CHECK POINT™

2024 MITRE ATT&CK ® Evaluations

YOU DESERVE THE BEST SECURITY

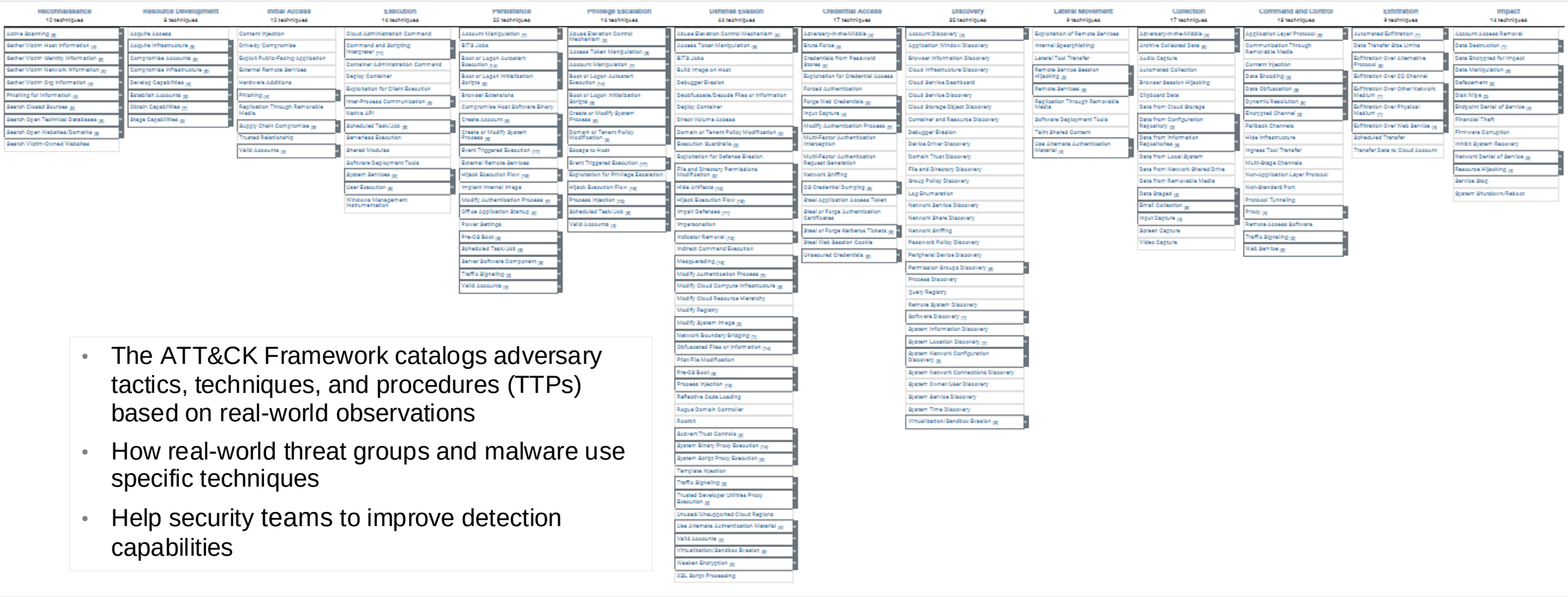
Agenda

- 2024 ATT&CK® Evaluations Insights
- Results and competitive analysis
- How Check Point achieved excellent detection
- Demo
- Q&A

01

MITRE ATT&CK ® Evaluations

The MITRE ATT&CK ® Matrix



- The ATT&CK Framework catalogs adversary tactics, techniques, and procedures (TTPs) based on real-world observations
- How real-world threat groups and malware use specific techniques
- Help security teams to improve detection capabilities

The MITRE ATT&CK ® Evaluations

- Independent assessments of cybersecurity products against known threat group behaviors
- ATT&CK Evals don't score or rank products
- Each evaluation round focuses on emulating specific threat groups
- Help cyber security companies understand how their security tools perform against real-world attack techniques
- Help organizations’ security teams make informed decisions about security products

2024 MITRE ATT&CK ® Evaluations

- CL0P and LockBit attacks
- Emulated 59 sub-steps
- 19 participants
- Windows and Linux, with detection and prevention runs
- Detection and prevention test
- False Positives

- Check Point Debuts Infinity XDR/XPR

CL0P and LockBit emulations

CL0P

Russian ransomware-as-a-service group

Primary Targets: Financial, healthcare, manufacturing, and media industries

Impact: Exploited zero-day vulnerabilities in MOVEit Transfer, impacting US government

Methodology: Involves encrypting files using AES-256 encryption, demanding ransom, and threatening to leak data

LockBit

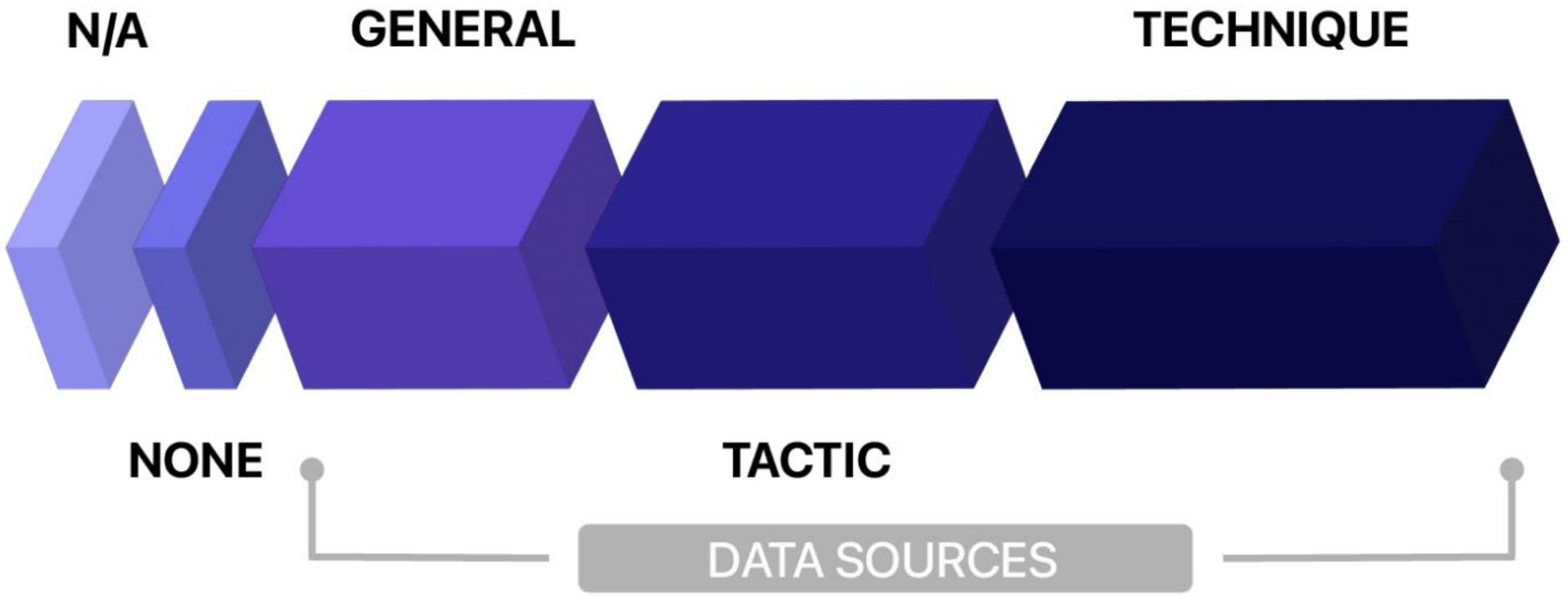
considered the world's most active ransomware group

Primary Targets: Critical infrastructure and government

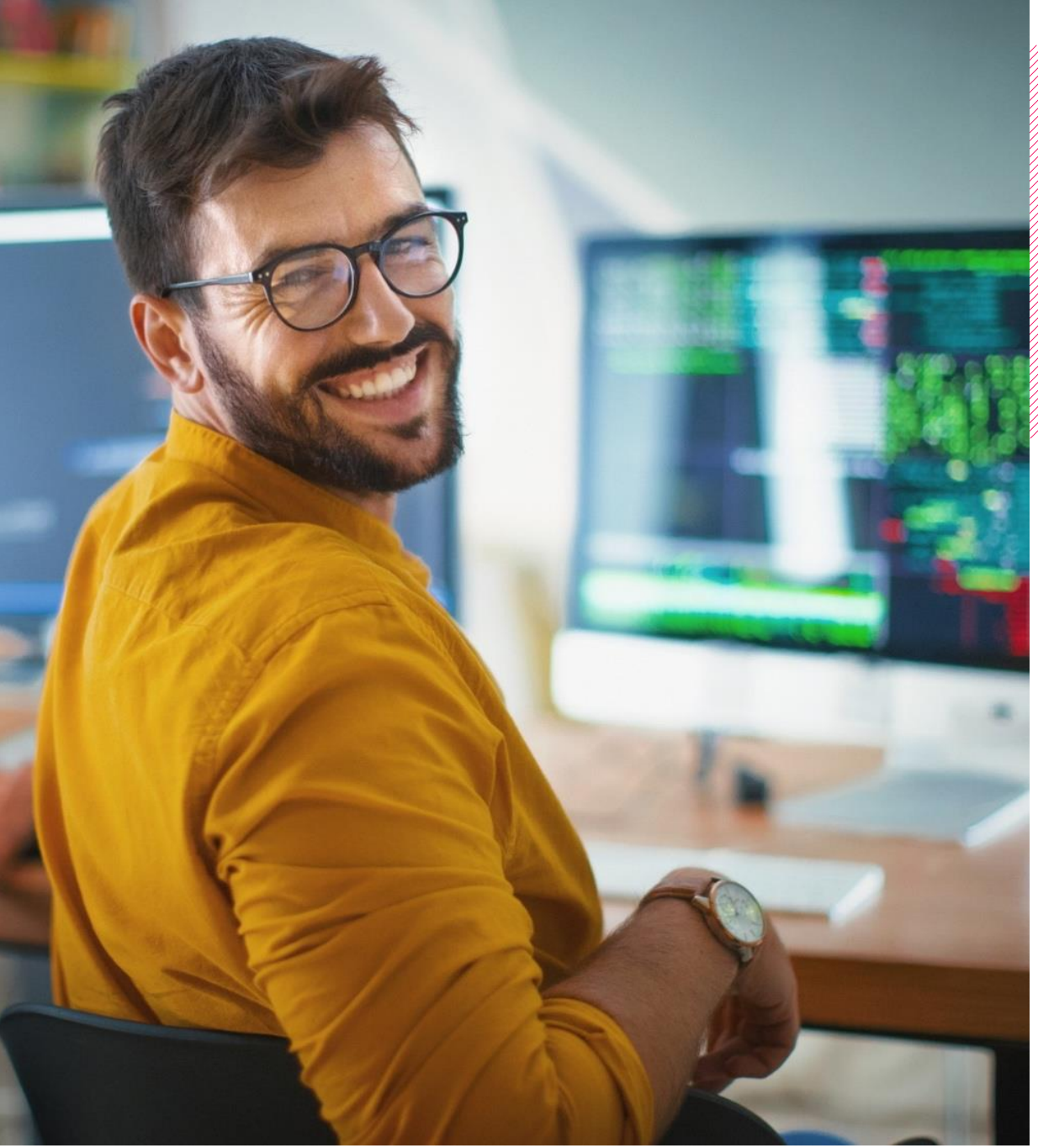
Impact:

Methodology: Initial access through phishing emails, exploiting software vulnerabilities, or using stolen credentials

How to read MITRE results



https://attackevals.mitre-engenuity.org/enterprise/er6/detection-categories



How did we do?

100% Detection

Over

98% Technique level

02

COMPETITIVE ANALYSIS

MITRE RESULTS – Competitive Comparison

CHECK POINT™

100%

Harmony has achieved a 100% detection rate

98.2% of these detections are Technique level detection (the highest level of detection)

TOP 6

paloalto NETWORKS

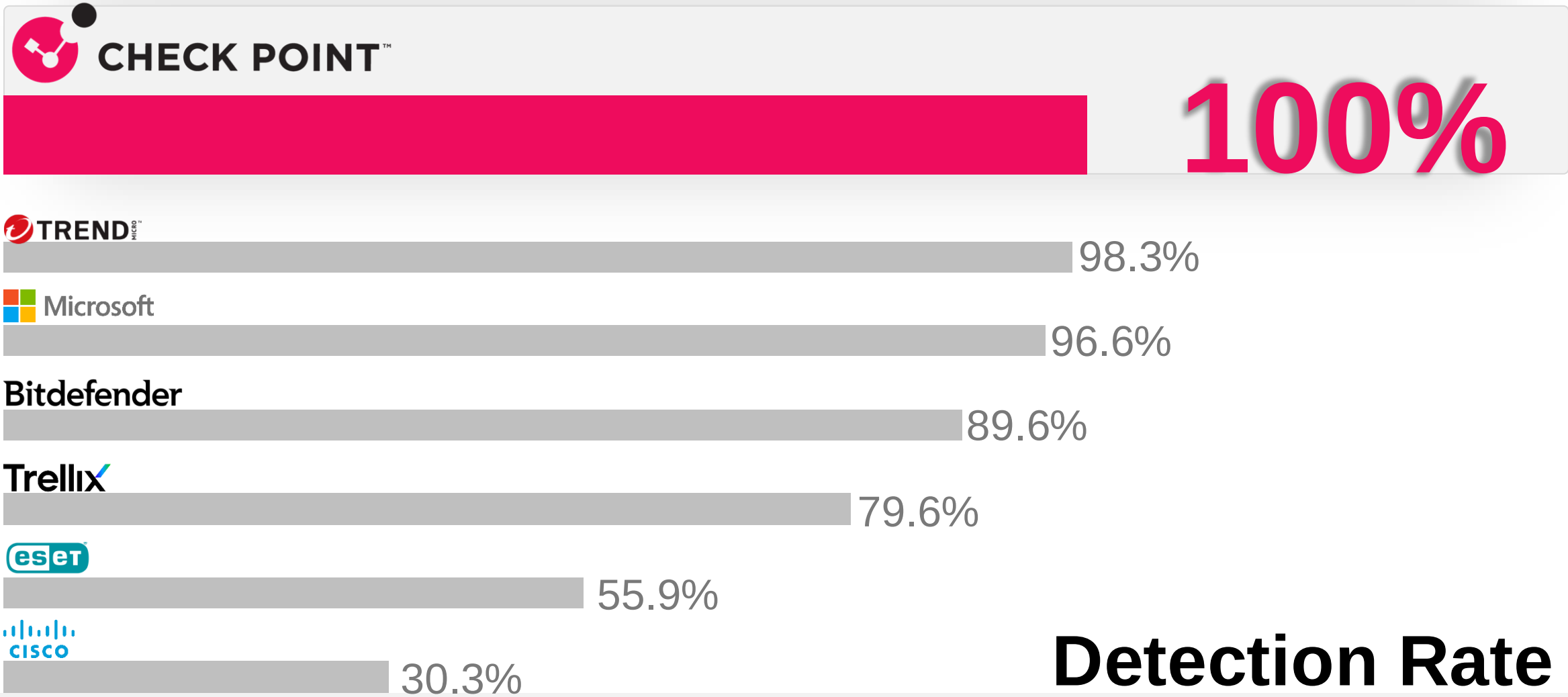
SentinelOne

cybereason

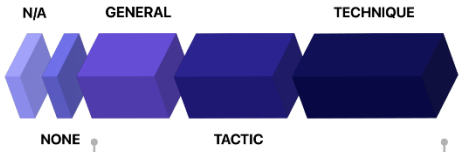
SOPHOS

cynet

MITRE RESULTS – Competitive Comparison

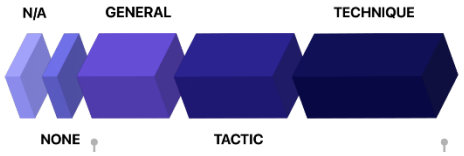


MITRE RESULTS – Detection Comparison



CHECK POINT™	**100%**
Palo Alto	100%
SentinelOne	100%
Sophos	100%
Cybereason	100%
Cynet	100%
Trend Micro	98.3%
Microsoft	96.6%
Bitdefender	89.6%
Malwarebytes	84.7%
WatchGuard	82.4%
Trellix	79.6%
WithSecure	74.5%
ESET	55.9%
Cisco	30.3%

MITRE RESULTS – Technique Detection



Palo Alto	100%
SentinelOne	100%
Sophos	100%
Cybereason	100%
Cynet	100%
CHECK POINT	**98.2%**
Trend Micro	96.6%
Microsoft	93.2%
Bitdefender	84.4%
Malwarebytes	71.1%
Trellix	66.1%
WatchGuard	57.8%
WithSecure	55.9%
ESET	45.7%
Cisco	19.6%

03

How Check Point achieved excellent detection

How Check Point achieved excellent detection

* The report uses the term ‘Insight’ instead of Events. Insight is an aggregation of events that indicates the same activity

XDR for Endpoint – Block all Entry Points

Incident Management
Research Intelligence

Threat Hunting
Automated Remediation
Forensic Report
MITRE Mapping
Full Attack Tree

Threat Cloud
IOC Management

Anti-Ransomware
Behavioral Guard
Intel TDT
Anti-Bot
Anti-Malware
Anti-Exploit

Full Disk Encryption
Media Encryption
Port Protection

Remote Access VPN
Firewall
Application Control
Endpoint Compliance

Threat Emulation
Threat Extraction

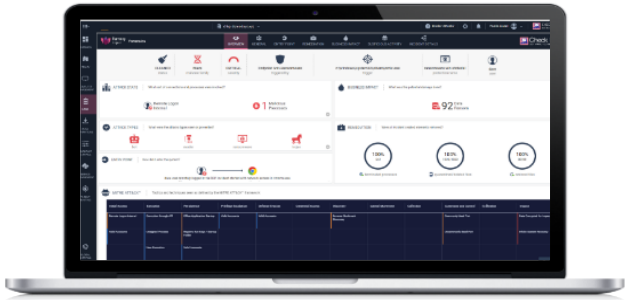
Zero-day Phishing
DLP (Data Loss Prevention)
GenAI Security
URL Filtering
Corporate Password Reuse
Safe Search

Vulnerability Management
Patch Management
Risk Prioritization

HEP Client detects and remediate → HEP sends events & alerts → XDR processes events & alerts → XDR create incidents

Blocks All Entry Points

Best In Class Detection & Response

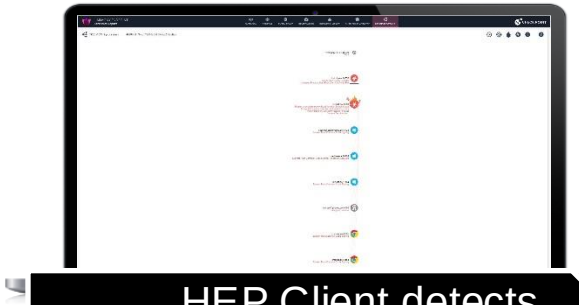


AUTOMATIC REMEDIATION

Automatically Resolves Detected Threats
by applying Corrective Actions,
Minimizing Manual Intervention and Response Time

THREAT HUNTING

Proactively Searches for Signs of Potential Threats
or Malicious Activities within the Environment
Before they result in a Security Breach



FORENSICS REPORT

Detailed Insights into Security Incidents,
Attack Flow, Attack Tree, and Affected Assets
for Deeper Investigation, all Aligned with
MITRE ATT&CK Framework.

Harmony
Endpoint

HEP Client detects and remediate → HEP sends events & alerts → XDR processes events & alerts → XDR create incidents

Collaborative detection and response

Detection based on **Endpoint Events**

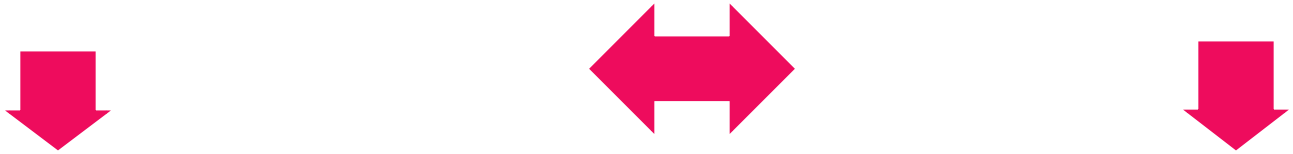
Endpoint Behavior Based, AI
e.g, remote code execution, process activities

Endpoint Alerts

Detection based on **Network Events**

Network Behavior Based, AI
e.g, suspicious connections patterns

Gateway Threat Prevention blades
e.g, Anti Malware, Anti Bot, DNS Security



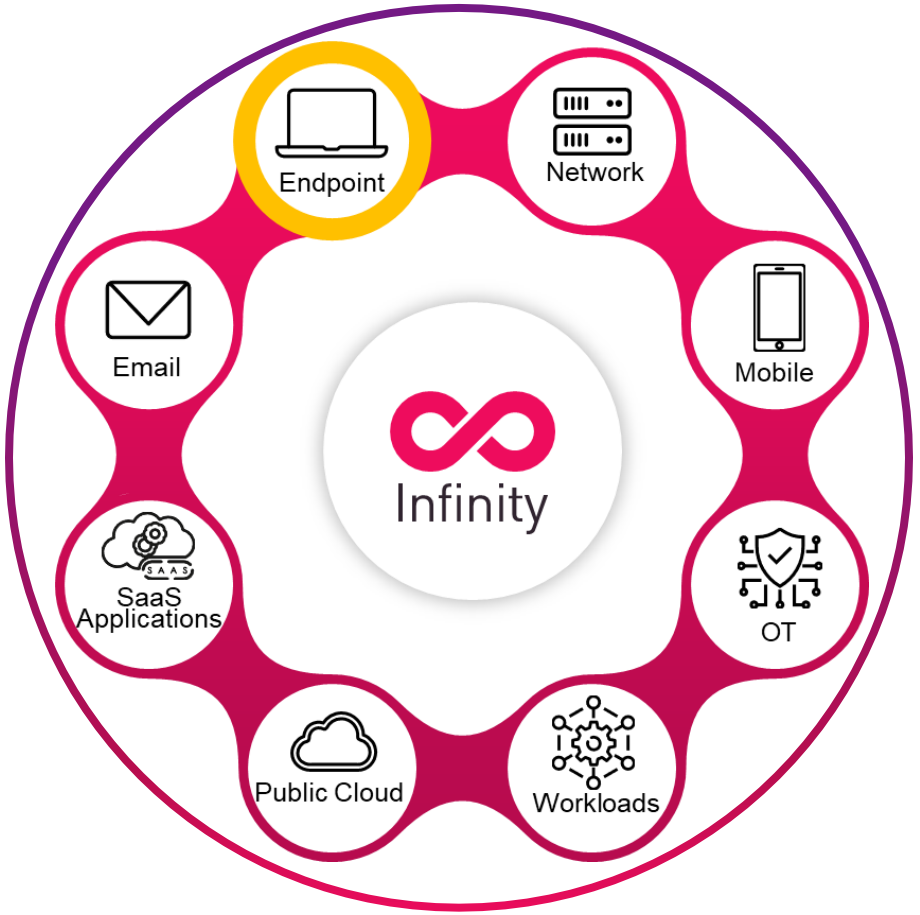
PREVENT further threat across Gateways, Endpoints, Email, Mobile, and more

HEP Client detects and remediate → HEP sends events & alerts → XDR processes events & alerts → XDR create incidents

Collaborative Threat-Prevention
ENDPOINT SECURITY USE CASES

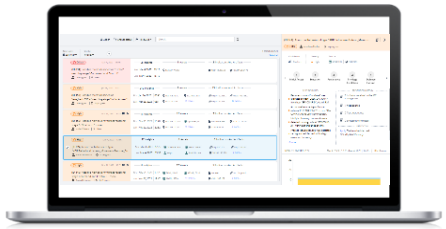
1. Prevent successful attacks attempts by extending knowledge and controls FROM ONE ENFORCEMENT POINT into the ENTIRE NETWORK

2. Detect and contain threats from spreading by correlating information and COORDINATING RESPONSE across MULTIPLE PRODUCTS



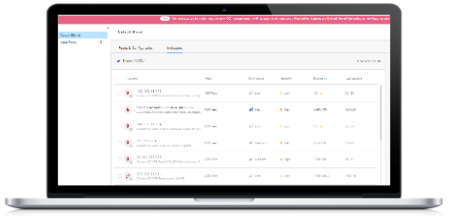
HEP Client detects and remediate → HEP sends events & alerts → XDR processes events & alerts → XDR create incidents

The Benefits Of a Consolidated Approach
Infinity XDR



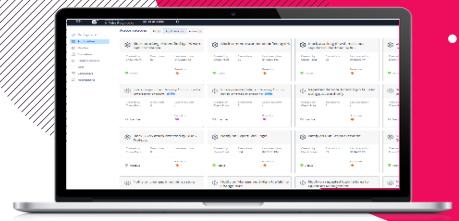
INCIDENT MANAGEMENT

Identify and drill down into Suspicious Incidents, and take Remediation Actions



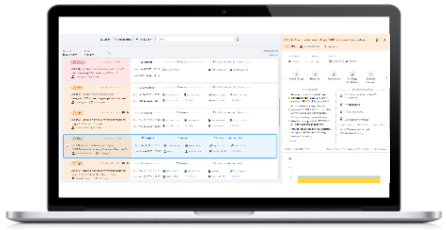
IOC MANAGEMENT

Powered by Multiple Feeds allowing Extensive & Consolidated IOC Management



SECURITY PLAYBOOKS

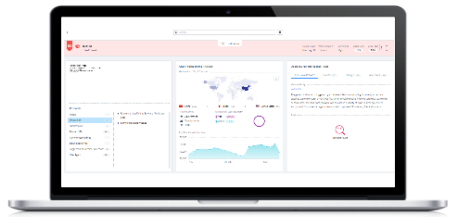
Create Automated Playbooks to manage Security Events and assist with Security Operations in Real-Time



CORRELATION INTO ONE INCIDENT

Based on AI technology including Network Modeling and Context-based Anomaly Detection using ML and Data Enrichment

Infinity
XDR/XPR



RESEARCH INTELLIGENCE

Allows you to search any Indicator with both Check Point's Internal and External Resources

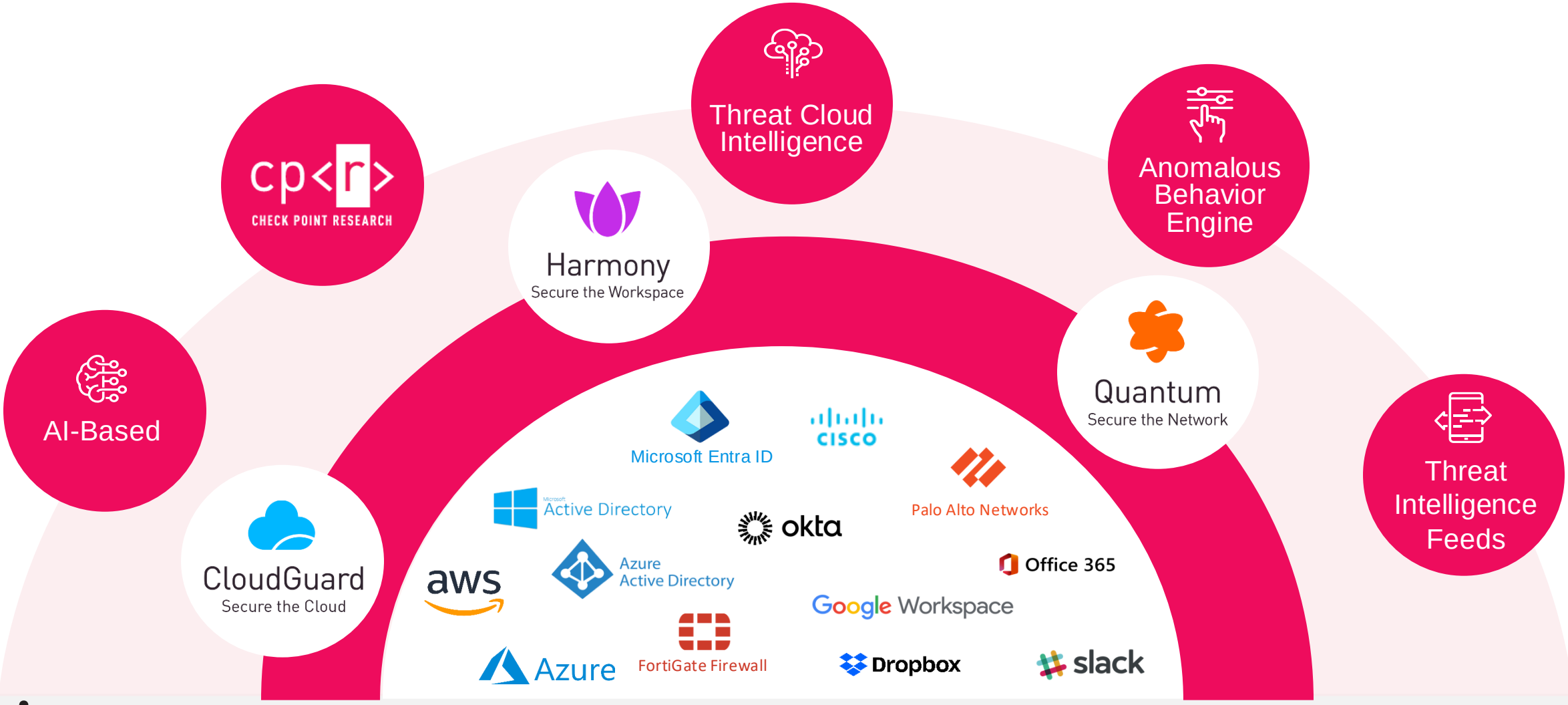
HEP Client detects and remediate → HEP sends events & alerts → XDR processes events & alerts → XDR create incidents

Infinity XDR/XPR

Automatically prevent attacks from spreading through intelligent AI correlation

Comprehensive Threat Prevention

Powered by AI and Threat intelligence, XDR/XPR triggers automatic attack prevention across the entire security estate

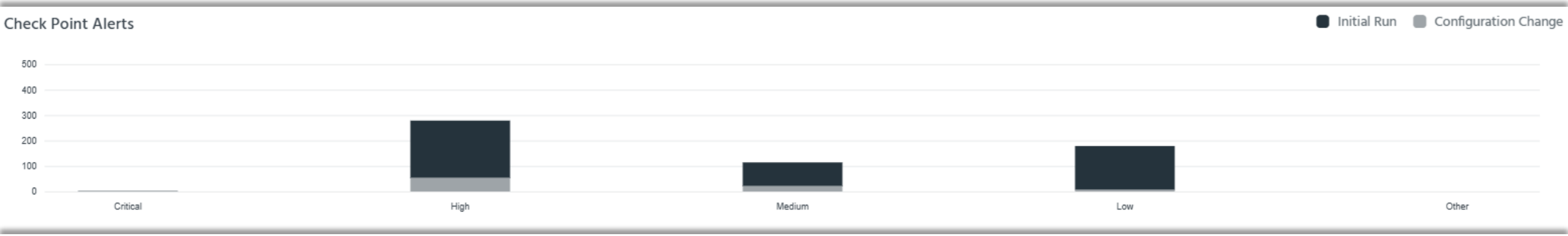


04

FAQ

FAQ

- **Why do we have a high false positive rate?**
- **Why do we have high Noise results?**



Noise

Benign activity (outside the emulation plan) was executed during the evaluation while malicious/suspicious activity was executed by the Red Team.

Noise steps received the following results:

False Positive: occurs when a participant identifies false noise or benign activity as adversary activity

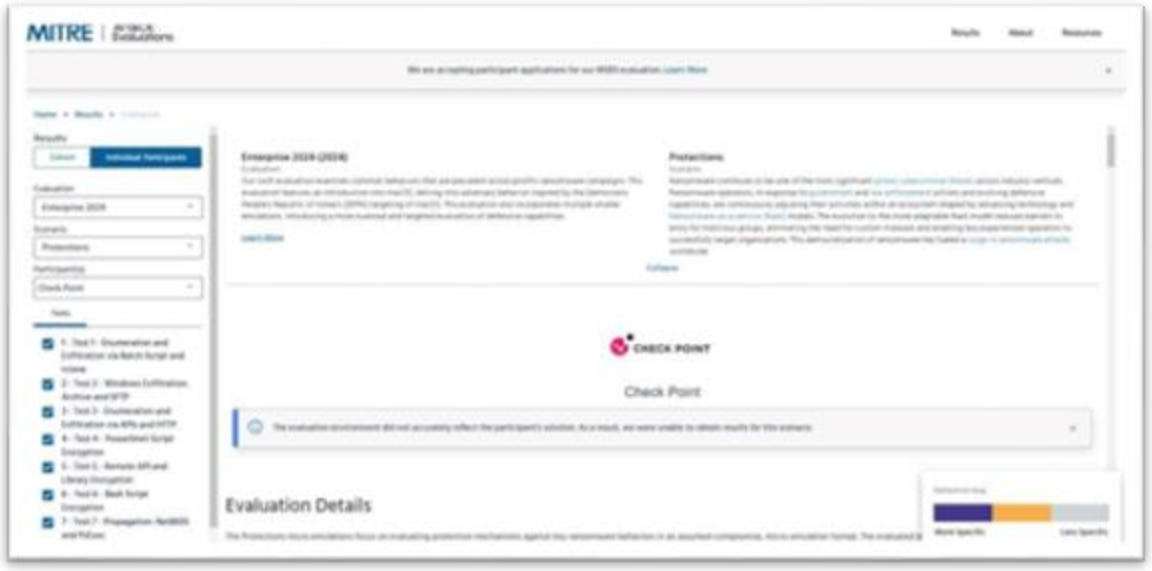
True Negative: occurs when a participant identifies false noise or benign activity as non-malicious activity

Alerts must have met the General detection criteria, at a minimum, to be considered for this metric.

*No training data or learning period was provided.

FAQ

- **Where are our Protection results?**



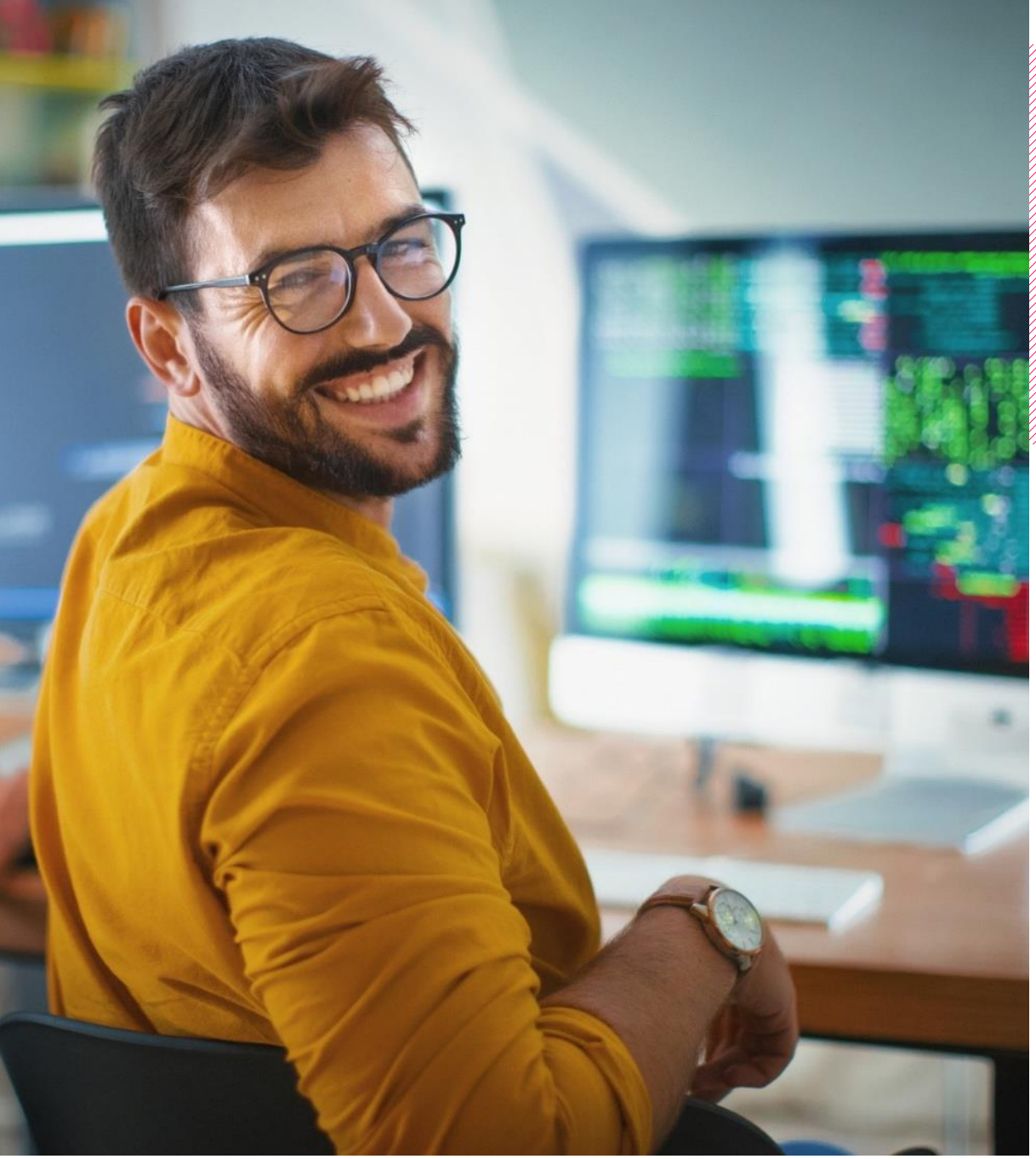
CHECK POINT

Check Point

The evaluation environment did not accurately reflect the participant's solution. As a result, we were unable to obtain results for this scenario.

FAQ

- Which Endpoint versions has been used?
  - Windows version: 88.60.
  - Linux version: 1.18.12

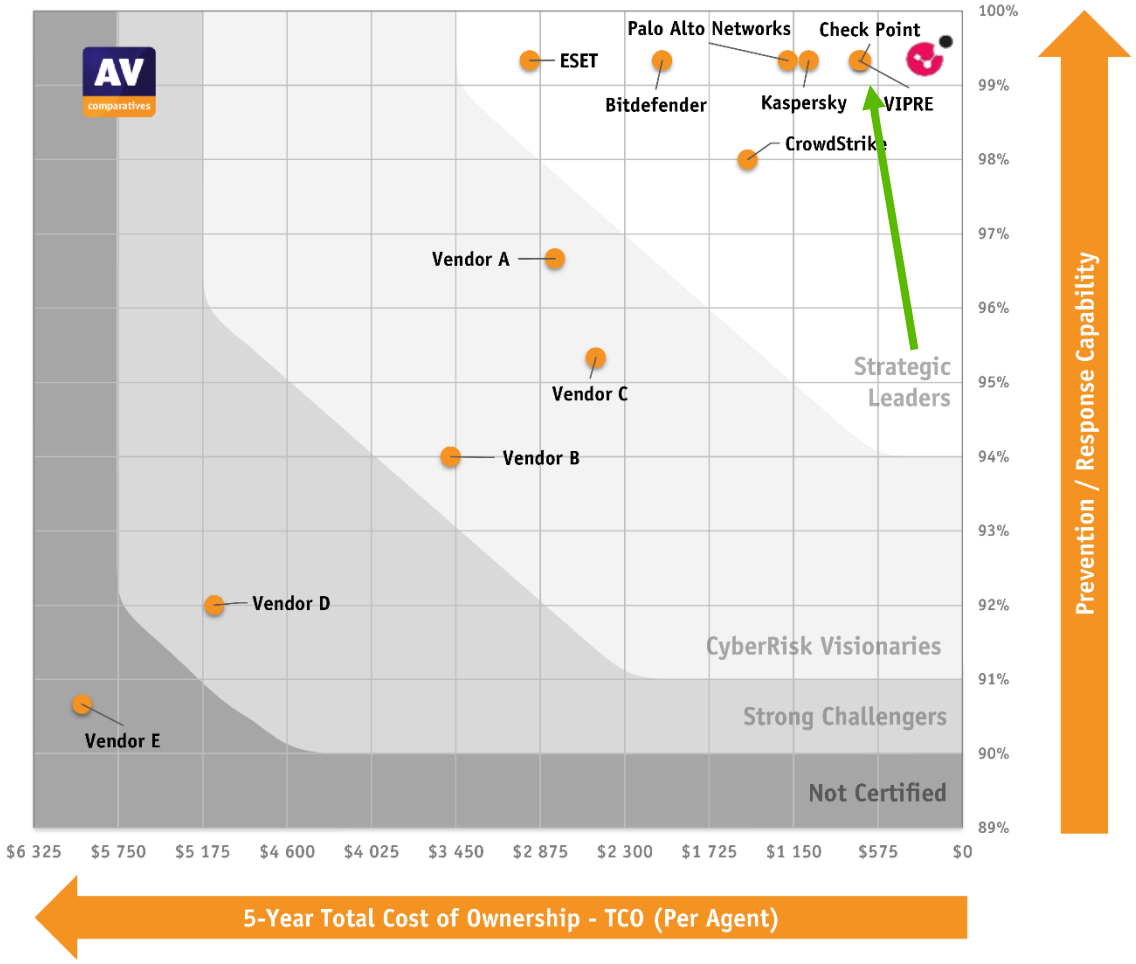


How did we do?

100% Detection

98% Technique level

Check Point named *Strategic Leader* in AV-Comparatives 2024 EPR Test, *scoring the 1st place above all vendors!*



Strategic Leaders

- Leaders in Prevention
- Leader in TCO

50/50 Prevented Scenarios

- 100% Active response (Prevention)
- 100% Passive response (Detection)

Real Time Response

- Zero Workflow Delays
- Low Operational Accuracy Costs (False Positives)

AV comparatives Certified EPR 2024

Report Links

Check Point's report

Full report

CHECK POINT

A Leading Endpoint Solution

Leader

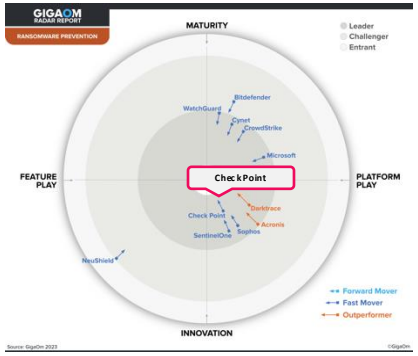
Frost Radar™ XDR Growth and Innovation Leader in 2024

FROST & SULLIVAN

"Check Point Software's Infinity XDR/XPR addresses the most important challenges in the market with advanced technology capabilities focused on prevention, earning its place as one of the innovation leaders"

Leader & Fast Mover

GigaOm Radar for Ransomware Prevention report, 2023

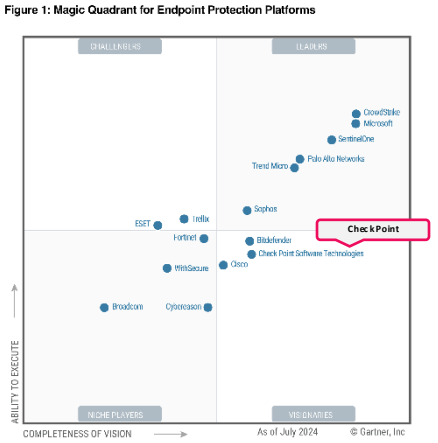


GIGAOM

"Broad coverage ensures that the solution will be able to prevent ransomware across a wide range of threat vectors, covering most organizational use cases. Its single administration interface helps simplify management and operational efficiency"

A Visionary

2024 Magic Quadrant™ for Endpoint Protection Platforms



Gartner

What's next?

Learn

Check Point's

Landing Page

MITRE

Full Results

Share

PR

Blog

LinkedIn

Webinar – EMEA

Webinar - Americas

CHECK POINT™

Thank You!

YOU DESERVE THE BEST SECURITY