On the Intersection of AI and Cyber Security

AI-powered Security Management and Automation

Konstantina Koukou

Cyber Security Specialist , Office of the CTO @ Check Point Software Technologies

Stay relevant / AI is changing the world

Revolutionize your space

- Leapfrog with AI
- Hard to predict, especially the future

This is the place to write your own predictions and execute on them

Example on SOC

Beyond automating what you do today, how can it be done differently?

Note! We have time:

We tend to overestimate the effect of a technology in the short run and underestimate the effect in the long run

Security intersection with AI

Four main points of view when AI meets cyber

AI used by attackers

- Force multiplier
- More targeted
- Increase success rate (test before you do)
- New attacks forms

How to secure AI Usage in my org

- Govern access to AI services & data
- Secure AI pipeline
- New things: Secure prompts, prevent poisoning, secure the AI models

AI Used for Defense

- Force multiplier
- Precision
- New interface, conversational, & generative
- New ways to defend, better operations

And then, like every organization, your team can leverage AI and be better

- More efficient, better operations & quality, growth, development & more

AI Meets cyber **#1:** AI used by attackers

Force multiplier

- Automation and operationalization of attacks becomes simpler
- Creating mass campaigns

More targeted

- Develop and test targeted attacks
- Phishing and deep fake
- Increase success rate (test before you run)

New attacks forms

- Exploit methods are still hard to invent
- New attack surface - attack AI models, prompt injection: exposing and poisoning the data
- Wars between defender AI and attacker AI

AI meets cyber **#2:** AI used for defense

Force multiplier

- Automation and remediation becomes amazingly simple
- Enrich your data, hunt threats, find the needle in the haystack

Precision

- The deep part of prevention depends on the deeper aspects of AI
- Smarter decisions due to enrichment and context

New interface

- Conversational & generative
- Simpler and for wider audience

Better operations that are more resilient

Addressing new needs

- Changing how we perform cyber jobs

AI meets cyber **#3:** Protect your AI & data usage (2/3)

Data criticality and data security aspects

- AI is only as good as your data; hygiene and trust in the data is critical
- One big data lake and/or connected data: privacy/safety of data is critical
- Balance data collection and safety
- Integrating data management into your security operations: Data is on the critical path
- Ethical and bias challenges to consider

AI meets cyber **#3:** Protect your AI & data usage (3/3)

New things: secure prompts, prevent poisoning, secure the AI models

- Prompt injection controls: exposure, unintended outcome or poisoning
- Adversary attack on the AI model
- Avoid prompt injection privilege access to data or execute non-approved actions
- Hallucinations and reliability problems in AI

In 2024 we are taking AI to the **Next Level**

Check Point 2024:

The Platform Company

AI-Powered

Cloud-Delivered

Comprehensive | Consolidated | Collaborative

MBH

THREATCLOUD AI

Real-Time Threat Prevention

90+
Security Engines

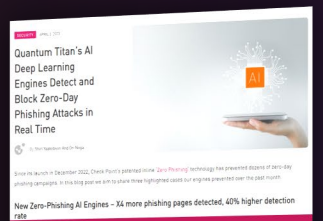
50+
Are AI-Powered

3B
Yearly Attacks Prevented

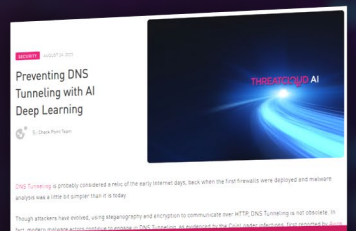
<2 Sec
Synced globally to all enforcement points

THREATCLOUD AI

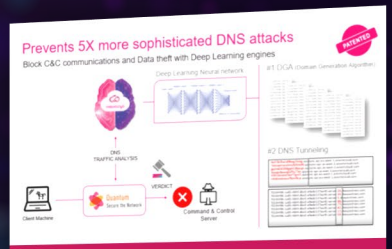
10 New Engines, **AI-Powered**



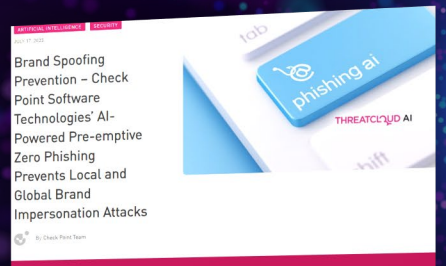
Zero Phishing



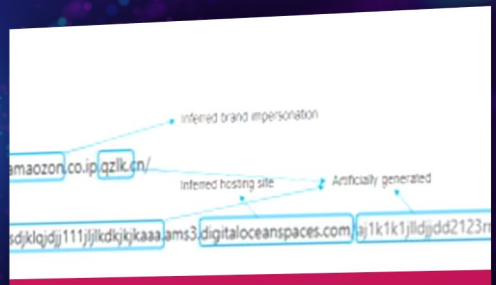
Deep DNS



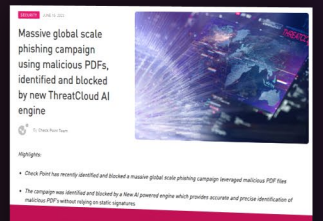
Deep DGA



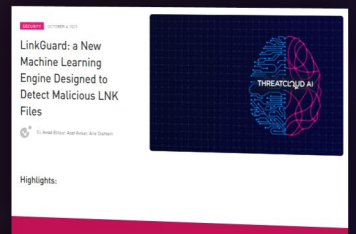
Brand Spoofing



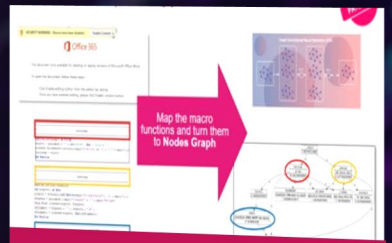
ClearSite - URLs



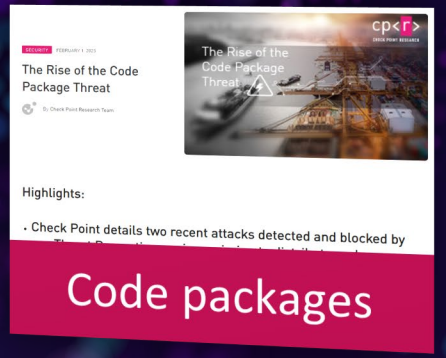
Deep PDF



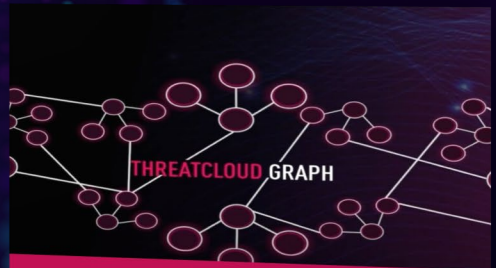
LNK Guard



DeepVBA



Code packages



Graph - URLs

Infinity ThreatCloud AI

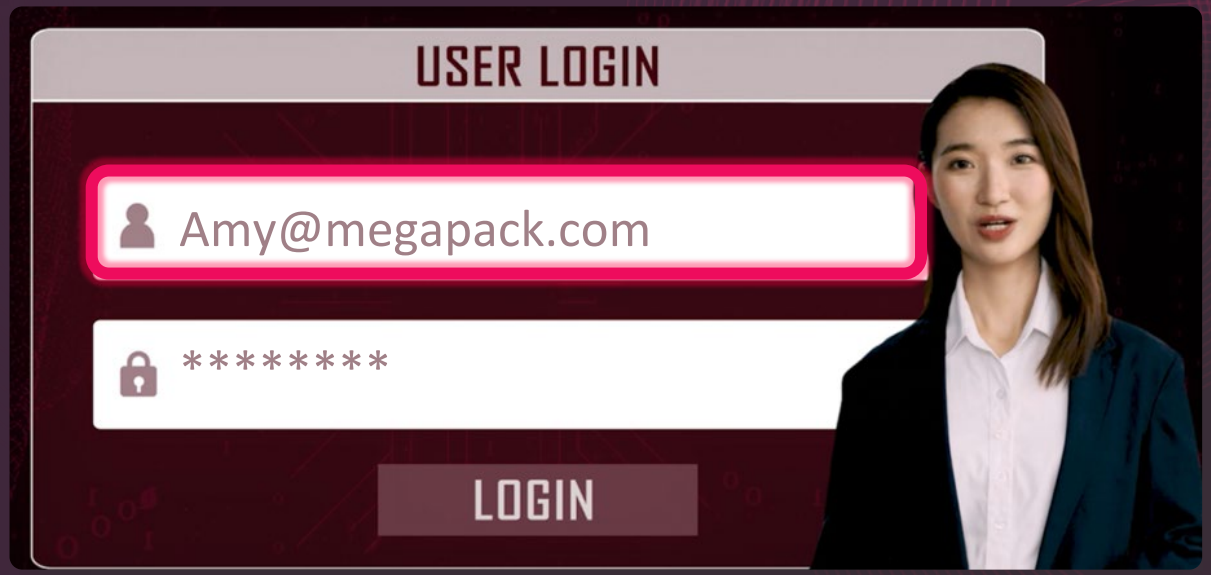
Brand Spoofing NEW

Prevent access to sites impersonating to local brands

Coming Soon: PATENT PENDING

Deep Brand Clustering

Ultra Scale. Autonomous.



Dec' 2023 Preventions:

560k
Preventions

160
Countries

Available Today Across:
Quantum, Harmony, CloudGuard

ThreatCloud AI

#1 Miercom

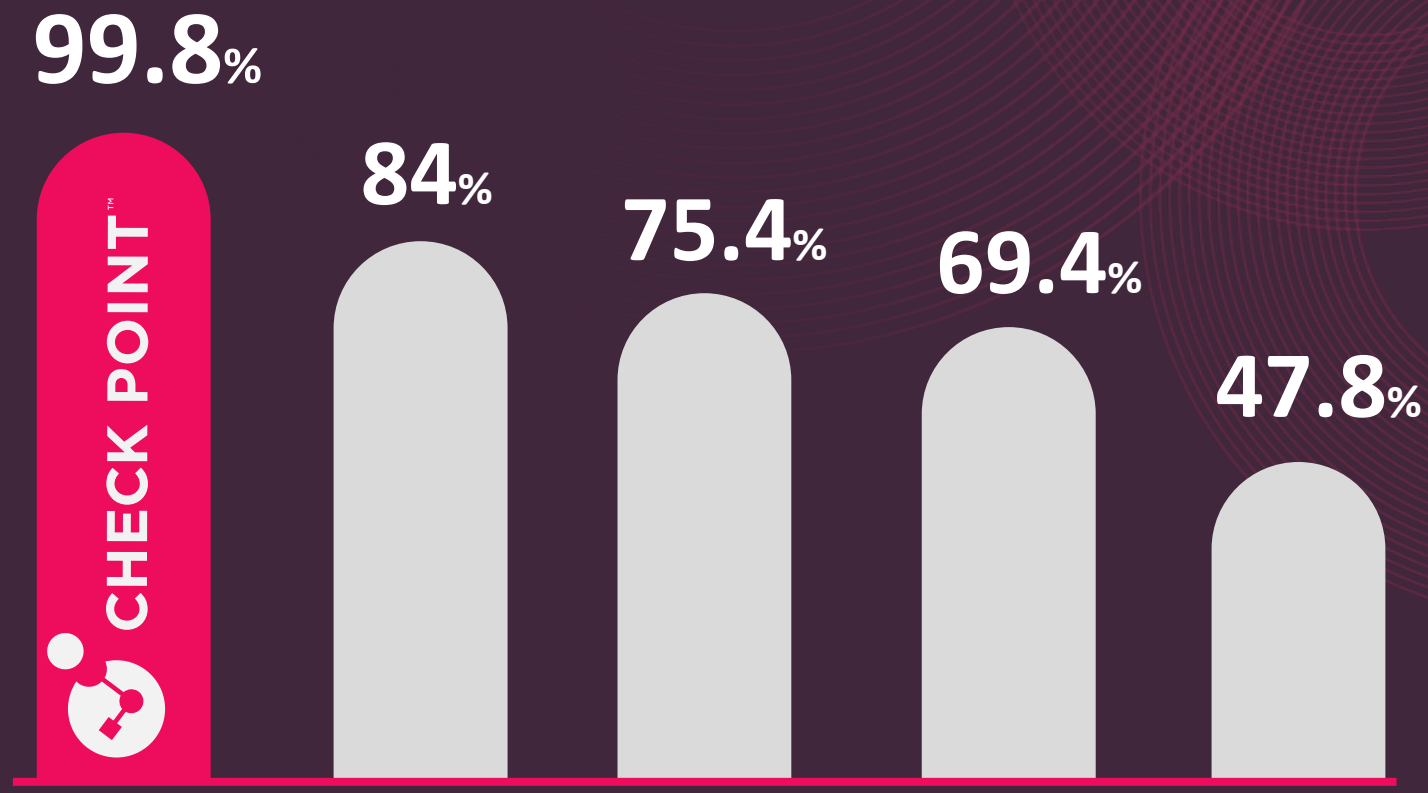
In Threat Prevention.
AGAIN

99.8%
Unknown Attacks
Prevented

100%
Zero Phishing Attacks
Prevented

2024 Security Benchmark Report

Zero+1 Malware Prevention Rate



ThreatCloud AI

#1 Miercom

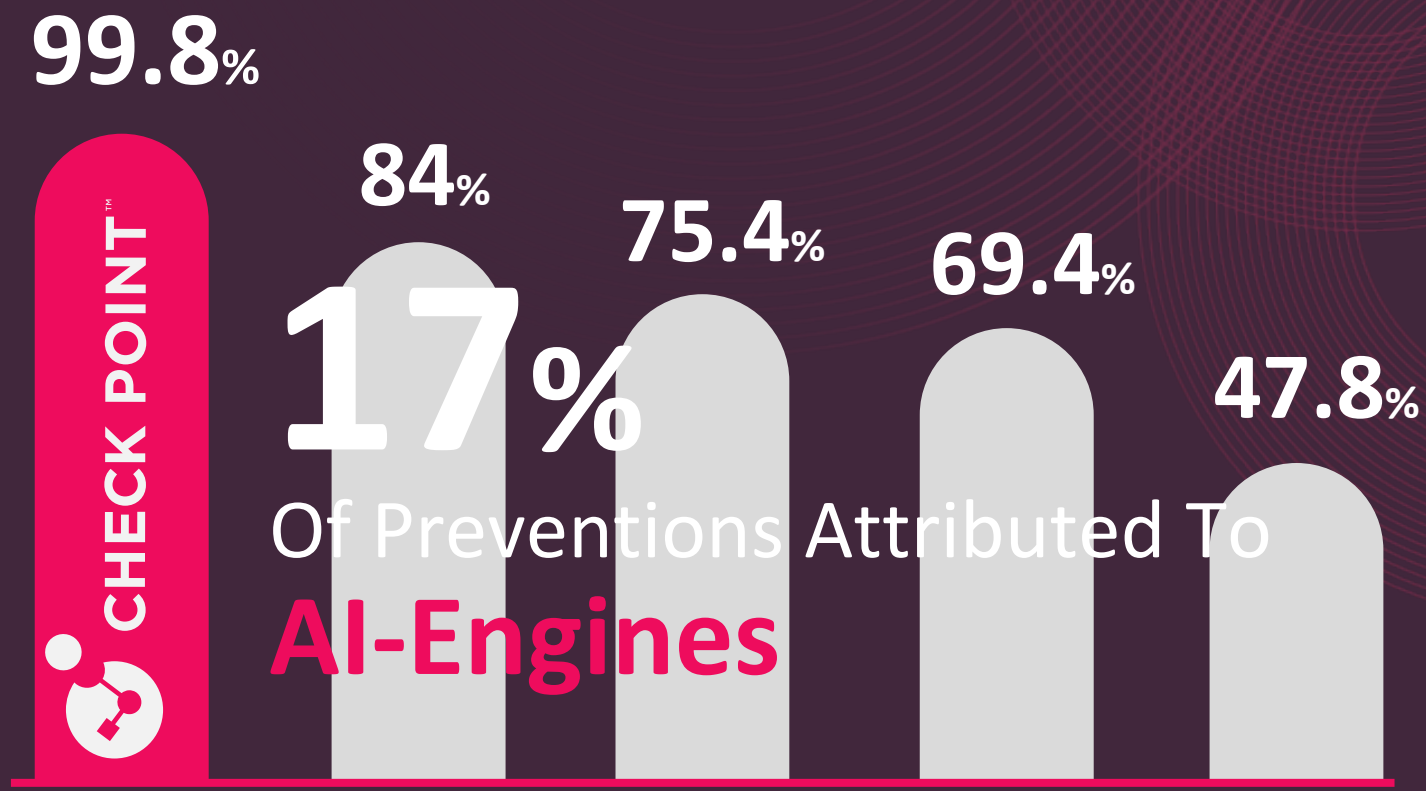
In Threat Prevention.
AGAIN

99.8%
Unknown Attacks
Prevented

100%
Zero Phishing Attacks
Prevented

2024 Security Benchmark Report

Zero+1 Malware Prevention Rate



17%
Of Preventions Attributed To
AI-Engines

Infinity AI Copilot

Your Most Powerful Security Teammate

Powerful, Generative AI engine

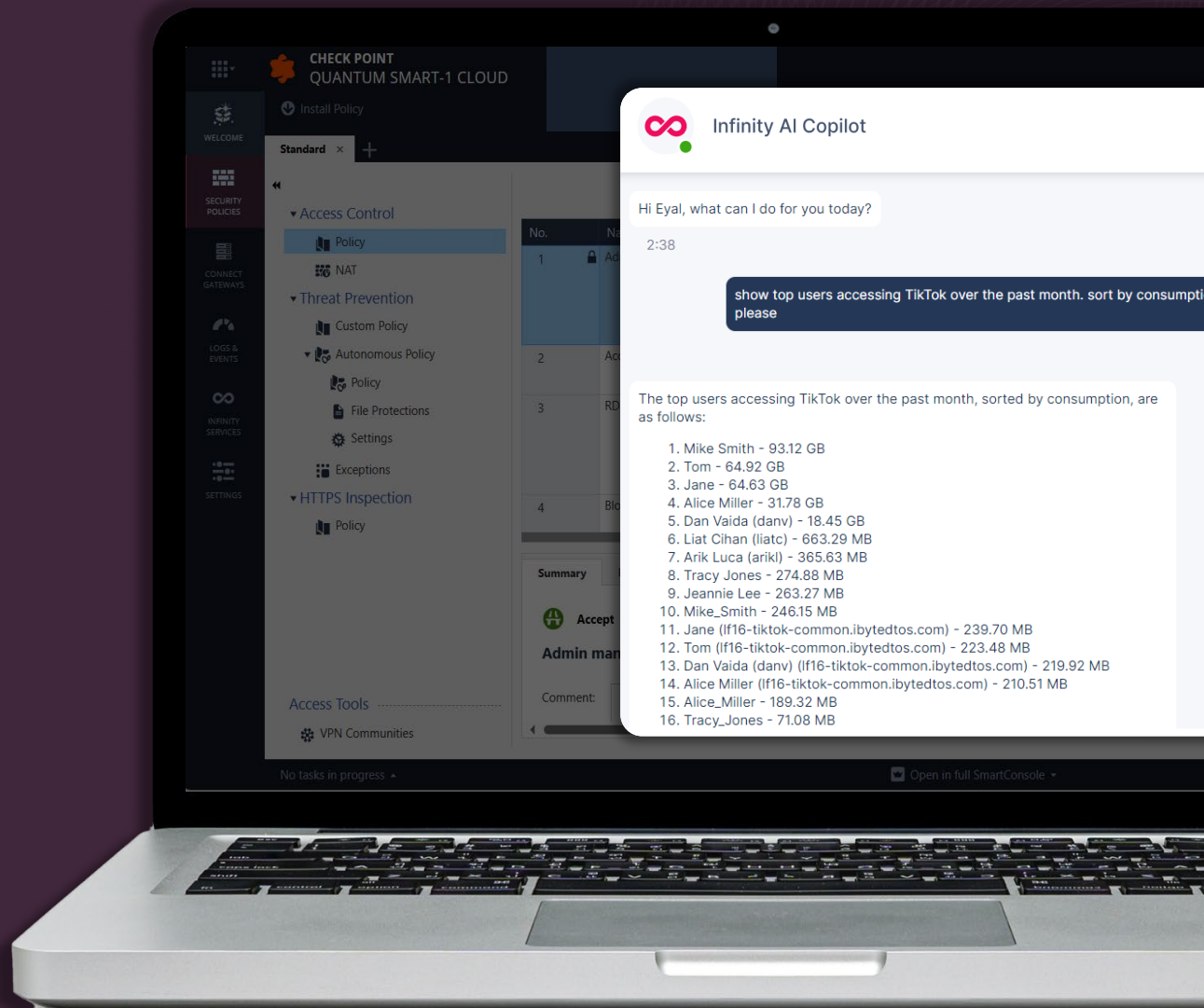
Embedded in the Infinity Platform

NEW

Security Admin Copilot

NEW

Security Analyst Copilot



Summary

AI is a force multiplier:
Leverage it and don’t stay behind.

Both attackers and defenders use AI.

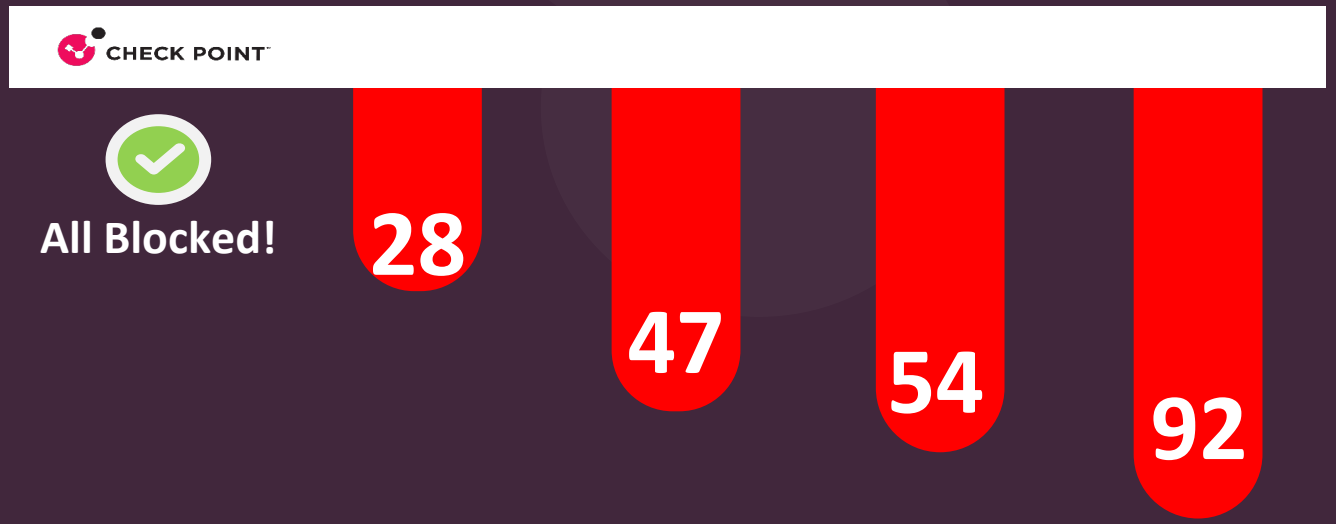
Check Point is one step ahead delivering Best Security . AI Powered & Cloud Delivered

Miercom

#1 in Miercom 2024
Security Benchmark

99.8 %

Zero Day+1 Attacks Prevented



THANK YOU