



On the Intersection of AI and Cyber Security

Why should you care about AI

AI as a force multiplier

Safety

Success / force multiplier

- Be more effective
- Innovate
- Change how we develop and operate

Social

If you will not leverage the AI-multiplier, you will lag behind. You have the right to be concerned about:

- Fake and manipulative information
- Bias, ethics and more

Why should leaders and organizations care about AI

AI as a force multiplier

Efficiency

Business growth

- Increase win rate
- Manage workforce to success
- Customer satisfaction

Development

- Configuration and testing
- Develop conversational applications

Operations continues

- Monitoring
- Remediation
- Quality

If you do not leverage the AI-multiplier, you will lag behind

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



**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 uses 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 uses 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 (1/3)



See OWASP Top 10



Govern access to AI & data

- Access to AI services (SaaS security & application control aspects).
- Data leak prevention, Intellectual property.
- You [start to] collect all the data. Who can access [customer] data?



Monitoring your security

- Requires new type of red team against the AI (these are different practices)?



Secure AI & data pipeline (supply chain)

- AI create a pipeline of development-delivery-production, which carries all supply chain and secure coding issues.

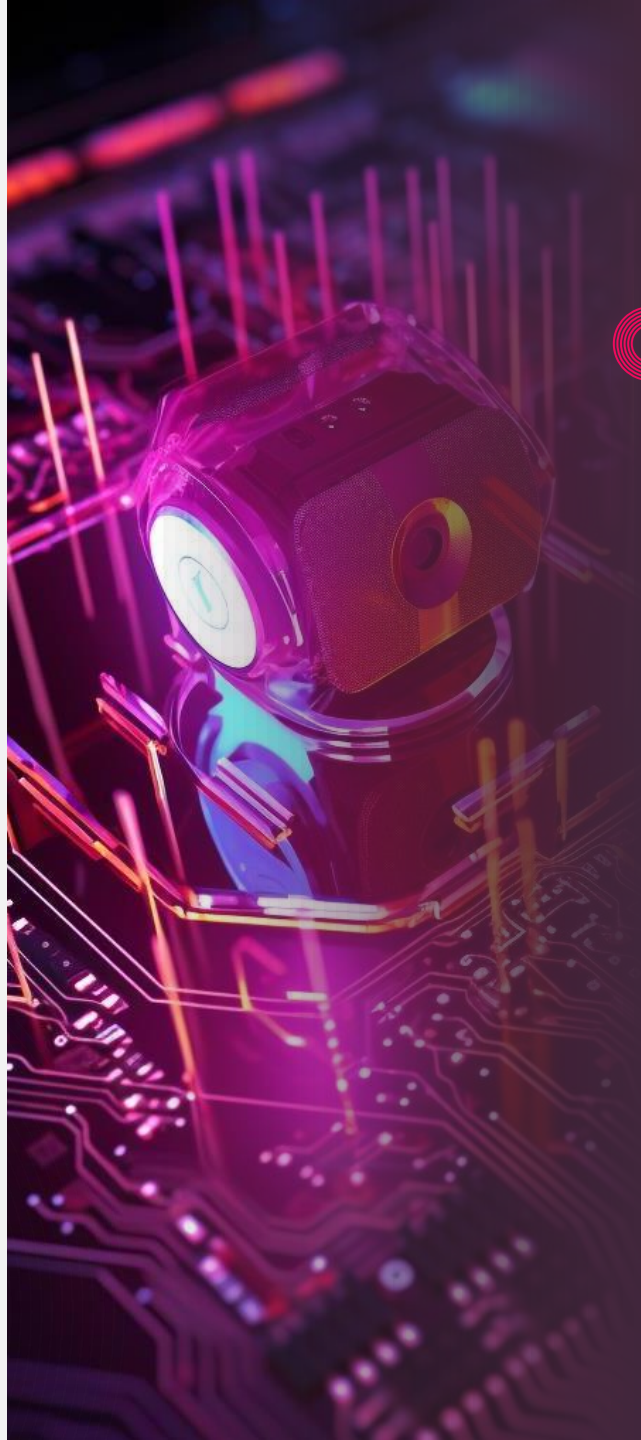
AI meets cyber #3: Protect your AI & data usage (2/3)



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

Infinity Portal – an AI Powered solution

We Delivered



Quantum
Secure the Network



CloudGuard
Secure the Cloud



Harmony
Secure the Workspace



Infinity Core Services



Our Mission:

Best Threat Prevention

**Check Point
Infinity Platform**

AI-Powered. Cloud-Delivered.



10 New Engines, AI-Powered

Quantum Titan's AI Deep Learning Engines Detect and Block Zero-Day Phishing Attacks in Real Time

Since its launch in September 2022, Check Point's Quantum Titan AI Deep Learning engines have processed over 100 million phishing pages, identifying and blocking over 100,000 zero-day phishing attacks in real time.

New Zero-Phishing AI Engines - 34 more phishing pages detected, 40% higher detection rate

Zero Phishing

Preventing DNS Tunneling with AI Deep Learning

DNS Tunneling is a technique used by attackers to exfiltrate data and bypass security controls. Check Point's AI Deep Learning engines can detect and block DNS tunneling attacks in real time.

Deep DNS

Prevents 5X more sophisticated DNS attacks

Block C&C communications and Data theft with Deep Learning engines

Deep Learning engines can detect and block sophisticated DNS attacks, including Domain Generation Algorithms (DGA), in real time.

Deep DGA

Brand Spoofing Prevention - Check Point Software Technologies' AI-Powered Pre-emptive Zero Phishing Prevents Local and Global Brand Impersonation Attacks

Check Point's AI-Powered Pre-emptive Zero Phishing engines can detect and block brand impersonation attacks, including local and global brand impersonation, in real time.

Brand Spoofing

ClearSite - URLs

ClearSite - URLs is a new engine that can detect and block malicious URLs, including those generated by artificial intelligence, in real time.

Massive global scale phishing campaign using malicious PDFs, identified and blocked by new ThreatCloud AI engine

Check Point has recently identified and blocked a massive global scale phishing campaign that targeted millions of users with malicious PDF files.

Deep PDF

LinkGuard: a New Machine Learning Engine Designed to Detect Malicious LNK Files

LinkGuard is a new machine learning engine designed to detect and block malicious LNK files, which are often used to deliver malware.

LNK Guard

Map the macro functions and turn them to Node Graph

DeepVBA is a new engine that can detect and block malicious VBA macros, which are often used to deliver malware.

DeepVBA

The Rise of the Code Package Threat

Check Point details two recent attacks detected and blocked by the new Code Package engine.

Code packages

THREATCLOUD GRAPH

Graph - URLs is a new engine that can detect and block malicious URLs, including those generated by artificial intelligence, in real time.

Graph - URLs

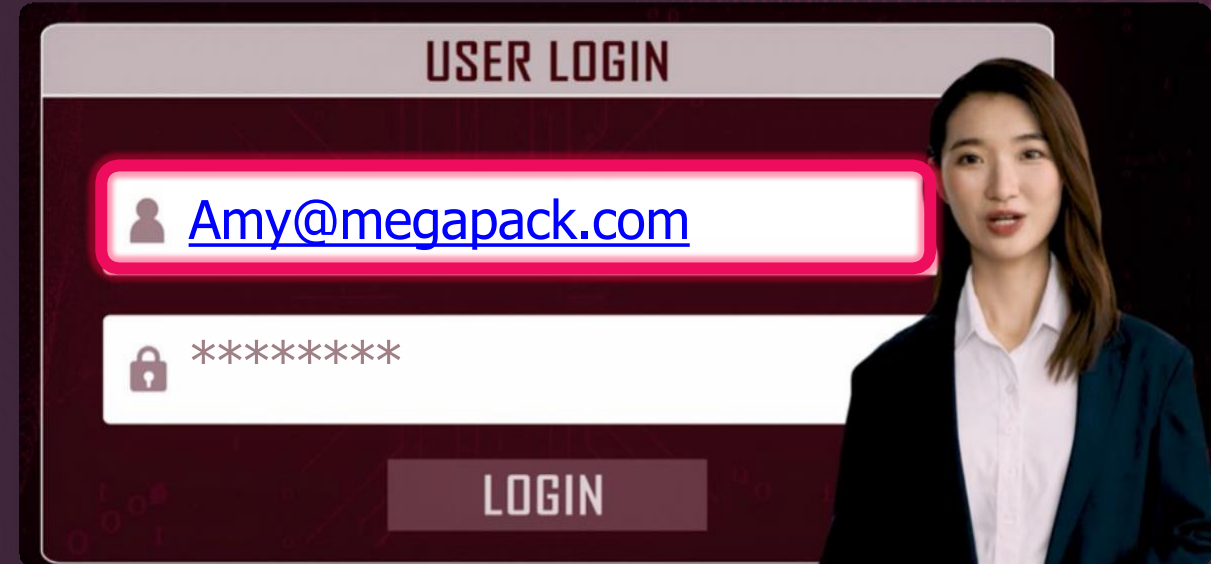
Infinity ThreatCloud AI

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



 Infinity Core Services

Our Mission:

Best Threat Prevention

**The Most Effective Security
Management**

**Check Point
Infinity Platform**

AI-Powered. Cloud-Delivered.



Real-Time Threat Prevention

90+

Security Engines

50+

Are AI-Powered

3B

Yearly Attacks
Prevented

<2 Sec

Synced globally to all
enforcement points



Infinity AI Copilot

Your Most Powerful Security Teammate

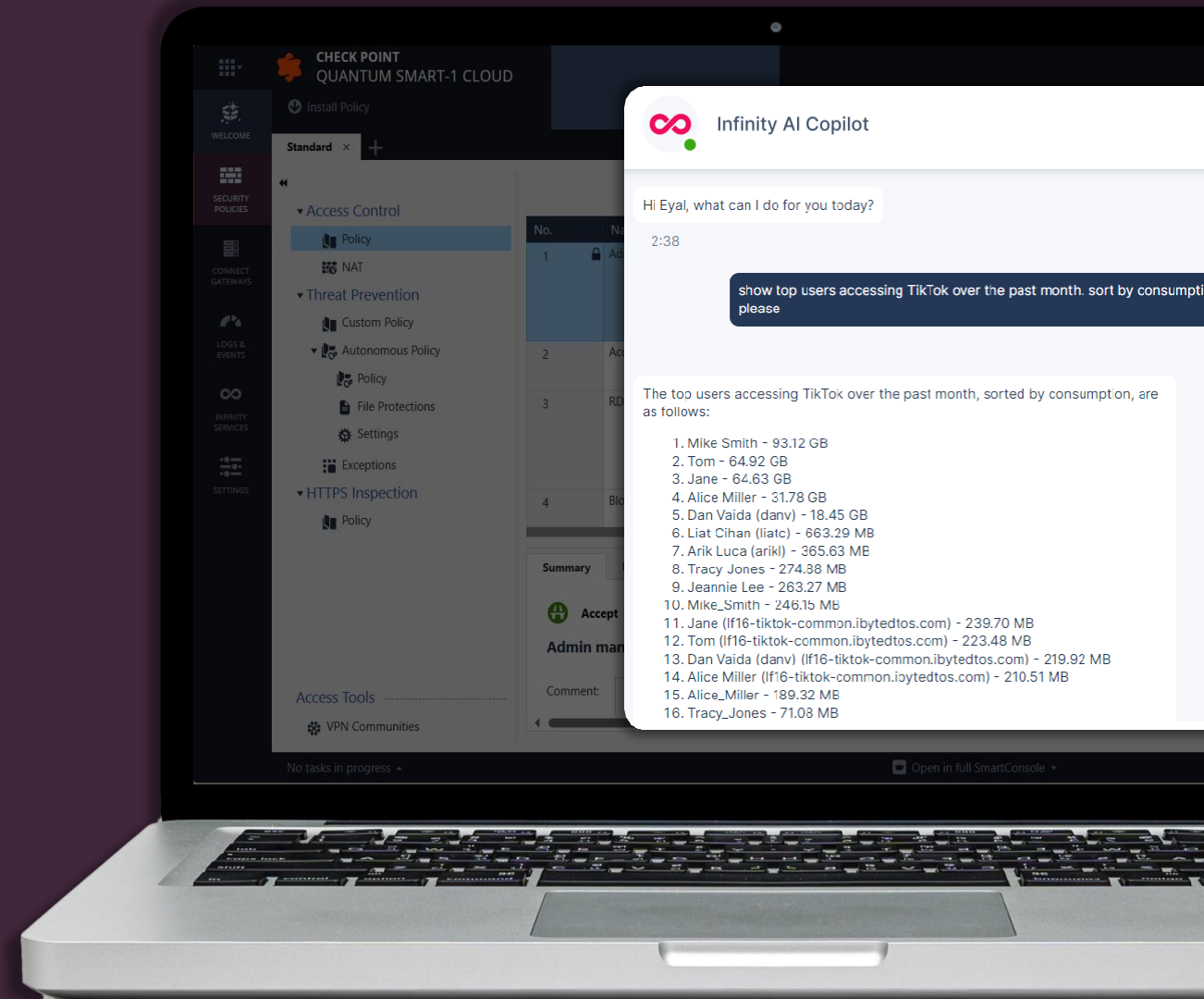


Powerful, Generative AI engine
Embedded in the Infinity Platform

Security Admin Copilot



Security Analyst Copilot



We need a **platform** to
defend against what's coming

AI = friendship



Check Point 2024:

The Platform Company

AI-Powered



Cloud-Delivered

Comprehensive | Consolidated | Collaborative

THANK
YOU

