CHECK POINT™

XDR/XPR & Playblocks and more..

Tomas Vobruba | Lead SE Slovakia

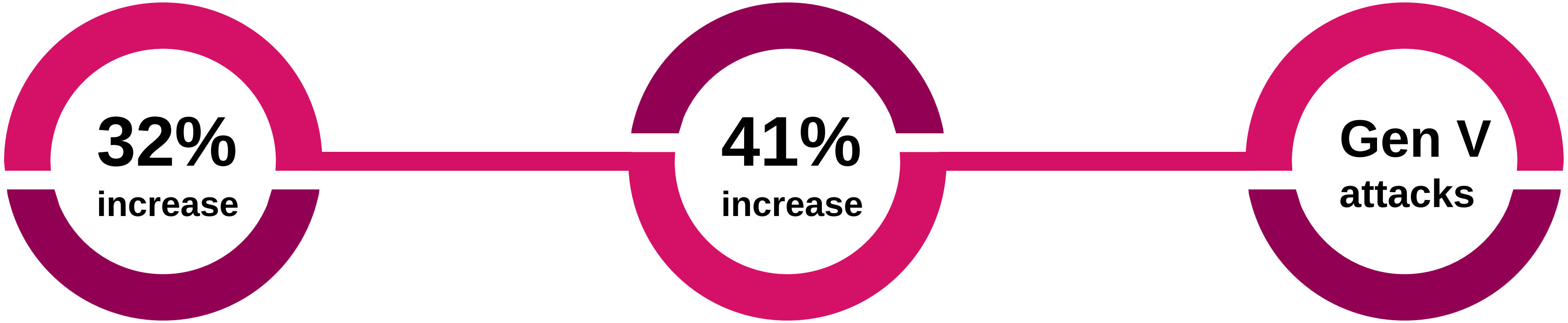
UNINFOS 2024 Kosice

YOU DESERVE THE BEST SECURITY

SOC

TEAM CHALLENGES

Cyber attacks become more sophisticated and costly



32% **increase**

in global weekly cyber attacks (YoY)

41% **increase**

in ransomware attacks

Gen V **attacks**

at nation state scale

Report: Phishing attacks jump 61% in 2022, with 255M attacks detected

*(Check Point ThreatCloud)

SOC analysts are overwhelmed with alerts

277 Days to identify and contain a breach*

Security teams struggle to shutdown attacks before damage spreads

- Endless alerts, false positives
- Multiple tools in silos
- Narrow view of attacks
- Cyber skills shortage

**(IBM report 2021)*

Infinity
XDR/XPR

Collaborative Improves Security

Overcome Limitations of Silos

to prevent attacks across
the entire security estate

Make Security Collaborative

make products, people
& processes work together

Existing XDR solutions focus on detection

"Stitch together threat signals"

"Hunt, Investigate and Remediate"

"Connect the dots"

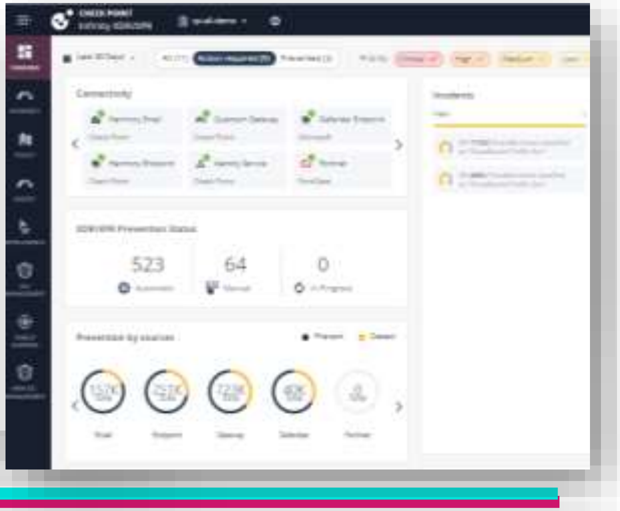
What's preventing attacks from spreading?

**(IBM report 2021)*

Infinity: Prevention-First Security Operations

Infinity
XDR/XPR

Comprehensive threat prevention across your entire estate through **collaborative, intelligent AI** correlation



CloudGuard
Secure the Cloud

Quantum
Secure the Network

Harmony
Secure Users & Access

aws

Azure

Microsoft Active Directory

Microsoft Defender

Azure Active Directory

Office 365

Google Workspace

slack

Dropbox

YOU NEED AN XDR SOLUTION THAT FOCUSES ON PREVENTION

Infinity
XDR/XPR

Infinity XDR/XPR

Automatically prevent attacks from spreading through intelligent AI correlation

Fast Onboarding, As a Cloud Service

Automatic Prevention Responses

Infinity XDR/XPR

AI Based Correlations

Simple Investigation Experience

RELEASED IN 2023

3 Months of XDR/XPR Efficiency

2 TRILLION
EVENTS

99%
NOISE REDUCTION

600K
HIGH/CRITICAL
INCIDENTS

XDR/XPR

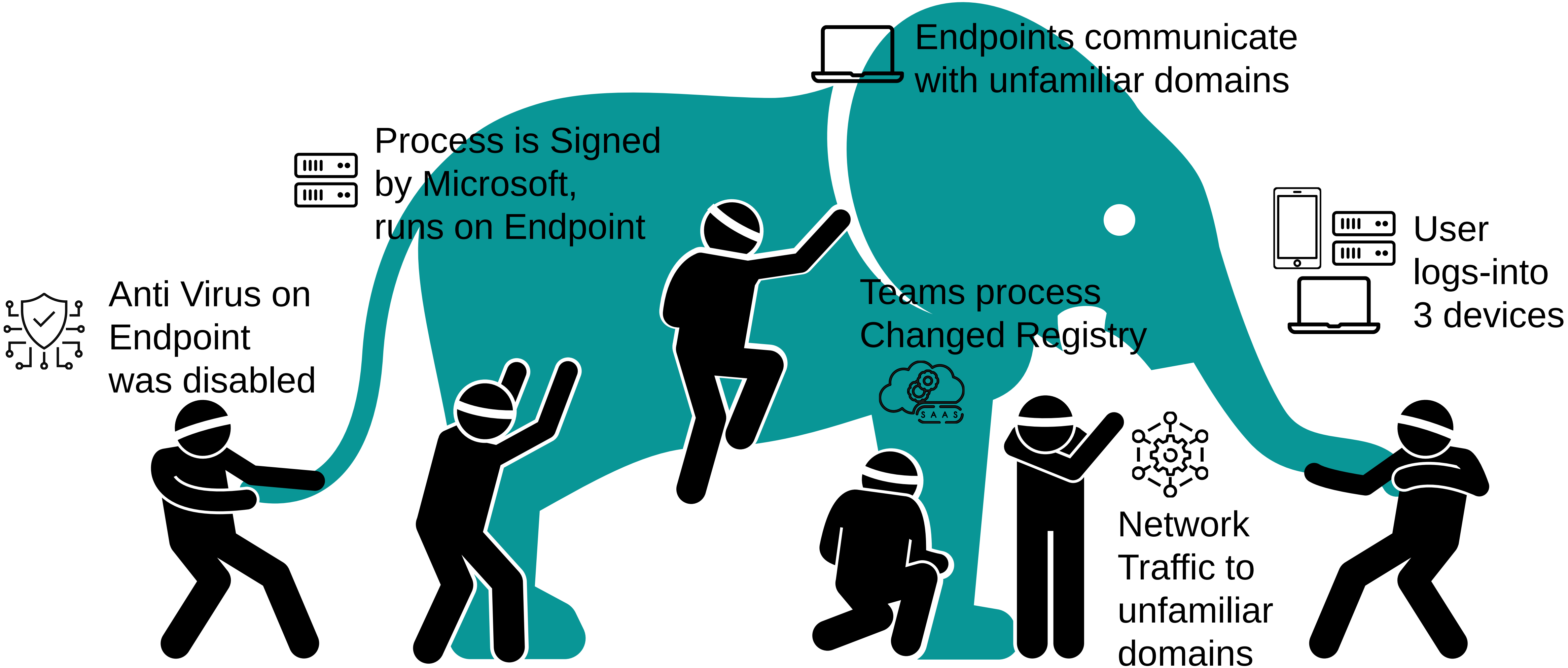
REAL USE CASES

The Challenge: Security and Data Silos

The Goal:
Bringing it all Together

Infinity XDR/XPR

Example - A bank in Europe



Endpoints communicate with unfamiliar domains

Process is Signed by Microsoft, runs on Endpoint

Anti Virus on Endpoint was disabled

Teams process Changed Registry

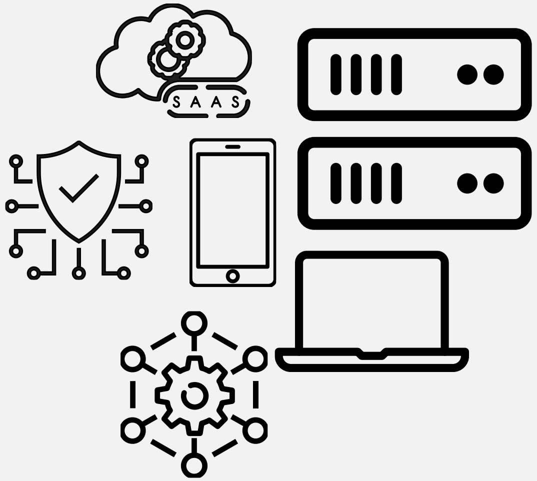
User logs-into 3 devices

Network Traffic to unfamiliar domains

Infinity
XDR/XPR

Endpoint and Gateway Detections Correlated Into XDR/XPR Incident

CORRELATION



DETECTION

High Severity Breach
Is Active on 3 Endpoints
Compromised 1 User

COMPREHENSIVE PREVENTION

- Isolated Infected endpoints
- Blocked Malicious URLs
- Removed Reset Password for user
- Processes from devices

Quantum Harmony CloudGuard

Bank, EMEA

Infinity
XDR/XPR

Endpoint and Gateway Detections Correlated Into XDR/XPR Incident

CORRELATION

XDR/XPR behavioral signatures with evidences detected about the malware activity

Quantum Harmony Infinity XDR/XPR

DETECTION

“Raspberry Robin” malware incident with compromised Endpoint

COMPREHENSIVE PREVENTION

- Isolated Infected endpoint
- Blocked Malicious IP addresses on all connected products to XDR/XPR

Quantum Harmony CloudGuard

Government, LATAM

Infinity XDR/XPR

Raspberry Robin Incident

Thank you very much for your alerting us about this. Initial checks the user inserted a USB just prior to the incident. The USB was subsequently scanned, and the endpoint and the user account password was changed. Followed your advice and isolated the endpoint through the XDR/XPR portal this morning.

Government Company, LATAM

HOW XDR/XPR WORKS

Infinity
XDR/XPR

XDR/XPR addresses cyber complexity with the 3Cs of Best Security

COMPREHENSIVE
THREAT PREVENTION

Automatic attack prevention across the entire security estate

INTELLIGENT
CORRELATIONS

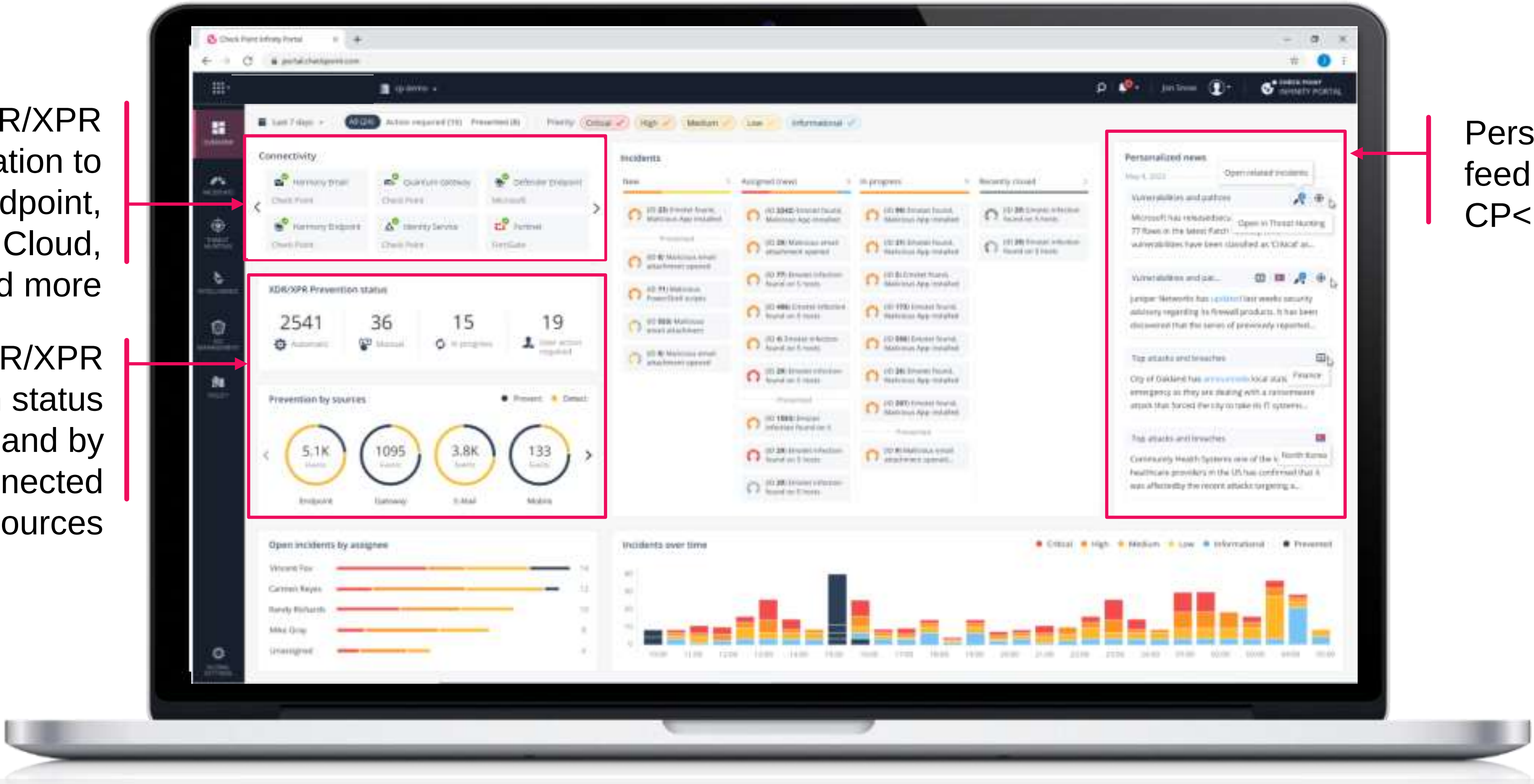
Powered by AI and Threat intelligence Correlating Check Point & Third-Party Events

CONSOLIDATED
ANALYTICS

Improve posture through visibility to attack behavior, context and damage

Comprehensive Threat Prevention

XDR/XPR takes immediate, comprehensive prevention actions across all parts of the security estate



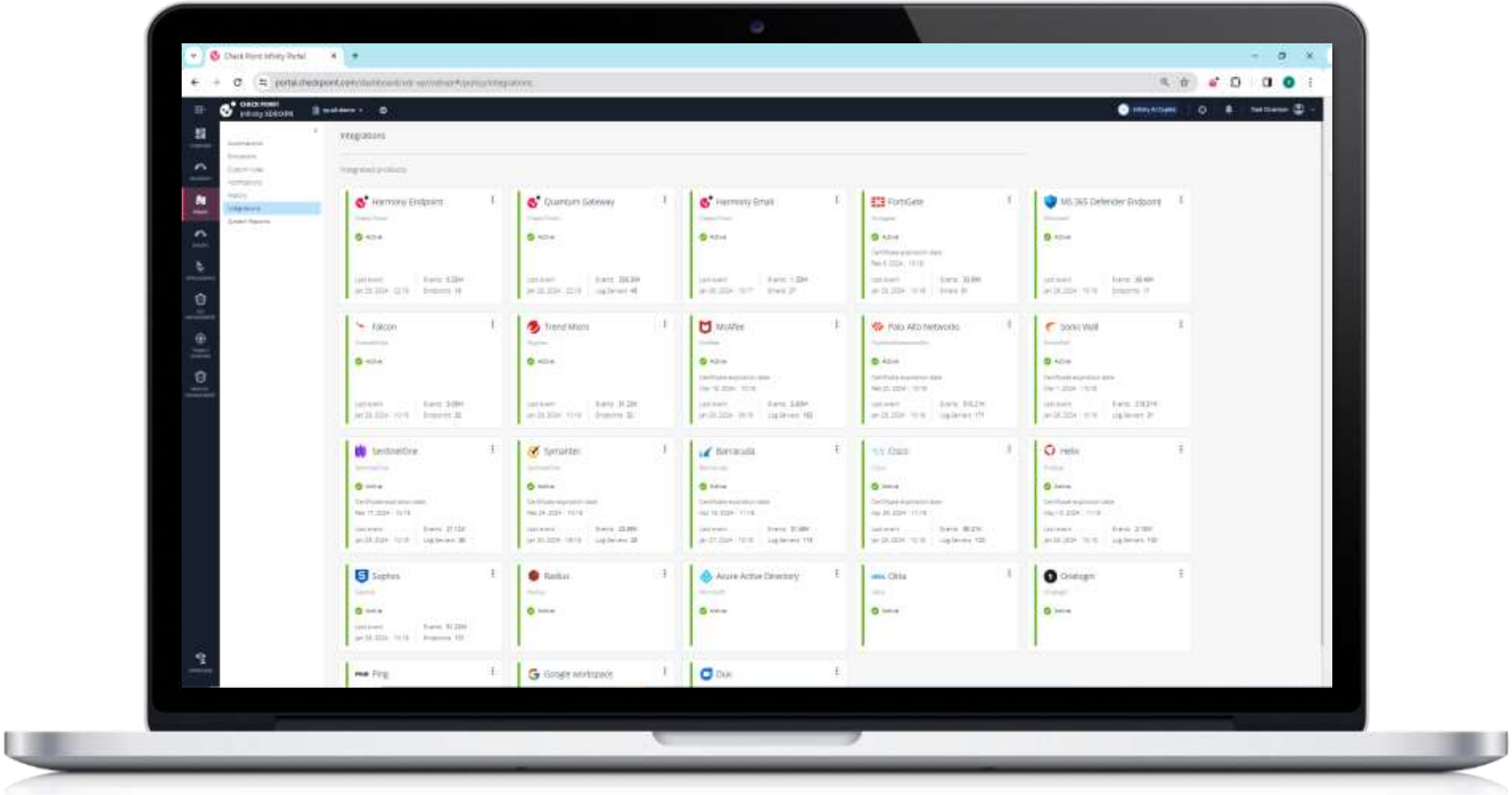
XDR/XPR integration to Endpoint, Network, Cloud, Mobile and more

XDR/XPR Prevention status and by connected sources

Personalized new feed powered by CP<r>

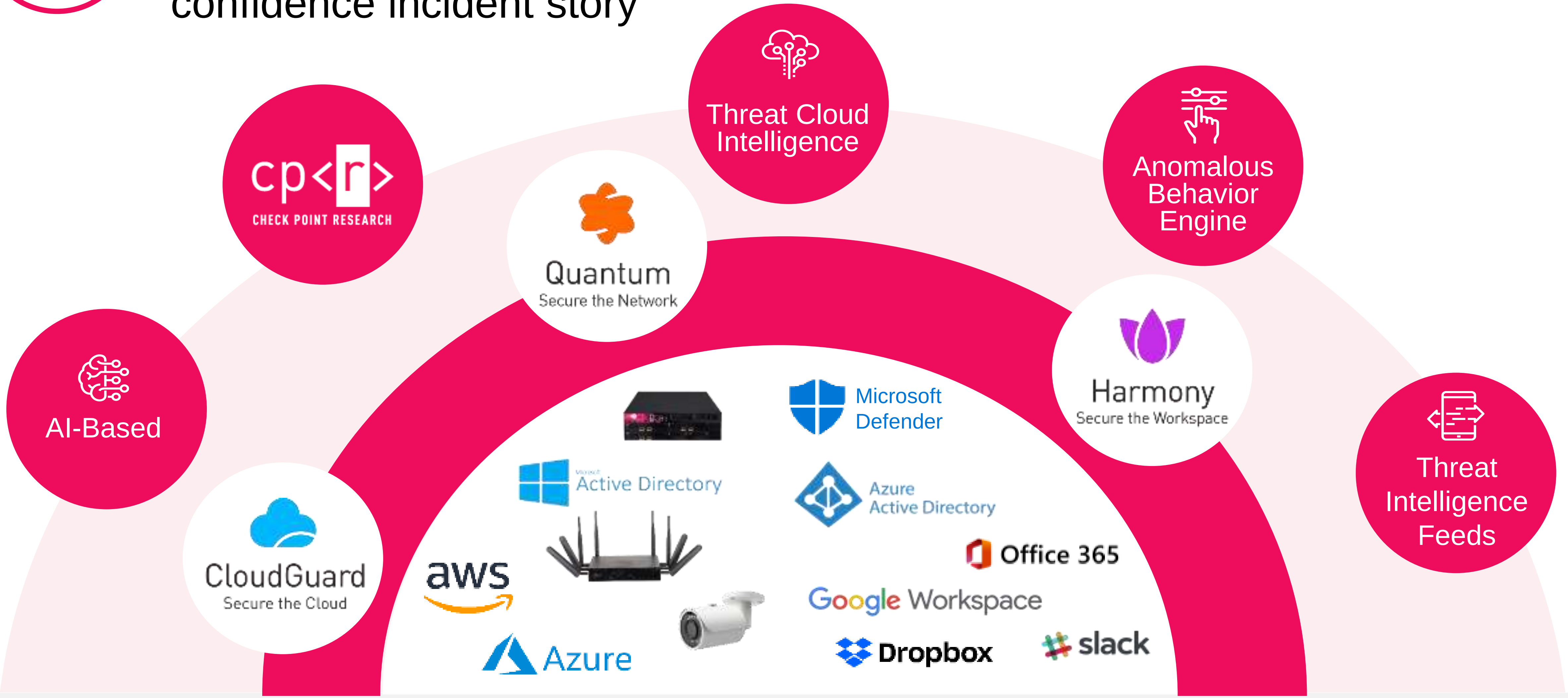
Comprehensive Threat Prevention

20+ integrations with Check Point and third-party solutions



Intelligent Event Correlation

XDR/XPR determines advanced attacks from millions of events to high confidence incident story



Threat Cloud Intelligence

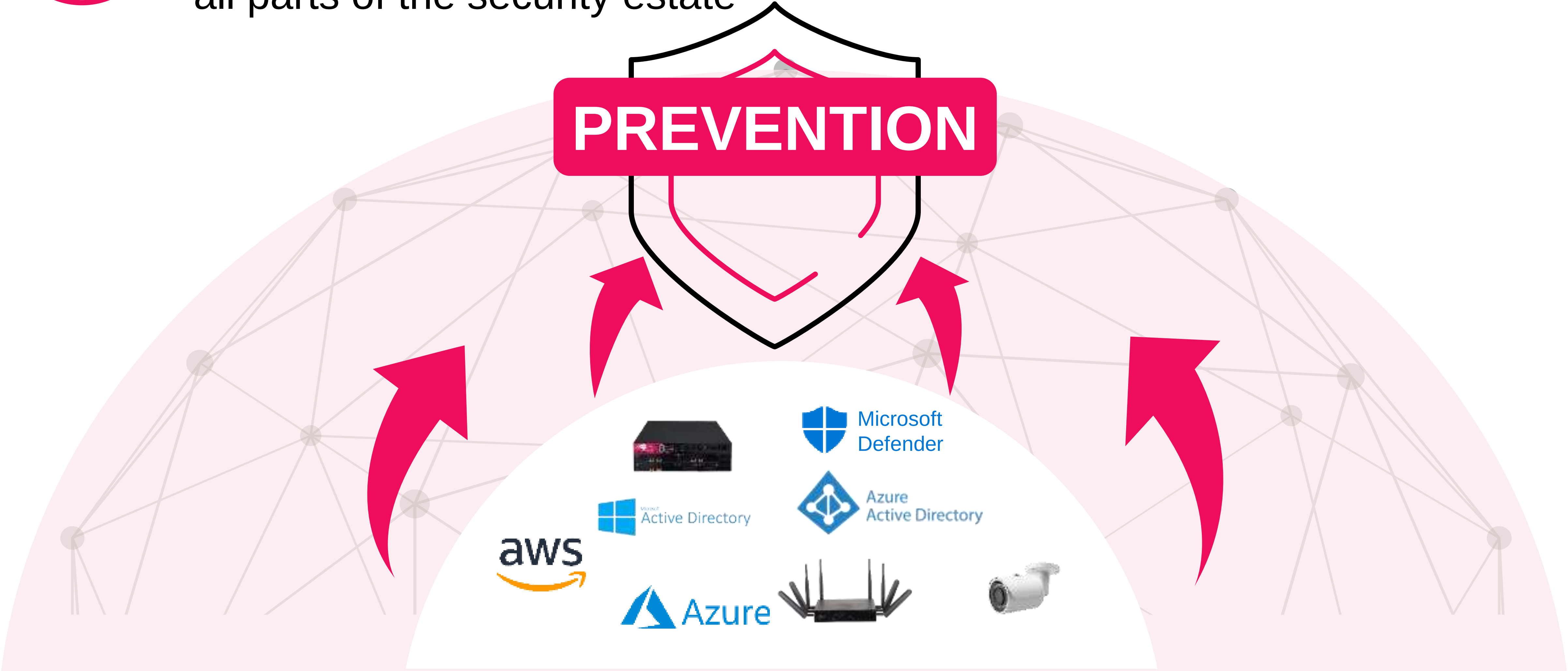
Anomalous Behavior Engine

AI-Based

Threat Intelligence Feeds

Comprehensive Threat Prevention

XDR/XPR takes immediate, comprehensive prevention actions across all parts of the security estate

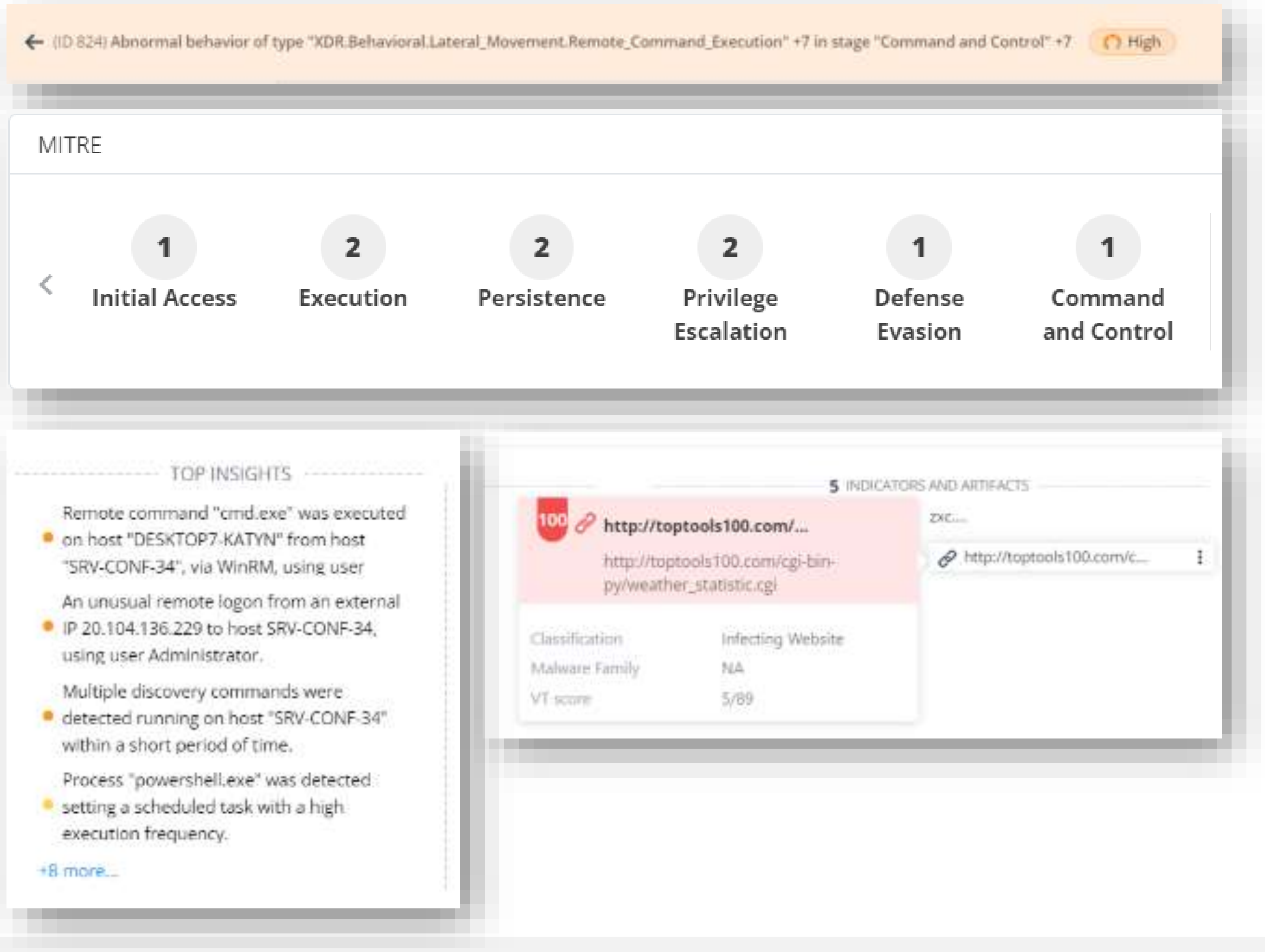


Consolidated Analytics

XDR/XPR improves posture through visibility to attack behavior, context and damage

Understand the Attack chain using MITRE mapping

Visibility to all compromised entities



← (ID 824) Abnormal behavior of type "XDR.Behavioral.Lateral_Movement.Remote_Command_Execution" +7 in stage "Command and Control" +7 High

MITRE

1	2	2	2	1	1
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Command and Control

TOP INSIGHTS

- Remote command "cmd.exe" was executed on host "DESKTOP7-KATYN" from host "SRV-CONF-34", via WinRM, using user
- An unusual remote logon from an external IP 20.104.136.229 to host SRV-CONF-34, using user Administrator.
- Multiple discovery commands were detected running on host "SRV-CONF-34" within a short period of time.
- Process "powershell.exe" was detected setting a scheduled task with a high execution frequency.

+8 more...

5 INDICATORS AND ARTIFACTS

100 http://toptools100.com/...

http://toptools100.com/cgi-bin-py/weather_statistic.cgi

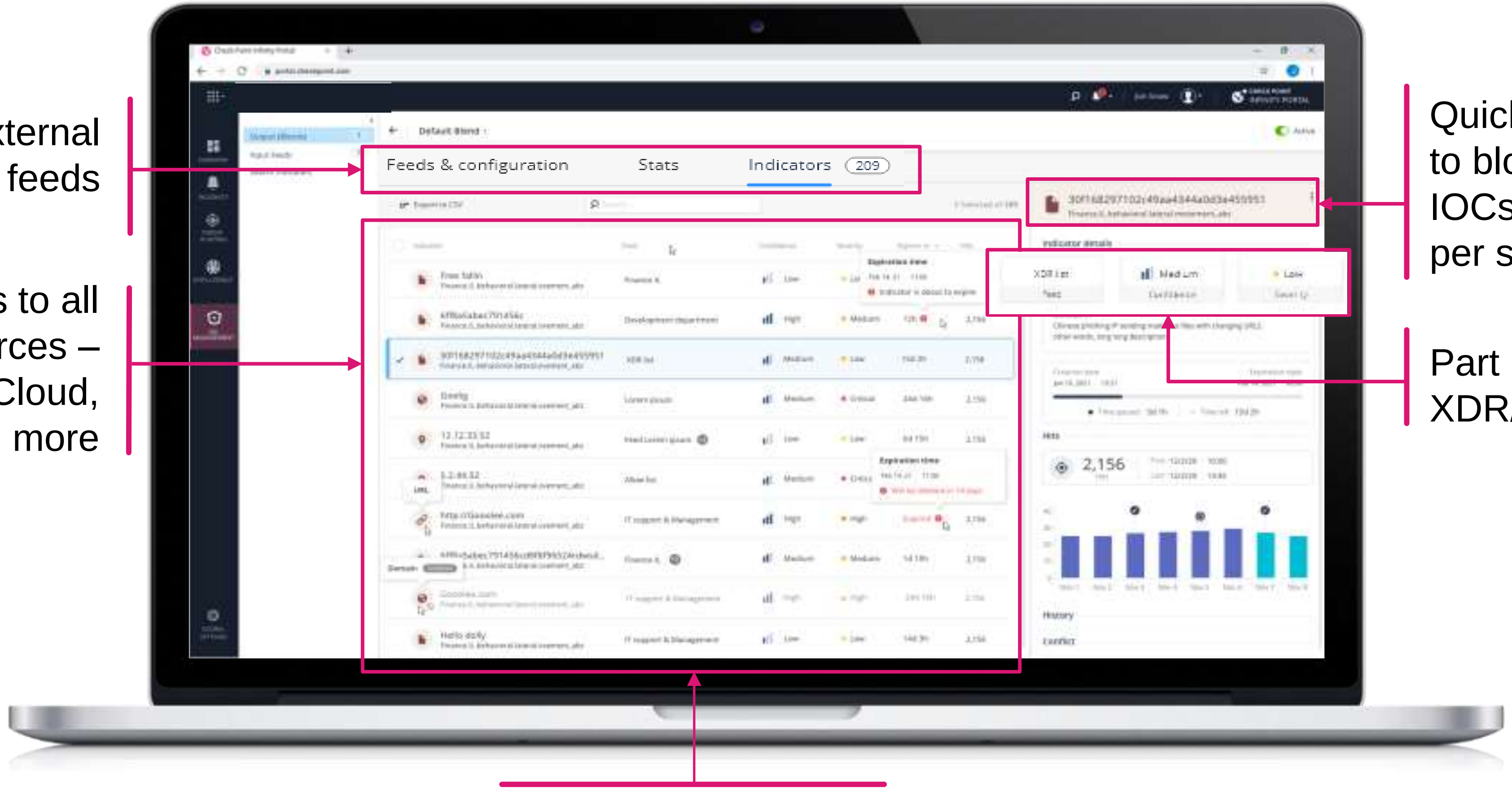
Classification	Infecting Website
Malware Family	NA
VT score	5/89

zxc...

http://toptools100.com/c...

Immediate Prevention of the Attack

IOC Management and enforcement across the entire IT environment



Ingestion of external third-party feeds

Single pane of glass to all IOCs from all sources – Network, Endpoint, Cloud, Email, and more

Quick responses to block/allow IOCs globally or per source

Part of Infinity XDR/XPR

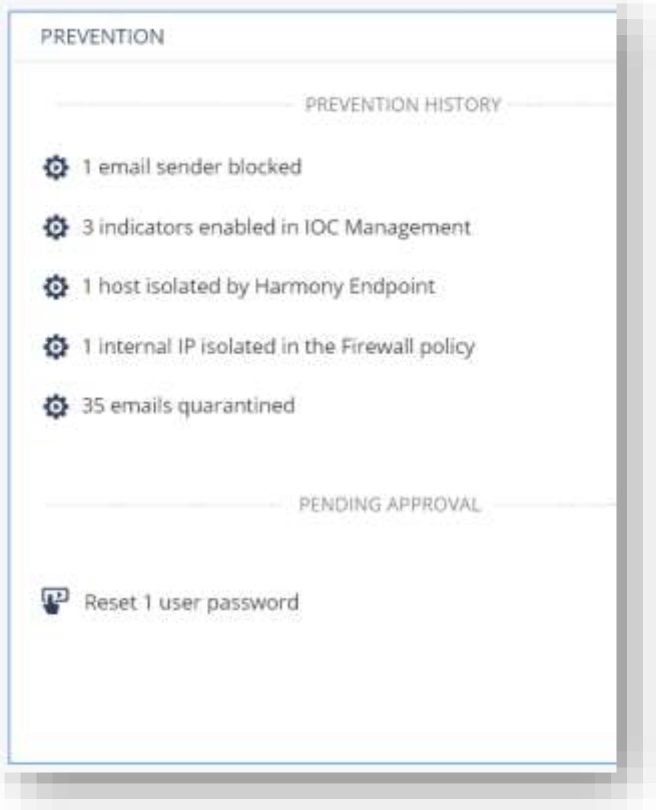
Multi-tenant ready for MSSPs

Immediate Prevention of the Attack

Automatic Response Playbooks across the entire organization

Auto Mitigation and Response

- Isolate compromised endpoint
- Block malicious indicators
- Quarantine email
- Endpoint Forensics analysis
- Terminate a process
- Force password change



PREVENTION

PREVENTION HISTORY

- 1 email sender blocked
- 3 indicators enabled in IOC Management
- 1 host isolated by Harmony Endpoint
- 1 internal IP isolated in the Firewall policy
- 35 emails quarantined

PENDING APPROVAL

- Reset 1 user password

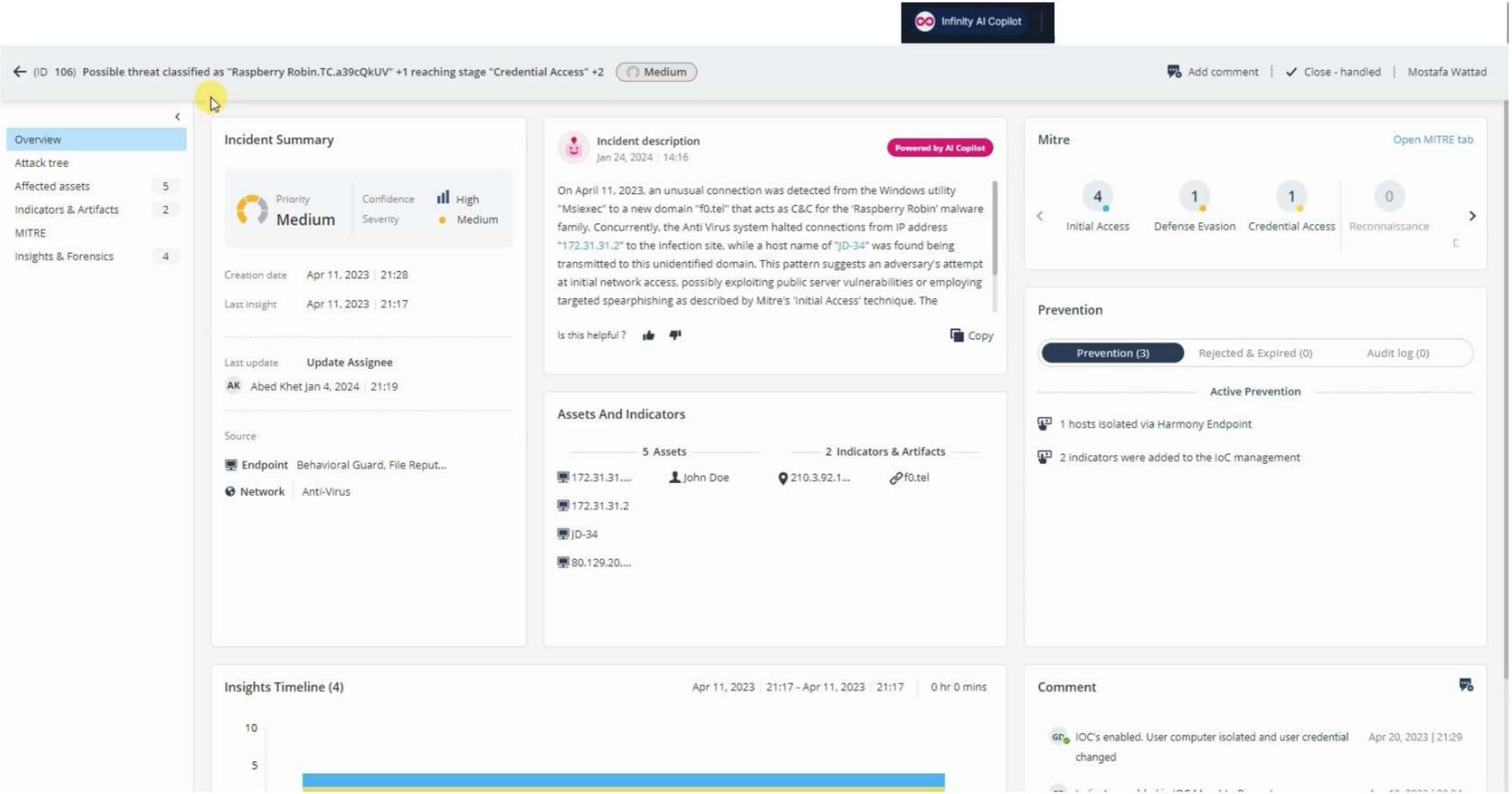
Infinity

Playblocks

Security Automation & Response

Collaborative Security In Action

Raspberry Robin XPR incident for Government company



Infinity AI Copilot

← (ID 106) Possible threat classified as "Raspberry Robin.TC.a39cQkUV" +1 reaching stage "Credential Access" +2 Medium

Add comment | ✓ Close - handled | Mostafa Wattad

Overview	
Attack tree	
Affected assets	5
Indicators & Artifacts	2
MITRE	
Insights & Forensics	4

Incident Summary

Priority: Medium
Confidence: High
Severity: Medium

Creation date: Apr 11, 2023 | 21:28
Last insight: Apr 11, 2023 | 21:17

Last update: Update Assignee
AK Abed Khet Jan 4, 2024 | 21:19

Source
Endpoint | Behavioral Guard, File Reput...
Network | Anti-Virus

Incident description
Jan 24, 2024 | 14:16
Powered by AI Copilot

On April 11, 2023, an unusual connection was detected from the Windows utility "Msiexec" to a new domain "f0.tel" that acts as C&C for the 'Raspberry Robin' malware family. Concurrently, the Anti Virus system halted connections from IP address "172.31.31.2" to the infection site, while a host name of "JD-34" was found being transmitted to this unidentified domain. This pattern suggests an adversary's attempt at initial network access, possibly exploiting public server vulnerabilities or employing targeted spearphishing as described by Mitre's 'Initial Access' technique. The

Is this helpful ? Copy

Assets And Indicators

5 Assets
172.31.31.... | John Doe
172.31.31.2
JD-34
80.129.20....

2 Indicators & Artifacts
210.3.92.1... | f0.tel

Mitre Open MITRE tab

4	1	1	0
Initial Access	Defense Evasion	Credential Access	Reconnaissance

Prevention

Prevention (3) | Rejected & Expired (0) | Audit log (0)

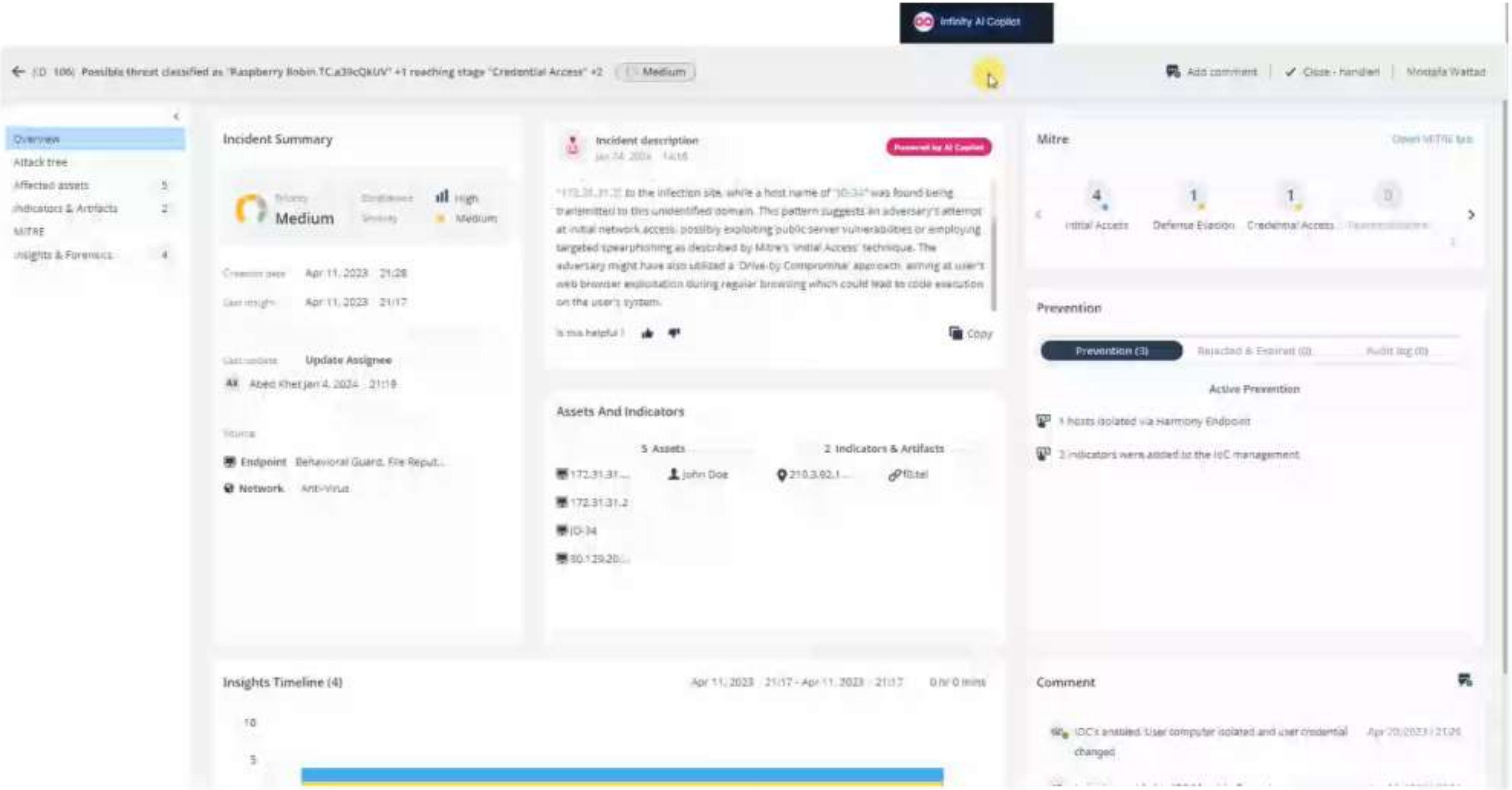
Active Prevention
1 hosts isolated via Harmony Endpoint
2 indicators were added to the IoC management

Insights Timeline (4) Apr 11, 2023 | 21:17 - Apr 11, 2023 | 21:17 | 0 hr 0 mins

Comment

GD IOC's enabled. User computer isolated and user credential changed Apr 20, 2023 | 21:29

Using Infinity AI Copilot for further investigation



Infinity AI Copilot

← ID 106) Possible threat classified as "Raspberry Robin.TC.a39cQkUV" +1 reaching stage "Credential Access" +2 Medium

Add comment | ✓ Close - handled | Mostafa Wattad

Overview
Attack tree
Affected assets 5
Indicators & Artifacts 2
MITRE
Insights & Forensics 4

Incident Summary

Priority Medium
Confidence High
Severity Medium

Creation date Apr 11, 2023 21:28
Last insight Apr 11, 2023 21:17

Last update Update Assignee
AK Abed Khet Jan 4, 2024 21:19

Source
Endpoint Behavioral Guard, File Reput...
Network Anti-Virus

Incident description

Jan 24, 2024 14:16

Powered by AI Copilot

"172.31.31.2" to the infection site, while a host name of "ID-34" was found being transmitted to this unidentified domain. This pattern suggests an adversary's attempt at initial network access, possibly exploiting public server vulnerabilities or employing targeted spearphishing as described by Mitre's 'Initial Access' technique. The adversary might have also utilized a 'Drive-by Compromise' approach, aiming at user's web browser exploitation during regular browsing which could lead to code execution on the user's system.

Is this helpful ? Copy

Assets And Indicators

5 Assets
172.31.31...
John Doe
172.31.31.2
ID-34
80.129.20...

2 Indicators & Artifacts
210.3.92.1...
f0.tel

Mitre

Open MITRE tab

4 Initial Access
1 Defense Evasion
1 Credential Access
0 [illegible]

Prevention

Prevention (3) | Rejected & Expired (0) | Audit log (0)

Active Prevention

1 hosts isolated via Harmony Endpoint

2 indicators were added to the IoC management

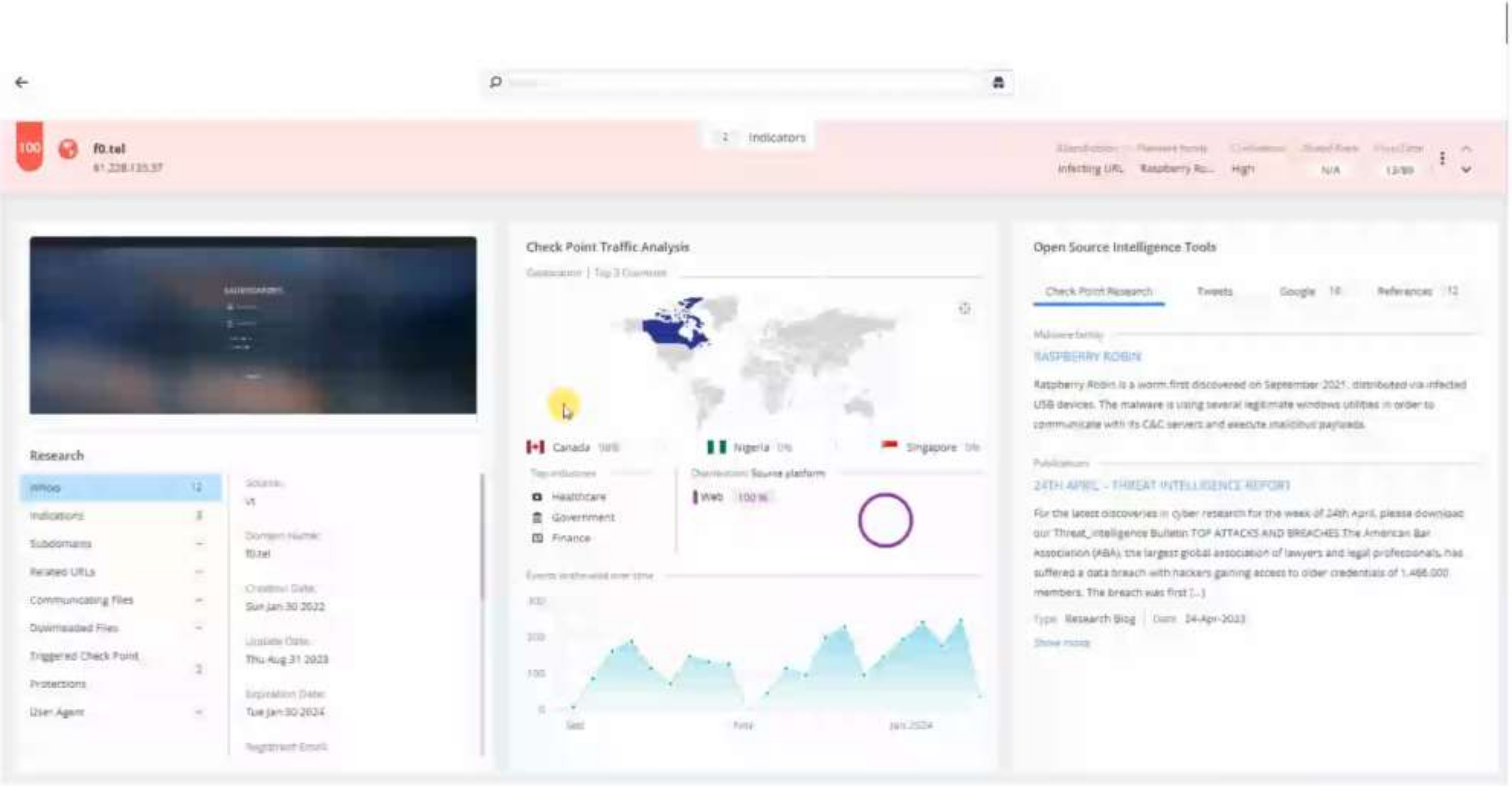
Insights Timeline (4)

Apr 11, 2023 21:17 - Apr 11, 2023 21:17 0 hr 0 mins

Comment

IOC's enabled. User computer isolated and user credential changed Apr 20, 2023 / 21:26

VirusTotal Seamlessly Integrated in Infinity XDR/XPR



100 f0.tel
61.228.135.37

2 Indicators

Infecting URL | Raspberry Ro... | High | N/A | 13/89

Check Point Traffic Analysis

Geolocation | Top 3 Countries

Canada 98% | Nigeria 1% | Singapore 1%

Top industries

- Healthcare
- Government
- Finance

Distribution: Source platform

Web 100 %

Events worldwide over time

Research

Whois	12
Indications	3
Subdomains	–
Related URLs	–
Communicating Files	–
Downloaded Files	–
Triggered Check Point Protections	2
User Agent	–

Source:
VT

Domain Name:
f0.tel

Creation Date:
Sun Jan 30 2022

Update Date:
Thu Aug 31 2023

Expiration Date:
Tue Jan 30 2024

Registrant Email:

Open Source Intelligence Tools

Check Point Research | Tweets | Google 18 | References 12

Malware family

RASPBERRY ROBIN

Raspberry Robin is a worm first discovered on September 2021, distributed via infected USB devices. The malware is using several legitimate windows utilities in order to communicate with its C&C servers and execute malicious payloads.

Publications

24TH APRIL – THREAT INTELLIGENCE REPORT

For the latest discoveries in cyber research for the week of 24th April, please download our Threat_Intelligence Bulletin TOP ATTACKS AND BREACHES The American Bar Association (ABA), the largest global association of lawyers and legal professionals, has suffered a data breach with hackers gaining access to older credentials of 1,466,000 members. The breach was first [...]

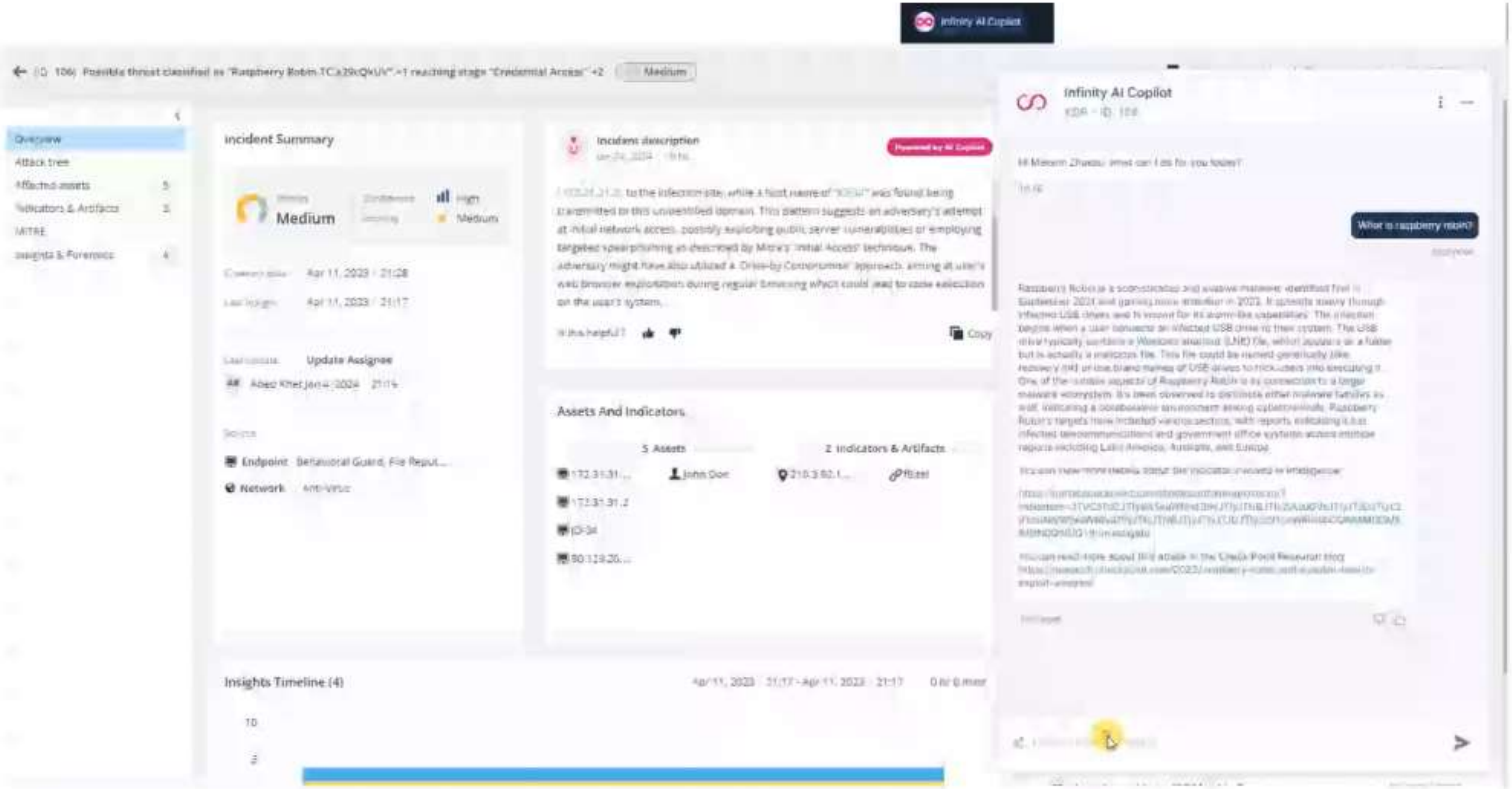
Type: Research Blog | Date: 24-Apr-2023

Show more

CHECK POINT

©2022 Check Point Software TechnologiesLtd.

Using Infinity AI Copilot for forensic details in TH



Apr 11, 2023 · 21:28

Apr 11, 2023 · 21:17

Abed Khet Jan 4, 2024 · 21:14

... to the infection site, while a host name of "..." was found being transmitted to this unidentified domain. This pattern suggests an adversary's attempt at initial network access, possibly exploiting public server vulnerabilities or employing targeted spearphishing as described by Mitre's 'Initial Access' technique. The adversary might have also utilized a 'Drive-by Compromise' approach, aiming at user's web browser exploitation during regular browsing which could lead to code execution on the user's system.

Is this helpful?

Apr 11, 2023 · 21:17 - Apr 11, 2023 · 21:17

Hi Meirem Zhaou, what can I do for you today?

Raspberry Robin is a sophisticated and evasive malware identified first in September 2021 and gaining more attention in 2022. It spreads mainly through infected USB drives and is known for its worm-like capabilities. The infection begins when a user connects an infected USB drive to their system. The USB drive typically contains a Windows shortcut (LNK) file, which appears as a folder but is actually a malicious file. This file could be named generically like recovery.lnk or use brand names of USB drives to trick users into executing it. One of the notable aspects of Raspberry Robin is its connection to a larger malware ecosystem. It's been observed to distribute other malware families as well, indicating a collaborative environment among cybercriminals. Raspberry Robin's targets have included various sectors, with reports indicating it has infected telecommunications and government office systems across multiple regions including Latin America, Australia, and Europe.

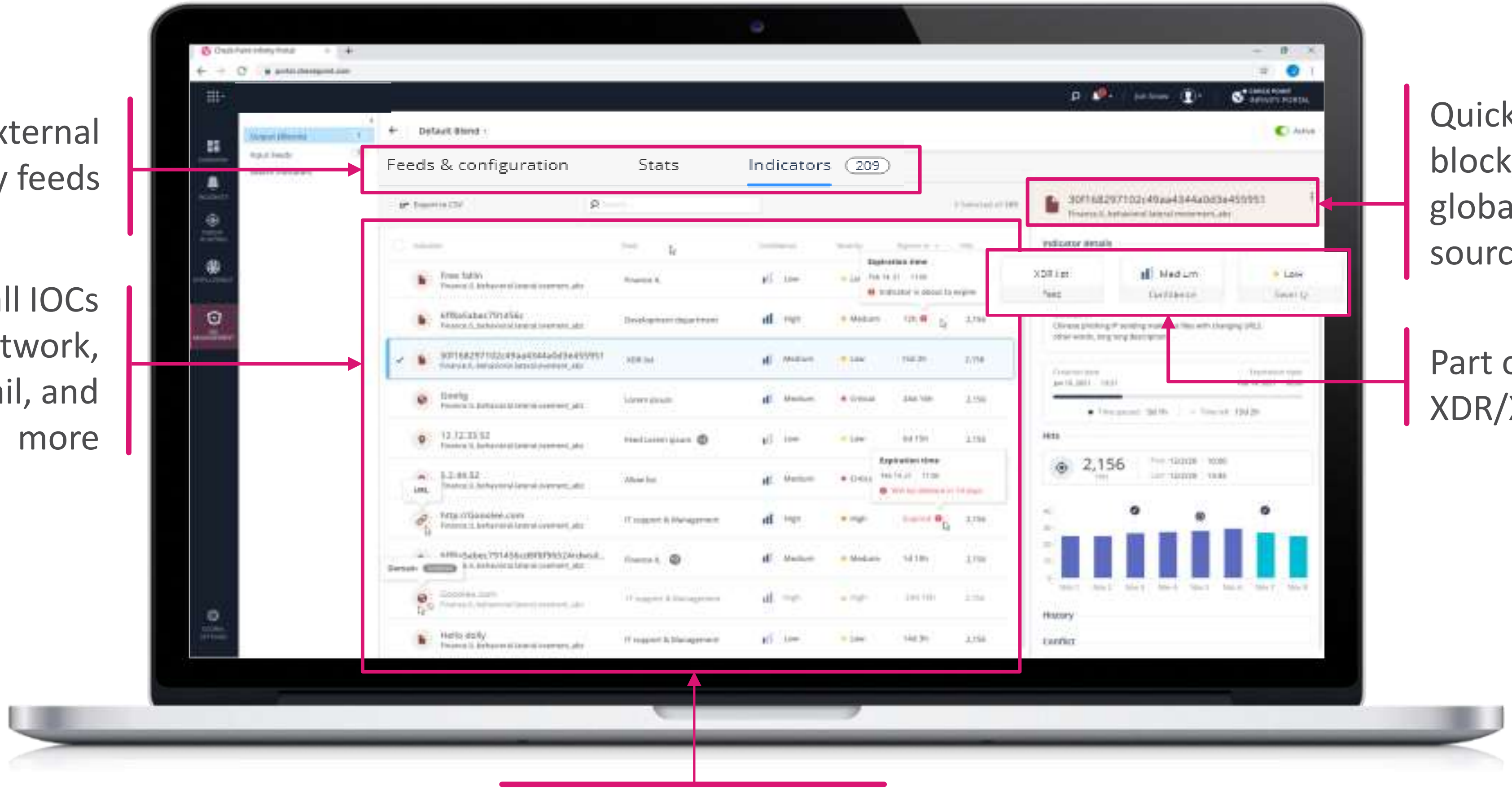
You can view more details about the indicator related in Intelligence:

[illegible]

You can read more about this attack in the Check Point Research blog: [illegible]

Immediate Prevention of the Attack

IOC Management and enforcement across the entire IT environment



Ingestion of external third-party feeds

Single pane of glass to all IOCs from all sources – Network, Endpoint, Cloud, Email, and more

Quick responses to block/allow IOCs globally or per source

Part of Infinity XDR/XPR

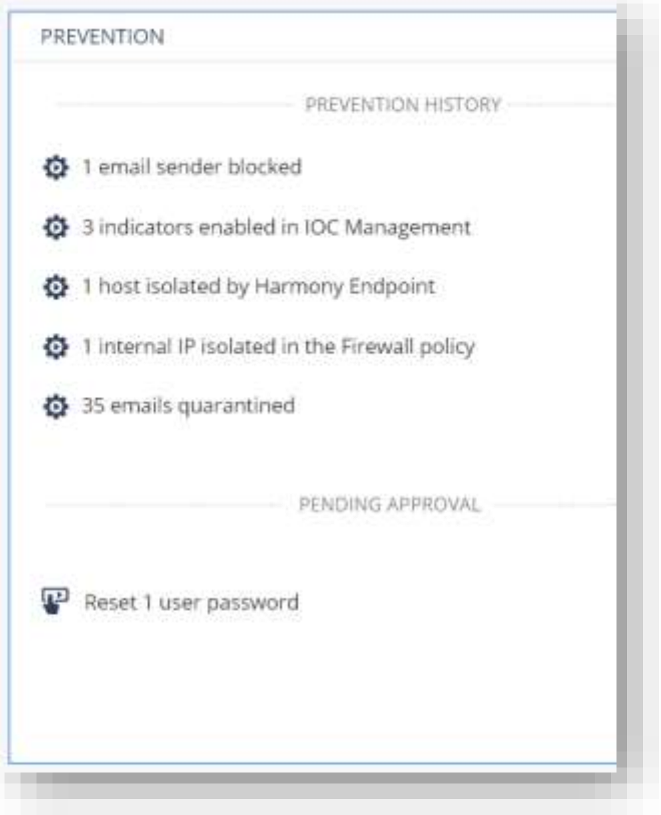
Multi-tenant ready for MSSPs

Immediate Prevention of the Attack

Automatic Response Playbooks across the entire organization

Auto Mitigation and Response

- Isolate compromised endpoint
- Block malicious indicators
- Endpoint Forensics analysis
- Terminate a process
- And many more…



PREVENTION

PREVENTION HISTORY

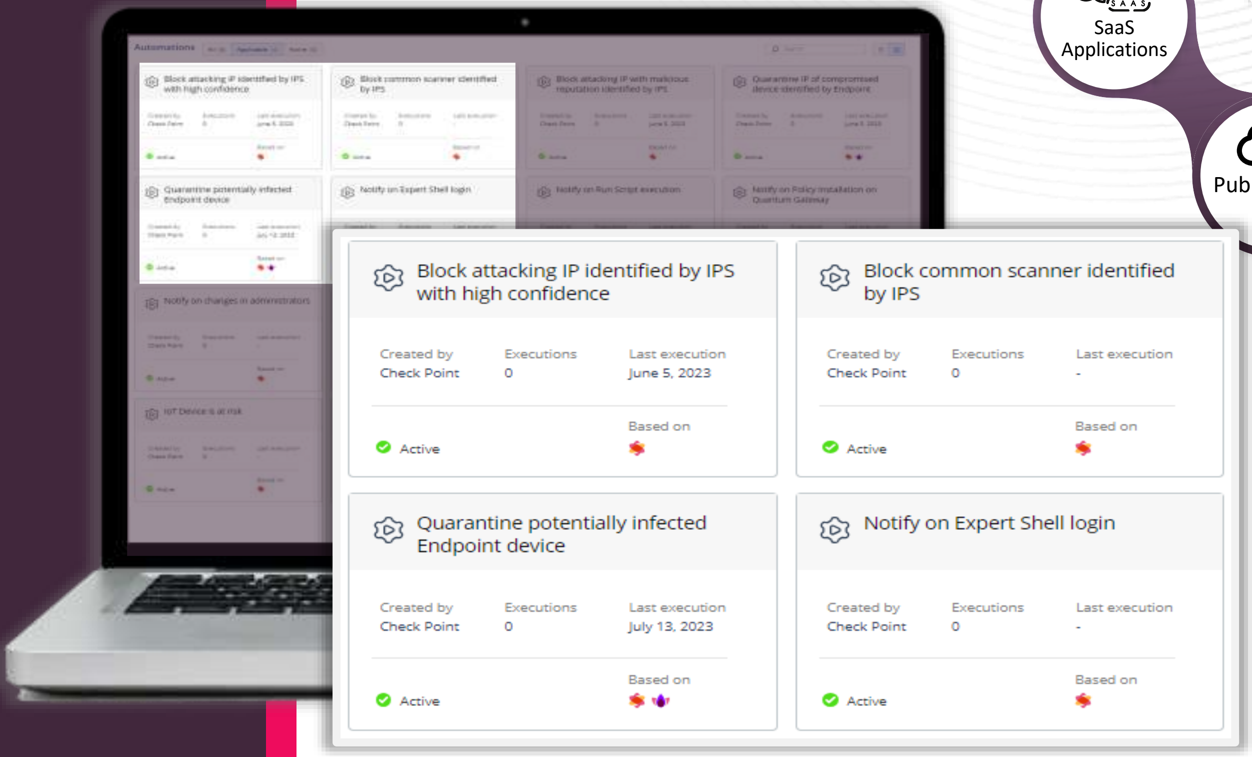
- 1 email sender blocked
- 3 indicators enabled in IOC Management
- 1 host isolated by Harmony Endpoint
- 1 internal IP isolated in the Firewall policy
- 35 emails quarantined

PENDING APPROVAL

- Reset 1 user password

Infinity Playblocks

COLLABORATIVE
SECURITY
IN ACTION



Automations

Block attacking IP identified by IPS with high confidence

Block common scanner identified by IPS

Block attacking IP with malicious reputation identified by IPS

Quarantine IP of compromised device identified by Endpoint

Quarantine potentially infected Endpoint device

Notify on Expert Shell login

Notify on Run Script execution

Notify on Policy installation on Quantum Gateway

Notify on changes in administrators

IoT Device is at risk

Block attacking IP identified by IPS with high confidence

Created by: Check Point
Executions: 0
Last execution: June 5, 2023
Active
Based on

Block common scanner identified by IPS

Created by: Check Point
Executions: 0
Last execution: -
Active
Based on

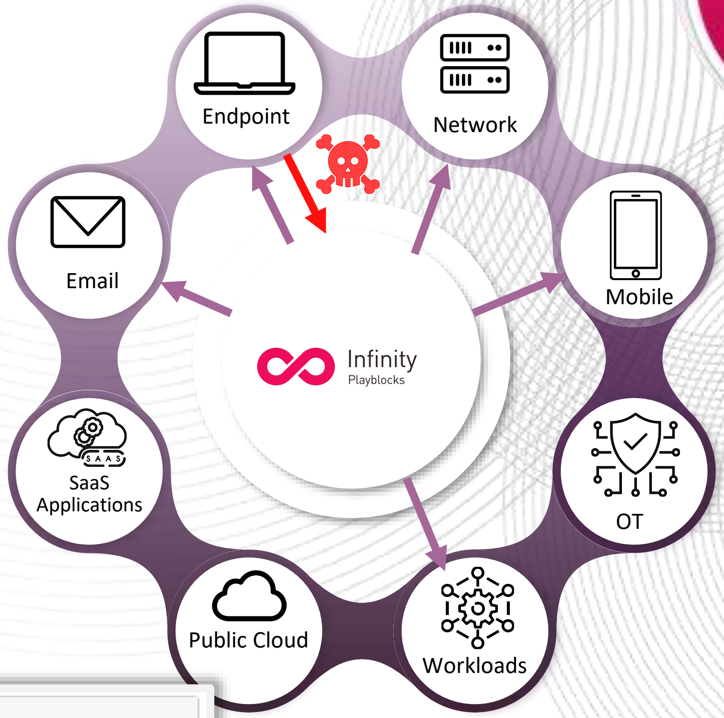
Quarantine potentially infected Endpoint device

Created by: Check Point
Executions: 0
Last execution: July 13, 2023
Active
Based on

Notify on Expert Shell login

Created by: Check Point
Executions: 0
Last execution: -
Active
Based on

RELEASED IN 2023



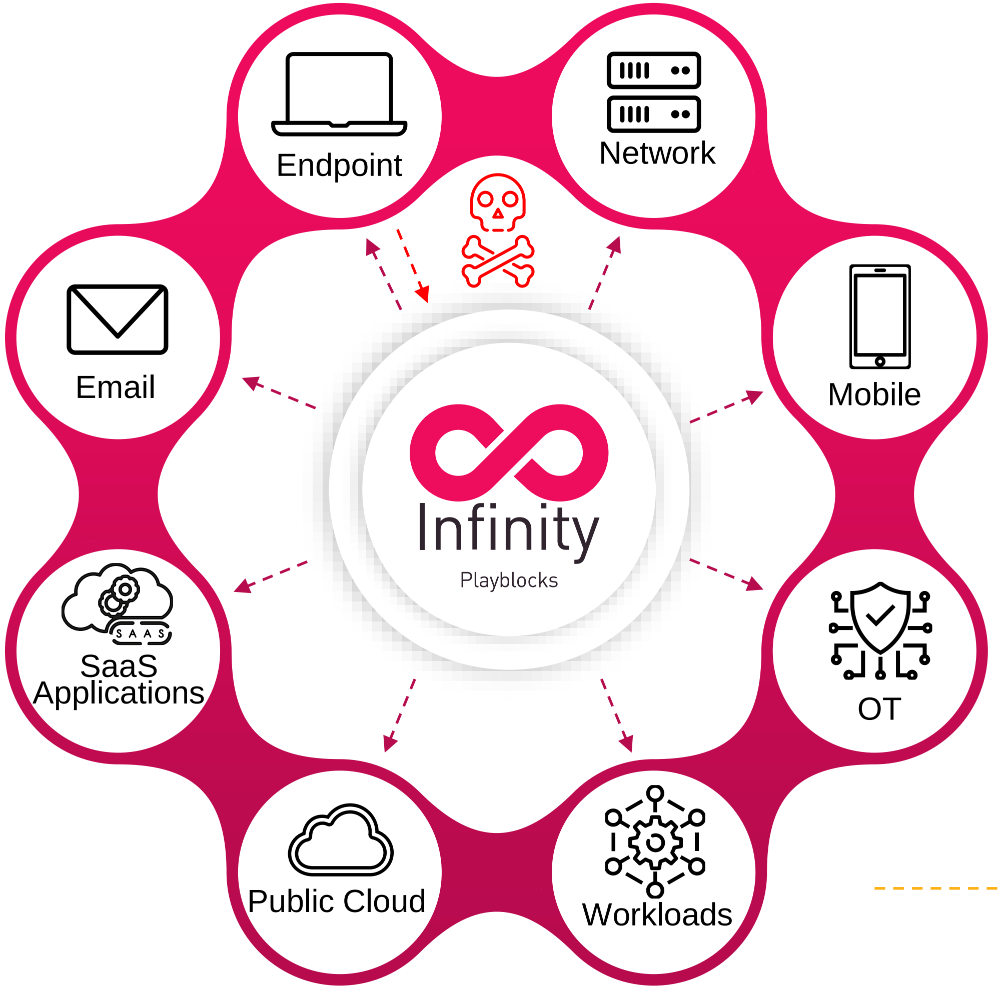
NEW

50+

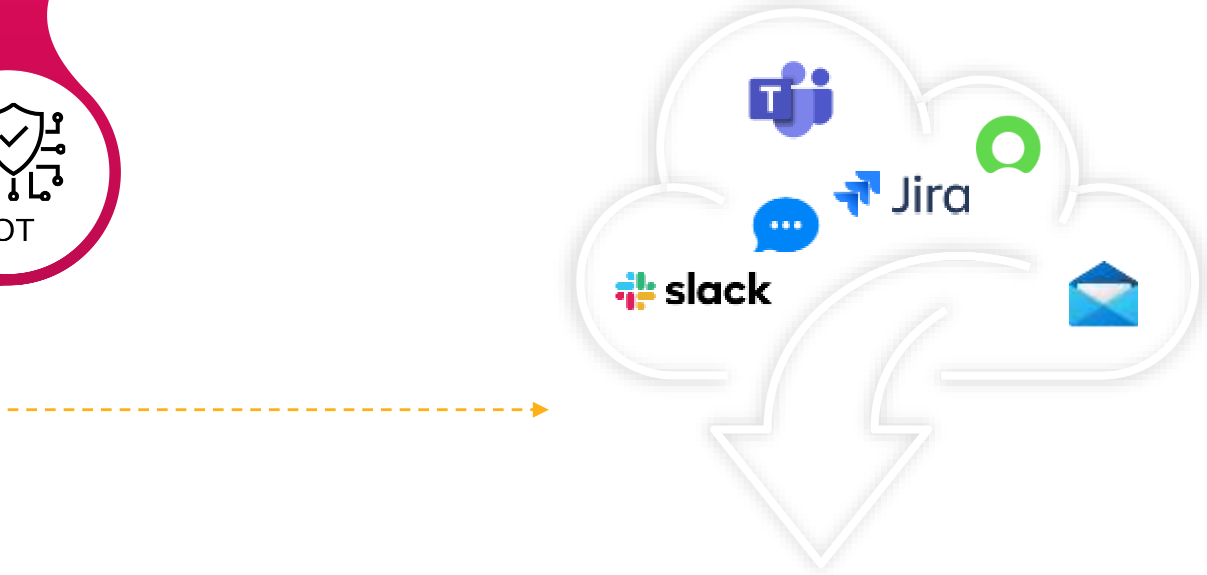
Out of the box
Playbooks

CHECK POINT

Automated, Collaborative Security Across the Enterprise



When an enforcement point identifies a potential security threat, it triggers **preventative actions across the entire security infrastructure and alerts security teams.**



Collaborative Security In Action

	I. Stop Web Vulnerability Exploits	II. Prevent Lateral Movement	III. Proactive Zero-Trust Policy Assignment
☠	Attacker identified on gateway in one geo	Endpoint file detected on Endpoint	New type of IoT device detected in network
Infinity Playblocks	Blocked attacker's IP across all international gateways & alerted admin	Quarantined infected device and blocked Trojan attack	Automatically assigned correct zero-trust policy & informed admin

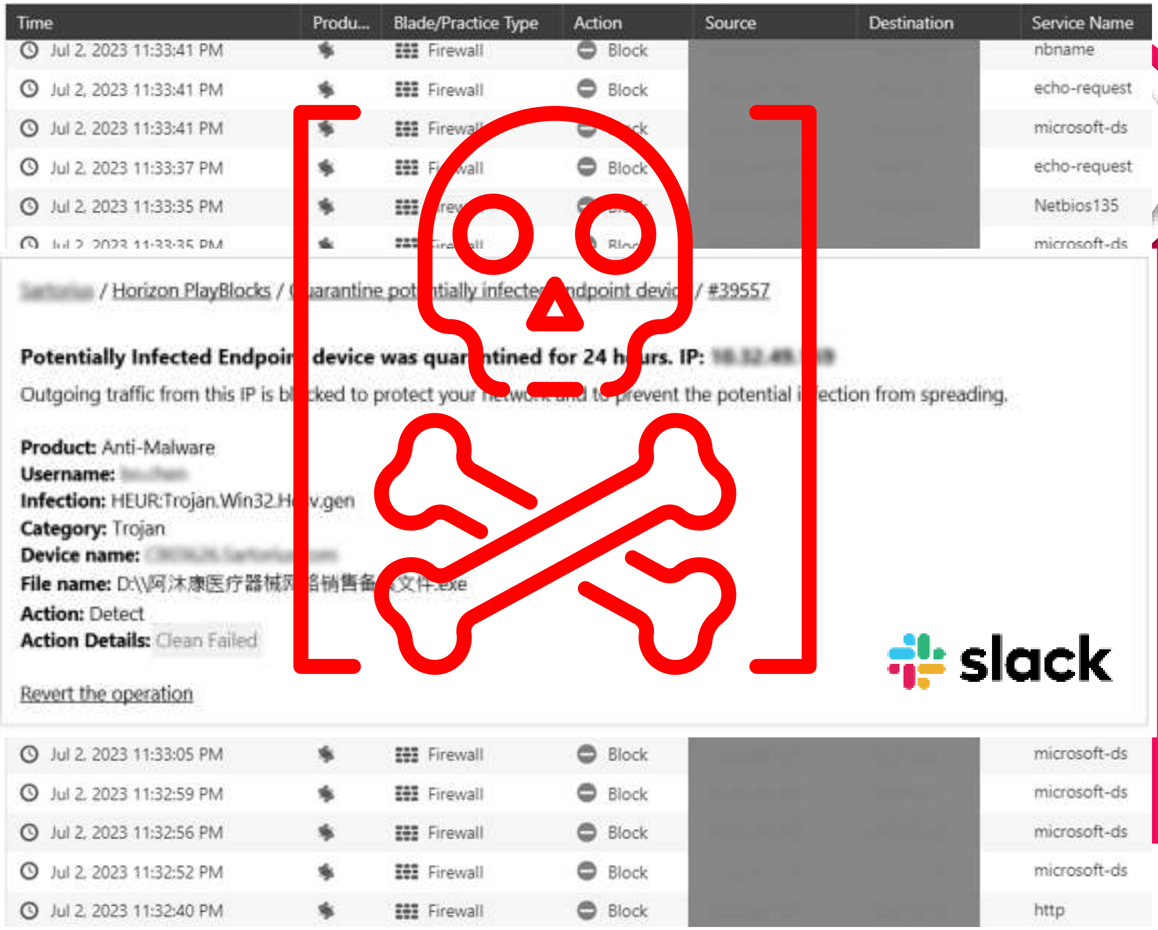
Stop Lateral Movement
Pharma – **14,000 users**

- Chinese Trojan detected on endpoint
- Endpoint solution unable to mitigate device

- Infected device automatically quarantined
- Prevented outbound traffic
- Team notified on Slack

Infinity
Playblocks

- **Playblocks blocked** outgoing traffic to 5 other devices on Gateway



Time	Produ...	Blade/Practice Type	Action	Source	Destination	Service Name
Jul 2, 2023 11:33:41 PM		Firewall	Block	[redacted]	[redacted]	nbname
Jul 2, 2023 11:33:41 PM		Firewall	Block	[redacted]	[redacted]	echo-request
Jul 2, 2023 11:33:41 PM		Firewall	Block	[redacted]	[redacted]	microsoft-ds
Jul 2, 2023 11:33:37 PM		Firewall	Block	[redacted]	[redacted]	echo-request
Jul 2, 2023 11:33:35 PM		Firewall	Block	[redacted]	[redacted]	Netbios135
Jul 2, 2023 11:33:35 PM		Firewall	Block	[redacted]	[redacted]	microsoft-ds

[redacted] / Horizon PlayBlocks / Quarantine potentially infected endpoint device / #39557

Potentially Infected Endpoint device was quarantined for 24 hours. IP: [redacted]

Outgoing traffic from this IP is blocked to protect your network and to prevent the potential infection from spreading.

Product: Anti-Malware
Username: [redacted]
Infection: HEUR:Trojan.Win32.H[illegible]v.gen
Category: Trojan
Device name: [redacted]
File name: D:\\阿沐康医疗器械[illegible]络销售备[illegible]文件.exe
Action: Detect
Action Details: Clean Failed

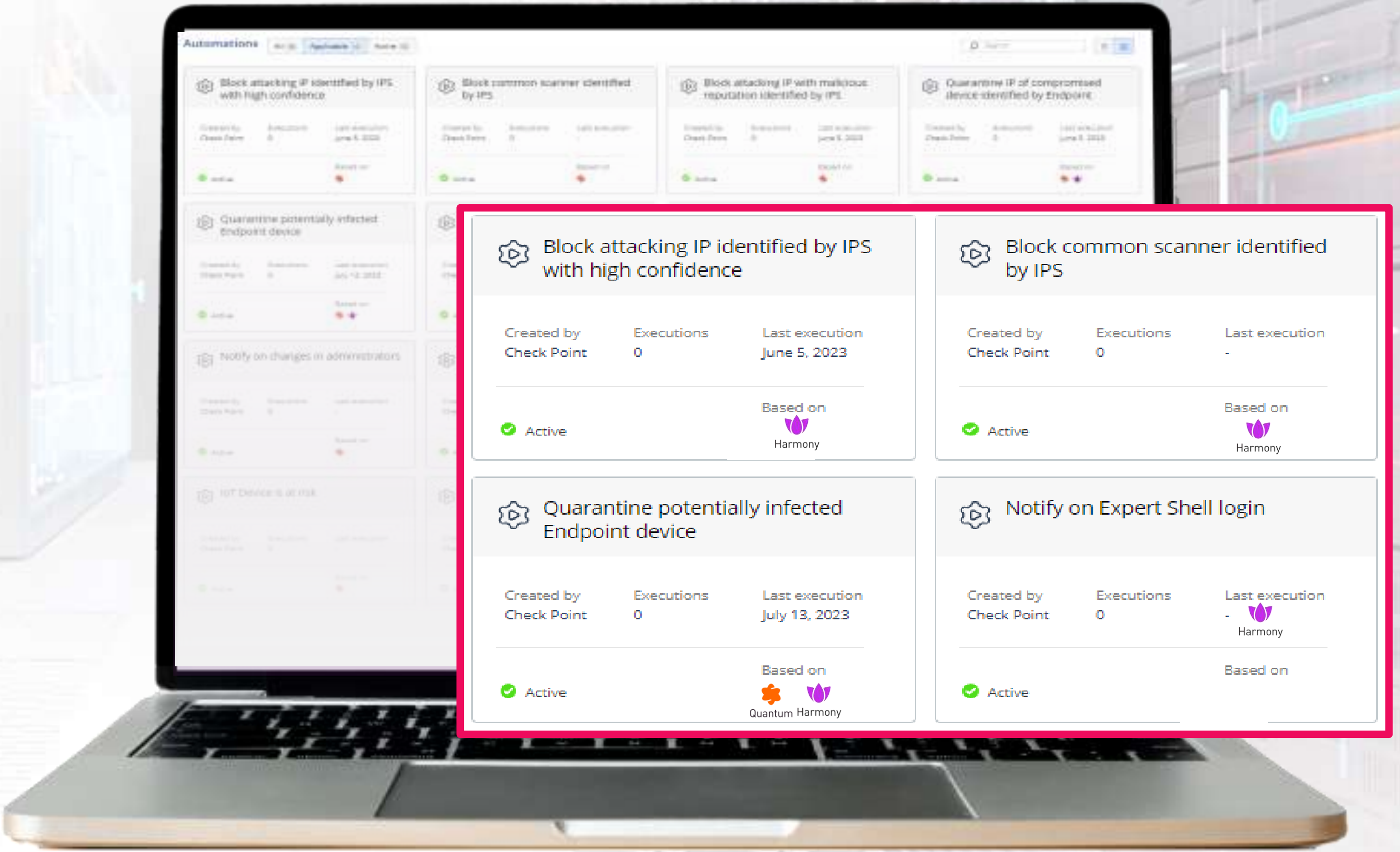
Revert the operation

Time	Produ...	Blade/Practice Type	Action	Source	Destination	Service Name
Jul 2, 2023 11:33:05 PM		Firewall	Block	[redacted]	[redacted]	microsoft-ds
Jul 2, 2023 11:32:59 PM		Firewall	Block	[redacted]	[redacted]	microsoft-ds
Jul 2, 2023 11:32:56 PM		Firewall	Block	[redacted]	[redacted]	microsoft-ds
Jul 2, 2023 11:32:52 PM		Firewall	Block	[redacted]	[redacted]	microsoft-ds
Jul 2, 2023 11:32:40 PM		Firewall	Block	[redacted]	[redacted]	http

Collaboration Powers the Best Prevention

- Any security product can trigger Playblocks to carry out automated preventative actions
- Collaboration between security products prevents attack from spreading across environment
- Automatic Check Point integration:

CloudGuard Harmony Quantum



Block attacking IP identified by IPS with high confidence
Created by Check Point
Executions 0
Last execution June 5, 2023
Active
Based on Harmony

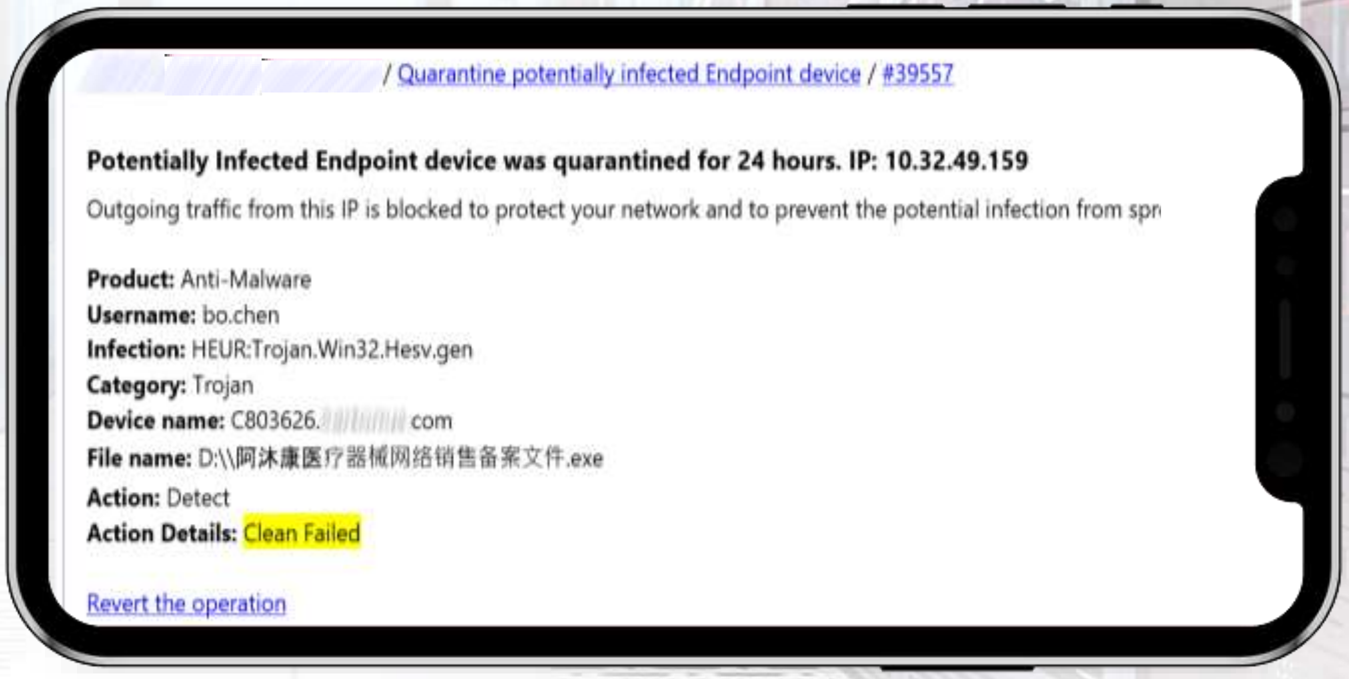
Block common scanner identified by IPS
Created by Check Point
Executions 0
Last execution -
Active
Based on Harmony

Quarantine potentially infected Endpoint device
Created by Check Point
Executions 0
Last execution July 13, 2023
Active
Based on Quantum Harmony

Notify on Expert Shell login
Created by Check Point
Executions 0
Last execution -
Harmony
Active
Based on

Collaboration Optimizes Operations

- Leverage existing IT workflows to keep your teams updated



[redacted] / Quarantine potentially infected Endpoint device / #39557

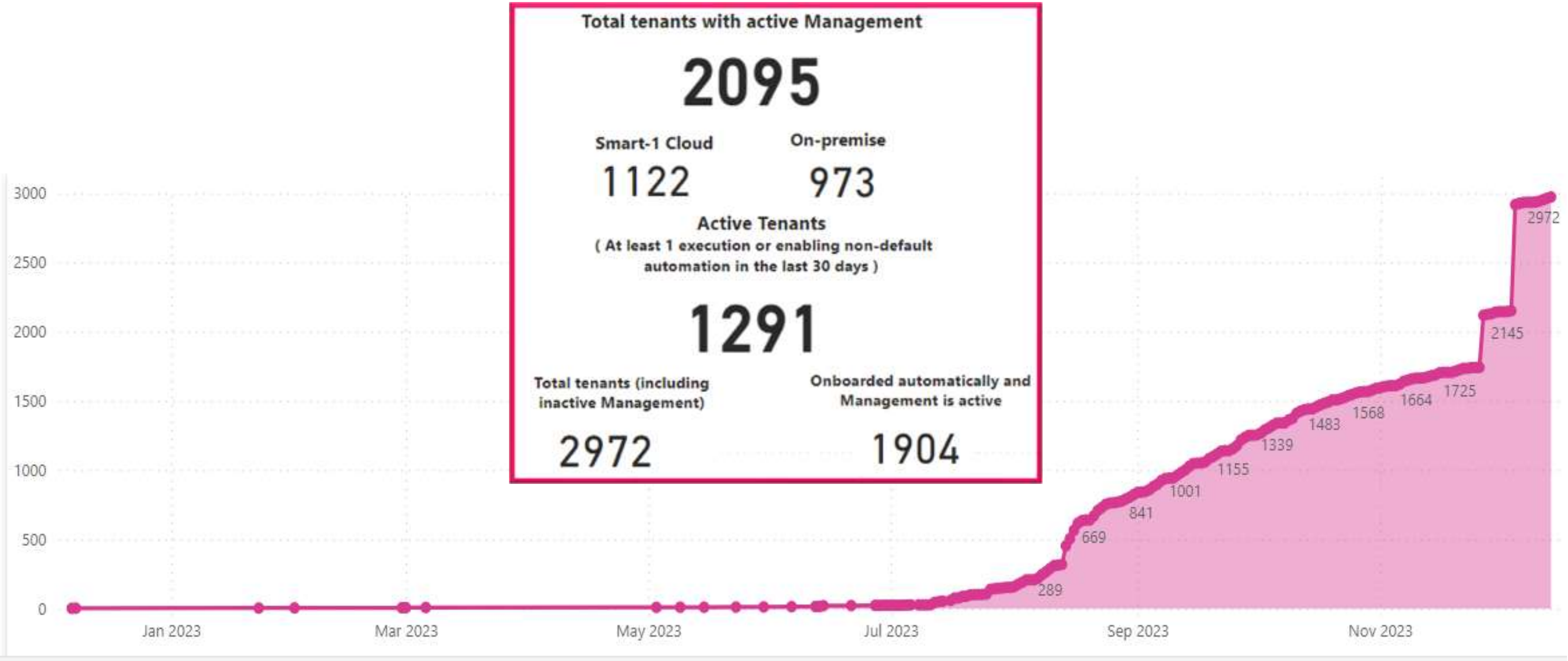
Potentially Infected Endpoint device was quarantined for 24 hours. IP: 10.32.49.159

Outgoing traffic from this IP is blocked to protect your network and to prevent the potential infection from spr

Product: Anti-Malware
Username: bo.chen
Infection: HEUR:Trojan.Win32.Hesv.gen
Category: Trojan
Device name: C803626.[redacted]com
File name: D:\\阿沐康医疗器械网络销售备案文件.exe
Action: Detect
Action Details: Clean Failed

Revert the operation

Thousands of Customers Already Enjoy Playblocks



Total tenants with active Management

2095

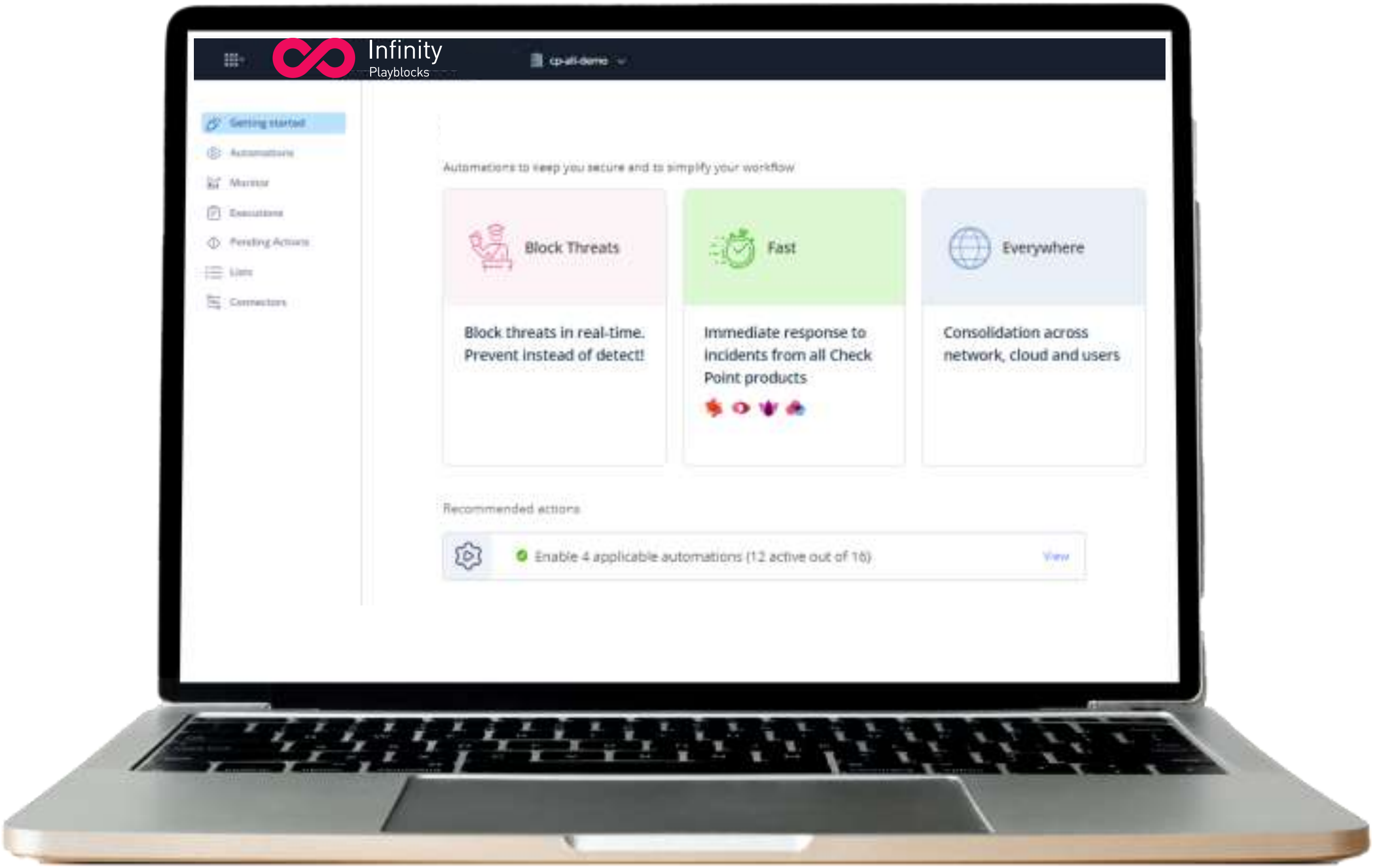
Smart-1 Cloud	On-premise
1122	973

Active Tenants
(At least 1 execution or enabling non-default automation in the last 30 days)

1291

Total tenants (including inactive Management)	Onboarded automatically and Management is active
2972	1904

Playblocks is Available Today



Infinity Playblocks

cp-all-demo

- Getting started
- Automations
- Monitor
- Executions
- Pending Actions
- Lists
- Connectors

Automations to keep you secure and to simplify your workflow

Block Threats

Block threats in real-time. Prevent instead of detect!

Fast

Immediate response to incidents from all Check Point products

Everywhere

Consolidation across network, cloud and users

Recommended actions

Enable 4 applicable automations (12 active out of 16) View

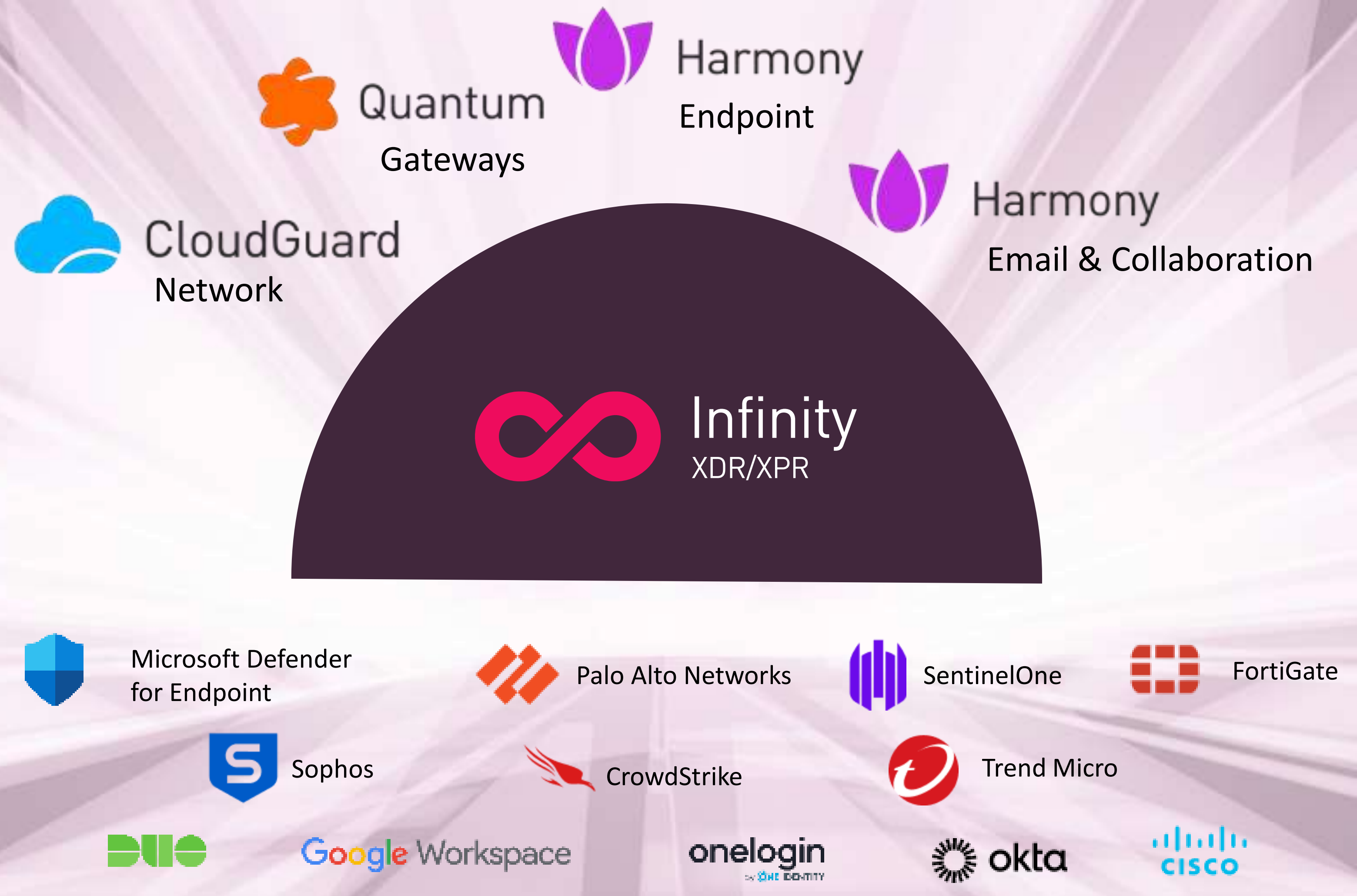
Infinity

Playblocks

- +50 out-of-the-box Playbooks
- 2-minute deployment
- Available as cloud service

20

New XDR/XPR Sources



Quantum

Gateways

Harmony

Endpoint

CloudGuard

Network

Harmony

Email & Collaboration

Infinity

XDR/XPR

Microsoft Defender for Endpoint

Palo Alto Networks

SentinelOne

FortiGate

Sophos

CrowdStrike

Trend Micro

DUO

Google Workspace

onelogin

okta

cisco

CHECK POINT™

Thank You!

YOU DESERVE THE BEST SECURITY