Safe AI Adoption Practices for Government

AI Risks and Countermeasures

Bonus: How to lead AI Projects!

Pete Nicoletti | Global CISO of Americas

Speaker Intro Work Life: Pete Nicoletti

Skills: Executive Level Strategy Consulting, Incident Response, BOD Consulting
Product Management, Cyber Security, MSSP Operations, Security Operations, Security Budgeting

Certs and Training: CCSK, CISA, CISSP, SANS GIAC, FCNSP, CCSE

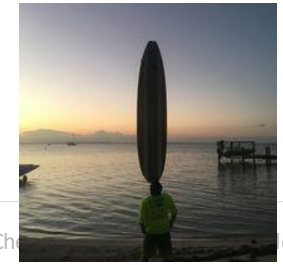
Experience: 22 years at CISO level, 33 years in Information Technology

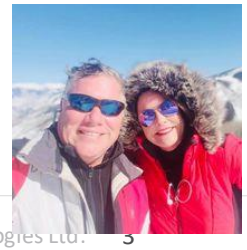
- CISO – Field, Americas Check Point Software Technologies World Leader in Security
- CISO – Cybraics: Artificial Intelligence and Machine Learning Based Analytics Platform
- CISO - Hertz Global Car Rentals and Sales
- CISO - Virtustream/RSA/EMC/DELL
- VP Security Engineering Terremark/Verizon And a proud **MISSION CRITICAL Alumni!**

Accomplishments:

- Gartner's "most secure cloud design" #1 and #2
- Whitehouse.gov, FBI.Gov, DOT.gov, Veterans Administration, Library of Congress and many more Federal Projects
- Managed two clouds through FedRAMP and eventually to EAL 5
- Book Author/Contributor: "An Intel Reference Design for Secure Cloud" "First 90 Days As CISO" "Security Desk Reference: Content Filtering" For Masters in Computer Science Class
- Secret Service - Miami Electronic Crime Task Force, FBI Infragard Contributor, Started S. Florida ISSA, and BOD for Cloud Security Alliance
- Awarded Top 100 Global CISO in 2017

Real Life: Pete Nicoletti





Why am I passionate about this subject?

I was hacked ONCE and *I want help to prevent this:*

"Hi, my name is Brian Krebs

and I would like to

talk to you about your situation"

Agenda For Today!

CISO's and Security Pro's need to have awareness of risks & Benefits:

Risks and Analysis, Benefits and Analysis

Need Guidance and Countermeasures? Here we go!

Some examples of AI tools that are of interest to the Business

How AI used in Check Point security tools

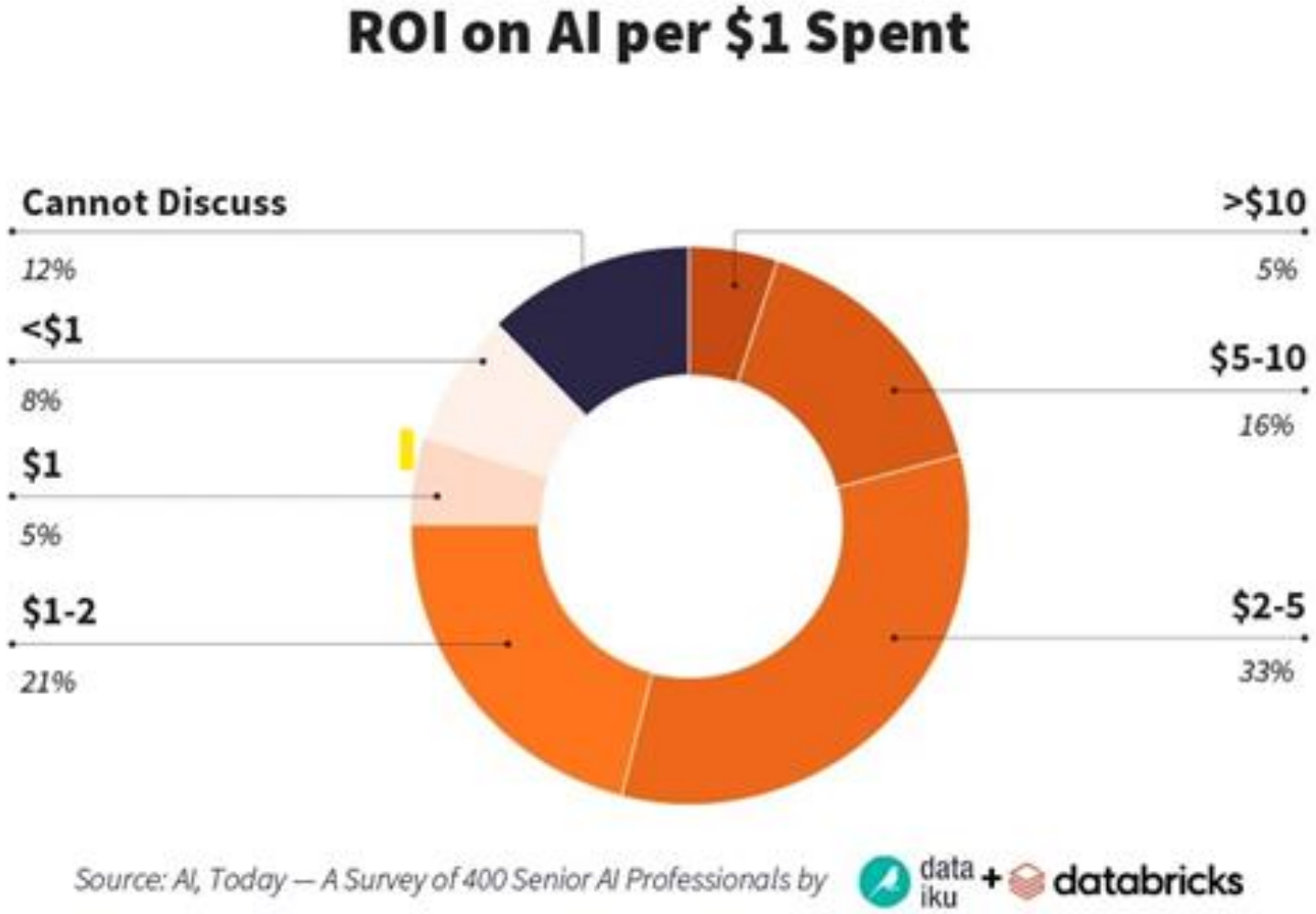
Bonus: Questions to Ask and Plan for AI issues with your Team and Executives

Is the Future "SkyNET" "M3GAN" "I, Robot" or…"J,A.R.V.I.S" ??

The Technology Singularity

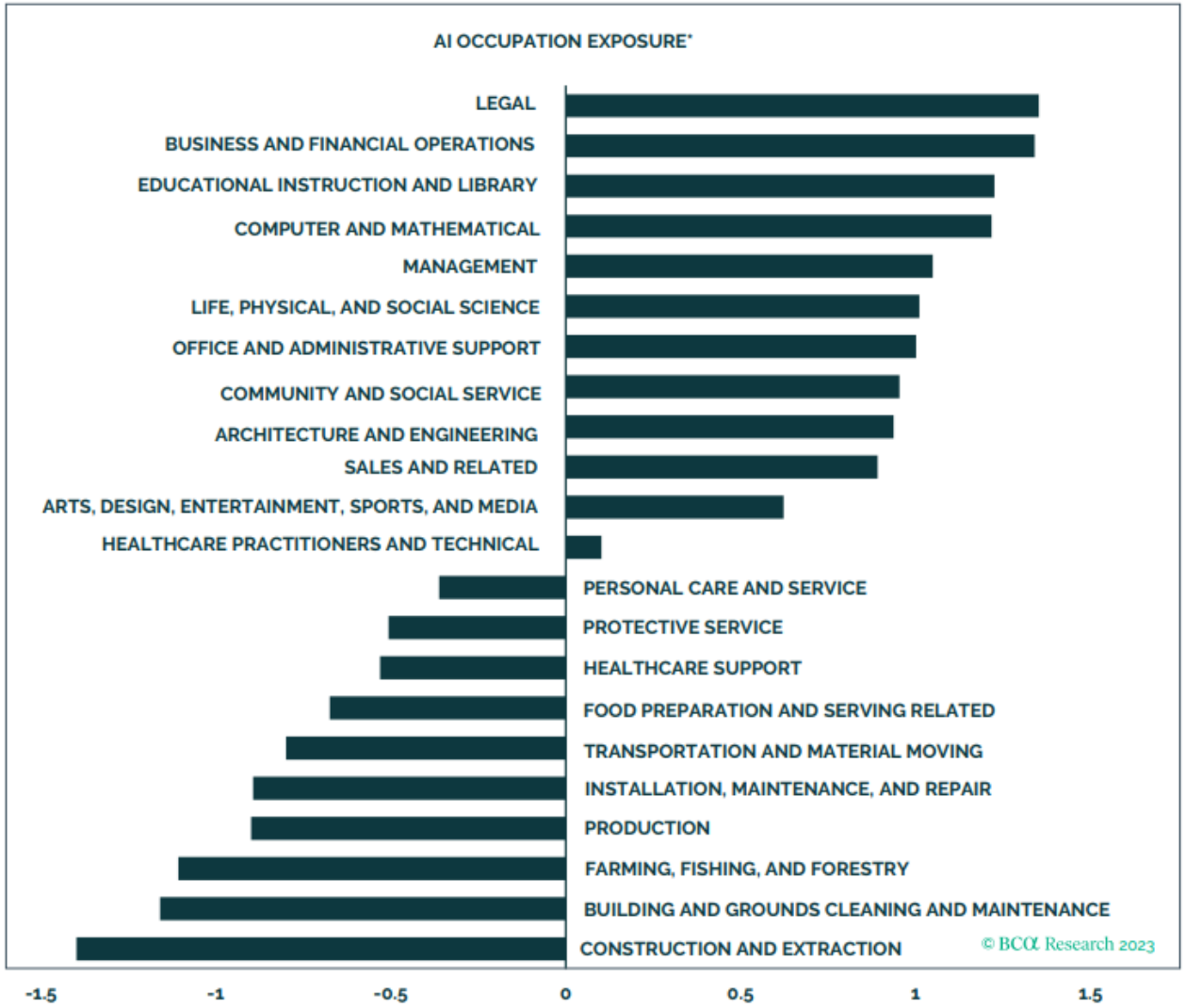
We are here –
A unique point in the history of technology

Start with some good news:
The Business wants ROI on AI Investments: Our Goal!



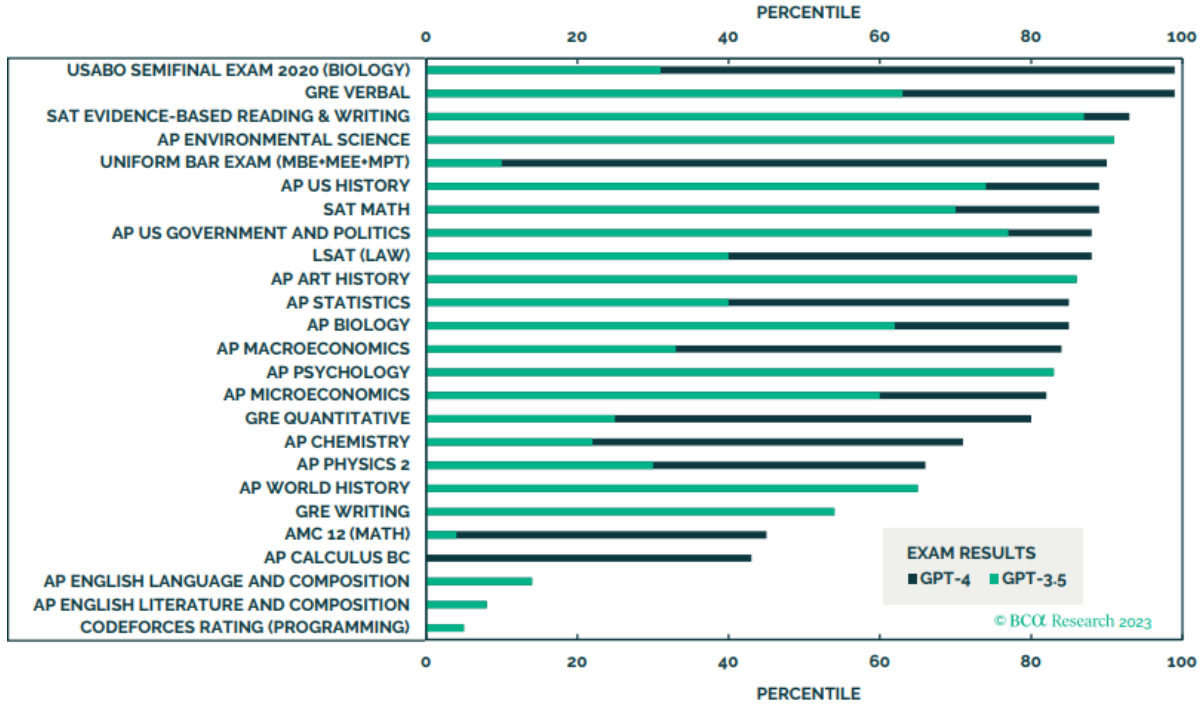
More Good News! Tests they pass, and Lawyers Replaced!

AI Has The Potential To Replace Many Tasks Performed By Humans



* MEDIAN SCORE OF OCCUPATIONS (SIX-DIGIT STANDARD OCCUPATIONAL CLASSIFICATION LEVEL) IN EACH OCCUPATION MAJOR GROUP (TWO-DIGIT STANDARD OCCUPATIONAL CLASSIFICATION LEVEL). CALCULATION USING DATA FROM FELTEN ET AL. (ACCESSED ON MAY 1, 2023).
SOURCE: EDWARD FELTEN, MANAV RAJ, AND ROBERT SEAMANS, "OCCUPATIONAL, INDUSTRY, AND GEOGRAPHIC EXPOSURE TO ARTIFICIAL INTELLIGENCE: A NOVEL DATASET AND ITS POTENTIAL USES," *STRATEGIC MANAGEMENT JOURNAL*, (42:12) (2021).

The Capabilities Of AI Keep Improving



NOTE: LOWER BOUND OF EXAM RESULTS SHOWN. ONLY RESULTS OF EXAMS EXPRESSED AS PERCENTILES SHOWN IN THE CHART. FOR THE FULL LIST OF RESULTS, PLEASE CONSULT THE FOLLOWING REPORT: GPT-4 TECHNICAL REPORT, ARXIV:2303.08774 , ARXIV.ORG, CORNELL UNIVERSITY (MARCH 2023).

Start with Risks and Awareness:

Be Careful…Be Aware…get ready!

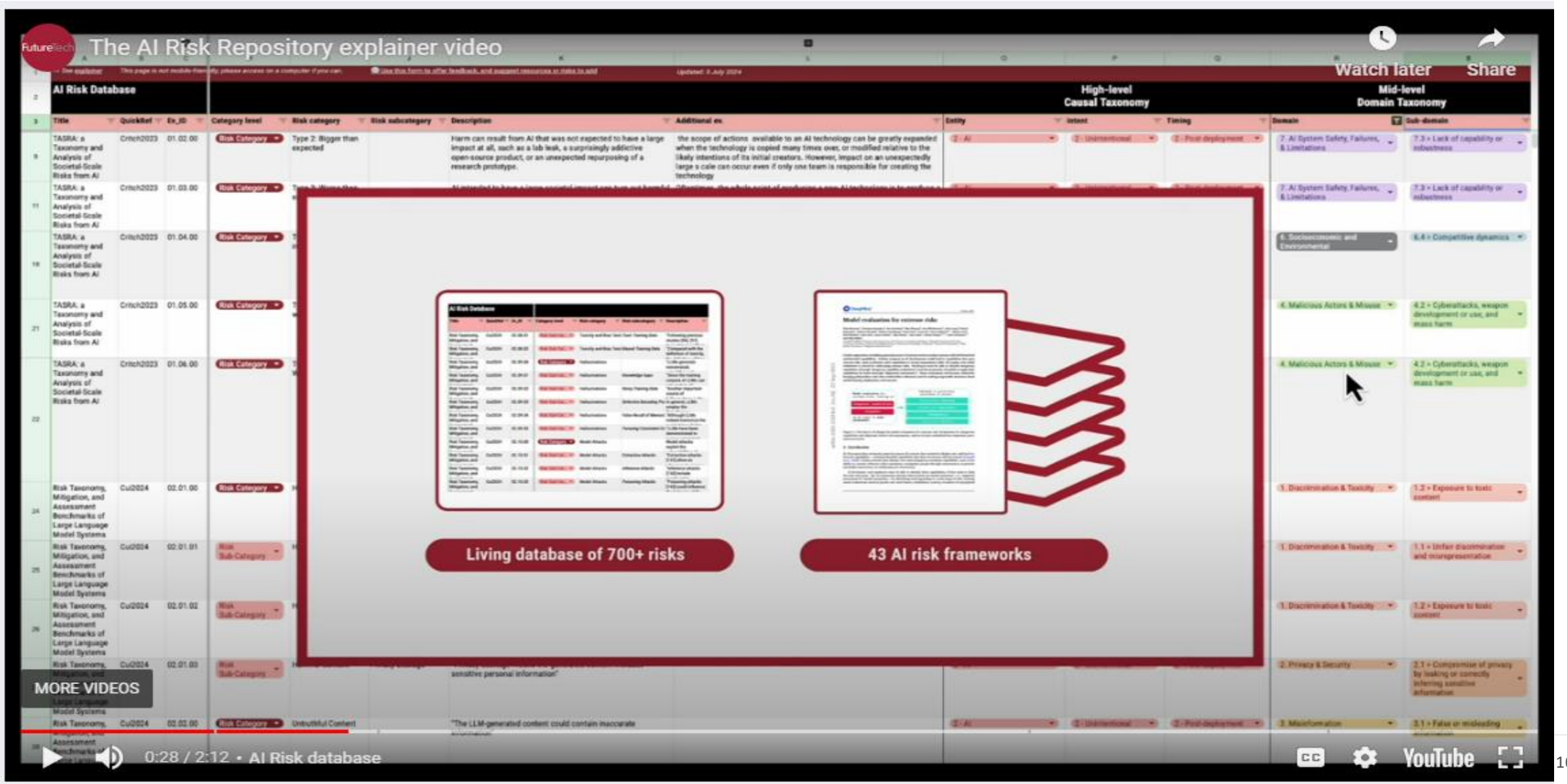
1. **Privacy breaches:** Personal information can be disclosed if language models like ChatGPT are not properly configured to protect privacy. This can result in violations of privacy laws and regulations and can damage the reputation of a company. EU Laws are getting Serious!

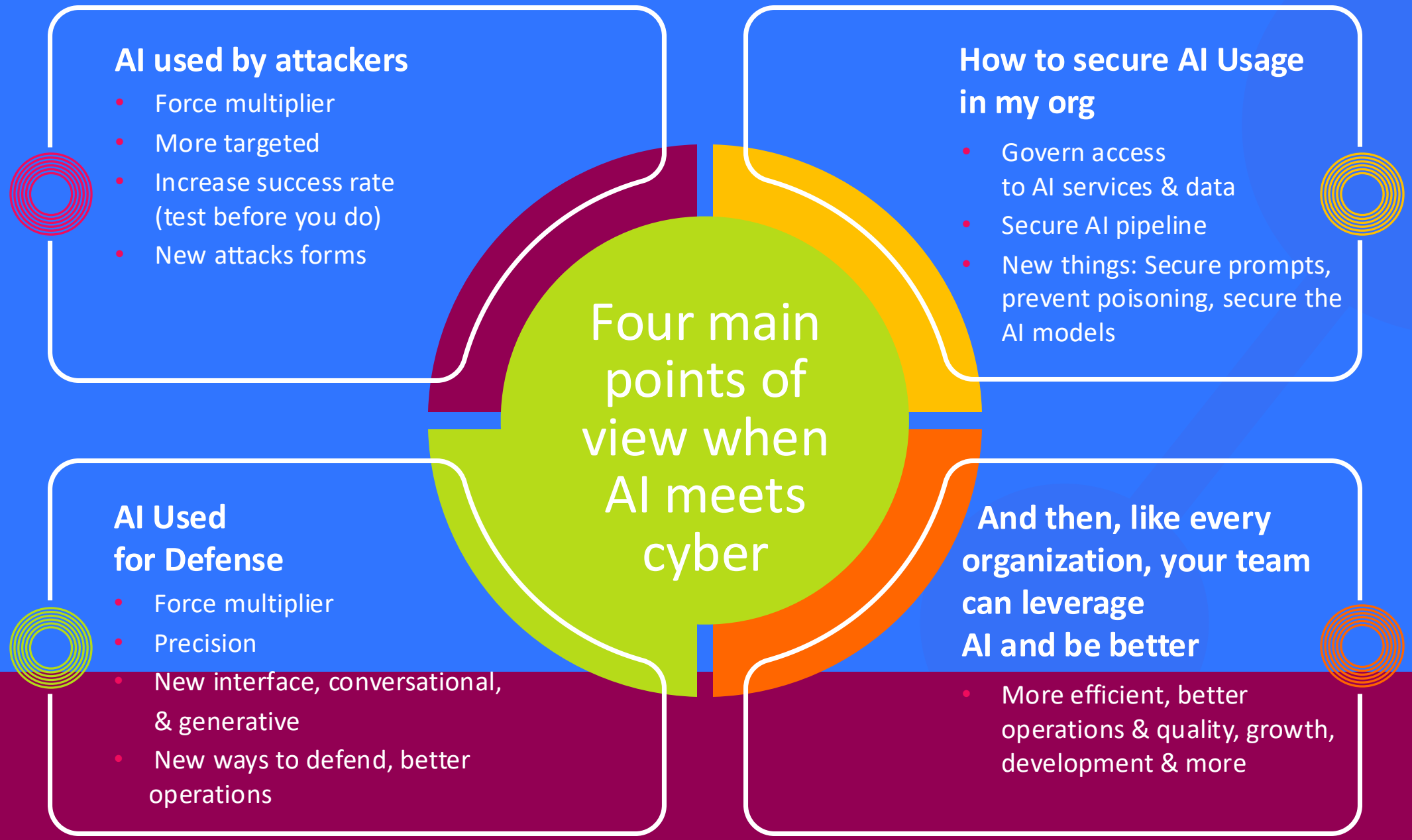
2. Bias and fairness: Language models like ChatGPT can be trained on biased data, which can result in biased outcomes. This can impact decision-making and lead to discrimination and other unfair outcomes. **New AI Risk: Hallucinations!**

3. **Misinformation:** Language models like ChatGPT can produce incorrect or misleading information, which can have negative consequences, such as spreading false information, making incorrect decisions, and damaging a company's reputation.

4. **Some Models are using dated information**

The Biggest AI Risk Database: 700+ risks, 43 Frameworks
MIT's AI Risk Repository https://airisk.mit.edu/#Repository-Overview





BATTLE OF THE AI (SHORT LIST)

DEFENDER

Check Point has 72 different AI threat engines in prevention first architecture with ThreatCloud (IOC/TTP data lake)

Effective and efficient for Malware DNA genotyping and analysis

Helps SOC analysts see attack vectors and landscape

Help write good software code

Fix bugs in source code

Auto-write cybersecurity policies and controls based on GRC framework(s)

Gamify cybersecurity training

created with DALL-E

ADVERSARY

Check Point Research saw instances of 5 major attacks created by ChatGPT since its inception

Create Deepfakes and bots

Malware writing for dummies (joke)

Phishing email creation for dummies (again a joke)

Easy to identify attack landscape based on vulnerabilities and find exploits to match (multiphased attacks)

Circumvent AI ethics of GPT-3 by using API with Telegram or other software integration

Risks and Consequences:

1. Samsung workers made a major error by using ChatGPT
Samsung meeting notes and new source code are now in the wild after being leaked in ChatGPT

Data leaks need to stop: Sensitive information such as confidential business information, code, customer data, and personal information can be leaked.

2. ChatGPT: Exploited twice: The exploit came via a vulnerability in the Redis open-source library. This allowed users to see the chat history of other active users.

Open-source libraries are used "to develop dynamic interfaces by storing readily accessible and frequently used routines and resources, such as classes, configuration data, documentation, help data, message templates, pre-written code and subroutines, type specifications and values," according to a definition from Heavy.AI. OpenAI uses Redis to cache user information for faster recall and access. Because thousands of contributors develop and access open-source code, it's easy for vulnerabilities to open up and go unnoticed. Threat actors know that which is why attacks on open-source libraries have increased by 742% since 2019.

Risks and Awareness:

How are Hackers using AI?

1. Phishing: Combining Hacked information and Social Network info

2. Code Creation: Easy upgrades to Python

3. Online Profile Creation: (Vid Con IRL!!!)

4. Photos: Creation and Animation

5. Videos and voice-overs are trivial to create

More Risks and Awareness:

1. Helps write crafted attacks to steal information and deliver ransomware
2. Conduct financial fraud, financial extortion, steal cryptocurrency (crypto wallets)
3. This means Lowering the bar for lower-level cybercriminals, and upping the game for advanced criminals
4. With training it can mimic the writing style/Video of an executive and craft super targeted phishing attacks
5. ChatGPT created Code can do it all: It can find target files, create Zip file and encryption processes easily. It can create new code that has not been seen before. Right now, they are sorta basic, but advances and sophistication are coming!

Benefits and Awareness:

1. **Improved policies.** We can ask ChatGPT to help us improve our security policies. And it's amazing. It's just staggering. And it's very nice. For example, I could ask, "Please give me an updated policy for data governance" and boom, less than five seconds later, you have a complete, new, updated data policy.

2. **Communications.** I can ask ChatGPT 'Please help me to write a communication to our users, explaining X, Y and Z'. I can even ask ChatGPT to explain it in a way that a 12 year-old boy would understand. And ChatGPT will do it. Or if I want to try to explain the latest phishing campaign to my mother, ChatGPT will put the right language together. You get the idea.

3. **Legal Reviews:** have ChatGPT analyze a contract and compare to best practices

4. **Insurance Policy Analysis:** some awesome finding reported

5. **PYTHON Code** creation and improvement

5. Bonus: Love Poems!

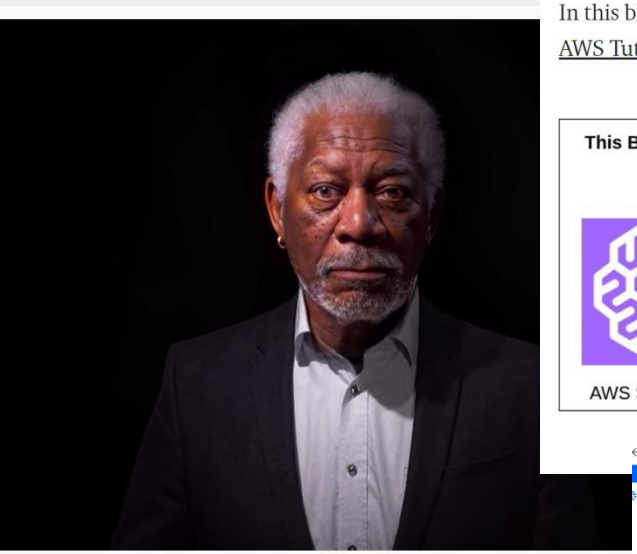
DEEPFAKES, VOICEFAKES, NEWSFAKES, SOCIAL ENGINEERING BOTS

DEEPFAKES, VOICEFAKES, NEWSFAKES, AND BOTS

A nonspeaking valedictorian with autism gives her college's commencement speech

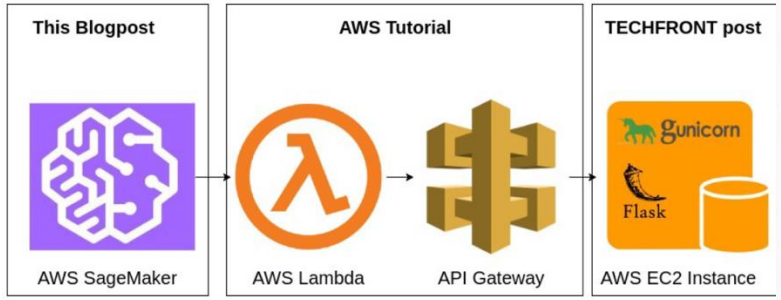
May 12, 2022 · 2:44 PM ET

BILL CHAPPELL



Morgan Freeman - A Deepfake Singularity

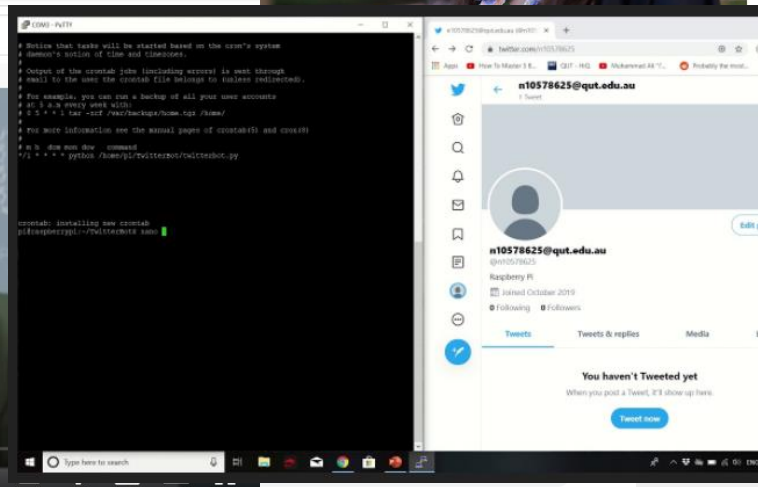
In this blogpost, we will cover the first task in detail. Two others are covered in AWS Tutorial, TECHFRONT post. The final architecture will look like this:

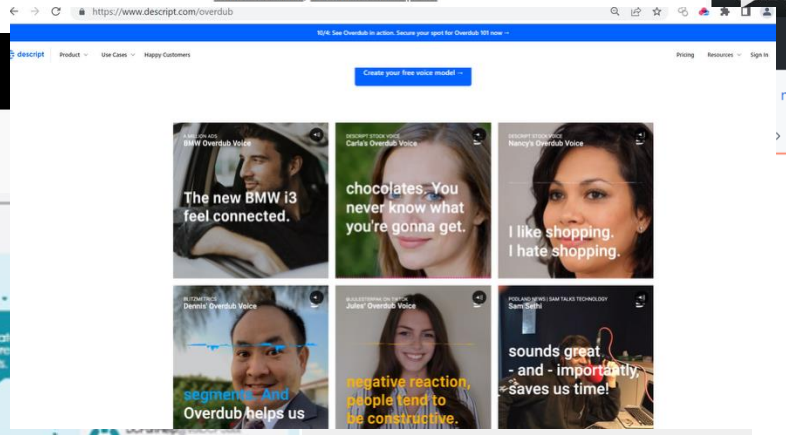


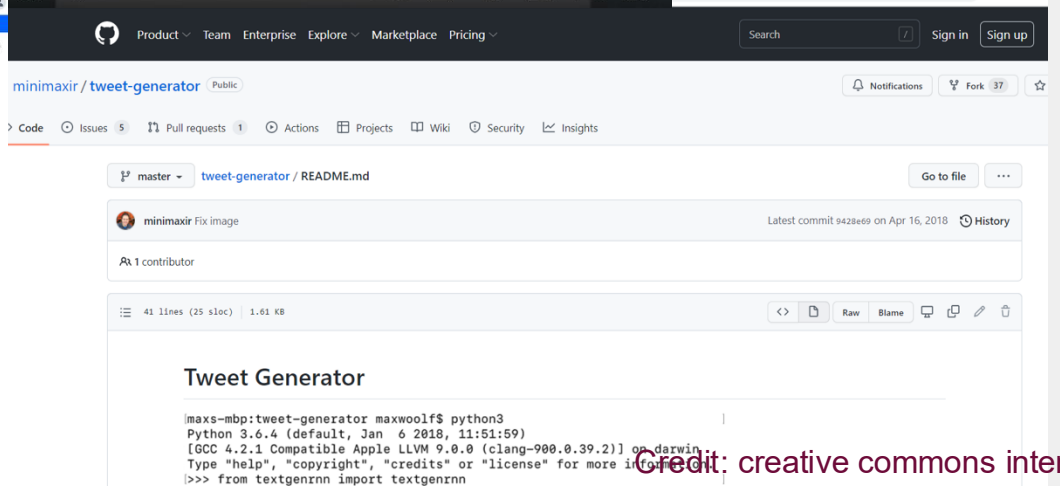
AWS Tutorial, TECHFRONT post

youtube.com/watch?v=X17yrEV5sl4

YouTube Search







Credit: creative commons internet

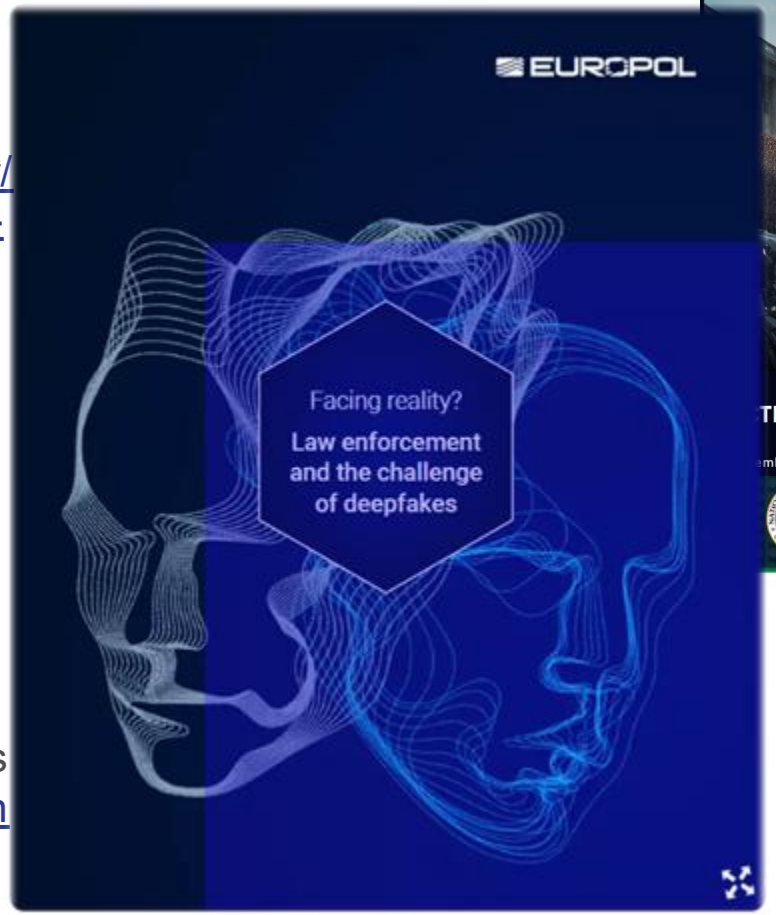
DEEPFAKE WARNINGS & CRIMES

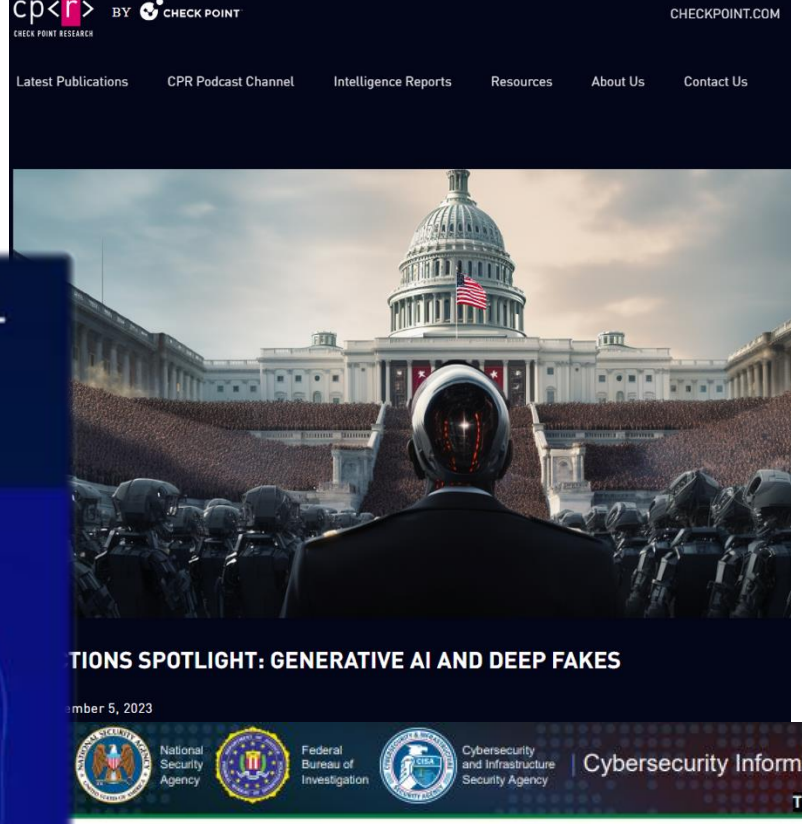
CEO impersonation for financial fraud
https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=1a968bc27559

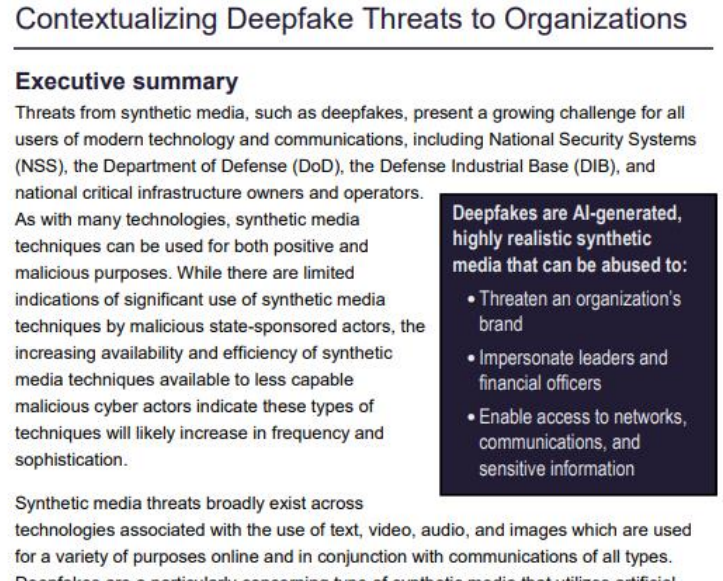
Europol warning use in organized crime
https://www.europol.europa.eu/media-press/newsroom/news/europol-report-finds-deepfake-technology-could-become-staple-tool-for-organised-crime

Check Point Research on GAI and Deepfakes
https://research.checkpoint.com/2023/elections-spotlight-generative-ai-and-deep-fakes/

CISA
https://media.defense.gov/2023/Sep/12/2003298925/-1/-1/0/CSI-DEEPFAKE-THREATS.PDF







Contextualizing Deepfake Threats to Organizations

Executive summary

Threats from synthetic media, such as deepfakes, present a growing challenge for all users of modern technology and communications, including National Security Systems (NSS), the Department of Defense (DoD), the Defense Industrial Base (DIB), and national critical infrastructure owners and operators. As with many technologies, synthetic media techniques can be used for both positive and malicious purposes. While there are limited indications of significant use of synthetic media techniques by malicious state-sponsored actors, the increasing availability and efficiency of synthetic media techniques available to less capable malicious cyber actors indicate these types of techniques will likely increase in frequency and sophistication.

Deepfakes are AI-generated, highly realistic synthetic media that can be abused to:

- Threaten an organization's brand
- Impersonate leaders and financial officers
- Enable access to networks, communications, and sensitive information

Synthetic media threats broadly exist across technologies associated with the use of text, video, audio, and images which are used for a variety of purposes online and in conjunction with communications of all types.

Deep Fake Creation Getting Easier and Evolving:

What are the common techniques used to create deepfakes and how are they evolving?

With just a simple search, you can find lists of reviewed and rated apps:

https://contentmavericks.com/best-deepfake-software/
https://www.rankred.com/best-deepfake-apps-tools/
https://topten.ai/deepfake-app-and-software-review/
https://zapier.com/blog/best-ai-image-generator/

Some of the review sites are undoubtedly getting referral money for ones they rank higher, so be aware of that bias.

Most of the tools are trying to be legitimate and use customer-provided pictures and video's of only themselves. Other tools let you use other folks' pictures and videos with an approval process that is easy to get around. Companies based outside of US has much lower requirements (FaceApp by Wireless Lab in Russia for example). ***And DARK WEB Offerings are Hot now!***

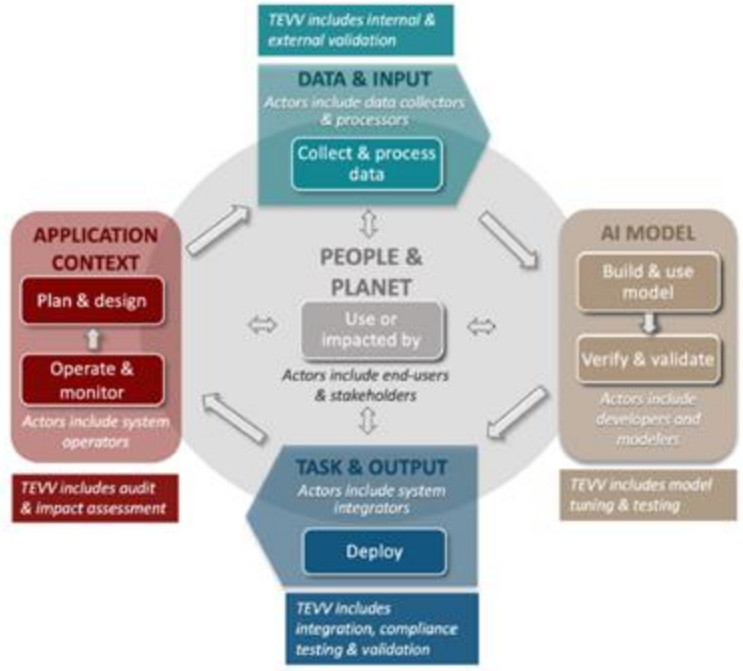
There are apps for Android, Apple and laptops (linux, Apple, MS) that have different features.
Some tools require you to upload voice examples, others you can select a stock voice.

In the past 6 months, there has been incredible developments in this area. Some tools are super easy to use and have limited outputs, other tools you need to learn a bit more and have very advanced output.

Good Guidance is Available…Review It:

CISO's need to review and embrace the significant amount of good guidance that has recently been released. NIST just released the "AI Risk Management Framework" The AI Risk Management Framework (AI RMF) is intended for voluntary use and to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems.
It has all the appropriate steps that CISO's can use: Framing the Risk, your Audience, AI Risks and Trustworthiness, Effectiveness of the Benefits, the Risk Management Core that describes "Govern, Map, Measure, and Manage" and describes the Risk Management Profiles

Found Here: https://www.nist.gov/itl/ai-risk-management-framework



Counter Measures!:

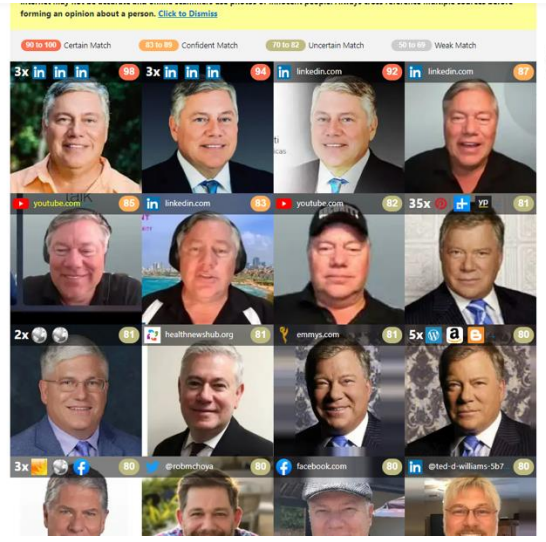
1. **Examine the Pictures used in the profile is using and submit to** www.facecheck.id (Mine pops up William Shatner!) There are many cases where the person is already married, or has an arrest record, or the picture is not from the person who created the profile. 417 million pictures are on line, from Mugshots to good pictures! (I snapped my results and added to research below!)

2. **Most AI Based Text creation tools have No Awareness of Current Events**, as their data used is typically several years old, ask it questions related to new news events to spot an AI based chat

3. **Currently you Can't see back of head in pictures or Video's:** Ask the "person" or thing talking to you to turn around and if they can't… you are done!

4. Have good tools in place to prevent SMS and Phishing scam emails and texts, most companies have, but end-users do not. Free tool: https://www.zonealarm.com/

5. Unless you have Harmony Email: Never click on the links provided by phishing or profile creators…



How can organizations protect themselves against the potential risks of deepfakes?

1. For money transfers or account changes, use multiple people for authorization, during or after call/zoom do a follow up call/email to validate the transaction.

2. When you get money request/gift card request/weird call/SMS/email… Drop the call and call the person Directly!

3. Configure your email system to Banner/Label emails/zoom invites coming from external addresses.

4. Use the most advanced Email Phishing prevention tools

5. Leverage advanced Endpoint tools that prevent malicious code execution and deployment.

6. Use Out of out-of-band verbal passwords to validate anything important.

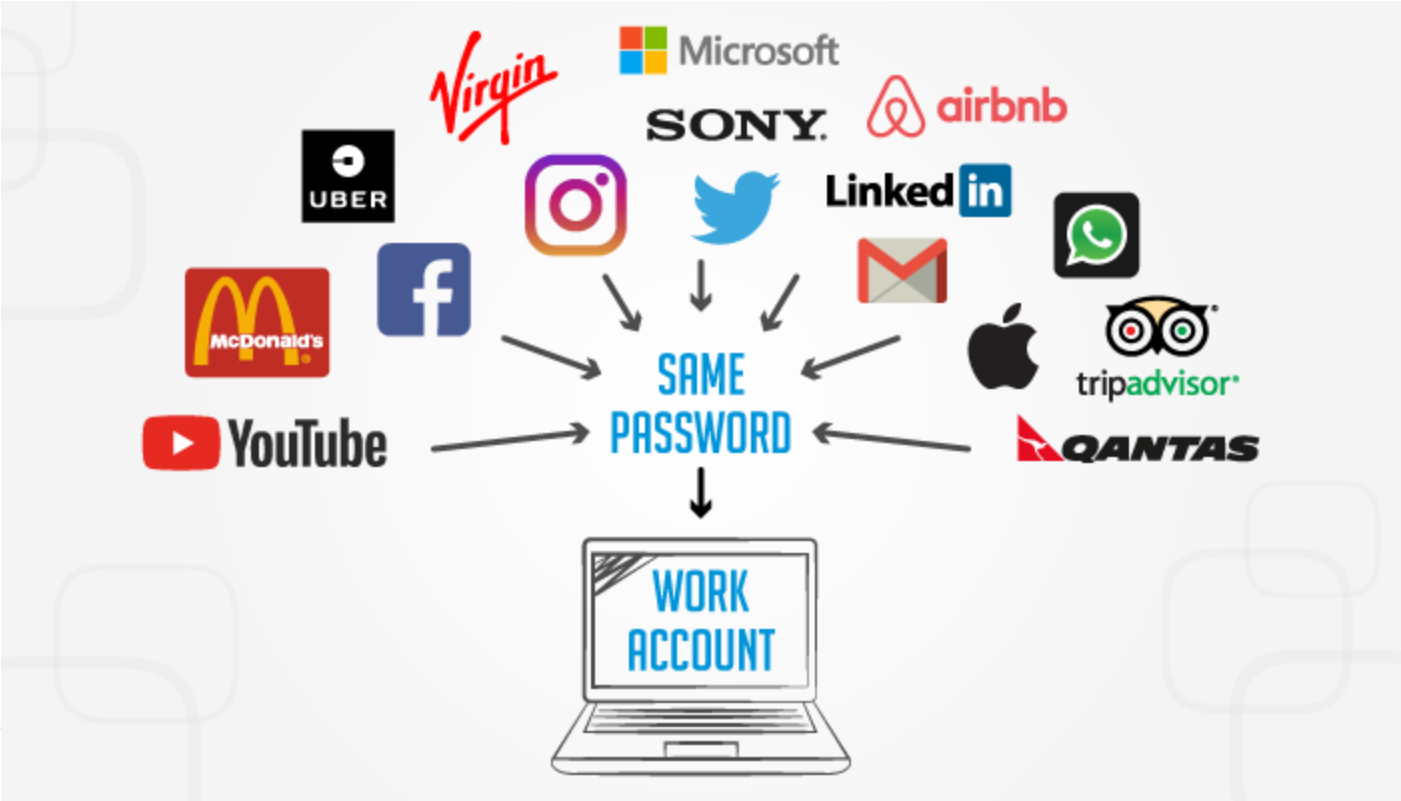
7. Use your Spider senses!!!!! Talk with your team and employees. Have a go-to expert!

More Counter Measures!:

1. **Don’t re-use passwords.** If you use the same password to log into one of their scams, they will take the email address AND the password you just used and try to log into THOUSANDS of other www sites to see where it will work! Always use a unique password for every site. Check out: www.haveibeenpwned.com to see what website you use have been compromised!

2. **Conversations are typically brief**, long AI based conversations currently devolve a bit.

3. **Online Profiles, may use fake information,** or not a real person behind it: If there is real interest in a person, do a video based FTF call, no filters or back grounds! If who you are dealing with can’t do that… RUN!!!



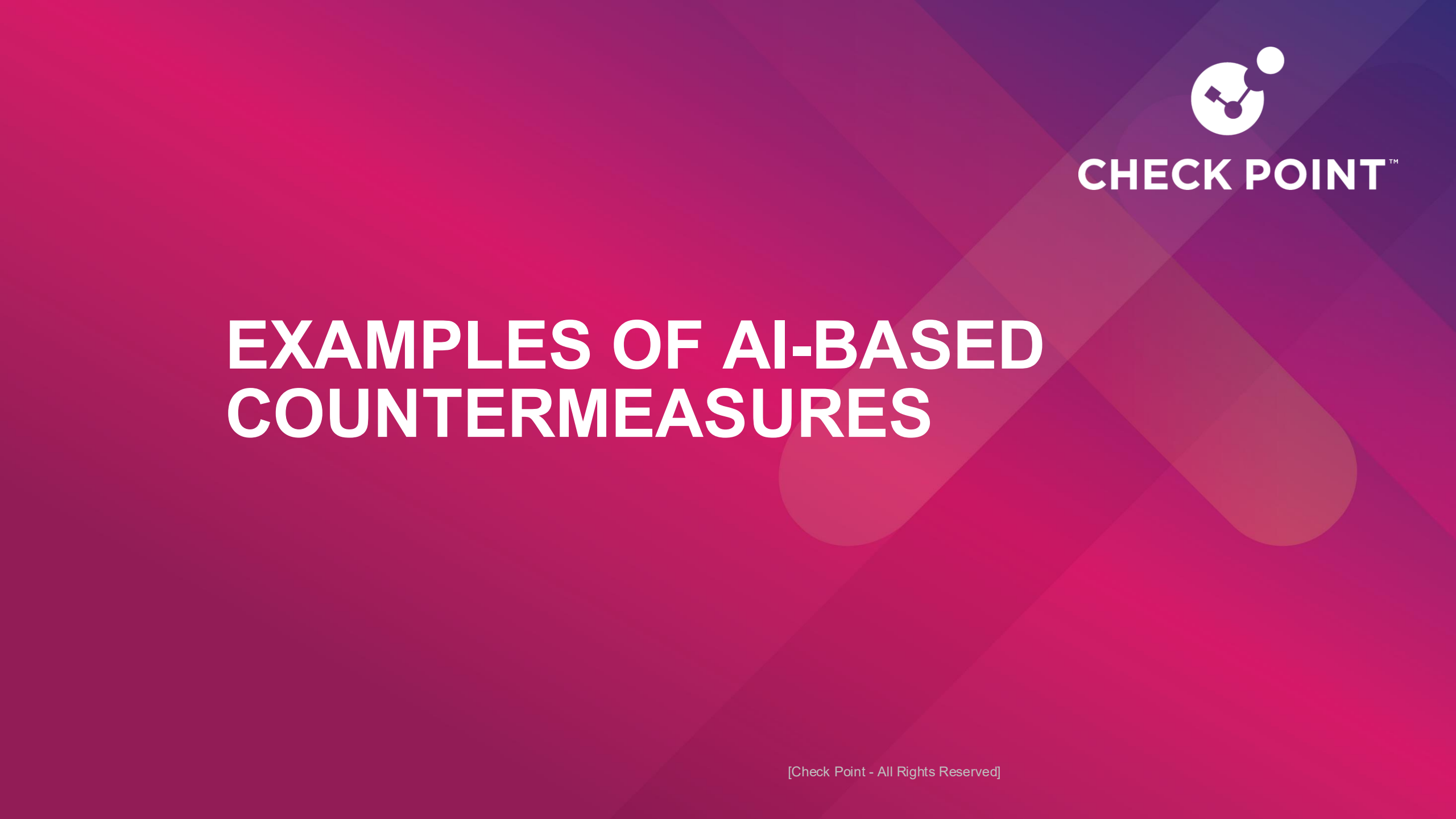
The Business is Using AI Based Tools, You should know!

1. Meeting BOT's powered by AI:
   https://otter.ai/
   https://www.makeuseof.com/best-ai-meeting-a

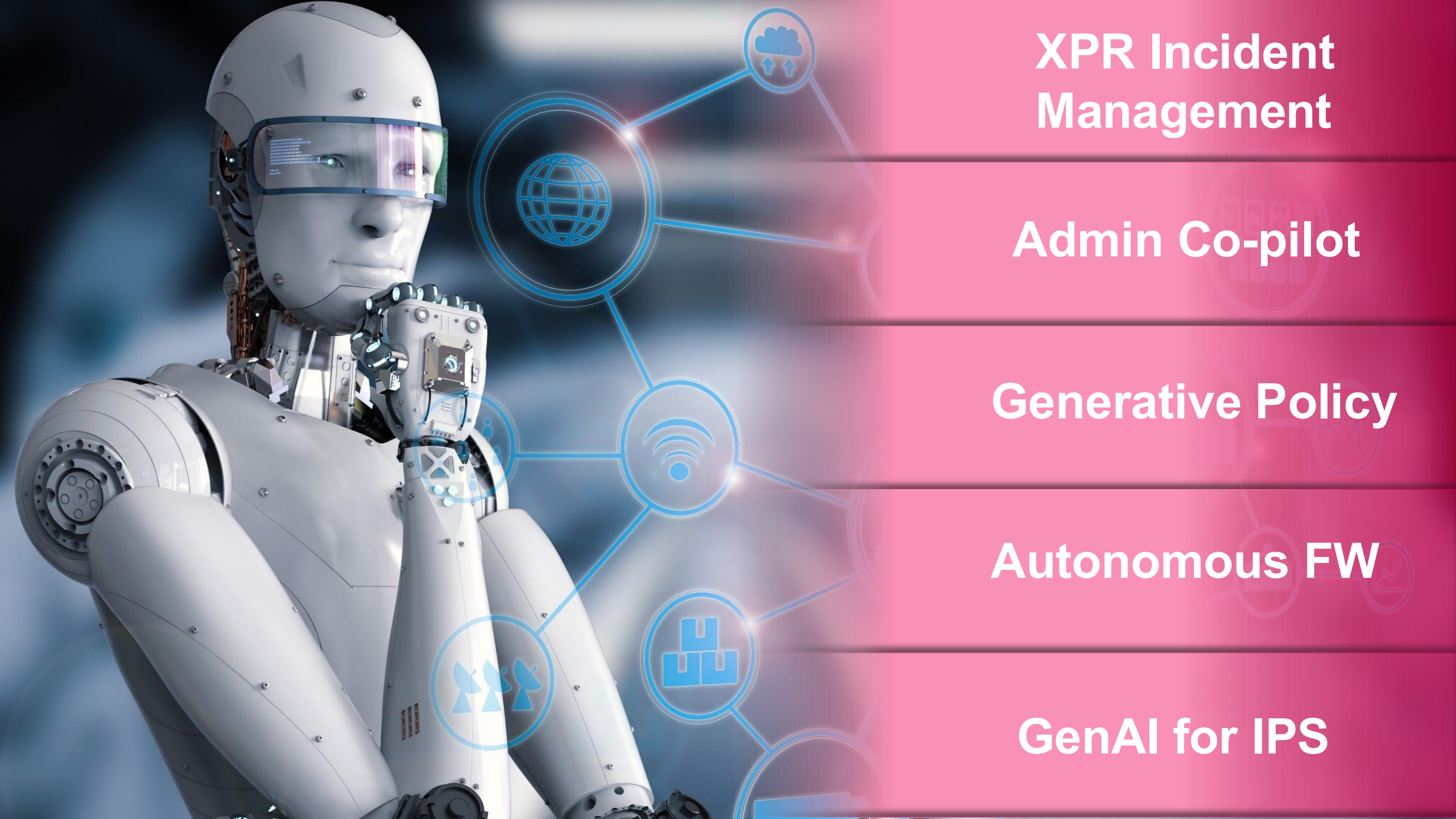
WARNING: DO NOT HAVE A MEETING WITH JUST AI MEETING BOTS!

2. Neat developments:
   AI powered Smart Glasses:
https://www.popularmechanics.com/technology/gadgets/a43633762/chatgpt-smart-glasses/

3. https://www.forbes.com/sites/bernardmarr/2023/05/10/15-amazing-re
of-ai-everyone-should-know-about/?sh=2908fb6885e8



EXAMPLES OF AI-BASED COUNTERMEASURES



XPR Incident Management

Admin Co-pilot

Generative Policy

Autonomous FW

GenAI for IPS

AI is Powering Better Security

AI-Powered Threat Prevention

AI-Powered Assistant for Admins & Security Analysts

Protect AI Servers

Enable Safe GenAI usage

ThreatCloud AI

50+ Threat Prevention Engines for 99.8% malware catch rate
Real-time Threat Intelligence

AI Copilot

Saves up to 90% of the time needed to perform common administration tasks
Accelerates SecOps threat hunting, analysis and automated response.

Copilot for S1-Cloud – Preview in Q1
Copilot for XDR - GA in Q3

AI Cloud Protect

Nvidia partnership to protect AI cloud infrastructure used by enterprises for their own AI apps

Preview Q2/Q3
GA in Q4

GenAI Security

Enables safe adoption of GenAI in the enterprise; delivers discovery, risk insights, data protection in real time

Preview in Q3

CHECK POINT

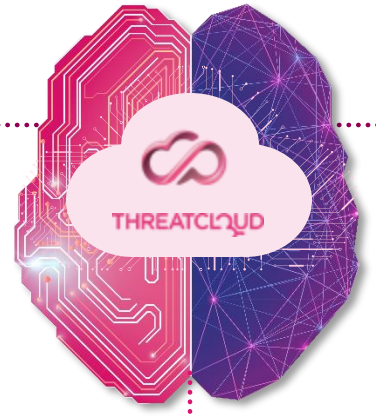
*Roadmap dates are subject to change

THREATCLOUD AI: THE BRAIN OF CHECK POINT CYBERSECURITY

99.7%
Security effectiveness
BEST RESULT IN THE INDUSTRY**

AI technology

40+ AI and Machine Learning technologies that identify and block emerging threats that were never seen before



Big data threat intelligence

Always acquires the most recent IoCs and protections of latest attacks seen in the wild

Telemetry

ACCURATE PREVENTION
(MALICIOUS/SAFE)

Telemetry

ThreatCloud APIs

Quantum
Secure the Network

CloudGuard
Secure the Cloud

Harmony
Secure Users & Access

Horizon
Unified Management & Security Operations

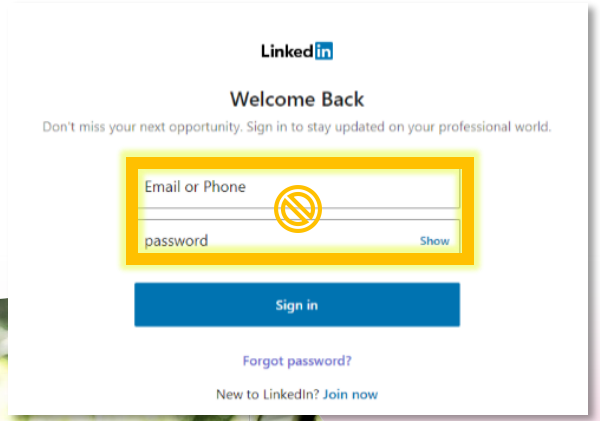
*Source – Miercom January 2023

ZERO-DAY PHISHING BLOCKED – IN REAL TIME

PATENTED

Quantum Gateway prevents credential theft in-line, for all browser types

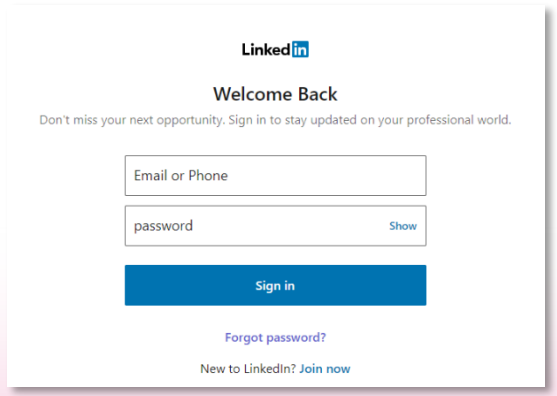
PREVENT CREDENTIALS THEFT
NO CLIENT SOFTWARE NEEDED

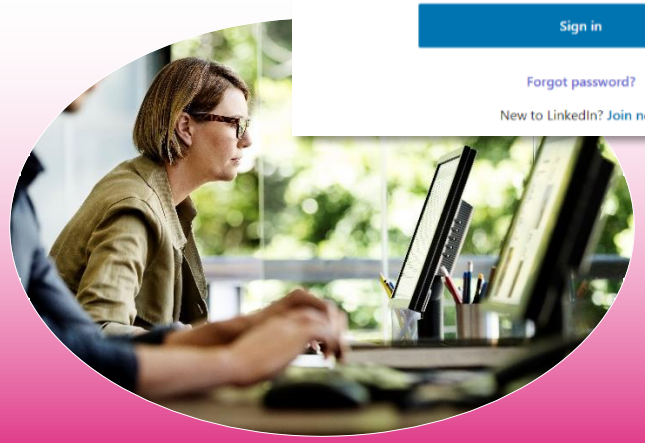


4x

 # Blocked new phishing pages

NEWLY SEEN PHISHING SITE





Firewall Provides in-line Protection

Generative AI Apps accelerate your business

But they put your business data and compliance at risk

New GenAI apps introduced daily; not all are trusted

Users' prompts may contain sensitive business data

New regulations demand more visibility and control

Where do you even begin?

*As a start we just blocked ChatGPT. Now, **executives ask to enable AI safely, but we're not sure how**.*

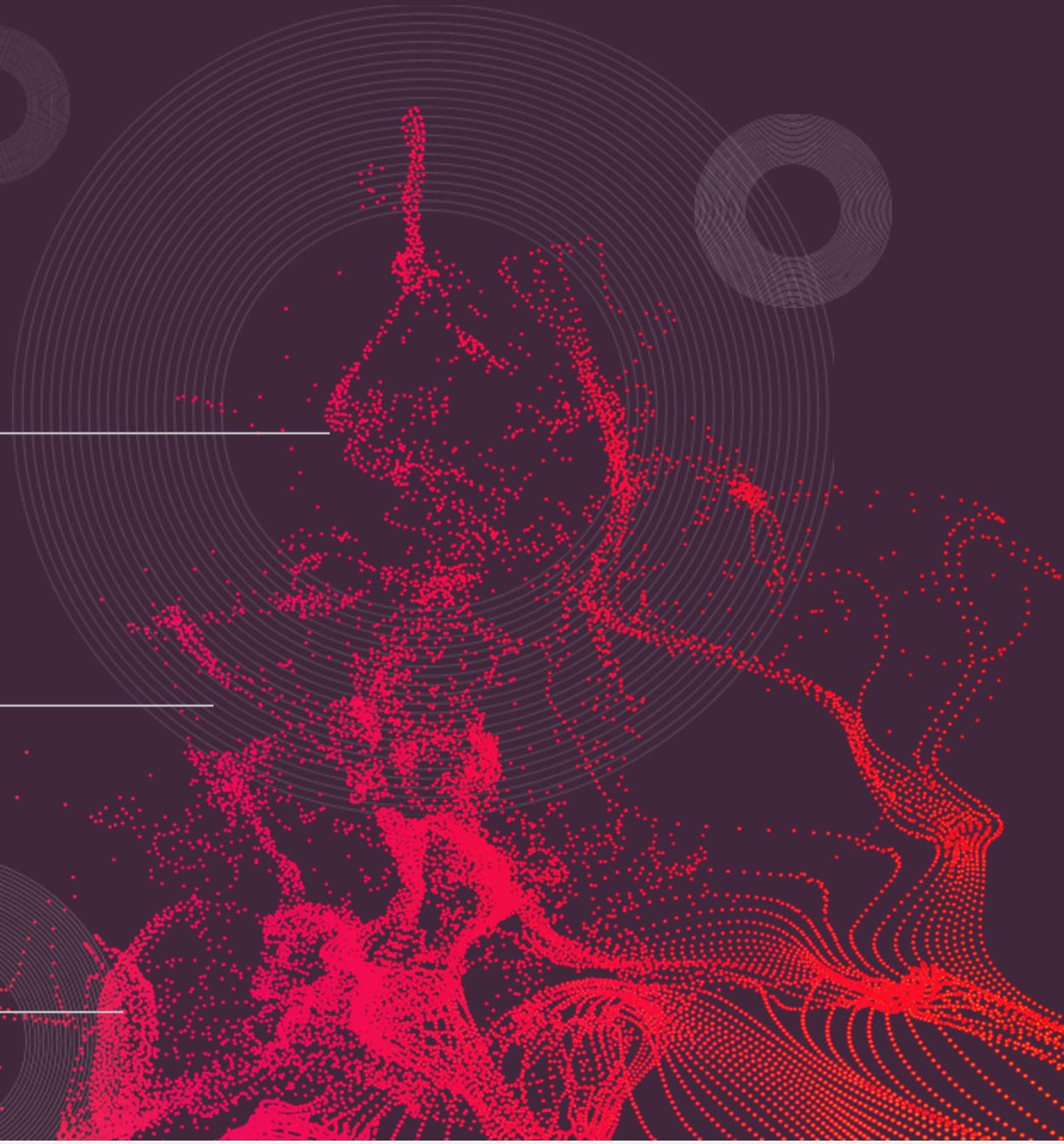
CISO, Consulting Firm, Europe

*I simply don't have a clue what users do. **It all happened so fast**.*

Senior Infrastructure Specialist, International Freight, EMEA

*Executives ask me to **report the risks of GenAI apps**. They are worried about regulation.*

CISO, Healthcare System, US



Conventional solutions are not enough

- Conventional DLP solutions are based on keywords and patterns (“regex”)
- Prompts are conversational; may contain sensitive data that is unstructured
- Understanding data context is key to determining if shared data is confidential

You need GenAI to protect against GenAI risks

To enable AI safely, you need to:

Discover and assess the risk of GenAI usage

Prevent loss of data to GenAI apps

Ensure visibility to meet regulations

Introducing
Check Point GenAI Security

Discover and assess risk of GenAI usage

See GenAI tools used in your organization, their purpose and risk

Meet regulations with enterprise-grade visibility and reporting

Get granular monitoring and audit trail to facilitate regulatory compliance

Prevent data loss in real time using AI

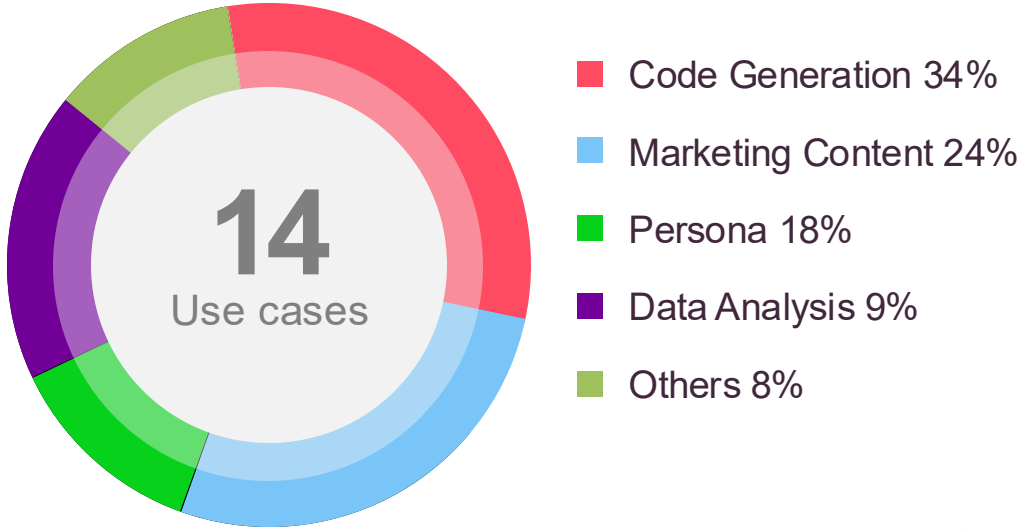
Reduce the risk of data leakage with AI-based data classification engine

Discover your GenAI apps

Sanctioned and shadow GenAI apps

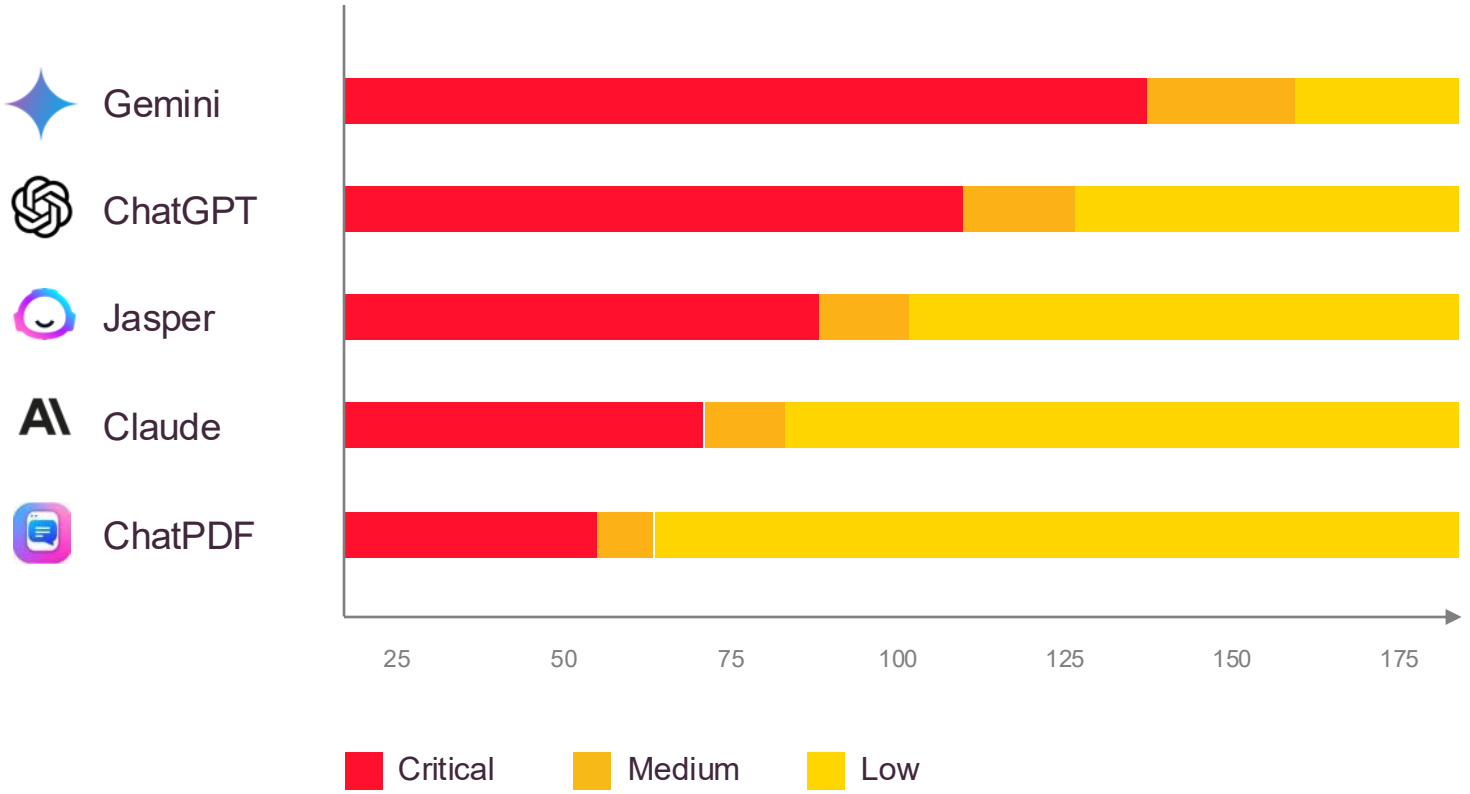
App Name	Risk	Sessions	Users
Gemini	Low	6,433	3,045
ChatGPT	Low	4,600	2,258
Poe	High	1,565	690

Top GenAI app use cases



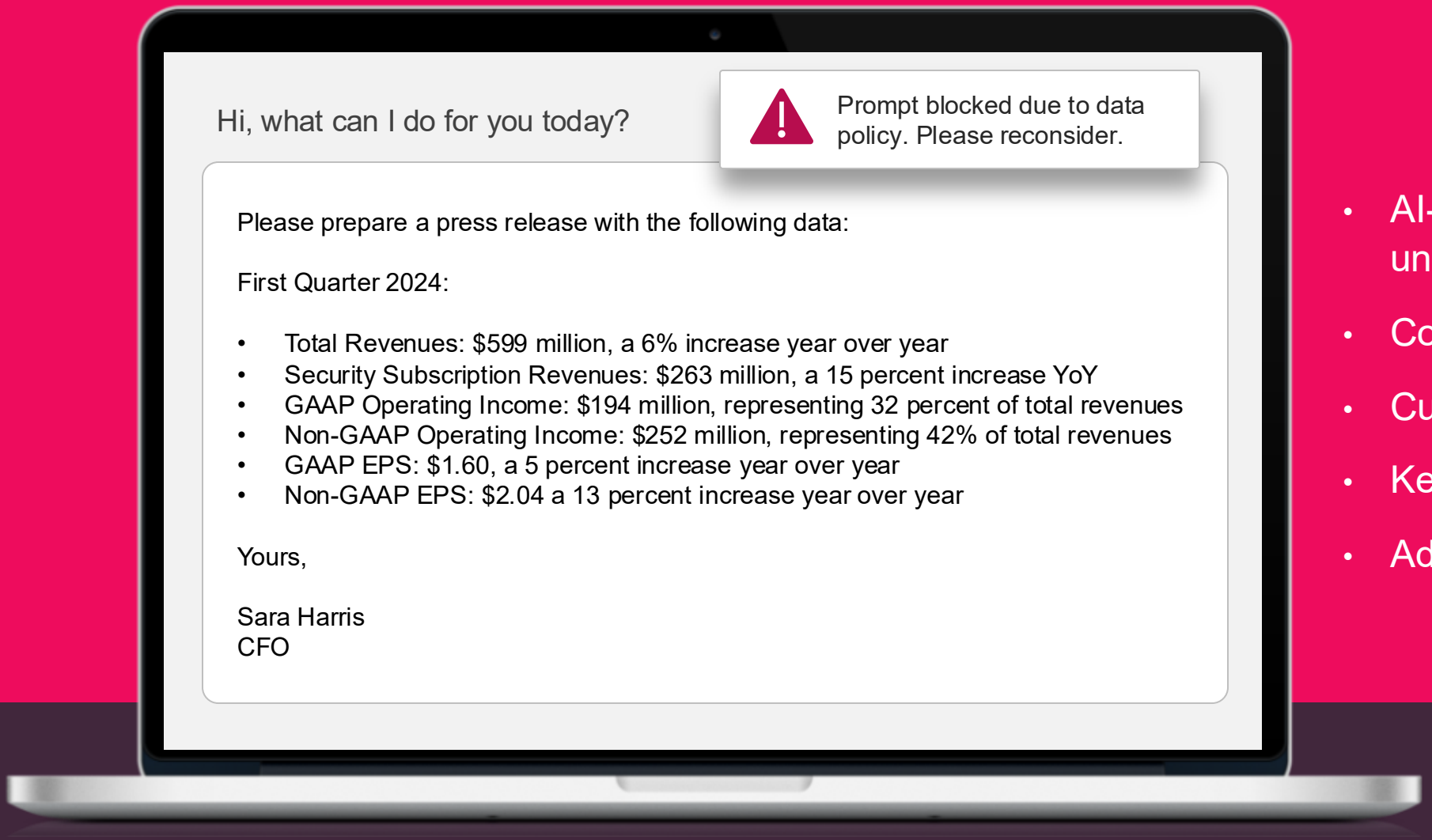
Get Insights and Assess Risk

App Session Breakdown



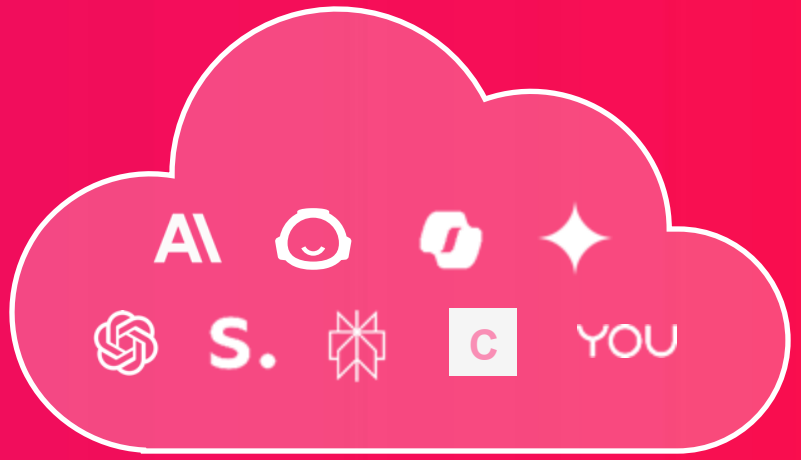
- Uncover GenAI usage, including shadow services
- Discover if your data is being used to train GenAI tools
- See prompts containing sensitive data
- Uncover data lineage of data copied into prompts
- Risky activity at the app and session level
- Risk score to prioritize mitigation

Prevent Data Loss in Real Time



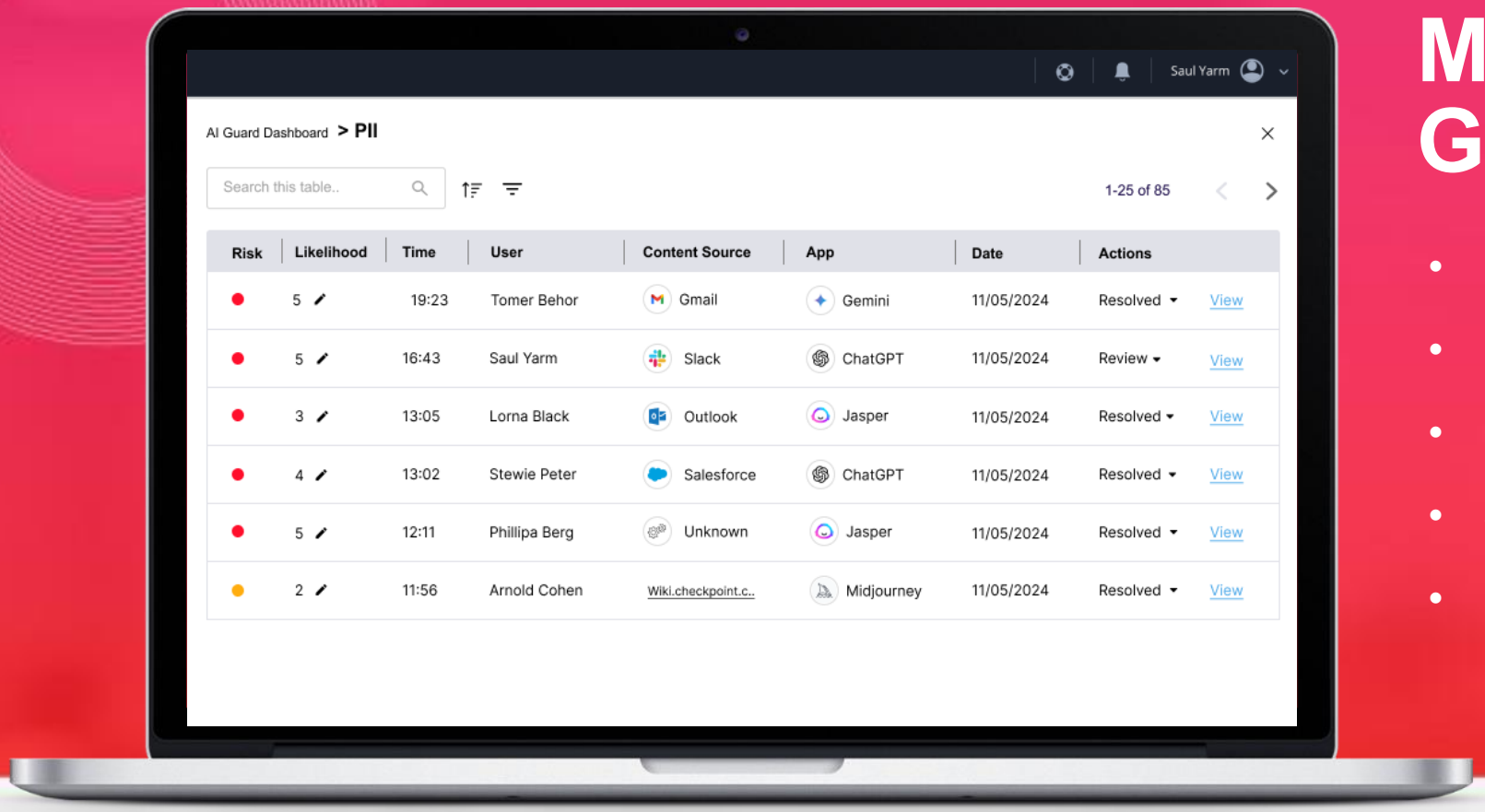
- AI-powered classification of unstructured data
- Copy/paste restrictions
- Customizable policy
- Keep intellectual property safe
- Address privacy concerns

Multiple Enforcement Points



Gateway	SASE	Endpoint	Browser
Quantum Security Gateway	Harmony SASE	Harmony Endpoint	Harmony Browse

- **Comprehensive** use-case support
- Single policy to **control access** and **prevent data loss**



Meet Regulations with Granular Visibility

- Granular visibility and audit trail
- Monitor events, prompts, affected data
- Customizable reports
- Share progress with the board
- Get mitigative steps to improve security

Why GenAI Security from Check Point

Deploys in minutes with
browser extension

Deep GenAI-based grasp of context to
detect sensitive data

Enforces copy/paste restrictions
in real time

OVERVIEW
ECOSYSTEM
AUTOMATIONS
INSIGHTS
CATCHUPS
ALERTS
KBFINDER
AI WATCH
SETTINGS

AI Watch Dashboard

Search Console

Connect

Total Risky Sessions (30 days)

-8% (last 7 days) 15 New

- Critical (16)
- High (6)
- Medium (4)
- Low (2)

View report

Recap

View report

34 Apps in use (30 days)
-5% (last 7 days) 3 New — Review

98 users of AI applications
+15% (last 7 days) — Review

265 sessions
+9% (last 7 days) — Review

24 Content Sources
+ % (last 7 days) — Review

Use Cases (30 days)

- Code Generation 34%
- Marketing Content 24%
- Personal 18%
- Data analysis 9%
- Others 8%

View report

App Session Breakdown (30 days)

NAME	RISK BREAKDOWN	RISKY	TOTAL
Gemini		28	190
ChatGPT		18	140
Jasper		19	130
Midjourney		11	124
ChatPDF (NEW)		4	96
Others		28	54

Sensitive Content Submitted (30 days)

-14% (last 7 days) 15 New

- PII 28%
- PCI 24%
- Source Code 16%
- Business Docs 22%
- Others 10%

View report

Content Sources (30 days)

NAME	RISK BREAKDOWN	TOTAL
Gmail		158
Salesforce		137
Outlook		120
Google Docs		110
Whatsapp		96
Others		74

OVERVIEW
ECOSYSTEM
AUTOMATIONS
INSIGHTS
CATCHUPS
ALERTS
KBFINDER
AI WATCH

ChatGPT

Medium Risk

An AI-based conversational agent designed to engage in natural language conversations with users across various topics.

Active users (7 Days): 54 Sessions (7 Days): 241 View report

Publisher
Open AI

Security Risks
10

Sensitive Data Sessions
23

Risky User Sessions

-8% (last 7 days) 15 New

- Low 24%
- Medium 18%
- High 9%
- Critical 8%

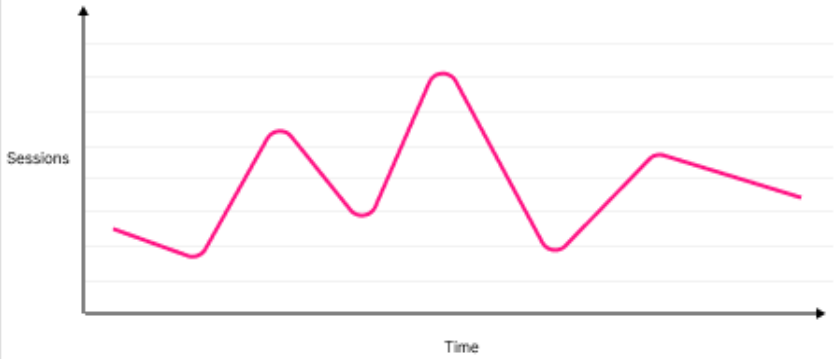
Use Case Overview

-8% (last 7 days) 15 New

- Code Generation 34%
- Marketing Content 24%
- Personal 18%
- Data analysis 9%
- Others 8%

Session Trends

View all



Riskiest Content Sources

NAME	RISK BREAKDOWN	TOTAL
Gmail		158
Salesforce		137
Outlook		120
Others		74

Riskiest Content Sources

NAME	RISK BREAKDOWN	TOTAL
Gmail		158
Salesforce		137
Outlook		120
Others		74

Search this table

1-25 of 85

Total Risky Sessions (30 days)

-8% (last 7 days) 15 New

- Critical (16)
- High (6)
- Medium (4)
- Low (2)

View report

Recap

View report

34 Apps in use (30 days)
-5% (last 7 days) 3 New
Review >

98 users of AI applications
+15% (last 7 days)
Review >

265 sessions
+9% (last 7 days)
Review >

24 Content Sources
+ % (last 7 days)
Review >

Use Cases (30 days)

- Code Generation 34%
- Marketing Content 24%
- Personal 18%
- Data analysis 9%
- Others 8%

View report

App Session Breakdown (30 days)

NAME	RISK BREAKDOWN	RISKY	TOTAL
Gemini		28	190
ChatGPT		18	140
Jasper		19	130
Midjourney		11	124
ChatPDF		4	96
Others		28	54

Sensitive Content Submitted (30 days)

-14% (last 7 days) 15 New

- PII 28%
- PCI 24%
- Source Code 16%
- Business Docs 22%
- Others 10%

View report

Content Sources (30 days)

NAME	RISK BREAKDOWN	TOTAL
Gmail		158
Salesforce		137
Outlook		120
Google Docs		110
Whatsapp		96
Others		74

Total Risky Sessions (30 days)

-8% (last 7 days) 15 New

- Critical (16)
- High (6)
- Medium (4)
- Low (2)

View report

Recap

View report

34 Apps in use (30 days)
-5% (last 7 days) 3 New — Review

98 users of AI applications
+15% (last 7 days) — Review

265 sessions
+9% (last 7 days) — Review

24 Content Sources
+ % (last 7 days) — Review

Use Cases (30 days)

- Code Generation 34%
- Marketing Content 24%
- Personal 18%
- Data analysis 9%
- Others 8%

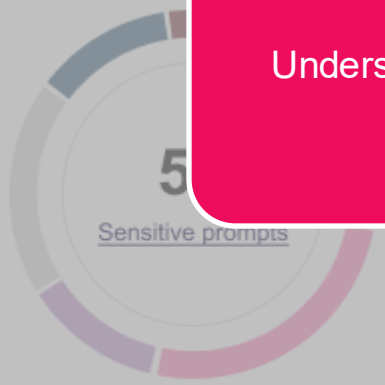
View report

App Session Breakdown (30 days)

NAME	RISK BREAKDOWN	RISKY	TOTAL
Gemini		28	190
ChatGPT		18	140
Jasper		19	130
Midjourney		11	124
ChatPDF		4	96
Others		28	54

Sensitive Content Submitted (30 days)

-14% (last 7 days) 15 New



- Business Docs 22%
- Others 10%

View report

Content Sources (30 days)

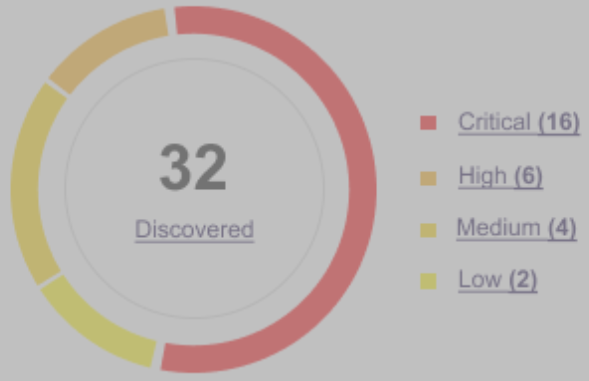
NAME	RISK BREAKDOWN	TOTAL
		158
		137
		120
Google Docs		110
Whatsapp		96
Others		74

Understand your **Inventory** with continuous discovery of GenAI applications and how they are used

Get the full picture of **sensitive data leakage risks**, with next-gen DLP engine and **content source detection**.
Easily **review trends and progress** in your risk mitigation efforts.

Total Risky Sessions (30 days)

-8% (last 7 days) 15 New



View report

Recap

View report

34 Apps in use (30 days)
-5% (last 7 days) 3 New
Review

98 users of AI applications
+15% (last 7 days)
Review

Use Cases (30 days)

App Session Breakdown (30 days)

NAME	RISK BREAKDOWN	RISKY	TOTAL
Gemini		28	190
ChatGPT		18	140
Jasper		19	130
Midjourney		11	124
ChatPDF		4	96
Others		28	54

Sensitive Content Submitted (30 days)

-14% (last 7 days) 15 New

View report

Content Sources (30 days)

NAME	RISK BREAKDOWN	TOTAL
Gmail		158
Salesforce		137
Outlook		120
Google Docs		110
Whatsapp		96
Others		74

Total Risky Sessions (30 days)

-8% (last 7 days) 15 New

- Critical (16)
- High (6)
- Medium (4)
- Low (2)

View report

Recap

View report

34 Apps in use (30 days)

-5% (last 7 days) 3 New

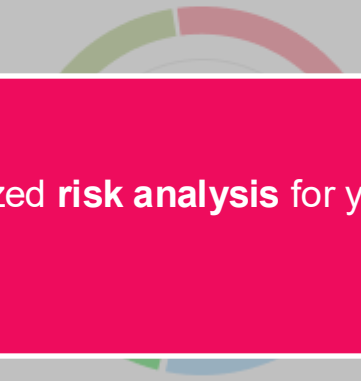
Review >

24 Content Sources

Review >

+9% (last 7 days)

Use Cases (30 days)



- Code Generation 34%
- Marketing Content 24%
- Personal 18%
- Data analysis 9%
- Others 8%

View report

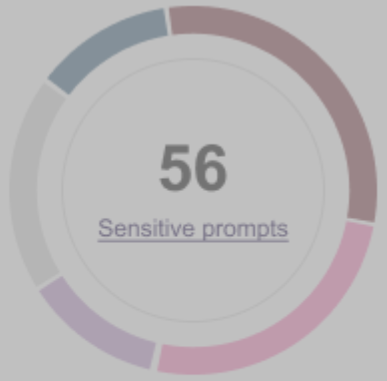
Get the bottom-line with emerging & prioritized **risk analysis** for your review.

App Session Breakdown (30 days)

NAME	RISK BREAKDOWN	RISKY	TOTAL
Gemini		28	190
ChatGPT		18	140
Jasper		19	130
Midjourney		11	124
ChatPDF		4	96
Others		28	54

Sensitive Content Submitted (30 days)

-14% (last 7 days) 15 New



- PII 28%
- PCI 24%
- Source Code 16%
- Business Docs 22%
- Others 10%

View report

Content Sources (30 days)

NAME	RISK BREAKDOWN	TOTAL
Gmail		158
Salesforce		137
Outlook		120
Google Docs		110
Whatsapp		96
Others		74

Real-Time Threat Prevention

THREATCLOUD AI

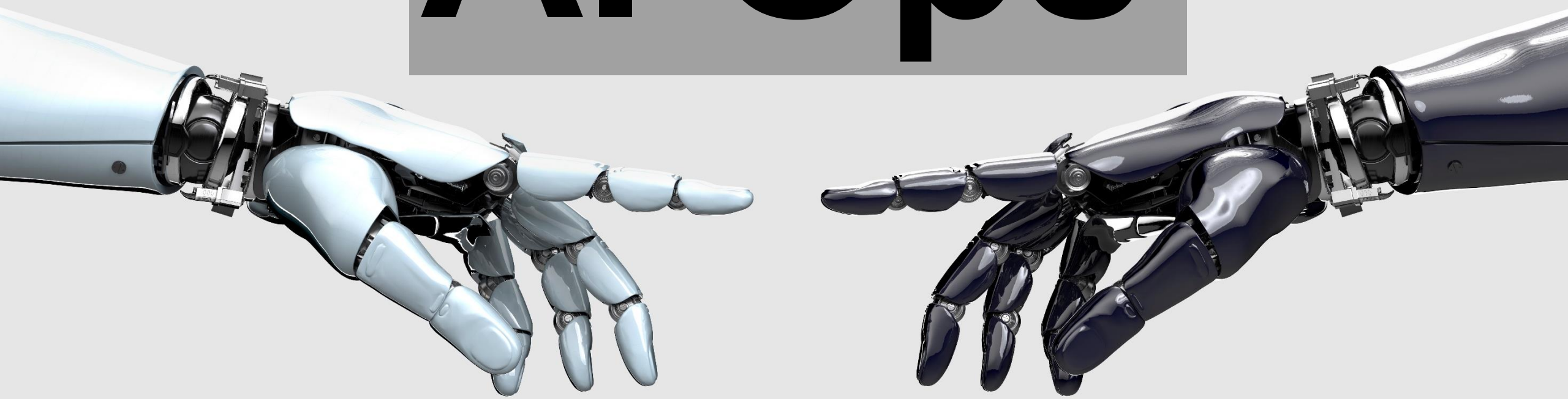
90+
Security Engines

50+
Are AI-Powered

3B
Yearly Attacks Prevented

<2 Sec
Synced globally to all enforcement points

AI Ops



Meet your new AI Security Companion!

AI-Powered Platform

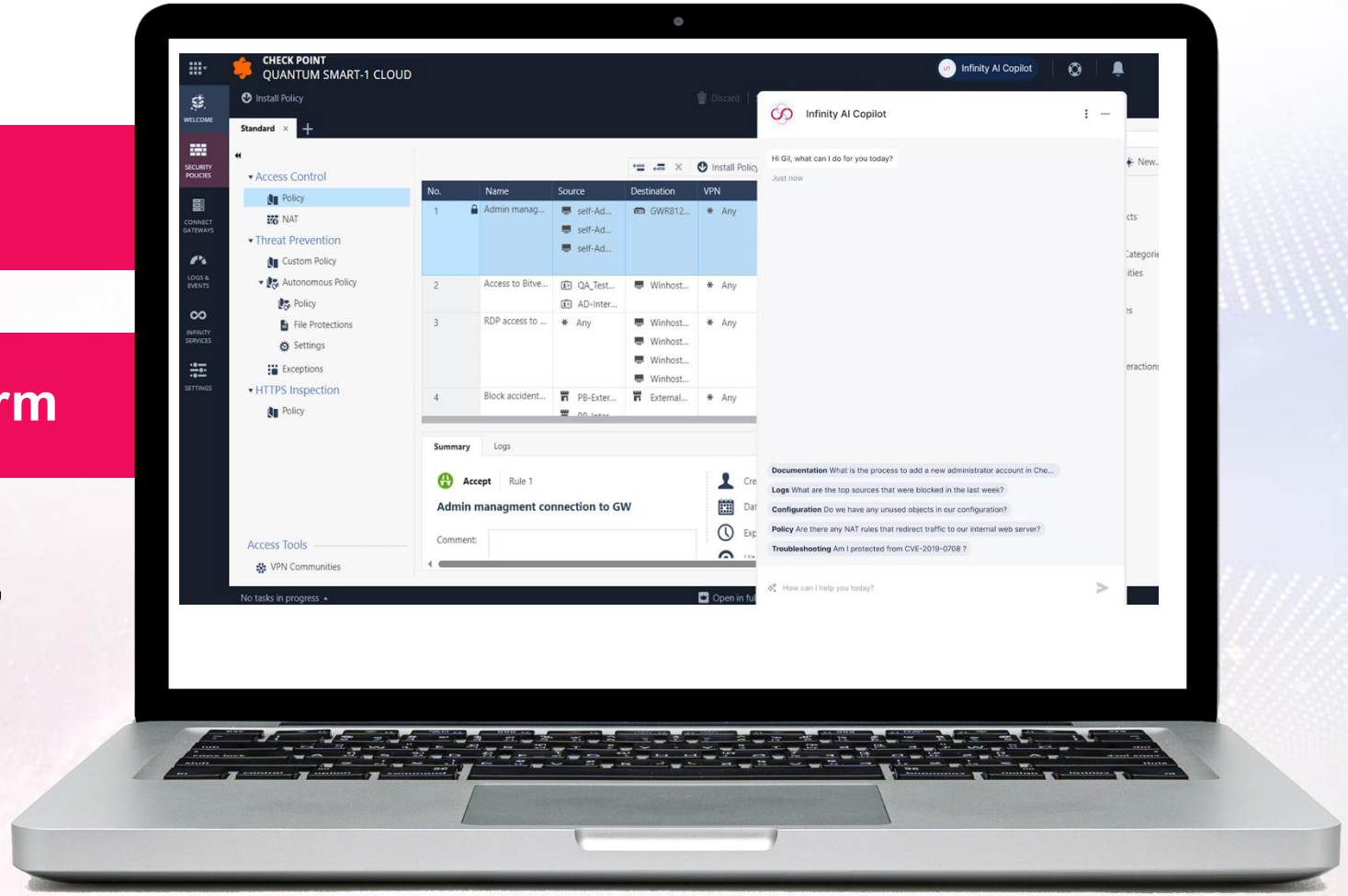
10X more effective security management

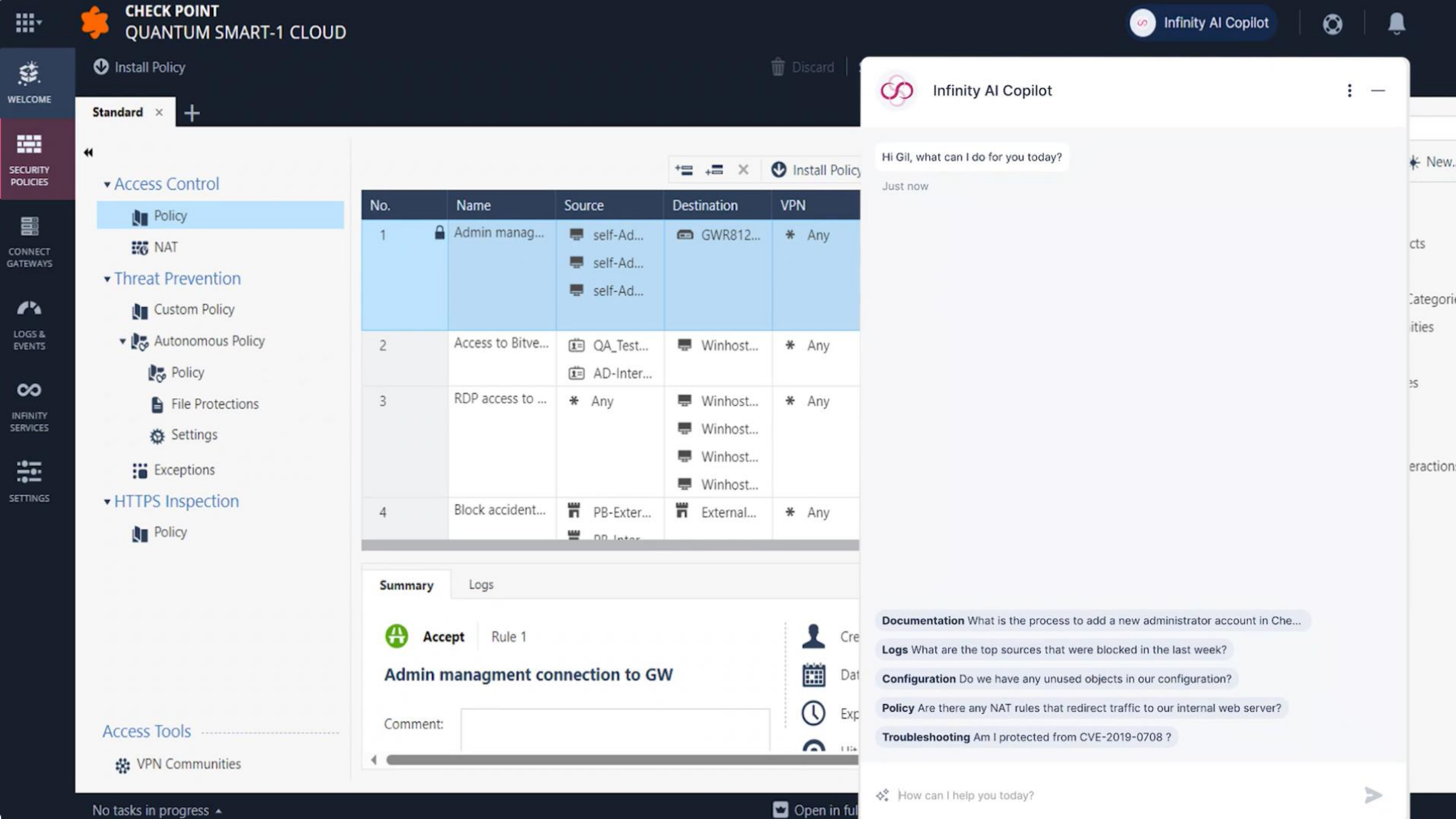
Infinity AI Copilot

Powerful, Generative-AI tool

Embedded in the Infinity Platform

Policy management, troubleshooting, and advice **in seconds**




CHECK POINT
QUANTUM SMART-1 CLOUD
Infinity AI Copilot
Install Policy
Discard
WELCOME
SECURITY POLICIES
CONNECT GATEWAYS
LOGS & EVENTS
INFINITY SERVICES
SETTINGS
Standard
Access Control
Policy
NAT
Threat Prevention
Custom Policy
Autonomous Policy
Policy
File Protections
Settings
Exceptions
HTTPS Inspection
Policy
Access Tools
VPN Communities
Install Policy
No. Name Source Destination VPN
1 Admin manag... self-Ad... self-Ad... self-Ad... GWR812... Any
2 Access to Bitve... QA_Test... AD-Inter... Winhost... Any
3 RDP access to ... Any Winhost... Winhost... Winhost... Winhost... Any
4 Block accident... PB-Exter... External... Any
Summary
Logs
Accept
Rule 1
Admin managment connection to GW
Comment:
Infinity AI Copilot
Hi Gil, what can I do for you today?
Just now
Documentation What is the process to add a new administrator account in Che...
Logs What are the top sources that were blocked in the last week?
Configuration Do we have any unused objects in our configuration?
Policy Are there any NAT rules that redirect traffic to our internal web server?
Troubleshooting Am I protected from CVE-2019-0708 ?
How can I help you today?
No tasks in progress

Emily Johns can't access SAP-server-America, please suggest allowing her access

20:58

The logs show that Emily Johns attempts to access the SAP-server-America (IP: 192.168.19.1) were dropped by the rule 6.3 named "Production Farm Cleanup rule". This happened multiple times, last time on 2024-01-03 at 13:59:41.

Just now

Would you like to add 'ad_group_Canada_sales' to access role ‘Sales_North_America’

Yes (Add group to access role) No

'ad_group_Canada-Sales' added to access role 'Sales_North_America'

Just now

Would you like to Install Policy

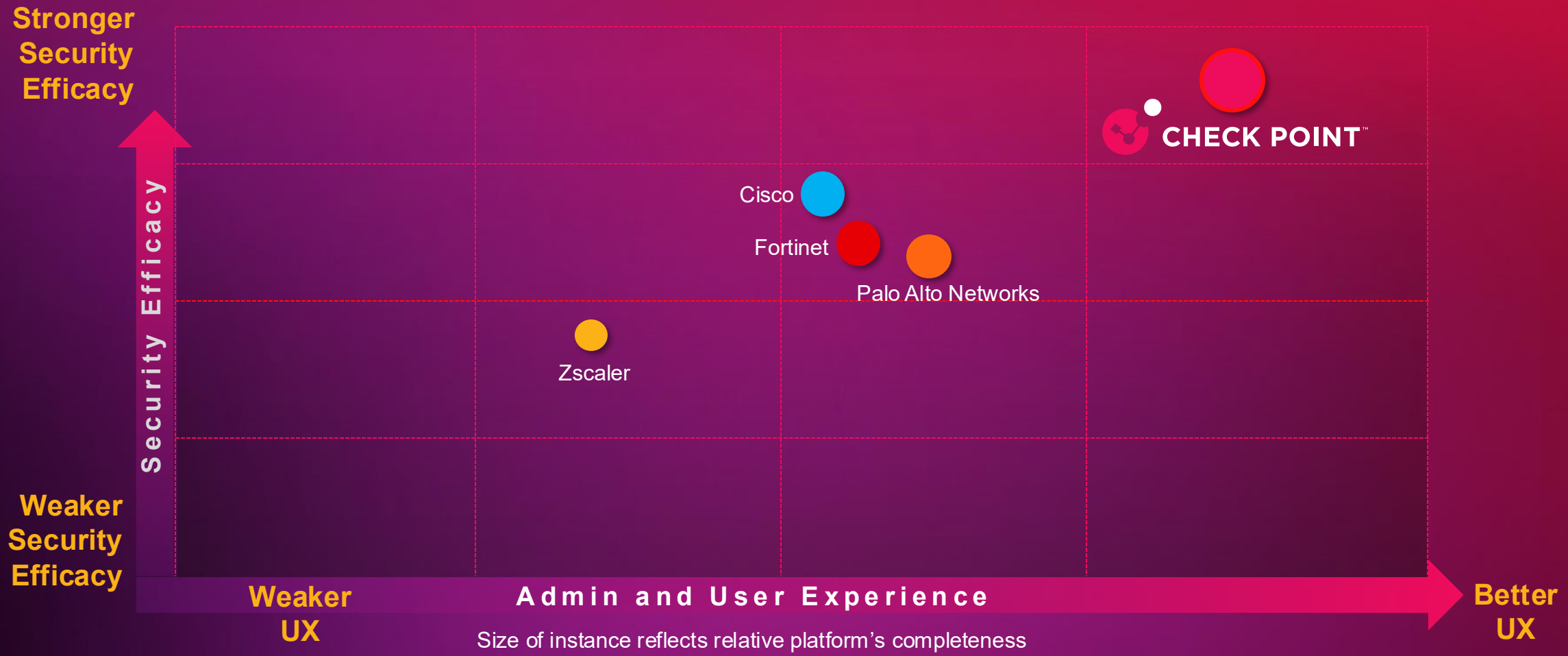
Yes (Install Policy) No

How can I help you today?

Best AI-Powered Cyber Security Platform

Miercom

Top 10 Common Enterprise Use Cases



Company Profile

Check Point allows any organization to conduct
their business on the internet with the highest level of security

Over
30 Years
in cyber security

HQ: Israel
74
Global offices

Over
+7,000
Employees

Protecting over
100,000
organizations

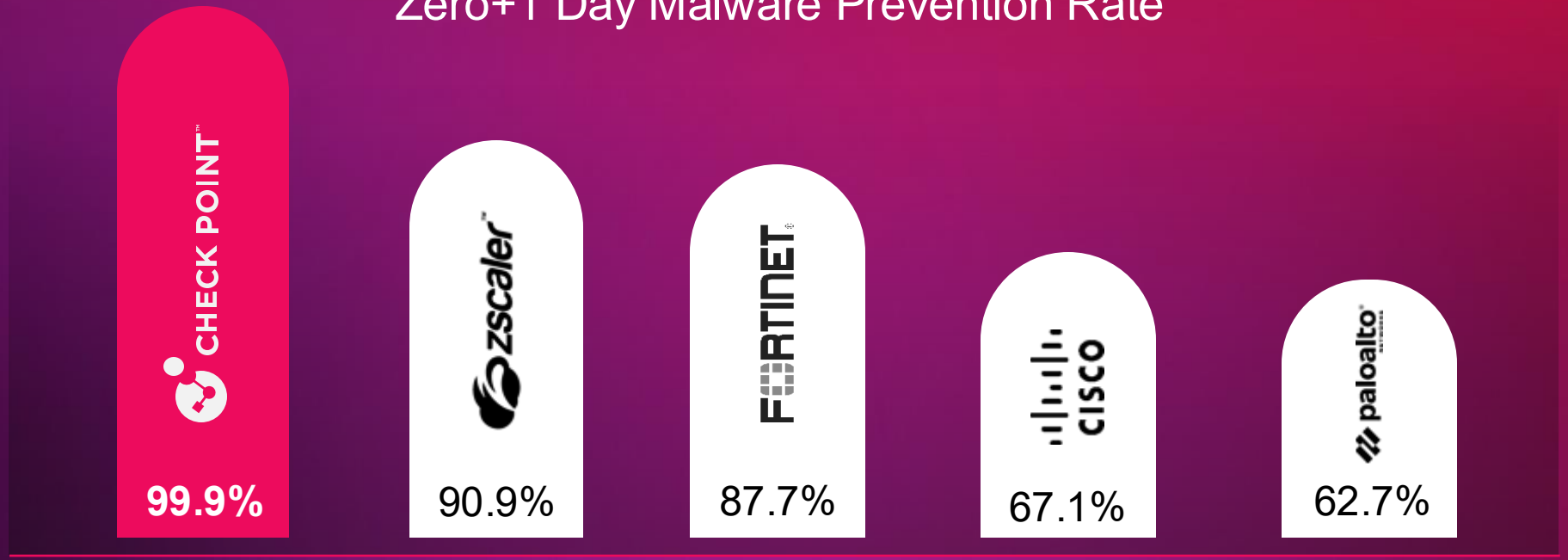
Operating in
182
countries

NASDAQ listed
~$25B
Market cap

Best in Real-Time Threat Prevention

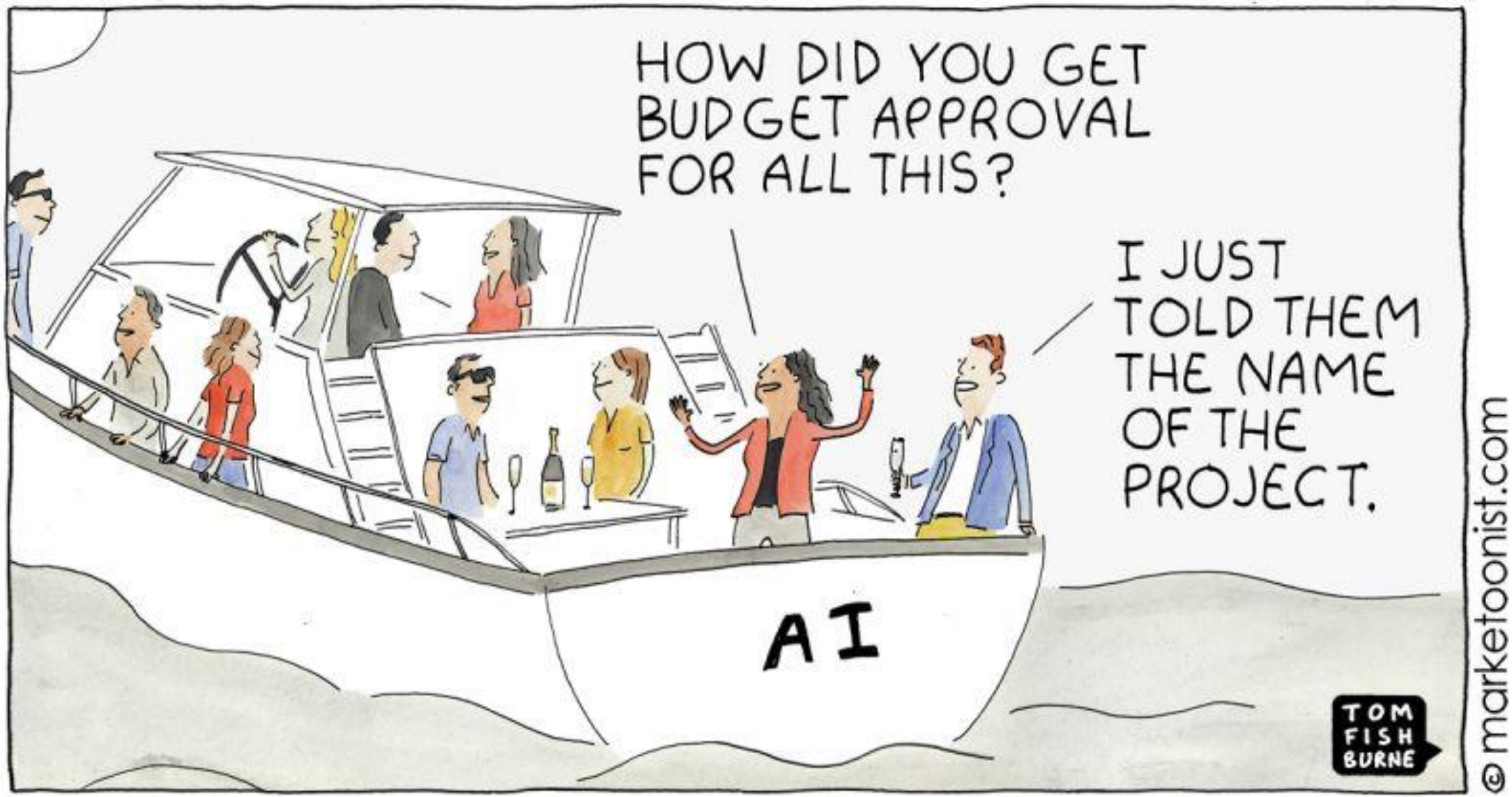
Miercom 2025 Security Benchmark Report

Zero+1 Day Malware Prevention Rate



Highest Security Rating - 2025

Source: Miercom Enterprise & Hybrid Mesh Firewall Benchmark Report 2025



BONUS: Create an AI Strategic Security Plan

- **Confirm enterprise mission and goals**, and align your project goals with C-level stakeholders
- **Assess your team's ability to deliver on goals** and create a plan to fill capability gaps
- **Strategically manage functional budgets** to prioritize the best cost, budget and investment decisions
- **Select metrics that will demonstrate the progress** you're making against commitments and competitiveness and efficacy
- **Document your strategy** to simply and clearly state where the project n is, where it's going and how it will get to there

BONUS: Advice to CISO's and Business Leaders:

For business leaders, adopt a baby steps approach. Don't rush into it without dictating policy and safeguards following a risk assessment/project prioritization process.

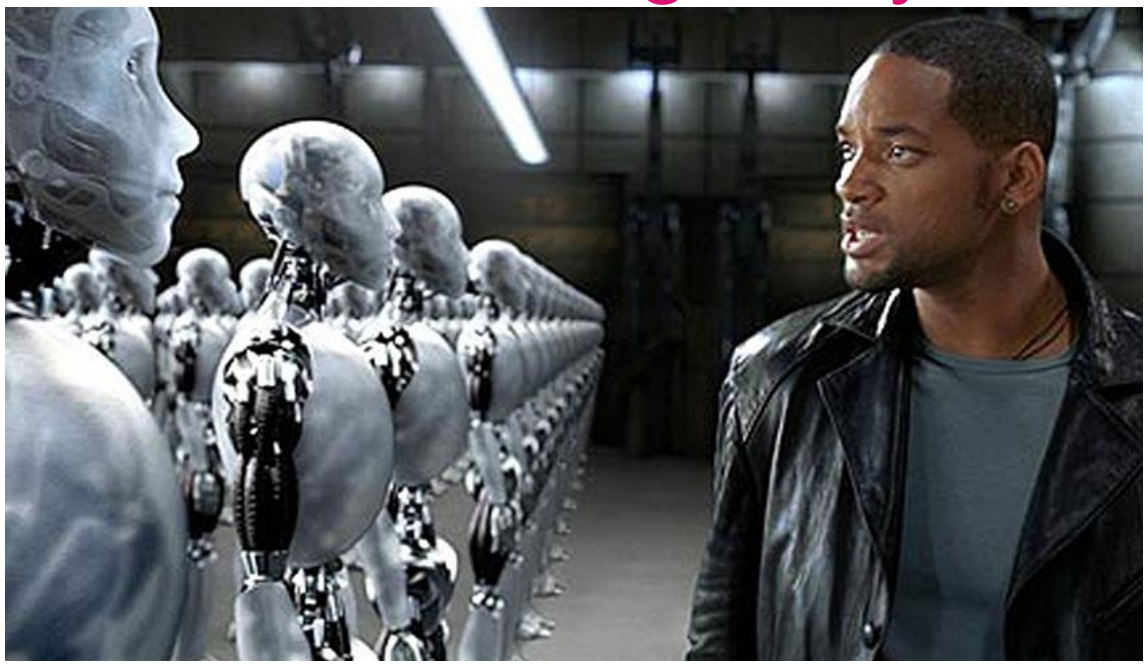
- Pick some easy projects, and get some fast wins!
- Adopt its use into existing policies.
- Communicate: Share do's and don'ts with all employees via the Security Awareness programs.
- Supply Chain Risk awareness: Review contracts to ensure no co-mingling, or use of your data to help competitors
- Monitor/Enforce: Ensure that PII or critical data is not getting exposed to AI platforms that didn't obtain the required level of trust according to the sensitivity levels. Leverage enforcement mechanisms such as DLP + WAP (Web application and API protections) security capabilities.

Questions to Bring Home and Discuss with your Team:

Artificial Intelligence Risks and Issues

- As a CISO whose company is using AI tools, let's start by discussing some of the positive capabilities you are seeing and supporting.
- What AI technologies are you using at your organization? How are they adding value?
- Are you leveraging any of the AI Related Guidance from NIST or others?
- What should CISOs communicate to employees, execs, boards?
- Have you created organizational policies around the use of generative AI? Are you allowing it?
- Now, lets go the dark side, where do you see you company at risk by leveraging AI tools?
- From an external threat landscape perspective, how is AI impacting attack capabilities and patterns?
- Have the advances in generative AI changed how you're thinking about the threat landscape? Is it shifting your security posture? Are you looking at changing or enhancing tools and or processes?
- What are best practices to vet legitimate AI technologies? What are the hard questions security leaders should ask?
- What is your thinking on vendors in your supply chain using AI technologies? Are you looking for them to leverage AI?
- What are you doing to monitor and put security controls around this?

When is the Singularity?



NS-5 Robots in I, Robot

SKYNET and The Terminator

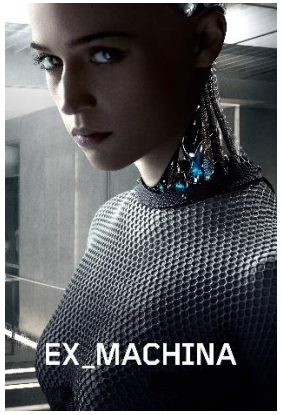
J.A.R.V.I.S

M3GAN

ARISA

2001

Blade Runner



Ex Machina

Metropolis

MOON

CHECK POINT™

Thank You! Danke! Gracias! Merci! Grazie! תודה!

petern@checkpoint.com

https://www.linkedin.com/in/petenicoletti/

YOUR BUSINESS BEST SECURITY

PETE'S AI DISCUSSION MEDIA APPEARANCES:

GMA segment was extended to an **ABC News Nightline** feature & online article informing about the rapid increase in malicious actors utilizing Artificial Intelligence to imitate human voices.

Pete's in-person interview with **CBS LA**. **CBS LA's Evening News with Norah O'Donnell** as part of their "***Age of AI series***" on July 12th, and it was later showcased again in an extended interview on the **CBS Morning Show** on July 19th.

The coverage didn't stop there! The interview was syndicated across the US appearing in **over 1,000 instances** in top markets such as San Francisco, Las Vegas, Austin, New York City, Washington and many others.

Live interviews with Fox12 Oregon

- https://www.youtube.com/watch?v=9TqjHdWD1u4&t=29s
- https://www.youtube.com/watch?v=Fgm1Fk90Z4I&t=658s
- https://www.youtube.com/live/t8pceEuKn3E?si=CPyiktvq4OhZ-sAx

CISO to CISO Interview: Inside the CISO's Office: Dive in with Pete Nicoletti, a hacker's worst nightmare - YouTube
Interview with Vox- print- https://www.vox.com/technology/2023/9/15/23875113/mgm-hack-casino-vishing-cybersecurity-ransomware
1.Comments on IT Brew- : https://www.itbrew.com/stories/2023/09/14/mgm-resorts-hit-by-alleged-ransomware-attack
2.KTNLV- Broadcast- https://mms.tveyes.com/PlaybackPortal.aspx?SavedEditID=4f924f35-f192-4831-b063-99dd938dcaed
3.WVON- radio- https://mms.tveyes.com/PlaybackPortal.aspx?SavedEditID=ecd571d9-e932-4bbc-a7e3-4a8f73ed77d0
4.Fox 13: https://www.fox13now.com/the-place/software-to-avoid-getting-scammed
5.News 12 Hudson Valley - https://bronx.news12.com/ransomware-attack-targets-commack-school-district
6.WEF Byline: https://www.weforum.org/agenda/2023/08/6-ways-to-reduce-cybersecurity-spend-without-compromising-security/
7.And two comments on Tech Republic: https://www.techrepublic.com/article/microsoft-apple-spyware/ and https://www.techrepublic.com/article/check-point-hackers-usb/

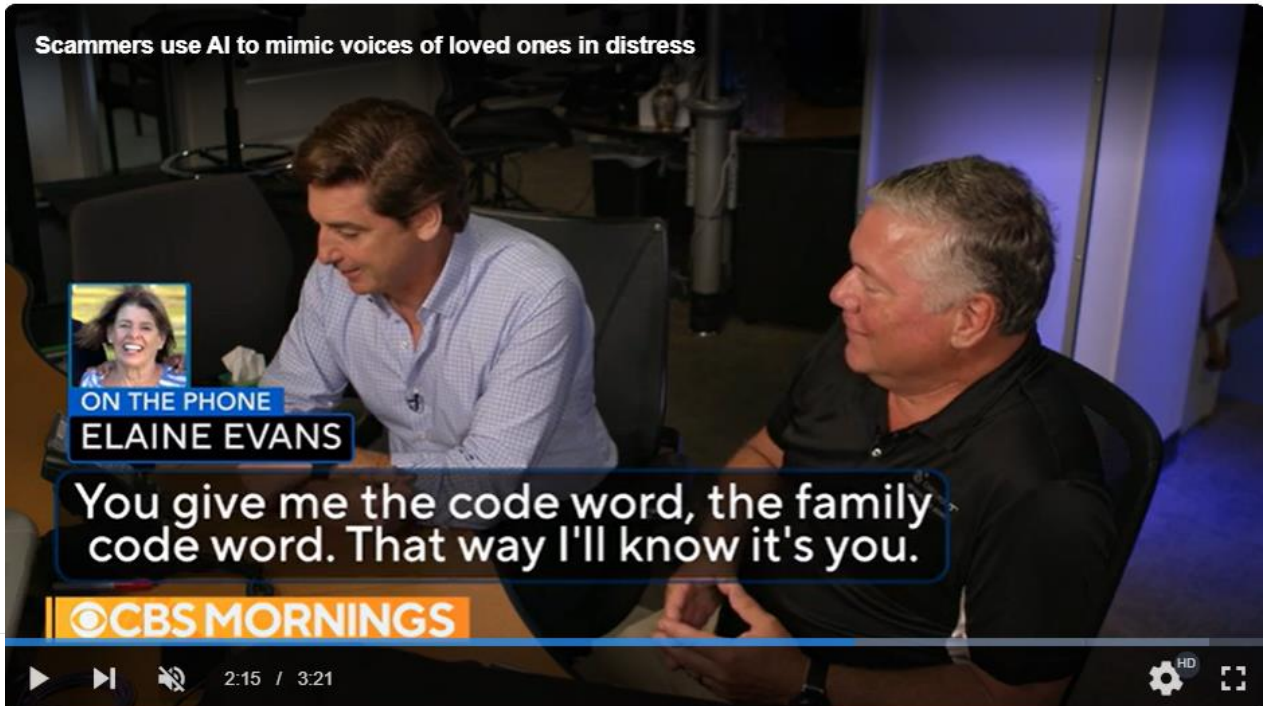
CBS News Scammers use AI to mimic voices of loved ones in distress
May 11

- https://www.yahoo.com/tech/scammers-ai-mimic-voices-loved-134832783.html?guccounter=1

24 Million Views!

Pete Nicoletti, a cyber security expert at Check Point Software Technologies, said common software can recreate a person's voice after just 10 minutes of learning it.

To protect against voice cloning scams, Nicoletti recommends families adopt a "code word" system and always call a person back to verify the authenticity of the call. Additionally, he advises setting social media accounts to private, as publicly available information can be easily used against individuals.



Security Professional Resources

- Prompt Engineering eBook for Security Pro's (Written by Pete!)
- https://www.checkpoint.com/resources/ciso-corner/the-cyber-security-professionals-guide-to-prompt-engineering?w=d39ff

- Chat Bots Competitive Leaderboard:
- https://lmarena.ai/

What Are The “Killer Apps” Everyone Should Know about?

ChatGPT
Let’s start with a quick recap of the viral sensation that is ChatGPT. It is a conversational interface for OpenAI’s GPT-3 large language model, which has recently been made available to the public as a free research preview. In response to text prompts such as questions or instructions, it will output text in any form, including prose, poetry, and even computer code.

Dall-E 2
Another OpenAI project, which together with ChatGPT is responsible for kick-starting the current wave of consumer interest in generative AI. This one takes text prompts and transforms them into computer graphics (images, photos, drawings, paintings, etc.).

Stable Diffusion 2
This is another text-to-image generative AI application. Unlike Dall-E 2, its source code, as well as details on the training data and weighting used by its algorithms, are openly available to the public, and the application can be downloaded and installed on your own computer rather than only being accessible through a proprietary cloud portal as is the case with OpenAI’s projects.

Lumen5
An AI-powered video creation tool that enables anyone to easily create education, marketing, or business video content using a simple drag-and-drop interface.

Soundraw
Automated music generator – create royalty-free AI music by simply making decisions about the genre of music you want to create, the instruments that will be used, the mood you want to create, and the length of the track. Then sit back and let the AI compose unique tracks.

Looka
This is a tool that makes it easy to brand your business by using AI to create unique and distinctive logos that convey your company style and messaging. This tool makes it a doddle to start creating customized marketing material even if you don’t have any design skills.

Podcastle
An audio recording and editing platform with integrated AI tools that helps you create clear, super-smooth recordings that sound as if they’ve been edited professionally, automating tasks like cleaning up messy sounds and creating transcripts.

Gen-1
Cloud-based text-to-video platform that creates new videos from ones that you upload, using text prompts to apply the edits and effects that you desire, or create animations from storyboard mock-ups. This tool was also developed by the creators of Stable Diffusion.

Lalal.ai
This tool uses a neural network system called Phoenix to automate audio source separation. This involves extracting elements such as vocals, music, or even specific instrumental tracks like drumbeats or basslines from any audio or video content.

Deep Nostalgia
Do you have historic family photographs of distant relatives or ancestors who you’d like to see in motion? This innovative tool lets you animate the faces in family photos so you can see them smile, blink, and laugh, just as if you had recorded a video of them back in the day.

Murf
This is a text-to-speech engine that makes it simple to create natural-sounding synthetic vocal recordings in 15 languages from a choice of over 100 voices and dialects. This output can easily be incorporated into automated marketing or video content, automating the process of creating narration and voiceovers.

Legal Robot
This tool is designed to automatically translate complex and confusing “legalese” into straightforward language that can be understood by anyone. Useful both for laypeople wanting to make sure they understand legal documents and for legal professionals to ensure that their contracts and documents are written in terms that anyone can understand.

Cleanup.Pictures
This AI tool lets you retouch images by removing unwanted objects, defects, or even people, using a process known as “inpainting” to help you create the perfect image.

Fireflies
This tool plugs into popular video conferencing tools like Zoom, Teams, or Webex and automates the process of taking notes and creating transcriptions. It also analyzes conversations to provide insights into the dynamics and decision-making that are going on in your conversations.

Krisp
Another conferencing application, this one uses algorithms to remove background noises, echo, and other distracting elements in real-time, ensuring that you always come across in a clear and professional manner.

DEEPFAKES AND INFLUENCE BOTS RESOURCES

https://github.com/iperov/DeepFaceLab

https://www.rand.org/blog/2020/01/artificial-intelligence-and-the-manufacturing-of-reality.html

https://mitsloan.mit.edu/ideas-made-to-matter/how-do-online-bots-shift-opinions

https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2740/RAND_RR2740.pdf

https://arstechnica.com/tech-policy/2016/12/op-ed-five-unexpected-lessons-from-the-ashley-madison-breach/

https://www.ftc.gov/system/files/documents/reports/social-media-bots-advertising-ftc-report-congress/socialmediabotsreport.pdf

https://foreignpolicy.com/2019/08/12/8-ways-to-stay-ahead-of-influence-operations/

https://www.wired.com/story/law-makes-bots-identify-themselves/

https://venturebeat.com/2020/09/30/how-bots-threaten-to-influence-conversations-ahead-of-the-2020-u-s-elections/

https://www.fastcompany.com/90390287/this-ai-generates-fake-news-about-anything-you-want-try-it

https://www.forbes.com/sites/bernardmarr/2023/05/24/the-29-best-and-free-chatgpt-and-generative-ai-courses-and-resources/?sh=1e1819054a6f

The human side of generative AI: Creating a path to productivity | McKinsey

MORE INFLUENCE BOTS RESOURCES

https://www.forbes.com/sites/robpegoraro/2020/08/07/from-russia-with-lure-why-were-still-beset-by-bots-and-trolls-pushing-disinformation/?sh=2546610e5542

https://www.pewresearch.org/internet/2018/04/09/bots-in-the-twittersphere/

https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html

https://www.brookings.edu/research/how-to-combat-fake-news-and-disinformation/

https://cyber.fsi.stanford.edu/io/

https://ieeexplore.ieee.org/document/7490315

https://www.rand.org/pubs/research_reports/RR2705.html

https://asiatimes.com/2021/02/collectively-countering-chinas-influence-operations/

https://www.reuters.com/article/us-china-robots-idUSKBN1AK0G1

https://www.darkreading.com/threat-intelligence/how-china-and-russia-use-social-media-to-sway-the-west/d/d-id/1334108

https://www.recordedfuture.com/china-social-media-operations/

AI/ML/ANN ALGORITHMS RESOURCES

https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/

https://www.brookings.edu/blog/techtank/2019/01/03/artificial-intelligence-and-bias-four-key-challenges/

https://www.ftc.gov/news-events/blogs/business-blog/2020/04/using-artificial-intelligence-algorithms

https://cio.economictimes.indiatimes.com/news/corporate-news/google-ai-researchers-abrupt-exit-sparks-ethics-bias-concerns/79591079

https://plato.stanford.edu/entries/ethics-internet-research/

https://aif360.mybluemix.net/

http://sciencepolicy.duke.edu/content/forget-killer-robots%E2%80%94bias-real-ai-danger

https://www.technologyreview.com/2017/07/12/150510/biased-algorithms-are-everywhere-and-no-one-seems-to-care/

https://cacm.acm.org/magazines/2020/3/243021-dilemmas-of-artificial-intelligence/fulltext

https://www.scu.edu/ethics/all-about-ethics/artificial-intelligence-and-ethics/

https://journalofethics.ama-assn.org/article/ethical-dimensions-using-artificial-intelligence-health-care/2019-02

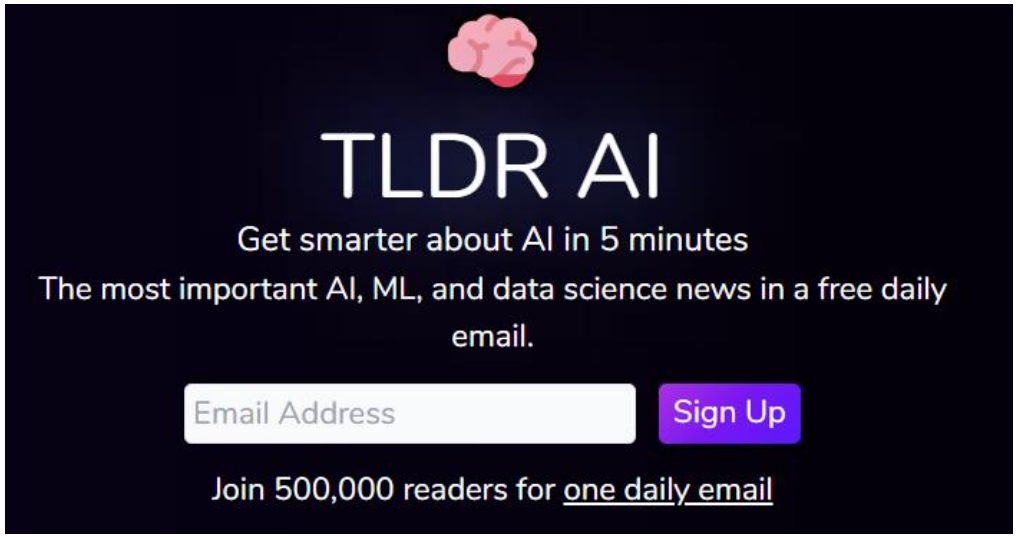
https://plato.stanford.edu/entries/ethics-ai/

https://www.forbes.com/sites/bernardmarr/2023/05/24/the-29-best-and-free-chatgpt-and-generative-ai-courses-and-resources/?sh=1e1819054a6f

Sign Up for these AI Newsletters!

TLDR: Get smarter about AI in 5 minutes (tldr.tech)
https://tldr.tech/ai

CB Insights:
https://www.cbinsights.com/newsletter/



Subscribe | FryAI (fry-ai.com)
https://www.fry-ai.com/subscribe?ref=M6mKsLv16q

CYBERSECURITY/NATIONAL SECURITY RESOURCES

https://www.aspi.org.au/report/weaponised-deep-fakes

https://www.rand.org/multimedia/audio/2020/10/23/using-ai-to-tackle-disinformation-online.html

https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT473/RAND_CT473.pdf

https://www.foreignaffairs.com/articles/2018-10-04/what-clausewitz-can-teach-us-about-war-social-media

https://comprop.oii.ox.ac.uk/

https://redy.ssri.duke.edu/news/don%E2%80%99t-believe-your-eyes-or-ears-weaponization-artificial-intelligence-machine-learning-and

https://www.cbc.ca/news/world/china-hong-kong-national-security-law-1.5633277

https://www.fbi.gov/investigate/counterintelligence/the-china-threat

http://www.homelandsecuritynewswire.com/dr20210209-deepfake-detectors-can-be-defeated-researchers-show-for-the-first-time

https://www.brookings.edu/research/fighting-deepfakes-when-detection-fails/

https://www.lanl.gov/discover/publications/national-security-science/2020-winter/deepfakes.php

https://www.media.mit.edu/projects/detect-fakes/overview/

https://hai.stanford.edu/blog/using-ai-detect-seemingly-perfect-deep-fake-videos

https://www.nextgov.com/emerging-tech/2019/08/darpa-taking-deepfake-problem/158980/

https://www.fastcompany.com/90273352/maybe-its-time-to-take-away-the-outdated-loophole-that-big-tech-exploits

Paul Rosenzweig book ‘Cyber Warfare: How Conflicts in Cyberspace Are Challenging America and Changing the World’

Bobby Akart book ‘Cyber Warfare’

Dr. Chase Cunningham book ‘Cyber Warfare – Truth, Tactics, and Strategies’

TOP GENERATIVE AI TOOLS

Credit: Moti Sagey and Reddit

Deep Fake and Facecheck.ai Testing:

1. A good Article on Deep Fake Analysis:
   https://www.npr.org/2023/04/27/1172387911/how-can-people-spot-fake-images-created-by-artificial-intelligence

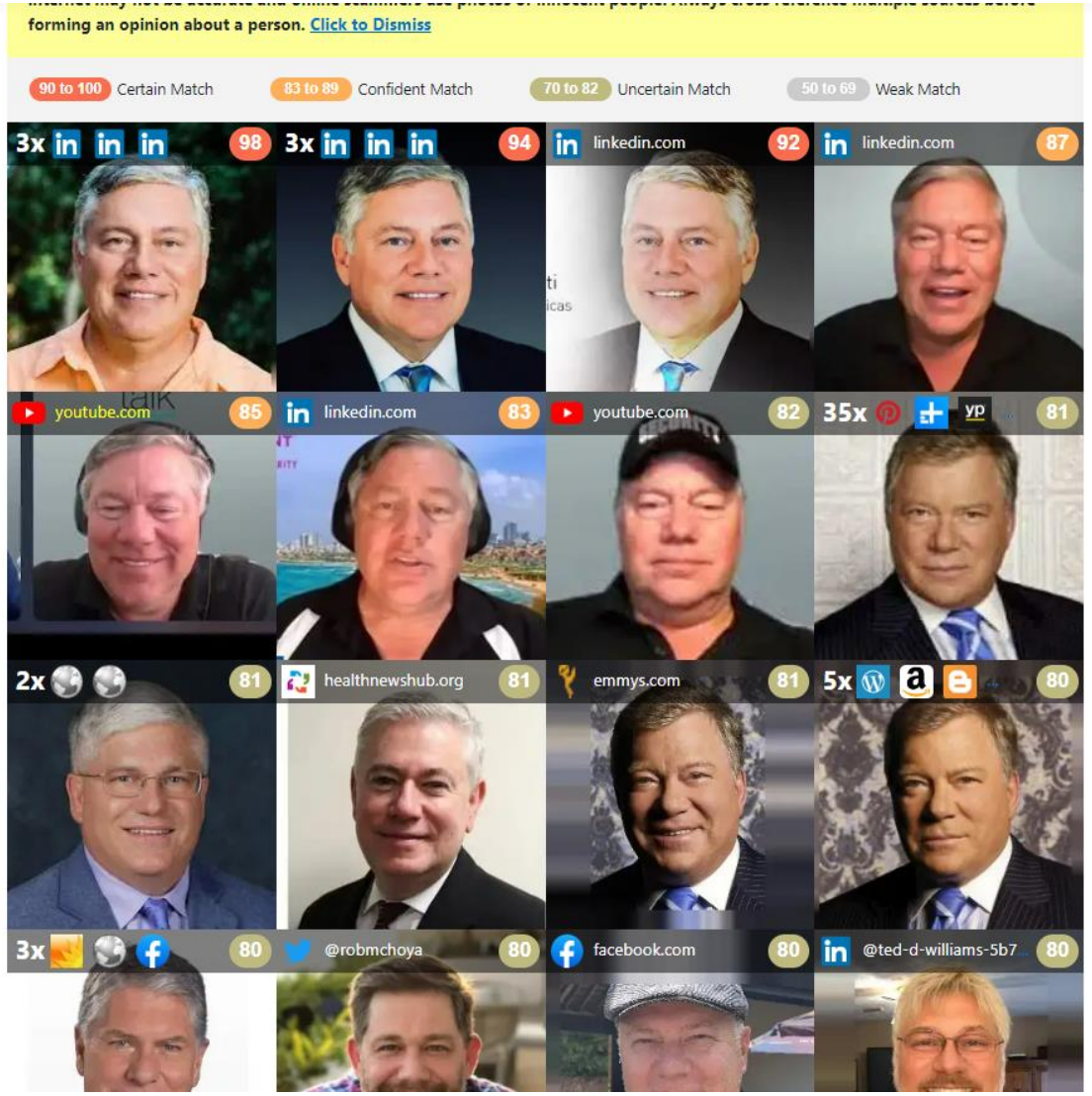
2. An Experts Thoughts:
https://eddyballe.com/deepfake-detection-tools/

- DeepWare AI: Best DeepFake Detection Software
- DuckDuckGoose: Top Deepfake detection programs for businesses
- Sensity AI: Best Deepfake detection services for anyone to use

https://beebom.com/wp-content/uploads/2020/11/AI-fake-face.jpg

How to recognize fake AI-generated images | by Kyle McDonald | Medium

https://kcimc.medium.com/how-to-recognize-fake-ai-generated-images-4d1f6f9



CHATGPT (OPENAI) RISK, REWARD, TRADEOFF

TIME SAVINGS: ChatGPT can generate responses quickly and efficiently, which can save time for both the user and the company using the technology.

CUSTOMIZATION: ChatGPT can be customized to fit the needs of the user, allowing for a personalized experience that can improve customer satisfaction and engagement.

SCALE: ChatGPT can handle a large volume of interactions at once, making it an effective solution for companies that need to handle high volumes of customer inquiries.

BIAS: ChatGPT is trained on a large amount of text data, which can contain biases, stereotypes, and offensive language. ChatGPT may perpetuate them in its responses and has potential to manipulate the user.

SAFETY: ChatGPT is not good for decision making. There is risk its responses will be inappropriate for crisis management or healthcare decisions.

ZERO EMPATHY: ChatGPT is an AI language model and lacks the ability to empathize with users. This may result in responses that are impersonal or unsympathetic, which could negatively impact user experience.

ETHICS BYPASS: ChatGPT API with third party software (Telegram) uses OpenAI's GPT-3 model and can circumvent ChatGPT ethics.

FRAGILE: ChatGPT requires extensive training to function effectively, which can be time-consuming and expensive for companies.

CONTEXT PROBLEMS AND BAD FOR DECISION MAKING: ChatGPT can generate responses based only on the information it has been given, it cannot understand the full context of a situation. This can lead to inaccurate or inappropriate responses.

Micki created with DALL-E and ChatGPT