INFINITY XDR/XPR

EXTENDED PREVENTION & RESPONSE

Comprehensive threat prevention across the entire security estate,
powered by collaborative AI-driven correlations

CONTENTS

Executive Summary

According to Check Point Research, the rate of global weekly cyberattacks is growing at 32% year-over-year, with the annual increase in ransomware exploits coming in at 41%tw[1].

To improve detection and response capabilities against the ever-rising threat of attack, security teams seek tools to consolidate data and gain a wider view of everything across the security estate.

Extended detection and response (XDR) aims to address the need. But can it deliver on the promise?

In this paper we will discuss the current threat landscape and why standard XDR may improve visibility, detection, and response, but it stops short of providing the preventive protection organizations need.

We will also introduce Infinity XDR/XPR, part of the AI-powered, Cloud-delivered Check Point Infinity cyber security platform. XDR/XPR is a powerful AI tool that empowers security operations center (SOC) teams to prevent and remediate attacks faster and more efficiently.

And we will share how four different organizations around the world leveraged Infinty XDR/XPR to make previously unattainable correlations, detecting and preventing the damage of malware, phishing, and other attacks.

[1] Check Point Research, July 26, 2022

Introduction

The threat landscape

Cyberattacks are more frequent, sophisticated, and costly than ever before. This is making it very difficult for security operations teams to keep up with the required tools and knowledge for accelerating threat handling and ensuring its efficacy.

The Growing Risk of Cyberattacks

(Source: Check Point Research)

Moreover, the operational overhead has never been greater:

- Analysts are charged with managing **multiple, siloed detection tools**
- They must sift through and review an **overwhelming number of alerts**
- Alerts are **delivered without context**
- The rate of **false positives** is high

Too often this makes shutting down an attack before the damage spreads a profoundly difficult task.

It's no surprise then, that the average time to identifying and containing a breach is at an astounding 277 days (about 9 months).[2]

The SOC challenge to robust protection

- Keeping up with new cyber skills requirements
- Multiple tools in silos
- Endless alerts
- High rates of false positives
- Narrow view of attacks

[2] IBM, Cost of a Data Breach Report 2023

What the SOC needs to mitigate the risk

To mitigate the risk of today's challenging threat landscape, security teams need to be able to work at peak efficiencies for rapid prevention.

This means automatically consolidating security data from every relevant source and making fast intelligence-driven correlations for faster and more accurate investigations and incident handling.

They also need to be able to focus only on the events that require handling and to catch them at the earliest possible stages, so they can boost prevention with fewer resources.

And they need to be able to do all this for the entire estate, including networks, endpoints, cloud, email, and IoT.

The SOC need

- Comprehensive coverage for the entire security estate
- Consolidating security data from every source
- Correlations among separate events
- Focus only on events requiring action
- Maximizing resources to do more with less

The traditional XDR approach & why it falls short

Today's extended detection and response (XDR) approach aims to address these needs by integrating data from multiple security sources and automating detection and response.

But the current approach still falls short as it does not provide complete coverage with the requisite intelligence-driven correlations for discovering incidents before they propagate and spread across the organization.

Traditional XDR may reduce the alarm queue and number of false positives for improved detection. But detection is not enough.

What organizations need is a way to derive a higher level of value from all the data consolidated by XDR and leverage it for intelligence-driven correlations that uncover severe threats currently flying under the radar of standard XDR solutions. This comprehensive prevention-first approach goes beyond simple detection and response to prevent damage from the stealthiest attacks and help SOC analysts focus their attention where they can have the most impact. Otherwise, the day-to-day mission to protect will remain cumbersome, analysts will still be overwhelmed by too much information, they will still lack the visibility into how what's happening on the network relates to what's happening on the endpoint, email, and cloud, for example, as well as what they need to do to stop threats fast and efficiently.

The limitations of traditional XDR

- Coverage is not comprehensive
- No intelligence-driven correlations of behaviors and events
- Limited early detection of incidents
- Not preventive, detection only

This is where Infinity XDR/XPR comes into play.

Prevention-first protection with Infinity XDR/XPR

Infinity XDR/XPR from Check Point is a comprehensive security operations platform that empowers SOC teams with prevention-first XDR/XPR across the entire security estate.

It delivers clarity and enables focus with intelligence-driven correlations, collaborative AI insights, and consolidated analytics.

XDR/XPR identifies and connects multiple complex security events, which may seem to be unrelated and benign, but are in fact part of a single critical threat. This is how it stops threats from propagating and spreading within the organization at the earliest possible stage.

Moreover, event context and insights, with built-in guidelines for response are accessible to analysts through a single pane of glass, for unprecedented visibility, speed, and operational efficiency.

For additional preventive support, Infinity XDR/XPR is also offered as an end-to-end security operations service, with 24/7 managed prevention and response (MDR/MPR).

Infinity XDR/XPR: comprehensive, collaborative, and consolidated

Comprehensive Threat Prevention
Accurate attack prevention across the entire security estate

Collaborative Threat & Event Correlation
Powered by AI and threat intelligence, correlating Check Point and third-party events

Consolidated Analytics
Improving security posture with visibility into attack behavior, context, and damage

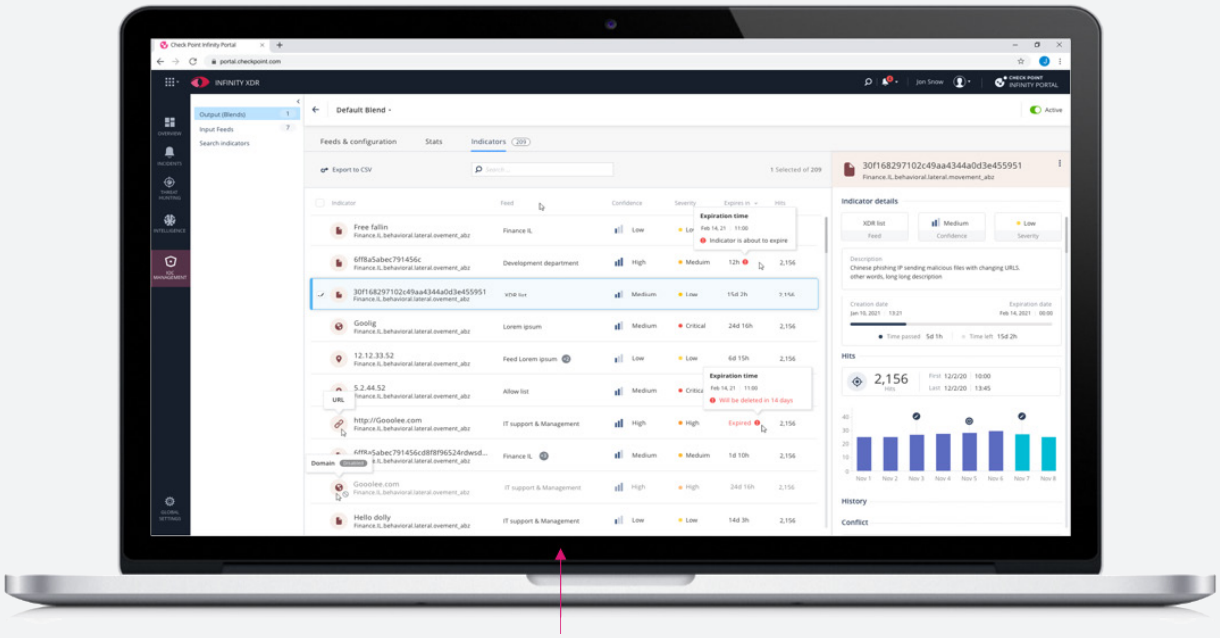
Comprehensive threat prevention

Part of the Check Point Infinity cyber-security platform, XDR/XPR is AI-powered and cloud-delivered and enables accurate attack prevention across the entire security estate, including networks, endpoints, emails, cloud, and IoT.

Infinity XDR/XPR integrates with both Check Point and third-party security solutions and can ingest data from a broad spectrum of sources, integrating with multiple gateways, and connecting to third-party data feeds.

Moreover, with advanced IoC management, the XDR/XPR automatically blocks malicious indicators that are identified on any connected product or external data feed.

IoC management and enforcement



An overview of the current security status, as aggregated from every connected data source, provides analysts ongoing visibility into the preventive actions and auto-responses that have been executed, as well as into those awaiting manual response and handling.

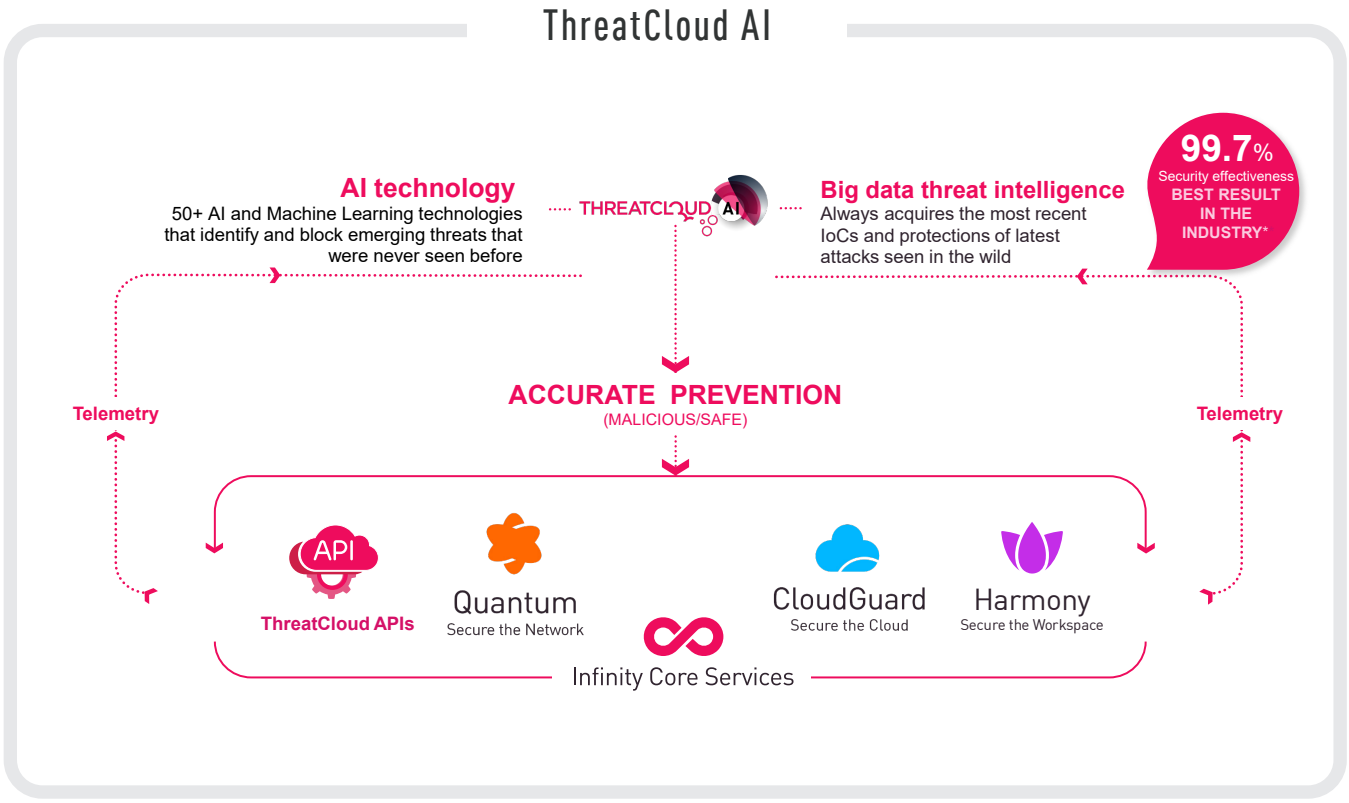
Transforming millions of events into one unified incident

- **Access** the status of all products connected to Infinity XDR/XPR
- **See** only the logs that require action, from among millions of alerts
- **Connect** all relevant logs into one incident that requires action
- **Correlate** network, endpoint, email, cloud, and IoT
- **Get deep dive visibility** into high priority, high severity incidents

Collaborative, intelligence and AI-based threat & event correlation

ThreatCloud AI

XDR/XPR is powered by Check Point Infinity ThreatCloud AI, a real-time global threat intelligence platform that monitors networks around the world for emerging threats and vulnerabilities, providing intelligence-driven insights and context.



Check Point Research cp<r>

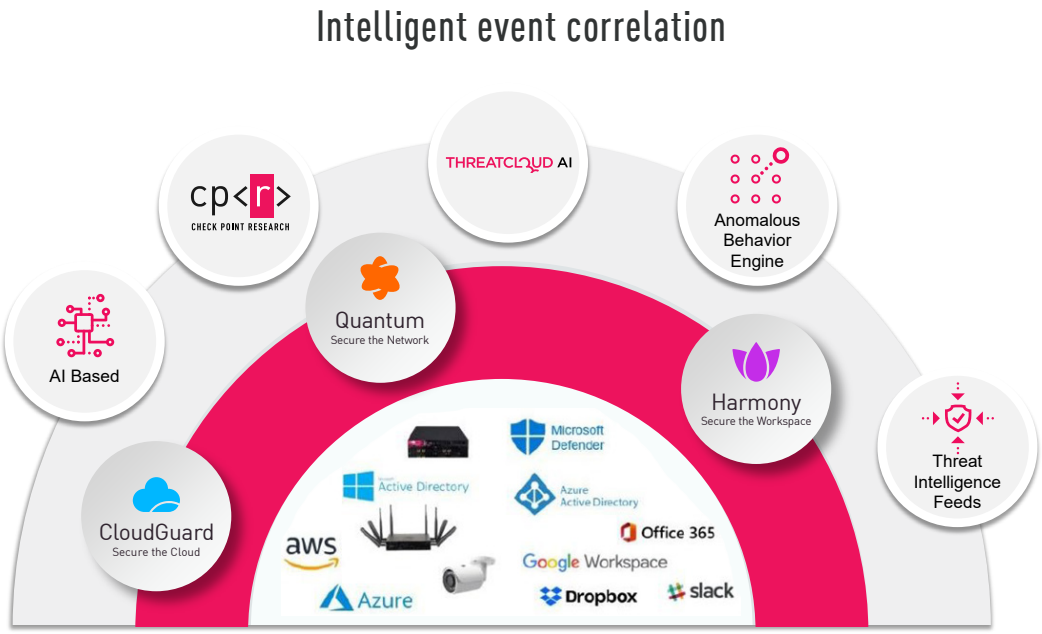
Hundreds of in-house analysts power Check Point's leading cyber security research, which enriches Infinity XDR/XPR with an additional threat intelligence feed. Using proprietary AI modules, anomaly detection, reverse engineering, and threat hunting techniques the Check Point team leads the global effort to prevent cyberattacks.

Cross-product detection

Infinity XDR/XPR provides cross-product detection and correlations even when connected to a single data source. By running behavioral analytics and machine learning models based on all the collected data, analysts can review insights from any security solution through a single pane of glass and improve detection even further by connecting events across the complete attack flow and every product.

Shared IoCs

Indicators of compromise, such as the details of a suspicious URL detected in an email, are shared across networks, endpoints, mobiles, cloud, and email, to prevent additional attack attempts.



Consolidated user and entity behavior analytics

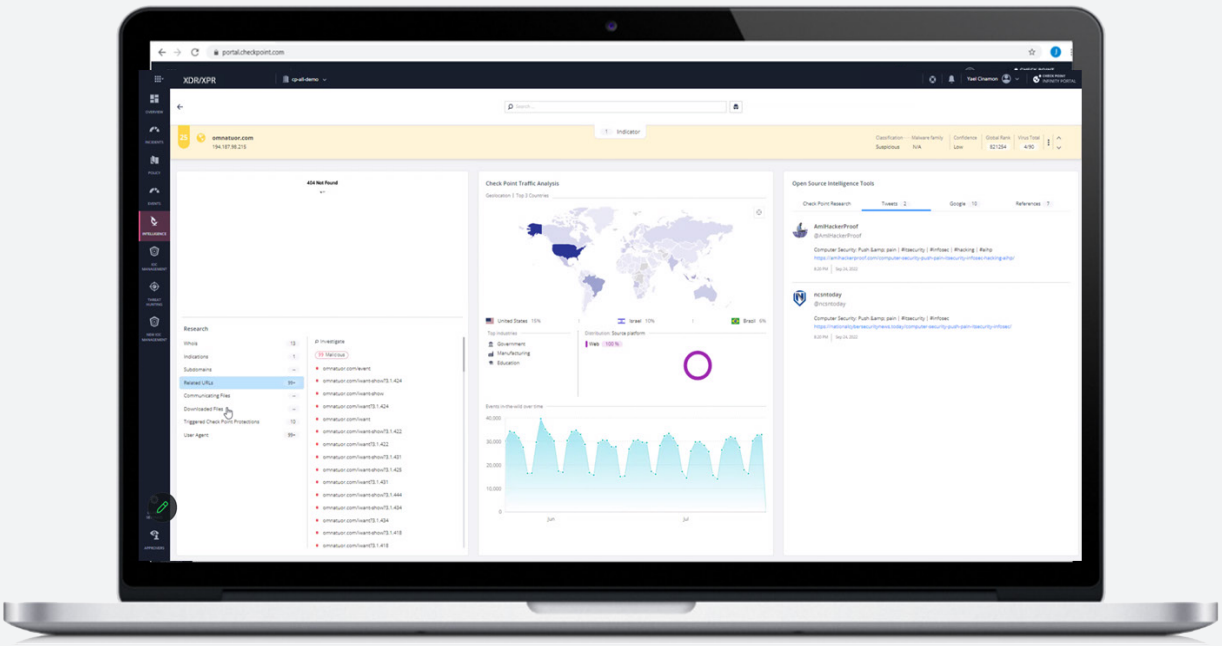
Infinity XDR/XPR performs analytics on data aggregated from across all relevant data sources, connected security products, and first and third-party intelligence feeds to provide the broadest visibility into attack behavior, context, and damage.

This way, analysts can identify anomalous behavior indicative of a potential threat and gain a fast and accurate understanding of where the attack is within the kill chain.

Moreover, incidents are fully mapped to MITRE, enabling analysts to review the tactics detected in the attack and the assets involved, along with the fuller context of the malicious indicators of compromise with intelligence enrichment for each.

By combining intelligence-based correlations and consolidated analytics, analysts can conclude with confidence what the severity level of the event is, eliminating the noise, reducing false positives, and focusing only on the events that require action.

Infinity XDR/XPR insights consolidation for incident investigation



Automated response

Infinity XDR/XPR automates incident response for a significant reduction in the time required to manage an incident and achieve resolution.
Automated actions include isolating the compromised endpoint, blocking malicious indicators, email quarantine, endpoint forensics analysis, process termination, and enforcing password change.

Infinity XDR/XPR highlights

- **Prevention-first XDR/XPR** built from the ground up as a prevention first solution across all products
- **Comprehensive coverage** for any data source, including network, cloud, endpoint, mobile, email and identities
- **Exclusive Check Point Research intelligence** with attack statistics from ThreatCloud AI
- **Immediate IoC sharing** across all connected products for optimized enforcing and blocking of malicious indicators
- **Off-the-shelf built in responses and playbooks** for accelerated operational efficiency

Use cases

European bank: intelligent correlations

A bank in Europe had detected seemingly benign events on the gateway logs and several endpoints, which didn't raise suspicion, as they seemed to be isolated and unrelated.

The events included:

- Process signed by Microsoft and running on the endpoint
- Anti-virus on endpoint disabled
- Endpoints communicating with unfamiliar domains
- Network traffic on unfamiliar domains
- Teams process changing the registry
- User logging into three devices

Typically, each on their own would have been deemed to be low severity events.

However, Infinity XDR/XPR correlated all these events, identifying that this was a high severity breach that reached the command-and-control stage.

As a result, all the required responses were automatically triggered, XDR/XPR isolated the machines, blocked the malicious URLs, terminated the processes on all the devices, and restored Windows Defender policy, resolving the incident immediately.

Government organization in Latin America: Raspberry Robin malware detection

Raspberry Robin is one of the most distributed malwares currently active. It has several entry vectors that lead to the main sample. The most prevalent one is an LNK disguised as a USB drive or a network share which launches msiexec.exe that downloads the main component.

At one government organization in Latin America, Infinity XDR/XPR had correlated multiple low severity detections from the endpoint and the gateway. It identified malware activity, detecting that it was Raspberry Robin malware that had compromised an endpoint. Upon detection, the malware was automatically blocked and prevented from spreading.

Moreover, with the threat hunting capabilities of Infinity XDR/XPR, the government organization's security team determined that a USB drive was inserted into the infected machine right before the attack. And with data from Check Point Research about the targets and timeline of the attack, it was uncovered that government organizations are the second most targeted vertical for this type of malware.

> " Thank you very much for alerting us to this incident. The USB in question was subsequently scanned, and we changed the password for the endpoint and user account. We also took your advice to isolate the endpoint through the XDR/XPR portal."

European financial institution: phishing prevention

At this European financial institution, Infinity XDR/XPR had correlated an informational password re-use alert with URL and IP reputation to discover a medium severity incident of credentials leakage to an unknown phishing website.

Had preventive action not been taken by XDR/XPR, the attacker would have succeeded at leveraging these credentials to gain direct access to 18 additional machines, including domain controllers and other critical assets.

Instead, the financial institution prevented potential damage from an unknown phishing website, blocking malicious indicators on all products connected to Infinity XDR/XPR and forcing password renewal across the organization.

Oil & gas company in Latin America: gateway logs correlation

Infinity XDR/XPR connected with Check Point Quantum correlated more than 100 logs on the gateway to identify a high severity threat at a Latin American oil and gas company, which could have potentially reached the command-and-control stage.

Having identified recurrent and periodic calls to the command and control, it was concluded that a critical asset, a mail server, was infected.

Infinity XDR/XPR alerted the security team that the endpoint does not have Harmony Endpoint installed, underscoring the heightened risk. As a result, the organization installed anti-virus on the relevant endpoint for proactive prevention.

Conclusion

The damage trajectory of cyberattacks is accelerating. Current XDR solutions aim to help SOC teams with improved detection. But detection is not enough. Prevention is key.

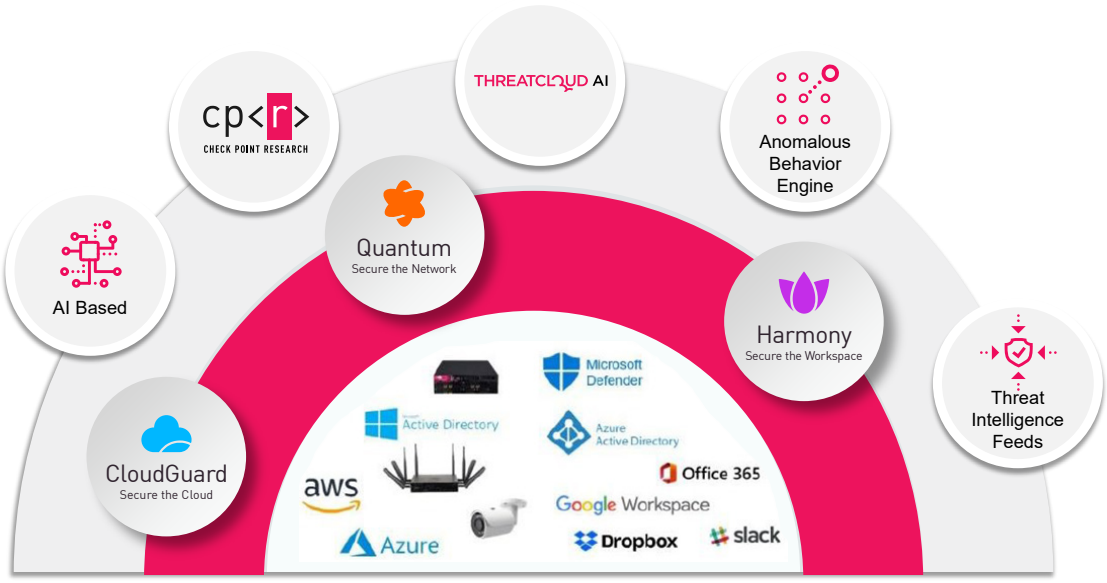
This is what Infinity XDR/XPR is all about, bringing prevention-first detection and response with complete visibility and efficient operation across the entire IT environment from a single pane of glass.

It is comprehensive, collaborative, and consolidated, powering fast intelligence-driven correlations and even faster, more accurate investigations and response, ensuring the robust protection to which every organization aspires.

The Infinity XDR/XPR advantage

- **Comprehensive** coverage of the entire security estate
- **Focusing** on only viable threats
- **Automatically connecting** all activities across attack flow
- **Intelligence-driven insights** from all sources and products
- **Single pane of glass** for status, insights, intelligence, actions
- **Out-of-the-box playbooks** connected to productivity tools
- **Fast onboarding** as a cloud service
- **Available as managed service** for prevention and response

Infinity XDR/XPR:
comprehensive prevention-first protection



"The behavior insights of Infinity XDR/XPR brought a unique value that we didn't have before. Thanks to its behavior detection and correlated events from the endpoint and the gateways, a high severity attack of an evasive malware was prevented."

— Retail Company, North America

To see how Infinity XDR/XPR can help you detect incidents sooner and resolve them faster with greater efficiency, we invite you to book a demo here.
To learn more, visit our website.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com