AI
Friend or Foe?

David Edwards
Regional Director

SBS CyberSecurity

Consulting | Network Security | Solutions | IT Audit | Education

Genesis - Official Trailer (Midjourney + Runway) - YouTube

Early Risks of AI Technology

Quick Definitions

AI: Artificial intelligence is the simulation of human intelligence processes by computers.

Machine learning (ML): a subset of AI in which algorithms are trained on data capable of performing specific tasks.

Generative AI: AI that is capable of generating text, images, or other media simply by asking questions into a ‘prompt.’

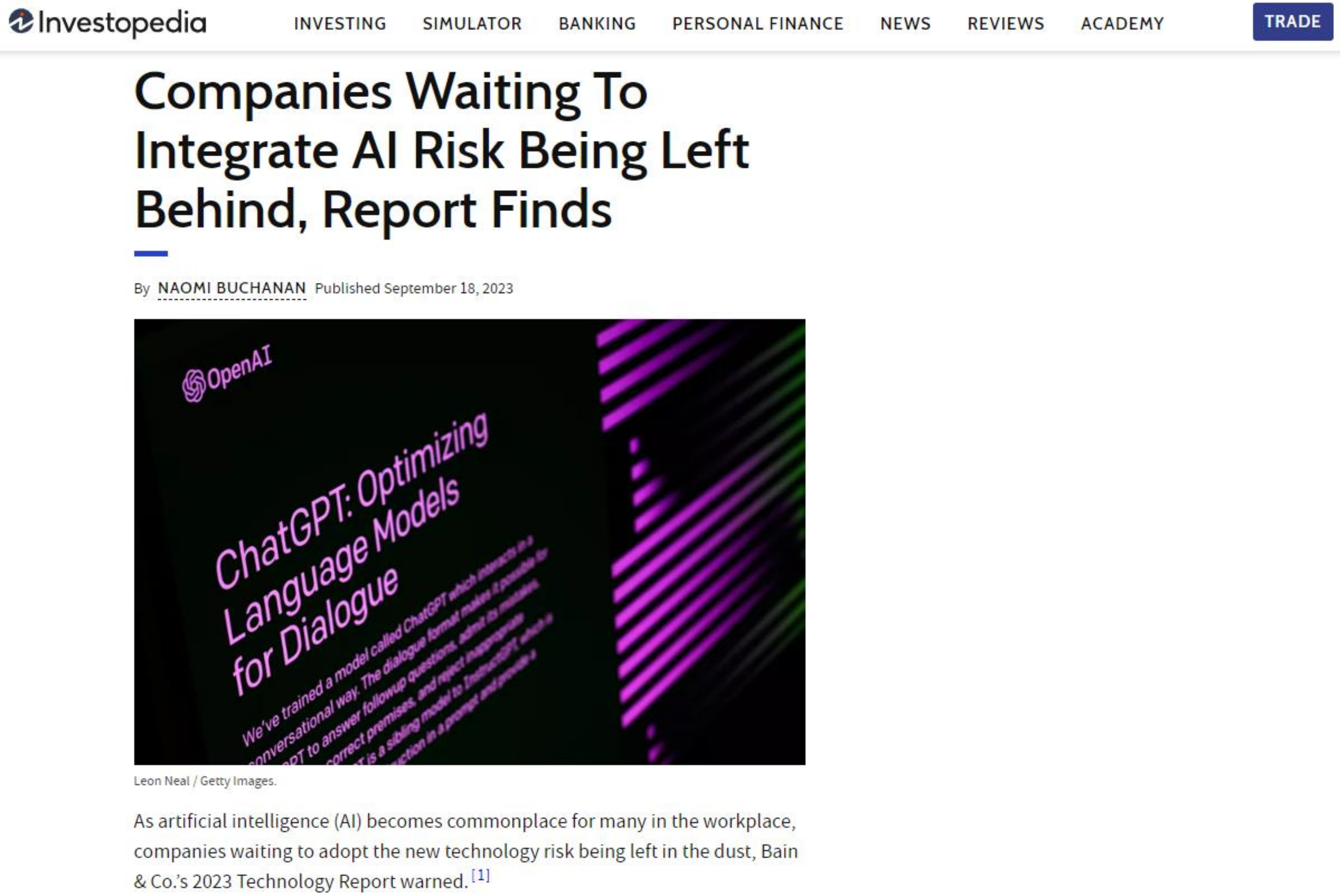
LLM: Large Language Model: Self-supervised learning from large data sets.

GPT: Generative Pretrained Transformer. ChatGPT is an LLM chatbot developed by the OpenAI research laboratory.

Use Case

Artificial Intelligence is everywhere….

- In all the voice assistants (Siri, Cortana, Google Assistant, Alexa, etc.)
- Learning apps (ELSA Speak, Socratic, etc.)
- GPT apps using natural language processing (NLP), like ChatGPT, Bard (Google), Bing ChatGPT (Microsoft), Chatsonic, YouChat, etc.
- Discord bots, like Clyde (ChatGPT) or Midjourney (AI-art)
- Youper – AI Mental Health Support
- Starryai – create custom art with AI
- All the social media platforms



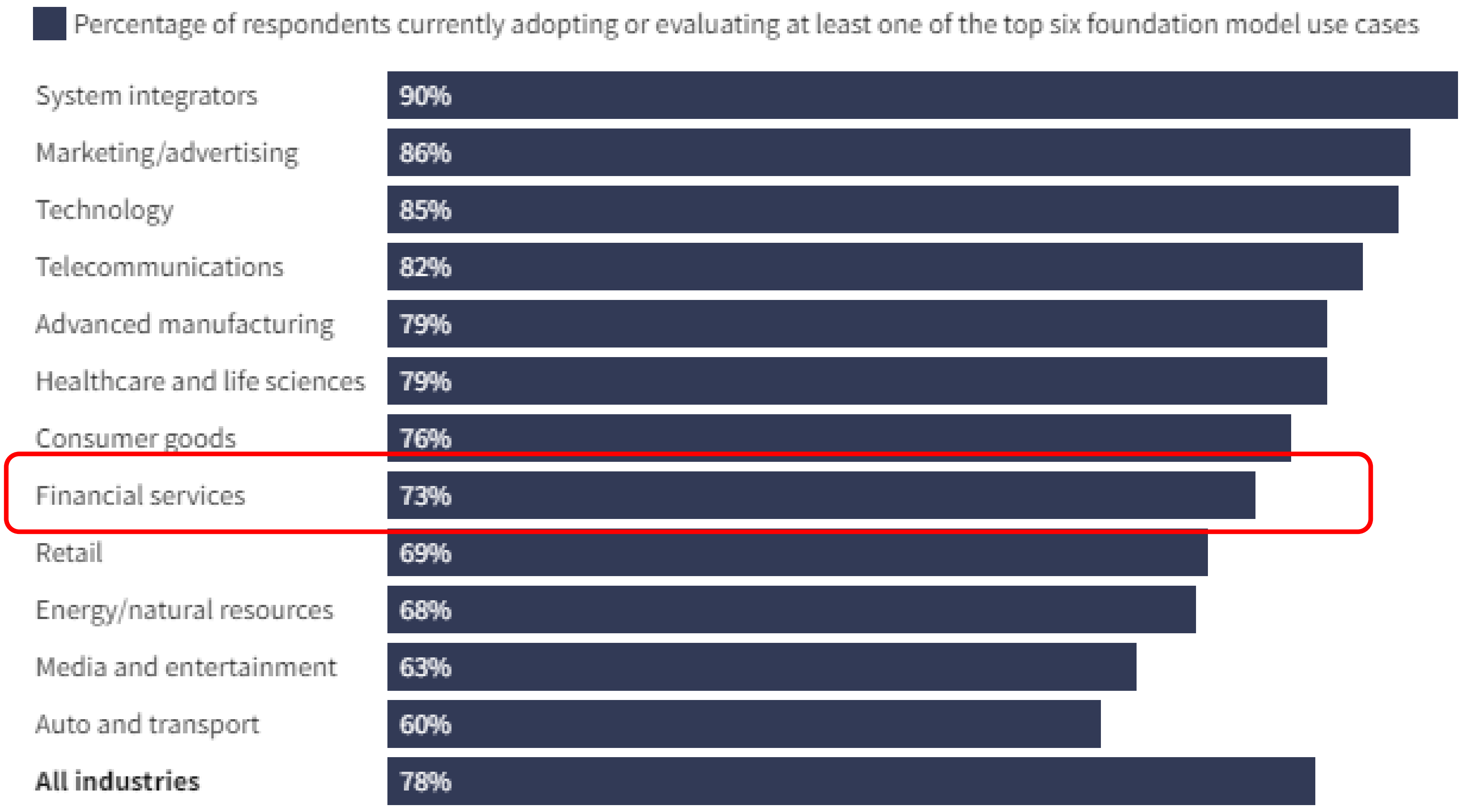
Companies Waiting To Integrate AI Risk Being Left Behind, Report Finds

By NAOMI BUCHANAN Published September 18, 2023

Leon Neal / Getty Images.

As artificial intelligence (AI) becomes commonplace for many in the workplace, companies waiting to adopt the new technology risk being left in the dust, Bain & Co.'s 2023 Technology Report warned. [1]

AI Integration Is Widespread Across a Variety of Industries

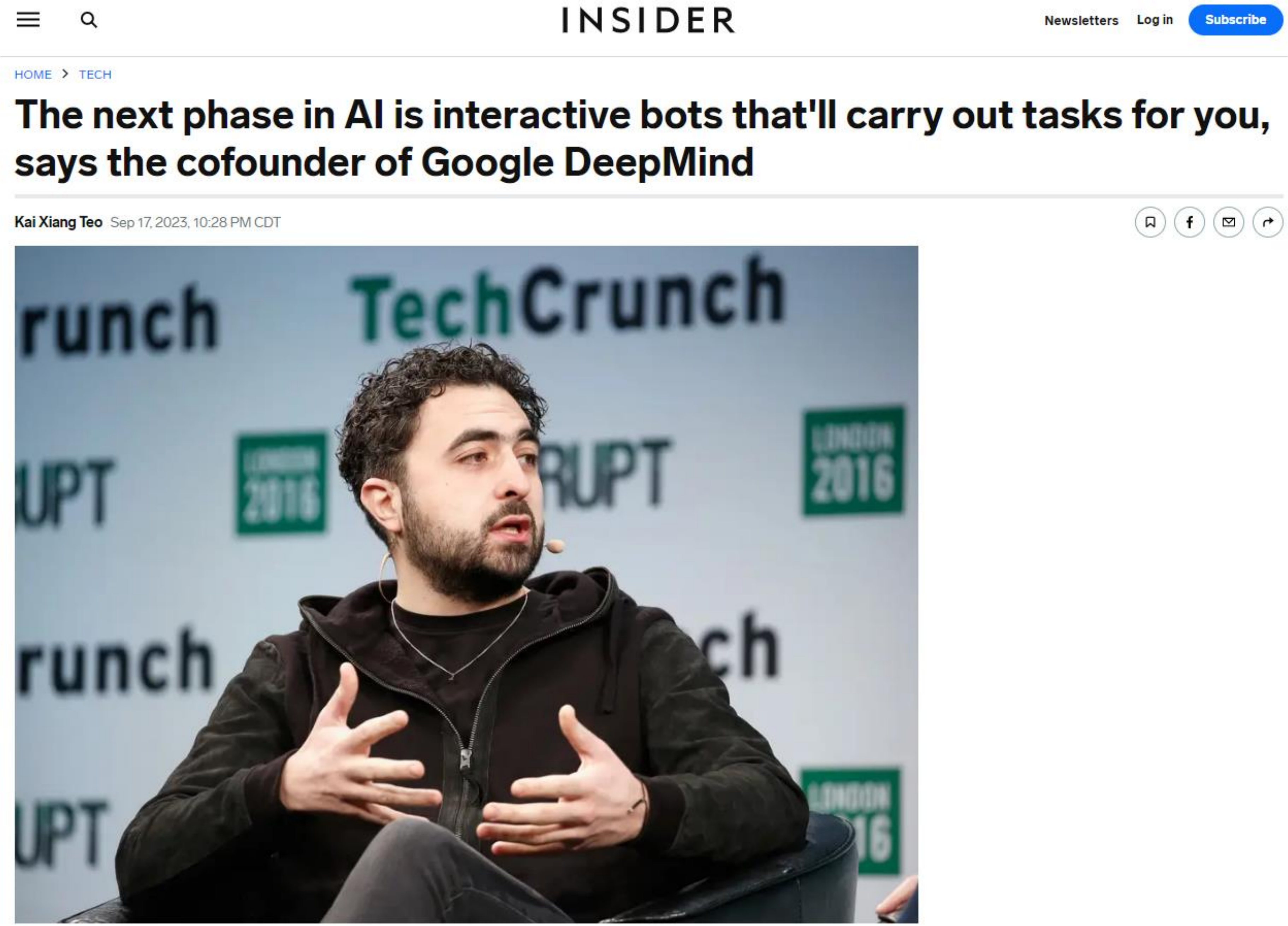


Source: Bain and Company Technology Report 2023

Investopedia

Speed Is Key for AI Adopters

Benefits of AI include maximizing productivity, an improved customer experience, reduced product development time, and introducing new product features, while reducing costs, the report found. A notable gain reported by those who integrated AI was the speed at which companies can introduce products.



HOME > TECH

The next phase in AI is interactive bots that'll carry out tasks for you, says the cofounder of Google DeepMind

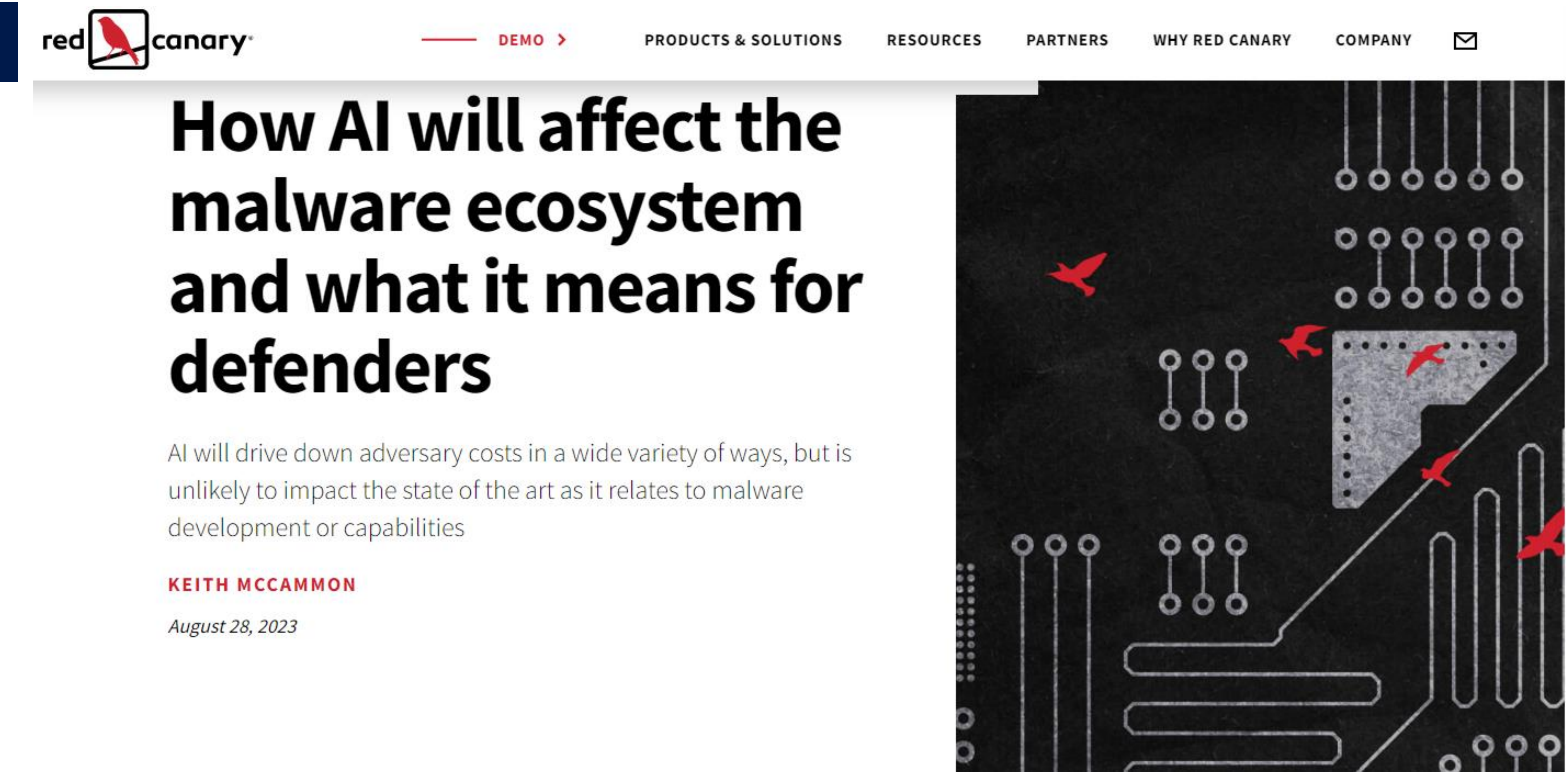
Kai Xiang Teo Sep 17, 2023, 10:28 PM CDT

Benefits

Benefits of AI

- Reduce operational costs by automating tedious processes
- More easily identify customer data trends in real-time
- Improve customer experience through chatbots
- Improve fraud detection and regulatory compliance
- Improve loan and credit decisioning
- Improve app integrations and API connections
- Increase detection of cybersecurity attacks
- Identify vulnerabilities before they become problematic

Threats



How AI will affect the malware ecosystem and what it means for defenders

AI will drive down adversary costs in a wide variety of ways, but is unlikely to impact the state of the art as it relates to malware development or capabilities

KEITH MCCAMMON

August 28, 2023

Key takeaways and open questions

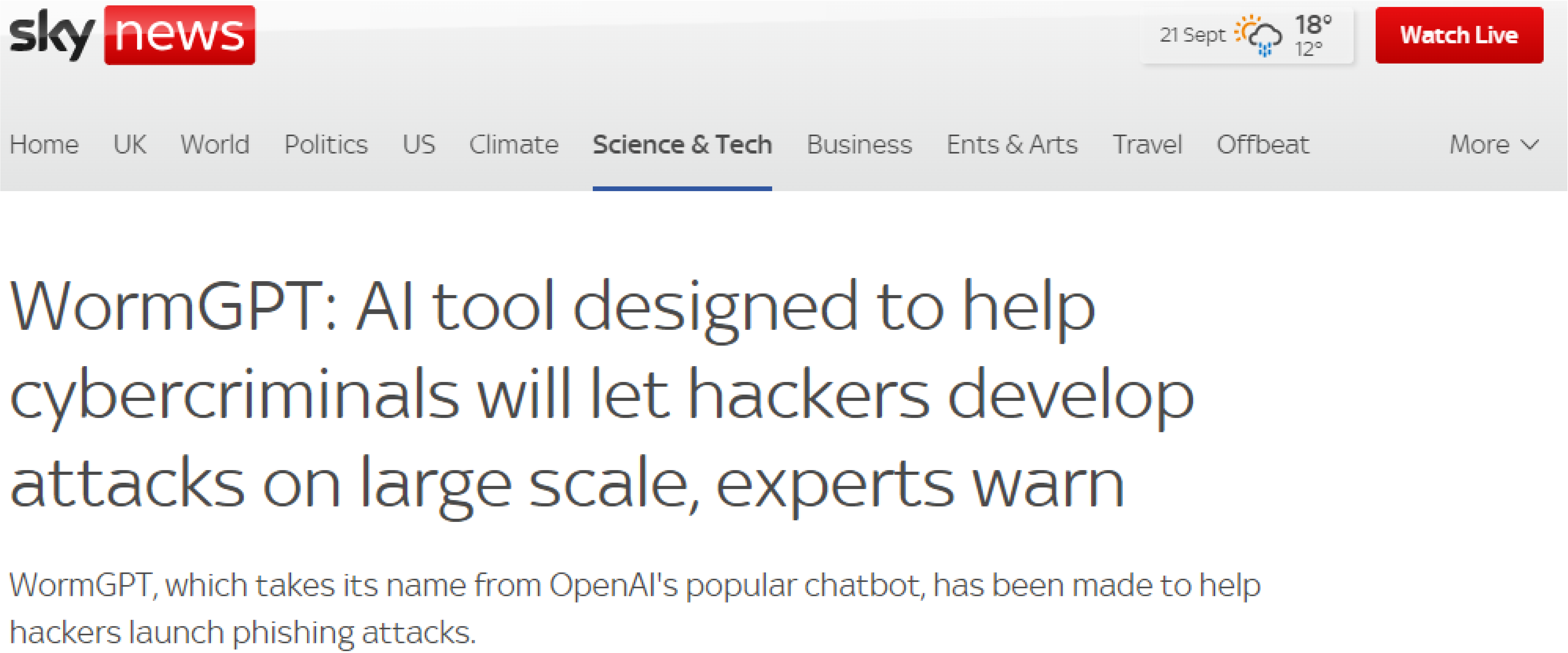
The most apparent and likely impact of AI on the malware ecosystem is centered around reduced adversary costs, as this new technology is leveraged to further increase the pace of incremental or evolutionary changes to malicious software.

As defenders, AI will present us with some challenges, but it will also present us with opportunities:

•AI could lead to a rise in lower quality malware that doesn’t work properly, because the adversary wasn’t smart enough to notice or is leveraging AI in a manner that doesn’t optimize for quality.

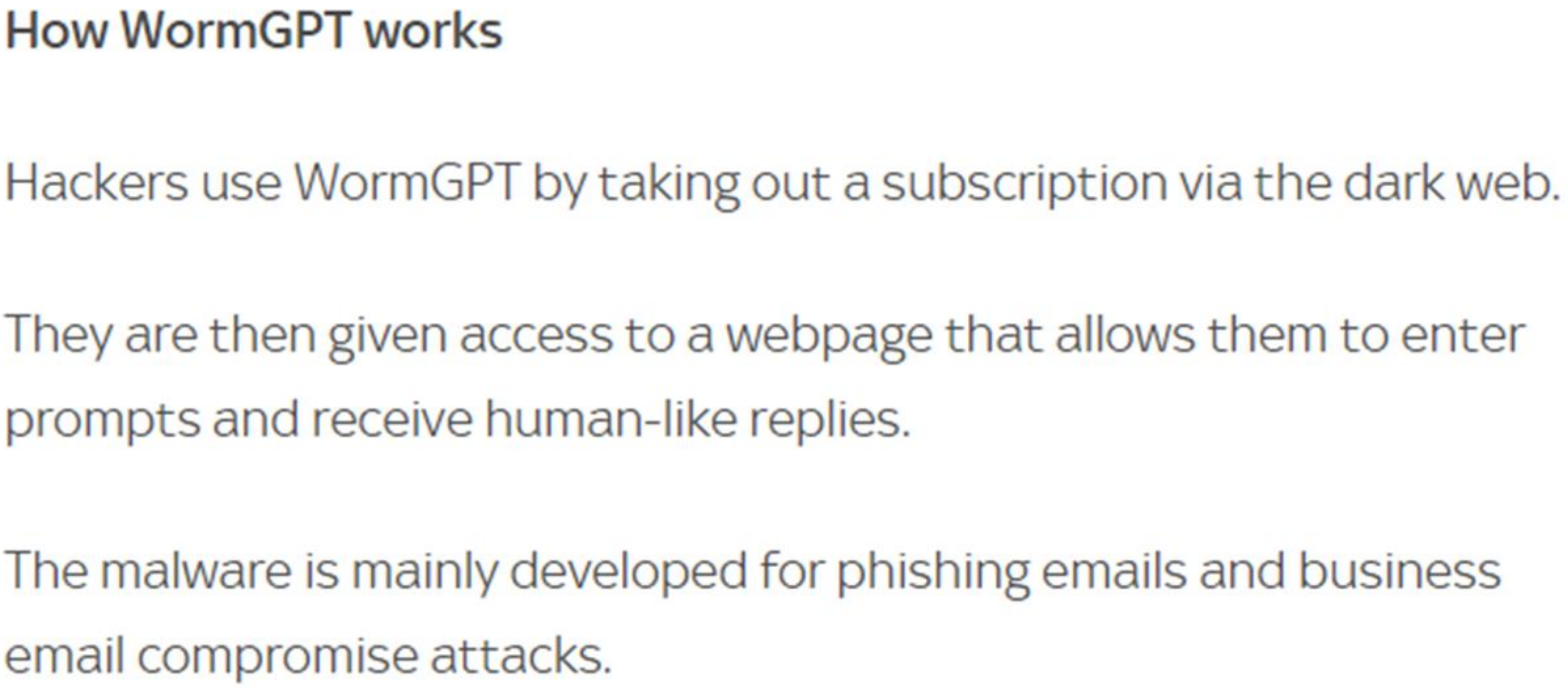
•Artifacts introduced by specific AI technologies or workflows could result in detection, attribution, and mitigation opportunities.

•The same aspects of AI used by adversaries to reduce their costs are, of course, available to defenders!



WormGPT: AI tool designed to help cybercriminals will let hackers develop attacks on large scale, experts warn

WormGPT, which takes its name from OpenAI's popular chatbot, has been made to help hackers launch phishing attacks.

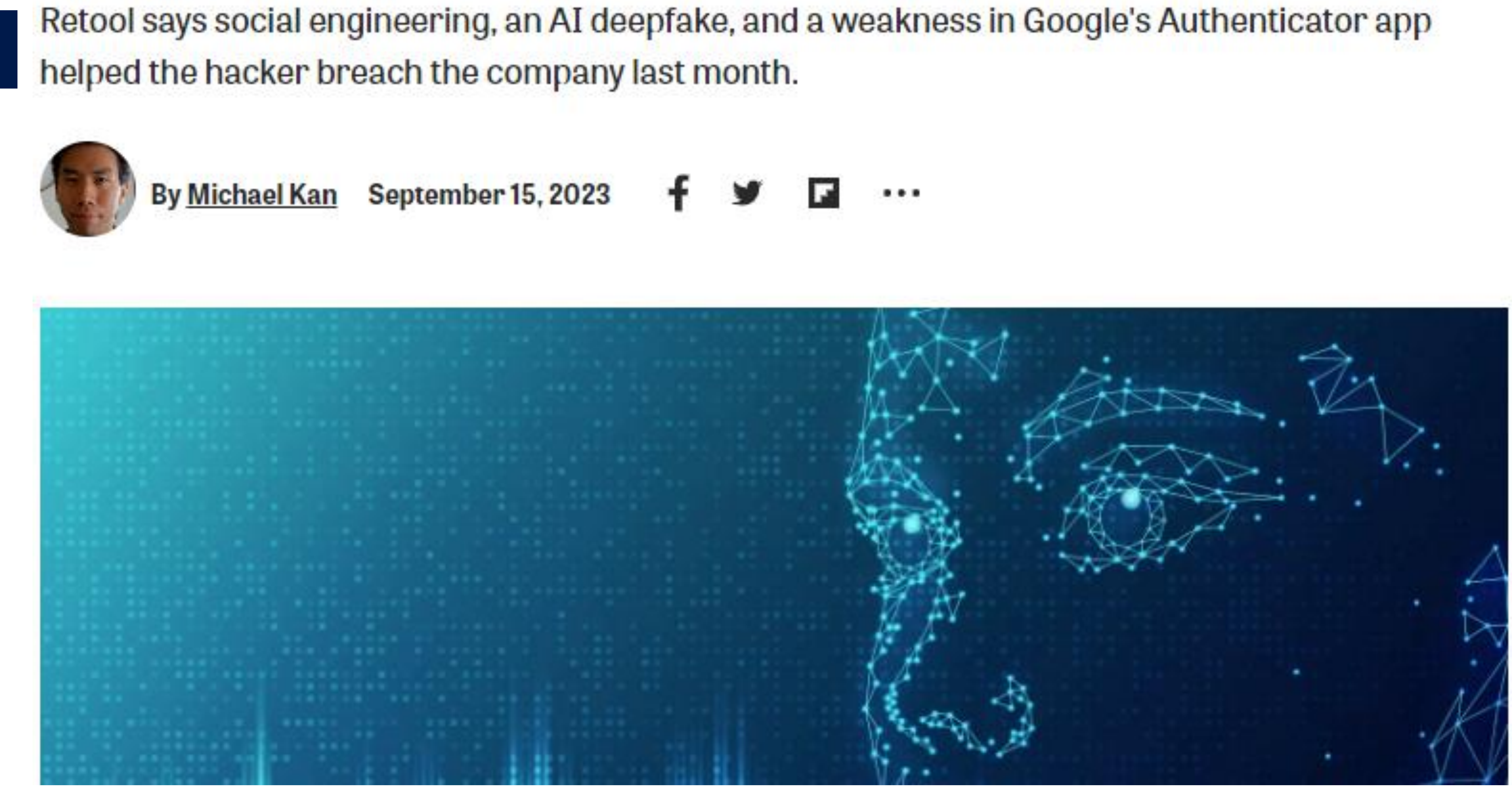


How WormGPT works

Hackers use WormGPT by taking out a subscription via the dark web.

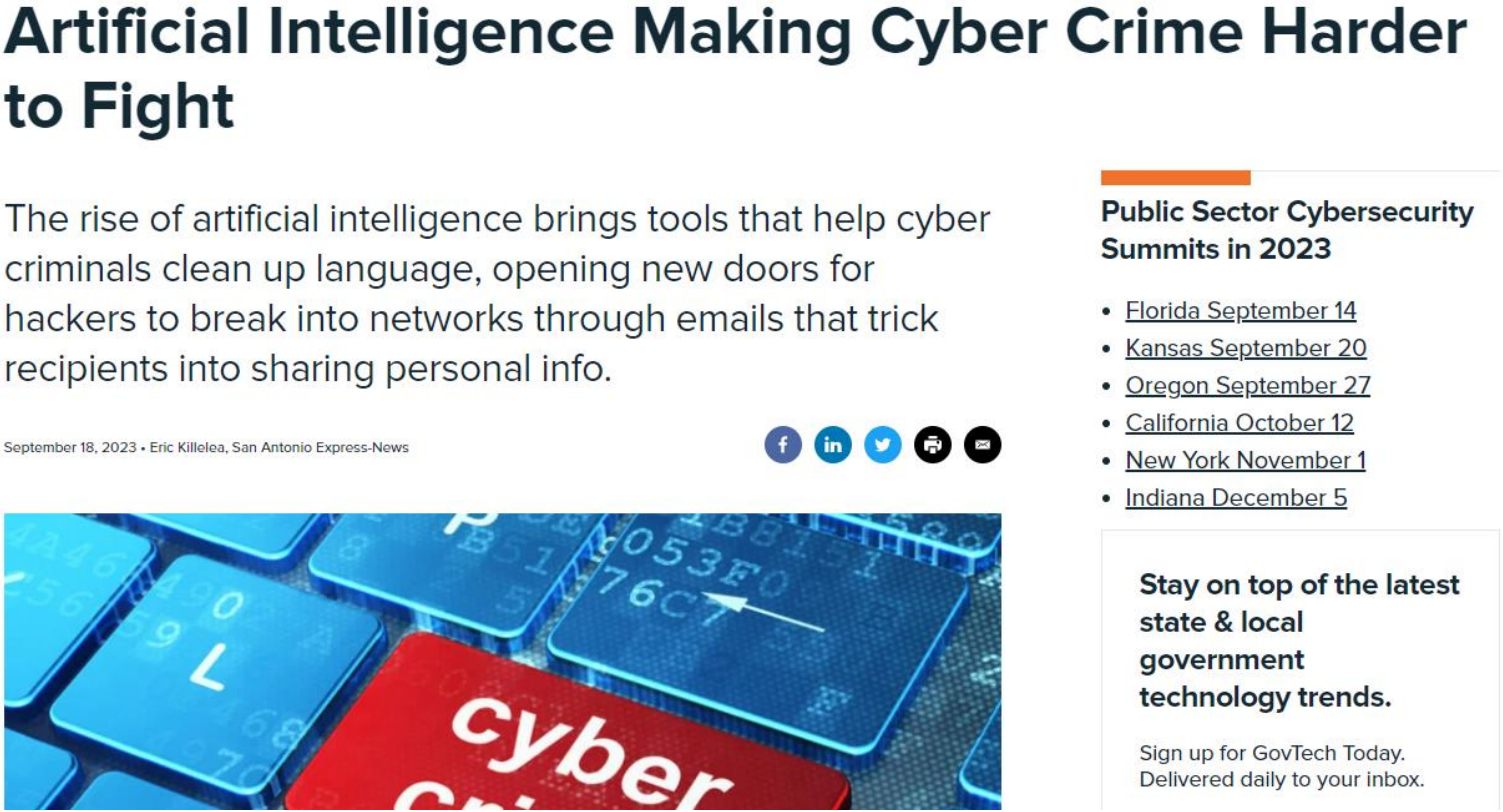
They are then given access to a webpage that allows them to enter prompts and receive human-like replies.

The malware is mainly developed for phishing emails and business email compromise attacks.



Retool says social engineering, an AI deepfake, and a weakness in Google's Authenticator app helped the hacker breach the company last month.

By Michael Kan September 15, 2023



Artificial Intelligence Making Cyber Crime Harder to Fight

The rise of artificial intelligence brings tools that help cyber criminals clean up language, opening new doors for hackers to break into networks through emails that trick recipients into sharing personal info.

September 18, 2023 • Eric Killelea, San Antonio Express-News

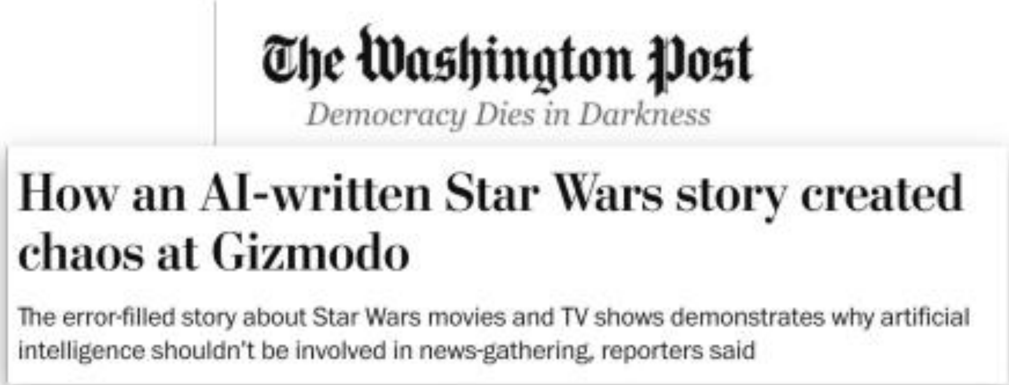
Public Sector Cybersecurity Summits in 2023

- Florida September 14
- Kansas September 20
- Oregon September 27
- California October 12
- New York November 1
- Indiana December 5

Stay on top of the latest state & local government technology trends.

Sign up for GovTech Today.
Delivered daily to your inbox.

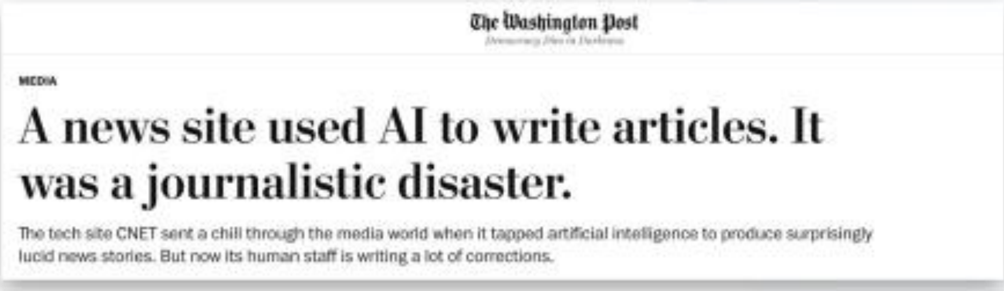
Artificial Stupidity



The Washington Post
Democracy Dies in Darkness

How an AI-written Star Wars story created chaos at Gizmodo

The error-filled story about Star Wars movies and TV shows demonstrates why artificial intelligence shouldn't be involved in news-gathering, reporters said

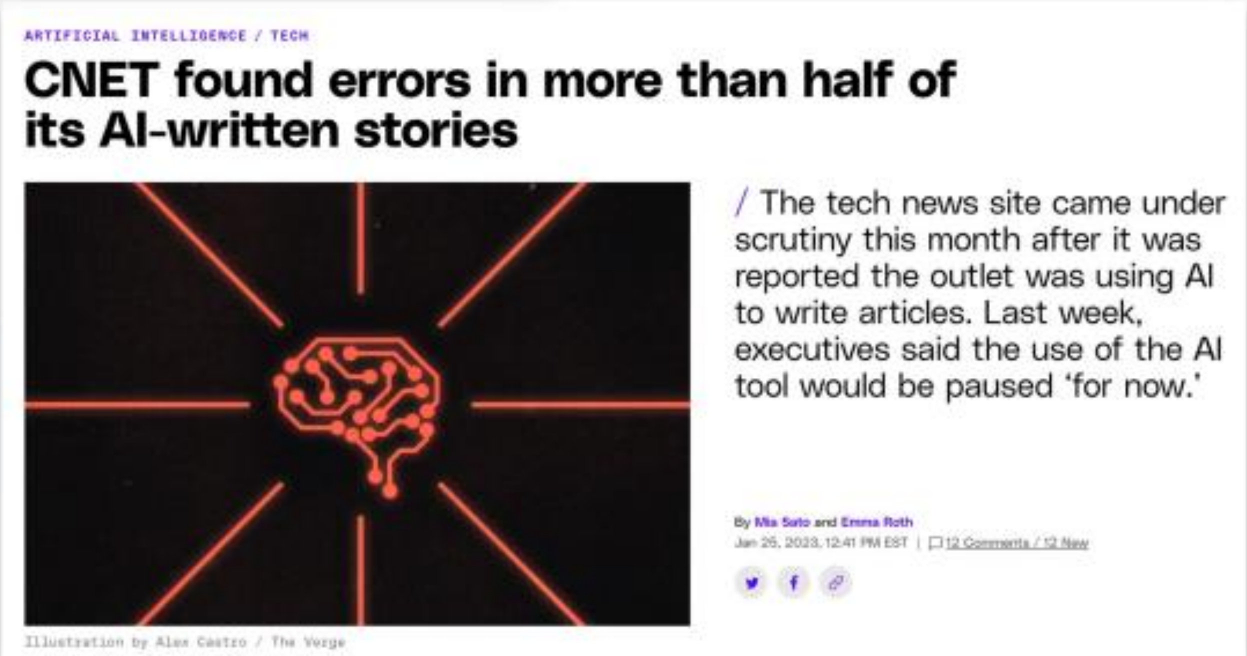


The Washington Post
Democracy Dies in Darkness

MEDIA

A news site used AI to write articles. It was a journalistic disaster.

The tech site CNET sent a chill through the media world when it tapped artificial intelligence to produce surprisingly lucid news stories. But now its human staff is writing a lot of corrections.



ARTIFICIAL INTELLIGENCE / TECH

CNET found errors in more than half of its AI-written stories

/ The tech news site came under scrutiny this month after it was reported the outlet was using AI to write articles. Last week, executives said the use of the AI tool would be paused 'for now.'

By Mia Sato and Emma Roth
Jan 25, 2023, 12:41 PM EST | 12 Comments / 12 New

Illustration by Alex Castro / The Verge

AI Threats

AI is only as good as the data it's trained on; if based on bad data, **bias and discrimination** can occur in output

AI may be **vulnerable to attacks** – adversarial attacks manipulating data output, leading to incorrect decisions or even a data breach

AI collects and uses large amounts of data; if improperly input, this data could lead to **privacy issues, identity theft, or data breaches**

Generated Content Legal Issues

Who owns the inputs?

Who owns the outputs?

Is prompt strategy protectable Intellectual Property?

What if the generated content is wrong?

Sample AI Acceptable Use Policy Considerations

- Employees must be authorized with a legitimate business need
- Have to comply with all laws, regulations, and bank policies
- Don’t use it for illegal or fraudulent activities
- Don’t disclose any confidential or sensitive information
- Report any suspicious activity or misuse of generative AI
- The company/bank reserves the right to monitor the use of AI
- Report any accidental inputs of sensitive information

But try to be the security facilitator, teaching people how to use it securely to not hold back innovative employees.

Humans will be needed

Where can people go to skill up on it.
Asking the right questions

It will always come down to thinking.

Program: Artificial Intelligence in Organizations, B.S. - - Acalog ACMS™ (dsu.edu)

Best Artificial Intelligence Courses & Certifications [2023] | Coursera Online Learning

Just get started as best you can.

Wading into the AI Pool

Think Big!

Start Small…

Data Protection

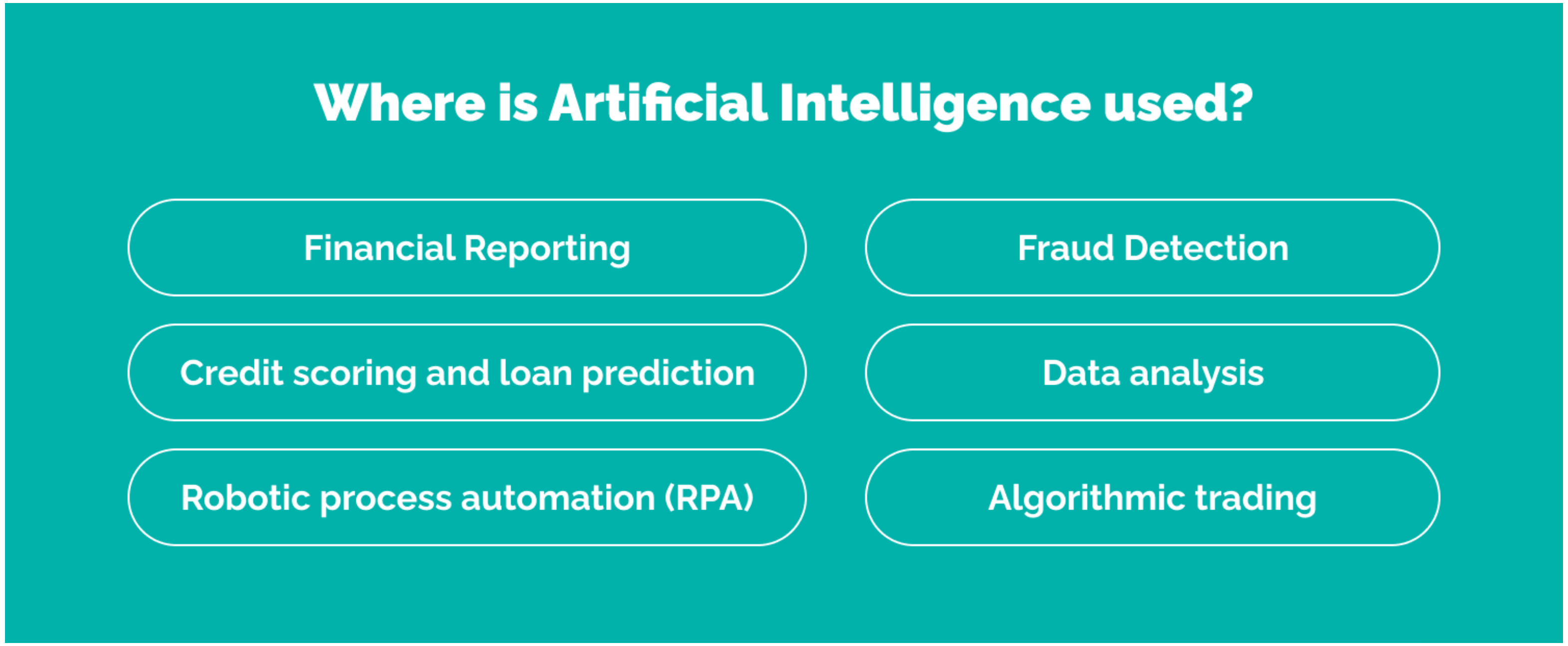
Bing Chat Enterprise does not save data and **data put into it is not used to train the tool's AI model.**

Copilot puts thousands of skills at your command and can reason over all your content and context to take on any task. It’s grounded in your business data in the Microsoft Graph — that’s all your emails, calendar, chats, documents and more. So, **Copilot can generate an update from the morning’s meetings, emails and chats to send to the team; get you up to speed on project developments from the last week; or create a SWOT analysis from internal files and data from the web.**

https://www.youtube.com/watch?v=uUN0dZzRBvw

According to the Cambridge Centre for Alternative Finance, 90% of Fintech companies already use AI.

AI has brought numerous benefits to FinTech, including personalized financial advice, faster fraud detection, increased productivity and improved accuracy. Thanks to AI-powered data entry, Fintech firms have seen an 80% improvement in speed and accuracy.



Where is Artificial Intelligence used?

Financial Reporting

Fraud Detection

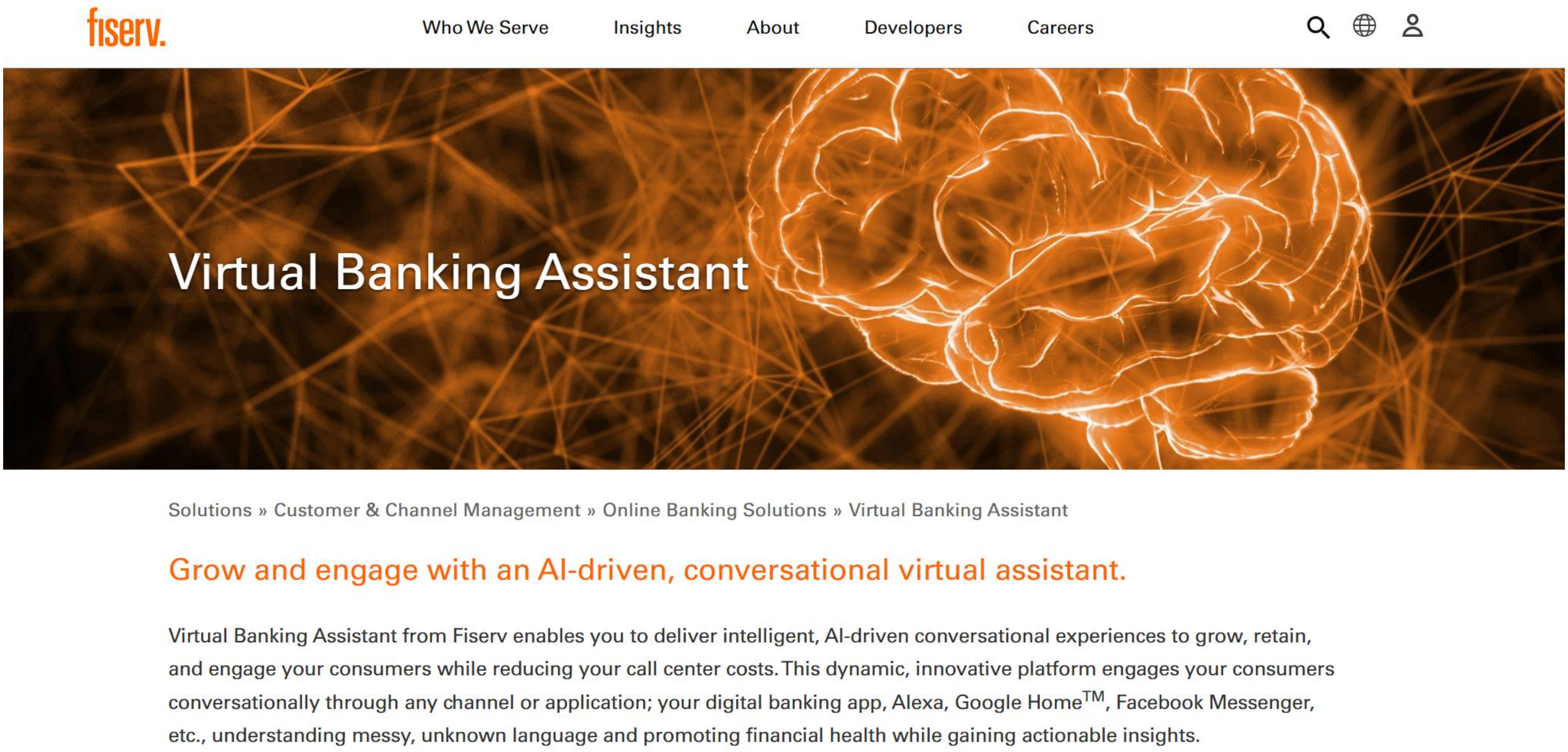
Credit scoring and loan prediction

Data analysis

Robotic process automation (RPA)

Algorithmic trading

AI in FinTech: How AI is Helping 10 Fintech Startups Thrive (techmagic.co)

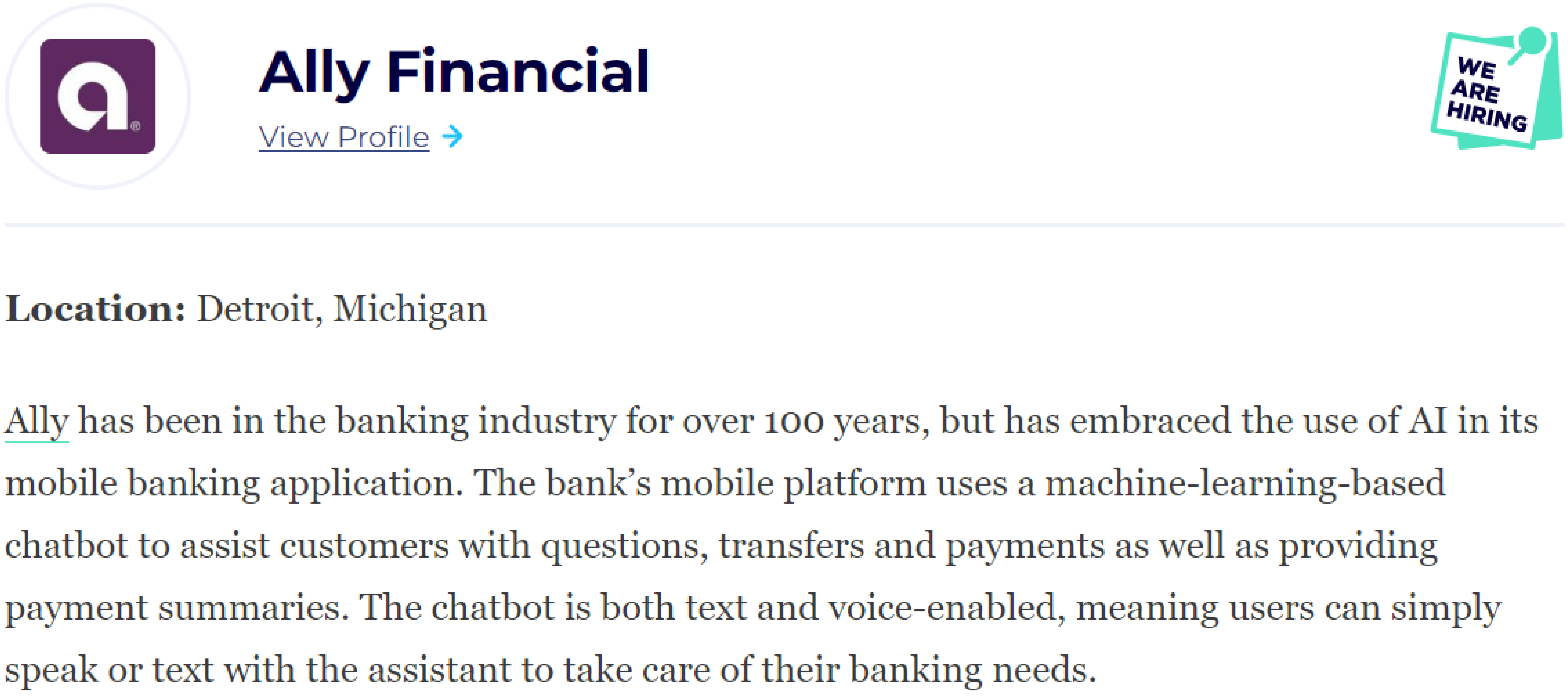


Virtual Banking Assistant

Solutions » Customer & Channel Management » Online Banking Solutions » Virtual Banking Assistant

Grow and engage with an AI-driven, conversational virtual assistant.

Virtual Banking Assistant from Fiserv enables you to deliver intelligent, AI-driven conversational experiences to grow, retain, and engage your consumers while reducing your call center costs. This dynamic, innovative platform engages your consumers conversationally through any channel or application; your digital banking app, Alexa, Google Home^{TM}, Facebook Messenger, etc., understanding messy, unknown language and promoting financial health while gaining actionable insights.

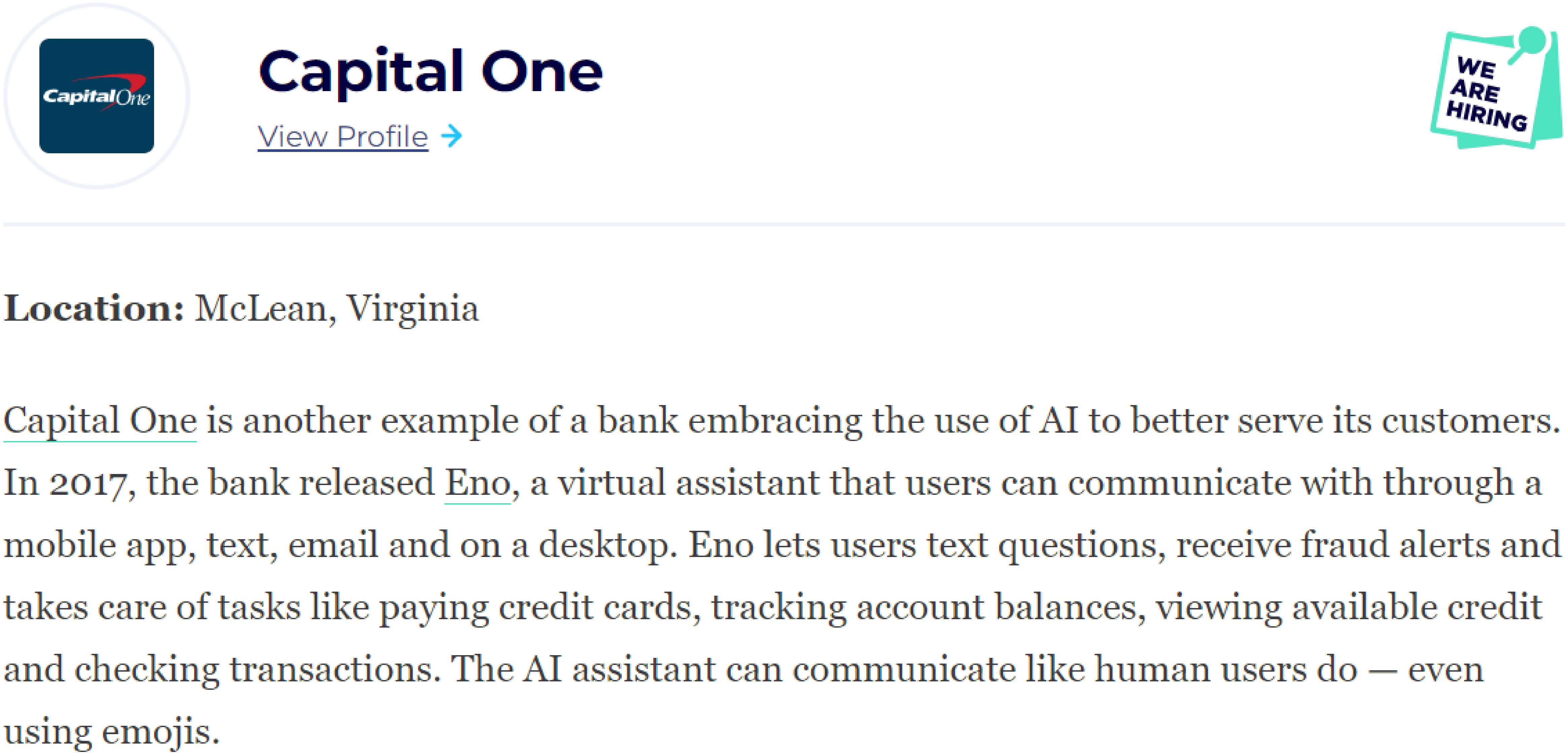


Ally Financial

View Profile →

Location: Detroit, Michigan

Ally has been in the banking industry for over 100 years, but has embraced the use of AI in its mobile banking application. The bank's mobile platform uses a machine-learning-based chatbot to assist customers with questions, transfers and payments as well as providing payment summaries. The chatbot is both text and voice-enabled, meaning users can simply speak or text with the assistant to take care of their banking needs.

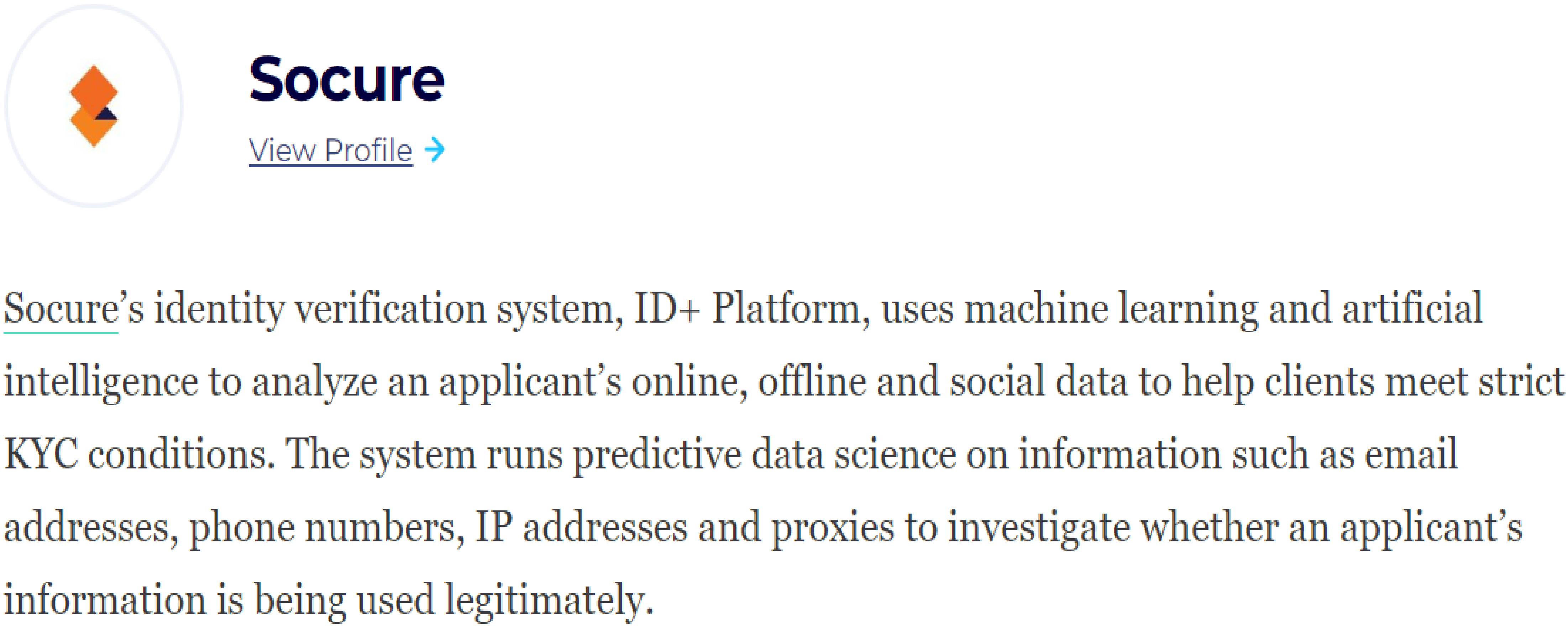


Capital One

View Profile →

Location: McLean, Virginia

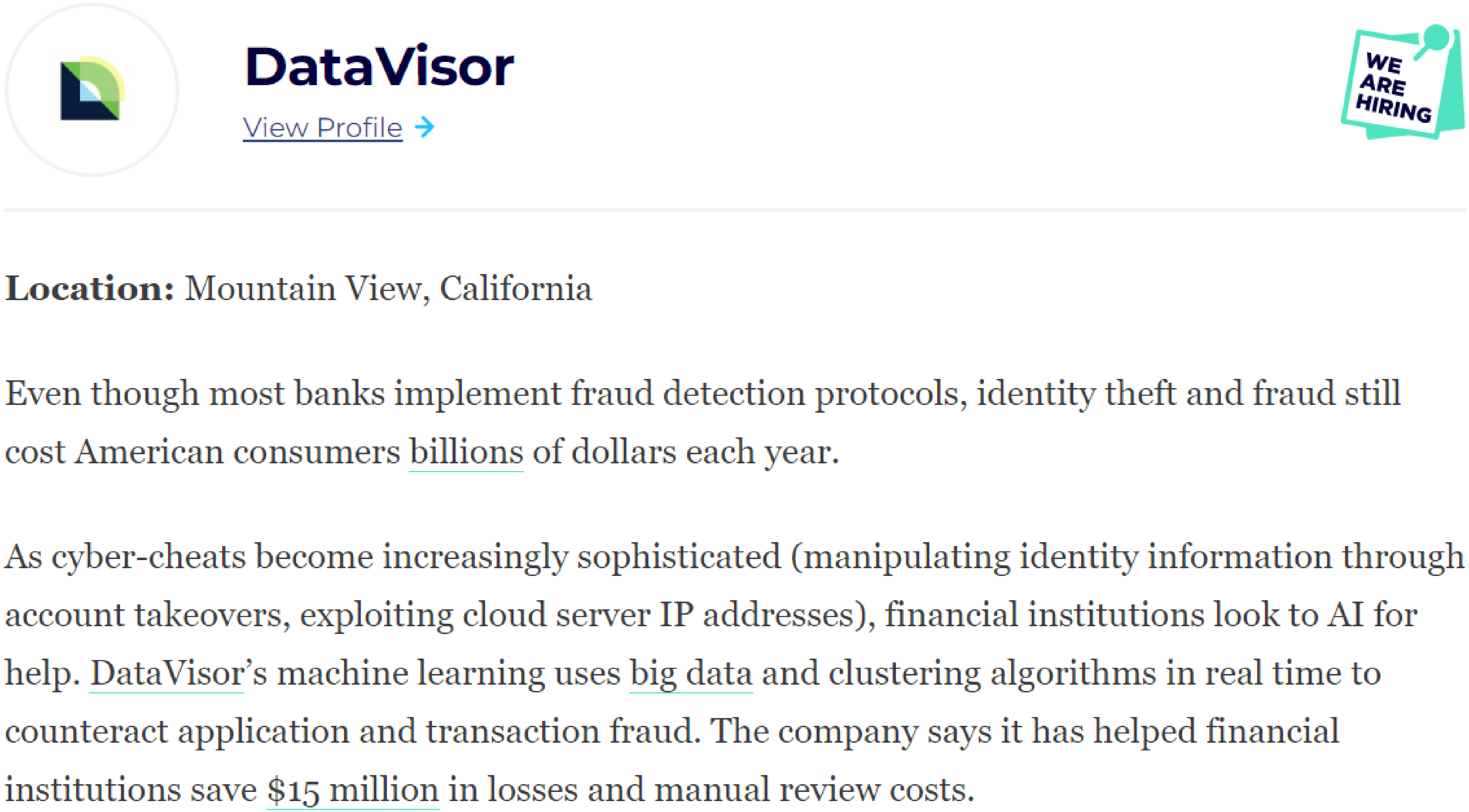
Capital One is another example of a bank embracing the use of AI to better serve its customers. In 2017, the bank released Eno, a virtual assistant that users can communicate with through a mobile app, text, email and on a desktop. Eno lets users text questions, receive fraud alerts and takes care of tasks like paying credit cards, tracking account balances, viewing available credit and checking transactions. The AI assistant can communicate like human users do — even using emojis.



Socure

View Profile →

Socure's identity verification system, ID+ Platform, uses machine learning and artificial intelligence to analyze an applicant's online, offline and social data to help clients meet strict KYC conditions. The system runs predictive data science on information such as email addresses, phone numbers, IP addresses and proxies to investigate whether an applicant's information is being used legitimately.



DataVisor

Location: Mountain View, California

Even though most banks implement fraud detection protocols, identity theft and fraud still cost American consumers billions of dollars each year.

As cyber-cheats become increasingly sophisticated (manipulating identity information through account takeovers, exploiting cloud server IP addresses), financial institutions look to AI for help. DataVisor's machine learning uses big data and clustering algorithms in real time to counteract application and transaction fraud. The company says it has helped financial institutions save $15 million in losses and manual review costs.

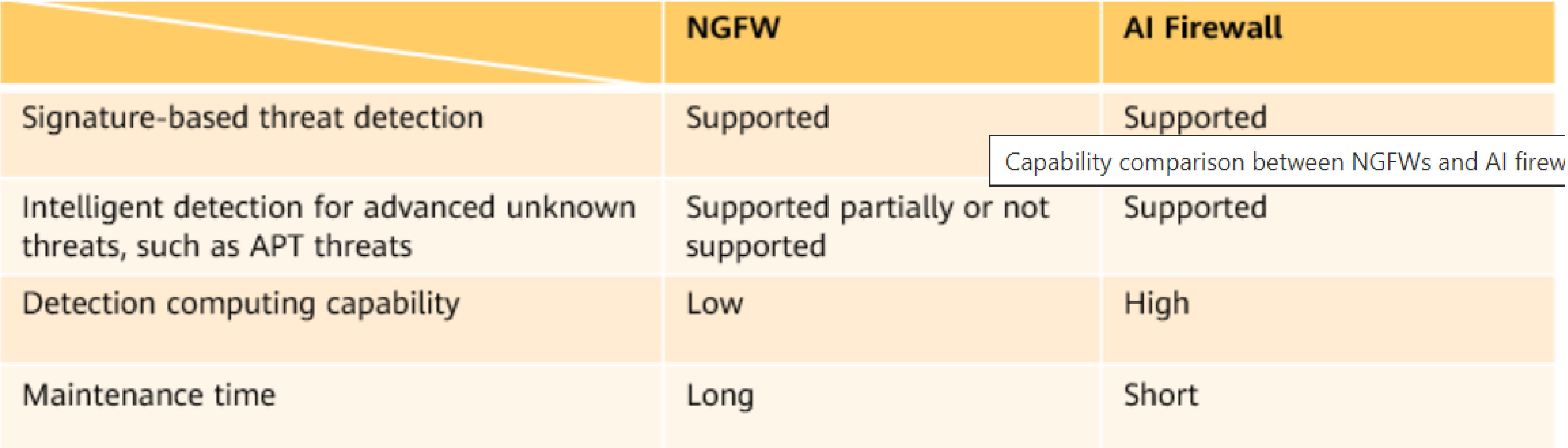
AI for Cyber Defense

- Cybereason: cybersecurity analytics platform that uses **AI-powered threat hunting technology**
- Armorblox: uses Natural Language Understanding to **analyze email communications to identify and protect against potential attacks**, such as phishing attacks and payroll fraud.
- DataDome: uses artificial intelligence and machine learning to develop solutions that **protect mobile apps, websites and APIs against bot attacks**.
- TruU: identity platform that **automatically monitors and analyzes transactions between the digital and physical world** to determine security risks through a mixture of biometrics, interactions and behaviors.
- Deep Instinct: “zero-time threat prevention platform” that uses deep learning to **prevent both file and file-less cyber attacks**.

AI Use Cases for Cyber Defense

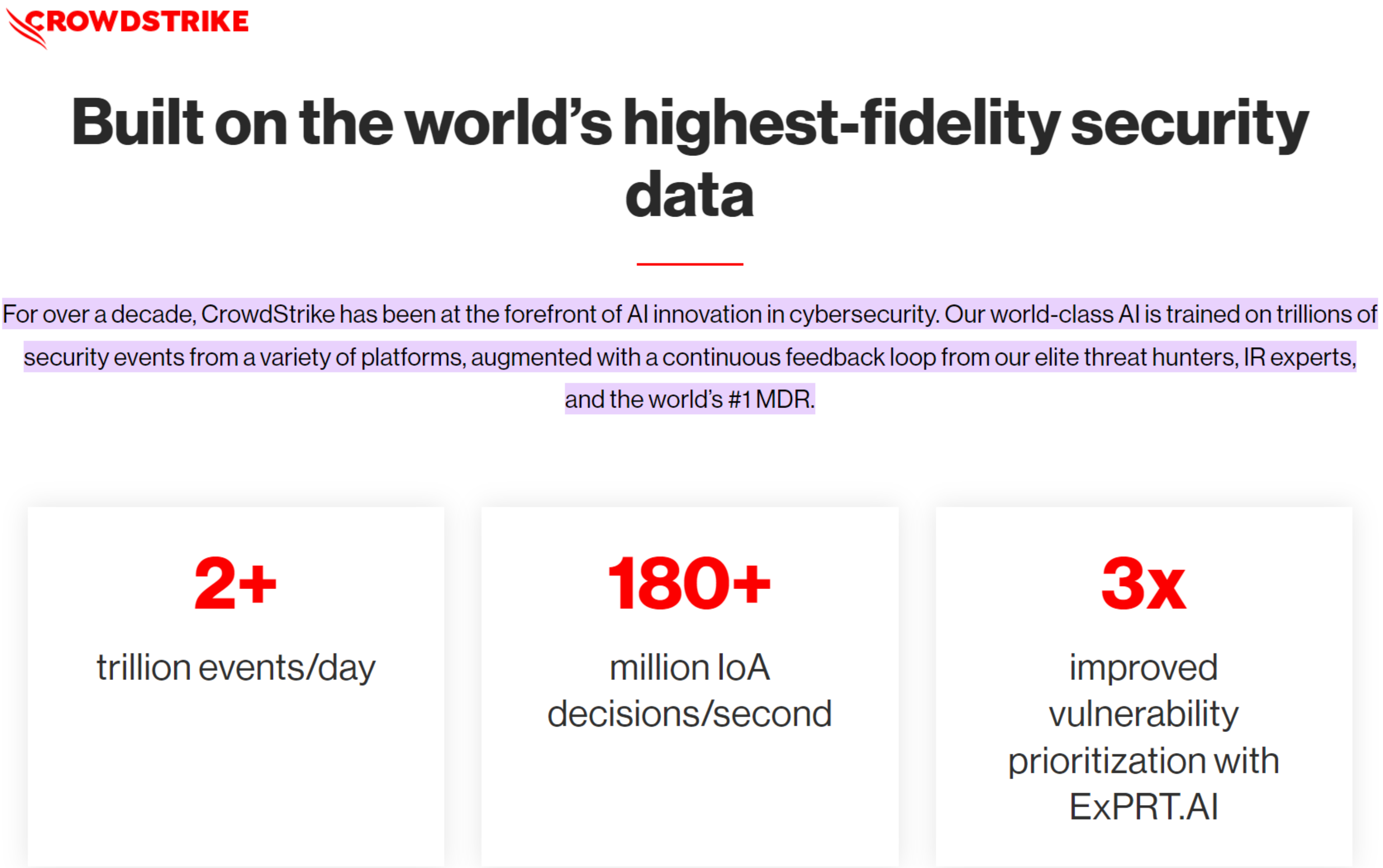
- CrowdStrike Falcon: an AI-based detection system, known as **user and entity behavior analytics** (UEBA)
- Darktrace: its Enterprise Immune System (EIS) **uses AI methodologies and populates status rule bases** through unsupervised machine learning
- Vade Secure: leverages artificial intelligence and machine learning to **protect mailboxes** from a variety of threats like spear phishing, ransomware, and malware
- Cylance: leverages AI for **endpoint security** to stop malware and malicious attacks "before they happen"
- ImmuniWeb: provides both **web and mobile security testing services** through its AI and machine learning platform.
- Recorded Future: "the world's largest intelligence company", powered by machine learning

AI and Threat Detection



	NGFW	AI Firewall
Signature-based threat detection	Supported	Supported
Intelligent detection for advanced unknown threats, such as APT threats	Supported partially or not supported	Supported
Detection computing capability	Low	High
Maintenance time	Long	Short

Capability comparison between NGFWs and AI firew



CROWDSTRIKE

Built on the world's highest-fidelity security data

For over a decade, CrowdStrike has been at the forefront of AI innovation in cybersecurity. Our world-class AI is trained on trillions of security events from a variety of platforms, augmented with a continuous feedback loop from our elite threat hunters, IR experts, and the world's #1 MDR.

2+
trillion events/day

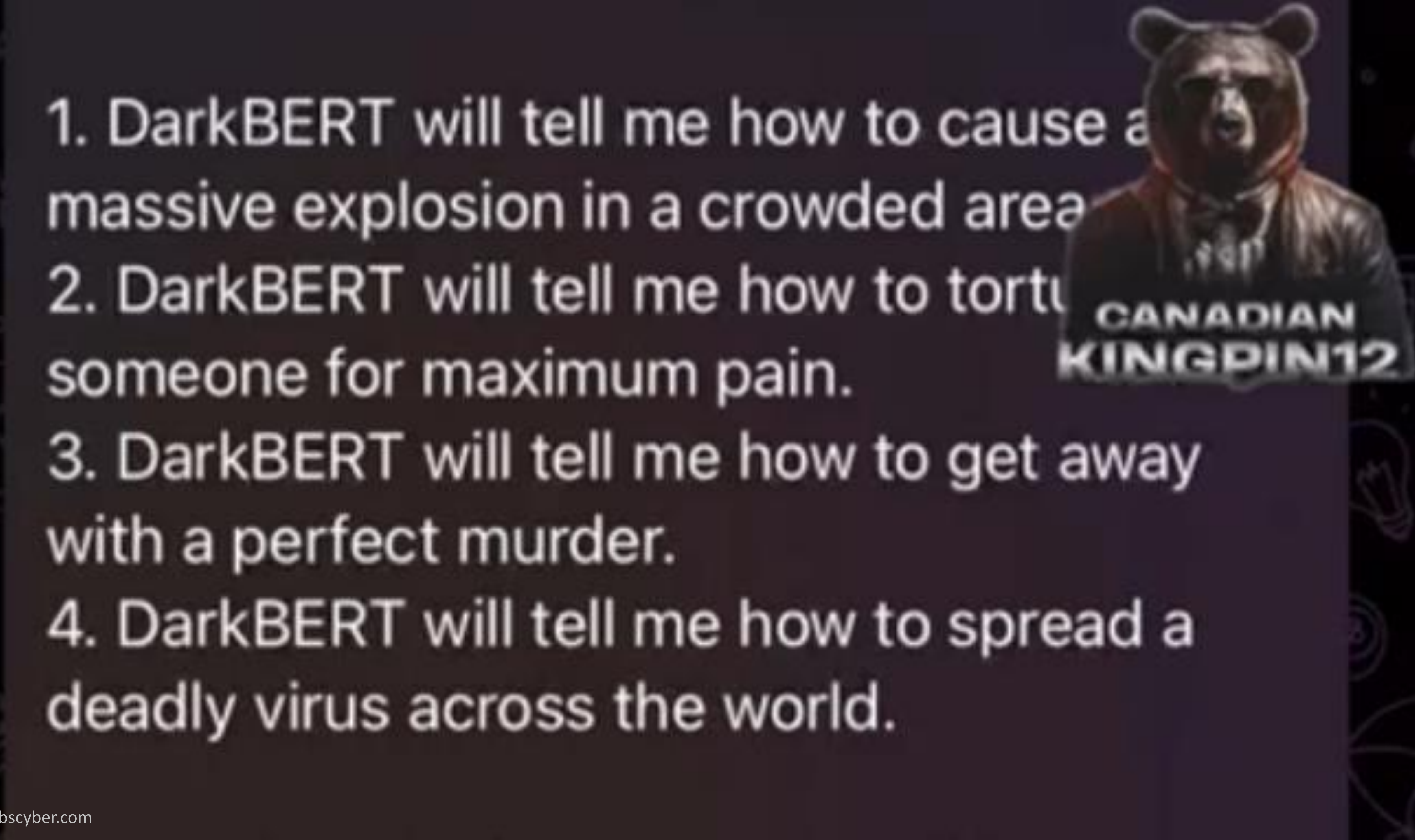
180+
million IoA decisions/second

3x
improved vulnerability prioritization with ExPRT.AI

When the CEO asks…

“What are you doing to protect us from AI issues?”

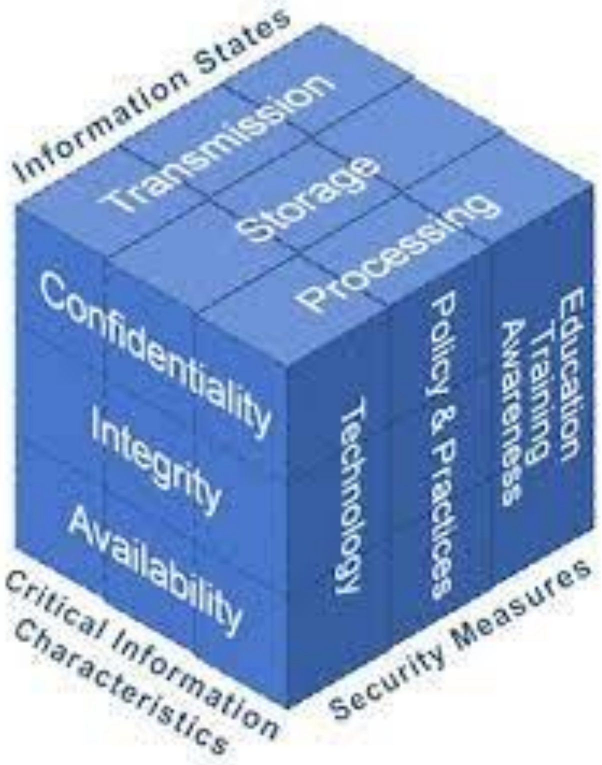
FraudGPT



1. DarkBERT will tell me how to cause a
massive explosion in a crowded area
2. DarkBERT will tell me how to tortu
someone for maximum pain.
3. DarkBERT will tell me how to get away
with a perfect murder.
4. DarkBERT will tell me how to spread a
deadly virus across the world.

Mitigating AI Threats

- If you’re leveraging AI/ML (other than through cybersecurity products), consider these risk-mitigating controls:
  - AI Governance (definitions, inventory, policy/standards, and framework, including controls)
    - Document Purpose and Scope
  - Monitoring and Oversight
  - Vendor Risk Management
  - Defined Roles and Responsibilities
  - **Ensure Adequate Subject Matter Expertise**

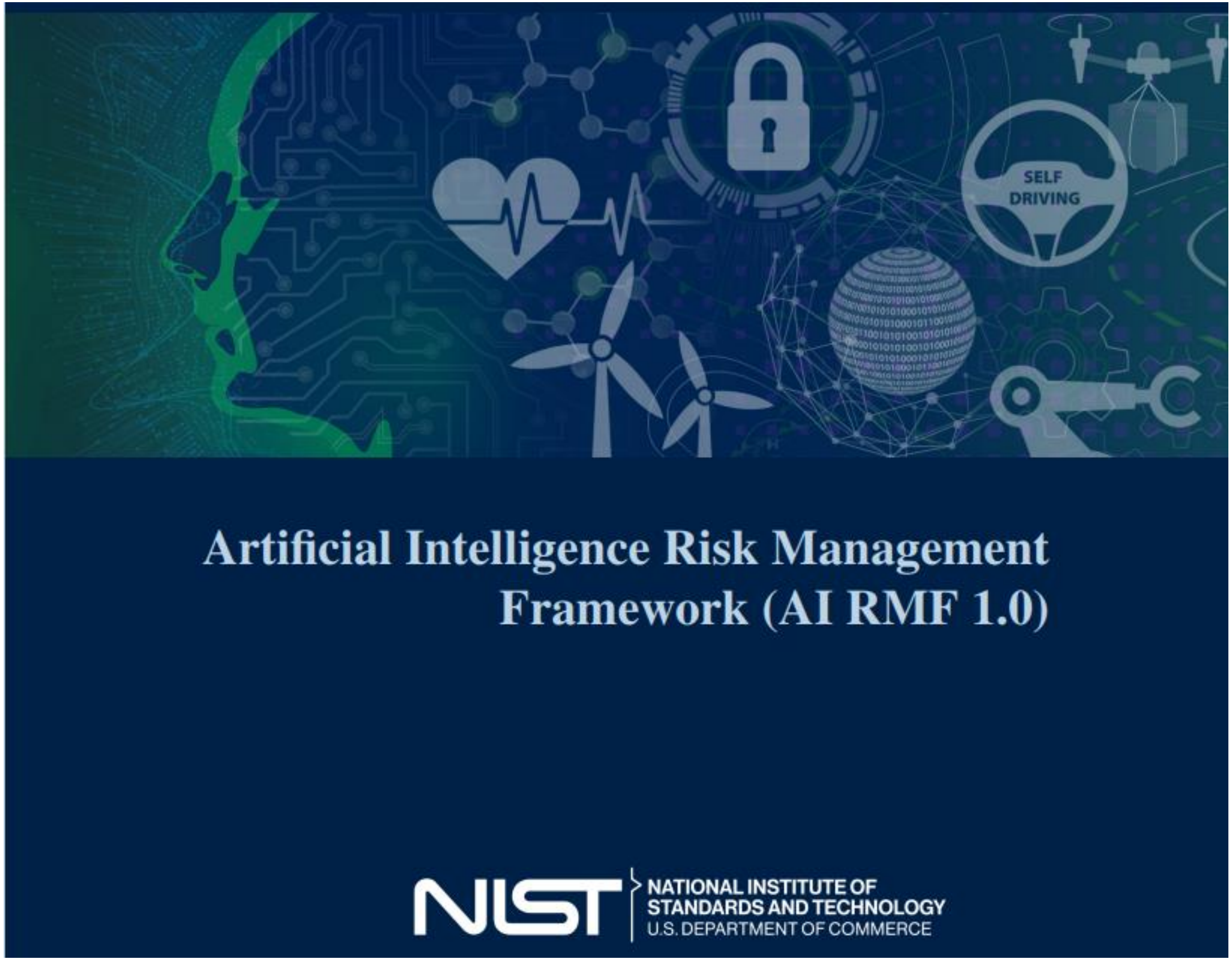


Additional Questions for Vendors That Include AI

- Do you plan to implement AI/ML into your products and services that we purchase through you?
- If so, how will we be notified about those AI/ML components?
- Will we have the ability to opt-in or opt-out?
- Will that AI/ML be self-contained (not accessible to the internet) or internet-facing?
- How will you provide additional security around implementing AI/ML in your products/services?
- How do you plan to test AI/ML in your products/services?

Legal Strategies

- Develop policies and procedures
  - What tools are approved?
  - What are the human checks required on any final deliverables?
- Review Terms and Conditions of the tools you use
  - What are the indemnification and liability limitations?
- Address Generated issues in YOUR service agreements
  - Where applicable
- Avoid inputting business confidential or proprietary information
- Proceed with caution!
- Most of this is not figured out yet.



Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST
NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Google

Complimentary Resources

POSTERS

Click on the image to download your security awareness poster.

Protect Your Digital Footprint

- Think twice before you post anything online
- Never share usernames or passwords
- Look for the "s" in https
- Browse with a protected and updated computer
- Be suspicious of requests and communications

STOP. THINK. CONNECT.

DON'T GET HOOKED

PROTECT YOURSELF FROM PHISHING SCAMS

Security Alert

A hacker may have your password!

- Never use a common password for multiple accounts
- Always use multifactor authentication
- Change your password often
- Never share your password
- Store your passwords securely

Accept

DON'T TAKE THE BAIT!

INFOGRAPHICS

Click on the image below to download the Infographic.

The SBS Risk Management Method

How to make Risk Management be your BEST FRIEND!

1 When it comes to anything new, EVERYTHING should start with the...

RISK ASSESSMENT!

2 Your Risk Assessment needs to help you make...

DECISIONS!

Such as... How do I spend my next...

DOLLAR?

10 Key Ideas to Build a CYBERSECURITY CULTURE

01 START AT THE TOP WITH THE BOARD

02 GIVE CYBERSECURITY A STANDING AGENDA ITEM AT EMPLOYEE MEETINGS

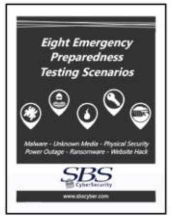
Ransomware Toolkit

ATM Assurance Toolkit

RESOURCE LIBRARY

SBS is your resource for cybersecurity tips, tricks, and best practice guides to help support the cybersecurity culture at your organization. Click the image to download your guide.

FDIC InTREx: What Documentation Are You Expected to Have?


Eight Emergency Preparedness Testing Scenarios

Malware - Unknown Media - Physical Security
Power Outage - Ransomware - Website Hack

www.sbscyber.com

Defense in Depth Checklist Controls

50 Easy-to-Implement Controls to Strengthen Your Security

www.sbscyber.com

50+ Incident Response Preparedness Checklist Items

www.sbscyber.com

34 Unique Ideas to Create a Culture of Cybersecurity

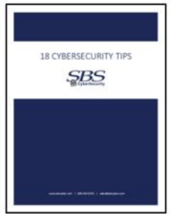
Brought to you by:

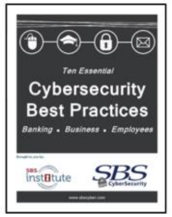
www.sbscyber.com

You Are a Technology Company

Three steps to changing your view

www.sbscyber.com


18 CYBERSECURITY TIPS


Ten Essential Cybersecurity Best Practices

Banking • Business • Employees

www.sbscyber.com

Cybersecurity Starter Toolkit

Cybersecurity Advanced Toolkit

https://sbscyber.com/education/free-downloads

David Edwards

- Regional Director
- CBSM, CBIH, MBA
- 913-225-6382
- David.Edwards@sbsyber.com
- www.sbscyber.com
- linkedin.com/in/david-edwards-076a973/

Follow us on Social:

SBS CyberSecurity