CHECK POINT™

Harmony
Endpoint

Harmony Endpoint

All the Endpoint Protection You Need

These days, cyberattacks are significantly increasing in volume and sophistication. According to Check Point Research Group, there was a 38% rise in the number of cyberattacks year-over-year, with an average of 1,150 attacks on each organization every week. However, organizations are still facing significant challenges when trying to protect their endpoints.

Security Gaps

As cyberattacks get more and more sophisticated, keeping your organization safe is more challenging than ever.

Multiple Security Products

To cover all attack vectors, enterprises require many different security products

Training & Cost

Maintaining a skilled security & IT team, with budget limitations is a never-ending job

Harmony Endpoint is a complete endpoint security solution built to protect the remote workforce from today's complex threat landscape. It provides a 360° endpoint protection with advanced EPP, EDR and XDR capabilities all in a single client. Its prevention-first approach ensures your organization is not exposed to attacks and it simplifies your security operations, reducing both costs and effort. With Harmony Endpoint, your organization gets all the endpoint protection it needs, at the quality it deserves, in a single, efficient, and cost-effective solution.

KEY PRODUCT BENEFITS

Comprehensive security with a prevention-first approach protects against the most imminent threats such as ransomware, phishing or drive-by malware.

Consolidated Solution - all the endpoint protection you need in a single, efficient and cost-effective solution.

Collaborative Operations - Seamless integration into your existing security ecosystem with an API-based augmentation to your current management and security tools.

MAIN CAPABILITIES

EPP, EDR & XDR in a single client and management console.

Zero-Phishing & Browser Protection: Blocks the most sophisticated phishing attacks with zero impact on end users.

ThreatCloud AI - Zero-Day protection with more than 60 AI engines.

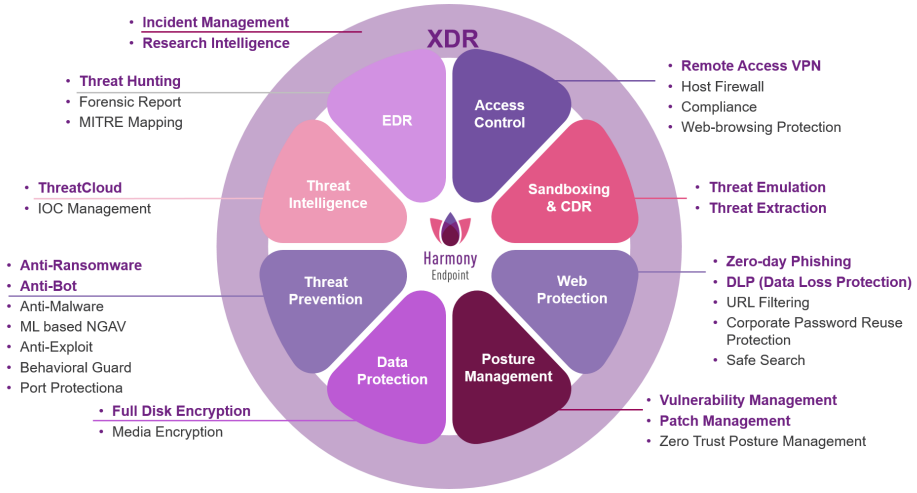
Posture Management: Reduce the attack surface with Risk assessment and Vulnerability & Patch management.

Ransomware Protection – cutting edge ransomware prevention, with rapid threat detection and seamless recovery.

Data Protection prevents data loss with custom policies to keep data safe and maintain compliance.

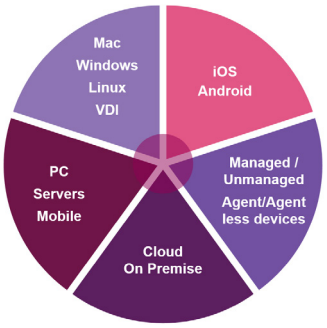
Comprehensive security

Harmony Endpoint is a Comprehensive solution that unifies Prevention, Detection and Response with unique prevention-first approach powered by ThreatCloud AI.



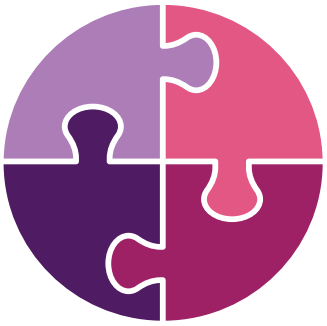
Consolidated Solution

Supports all Operating systems in a single client and management console.



Collaborative operations

Harmony Endpoint is a Collaborative solution with easy integration to third parties to augment security effectiveness.



Market-leading Endpoint Security Solution

Harmony Endpoint recognized as a Top Product in Corporate Endpoint Protection by AV-TEST

LEARN MORE

MITRE ATT&CK® Evaluations Highlight Check Point Leadership in Endpoint Security

LEARN MORE

Check Point Harmony Endpoint Recognized as a CyberRisk Visionary in Endpoint Protection Response test by AV-Comparatives

LEARN MORE

Technical Specifications

Harmony Endpoint Packages	
Packages	**Harmony Endpoint Prevent** – includes: Threat Intelligence – ThreatCloud and IOC Management Access Control - Firewall, Application Control, Endpoint Compliance, Remote Access VPN) Threat Prevention - Anti-Ransomware (Including Intel TDT), Anti-Malware, Anti-Bot, Anti-Exploit, Behavioral Guard, and Port Protection **Harmony Endpoint Basic** – includes Harmony Endpoint Prevent, plus: Browser Protection – Zero Phishing, URL Filtering, Corporate password Reuse, Safe Search EDR – Forensics collection & automated reports, MITRE Mapping, and Threat Hunting **Harmony Endpoint Advanced** – includes Harmony Endpoint Basic, plus: Sandboxing & CDR – Threat Emulation and Threat Extraction & Sanitization **Harmony Endpoint Complete** – includes Harmony Endpoint Advanced, plus: Data Protection – Full Disk Encryption and Removable Media Encryption **Data Protection** – includes Full Disk Encryption and Removable Media Encryption, including Port Protection, Remote Access VPN, Endpoint Compliance, Application Control and Firewall.
Optional Add-Ons	**Horizon XDR / XPR** – includes Research Intelligence**,** Incident Management**,** Events Correlation and Ticketing Management with 1-year data retention **Vulnerability Management** – includes Vulnerability Management for Operating Systems and 3rd party applications **Posture Management** – includes Vulnerability Management and Patch Management **Data Retention for Threat Hunting** – 1 month / 1 quarter / 1 year data retention
Centralized Management	
Cloud & On-Prem Management	**Cloud Management** **On-Premise Management** **MSSP Management**
Operating Systems	
Operating System	**Windows Workstation** – 7, 8, 10 and 11 **Windows Server** – 2008 R2, 2012, 2012 R2, 2016, 2019, 2022 **MacOS** – Mojave 10.14, Catalina 10.15, BigSur 11.x, Monterey 12x, Ventura 13.x **Linux** – Ubuntu (16.04, 18.04, 20.04, 22.04), Debian (9.12-11.5), RHEL (7.8-8.7), CentOS (7.8-8.5), Oracle (7.9-8.4), Amazon (2), OpenSUSE (15.3, 42.3), SUSE (12 SP5, 15 SP3) **VDI & Terminal Server** – VMware, Citrix, Terminal Server
Built-In Integrations	
Integrations & APIs	**API-based** – with easy integration to third parties **UEM Integrations** – Intune, Jamf **Azure Active Directory**

Feature Description

Threat Intelligence	
ThreatCloud	The brain behind Check Point Software's threat prevention power, combines big data threat intelligence with advanced AI technologies to provide accurate prevention to all Check Point Software customers.
IOC Management	Indicator of Compromise (IoC) is an indicator to cyber security professionals about unusual activity or an attack. Harmony Endpoint allows you to add IoCs for domains, IP addresses, URLs, MD5 Hash keys and SHA1 Hash keys that will automatically blocked.
Access Control	
Firewall	Firewall rules accept or drop network traffic to and from Endpoints, based on IP addresses, Domains, Ports and Protocols.
Application Control	Enable the option to restrict network access for specified applications. Application control rules define if to allow, block or terminate applications and processes.
Endpoint Compliance	The compliance component ensures Endpoint's compliance with the organization's security rules. Endpoints that do not comply show as "non-compliant" and the administrator can apply restrictive policies for them.
Remote Access VPN	Virtual private network (VPN) enables users who are working remotely to securely access and use applications and data that reside in the corporate data center and headquarters, encrypting all traffic the users send and receive
Threat Prevention	
Anti-Ransomware	Constantly monitors for ransomware specific behavior and identifies illegitimate file encryption, signature-less. Detect and quarantine all elements of a ransomware attack are identified by forensic analysis and then quarantined. Data Restoration - Encrypted files are automatically restored from snapshots to ensure full business continuity. Intel TDT – Implementing processor-level protection using Intel Threat Defense Technology.
Anti-Malware	Protection from all kinds of malware threats, ranging from worms and Trojans to adware and keystroke loggers.
Anti-Bot	A bot is a malicious software that can invade and infect Endpoints with many infection methods.Harmony Endpoint Anti-Bot component detects and prevents all bots threats.
Anti-Exploit	Provides protection against exploit-based attacks compromising legitimate applications, ensuring those vulnerabilities can't be leveraged. Harmony Endpoint Shuts down the exploited process upon detecting one, remediates the entire attack chain
Behavioral Guard	Adaptively detects and blocks malware mutations according to their real-time behavior. Identifies, classifies, and blocks malware mutations in real-time based on minimal process execution tree similarities.
Port Protection	Protects sensitive information by requiring authorization for access to storage devices and other input/output devices.
Attack Investigation	
Forensics Collection & Automated Reports	On detection of a malicious event, Forensics analysis is automatically initiated, and the entire attack sequence is presented as a Forensics Report. By using the Forensics report, the user can prevent future attacks and to make sure that all affected files and processes work correctly.
MITRE Mapping	The MITRE ATT&CK dashboard provides real-time visibility on all the techniques observed by Harmony Endpoint, it maps all events to MITRE tactics, Techniques and Procedure (TTPs).
Web Protection	
Zero-Phishing	Real-time protection from unknown zero-day phishing sites. Static and heuristic-based detection of suspicious elements across websites requesting private info
Corporate Credential Protection	Detection of corporate credentials reuse on external sites.
URL Filtering	Lightweight browser plugin, allow/block access to websites in real-time with Full visibility to HTTPS traffic
Safe Search	Safe search is a feature added to search engines that acts as an automated filter for potentially offensive and inappropriate content.
Threat Hunting	
Threat Hunting	Collection of all raw and detected events on the endpoint, enabling advanced queries, drill-down, and pivoting for proactive threat hunting and deep investigation of the incidents.
Sandboxing & Content Disarm & Reconstruction (CDR) across email and web	
Threat Extraction	Removes exploitable content, reconstructs files to eliminate potential threats and delivers sanitized content to users in a few seconds
Threat Emulation	Threat sandboxing capability to detect and block new, unknown malware and targeted attacks found in email attachments, downloaded files, and URLs to files within emails. Provides protection across widest range of file types, including Office, Adobe PDF, Java, Flash, executables, and archives, as well as multiple Windows OS environments. Uncovers threats hidden in SSL and TLS encrypted communications.
Data Protection	
Full Disk Encryption	Full disk encryption provides the highest level of data security. It combines boot protection and strong disk encryption to ensure that only authorized users can access the data.
Removable Media Encryption	Media Encryption enables users to create encrypted storage on removable storage devices that contain business-related data.

Why Harmony Endpoint?

Today more than ever, endpoint security plays a critical role in enabling your remote workforce. With 70% of cyber attacks starting on the endpoint , complete endpoint protection at the highest security level is crucial to avoid security breaches and data compromise.

Harmony Endpoint is a complete endpoint security solution built to protect the remote workforce from today's complex threat landscape. It prevents the most imminent threats to the endpoint such a

ransomware, phishing, or drive-by malware, while quickly minimizing breach impact with autonomous detection and response.

This way, your organization gets all the endpoint protection it needs, at the quality it deserves, in a single, efficient, and cost-effective solution.

Harmony Endpoint is part of the Check Point Harmony product suite, the industry's first unified security solution for users, devices and access. Harmony consolidates six products to provide uncompromised security and simplicity for everyone. It protects devices and internet connections from the most sophisticated attacks while ensuring Zero-Trust Access to corporate applications - all in a single solution that is easy to use, manage and buy.

Learn more: https://www.checkpoint.com/products/advanced-endpoint-protection/

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