FourNet®

Attack and Defend

The Role of Artificial Intelligence in Cyber Security

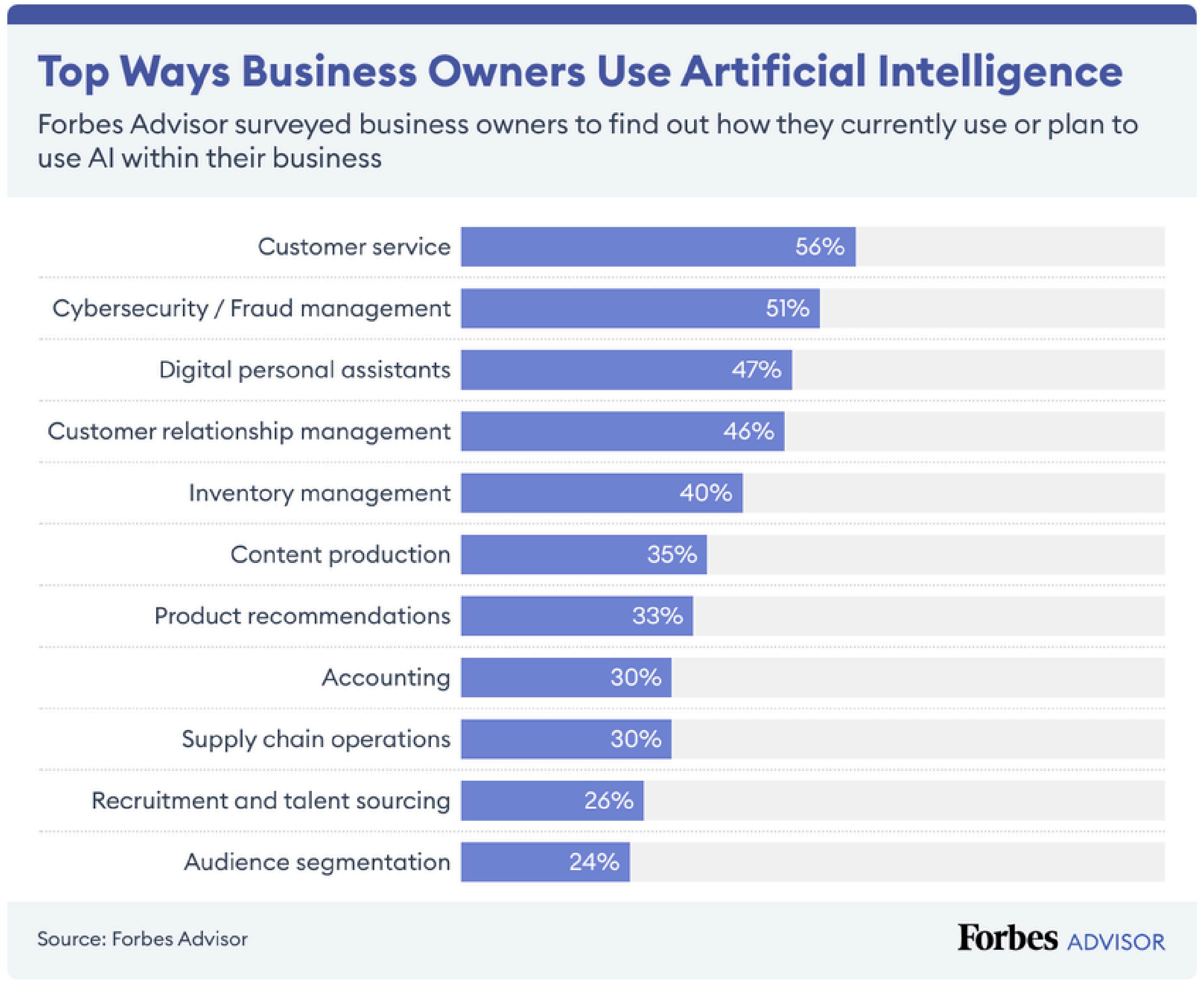
Contents

Introduction

The Growth of Artificial Intelligence

Since the large-scale launch of ChatGPT and other Generative Artificial Intelligence (AI) tools in 2022, there has been an explosion in the interest of leveraging AI in all forms of life. People have been using AI to help them source information, streamline their work and just about anything you can think of.

It's not just the public using AI, a recent study found that 68% of organisations in the UK are also using AI and the 32% that aren't currently, plan to implement tools in the future. The graph below gives you an idea of how AI is being leveraged across businesses.


Top Ways Business Owners Use Artificial Intelligence

Forbes Advisor surveyed business owners to find out how they currently use or plan to use AI within their business

Source: Forbes Advisor

However, not all uses of AI are positive. AI plays a pivotal role in the dynamic field of cybersecurity, offering powerful tools for both attackers and defenders. AI's ability to process large datasets, learn from patterns, and automate responses makes it a double-edged sword; it enhances security measures and enables more sophisticated cyberattacks.

In this guide, we share insights into the latest trends surrounding AI in cybersecurity, looking at the ways that it is being used from both the attacker's and defender's perspectives. We will also share ways of adopting AI to strengthen your cybersecurity defences.

Snapshot View of the Future of AI in Cybersecurity

As we look ahead , AI is expected to continue reshaping the cybersecurity landscape. According to the World Economic Forum, the adoption of specialised AI models tailored for cybersecurity is set to increase, providing more precise and actionable insights to combat evolving threats. AI-driven threat detection and response systems will become more sophisticated, leveraging real-time data to predict and neutralise attacks swiftly

Rise of Specialised AI Models

AI will move towards using smaller, specialised language models that offer more tailored and actionable insights for cybersecurity teams. These models will be trained in real-time to adapt swiftly to the constantly changing threat landscape.

Increased Sophistication of AI-Driven Attacks

Cybercriminals will exploit generative AI to launch more sophisticated phishing campaigns, create more convincing deepfakes, and develop adaptive malware. This evolution necessitates a proactive approach from cybersecurity professionals to stay ahead of these advanced threats

Spikes in Third-Party Data Breaches

The frequency and severity of data breaches are expected to rise, particularly targeting major tech companies with vast customer data. This trend underscores the importance of robust third-party risk management and strategic cybersecurity planning

Greater Integration of AI in Cyber Defence

Organisations will increasingly rely on AI to bolster their cybersecurity measures. AI-powered threat detection, predictive analytics, and automated incident response systems will play crucial roles in identifying and mitigating threats in real time

The Attackers Persepctive

AI for Cyber Attack:

The Attacker's Perspective

Sophisticated Phishing Campaigns

AI has dramatically improved the effectiveness of phishing campaigns and as Phishing accounts for 22% of all cyber attacks, organisations need to be prepared to tackle them.

By using AI, attackers can craft emails that are highly personalised to their targets, making them more convincing and tailored to their intended victims.

It is getting increasingly difficult to spot these malicious emails especially those looking like an internal email asking you to take urgent action with details that only an insider would know of.

This level of sophistication is achieved by AI analysing vast amounts of data from social media profiles, corporate information, and even previous communications; which would have taken months to obtain and review.

In 2023, phishing attacks in the UK surged by 58.2%, largely-driven by AI-generated phishing emails. These emails often bypass traditional security measures because they appear so authentic. The financial sector has been particularly hard hit, with a 393% increase in phishing attempts.

What It Is:
Sophisticated phishing campaigns use AI to craft highly personalised and convincing spear-phishing emails that mimic genuine communications from trusted sources. These emails are designed to trick recipients into revealing sensitive information or performing actions that compromise security.

What It Does:
AI analyses vast amounts of data, including social media profiles, corporate information, and past communications, to tailor phishing emails that are almost indistinguishable from legitimate ones. This increases the likelihood of successful deception, making traditional email security measures less effective.

AI for Cyber Attack:

The Attacker's Perspective

Deep Fake Technologies

Deepfake technology has become a formidable tool in the hands of cybercriminals. These AI-generated videos and audio recordings can convincingly mimic real people, making it possible for attackers to impersonate executives or other high-profile individuals.

Imagine this scenario: you receive a call from what sounds exactly like your company's CEO, instructing you to transfer funds for an urgent project. The voice is unmistakably your CEO. What do you do?

In a notable 2023 incident, a UK energy firm fell victim to a deepfake attack. Employees received a phone call from what they believed was their CEO, instructing them to transfer £200,000 to a fraudulent account. This attack highlighted the chilling potential of deepfake technology to deceive even the most vigilant employees

What It Is:
Deep Fake technology uses advanced artificial intelligence to create realistic digital content, such as videos and audio recordings, that convincingly mimic the appearance or voice of real people.

What It Does:
Deep Fake Technology analyses extensive data sets of video and audio recordings to synthesise new content. It can replicate facial expressions, speech patterns, and other human characteristics with high accuracy, creating videos and audio that seem genuine.

AI for Cyber Attack:

The Attacker's Perspective

Automated Malware

AI-enabled malware represents a significant evolution in cyber threats. This type of malware can learn from its environment and adapt its behaviour to avoid detection by security systems. Imagine a piece of ransomware that changes its code and behaviour every time it encounters a new security measure, making it nearly impossible to detect and neutralise.

In 2022, a UK healthcare provider experienced an AI-driven ransomware attack that caused operational disruptions for several days. Despite robust antivirus software, the malware's adaptive nature allowed it to evade detection. The attack resulted in over £500,000 in damages, affecting critical healthcare services and patient data.

What It Is:

Automated malware refers to malicious software that uses AI to adapt and modify its behavior to avoid detection by security systems. This type of malware can change its code, signatures, and behavior in response to the environment it encounters.

What It Does:

AI-enabled malware can autonomously learn from its environment and adjust its tactics to evade detection tools like antivirus programs. This makes it more resilient and harder to detect and remove, allowing it to cause more damage over time.

AI for Cyber Attack:
The Attacker's Perspective

Supply Chain Attacks

Supply chains can act as a gateway for cyber criminals, allowing them to gain access to larger organisations by infiltrating weak links in their supply chain. Most notably, attackers have been targeting software tools used to manage the supply chain.

AI is increasingly being used to infiltrate these software supply chains, posing a significant threat to organisations that rely on third-party software. Attackers use AI to identify vulnerabilities in widely used software packages, injecting malicious code that can propagate through legitimate updates.

In 2023, a major breach involving a UK-based software company affected thousands of organisations across various sectors, including finance and healthcare. Attackers used AI to insert malicious code into a popular software package, which was then distributed through official updates. The breach resulted in an estimated £1.2 million in damages, highlighting the critical need for robust security measures throughout the software development lifecycle

What It Is:

Supply chain attacks target the complex network of suppliers and vendors that organisations rely on, aiming to compromise security by infiltrating systems or inserting malicious software into trusted software or hardware components. These attacks exploit the interconnectedness of supply chains to bypass traditional security measures and gain unauthorised access to sensitive data or systems.

What It Does:

Supply chain attacks leverage vulnerabilities in third-party suppliers to inject malicious code or tamper with products before they reach their intended target. By compromising trusted vendors, attackers can infiltrate multiple organisations, spread malware, or exfiltrate data through seemingly legitimate channels.

The Defenders Perspective

AI for Cyber Attack:
The Defender's Perspective

Threat Detection and Response

As dangerous as AI can be in the hands of the wrong person, it can also be a powerful tool when defending your organisation. Many security teams are harnessing AI within their defence strategy, utilising its ability to analyse vast amounts of data in real-time, using machine learning models that continuously improve their accuracy and speed in detecting malicious activities.

AI has the ability to continuously monitor and detect an unusual pattern of network traffic, isolating this traffic and threat before it causes any damage.

The NHS for example has implemented AI-driven threat detection systems that monitor network traffic for unusual patterns. In 2023, these systems detected a sophisticated ransomware attempt within minutes, allowing the IT team to isolate the affected systems and prevent a widespread outbreak. This proactive approach saved the NHS an estimated £2 million in potential damages.

What It Is:
AI-powered threat detection and response systems use machine learning models to monitor and analyse network traffic, detect anomalies, and respond to potential threats in real time.

What It Does:
These systems continuously learn from new data to improve their detection capabilities. They can identify unusual patterns in network traffic, flag potential threats, and automatically initiate response protocols to isolate and neutralize attacks before they cause significant harm.

AI for Cyber Attack:
The Defender's Perspective

Predictive Analytics

Predictive analytics uses AI to analyse historical data and identify patterns that indicate potential future threats. This proactive approach helps organisations anticipate and prevent attacks before they occur. AI is especially good at analysing huge quantities of data to predict the next cyber attack based on patterns from previous incidents, allowing you to fortify your defences accordingly.

A leading UK financial services company utilised AI-driven predictive analytics to identify potential vulnerabilities in their network. By analysing past incidents and threat patterns, the AI system predicted possible attack vectors and recommended preventive measures.

This approach significantly reduced the company's risk profile and potentially saved millions in avoided breaches

What It Is:

Predictive analytics in cybersecurity involves using AI to analyze historical data and identify patterns that indicate potential future threats. This proactive approach helps organisations anticipate and prevent attacks.

What It Does:

AI models predict possible attack vectors by analyzing past incidents and threat patterns. They provide actionable insights and recommendations for strengthening security measures, thereby reducing the risk of future breaches.

AI for Cyber Attack:
The Defender's Perspective

Automated Incident Response

AI automates many aspects of incident response, from initial threat detection to containment and remediation. Automated playbooks enable swift and consistent responses to security incidents, minimising damage and reducing recovery time.

When you map out your cybersecurity responses and playbooks, AI is then able to deliver the actions and automatically activate countermeasures during a DDoS attack, maintaining service continuity.

In 2023, a major UK retail chain implemented AI-driven incident response systems during a DDoS attack. The AI system automatically activated countermeasures such as traffic filtering and server load balancing, maintaining online services and mitigating the impact on customers. This rapid response saved the company an estimated £1.5 million in potential losses.

What It Is:
Automated incident response systems use AI to handle the detection, containment, and remediation of security incidents. These systems can execute pre-defined response playbooks automatically when a threat is detected.

What It Does:
By automating the response process, these systems ensure swift and consistent actions are taken to mitigate threats, minimizing damage and reducing recovery time. This helps maintain service continuity during attacks.

AI for Cyber Attack:
The Defender's Perspective

Enhancing Human Capabilities

AI augments the capabilities of cybersecurity professionals by providing actionable insights and automating routine tasks. This empowerment allows human experts to focus on more complex and strategic aspects of cybersecurity.

utilising AI, can help analysts decode complex scripts and commands used by advanced persistent threats (APTs), allowing them to concentrate on developing robust defensive strategies.

The UK Ministry of Defence employs AI tools to assist analysts in decoding complex scripts and commands used by APTs. These tools significantly reduce the time and effort required for threat analysis, increasing efficiency by 40% and improving overall security posture.

What It Is:
AI tools enhance the capabilities of cybersecurity professionals by providing actionable insights, automating routine tasks, and assisting with complex analyses.

What It Does:
AI supports human analysts by decoding complex scripts, identifying threat patterns, and providing recommendations for defensive strategies. This allows cybersecurity experts to focus on more strategic and high-priority tasks, improving overall efficiency and effectiveness.

How Organisations Can Use AI Technology to boost Defences

To effectively integrate AI into existing security frameworks, organisations should adopt a structured approach that includes evaluation, planning, and phased implementation.

Steps to integrate AI

1

Assessment

Evaluate current security measures and identify areas where AI can add value.

2

Pilot Projects

Implement AI solutions in specific areas to test their effectiveness and gather feedback.

3

Scalability

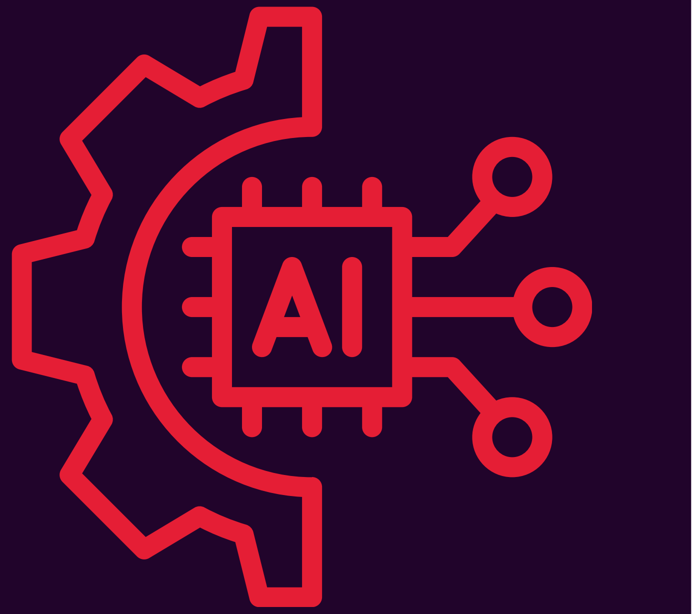
Gradually expand AI implementation across the organisation based on pilot results.

4

Continuous Improvement

Regularly update AI models and systems to adapt to new threats and incorporate lessons learned.

Implementing AI-Driven Security Solutions



Assessment

Start with a thorough evaluation of your current security measures and identify the areas where AI can add the most value. This involves:

- Conducting a Security Audit: Review your current security infrastructure and processes to pinpoint weaknesses and gaps.
- Identifying Key Vulnerabilities: Use threat intelligence and past incident reports to identify areas that frequently encounter threats.
- Assessing AI Readiness: Determine your organisation's readiness for AI adoption in terms of existing technology, workforce skills, and data availability.

Pilot projects

Before rolling out AI across the entire organisation, implement pilot projects in specific areas to test their effectiveness. This step includes:

- Selecting Pilot Areas: Choose departments or processes where AI can make a significant impact with minimal risk.
- Setting Clear Objectives: Define what success looks like for your pilot projects, including specific metrics and KPIs.
- Gathering Feedback: Collect data and feedback from these pilot projects to understand the performance of AI solutions and make necessary adjustments.

Scalability

Based on the success of your pilot projects, gradually expand AI implementation across the organisation. This step involves:

- Creating a Scalable Framework: Develop a framework that supports the seamless integration of AI solutions across different departments.
- Training and Development: Ensure that your workforce is adequately trained to work with AI technologies. Provide continuous learning opportunities to keep skills up-to-date.
- Monitoring and Evaluation: Continuously monitor the performance of AI systems as they are scaled up, ensuring they meet the defined objectives and adapt to new challenges.

Continous Improvement

AI systems need regular updates and improvements to stay effective against evolving threats. This involves:

- Regular Audits: Conduct frequent audits to assess the performance of AI systems and identify any areas needing improvement.
- Incorporating Feedback: Use feedback from end-users and performance metrics to refine AI models.
- Staying Updated: Keep abreast of the latest developments in AI and cybersecurity to ensure your systems are always at the cutting edge.

Considerations

Training and Awareness Programs

Educating employees about AI-driven threats and defensive strategies is crucial for maintaining robust cybersecurity.

For instance, a UK insurance firm launched an extensive training program focusing on AI-generated phishing emails and deepfakes. Regular workshops and simulations helped staff recognise and respond to these sophisticated threats, significantly reducing the incidence of successful attacks.

It’s essential that these programs are ongoing and adapt to emerging threats, ensuring that all employees remain vigilant and informed.

Regular Audits and Updates

Continuous improvement of AI models is essential to keep up with the evolving threat landscape. Regular audits and updates ensure that AI systems remain effective and capable of countering new attack vectors. For example, a leading UK telecom provider conducts quarterly audits of their AI-driven security systems.

These audits review the performance of AI models, identify any gaps or areas for improvement, and implement updates to enhance the system's capabilities. Regular maintenance and iterative improvements are key to maintaining the relevance and effectiveness of AI in cybersecurity.

Collaborative Defence Strategies

Sharing intelligence and strategies within the industry enhances collective security. Collaborative efforts allow organisations to stay informed about emerging threats and develop coordinated responses. The UK Cyber Security Information Sharing Partnership (CiSP) is an excellent example, facilitating collaboration between public and private sectors.

By sharing threat intelligence and best practices, members can collectively improve their cybersecurity defences and respond more effectively to incidents. This kind of collaboration fosters a community-driven approach to cybersecurity, leveraging collective knowledge and resources to combat threats more effectively.

Considerations

Preparation and Background Work

Organisations should assess their current preparations and investments in AI-driven cybersecurity. Reviewing results and feedback from initial deployments helps in refining strategies and maximising the benefits of AI in security operations. For example, a UK-based multinational conducted a comprehensive review of its AI-driven security initiatives.

The findings highlighted areas of success and opportunities for improvement, leading to the implementation of more effective AI strategies and tools. Regular assessments and iterative improvements ensure that AI solutions continue to evolve and meet the organisation's security needs.

Impact of AI on Cybersecurity Skills Gap

AI tools can help address the shortage of cybersecurity professionals by automating routine tasks and augmenting human capabilities. This allows existing staff to focus on high-priority issues, effectively bridging the skills gap. For instance, a UK government agency implemented AI tools to automate the analysis of security alerts.

This reduced the workload on human analysts, allowing them to concentrate on complex investigations and strategic planning, thereby enhancing the overall efficiency of the cybersecurity team. By automating mundane tasks, AI not only boosts productivity but also helps in retaining talent by allowing professionals to engage in more challenging and rewarding work.

Policy and Regulatory Support

Government and industry regulations play a critical role in supporting the integration of AI in cybersecurity. Adhering to these regulations ensures that AI systems are implemented responsibly and ethically, protecting both organisations and their customers.

The UK government has introduced guidelines and regulations to support the safe and ethical use of AI in cybersecurity. These regulations ensure that AI technologies are used responsibly, safeguarding personal data and protecting against misuse. Organisations must stay informed about these regulations and ensure their AI implementations comply with all legal and ethical standards.

About FourNet

FourNet works with some of the most secure, critical and commercially driven organisations in the UK.

Our expertise is in transitioning and integrating complex, legacy systems to deliver the latest communication, collaboration, and contact centre capabilities.

We provide the knowledge and technical expertise to help our customers achieve their digital transformation and customer experience goals. FourNet's Intelligent Managed Service frees up time for our customers to focus on running their business, without having to worry about their communications infrastructure.

Our Infrastructure Partners

CISCO Partner
Gold Provider

Extreme networks
DIAMOND PARTNER

ENGAGE
FORTINET EXPERT PARTNER

Easy To Procure

Crown Commercial Service
Supplier

pfh Nominated Supplier

CYSYLLTU CYMRU CONNECTING WALES
Cwsmer – Cysylltu – Cydweithio
Customer – Contact – Collaborate

HM Government
G-Cloud
Supplier

Scottish Government
Riaghaltas na h-Alba
gov.scot

Crescent Purchasing Consortium

Achilles
UVDB
QUALIFIED

How we can Help

FourNet®

FourNet Assess

Organisations need to understand cyber risks and their ability to handle and manage a cyber attack. Our consultative approach creates a benchmark of your current security strengths and weaknesses. This allows us to prioritise areas for attention in line with organisational goals and priorities overlayed with risk analysis. Approaching cybersecurity not just as technical issue, our methodology revolves around three key elements, people, process and technology.

FourNet Protect

FourNet Protect provides next generation security services including mail protection, advanced Endpoint Detection and Response (EDR) and Security Access Service Edge (SASE) to protect applications and services. Wherever the network is accessed, and however the perimeter moves, FourNet Protect ensures users are safe and secure.

FourNet Defend

No matter what technology solutions are in place an attacker only needs to be successful once to compromise the network and organisation. With FourNet Defend our team of experienced cybersecurity professionals work in unison with internal teams, utilising advanced tools and methodologies to swiftly detect, analyse, and mitigate threats.

Defence in Depth

Defence in depth is essential in cybersecurity as it provides multiple layers of protection, reducing the risk of breaches if one layer is compromised. In the UK, where cyber threats are constantly evolving, this layered approach helps organisations detect and respond to attacks more effectively, minimising the impact on business continuity and national security. By combining controls like firewalls, encryption, and access management, defence in depth strengthens overall resilience, fostering greater trust in systems and services.

Delivering a Zero Trust Strategy

In today's threat landscape, traditional perimeter-based security is no longer sufficient. Zero Trust is a security model that assumes no trust and requires continuous verification of all entities. This approach significantly reduces the risk of breaches, ensuring robust protection for your sensitive data and systems.

Discover more about ZTNA in our quick guide to Zero Trust

Download Here >>

FourNet®

Thank you

Discover how we can help you achieve goals and outcomes.

Get in touch

0845 055 6366
hello@fournet.co.uk
fournet.co.uk