new threat landscape.**

Ed Macnair, CEO, Censornet

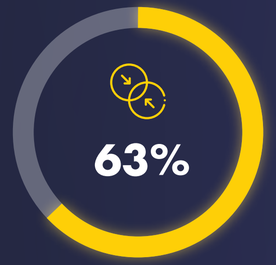
4 cointelegraph.com/news/openai-commits-1m-to-support-ai-driven-cybersecurity-initiatives
5 Global AI Software Forecast 2022 (September 29th 2022)

The move to autonomous AI-powered security

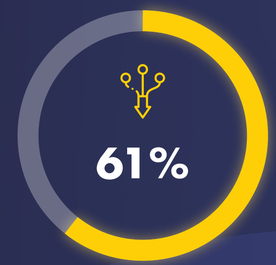
7 in 10 investing in autonomous alert-sharing

of SMEs investing in automated alert and state data-sharing tech to prevent cyberattacks in real time

The SME solution: AI-led, consolidated security

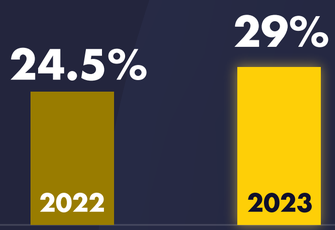


reduced their number of security vendors in the last 12 months



adopted a consolidated approach in the last 12 months

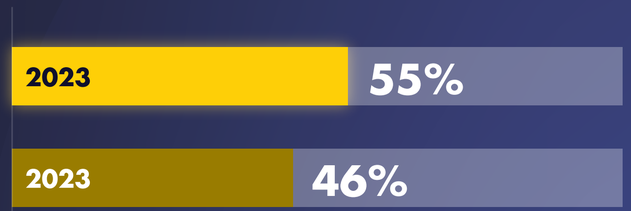
Increased demand for autonomous security to prevent attacks



% who say the ability to set rules that enable autonomous response to security events to prevent attacks (using ML/AI) - is their top cybersecurity wish

PRIVATE **31.4%** / PUBLIC **27.7%**

SME demand for the ability to automate responses on the rise



Over half say their top cyber security wish is an automated response to cyber threats

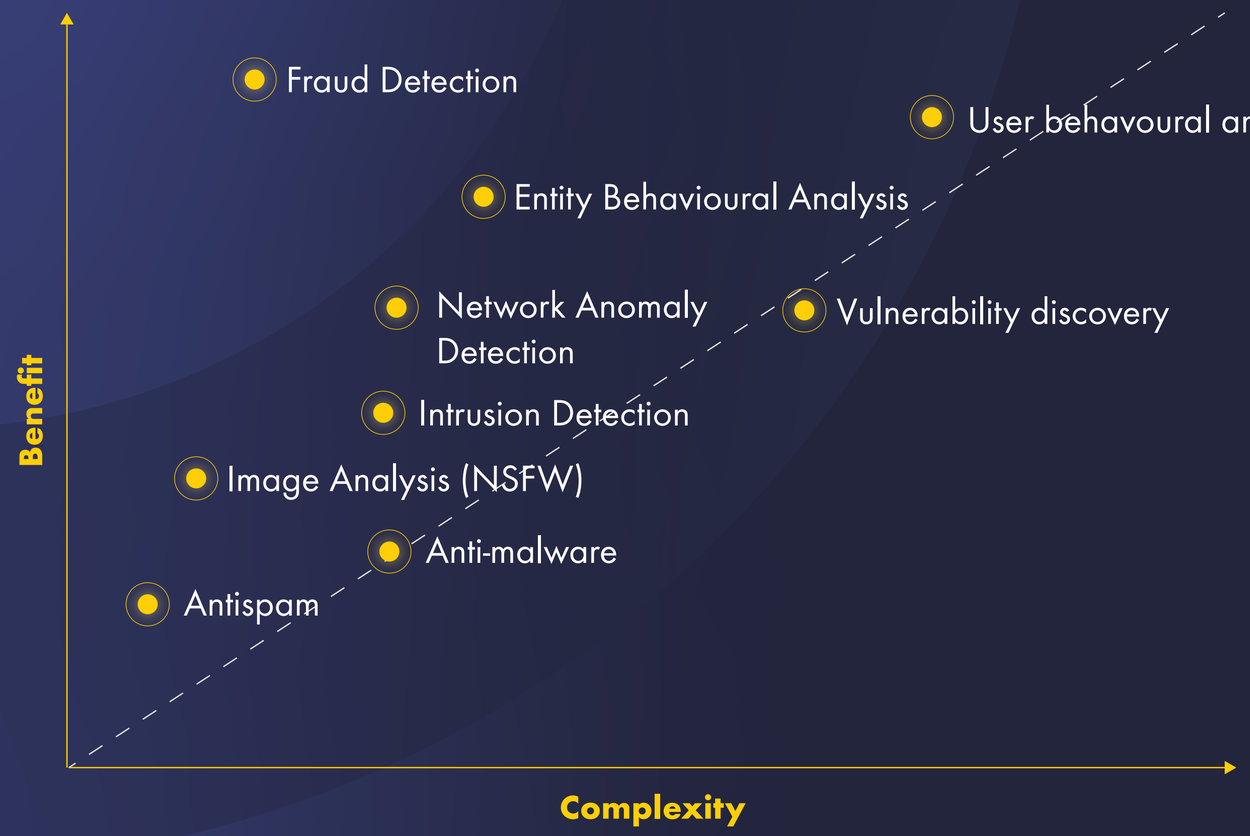
↑ Up 46% from 2022

censornet.

Organisations are placing their trust in AI to streamline security operations and save costs. But where can AI actually make a difference?

We have mapped out the use cases for AI, showing the complexity involved in developing the technology against the benefits:

Cyber Security use cases



Want to learn more about the uses of AI in cybersecurity?

We expose the hype and give you the 10 steps to effective AI.

Check out the whitepaper:

censornet.

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 AI-powered cloud security platform integrates attack intel across email, web, and cloud to ensure cyber defences react at lightning speed.

Research was conducted in April 2023, surveying 200 IT decision makers at UK mid-market organisations.

censornet.

www.censornet.com