CHECK POINT™

Horizon

Horizon XDR/XPR
Extended Prevention & Response

The Leading Prevention-First XDR/XPR

Horizon XDR/XPR is a security operations platform that integrates with either Check Point or third-party security solutions, to prevent threats across networks, endpoints, mobiles, cloud and email.

The platform immediately blocks cyber threats originating in any part of the environment and prevents them from impacting the org and propagating across additional entities.

XDR/XPR provides comprehensive threat prevention across the entire security estate through collaborative, intelligent AI correlation.

Comprehensive Threat Prevention

Accurate attack prevention across the entire security estate

Collaborative Threat & Event Correlation

Powered by collaborative, intelligent AI

Consolidated Analytics

Improve security posture with visibility into attack behavior, context and damage

OTD BİLİŞİM
GLOBAL VAD

Prevent Known & Zero-Day Attacks Across Networks, Endpoints, Cloud & Email.

XDR/XPR represents your last line of cyber defense; an additional layer of security across your consolidated security estate. Horizon XDR/XPR prevents complex attacks where seemingly benign events across different parts of the security estate, add up to a critical threat to your organization.

The platform can automatically stop threats from propagating and spreading within your organization, and provides clear forensics as extra validation for the SecOps user.

• Comprehensive threat prevention

Automatic, accurate attack prevention across the entire security estate, leveraging integrations with Check Point and 3rd party security solutions.

• Intelligent threat & event correlation

Prevention is powered by AI and threat intelligence, correlating Check Point and 3rd party data.

• Consolidated analytics

Improve security posture with visibility into attack behavior, context and damage. Understand where the attack is within the kill chain.

Prevention Powered by Collaborative, Intelligent, AI Based Correlation

The comprehensive coverage and visibility into the entire security estate, means that the platform has the unique ability to correlate multiple data sets to identify threats. The data used to prevent attacks include:

• Indicators of compromise from the customer's environment - these are shared across networks, endpoints, mobiles, cloud and email to prevent any additional attempts to attack (e.g. details of a suspicious URL detected in an email, is shared across mobile, endpoint, cloud and the network)

• Wisdom of the global threat landscape with indicators of compromise from Check Point's 150,000 gateways and millions of endpoints (ThreatCloud)

• CP<R> Check Point's research team comprised of hundreds of leading threat analysts who reverse engineer cyber-attacks to provide data toprevent further attacks

• User and entity behavior analytics to identify anomalous behavior indicative of a potential threat.

• Third-party threat intelligence feeds which provide additional threat intelligence from third-party security vendors.

With the unique ability to correlate seemingly benign individual events to discover well disguised significant threats, Horizon XDR/XPR prevents threats that other solutions would be unable to detect.

Horizon
XDR/XPR