FORRESTER®

The Emergence Of Offensive AI

How Companies Are Protecting Themselves Against Malicious Applications Of AI

Get started ⟶

FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY DARKTRACE | FEBRUARY 2020

Offensive AI Is Creating New Threats

In recent years, an onslaught of new cyberattacks and tactics has threatened organizations globally. Most cybersecurity decision makers foresee adversaries modifying their tactics to circumvent traditional/legacy security tooling and technology but also to infiltrate new areas of digitalization.

Artificial intelligence (AI) is no longer a tool only for the “good guys”; malicious actors now use it as a force multiplier as well. This new era of offensive AI leverages various forms of machine learning to supercharge cyberattacks, resulting in unpredictable, contextualized, speedier, and stealthier assaults that can cripple unprotected organizations.

In November 2019, Darktrace commissioned Forrester Consulting to evaluate the emergence of offensive AI, organizations’ current security practices, and how well prepared they are to fight off such attacks.

Key Findings

Digitalization expands firms’ surface area to more advanced attacks, causing concern for cybersecurity decision makers: 86% are concerned with threat actors leveraging AI to supercharge attacks.

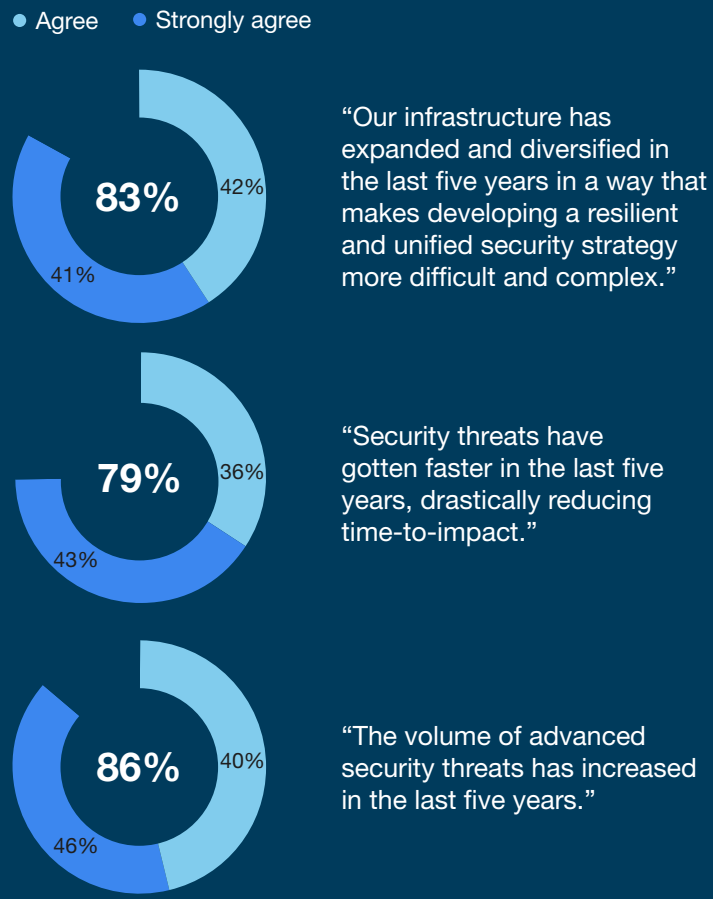
Firms are slow to respond to offensive AI attacks. Reliance on humans keeps them from quickly detecting and responding to the scale and speed of attacks, compromising business continuity, IP, and reputation.

Over 80% of respondents value tools that increase autonomous decision making and automate response actions to offset the shortcomings of human-based detection, interpretation, and response.

A Complexified Security Landscape Increases Vulnerability

Security has become more complex in the last five years. Decision makers in charge of cybersecurity tell us that: 1) their expanded infrastructure has complexified security; 2) security threats have gotten faster; and 3) advanced attacks have increased.

As organizations increase their digital capabilities across hybrid, multicloud, and internet-of-things (IoT) environments, they gain more areas to protect and control. It also enables criminals to damage operational reliability, undertake new types of crimes (like digital eavesdropping), and directly affect the running of a business. That will lead to even faster and more effective AI-powered attacks and exploits.[1] This type of offensive AI can supercharge criminal attacks through speech processing or automated lateral movement, intelligently shifting attack techniques given what it encounters in the network — without human input.



Base: 102 cybersecurity decision makers at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of Darktrace, November 2019

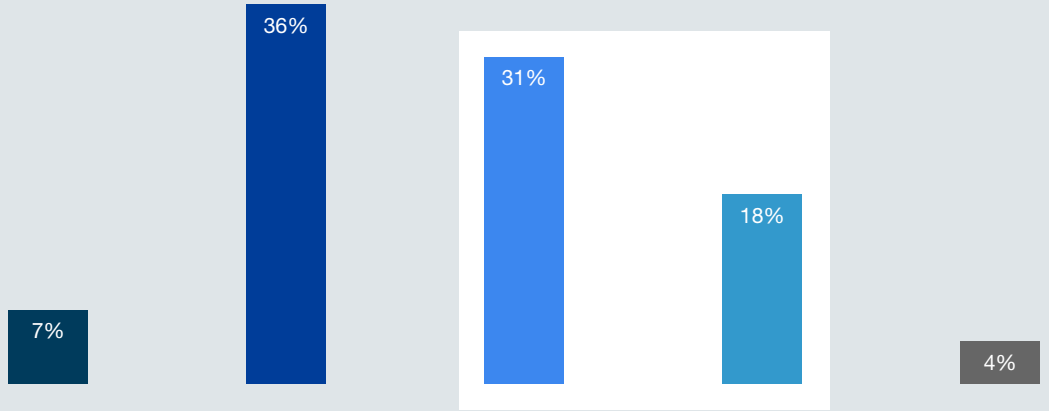
AI-Fueled Attacks Are Not Just Sci-Fi

Organizations are aware of the viability of AI-enabled attacks. Machines are already attacking machines, and humans attacking human trust — the future will include machines attacking human trust at speed and scale. Businesses aren't ready for this, and neither are consumers. Trust plays a big part in this. Forrester estimates that AI-enabled deepfakes will cost businesses a quarter of a billion dollars in losses in 2020.[2]

It's no surprise that 86% of cybersecurity decision makers are concerned with threat actors leveraging AI to supercharge attacks and a further 88% believe it's inevitable for AI-driven attacks to go mainstream. The scary future is not as far as some might think: Close to half of cybersecurity decision makers expect AI attacks to manifest themselves to the public in the next year.

"When do you think AI attacks will start manifesting themselves to the public?"

- In the next five years
- In the next three years
- In the next 12 months
- Within the next six months
- This is already happening



FORRESTER OPPORTUNITY SNAPSHOT: A CUSTOM STUDY COMMISSIONED BY DARKTRACE | FEBRUARY 2020

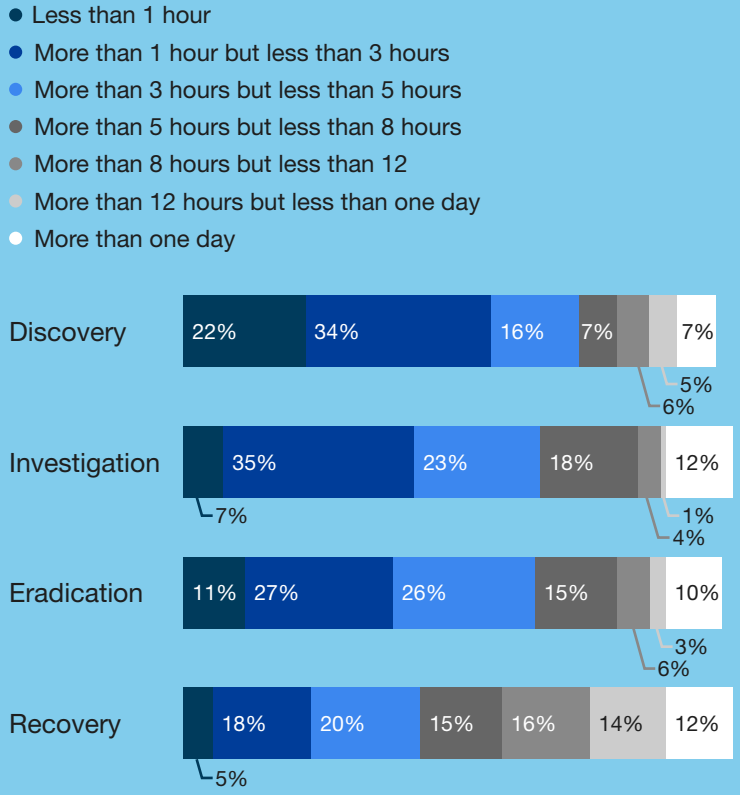
Base: 102 cybersecurity decision makers at global enterprises
Note: Not all responses shown.
Source: A commissioned study conducted by Forrester Consulting on behalf of Darktrace, November 2019

Cybercriminals' Speed Outpaces Security Teams

Traditional defenses that rely on prior assumptions will be outmatched against supercharged AI attacks. Organizations are aware of the need for speed-to-response; however, we found that they are slow to respond when they're triaging an incident across these stages:

- **Discovery.** It takes 44% more than 3 hours to become aware there's been an infection.
- **Investigation.** Close to 60% need more than 3 hours to understand the scope of the incident.
- **Eradication.** Less than 40% can remove the threat from the environment in less than 3 hours.
- **Recovery.** Less than a quarter can return to business as usual in less than 3 hours.

"On average, how long does each of these stages take your security team to triage an incident?"



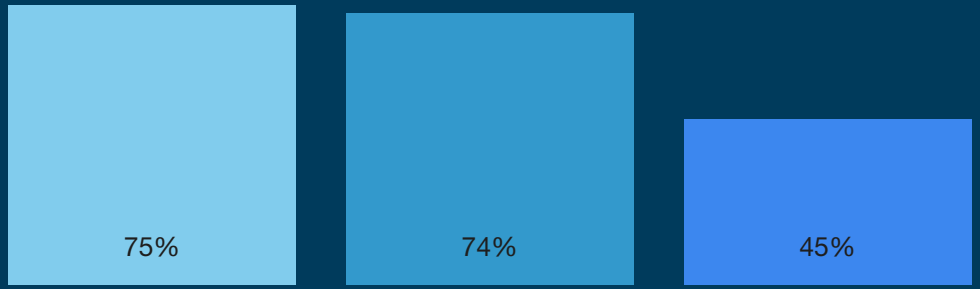
Base: Variable cybersecurity decision makers at global enterprises
Note: Percentages may not total 100 because of rounding.
Source: A commissioned study conducted by Forrester Consulting on behalf of Darktrace, November 2019

Failure To Prepare For Offensive AI Hurts Businesses

Speed-to-detect, -interpret, and -respond is the equalizer that organizations need, but their ability to do so remains mired in reliance on humans to enable those operations. As attackers modify their tactics and beat legacy security tooling, they will move deeper and more quickly into infected networks. Without faster and more autonomously enhanced analytics, organizations shift the balance of power to the attacker.

This lack of speed has serious implications. Cybersecurity decision makers are most concerned about systems or business interruption, IP or data theft, and reputational damage. Establishing automated detection and response negates the need for human-driven investigation.

"When/if weaponized AI becomes mainstream, which of the following security risks are you most concerned about?"
(Select all that apply.)

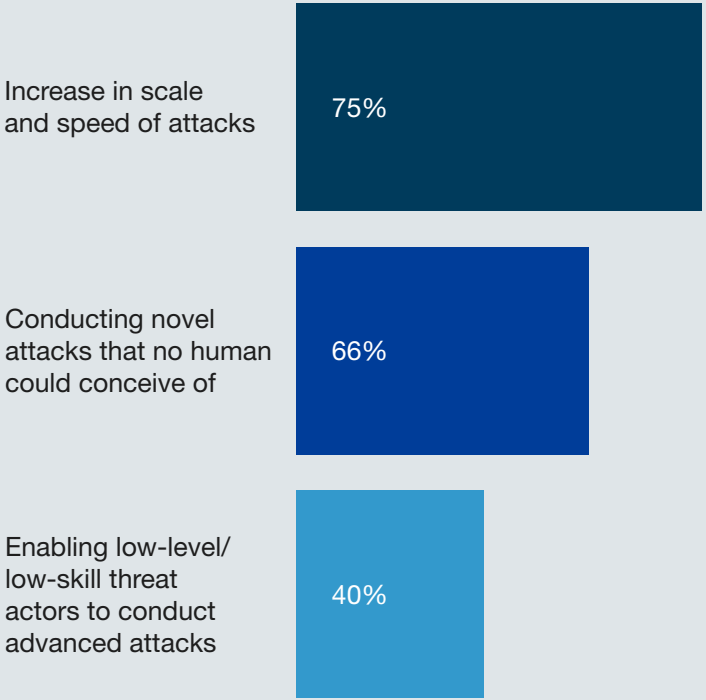


Base: 102 cybersecurity decision makers at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of Darktrace, November 2019

Traditional Security Approaches Cannot Detect Advanced AI Attacks

Close to 80% of cybersecurity decision makers anticipate offensive AI to increase the scale and speed of attacks. In addition to their quickness, 66% also expect offensive AI to conduct attacks that no human could conceive of. These attacks will be stealthy and unpredictable in a way that enables them to evade traditional security approaches that rely on rules and signatures and only reference historical attacks. In turn, this requires an approach that leverages AI defensively, where a system can continuously learn "normal" from scratch to flag the unusual activity of cyberthreats that have never been seen before.

"What do you anticipate the impact of weaponized AI to be?" (Select all that apply.)



Base: 102 cybersecurity decision makers at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of Darktrace, November 2019

Organizations Must Align Strategic Focus With AI As A Defensive Tactic

Organizations have an opportunity to drastically reduce time-to-identify, -interpret, and -respond to cyberthreats with targeted AI tooling.

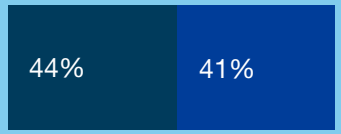
It will be crucial to use AI as a force multiplier and keep pace with attacker enhancements as they upscale their attack capabilities and efforts.

Increasing autonomous decision making and automating response actions offset the shortcomings of human-based response — too few human operators, overlooked crucial clues, and an inevitably delayed response time in the face of machine-speed threats.

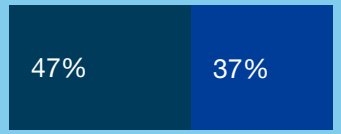
Over 80% of cybersecurity decision makers in this study agree that organizations require advanced cybersecurity defenses to combat offensive AI.

"To what extent do you agree with the following statements?" ● Agree ● Strongly agree

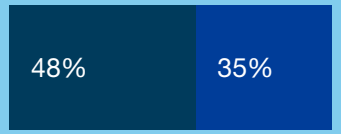
Organizations require cybersecurity defenses that provide unified coverage across the cloud, email, IoT, and corporate network to keep pace with AI-driven threats, leaving no place for attackers to hide.



Organizations require cyberdefenses that can respond with surgical precision and at machine speed to keep pace with AI-driven threats.



Organizations require AI augmentation that can adapt to shifting threat vectors, as well as reduce time-to-detection and time-to-meaning in understanding the full scope of an incident.



Base: 102 cybersecurity decision makers at global enterprises
Source: A commissioned study conducted by Forrester Consulting on behalf of Darktrace, November 2019

Beat Offensive AI With Defensive AI

Organizations need to bite the bullet and be honest about the fact that AI is just another digital capability in the ever-evolving cyber realm, and just as with every other innovation in this space, AI too will be manipulated for nefarious purposes. The real issue with this is that because AI moves faster and better than current legacy defenses, the “evil AI” will win in most instances. If an organization is not operating with AI-enabled defenses to counter AI-enabled attacks, how can it expect to win? The goal is to fight these advanced attacks with advanced tactics that detect, interpret, and respond to the threat before it has a chance to make an impact.

Conclusion

AI tooling and capabilities are no longer just the subject of science fiction, and AI is no longer just in the hands of the good guys. The reality in cybersecurity is that both the good and the bad sides of applied AI will have significant impacts on the future productivity of any organization. Organizations must leverage applied AI tooling to combat the coming threats that criminal organizations are increasingly using.

While many organizations understand the potential use cases for these types of applications of AI, most of them don't yet have the tools in place. The longer that organizations wait to leverage these powerful AI-based security applications, the more time the enemy has to bolster and research the offensive applications of similar systems. Time is not on the side of those who choose to wait; the time to implement AI-based security solutions is now.

Any useful application of an AI-based security solution needs to be applied to a narrow scope of potential outcomes. To gain the maximum benefit of the defensive capabilities that AI-based security solutions provide, organizations must be realistic and specific about what benefits they seek to gain from using these solutions. Apply AI with a focus on specific outcomes and measure the benefits gained by those systems when compared to the past human outputs of similar use cases, and you will see the benefits quickly.

AI-based security tools will help organizations move faster, secure more dynamically, and better understand and control complex hybrid infrastructures. The true benefit of these solutions is that operators boost their capacity and response times, all of which immediately benefit the organization.

Project Director:
Andia Tonner, Market Impact Senior Consultant

Contributing Research:
Forrester's Security and Risk research group

Methodology

This Opportunity Snapshot was commissioned by Darktrace. To create this profile, Forrester Consulting supplemented this research with custom survey questions asked of cybersecurity decision makers at cross-industry global enterprises. The custom survey began and was completed in November 2019.

ENDNOTES

[1] Source: "Using AI For Evil," Forrester Research, Inc., April 16, 2018.

[2] Source: "Predictions 2020: Cybersecurity," Forrester Research, Inc., October 30, 2019.

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© 2019, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to forrester.com. [E-45046]

Demographics

GEOGRAPHY

- United States: 23%
- United Kingdom: 23%
- The Netherlands: 15%
- Singapore: 25%
- Australia: 16%

TOP 5 INDUSTRIES

- Technology: 20%
- Manufacturing: 15%
- Financial services: 12%
- Retail: 11%
- Business services: 8%

TITLE

- C-level: 36%
- Vice president: 28%
- Director: 35%

RESPONSIBILITY

Cybersecurity technology:

- 66% final decision makers
- 33% influencing decisions

Cybersecurity strategy:

- 75% final decision makers
- 25% influencing decisions

FORRESTER®