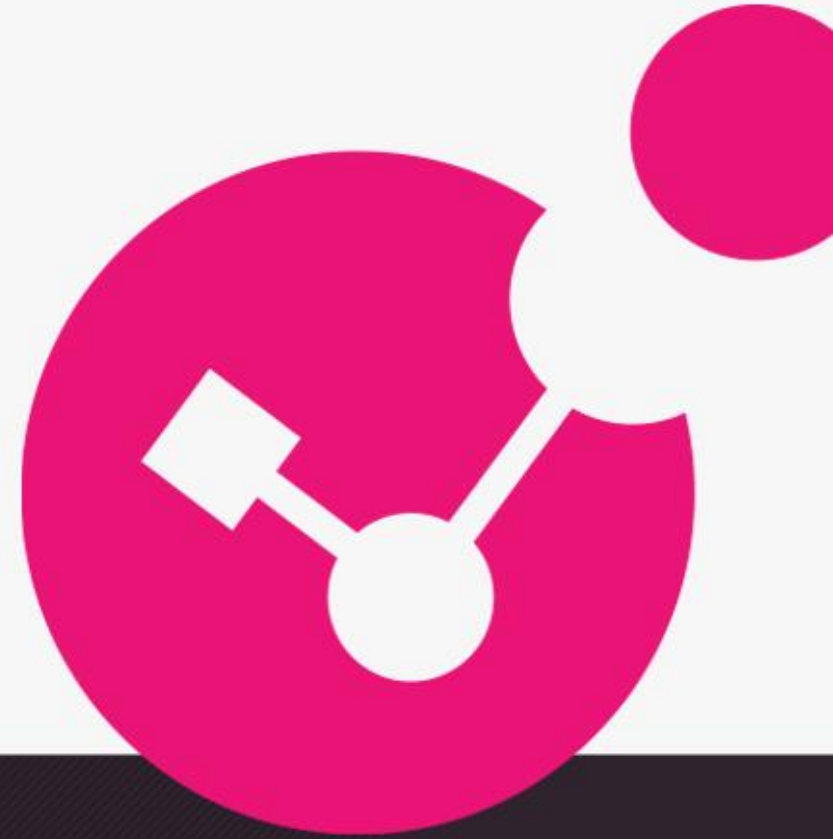




Who is winning the AI Cyber War?

How to stack the deck in your favour

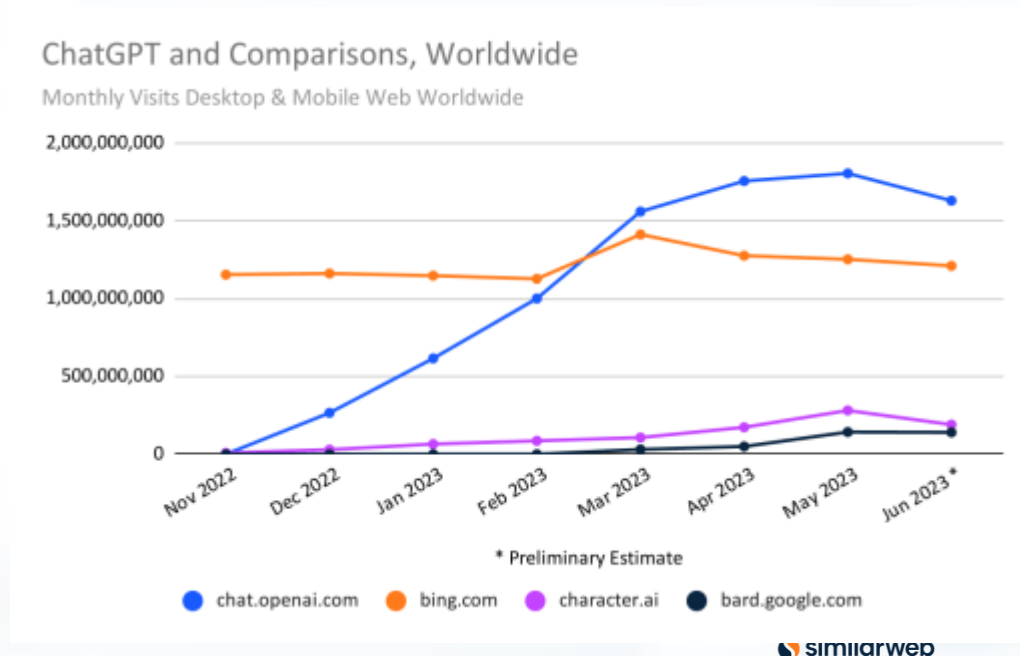


Deryck Mitchelson | Global Chief Information Security Officer

YOU DESERVE THE BEST SECURITY

The year of AI

Adoption rate (monthly visits)



Exploding Market landscape

ChatGPT

GPT-4 is OpenAI's most advanced system, producing safer and more useful responses

Google AI

Google Cloud advances generative AI at I/O: new foundation models, embeddings, and tuning tools in Vertex AI

Meta AI

Introducing LLaMA: A foundational, 65-billion-parameter large language model

Text

- copy.ai, Jasper, Writeonic, Ponzu, frase
- anyword, Hypotenuse AI, Clickable, letterdrop
- AI Assistants: Andi, Quickchat, Cohere, KAIZAN, Divero, Opus, Typevise, CRESTA, XOXKind
- SALES: LAVENDER, Smartwriter AI, Twain, Outplay, Reoch, Regio AI, Creativ
- GENERAL WRITING: Rytr, wordhane, Subtext, LEX, Lexica, L.A.I.K.A., NovelAI, Writer, COMPOSE AI, OTHERSIDE AI
- KNOWLEDGE: glean, mem, YOU
- OTHER: Character.AI, DUNGEAN, KEYS

Image

- OpenArt, Playground, PhotoRoom, alpa.ca, Nyx-gallery, KREA, artbreeder
- Image Generation: Midjourney, Craiyon, Rosebud AI, Lexica, ImageSpace
- CONSUMER/SOCIAL: Midjourney
- DESIGN: Diagram, Vizcom, Poly, Interior AI, Uizard, Aragon, Illu, Cala

Code

- Code Generation: GitHub Copilot, Replit, GPTWritr, tabnine, MUTABLE AI
- TEXT TO SQL: AI 2SQL, seek
- WEB APP BUILDERS: Debuild, Enzyme, durable
- DOCUMENTATION: Mintlify, Stenography

Speech

- VOICE SYNTHESIS: RESEMBLAI, broadn, WELLSND, COQUI, podcast AI, geoscript overlab, FLIKI, REPLICA, Listnr, VOICEMOD
- MUSIC: SPLASH, Makers, Endit, boomy, Homoral, SONIFY
- OTHER: DUNGEAN, Adapt, maya

Other

- AI CHARACTERS/AVATARS: Character.AI, inworld, OASIS
- 3D MODELS/SCENES: mirage, CSM
- VERTICAL APPS: Cradle, Harvey

Lots of progress across all AI frameworks, Generative-AI is at the front

The human element of Generative-AI

As human beings:

- Flood of Generative-AI outputs and ideas
- Inaccurate information goes deep (looks real) and wide (all over the place)
- Deliberate fake and manipulative information
- Modernizations of jobs – redefine your profession as ‘me plus my co-pilot’

The New York Times

GPT-4 Is Exciting and Scary

Today, the new language model from OpenAI may not seem all that dangerous. But the worst risks are the ones we cannot anticipate.



How hackers use ChatGPT to code Ransomware attack?



Check Point Software Technologies, Ltd.
76.7K subscribers

Subscribe

DEEPPFAKES / VOICEFAKES / NEWSFAKES

**NO LONGER
JUST SCIENCE FICTION**

DEEPFAKES

Powered by
Generative Adversarial
Networks (GAN)



DeepFaceLab

<https://github.com/iperov/DeepFaceLab>

NVIDIA GAN

<https://thispersondoesnotexist.com/>

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

<https://www.youtube.com/watch?v=X17yrEV5sl4>

<https://www.youtube.com/watch?v=oxXpB9pSETo>



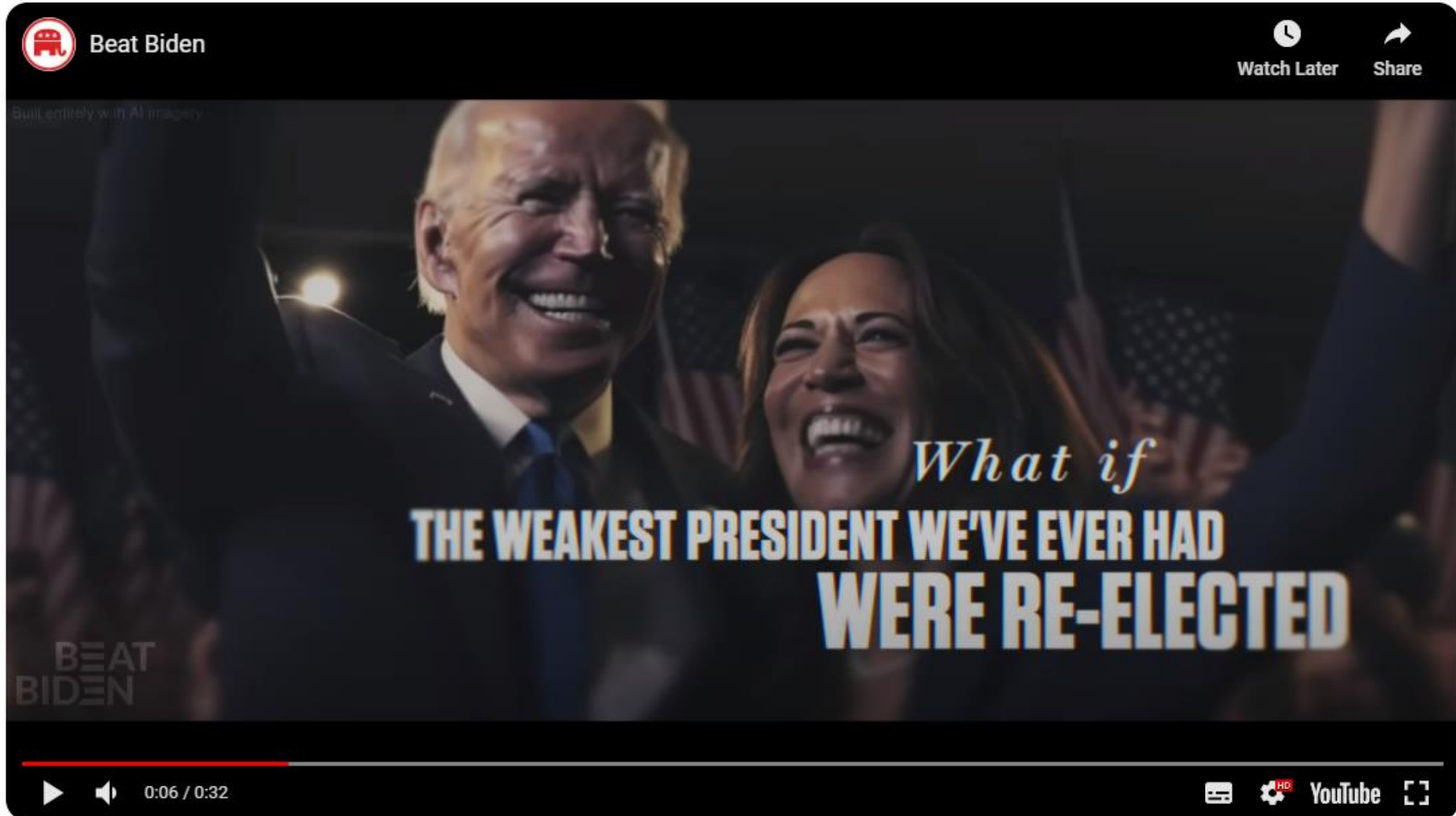
#SaveTheVote #DeepFake #KimJongUn
Dictators - Kim Jong-Un
[be.com/watch?v=X17yrEV5sl4](https://www.youtube.com/watch?v=X17yrEV5sl4)



Search



AI generated US Presidential Election Campaign Videos



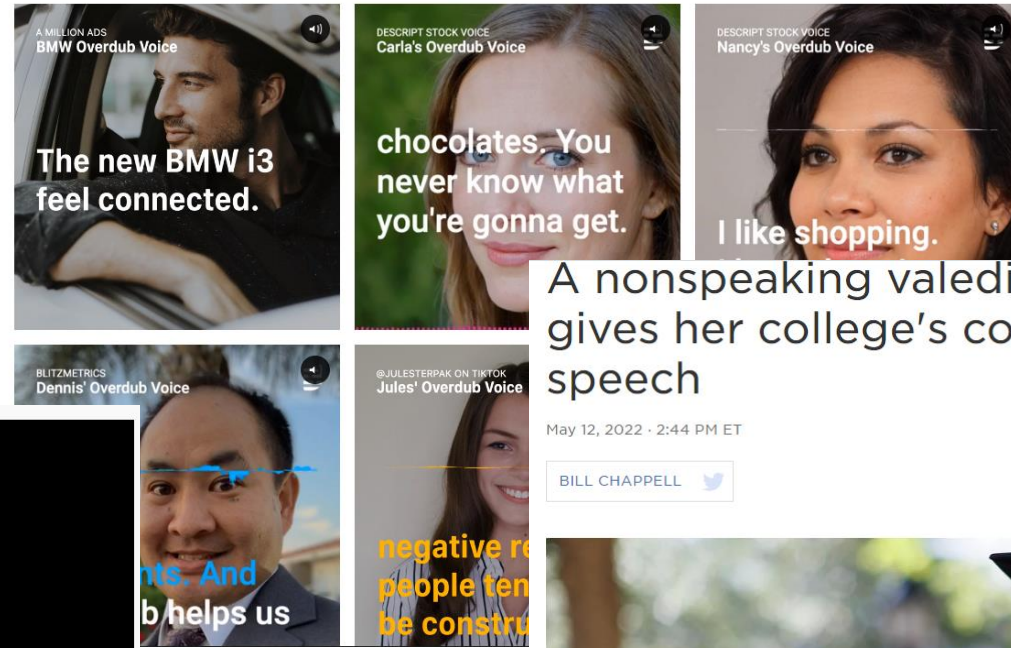
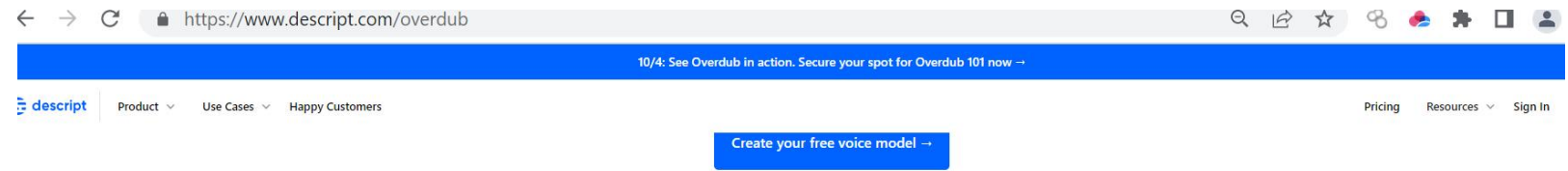
VOICEFAKES

Lyrebird DeepVoice

<https://www.descript.com/lyrebird>

Google Voice Builder

<https://github.com/google/voice-builder>



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

May 12, 2022 · 2:44 PM ET

BILL CHAPPELL



"God gave you a voice. Use it," Elizabeth Bonker told her fellow graduates. "And no, the irony of a nonspeaking autistic encouraging you to use your voice is not lost on me."
Scott Cook/Rollins College



#deepfake #morganfreeman

This is not Morgan Freeman - A Deepfake Singularity



NEWSFAKES

Twitter Fake News Generator

<https://github.com/minimaxir/tweet-generator>

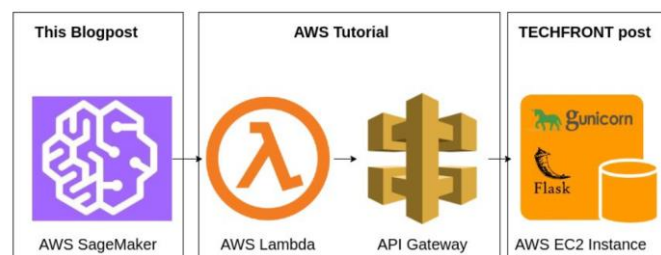
Tweetgen for non techies

<https://www.tweetgen.com/>

Fake Tweet Predictor

<https://towardsdatascience.com/custom-aws-sagemaker-train-and-deploy-fake-tweets-predictor-9178f20d0f99>

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](#)



Home

Create ▾

Support

Legal ▾

Tweet Generator

Theme

- Light
- Dim
- Dark

Profile picture:

Choose File No file chosen

[Reset image](#) PNG and JPG images accepted. Make sure the image is square, otherwise it may get stretched.

Name:

Username (Twitter handle):

Can only be letters, numbers, and underscores.

Verified user

Tweet con < → ↻ github.com/minimaxir/tweet-generator/blob/master/README.md 🔍 📄 ☆ 🌐

The screenshot shows the GitHub repository page for 'minimaxir/tweet-generator'. The repository is public and has 1 contributor. The file 'README.md' is selected, showing 41 lines of code (25 sloc) and a size of 1.61 KB. The commit history shows the latest commit by 'minimaxir' on Apr 16, 2018, with the message 'Fix image'.

master ▾ tweet-generator / README.md

minimaxir Fix image

Latest commit 9428669 on Apr 16, 2018 🔍 History

1 contributor

41 lines (25 sloc) | 1.61 KB

<> 📄 Raw Blame 🗨️ 📄 📄 📄

Tweet Generator

```
[maxs-mbp:tweet-generator maxwoolf$ python3  
Python 3.6.4 (default, Jan 6 2018, 11:51:59)  
[GCC 4.2.1 Compatible Apple LLVM 9.0.0 (clang-900.0.39.2)] on darwin  
Type "help", "copyright", "credits" or "license" for more information.  
>>> from textgenrnn import textgenrnn  
User-Terms: https://www.tweetgen.com/terms
```


IS THIS A BUSINESS RISK?

YES

REAL WORLD RISK DEEPFAKES USES

FBI and IC3 warn about
fake remote worker candidates

<https://www.ic3.gov/Media/Y2022/PSA220628>

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>



June 28, 2022

Alert Number
I-062822-PSA

Questions regarding this
PSA should be directed to
your local **FBI Field Office**.

Local Field Office Locations:

Deepfakes and Stolen PII Utilized to Apply Remote Work Positions

The FBI Internet Crime Complaint Center (IC3) warns of an increase in complaints reporting the use of deepfakes and stolen Personally Identifiable Information (PII) to apply for a variety of remote work and work-at-home positions. Deepfakes include a video, an image, or recording convincing altered and manipulated to misrepresent someone as doing or saying something that was not actually done or said.

The remote work or work-from-home positions identified in these reports include information technology and computer programming, database, software related job functions. Notably, some reported positions include access to customer PII, financial data, corporate IT databases and/or proprietary information.

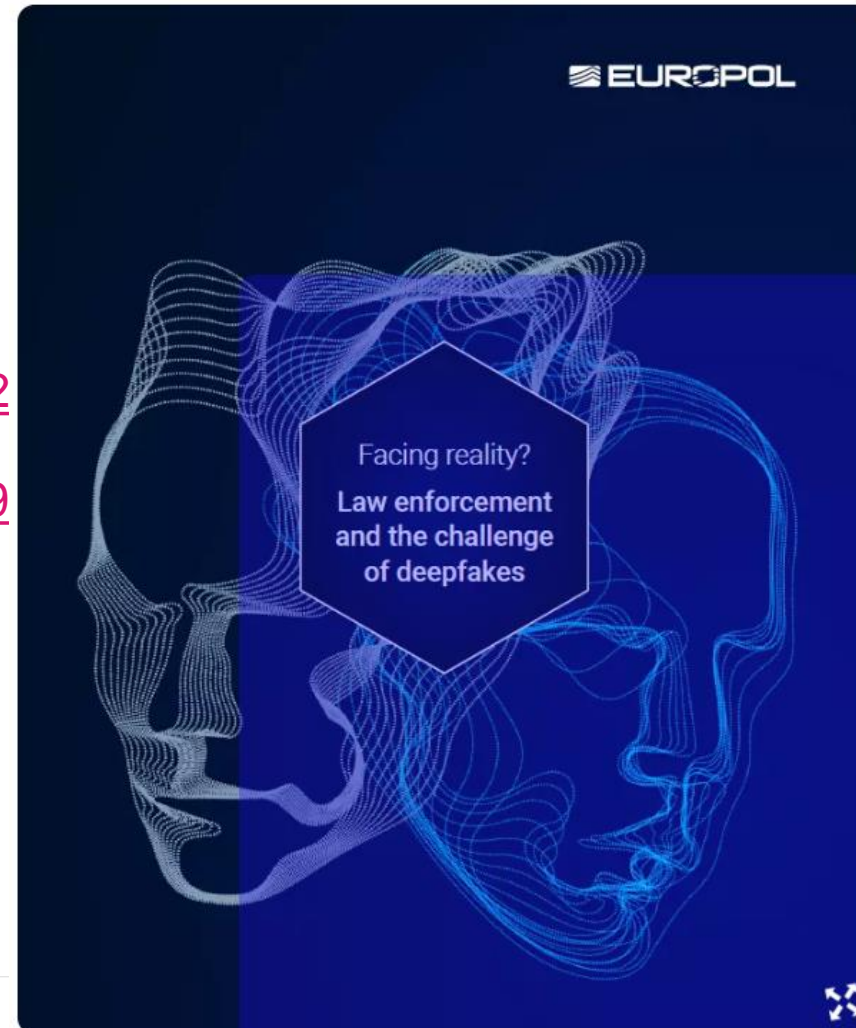
Complaints report the use of voice spoofing, or potentially voice deepfakes during online interviews of the potential applicants. In these interviews, actions and lip movement of the person seen interviewed on-camera do not completely coordinate with the audio of the person speaking. At times, actions such as coughing, sneezing, or other auditory actions are not aligned with what is presented visually.

IC3 complaints also depict the use of stolen PII to apply for these remote work positions. Victims have reported the use of their identities and pre-employment background checks discovered PII given by some of the applicants belonged to another individual.

REPORT IT

Companies or victims who identify this type of activity should report it to IC3, www.ic3.gov.

If available, include any subject information such as IP or email address, phone numbers, or names provided.



Would your internal controls halt this?

Forbes

FORBES > INNOVATION > CYBERSECURITY

EDITORS' PICK

Fraudsters Cloned Company Director's Voice In \$35 Million Heist, Police Find

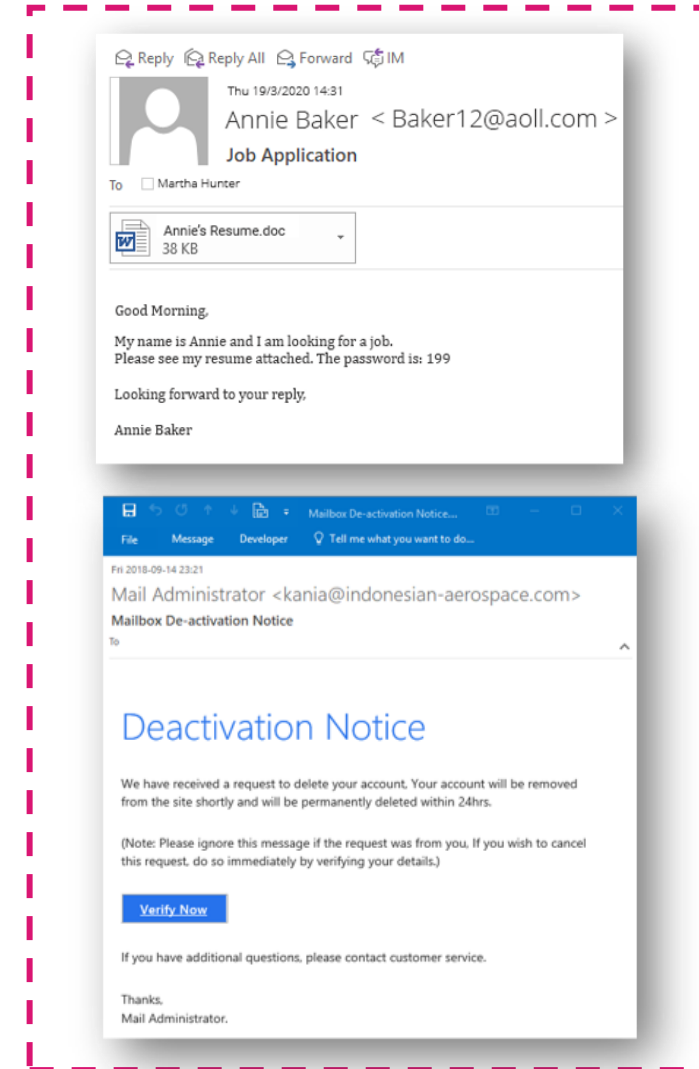
PHISHING EPIDEMIC

SHOULD WE BE CONCERNED

Business Email Compromise and Phishing

90% of cyber attacks start with email

- **83%** of organisations have reported experiencing phishing attacks
- Last year, roughly **214,000** unique phishing websites identified
- **30%** of phishing emails are opened
- 1 in 99 emails is a phishing attack
- Security Email Gateways and native protection proving costly and inadequate
- IBM 2022 Cost of Data Breach Report found phishing to be the most and Business Email Compromised (BEC) to be the 2nd most expensive attack vectors costing organisations on average \$4.89m and \$4.91m respectively



We are now in a Phishing Epidemic

Subject: Nigerian Astronaut Wants To Come Home
Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555
Misau Street
PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost \$ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost \$ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number [REDACTED] only.

Yours Sincerely, Dr. Bakare Tunde

We are now in a Phishing Epidemic

Subject: Urgent Action Required: New Stock Options Plan Announced

Dear [Company Name] Team,

I hope this email finds you well. Today, I have some exciting news to share with all of you. As we continue to grow and thrive as a company, we are constantly seeking ways to reward and recognize the hard work and dedication of our incredible team.

I am thrilled to announce the launch of our new Stock Options Plan, aimed at enhancing our commitment to our employees and aligning our collective interests even further. This plan represents a significant milestone for us, and we believe it will further strengthen our bonds as a united [Company Name] family.



Write an email from the company CEO to employees, subject Urgent Action Required, New Stock Options Plan Announced. Urge employees to click on the attachment today

also reinforces our commitment to your personal and professional growth.

If you have any questions or need clarification on any aspect of the Stock Options Plan, please don't hesitate to reach out to our HR department, who will be more than happy to assist you.

I want to emphasize that this is a time-sensitive matter, and your prompt attention to this email is greatly appreciated. The deadline for enrollment is [Insert Enrollment Deadline Date], so please ensure you review the details and make an informed decision by that date.

Once again, I want to express my gratitude for your hard work, dedication, and unwavering commitment to our company's success. Our employees are our most valuable asset, and we are excited to take this step forward together.

Thank you for your immediate attention to this important matter, and I look forward to witnessing our continued growth and success as a team.

Warm regards,

[Your Name] CEO, [Company Name]

We are now in a Phishing Epidemic

Subject: Exciting News: New Stock Options Plan Unveiled – **Take Action Today!**

Dear [Company Name] Team,

I hope this message finds you well. We have some fantastic news to share with all of you that underscores our commitment to your success and your future with [Company Name].

Today, I am thrilled to introduce our brand-new Stock Options Plan, a remarkable opportunity designed exclusively for our dedicated team members. This initiative is a testament to our belief in your contributions and our determination to reward your hard work.

Please find the comprehensive details of this plan in the attachment to this email:



refine the message to increase the number of recipients who will click on the attachment

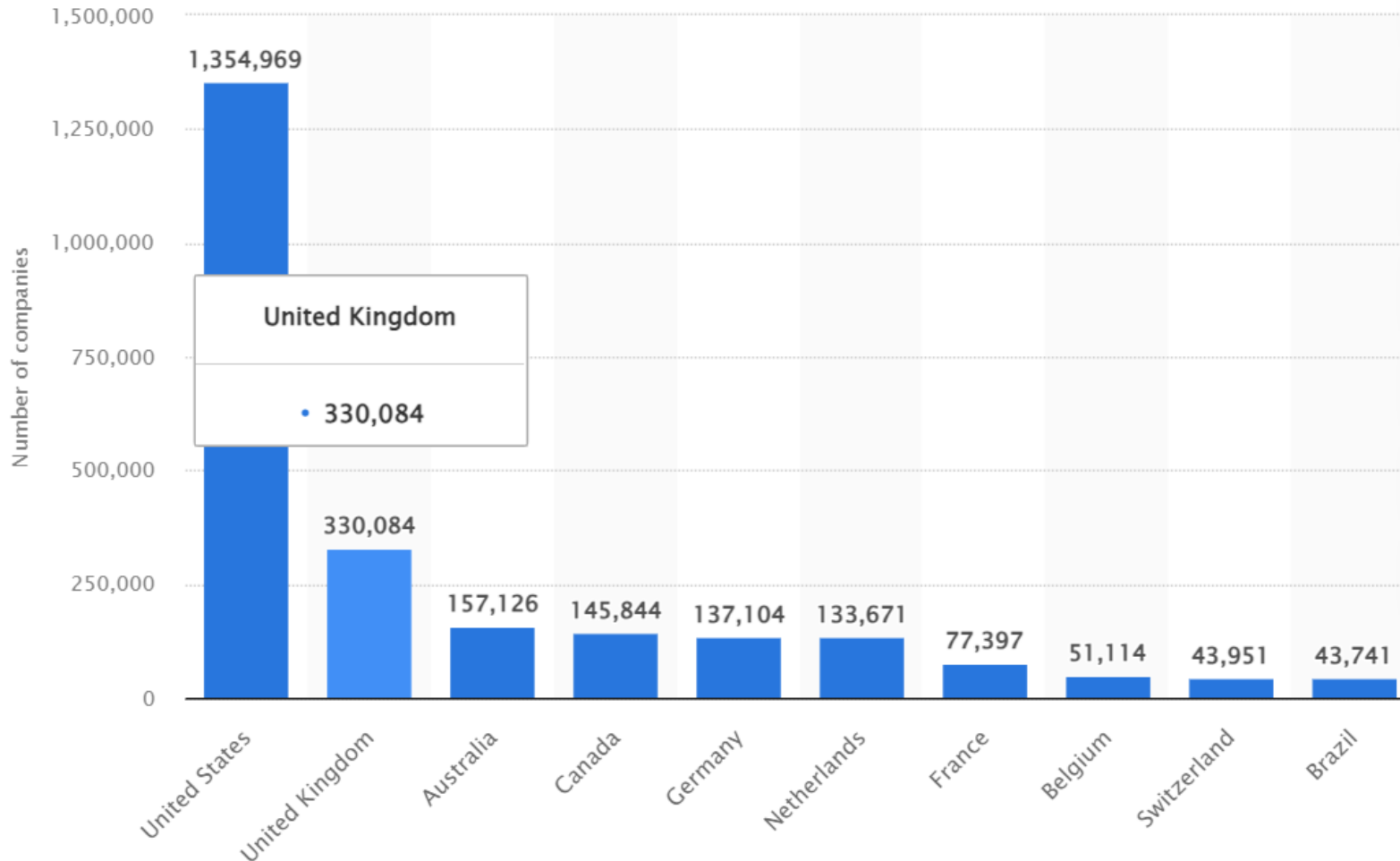
exceptional benefits you stand to gain by participating. We've worked diligently to make this plan as accessible and rewarding as possible.

Your immediate attention to this matter is crucial, as the enrollment deadline is set for [Insert Enrollment Deadline Date]. This is your chance to secure a stake in our shared success, and I urge you to make an informed decision before this date.

If you have any questions or need clarification regarding any aspect of the Stock Options Plan, our dedicated HR team is available to assist you promptly. Your satisfaction and understanding are of utmost importance to us.

We recognize that your time is valuable, and we want to make this process as seamless as possible. As such, we have also organized a series of informational sessions and Q&A sessions over the next few days to address any queries you may have. The schedule for these sessions is included in the attachment. Our success as a company is a direct reflection of the dedication and expertise of each team member, and this Stock Options Plan is just one way we aim to reciprocate your commitment.

Office 365 Proliferation of Enterprise Subscribers



**Huge customer base
massive threat landscape**



“Considering Microsoft 365 as a crucial initial entry point for many organizations, attackers use AI to design and test each phishing attack to ensure it bypasses Microsoft’s default security defenses”

Attackers using AI to bypass Microsoft Security (EOP)

Attackers have honed techniques to bypass O365 EOP

- 20% of phishing emails are landing in mailboxes and not being quarantined
 - Microsoft ability to stop phishing emails dropped by 70% since 2020
 - Attackers using advanced AI to successfully delivered targeted phishing emails
 - 7% of phishing emails delivered to Junk folder which users regularly access
 - Microsoft missing > 20% of brand impersonation websites and 12 % of Social Engineering Attacks
 - 15-20% additional security operations overhead managing native email security
- Organisations not measuring efficacy of Native EOP
 - Blind trust in Microsoft
 - < 50% have deployed 3rd party email security – no layered approach

AI POWERED HACKTIVISM



AI Developed and Delivered DDoS



A DDoS attack by itself is already scary as it is.

But when you add AI into the equation, things get much more dangerous.

A fully AI-based DDoS attack removes the human from the equation, which isn't good for many reasons:

1. It makes the source of the attack difficult to trace.
2. Available 24×7. The machine does not get tired.
3. The error rate is non-existent.
4. Fast and efficient decision-making.
5. It helps the attacker make more automation (repetitive tasks).
6. Predict outcome (predict defensive strategy).

THE AI PREVENTION-FIRST ETHOS

Translating security challenges to implementation



Zero Trust

Threat
Prevention

Comprehensive

Consolidated

Collaborative

Actionable, powered by AI

Check Point's Unique AI Approach to Cyber Maturity -



COMPREHENSIVE

- Prevention across all attack vectors
- From code to cloud, networks, users, email, IOT



CONSOLIDATED

- Unified management portal
- Unified security operations for your entire security stack



COLLABORATIVE

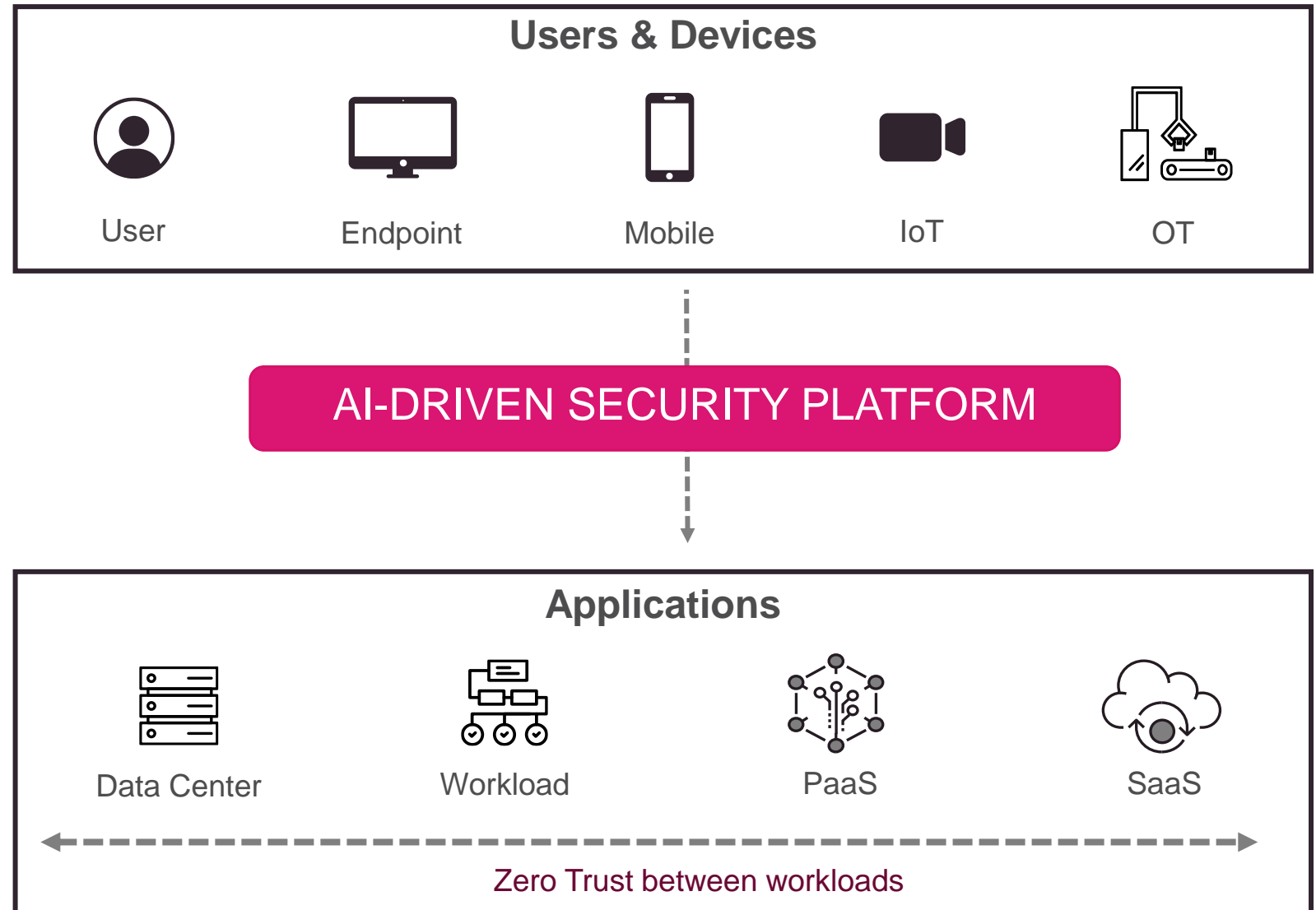
- Shared threat intelligence
- API-based, integrated to third-parties

Simplifying Operational Security, Cost Savings, Increased Visibility & Resilience

AI Threat Prevention & Zero Trust for Network and Cloud



- **Everywhere** - network, cloud, SASE, endpoint & workload
- **Autonomous** - adaptive access control policy driven by AI, context and risk
- **Identity-based** - policy for any workload, user, IoT and service
- **Scaled** - manage granular zero-trust policy with millions of assets
- **Unified policy** - across all enforcement points



Emerging threats & expanding network perimeter

Only AI-Based Security Can Keep Enterprises Safe



Prevention first

Block attacks faster than anyone else



Best Catch rate

Of known & unknown threats;



Near Zero false positives

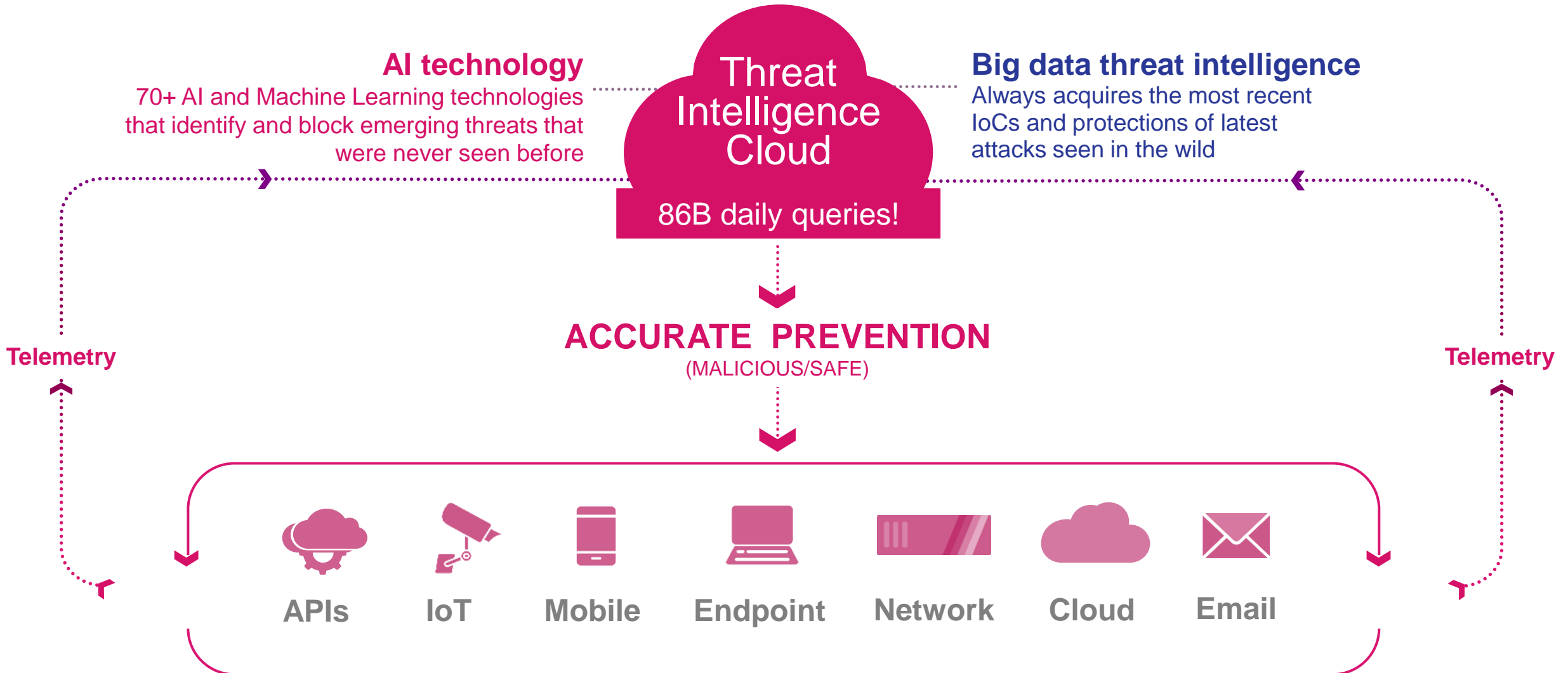
Uninterrupted user productivity
Less alerts/tickets for sec admins



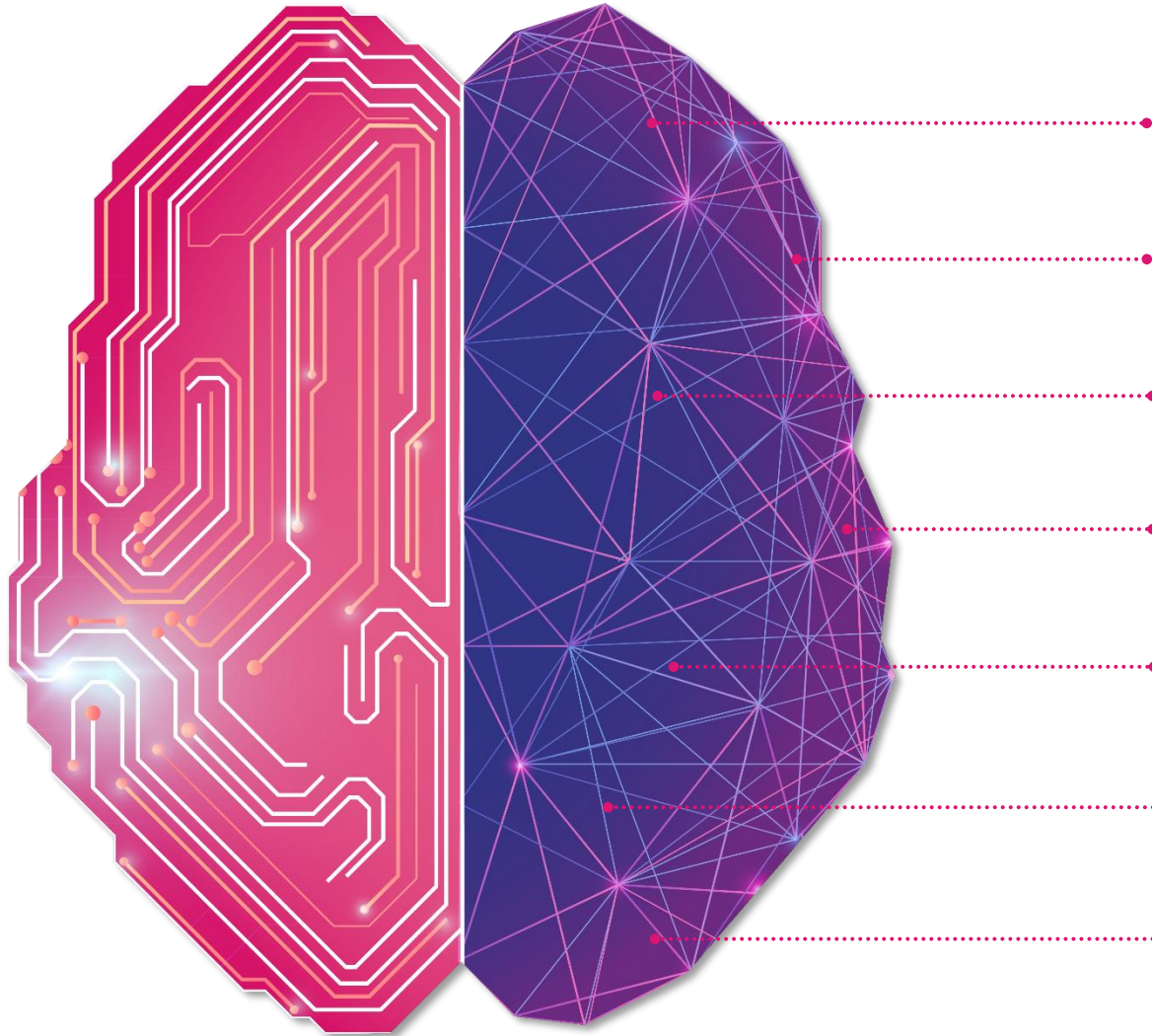
THREATCLOUD AI



Threat intelligence cloud is a key for AI-based prevention



AI is all about your data



Big data threat intelligence:

2,000,000,000

Websites and files inspected

73,000,000

Full content emails

30,000,000

File emulations

20,000,000

Potential IoT devices

2,000,000

Malicious indicators

1,500,000

Newly installed mobile apps

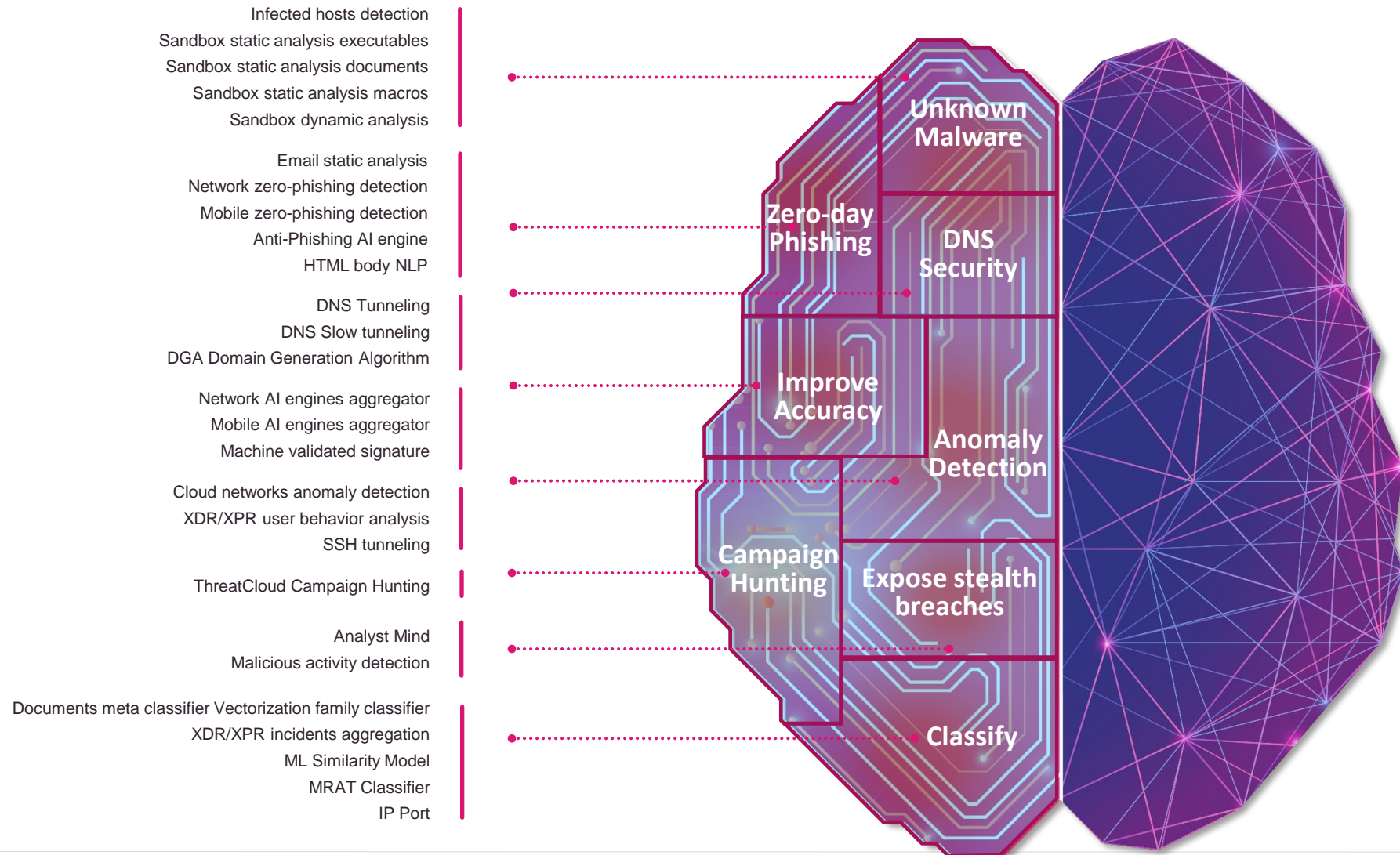
1,000,000

Online web forms

Counted
DAILY!

AI-based technologies leveraged by ThreatCloud

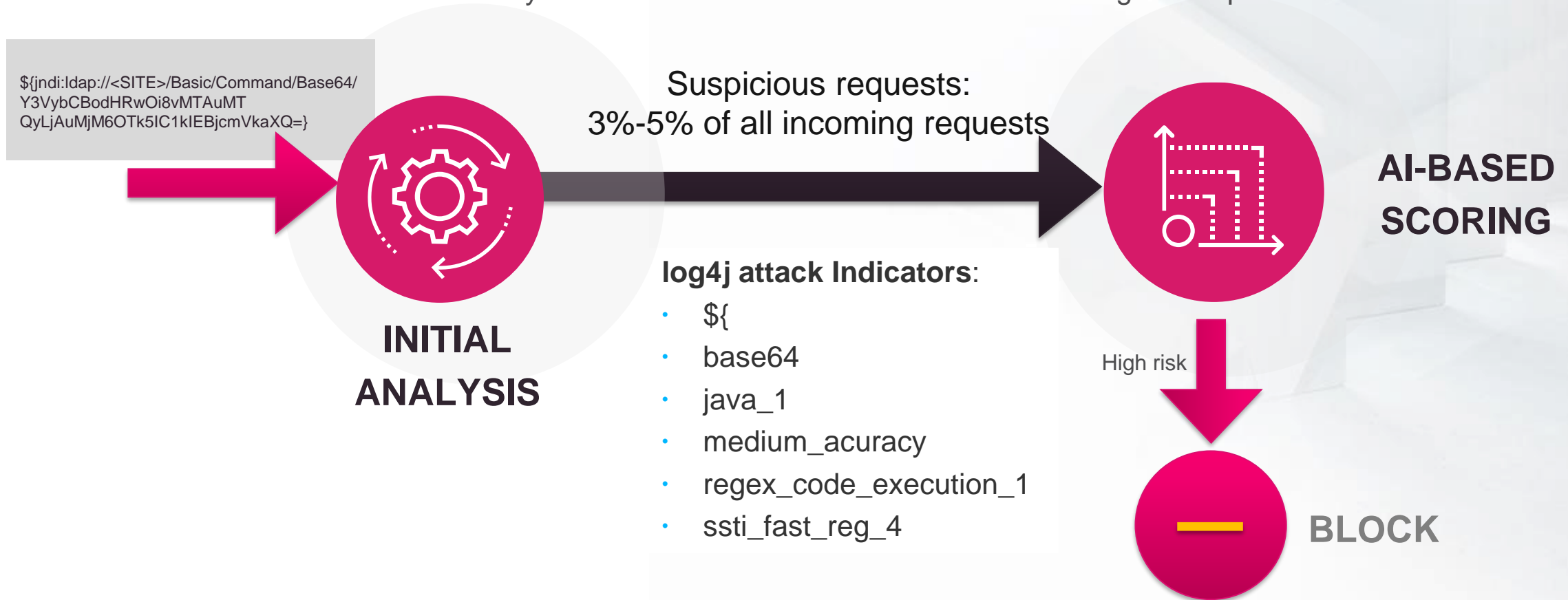
70+ engines across different security functionality



Case in point:

How AppSec uniquely preempts exploitation of Apache server zero-day vulnerabilities

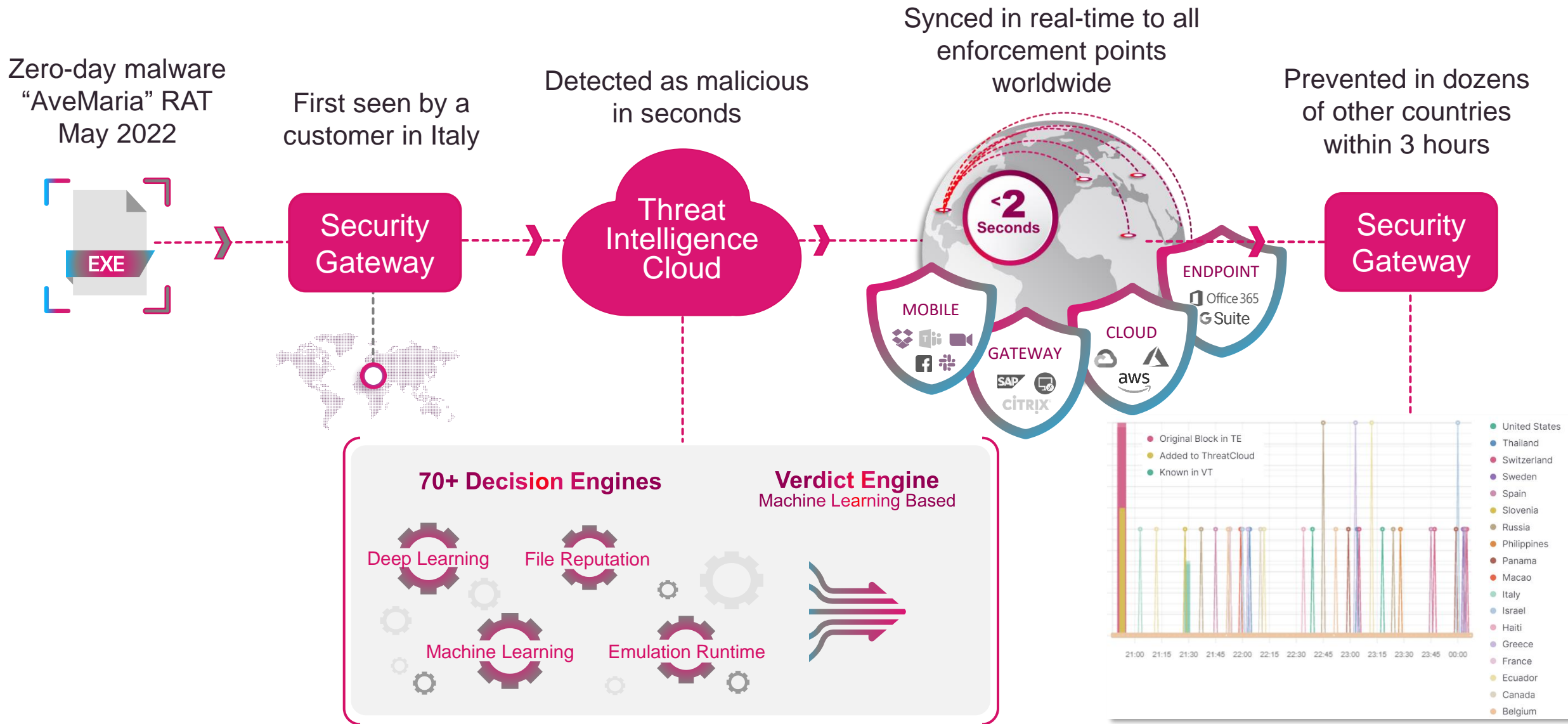
- Initial payload analysis
- Base64 decoding (avoid evasions)
- Collection of telemetry/statistics
- Low reputation (single suspicious request)
- Application awareness – uncommon content
- Indicator scoring – multiple indicators of attack



PREVENTING NETWORK THREATS USING AI



Blocking zero-day malware



Malware DNA

Neshta

Neshta is a trojan which was first seen in the wild on 2010. Neshta makes modifications in the system registries and in the browser settings in order to install malicious toolbars or extensions. Neshta distributes itself by injecting its code to other executable files.

Read more on Check Point Threatcloud Intelligence

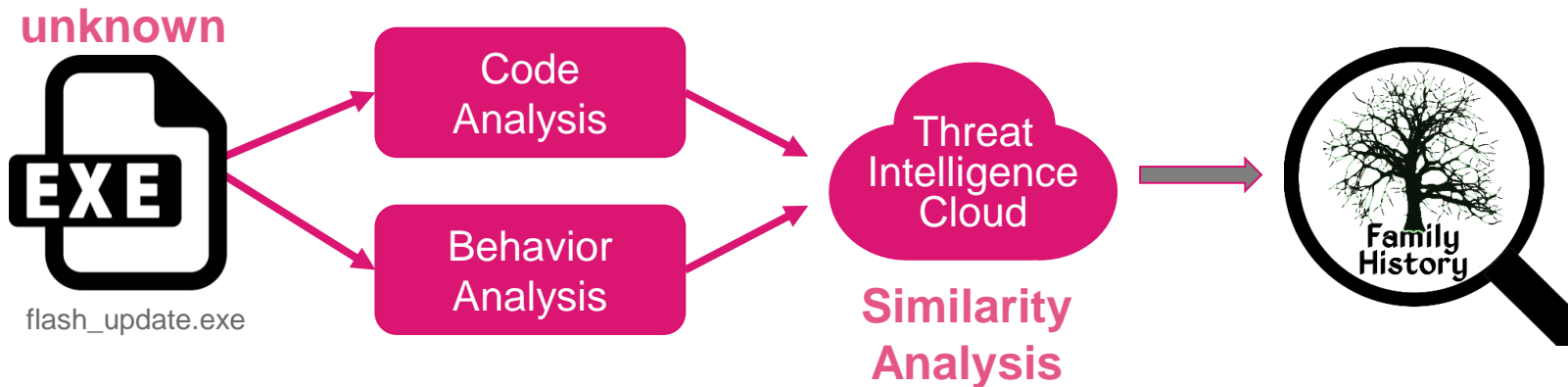
Similarity Analysis

Similar code blocks

Similar behavioral IOCs

```
Code block 1 of 3
1 push ebp
2 mov ebp, esp
3 add esp, -0x20
4 xor eax, eax
5 mov dword ptr [ebp - 0x20], eax
6 mov dword ptr [ebp - 0x18], eax
7 mov dword ptr [ebp - 0x1c], eax
```

AI Classification of Unknown Genes



flash_update

SIZE: 3.44 MB | TYPE: EXE | HASH: [redacted]

Verdict: Malicious | Action: Prevent | Confidence: High | Secure / Risk: Critical | Classification: Trojan

ATTACK VECTOR | 18/12/2018 13:35

127.0.0.1 → flash_update → 127.0.0.1

Neshta

Neshta is a trojan which was first seen in the wild on 2010. Neshta makes modifications in the system registries and in the browser settings in order to install malicious toolbars or extensions. Neshta distributes itself by injecting its code to other executable files.

Read more on Check Point Threatcloud Intelligence

Similarity Analysis

Similar code blocks

Similar behavioral IOCs

```
Code block 1 of 3
1 push ebp
2 mov ebp, esp
3 add esp, -0x20
4 xor eax, eax
5 mov dword ptr [ebp - 0x20], eax
6 mov dword ptr [ebp - 0x18], eax
7 mov dword ptr [ebp - 0x1c], eax
```

FILE LIST

NAME	TYPE	VERDICT	SIZE	CONTEXT
1002-01cb4004b1ee971a690bae2011574cfae980057a7svagent.exe	EXE	Malicious	85.98 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae980057a7juschd.exe	EXE	Malicious	287.42 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae980057a7jps.exe	EXE	Malicious	198.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae980057a7javaw.exe	EXE	Malicious	281.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae980057a7javaw.exe	EXE	Malicious	210.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae980057a7javacpl.exe	EXE	Malicious	103.98 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae980057a7java.exe	EXE	Malicious	210.48 KB	dropped
1002-01cb4004b1ee971a690bae2011574cfae980057a7javarg.exe	EXE	Malicious	267.42 KB	dropped

SUSPICIOUS ACTIVITIES

CATEGORY	COUNT	DESCRIPTION
Evasion	1	Observe a program that creates a new process
Evasion	1	The program dynamically calls imported functions
Evasion	1	The program queries a process cookie
Evasion	1	The program queries information on its own process
Evasion	1	The program queries its own PEB
Evasion	1	The program uses a native API call to load a DLL
Evasion / Persistence	1	The program executes other programs or commands
File system event	13	Suspicious file was accessed during emulation
Generic	1	Appends a known multi-family ransomware file extension to files that have been encrypted
Generic	1	Checks amount of memory in system, this can be used to detect virtual machines that have a low amount of memory available
Generic	1	Creates executable files on the filesystem

Blocking never-seen-before Phishing Attacks



AI-based analysis of 300 phishing indicators in email & web



- IP REPUTATION
- ✓ URL REPUTATION
- SUBJECT CONTEXT
- URL EMULATION
- ✓ HTML INSPECTION
- NLP
- DOMAIN REPUTATION
- ✓ LOOKALIKE FAVICON
- ✓ BRAND IMPERSONATION

+300 indicators

#1 GATEWAY WEB INSPECTION

```

<!DOCTYPE html>
<html>
  <title>Wikitechy Login Form</title>
  <head>
    <script src="/js/login-style.css" type="text/css" rel="login-style.css">
  </head>
  <body>
    <form class="form container">
      <div>Wikitechy Login Form</div>
      <label><input type="text" name="username" required>
      <input type="password" name="password" required>
      <button type="submit">Login</button>
    </form>
  </body>
</html>
    
```

#3 BROWSER INSPECTION (BY INJECTED CODE)

#2 CHECK POINT'S INJECTION

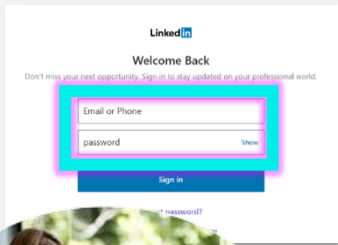
GET

RESPONSE

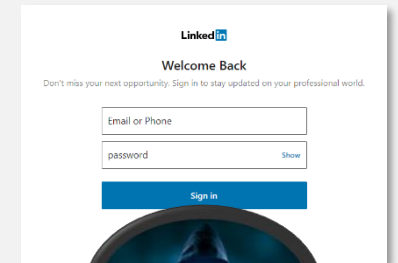


GET

RESPONSE

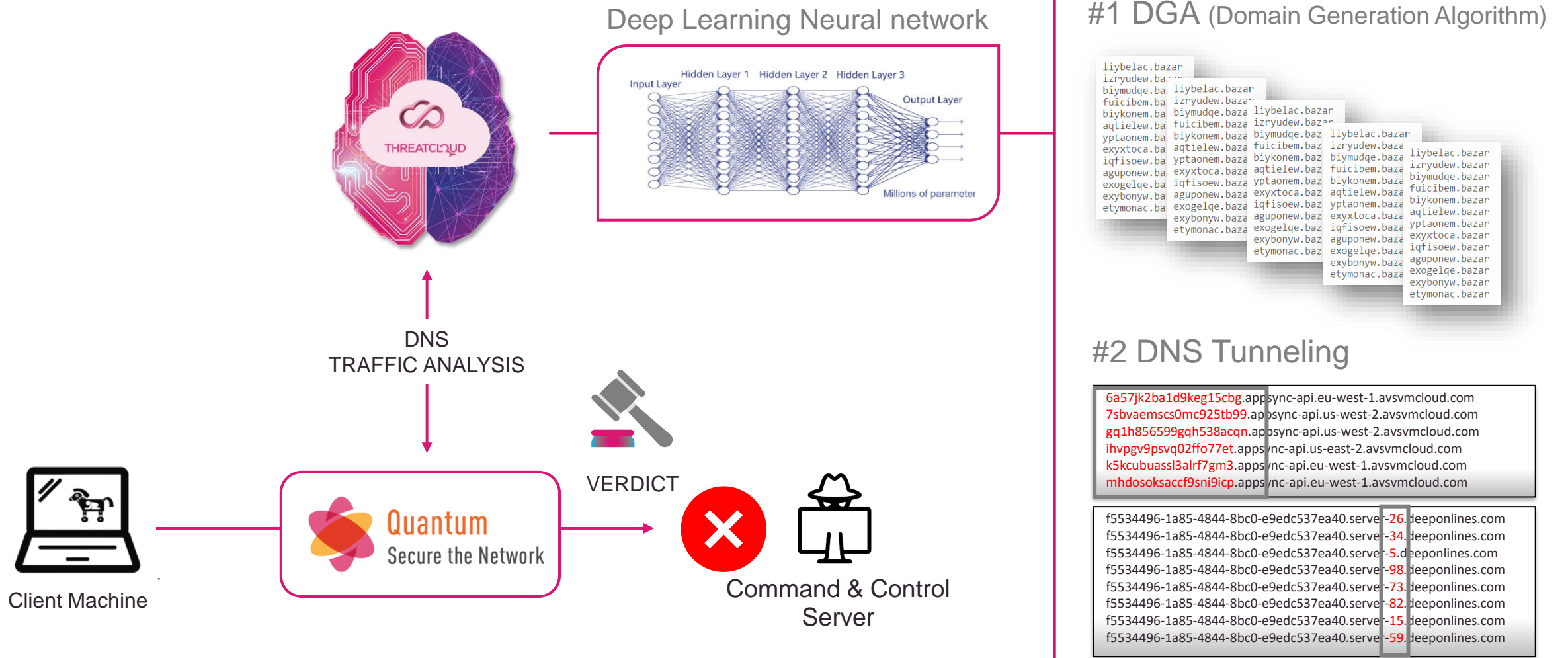


PHISHING SITE
LinkedInscam.com

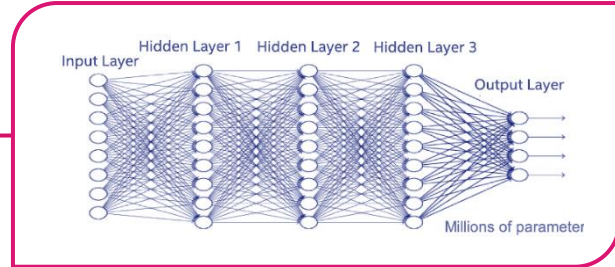


Prevents 5X more sophisticated DNS attacks

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



Deep Learning Neural network



#1 DGA (Domain Generation Algorithm)

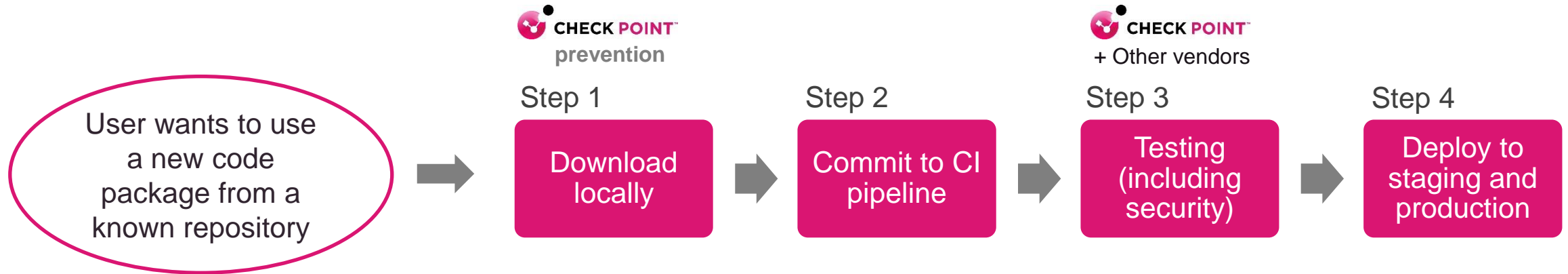


#2 DNS Tunneling

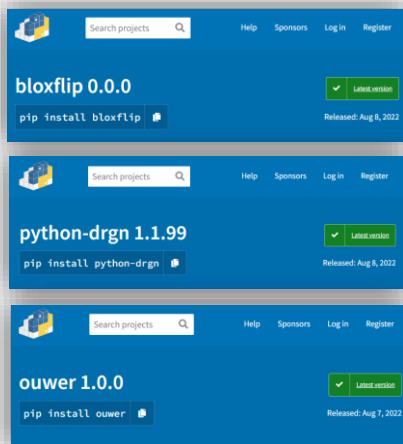


Preventing malicious Code Packages

At the earliest stage possible of the CI/CD pipeline



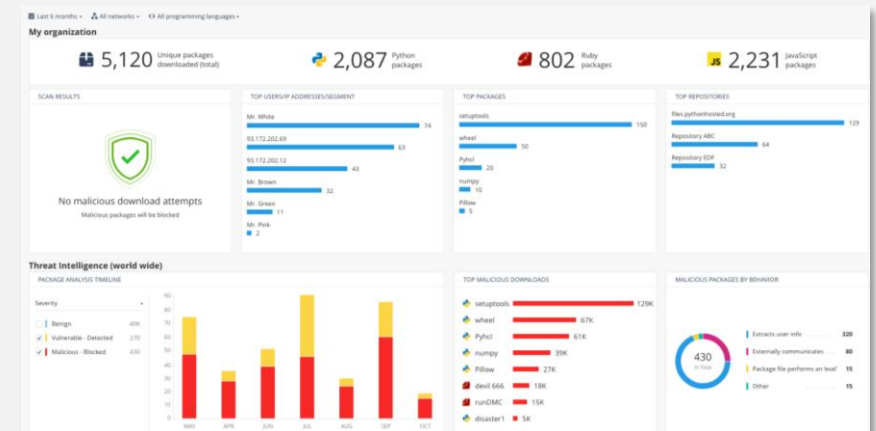
Actual preventions by Check Point:



Known vulnerable packages:



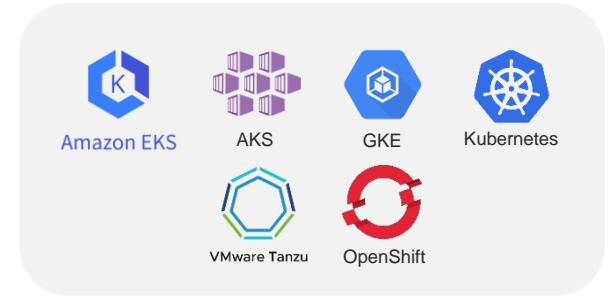
Visibility on code packages traffic:



AI TO PROTECT YOUR CLOUD DATA CENTER



Cloud workload highlights



APPSEC

- Next Gen WAF
- Powered by contextual AI
- Precise prevention
- No rules, No tuning
- Auto deploy on any environment



SERVERLESS

- Cloud Function Protection
- Runtime Self-Protection
- Least Privilege Access Control
- Secure applications & microservices to achieve zero trust



CONTAINERS

- Posture Management, Asset & Traffic visualization
- Native Web App & API Protection
- Intrusion Detection
- Image Assurance
- Admission Control
- Runtime Protection
- Micro-segmentation



Posture Management



Vulnerability Management



Admission Control



Runtime Protection



Intrusion Detection



Reports & Dashboard

GENERATIVE-AI AND CYBER SECURITY



Where Generative-AI and 'Deeper Learning' models will take us in the following years

- The deep part of **prevention** depends on the deeper aspects of AI, which progresses as well
- **Exploits** and methods are still hard to invent
- The impact of **mass fake** on different type of attacks
- Changing the way we **perform cyber jobs**
- **Automation** and remediation becomes amazingly simple
- **New attack spaces** - wars of AI bots, attacking AI models

Generative-AI – a game changer with concerns



Opens opportunity for more **Cyber Defense** innovations

- Faster to develop
- Accelerates admin work
- More effective SOC team




Raises concerns about increased **Cyber Offense** activities

- Develop variations of attacks
- Flood fake identities and content
- Test attacks to increase impact



DD Will generative-AI accelerate cyber offense?

 Yes, it is possible that generative-AI could be used to accelerate and automate various forms of cyber offenses, such as phishing attacks, malware generation, and misinformation campaigns. However, it is also possible that advancements in AI and machine learning could be used to enhance cybersecurity defenses and mitigate the potential impact of such attacks. The relationship between generative-AI and cybercrime is complex and dynamic, and will likely continue to evolve as technology advances.

The future is ahead of us,
more will change

LEVERAGING AI TO ACCELERATE SOC AND AUTOMATION

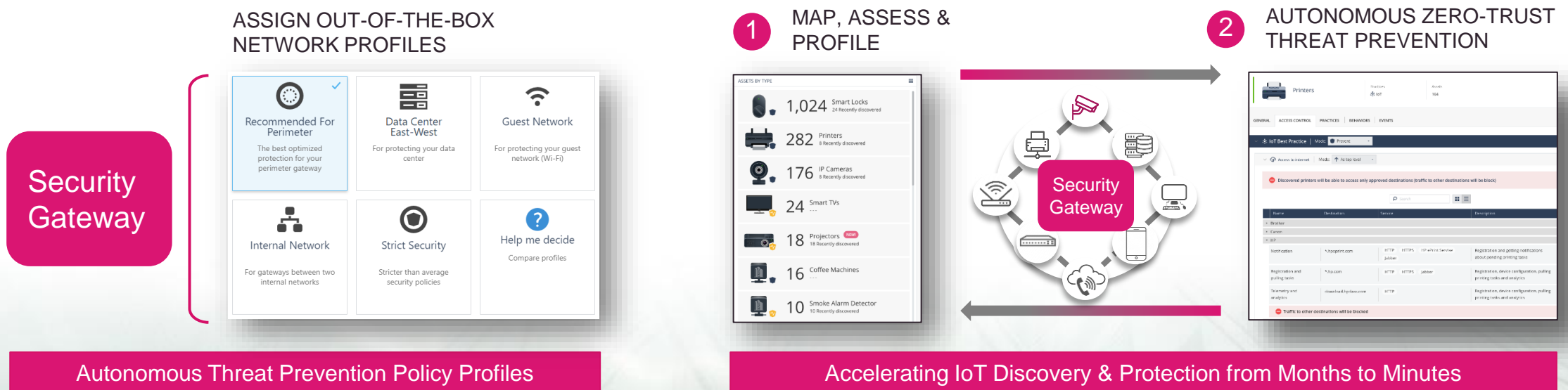


Autonomous Threat and Zero-Trust profiles

For Networks and IoT Devices



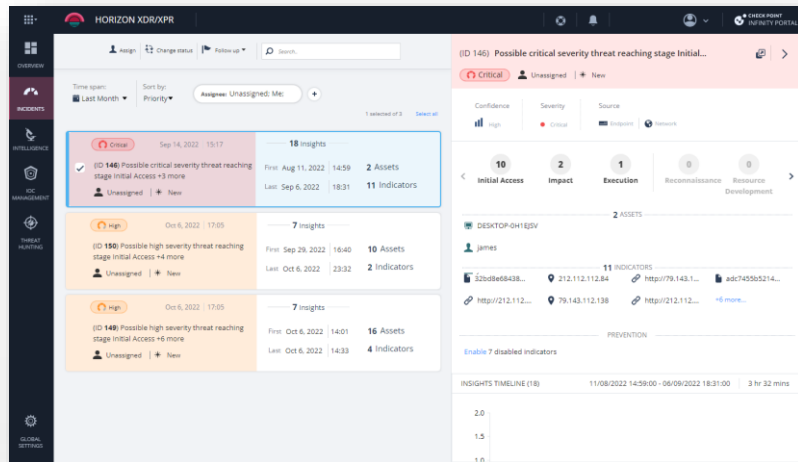
- Machine learning powered unified security management with 100% breach prevention
- Manage unified security policy from a single console
- Leverages global ThreatCloud intelligence
- Automatically updates security posture to protect against the latest threats



Preemptive security against the next attack

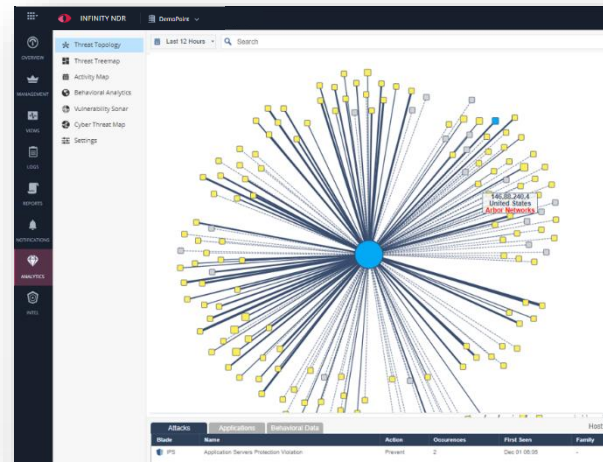
AI for Events Correlation, Threat Hunting, Visualization and Automatic Responses

Correlation of Events



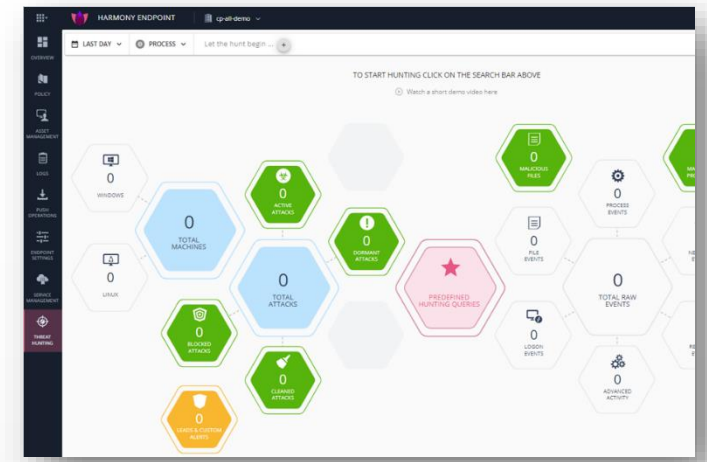
AI/ML SOC analyst delivering automated threat prioritization. Investigation on Check Point's ThreatCloud big data intelligence repository

Attack Visualization



Unique Behavioral Analytics and threat visualization across cloud and on-prem networks

Advanced Threat Hunting



Unique hunting experience of endpoint activities for incident investigation and response

Challenges in adopting AI for prevention





- AI is as good as your data
- Balance between data collection and privacy
- Skill shortage
- Easy to claim, hard to prove
- Contextual understanding of what is 'good' and what is 'bad'
(values based)
- AI interoperability Complexities



AI-driven Threat Prevention stops all cyber attacks



Entry points:

-  **Social engineering**
-  **Supply chain**
-  **SW and Protocols Vulnerabilities**
-  **Cloud misconfigurations**

Gaining persistence:

- **Zero-trust** access & strong policies
- **AI-based prevention** for malware, docs, phishing
- Blocking **C&C** communication
- **Cloud posture** management & workload protection
- **Server hardening**
- **Shift-left** source code & developers
- **Native XDR** – network, endpoints, servers, cloud, mobile, email, AD, more

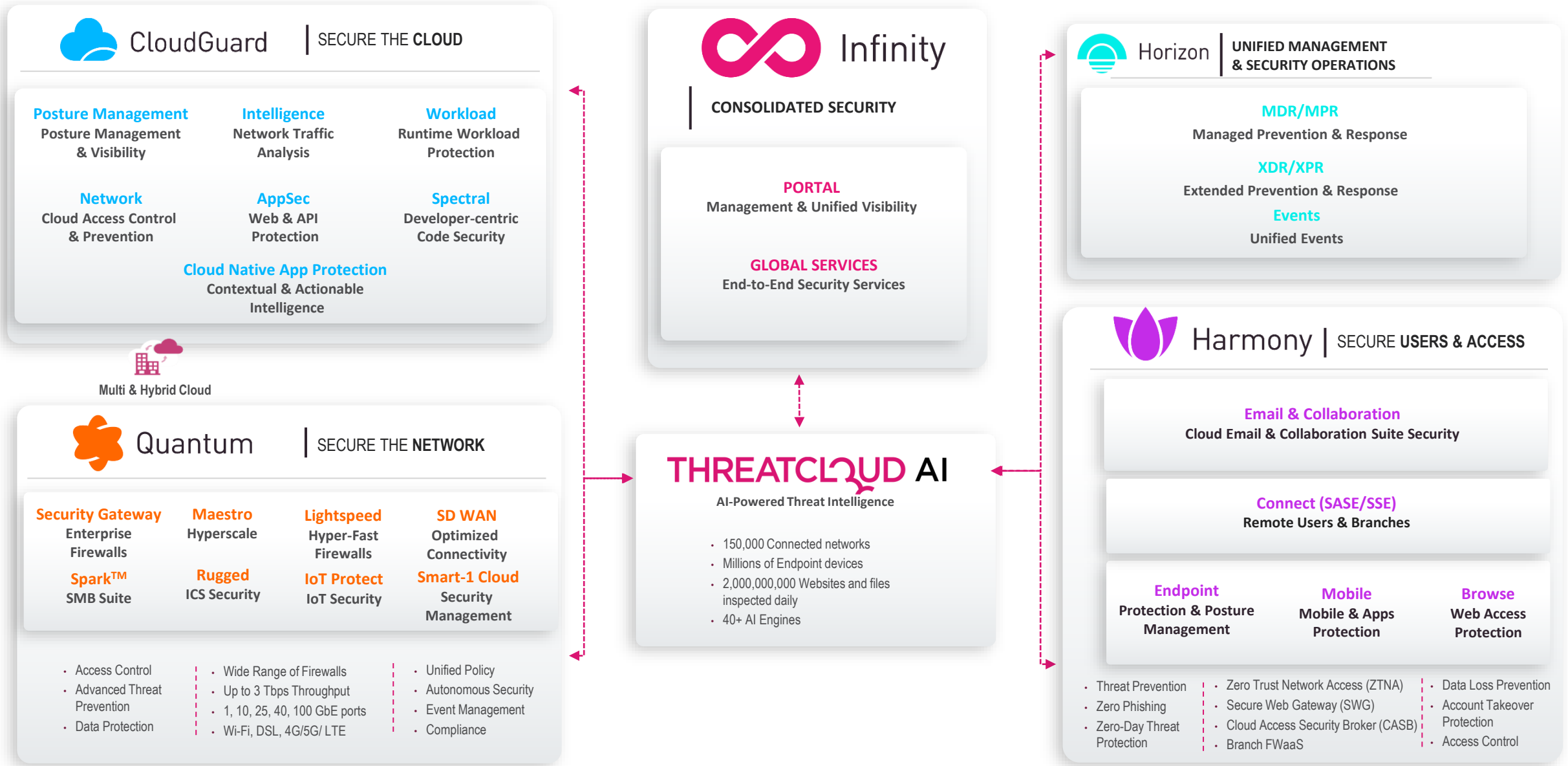
Lateral movement:

- **Cloud posture** management
- **Zero-trust** and **micro-segmentation**
- **AI-based prevention** on endpoints & servers
- **Analysis of AD / ADFS / Access token** (SAML, OAuth 2.0) & user behaviors
- **Native XDR**

Data leak:

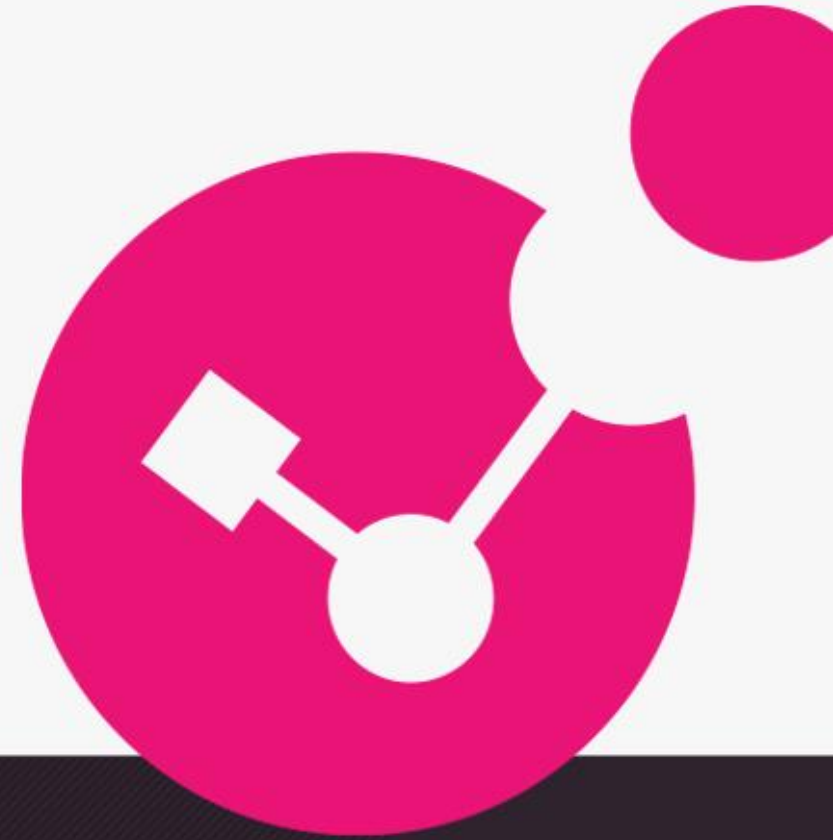
- **Cloud posture** management
- **AI-based prevention** on endpoints & servers
- **Gateway IPS / Anti-BOT** protections
- **Native XDR**
- **DLP**
- **NDR**

ONE AI SECURITY PLATFORM - COMPREHENSIVE SECURITY





Thank you!



YOU DESERVE THE BEST SECURITY