



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

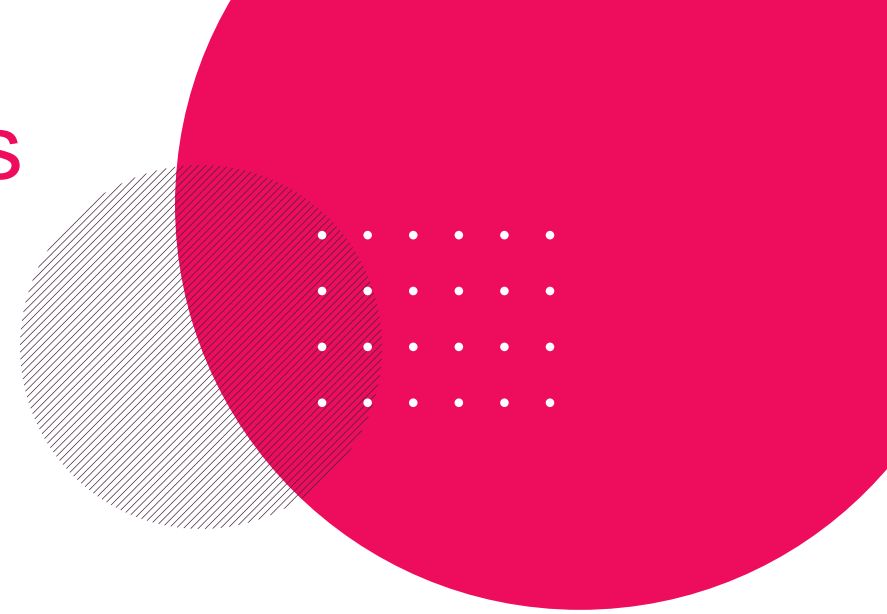


Reconnaissance 10 techniques	Resource Development 6 techniques	Initial Access 10 techniques	Execution 14 techniques	Persistence 20 techniques	Privilege Escalation 14 techniques	Defense Evasion 44 techniques	Credential Access 17 techniques	Discovery 22 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning (2)	Acquire Access (2)	Consent Injection	Cloud Administration Command	Account Manipulation (2)	Abuse Elevation Control Mechanism (2)	Abuse Elevation Control Mechanism (2)	Adversary-In-the-Middle (2)	Account Discovery (2)	Exploitation of Remote Service	Adversary-In-the-Middle (2)	Application Layer Protocol (2)	Automated Exfiltration (1)	Account Access Removal
Search Victim Host Information (2)	Acquire Infrastructure (2)	Drive-by Compromise	Command and Scripting Interact (1)	API Jobs	Abuse Token Manipulation (2)	Abuse Token Manipulation (2)	BitLocker (2)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (2)
Search Victim Identity Information (2)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Assistant Execution (2)	BitLocker Jobs	BitLocker Jobs	Credentialsteal from Password Stores (2)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Consent Injection	Exfiltration Over Alternative Protocol (2)	Data Encrypted for Impact
Search Victim Network Information (2)	Compromise Infrastructure (2)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (2)	Build Image on Host	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (2)	Exfiltration Over OS Channel	Data Manipulation (2)
Search Victim Org Information (2)	Develop Capabilities (2)	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Debugger Execution	Debugger Execution	Forced Authentication	Cloud Service Dashboard	Remote Service (2)	Browser Session Hijacking	Data Obfuscation (2)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (2)	Establish Accounts (2)	Phishing (2)	Inter-Process Communication (2)	Compromise Host Software Binary	Deobfuscate/Decode Files or Information	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Registration Through Removable Media	Clipboard Data	Dynamic Resolution (2)	Exfiltration Over Physical Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (1)	Replication Through Removable Media	Native API	Create or Modify System Process (2)	Domain or Tenant Policy Modification (2)	Domain or Tenant Policy Modification (2)	Input Capture (2)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel (2)	Exfiltration Over Web Service (2)	Endpoint Denial of Service (2)
Search Open Technical Databases (2)	Stage Capabilities (2)	Supply Chain Compromise (2)	Scheduled Task/Job (2)	Create Account (2)	Escape to Host	Escape to Host	Modify Authentication Process (2)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Fallback Channels	Scheduled Transfer	Financial Theft
Search Open Websites/Domains (2)		Trusted Relationship	Services Execution	Domain or Tenant Policy Modification (2)	Event Triggered Execution (1)	Event Triggered Execution (1)	Multi-Factor Authentication Interception	Debugger Execution	Use Alternate Authentication Material (2)	Data from Information Repositories (2)	Hide Infrastructure		Firmware Corruption
Search Victim-Owned Websites		Valid Accounts (2)	Shared Modules	Domain or Tenant Policy Modification (2)	Event Triggered Execution (1)	Event Triggered Execution (1)	Request Generation	Device Driver Discovery		Data from Local System	Ingress Tool Transfer		Inhibit System Recovery
			Software Deployment Tools	External Remote Services	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Multi-Stage Channels		Network Denial of Service (2)
			System Services (2)	Hijack Execution Flow (2)	Hijack Execution Flow (2)	Hijack Execution Flow (2)	OS Credential Dumping (2)	File and Directory Discovery		Data from Removable Media	Non-Application Layer Protocol		Resource Hijacking (2)
			User Execution (2)	Impair Defenses (1)	Impair Defenses (1)	Impair Defenses (1)	OS Credential Dumping (2)	File and Directory Permissions Modification (2)		Data Staged (2)	Non-Standard Port		Service Stop
			Windows Management Instrumentation	Impersonation	Impersonation	Impersonation	OS Credential Dumping (2)	File and Directory Discovery		Small Collection (2)	Protocol Tunneling		System Shutdown/Reboot
				Indirect Command Execution	Indirect Command Execution	Indirect Command Execution	OS Credential Dumping (2)	Group Policy Discovery		Input Capture (2)	Proxy (2)		
				Inhibit Command Execution	Inhibit Command Execution	Inhibit Command Execution	OS Credential Dumping (2)	Log Enumeration		Screen Capture	Remote Access Software		
				Malware Service (2)	Malware Service (2)	Malware Service (2)	OS Credential Dumping (2)	Network Service Discovery		Video Capture	Traffic Signaling (2)		
				Modify Authentication Process (2)	Modify Authentication Process (2)	Modify Authentication Process (2)	OS Credential Dumping (2)	Network Share Discovery			Web Service (2)		
				Modify Cloud Compute Infrastructure (2)	Modify Cloud Compute Infrastructure (2)	Modify Cloud Compute Infrastructure (2)	OS Credential Dumping (2)	Peripheral Device Discovery					
				Modify Cloud Resource Hierarchy	Modify Cloud Resource Hierarchy	Modify Cloud Resource Hierarchy	OS Credential Dumping (2)	Permission Group Discovery (2)					
				Modify Registry	Modify Registry	Modify Registry	OS Credential Dumping (2)	Process Discovery					
				Modify System Image (2)	Modify System Image (2)	Modify System Image (2)	OS Credential Dumping (2)	Query Registry					
				Network Boundary Widening (2)	Network Boundary Widening (2)	Network Boundary Widening (2)	OS Credential Dumping (2)	Remote System Discovery					
				Obfuscated Files or Information (2)	Obfuscated Files or Information (2)	Obfuscated Files or Information (2)	OS Credential Dumping (2)	Software Discovery (1)					
				Plist File Modification	Plist File Modification	Plist File Modification	OS Credential Dumping (2)	System Information Discovery					
				Pre-OS Boot (2)	Pre-OS Boot (2)	Pre-OS Boot (2)	OS Credential Dumping (2)	System Location Discovery (1)					
				Process Injection (2)	Process Injection (2)	Process Injection (2)	OS Credential Dumping (2)	System Network Configuration Discovery (2)					
				Reflective Code Loading	Reflective Code Loading	Reflective Code Loading	OS Credential Dumping (2)	System Network Connections Discovery					
				Rogue Domain Controller	Rogue Domain Controller	Rogue Domain Controller	OS Credential Dumping (2)	System Owner/User Discovery					
				Rootkit	Rootkit	Rootkit	OS Credential Dumping (2)	System Service Discovery					
				Subvert Trust Controls (2)	Subvert Trust Controls (2)	Subvert Trust Controls (2)	OS Credential Dumping (2)	System Time Discovery					
				System Binary Proxy Execution (2)	System Binary Proxy Execution (2)	System Binary Proxy Execution (2)	OS Credential Dumping (2)	Virtualization/Sandbox Evasion (2)					
				System Script Proxy Execution (2)	System Script Proxy Execution (2)	System Script Proxy Execution (2)	OS Credential Dumping (2)	Weaken Encryption (2)					
				Template Injection	Template Injection	Template Injection	OS Credential Dumping (2)	XML Script Processing					
				Traffic Signaling (2)	Traffic Signaling (2)	Traffic Signaling (2)	OS Credential Dumping (2)						
				Trusted Developer Utilities Proxy Execution (2)	Trusted Developer Utilities Proxy Execution (2)	Trusted Developer Utilities Proxy Execution (2)	OS Credential Dumping (2)						
				Unusual/Unapproved Cloud Regions	Unusual/Unapproved Cloud Regions	Unusual/Unapproved Cloud Regions	OS Credential Dumping (2)						
				Use Alternate Authentication Material (2)	Use Alternate Authentication Material (2)	Use Alternate Authentication Material (2)	OS Credential Dumping (2)						
				Valid Accounts (2)	Valid Accounts (2)	Valid Accounts (2)	OS Credential Dumping (2)						
				Virtualization/Sandbox Evasion (2)	Virtualization/Sandbox Evasion (2)	Virtualization/Sandbox Evasion (2)	OS Credential Dumping (2)						
				Weaken Encryption (2)	Weaken Encryption (2)	Weaken Encryption (2)	OS Credential Dumping (2)						
				XML Script Processing	XML Script Processing	XML Script Processing	OS Credential Dumping (2)						

- 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

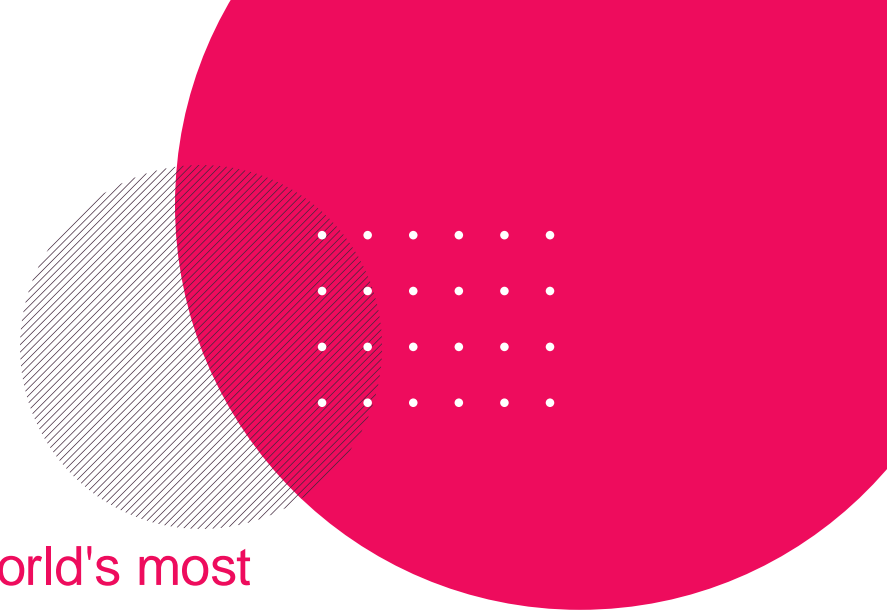
LockBit

considered the world's most active ransomware group

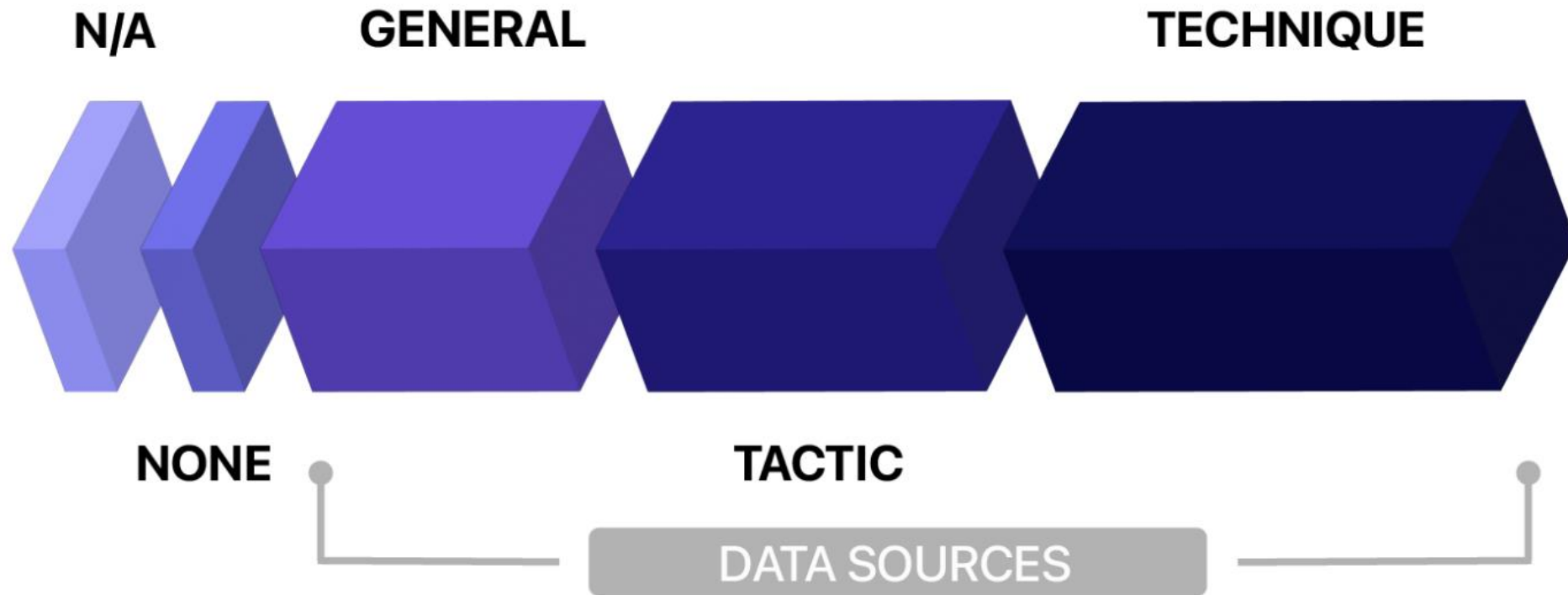
Primary Targets: Critical infrastructure and government

Impact:

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



How to read MITRE results



<https://attacker.vals.mitre-engenuity.org/enterprise/er6/detection-categories>



How did we do?

100% Detection

Over

98% Technique
level

02

COMPETITIVE ANALYSIS

MITRE RESULTS – Competitive Comparison



100%

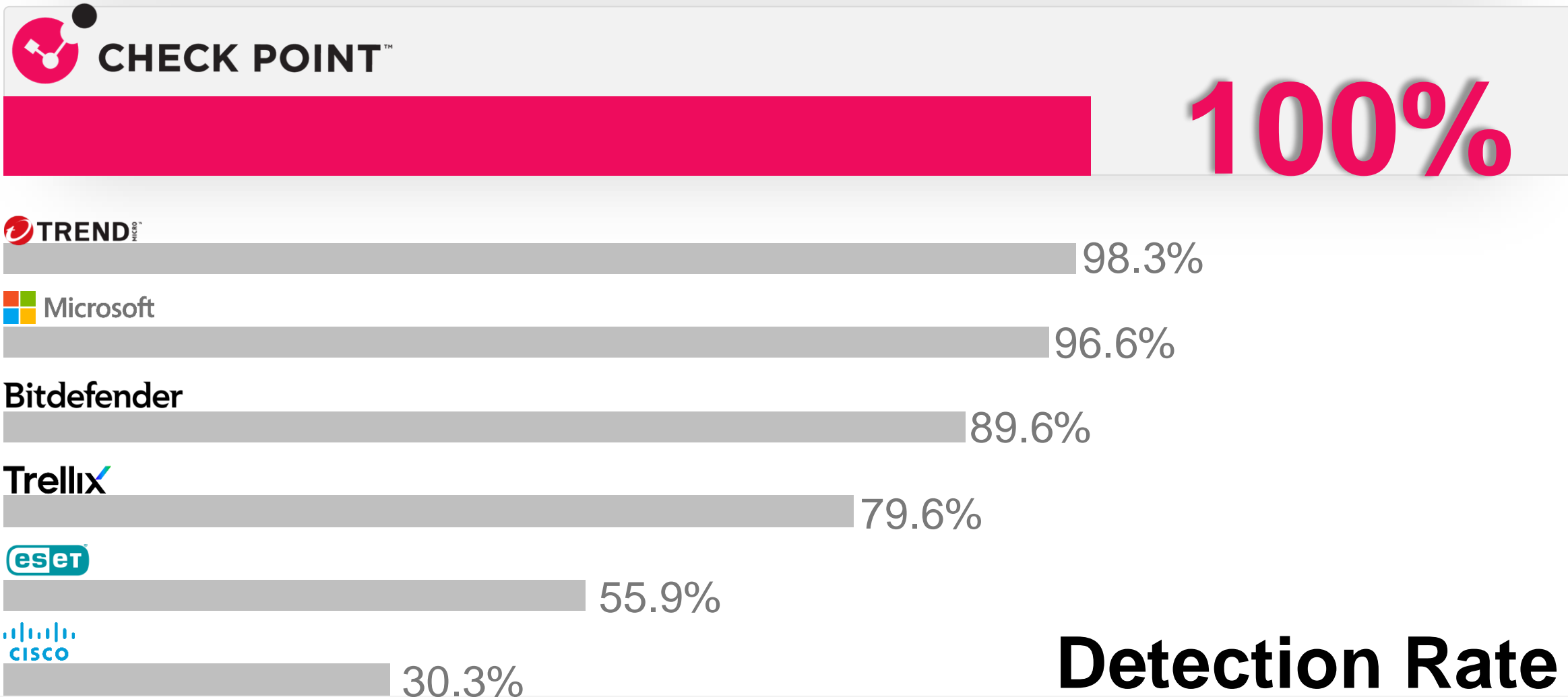
Harmony has achieved a 100% detection rate

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

TOP 6

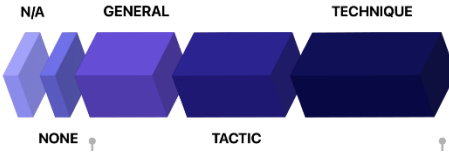



MITRE RESULTS – Competitive Comparison



Detection Rate

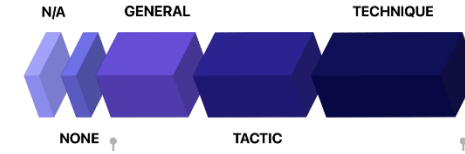
MITRE RESULTS – Detection Comparison




 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

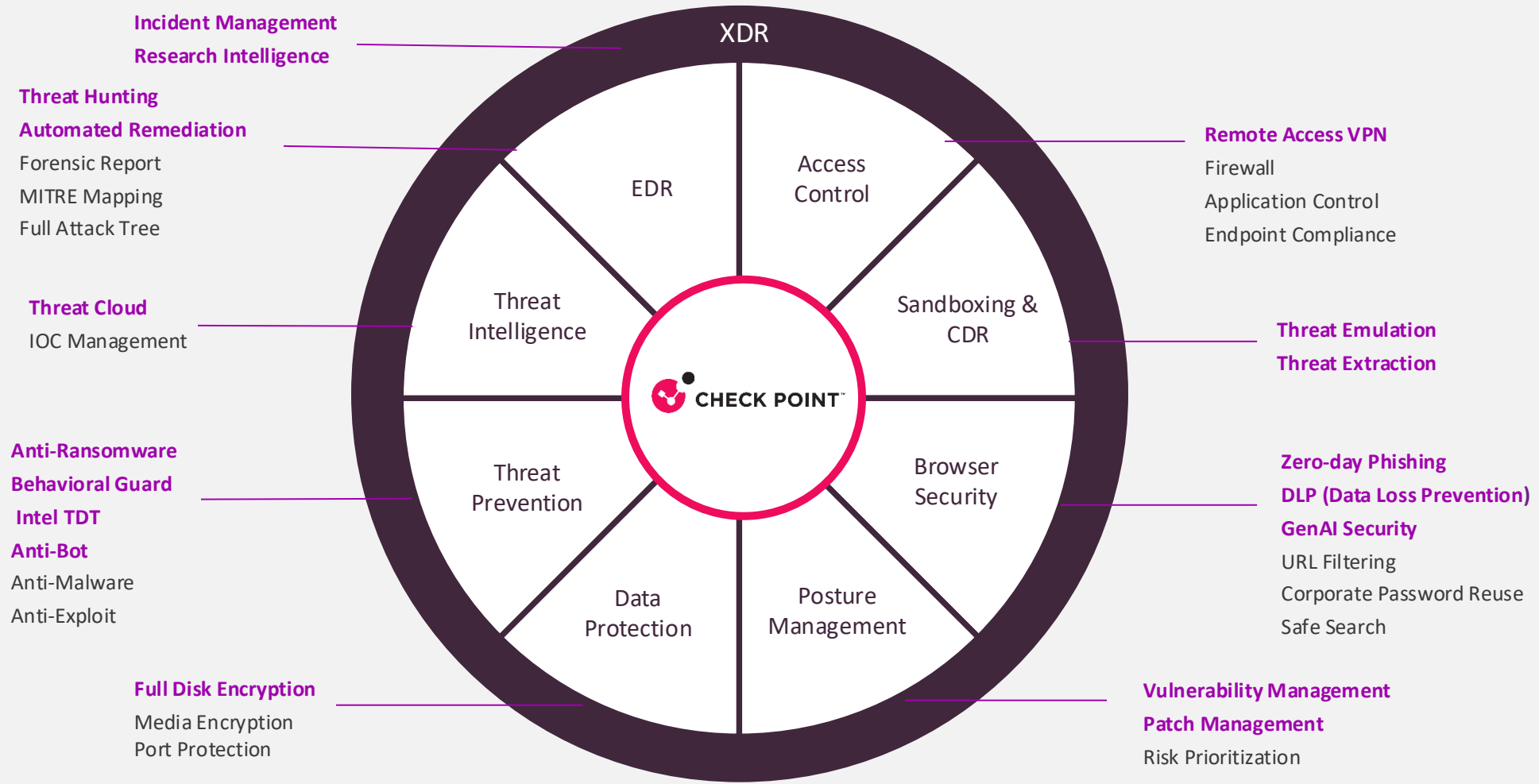
How Check Point achieved excellent detection

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



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



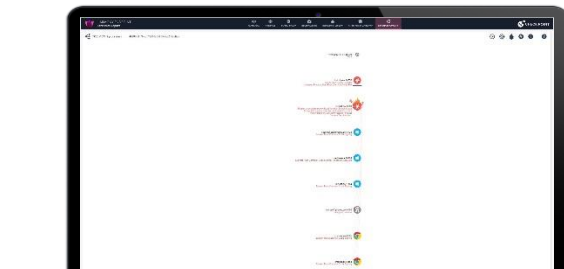
AUTOMATIC REMEDIATION

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



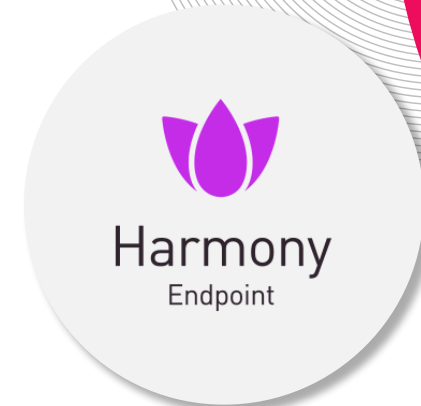
THREAT HUNTING

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.



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

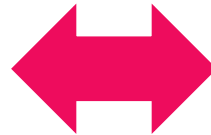
Endpoint Behavior Based, AI
e.g, remote code execution, process activities

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

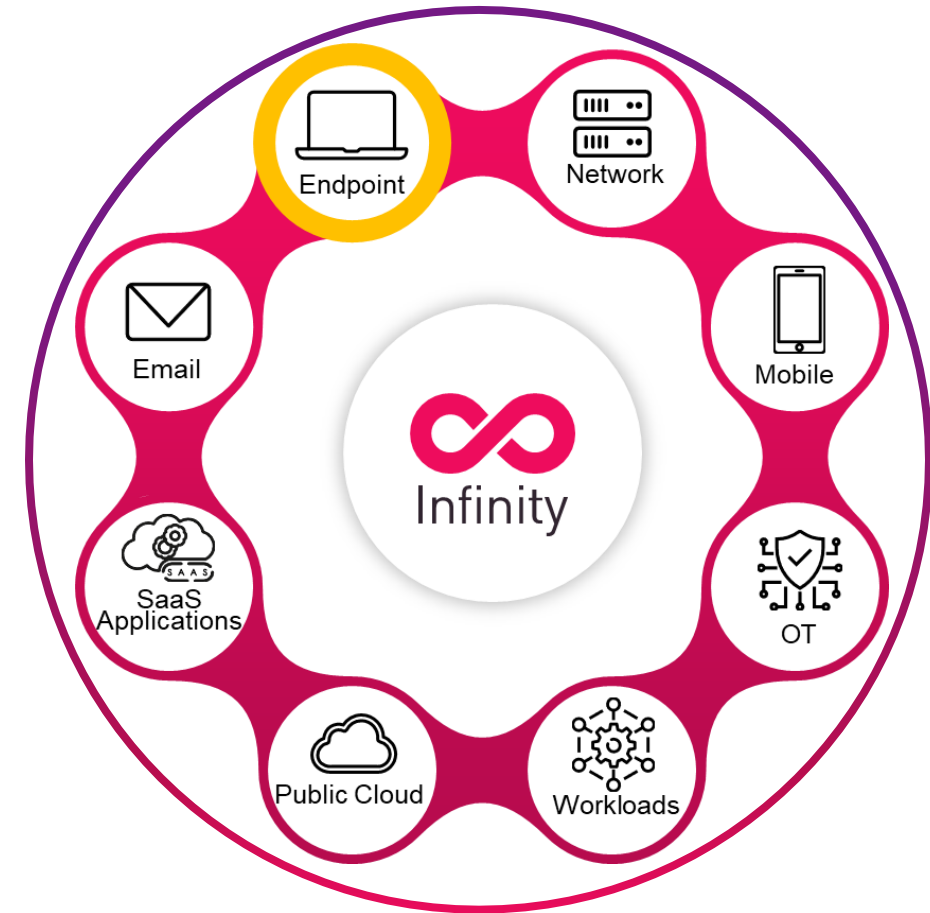
XDR processes
events & alerts

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

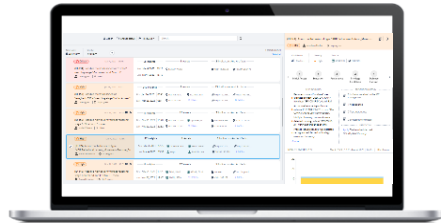
HEP sends events & alerts

XDR processes events & alerts

XDR create incidents

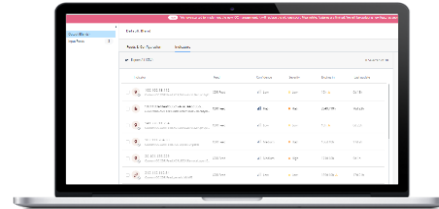
The Benefits Of a Consolidated Approach

Infinity XDR



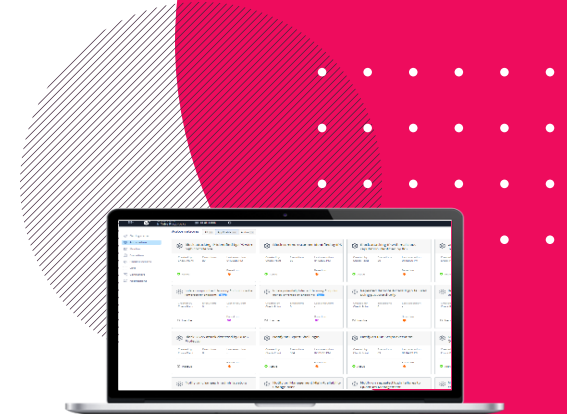
INCIDENT MANAGEMENT

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



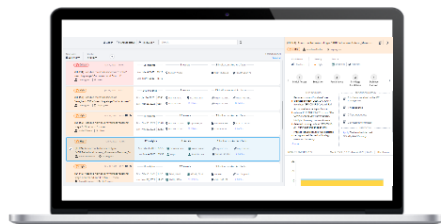
IOC MANAGEMENT

Powered by Multiple Feeds allowing Extensive & Consolidated IOC Management



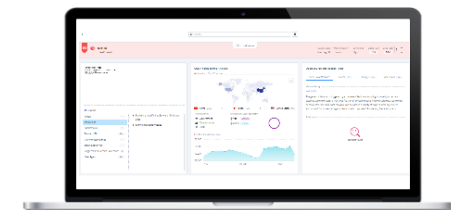
SECURITY PLAYBOOKS

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



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

Fast Onboarding,
As a Cloud Service

Automatic Prevention
Responses

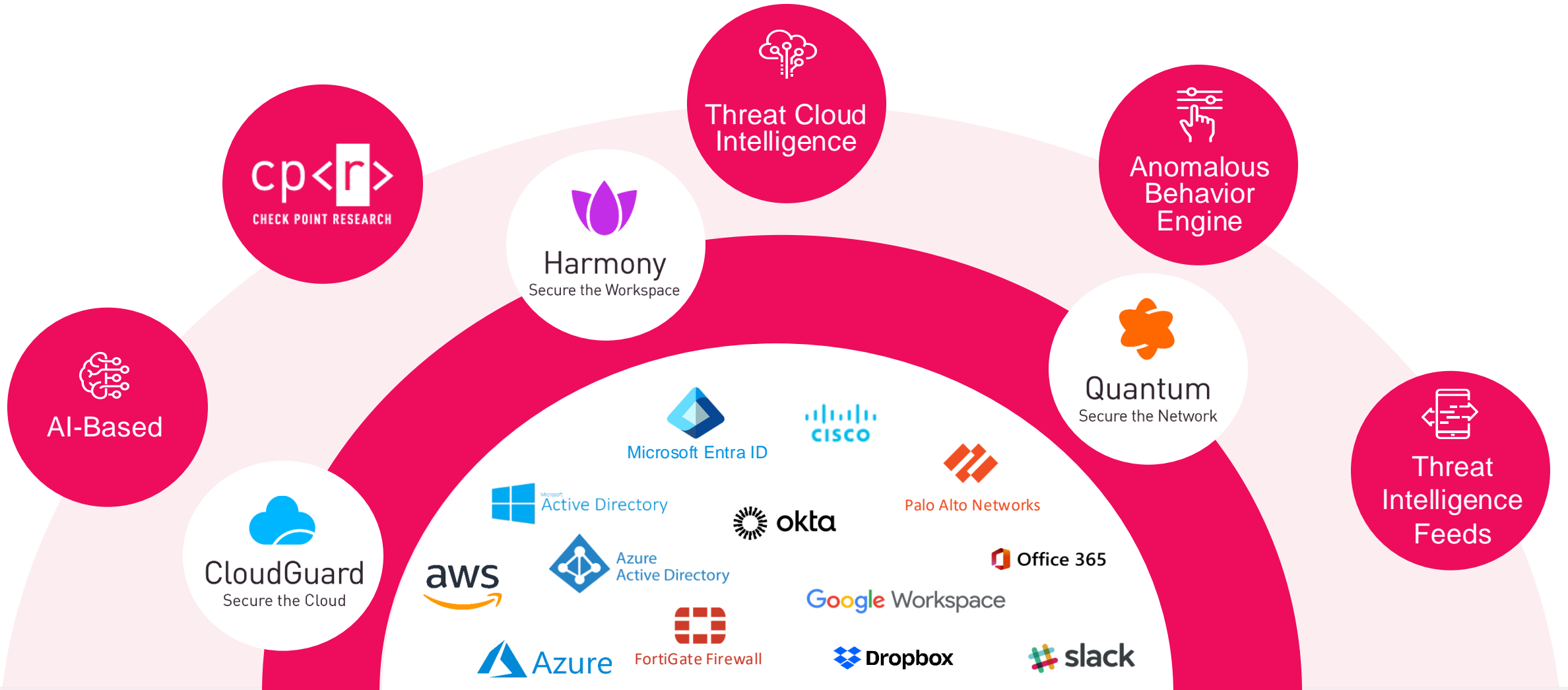


AI Based
Correlations

Simple Investigation
Experience

Comprehensive Threat Prevention

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

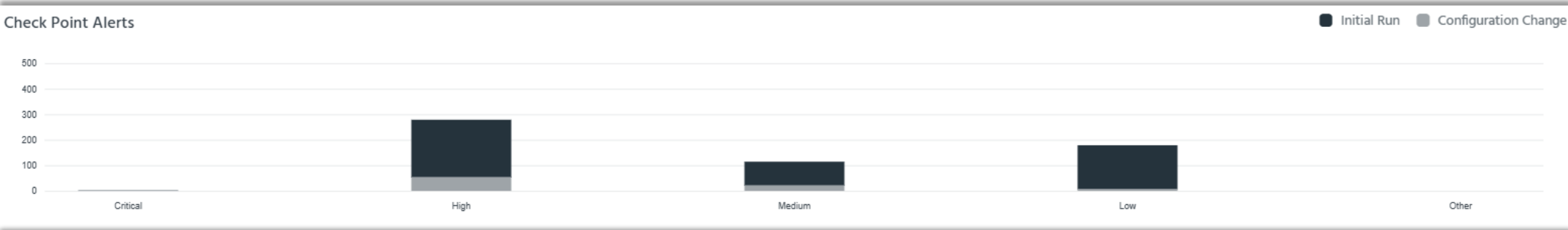


04

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.

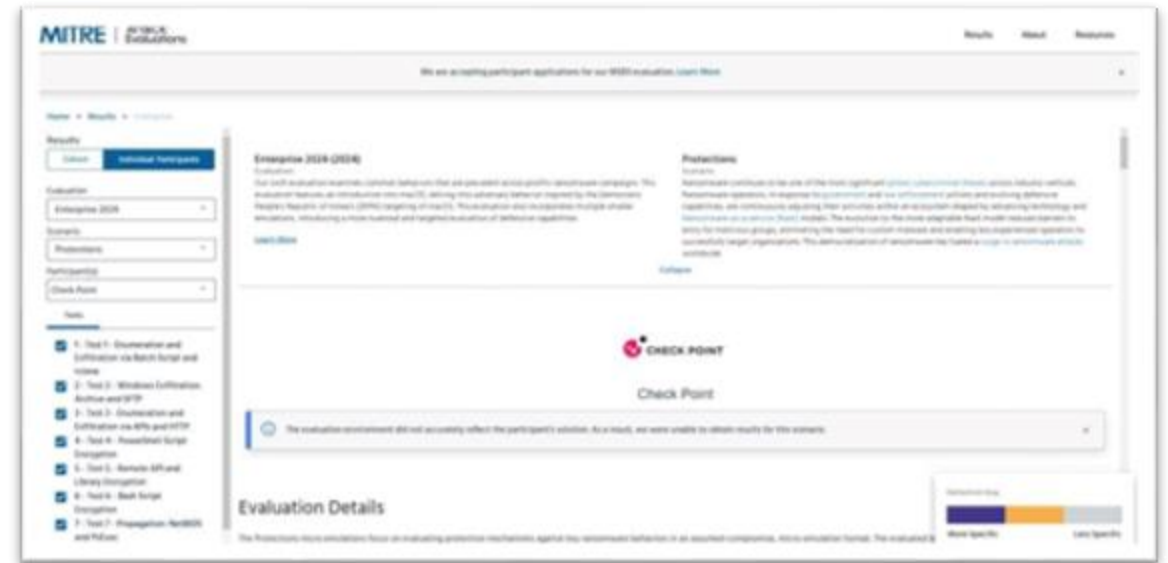
*No training data or learning period was provided.



6 false positives

FAQ

- Where are our Protection results?



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

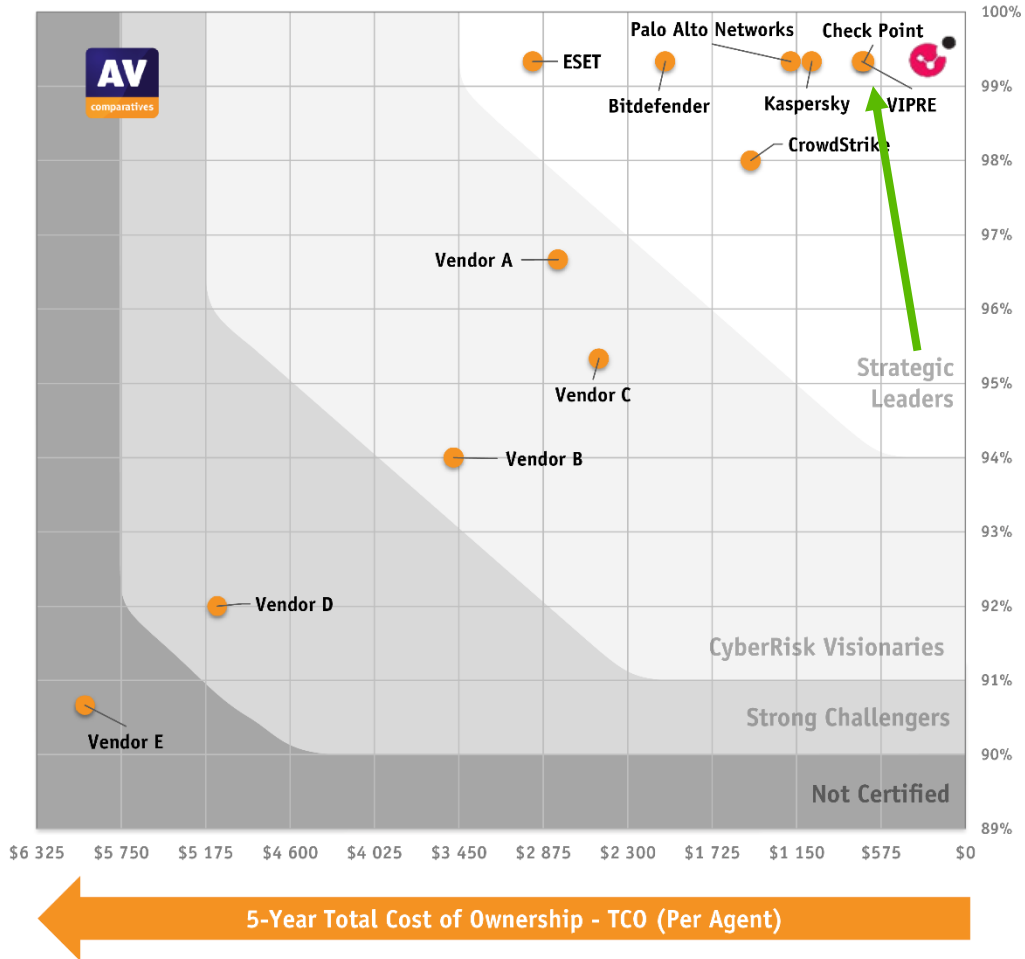


How did we
do?

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

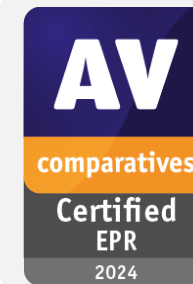
- Leaders in Prevention
- Leader in TCO

50/50 Prevented Scenarios

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

Real Time Response

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



Report Links



Check Point's report



Full report

A Leading Endpoint Solution

Leader

Frost Radar™ XDR Growth and Innovation Leader in 2024



FROST
SULLIVAN

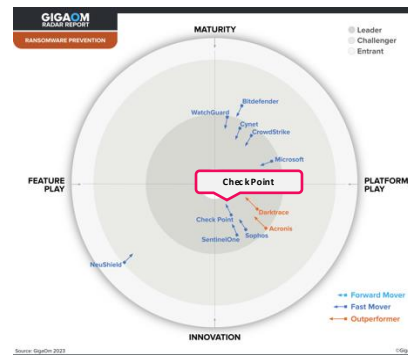
“

“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

“

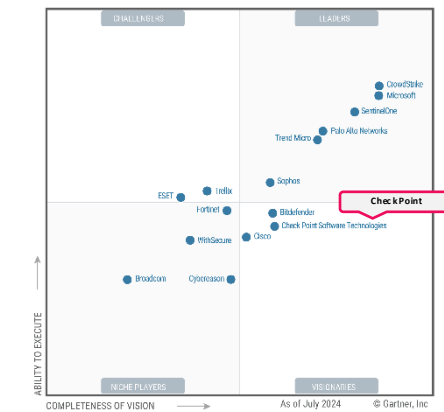
“Broad coverage ensures that the solution will be able to prevent ransomware across a wide range of threat vectors, covering most organizational use cases. Its single administration interface helps simplify management and operational efficiency”

”

A Visionary

2024 Magic Quadrant™ for Endpoint Protection Platforms

Figure 1: 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*





Thank You!

YOU DESERVE THE BEST SECURITY