CHECK POINT™

Horizon

Check Point Horizon

Unified Management & Security Operations

The cyber threat landscape becomes increasingly complex and dangerous every year. Cyber-attacks are more sophisticated than ever which makes threat prevention a fundamental component of any organization's security strategy. For many security operations teams, detecting real threats across their entire IT infrastructure is like finding a needle in the haystack. They are often forced to piece together information from multiple, costly, siloed tools and navigate through an absurd number of daily alerts. This combination of challenges - increased threat landscape, SOC teams running 24x7x365, headcount and skill shortages – means that critical attacks are sometimes missed until it's too late.

> *The WannaCry ransomware worm is estimated to have caused $4 billion USD in damages globally[1]. According to the Check Point Research (CPR) 2022 Mid-Year Cyber Trends report, attacks have increased globally by 42 percent[2]. Recent research reveals that 83% of security professionals suffer "alert fatigue" and struggle with managing alerts along with their other priorities.*

Horizon - Unified Management & Prevention-First Security Operations

Check Point's Horizon is the leading prevention-first security operations platform, with robust, powerful SOC operations tools and services - empowering SOC teams to boost prevention with fewer resources. The Horizon platform provides XPR/XDR, MPR/MDR, and Events Management solutions. Horizon's prevention-first approach offers complete coverage for the network, endpoints, cloud, email, IoT, and mobile devices - all from one pane of glass. It enables SOC analysts to proactively prevent, monitor, detect, investigate, hunt, respond, remediate attacks, and improve defenses to prevent future attacks, and to gain accurate prevention against the most advanced attacks through the power of ThreatCloud, the brain behind all of Check Point's products.

1 "Ransomware: A Constant Threat," Kirk Hayes, Infosecurity Magazine, Feb 21, 2022
2 Cyber attack Trends, Check Point Research 2022 Mid-Year Report," CPR, August 3, 2022

Security Operations Must Be Prevention-First

For Check Point customers, prevention starts by leveraging the holistic security architecture in prevention mode across all enforcement points, including endpoints, network, cloud, email, and IoT. This is the first step tp ensure the highest possible catch rate.

For SOC teams to gain further insights into security events, Horizon includes Events Management, which provides full visibility into logs across the entire security architecture so that SOC teams can understand where attacks have been prevented.

XPR/XDR is the Extended Prevention & Response solution powered by ThreatCloud – Check Point's threat intelligence platform – and designed by CP<R> experts who understand the needs of SOC teams. XPR/XDR optimizes prevention of attacks further by correlating events over time, across all Check Point products. This consolidated knowledge enables accurate prevention of threats and granular forensics for SOC teams.

Horizon also includes MPR/MDR for Managed Prevention & Response. This is a service layer on top of the Horizon platform where an organization's entire security real estate is monitored 27x7x365 so that threats are blocked by Check Point Experts in real time.

> *According to Gartner, "by 2025, 50% of organizations will be using MDR services for threat monitoring, detection and response functions that offer threat containment and mitigation capabilities[1]."*

Horizon MPR/MDR - Managed Prevention and Response

The leading prevention-first MPR/MDR solution: complete and powerful SOC operations delivered as-a-service. Check Point's MPR/MDR service is powered by the industry's top analysts, Incident Response, and research team experts, and leading AI technology to proactively prevent, monitor, detect, investigate, hunt, respond, and remediate attacks on customers' environments. Our experts discharge security operations teams from the desperate struggle with hundreds of millions of weekly alerts. We monitor your security estate 24X7, covering your entire infrastructure: network, endpoint, cloud, email, and more, and make informed decisions to stop attacks and improve defenses to prevent future attacks. With Horizon MPR/MDR you gain better protection and operational peace of mind and address the skill shortage while significantly reducing your security operations TCO.

1 Market Guide for Managed Detection and Response Services," by Pete Shoard, Craig Lawson, et. al, Gartner, October 25, 2021

Horizon XPR/XDR – Extended Prevention and Response

The leading prevention-first XPR/XDR solution - includes best practices to improve defenses and prevent future attacks. Increase your security operations efficiency with the ability to quickly detect, investigate, and automate responses to attacks across the entire IT infrastructure. XPR/XDR identifies threats inside the organization and prevents their expansion by leveraging data correlated from all products. Its unique Prevention-first approach significantly improves customers' overall security posture while detecting unknown zero-day threats. All via a single SaaS solution that increases ROI and reduces operational overhead. It detects and stops even the stealthiest attacks by combining advanced threat prevention powered by AI-based analytics, big-data threat intelligence, multi-layered incident analysis, machine learning, and enterprise-wide visibility into customer's network, cloud, email, endpoint, etc., all from a single pane of glass. In addition, XPR/XDR enables you to leverage your existing Check Point security stack.

Horizon Events - Unified Events Management

Horizon Events provides complete event visibility across all Check Point products for efficient monitoring, search, and threat hunting. Designed for security admins and analysts to investigate and troubleshoot all security incidents with a simple and intuitive SaaS cloud solution. It saves valuable time and eliminates complexity by unifying and synchronizing security events across your network, endpoint, mobile, IoT, and cloud environments. Horizon Events lets you quickly search and view security logs across all Check Point products, providing unified event visibility. Cyber analysis is made easy by fast and Intuitive troubleshooting and analysis for daily activities, and it delivers logs and events as a service, enabling the creation of custom alerts for critical events.

ThreatCloud – Powering Prevention Across The Enterprise

When you are using Check Point to secure your business, you gain accurate prevention against the most advanced attacks through the power of ThreatCloud. ThreatCloud, the brain behind all of Check Point's products, combines the latest AI technologies with big data threat intelligence to prevent the most advanced attacks while reducing false positives, keeping your business safe and productive. ThreatCloud aggregates and analyzes big data telemetry and millions of Indicators of compromise (IoCs) every day. Its threat intelligence database is fed from 150,000 connected networks and millions of endpoint devices, as well as Check Point Research and dozens of external feeds. ThreatCloud prevents zero-day attacks before the rest through 30+ highly trained AI-based engines.

Learn more about Horizon and sign up for a free demo.

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com