Report

Cyber security in the age of offensive AI

NETACEA

Contents

03 Foreword

04 Research overview

05 What is offensive AI?

06 How are attackers manipulating AI to their advantage?

07 83% of businesses reported they have no plan to adopt AI

09 Expectation vs. reality

11 Doing more, with less

13 Are security leaders ready to defend against offensive AI?

15 AI is creating a new generation of attacks

16 Take action against offensive AI

Foreword

Andy Still

CTO & Co-Founder, Netacea

As open artificial intelligence (AI) tools become more accessible, and the barrier to entry to cyber-attacks is lowered, it is crucial that businesses understand the significance of the technology and how it can be harnessed for both offensive and defensive means.

AI elevates the capabilities of cyber-attacks beyond fast and effective execution, to a new breed of cyber threat that can be trained to find and exploit software vulnerabilities, evade intrusion detection and even mimic human behavior. Stopping AI-driven attacks requires a fresh take on defensive strategies, with greater onus on processing large volumes of data to effectively detect patterns in user behavior.

Our research reveals that 93% of respondents believe that they will face daily AI attacks within the next 6 months, with the volume of AI attacks expected to increase in size and scale. And yet, adoption of AI is not universal across the security stack but weighted in favor of protection against high impact attacks such as ransomware and DDoS, vs. bot attacks.

We want to help CISOs and security leaders determine their greatest challenges and pressures in their approach to tackling offensive AI, while providing insights into the future of AI attacks from cyber-threat experts.

Research overview

Summary findings

Netacea spoke with 440 businesses across the UK and US to gauge how well understood the threat of AI-driven cyber-attacks are within enterprise organizations, and assess their readiness to defend against these attacks.

- 440 enterprises
- $1.9bn average online revenue
- 5 sectors

65%

of enterprises believe that offensive AI will become the norm

100%

reported an improvement across their security stack since deploying AI

61%

of security leaders stated that AI has reduced their operational overheads

What is offensive AI?

The term 'artificial intelligence', or AI, has had dangerous connotations since Hollywood made it something to fear in films like 2001: A Space Odyssey (1968) and The Terminator (1984). Subsequent advances in technology at the dawn of the new millennium have only added fuel to the fire. Aside from robots set on destroying the human race, how much do we understand about AI and crucially, how do we define AI in 2024?

Over the last decade the cyber security industry has played a role in devaluing the term with overuse without substantiation. 'AI' was deemed a buzzword that sought to bamboozle buyers into purchasing technology without truly understanding what role AI played in enhancing the product's capabilities, or, if it even utilized AI at all.

The relatively recent arrival of generative AI to the mainstream, spearheaded by OpenAI's ChatGPT, has resulted in a resurgence of interest in the technology and a fresh take on its use to both execute cyber-attacks, and defend against them. But how does this fit with our understanding of AI in the traditional sense?

> "Five years ago, AI was a buzzword used by a lot of businesses across a range of products. What they were actually delivering wasn't AI. It was heuristics and data analysis.
>
> "Since then, the underlying tech has advanced and become easily available to most people. Products that now say they are AI, are genuinely AI and apply it in a way that adds true value."
>
> Andy Still
> CTO and co-founder at Netacea

How are attackers manipulating AI to their advantage?

AI lowers the barrier to entry for anyone who wants to carry out a malicious attack on a business or individual. The skill previously required to carry out an attack has been removed, increased capability put in the hands of a would-be attacker and the opportunity for a successful attack instantly improved.

Not only is AI accessible and affordable, but those who want to carry out an attack don't even need to know how to use the technology themselves. The growing market for AI as a Service makes it exceedingly simple for anyone to harness the advantages of AI to execute attacks with increased versatility, efficiency and speed.

Attackers are using AI to identify patterns in security postures and devise bypassing strategies, culminating in sophisticated AI-powered social engineering attacks such as deep fakes that exploit voice and facial recognition, as well as our own tendency to trust other "humans". In this scenario it's clear that AI has been used to carry out the attack and manipulate the target. That isn't always the case.

Consider AI-powered web scraping attacks. On the surface this traffic is indistinguishable from regular web scraping traffic, but the attack has been executed faster and with far greater ease. The simplicity of such attacks makes them repeatable and accessible.
AI even allows attackers to source the optimal combination of residential proxy combinations, at the lowest cost, to further avoid detection.

"AI is a means to an end. The attacker has an objective and will use any and all tools available to achieve it as quickly and cheaply as possible.

"However, we are still in the test and learn phase. And yes, that applies to both the attackers and the defenders. As attackers become more confident, and proven use cases emerge, we can expect an explosion of offensive AI. That will require a reciprocal explosion in defensive AI."

Cyril Noel-Tagoe
Principal Security Researcher at Netacea

The majority of businesses reported they have no plan to adopt AI

According to a 2023 report from the Office of National Statistics, 83% of businesses stated they have no plan to adopt AI as they head into 2024.[1]

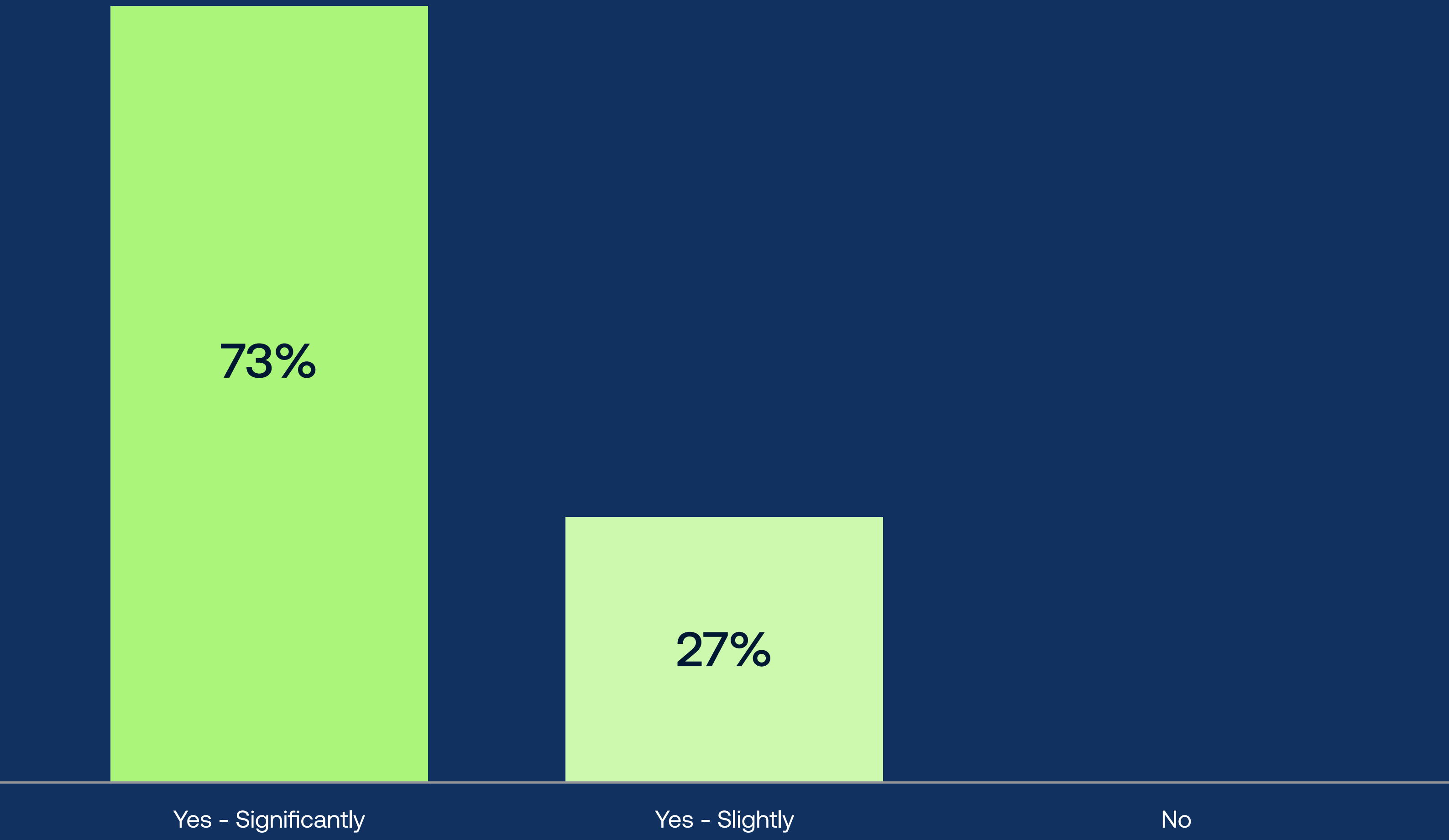
The report surveyed 10,000 responses from UK businesses, ranging in size from small to large enterprises. Small businesses (those with fewer than 250 employees) are least able to adopt AI, despite the UK government pouring £32m into funding businesses seeking to expand their AI initiatives and remove the financial blocker.

Meanwhile, large organizations with greater resources and AI literacy are busily identifying beneficial applications.

This aligns with Netacea's findings, which revealed that 100% of enterprises have incorporated AI within their security stack to some degree, and 100% have experienced improved efficacy.

Has the efficacy of your WAAP posture improved since deploying AI solutions?

Fig. 1



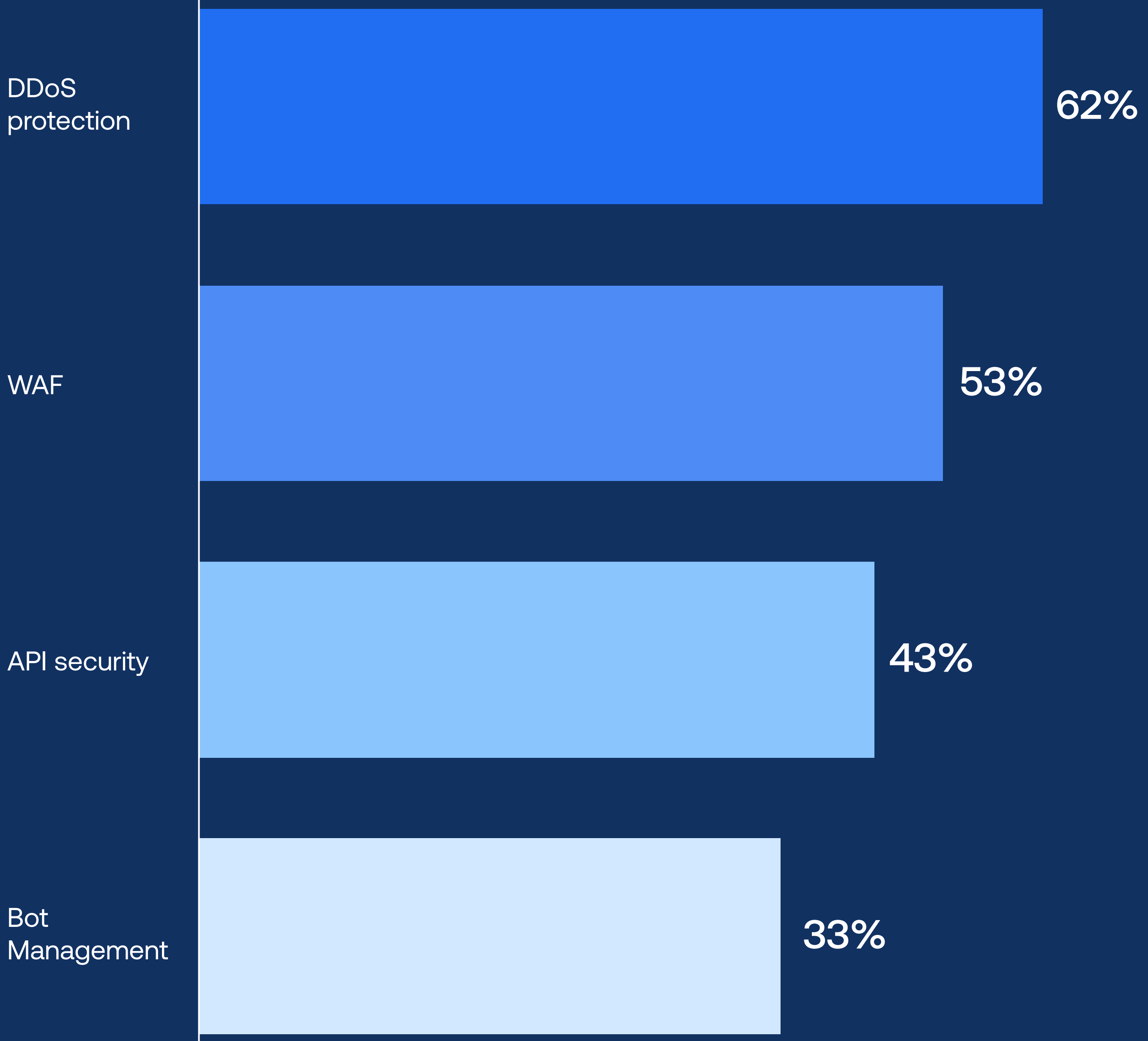
[1] ITPro.com, 2023 – 83% of UK organizations have no plan to use AI any time soon, but why?

However, adoption is not yet universal, but weighted towards high impact attack protection, such as DDoS, vs. investment in defenses against bot attacks, which currently lags.

Patterns in adoption are indicative of the ever-increasing pressure faced by CISOs to tackle the threats to their business, with ever-decreasing resources. Even in large enterprises, holistic adoption of AI across the security stack seems to be out of reach.

Which of your Web Application and API Protection (WAAP) solutions utilize AI?

Fig. 2



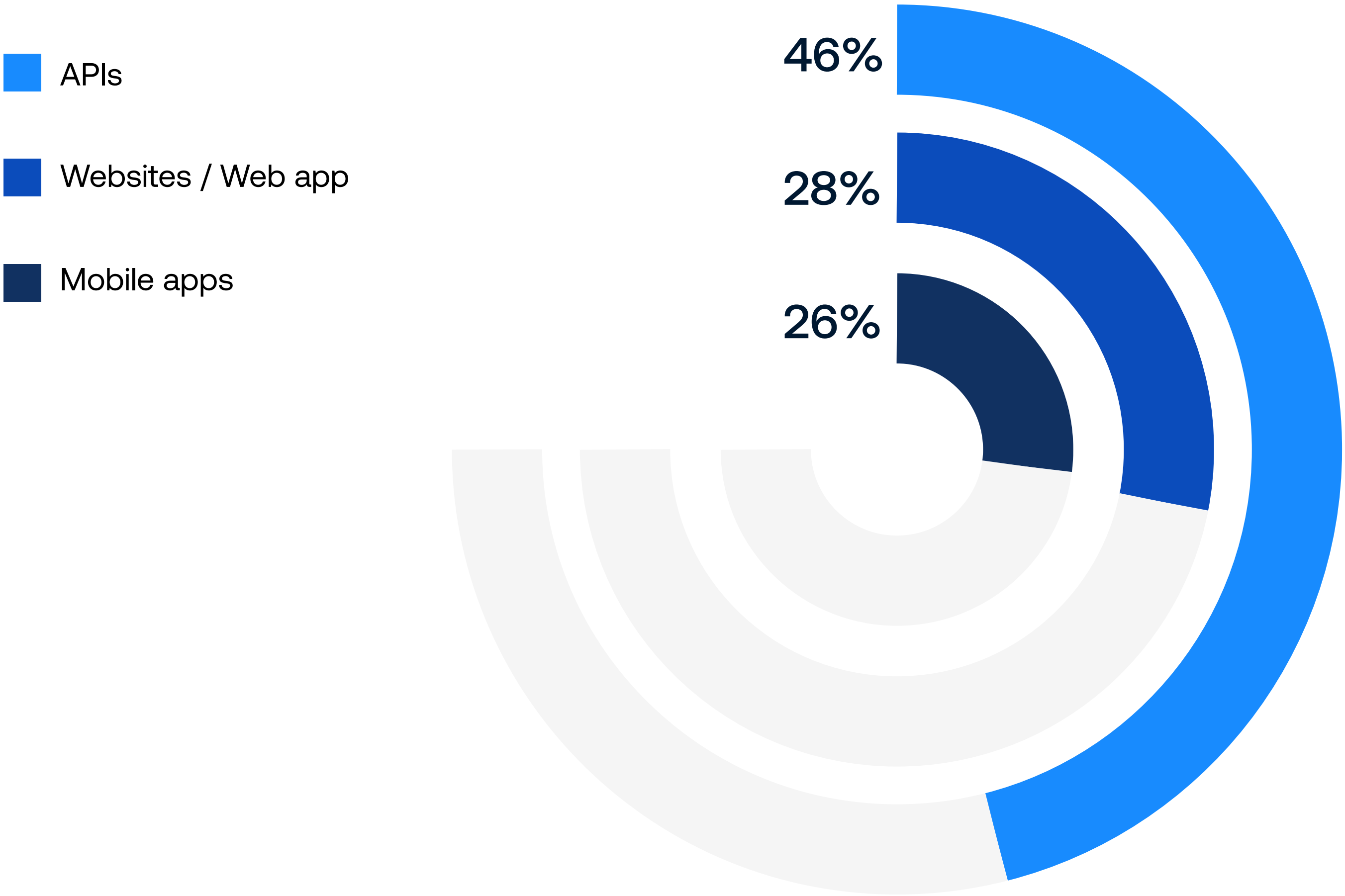
Expectation vs. reality

Security leaders have a challenge. To effectively defend their business, while channeling limited funds and resources in the right direction, they must equip themselves – and their board – with accurate, trusted data that reflects the current nature of the threat landscape. This starts with correcting fundamental discrepancies between the expectation and reality of the attack surface.

46% of businesses believe their API is the most secure vector, but this is a fallacy. All surfaces are attacked equally. We can speculate that this is due to the belief that API security is particularly robust, while in fact Netacea's 2023 report[2] revealed that 40% of organizations experienced API attacks in 2022, and attacks targeting mobile apps exceeded those targeting websites for the first time.

Which area of your business/attack vector do you feel is most secure?

Fig.3



[2] Netacea, 2023 – Death by a Billion Bots

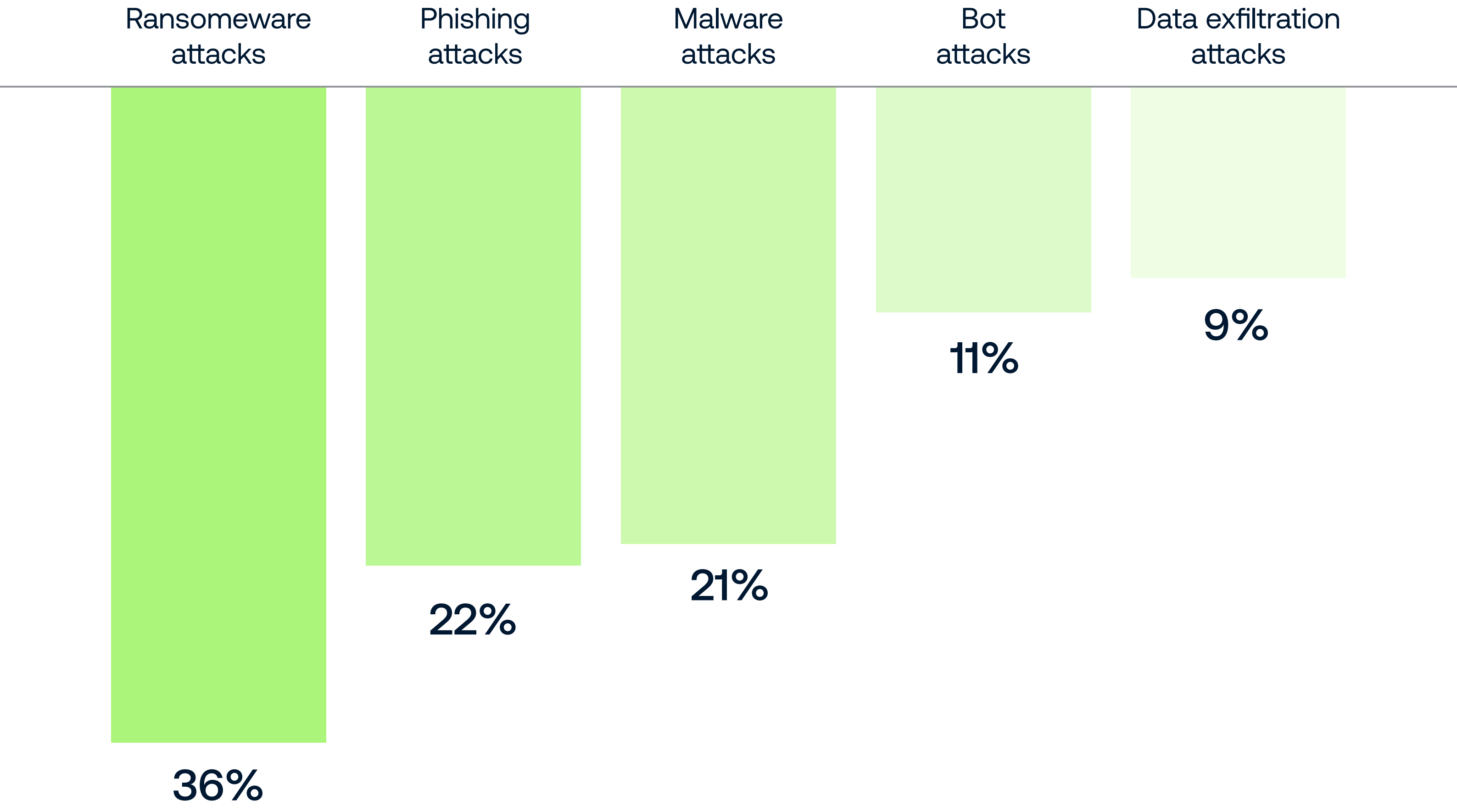
Businesses underestimate bot attacks

False perceptions reach beyond the attack surface, to attack type.

Just 11% believe that bot attacks will be the greatest cyber threat to their business in the next six months, vs. 36% who believe it will be a ransomware attack. A ransomware attack is an indisputably catastrophic event for any business, but we cannot underestimate the seismic impact of a steady stream of bot attacks over a sustained period.

What do you believe is the greatest cyber threat facing your business in the next six months?

Fig. 4



In Netacea's 2023 survey, enterprises reported that bots cost on average **4.3%** of their online revenue. For organizations exceeding $250m in revenue, that equates to $85.6m, which is more than fifty average ransomware payouts, or the eighth highest ever GDPR fine – every single year.

Doing more, with less

The pressure is on to do more, with less. The greatest challenge for CISOs is the effort they must put into alerts, and AI helps them make decisions. Or not need to make decisions at all.

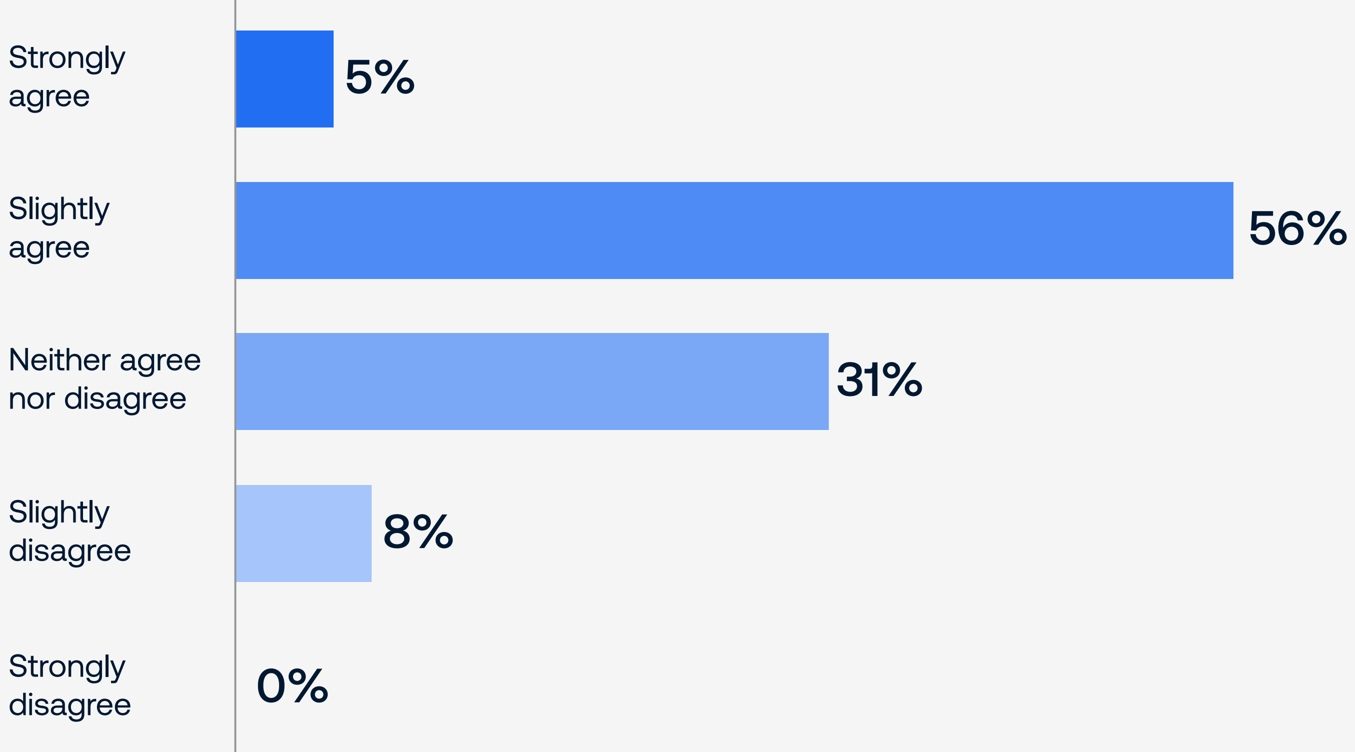
The responsibility shifts across to the automated process. While there is always a risk that this could go wrong, it must be treated like any other system; an appropriate amount of human validation is required.

A security leader becomes like a conductor of the orchestra. They make fewer decisions themselves but must ensure that every musician is playing in time. In other words, you need accurate data to trust that the application – or musician – will make the right decisions or play the right notes.

There is already evidence that AI-powered automation is having a positive impact that directly benefits CISOs, with 61% of people agreeing that AI has significantly decreased operational overheads.

To what extent do you agree or disagree with the following statement? 'Since deploying AI solutions, my business has significantly reduced its operational overhead.'

Fig. 5



“If we assume that people are happy with the technology that they have in place, then they won’t seek to change it. Once existing solutions become less able to protect against changing attacks, and attackers are able to bypass existing tools, buyers will turn to alternatives such as defensive AI.

“But should it take getting to this point to drive adoption? How can we create a more proactive approach to adopting effective technology?”

Cyril Noel-Tagoe

Principal Security Researcher at Netacea

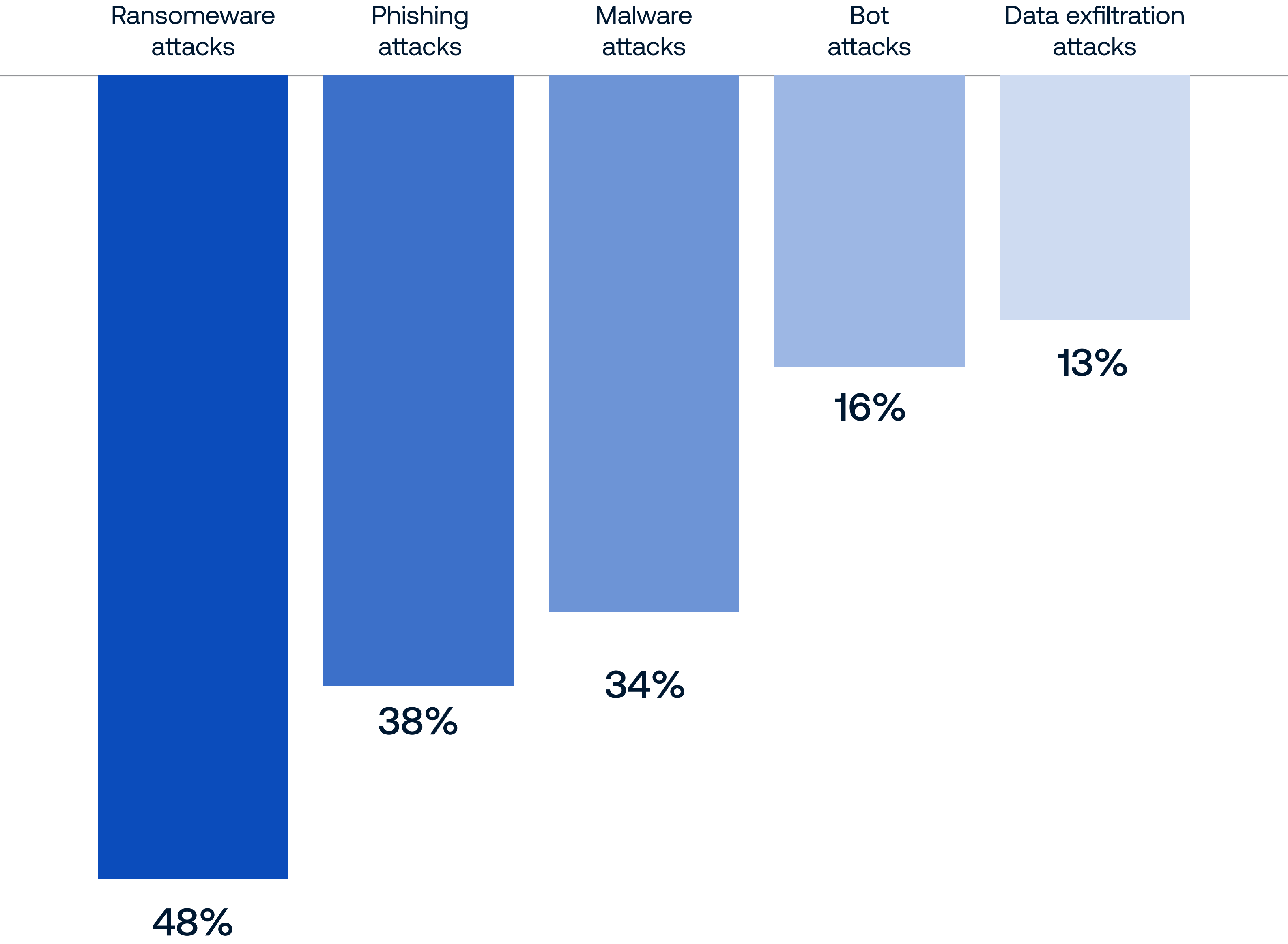
Are security leaders ready to defend against offensive AI?

93% of businesses believe that they will face daily AI attacks in the next year, with their predictions split across different attack types.

- **48%** of CISOs are afraid of AI-powered ransomware attacks
- **38%** believe that phishing attacks will be powered by AI
- **16%** stated that bot attacks will be driven by AI

What type of attacks will be powered by AI?

Fig 6



Offensive AI is on the radar, but is defensive AI a priority?

90% of respondents said they are confident in the defensive AI capabilities of perimeter defenses such as WAF, DDoS and API security, but just 60% of security leaders felt the same about bot management.

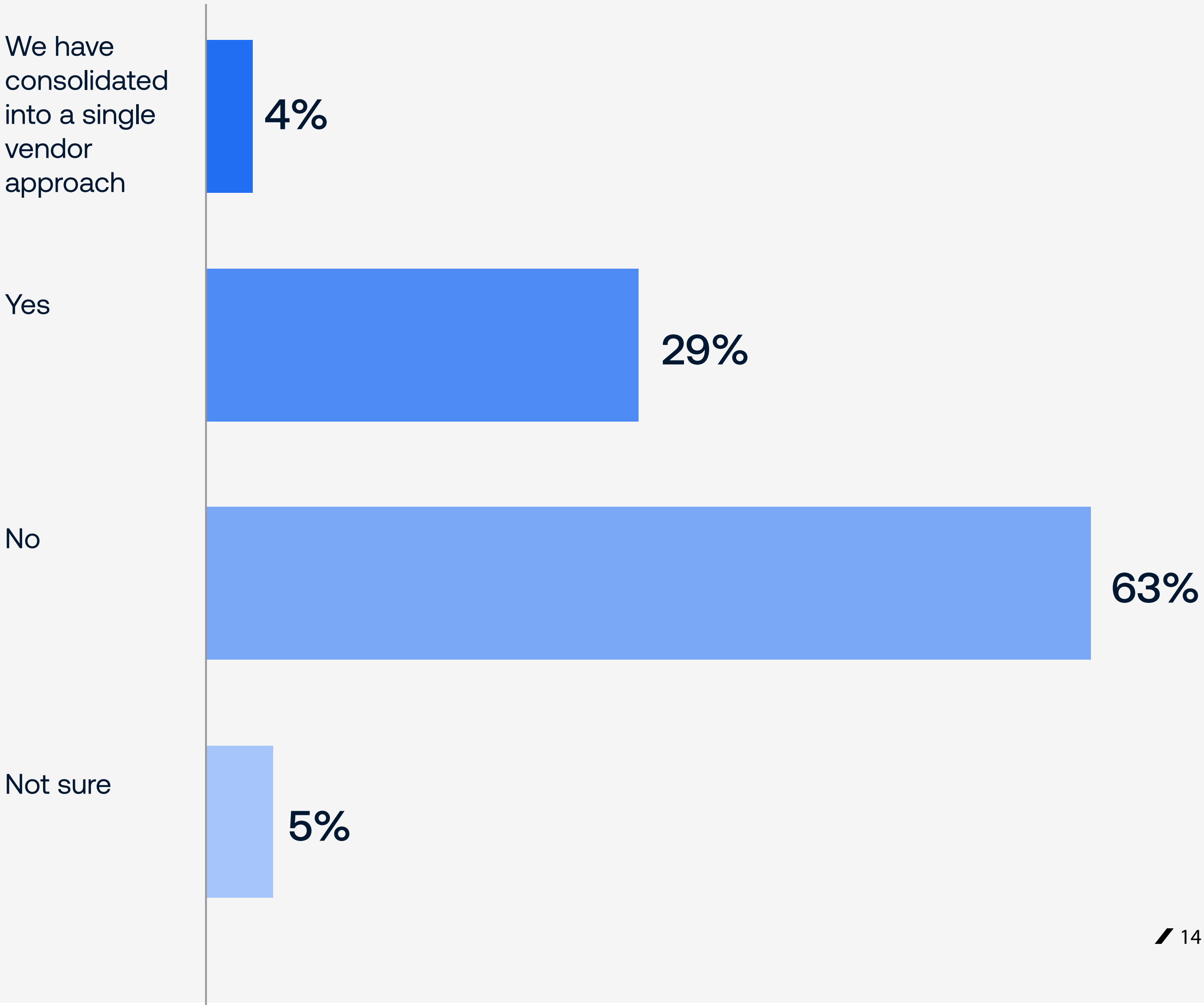
Once again, we come back to a clear favoring of high-impact attacks, that aligns with our understanding of where enterprises already have AI in place, with more utilizing AI in DDoS, WAF and API security than bot management (fig. 2).

This may be due to the tendency for CISOs to seek a single vendor approach to their security posture, with 33% having or planning to consolidate specialized solutions. Are these the businesses that already have AI within their stack? Is it due to an automatic bundling of security solutions, rather than a particular preference for a defensive tool? And are these bundled solutions equipped to tackle sophisticated AI attacks?

There is a call for specialized solutions that are equipped to handle offensive AI, and this is reflected in the data with 63% of respondents revealing a preference for trusted specialist solutions.

Are you planning to consolidate specialized solutions into a single vendor approach?

Fig. 7



AI is creating a new generation of attacks

The results suggest that security leaders understand the significance of offensive AI and expect the next six months to issue the dawn of a new generation of cyber security attacks.

Poor in time and burdened with a pressure to secure their organization against both known threats and those that are yet to rear their heads, security leaders are tasked with making sure offensive AI has a place in board level discussions, alongside high impact attacks such as ransomware and DDoS.

Leaders must address the scale of the problem, with AI's vast potential to exploit a business's vulnerabilities with greater accuracy and frequency than ever before, while keeping costs to a minimum. Yet all is not lost, while AI presents fresh opportunities to wreak havoc, AI offers security leaders their own profound advantages.

This report proves that CISOs are already benefiting from the deployment of AI in the security stack. All respondents agree that AI has improved the efficacy of their WAAP posture, and a majority state that AI has reduced operational overheads.

The ball sits firmly in the court of the security leader. Defense-in-depth in the environment of the unknown and unforeseen requires the holistic adoption of AI-driven technology across their security suite, to look beyond high impact attacks and to sophisticated attacks that have a slow but devastating effect on the bottom-line.

Security leaders must arm their businesses with a proactive approach to offensive AI, with defensive AI at its core.

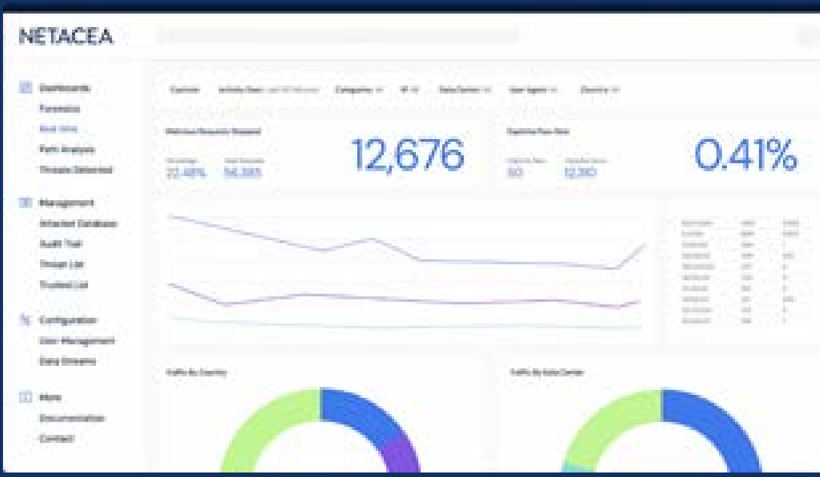
Discover automated bot protection from Netacea

Netacea has helped hundreds of enterprise security teams protect against sophisticated bot threats and large-scale automated attacks, before they even happen.

- Analyze all traffic and block 33x more bots with an unmatched 0.001% false positive rate.
- Automated, defensive AI performs real-time detection and response for websites, applications and APIs.
- Invisible to attackers and tough to bypass, Netacea stops the most sophisticated threats.

Book a demo today

Award winning bot protection software. Performs at scale. Trusted by enterprise.



LUISAVIAROMA Dr. Martens atida OFFICE OFFSPRING shutterstock