

# RSA® Conference 2022

San Francisco & Digital | June 6 – 9

SESSION ID: PART2-R02

## Leveraging AI & Deep Learning in the Battle against Zero Day Cyber Attacks

**Itai Greenberg**

Chief Strategy Officer

Check Point Software Technologies Ltd.

itaigr@checkpoint.com

# TRANSFORM



# Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

©2022 RSA Conference LLC or its affiliates. The RSA Conference logo and other trademarks are proprietary. All rights reserved.

# Today's Threat Landscape Is Exceptionally Dangerous

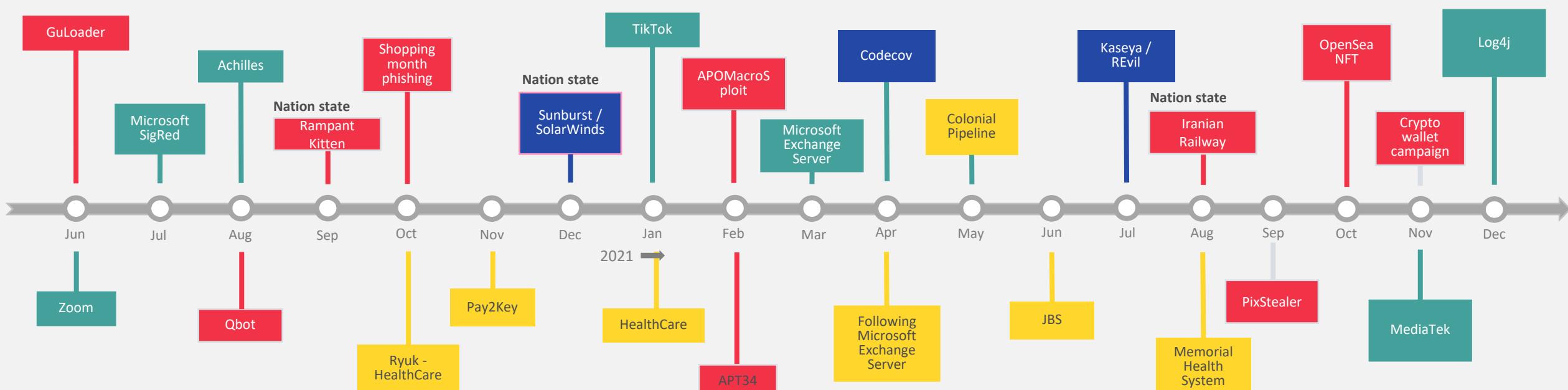


**Every month**

10's of millions of attacks  
400K zero days\*



- APT
- Supply chain
- Ransomware
- SW vulnerabilities



\*According to ThreatCloud

# Supply Chain Is The Modern Entry Point for Attacks

Supply Chain Attacks Keep Coming: The Latest is Log4J in Dec 2021



Jan 2021 – Apr 2021

Affected 29,000 customers



Mar 2020 – Dec 2020

Affected 18,000 customers



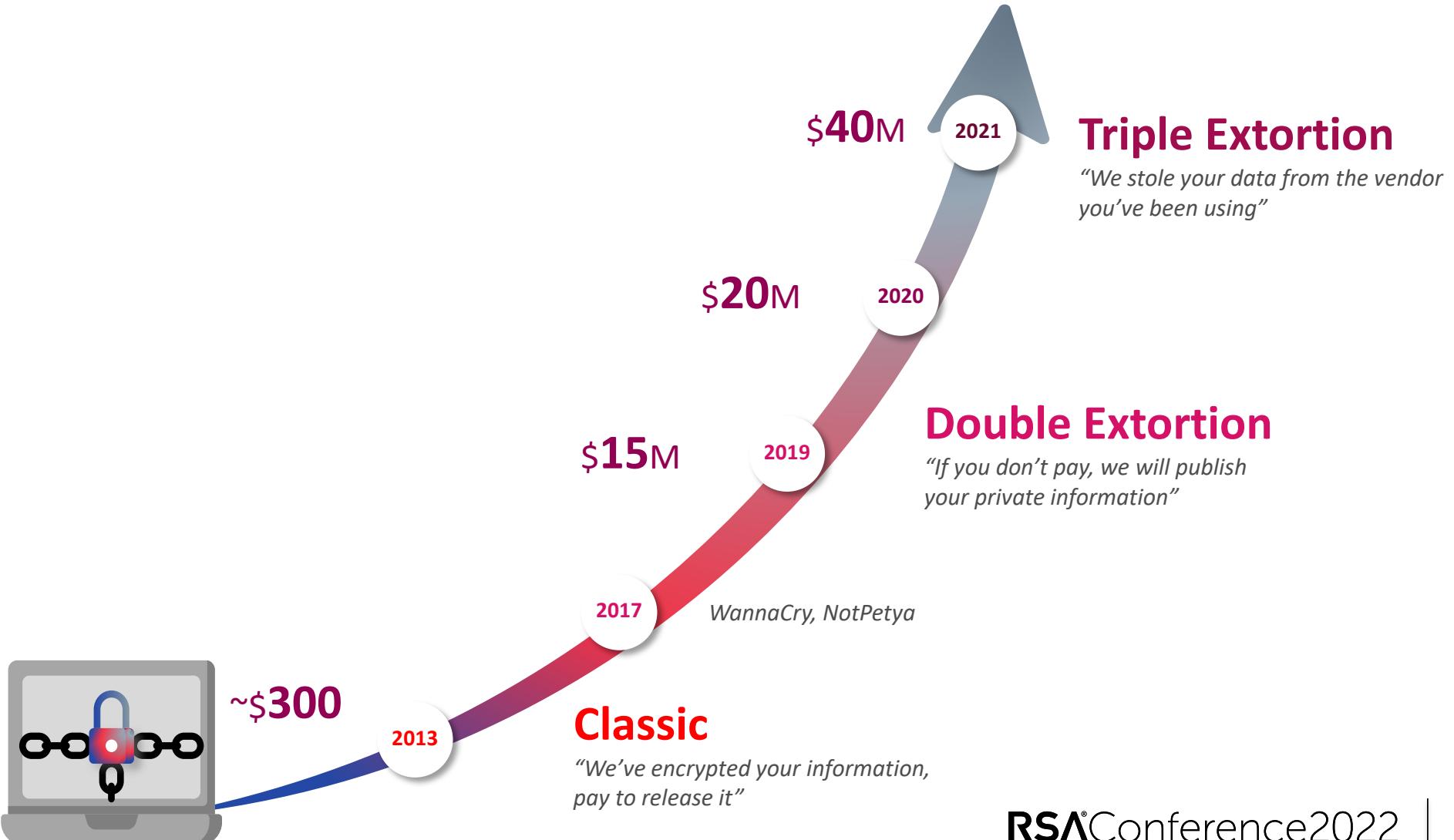
Dec 2021-..

Attempted exploit on **over 36.8% of corporate networks globally**

Check Point AI-driven security  
**prevented over 820,000 attempts**  
to exploit the Log4J vulnerability

# Ransomware Becoming More Evasive

Supply Chain + Ransomware is the latest Network Attack Strategy



# Enterprise Security Top Challenges



**Too many security alerts**

**Too many point products**

**Too slow to adopt new protections**

**RSA®**Conference2022

## OUR PHILOSOPHY





IN THE WORLD OF CYBER DETECTION IS NOT ENOUGH!

WE SHOULD ALL FOCUS ON PREVENTION  
POWERED BY AI & AUTOMATION

# ONLY AI-BASED SECURITY CAN KEEP SAFE



## Prevention first

Block attacks faster than anyone else



## Best Catch rate

Of known & unknown threats

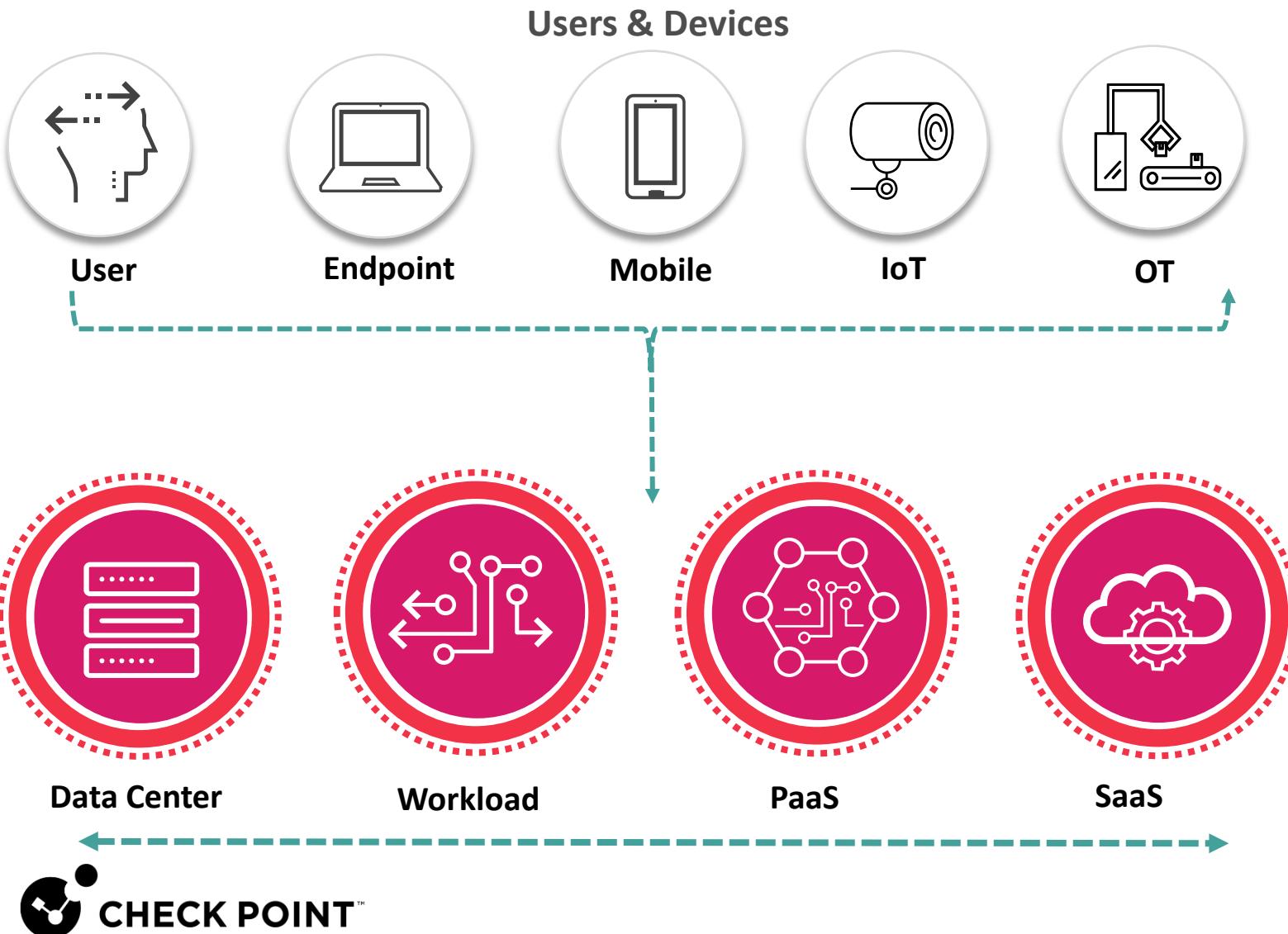


## Near Zero false positives

Uninterrupted user productivity  
Less alerts/tickets for sec admins



# YOU MUST AUTOMATE YOUR ZERO-TRUST POLICY



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

# USING AI & AUTOMATION EVERYWHERE

## QUANTUM

Secure the network



## CLOUDGUARD

Secure the cloud



## HARMONY

Secure users & access



THREATCLOUD

# AI Is All About Your Data

86B Overall Queries from any Check Point Enforcement Point

**2,000,000**  
Malicious indicators

**13,000,000**  
File emulations

**900,000**  
Newly installed  
mobile apps



**2,000,000,000**  
Websites and  
files inspected

**500,000**  
Online web forms

**20,000,000**  
Potential  
IoT devices

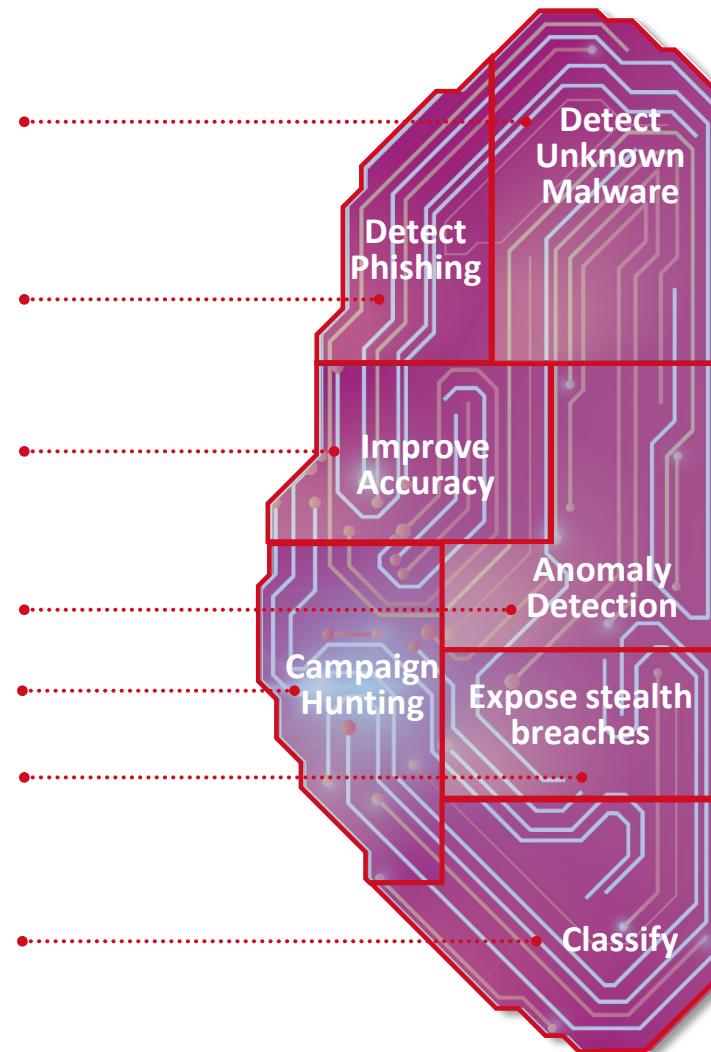
**800,000**  
Full content emails



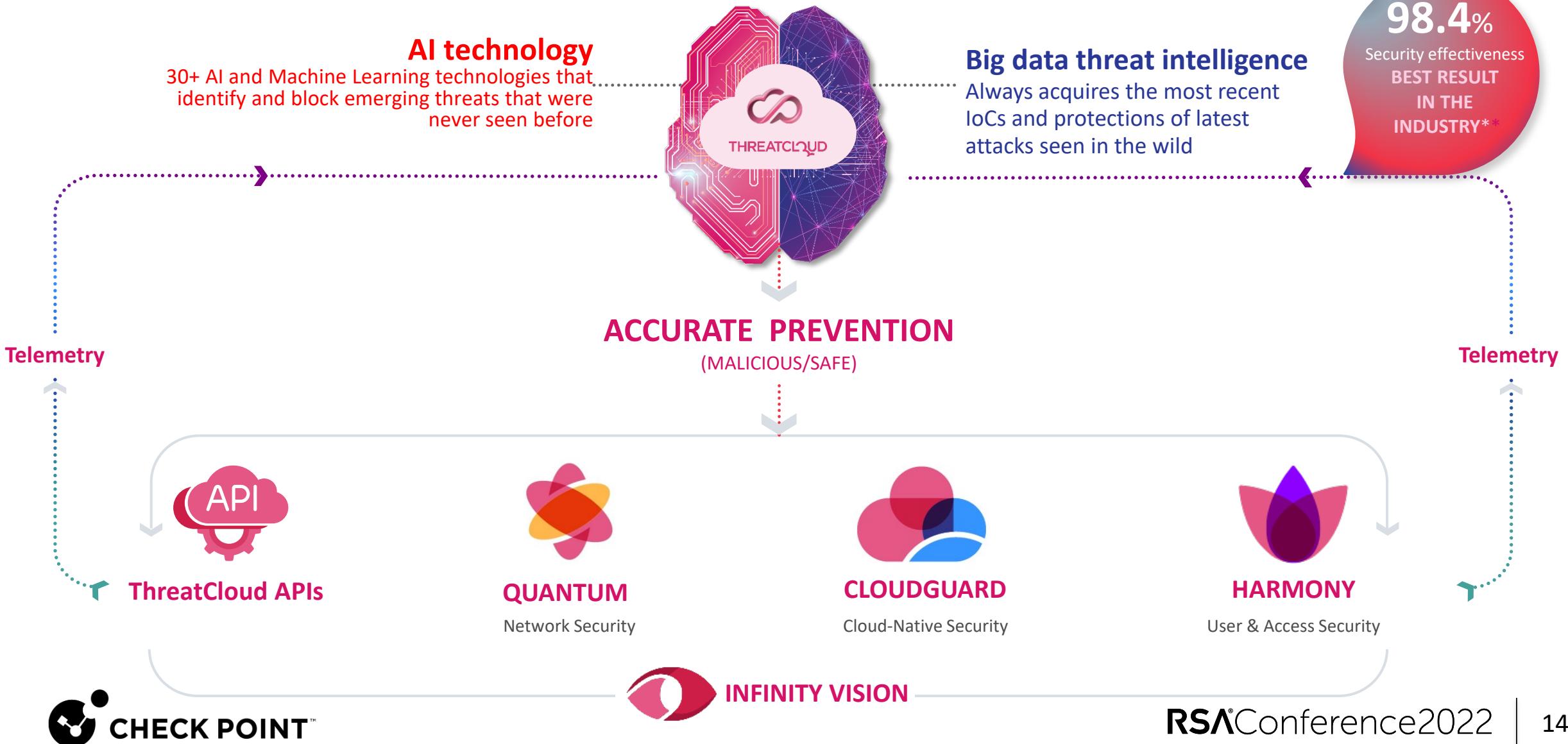
# AI Technologies Leveraged by ThreatCloud

## 30+ AI Engines For Different Security Functionality

- Infected hosts detection
- Sandbox static analysis
- Sandbox dynamic analysis
- Email static analysis
- Mobile zero-phishing detection
- Anti-Phishing AI engine
- Network AI engines aggregator
- Mobile AI engines aggregator
- Machine validated signature
- Cloud networks anomaly detection
- ThreatCloud Campaign Hunting
- Analyst Mind
- Malicious activity detection
- Documents meta classifier
- Vectorization family classifier
- ML Similarity Model
- MRAT Classifier



# ThreatCloud: AI Brain Behind Check Point Security



**RSA®**Conference2022

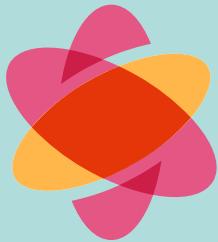
# USING AI & AUTOMATION TO PROTECT YOUR NETWORK



# USING AI & AUTOMATION EVERYWHERE

## QUANTUM

Secure the network



## CLOUDGUARD

Secure the cloud



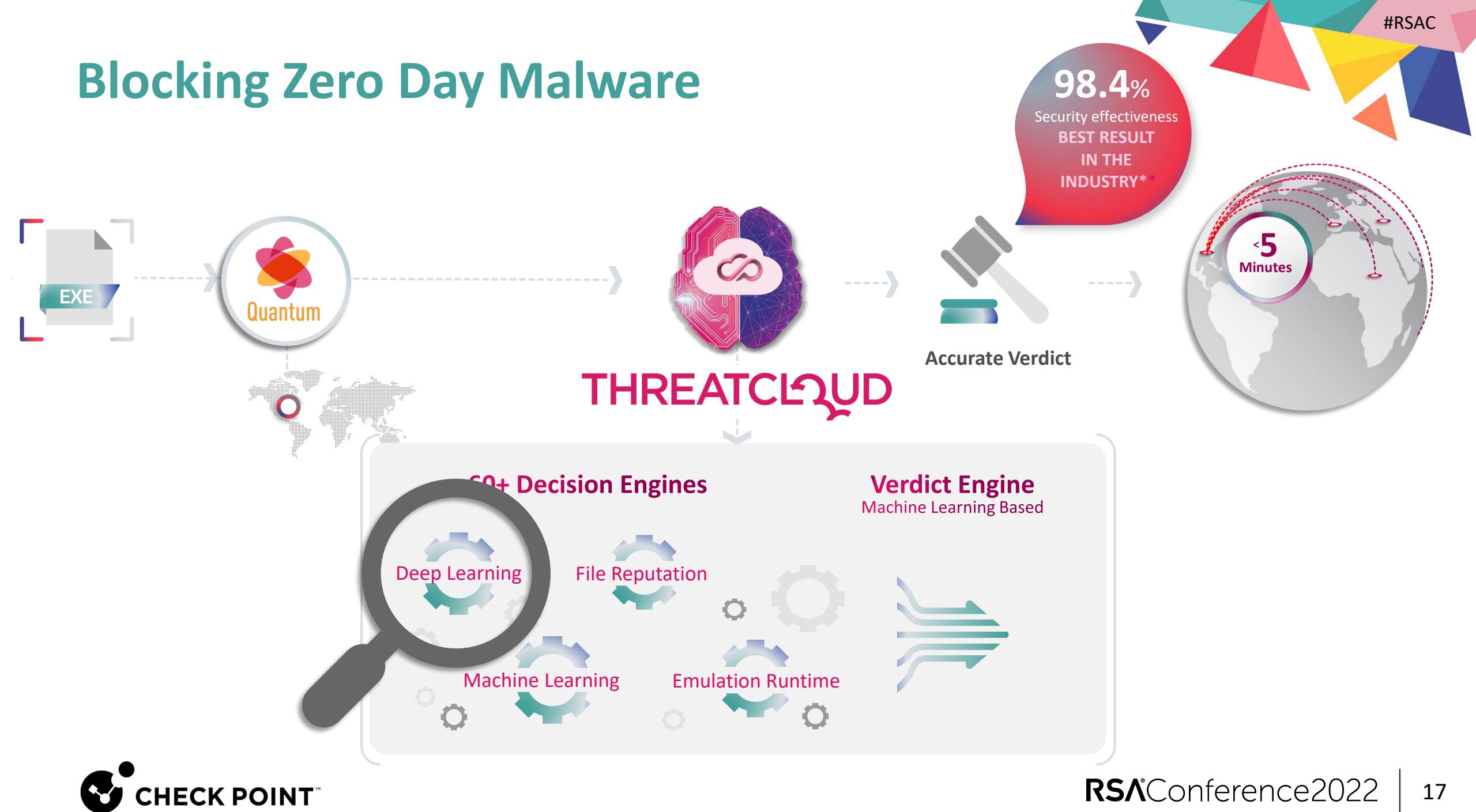
## HARMONY

Secure users & access



THREATCLOUD

# 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 injections its code to other executable files.

Read more on Check Point Threatcloud Intelligence

Similarity Analysis

Similar code blocks

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
```

Pioneer

Threat Details Report | Actions

flash\_update | EXE | SIZE: 3.44 MB | TYPE: EXE | HASH: 18/12/2018 13:35

Verdict: Malicious | Action: (selected in profile) Prevent | Confidence: High | Secure / Risk: Critical | Classification: Trojan

ATTACK VECTOR | 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 injections its code to other executable files.

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
```

Read more on Check Point Threatcloud Intelligence

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
```

Phantom

3576 2682 1788 894 0

19/12/11 21/11 25/11 29/11 03/12 07/12 11/12 15/12

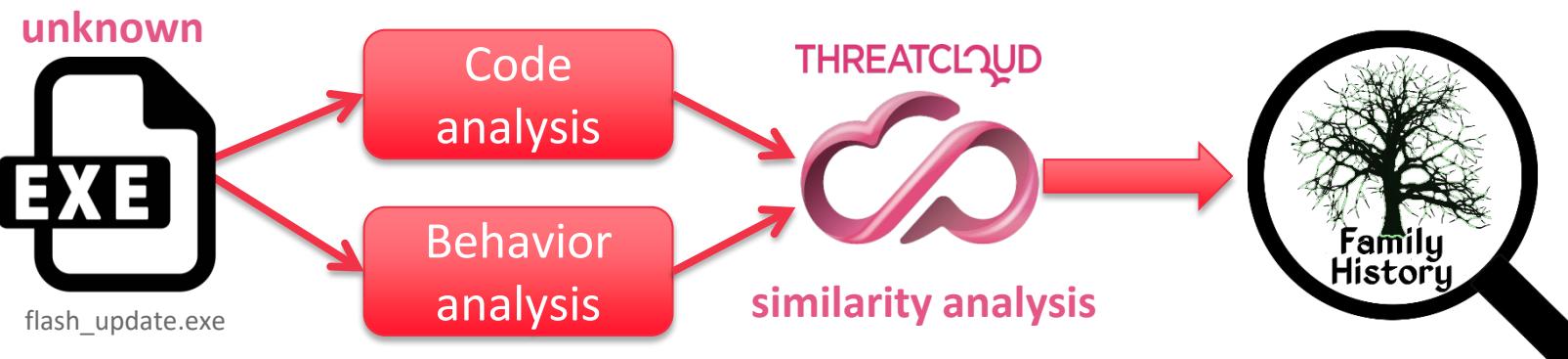
FILE LIST

NAME	TYPE	VERDICT	SIZE	CONTEXT
1002-01cb4004b1ee971a690bae2811574cfew98d057a/issagent.exe	EXE	Malicious	85.98 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfew98d057a/issched.exe	EXE	Malicious	237.42 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfew98d057a/jqs.exe	EXE	Malicious	198.49 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfew98d057a/jnews.exe	EXE	Malicious	281.48 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfew98d057a/javexec.exe	EXE	Malicious	210.48 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfew98d057a/java.exe	EXE	Malicious	103.98 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfew98d057a/jaureg.exe	EXE	Malicious	210.48 KB	dropped
1002-01cb4004b1ee971a690bae2811574cfew98d057a/jaureg.exe	EXE	Malicious	267.42 KB	dropped

SUSPICIOUS ACTIVITIES

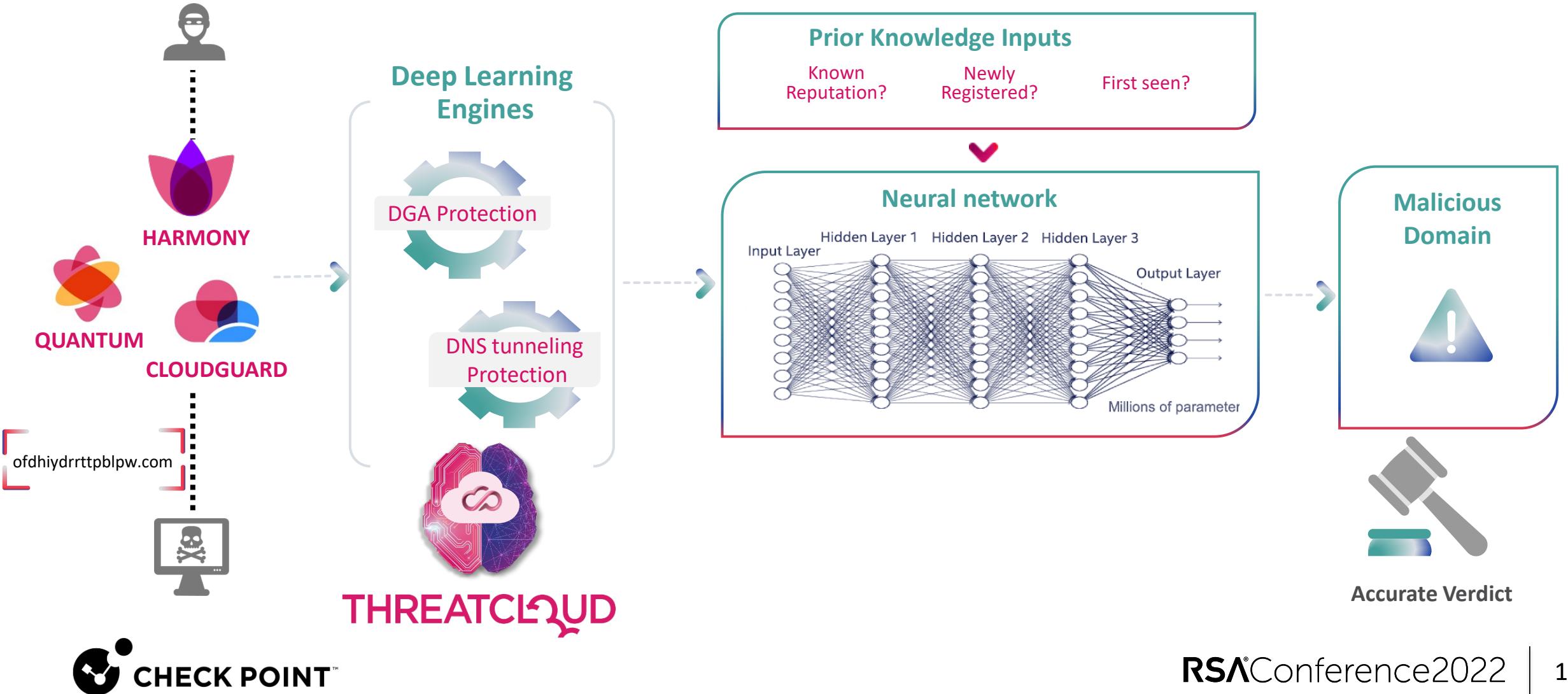
CATEGORY	COUNT	DESCRIPTION
Evasion	1	Observe a program that creates a new process
Evasion	1	The program dynamically calls imported functions
Evasion	1	The program queries a process cookie
Evasion	1	The program queries information on its own process
Evasion	1	The program queries its own PE2B
Evasion / Persistence	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

AI classification of unknown genes



# Protect Against DNS Tunneling and DGA Attacks

## Using Advanced Machine Learning Engines to Detect Zero-Days



# ThreatCloud Uses AI to Catch What Others Miss



3 Examples of malware variants detected by ThreatCloud before VirusTotal

TRICKBOT

12 days  
before VirusTotal

ZLOADER

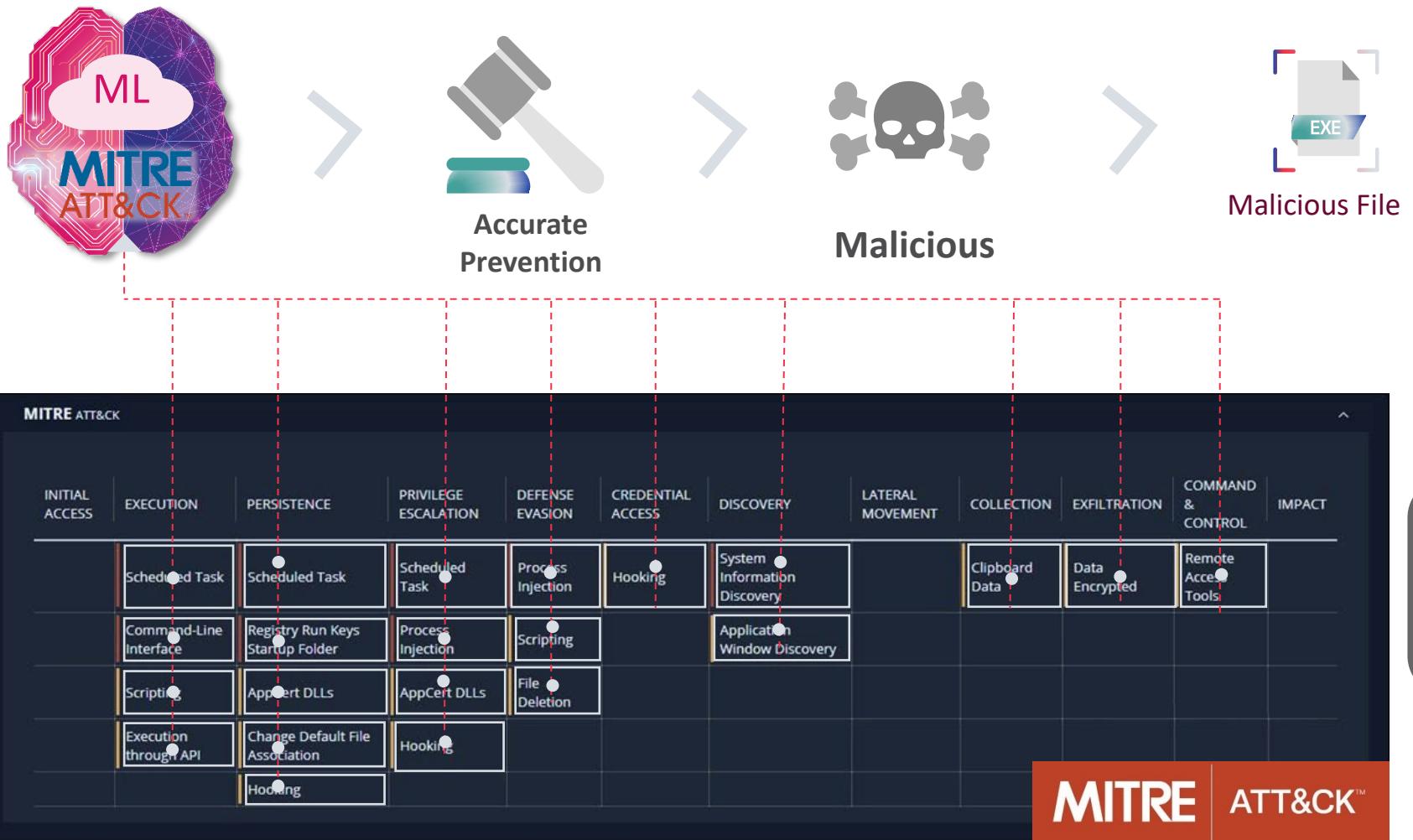
15 days  
before VirusTotal

HANCITOR

17 days  
before VirusTotal

THREATCLOUD

# Accurate Prevention Using AI & MITRE Framework



# Automate 90% of Changes with Sub-second Adaptive Policy

Learn pattern



▼ 13	Policy for access to Data Center servers	* Any	Data Center LAN	* Any	* Any	* Any	Data Center Layer
13.1	Datacenter Remote Access	Finance User	ERP Server	RemoteAccess	SAP	* Any	Accept
13.2	Datacenter Segmentation	Web Frontend	DB Backend	* Any	MS-SQL	* Any	Accept



# Autonomous Zero Trust Access Control Policies

- Policy is based on AI and behavioral analysis learning
- Automatically detect and protect new assets

The screenshot shows a user interface for the Check Point Infinity Portal. At the top, there's a navigation bar with icons for search, refresh, and notifications, followed by the user name "John Snow" and the portal logo. Below the navigation bar is a section titled "ASSETS BY TYPE" which lists various asset types with their counts and recent discovery details.

Asset Type	Count	Details
Smart Locks	1,024	24 Recently discovered
Printers	282	8 Recently discovered
IP Cameras	176	8 Recently discovered
Smart TVs	24	...
Projectors	18	NEW! 18 Recently discovered
Coffee Machines	16	...
Smoke Alarm Detector	10	10 Recently discovered

RSA® Conference 2022

# USING AI & AUTOMATION TO PROTECT YOUR CLOUD



# USING AI & AUTOMATION EVERYWHERE

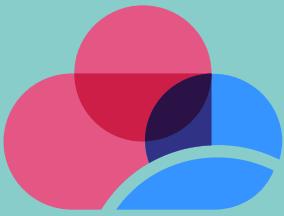
## QUANTUM

Secure the network



## CLOUDGUARD

Secure the cloud



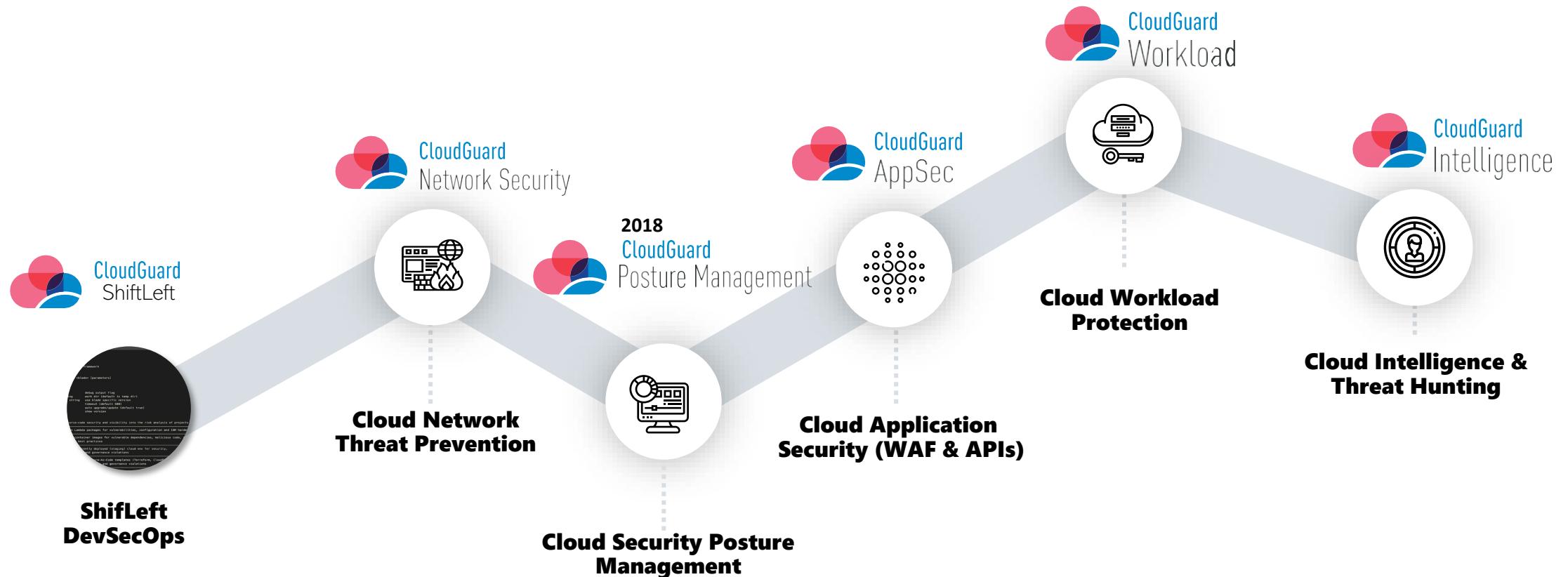
## HARMONY

Secure users & access

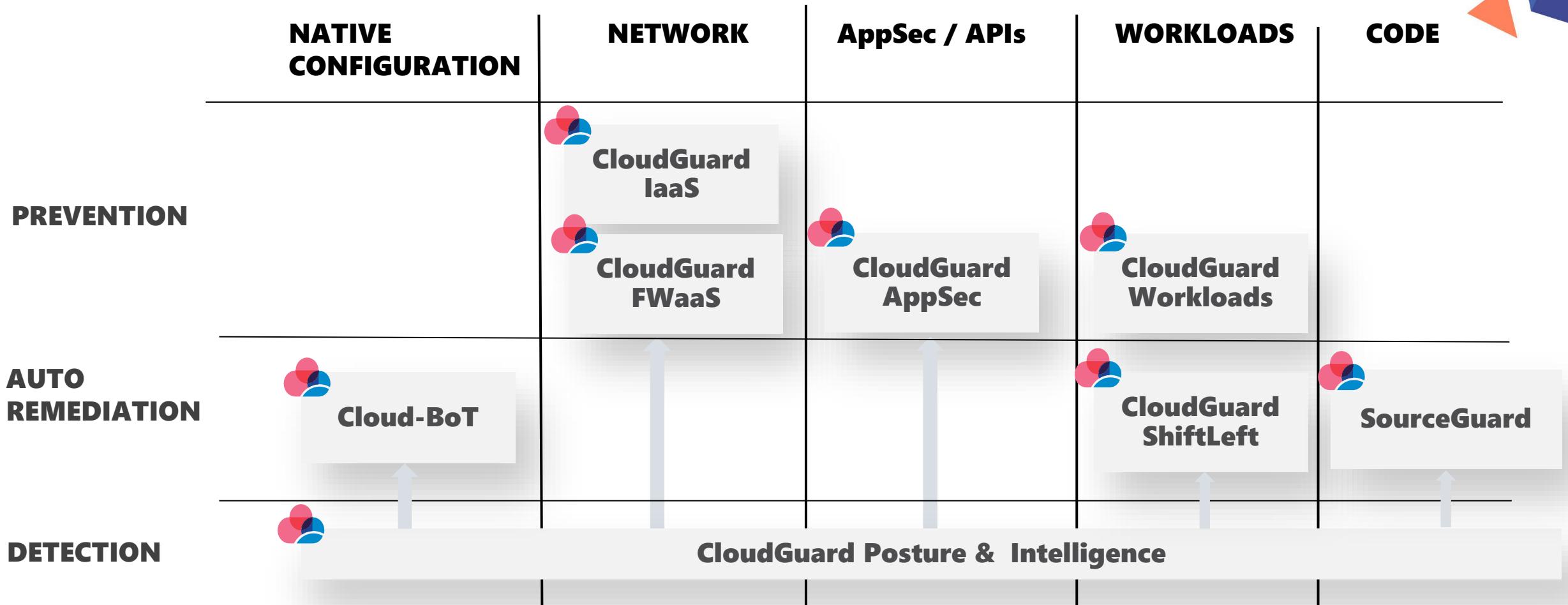


## THREATCLOUD

# CloudGuard - Unified Cloud Native Protection Platform



# CloudGuard

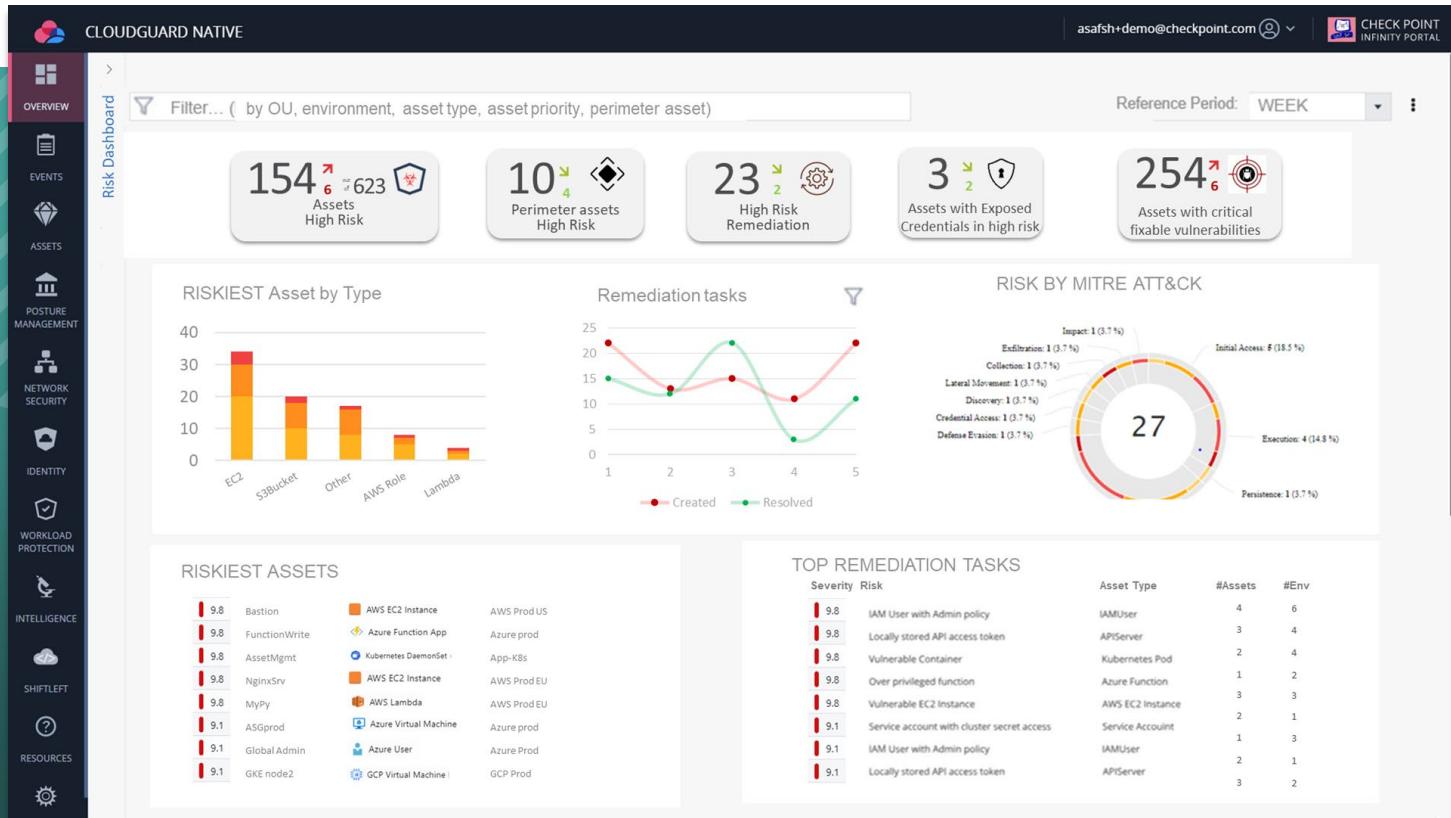


**YOU NEED TO PREVENT CYBER ATTACKS ALSO IN THE CLOUD**

# Expanding Cloud Native Application Protection



AUTOMATED  
EFFECTIVE RISK  
MANAGEMENT



# Cloud Workload Security Highlights



## APIs

- NextGen WAF
- API Security
- Bot Protection
- Application IPS
- Developer friendly experience
- More platforms - Envoy, Azure web apps
- Exciting features – Geo Blocking, Rate Limiting, Anti-Scraping



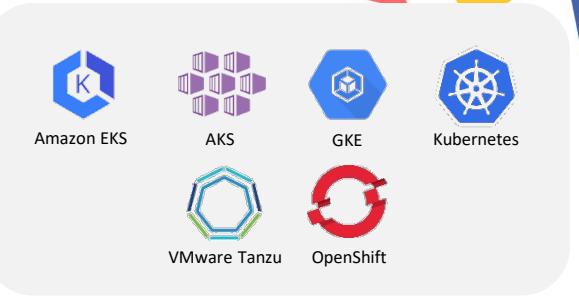
## SERVERLESS

- AWS Function Protection
- Runtime Self-Protection
- Least Privilege Access Control
- Azure FunctionApp Protection



## CONTAINERS

- Posture Management, Asset & Traffic visualization
- Native Web App & API Protection
- Intrusion Detection
- Image Assurance
- Admission Control
- Runtime Protection
- Micro-segmentation
- OpenShift and Tanzu Support
- Fargate ECS
- Registry scanning



DEV

CI/CD

Deployment

Runtime



Posture  
Management



Vulnerability  
Management



Admission  
Control



Runtime  
Protection



Intrusion  
Detection



Reports &  
Dashboard

# The only pre-emptive security against **LOG4J**



## APPLICATION SELF-PROTECTION

### Vendor and Product

**Pre-emptive protection  
before vulnerability published**

**Check Point  
CloudGuard AppSec**



AWS WAF



Azure WAF



Cloudflare WAF



Imperva WAF



F5 NGINX App Protect



F5 BIG-IP ASM/Advanced WAF



Akamai WAF



Fortinet Fortiweb

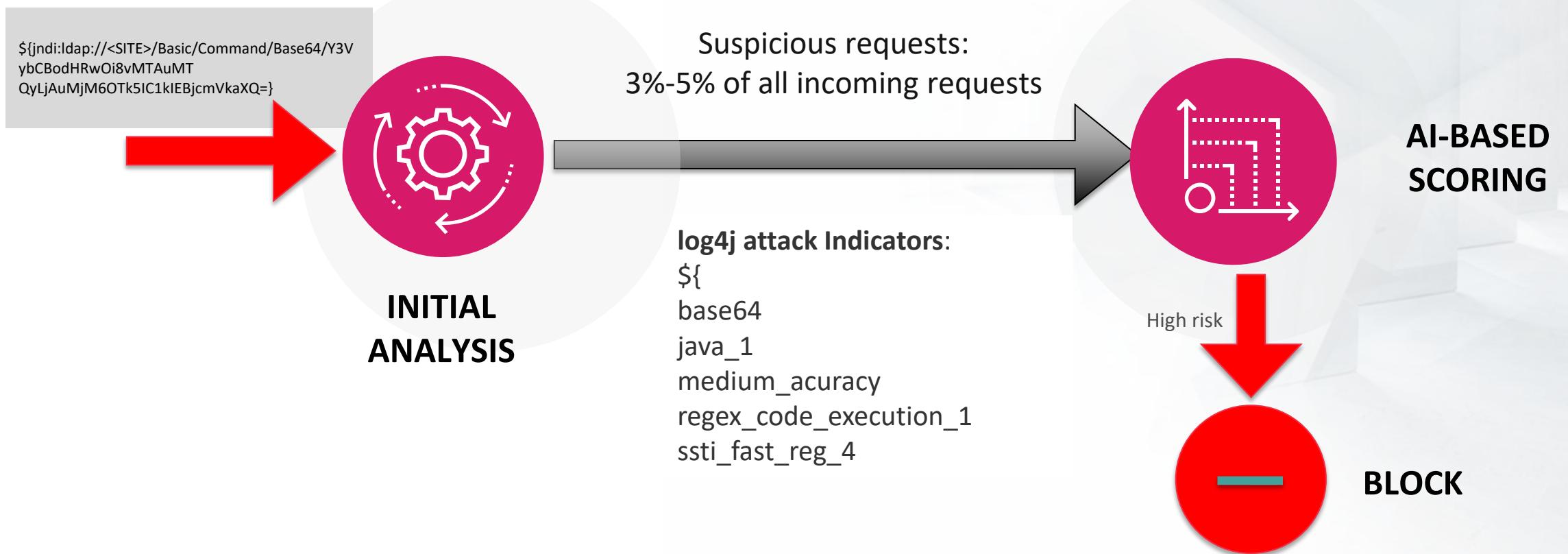


ModSecurity



# How AppSec Uniquely Preempts Log4j Attacks

- 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



**RSA®**Conference2022

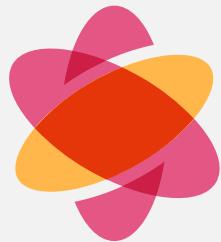
# USING AI & AUTOMATION TO PROTECT YOUR USERS



# USING AI & AUTOMATION EVERYWHERE

## QUANTUM

Secure the network



## CLOUDGUARD

Secure the cloud



## HARMONY

Secure users & access



THREATCLOUD

# Blocking Unknown Phishing Attacks

## Email and Websites

**Microsoft Outlook inbox:**

Ms. Cheng Margert has a order...  
LinkedIn <docs@skynet.net>  
Ms. Cheng Margert has a order request with your company  
To: Recipients

in

Ms. Cheng Margert sent you a order request on LinkedIn, and would like to do business with your company. kindly view or accept order request.

Ms. Cheng Margert  
DOUBLE PILOTS GROUP  
HOLDING CO.LIMITED.

Accept Order  
View Order

Unsubscribe | Help  
You are receiving invitation emails.  
This email was intended for You (MBK KOREA - VP). Learn why we included this.  
LinkedIn Mailing address: Room 817, 18F, Building 18, #1 DiSheng Bei Road, Beijing Yizhuang Development Area, China. LinkedIn and the LinkedIn logo are registered trademarks of LinkedIn.

**LinkedIn Login Page:**

Welcome Back  
Don't miss your next opportunity. Sign in to stay updated on your professional world.

Email or Phone  
password Show

Sign in  
Forgot password?  
New to LinkedIn? Join now

LinkedIn © 2020 User Agreement Privacy Policy Community Guidelines Cookie Policy Copyright Policy Send Feedback

**Search Threat Prevention Results:**

Search Threat Prevention

Samuelb

Samuelb 5:48 PM Monday, May 24th https://storage.googleapis.com/v0/b/dgfhfjfkrlr.appspot.com/o/hdgfjfkf/index.html?alt=media&token=f22c5ef2-7b46-46e3-a7ea-44daff21d1bf (edited)

LinkedIn Log In or Sign Up  
750 million+ members | Manage your professional identity. Build and engage with your professional network. Access knowledge, insights and opportunities.



- IP REPUTATION
  - ✓ URL REPUTATION
  - SUBJECT CONTEXT
  - URL EMULATION
  - ✓ HTML INSPECTION
  - NATURAL LANGUAGE PROCESSING
  - DOMAIN REPUTATION
  - ✓ LOOKALIKE FAVICON
  - ✓ BRAND IMPersonation
- +300 indicators

# RSA® Conference 2022

## SUMMARY



# AI-Driven Threat Prevention Stops Cyber Attacks



Entry points:



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

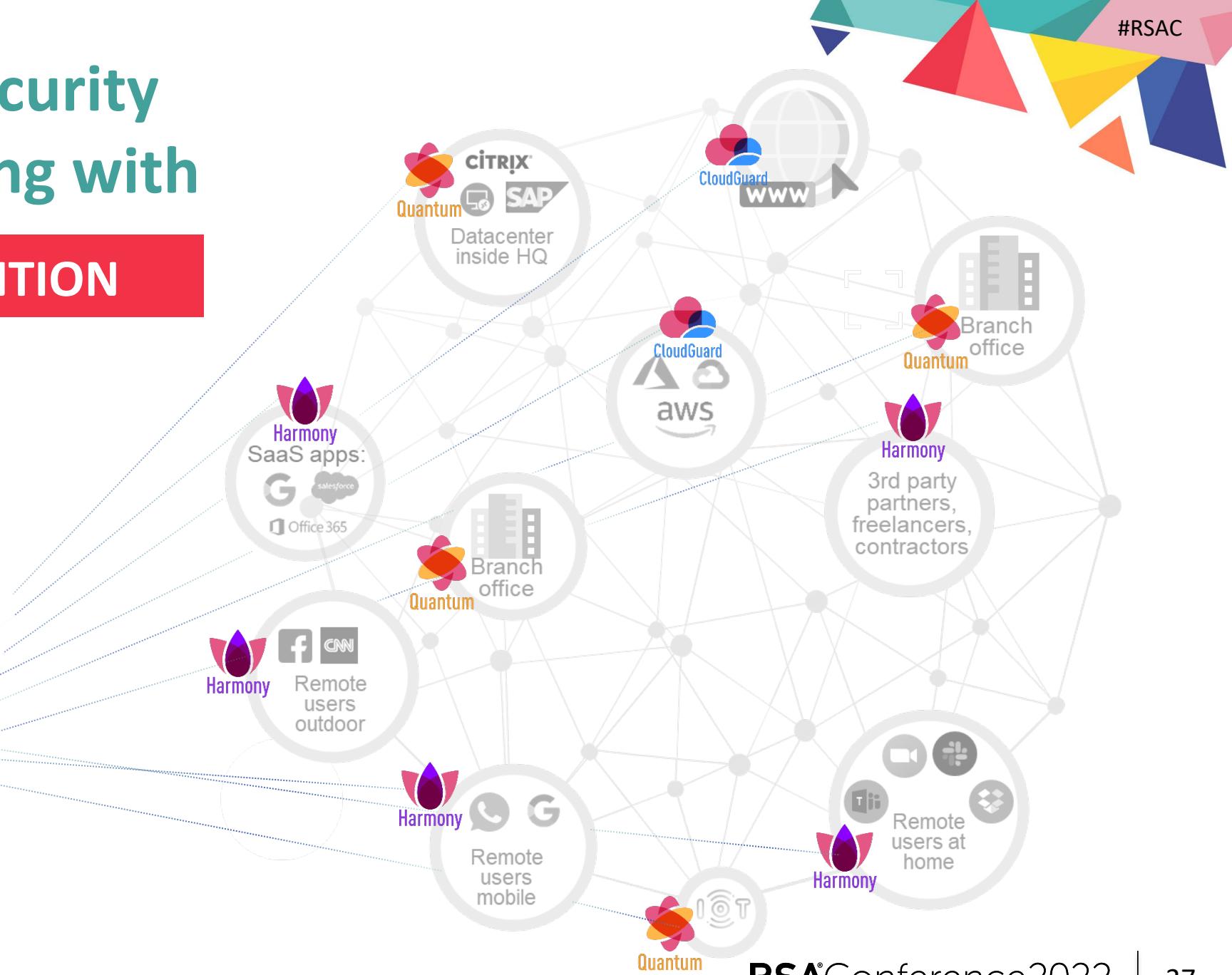
Data leak:

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

# Check Point AI Security Protects Everything with

## ACCURATE PREVENTION

Powered By Threatcloud



# Organizations Choose Check Point for Best Security



# RSA® Conference 2022

THANK YOU

