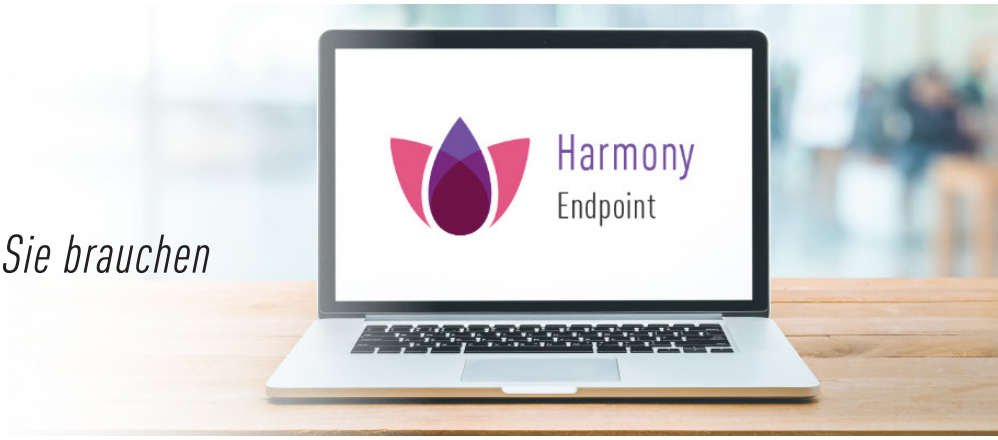
Check Point
SOFTWARE TECHNOLOGIES LTD

Harmony Endpoint –

der Schutz für Endgeräte, den Sie brauchen



Harmony Endpoint ist eine umfassende Sicherheitslösung für Endgeräte, die Remote-Mitarbeiter vor der komplexen Bedrohungslandschaft von heute schützt. Es verhindert unmittelbare Bedrohungen für Endgeräte wie Ransomware, Phishing oder Drive-by-Malware und minimiert gleichzeitig die Auswirkungen von Sicherheitsverletzungen durch autonome Erkennung und Reaktion.

Auf diese Weise erhalten die Endgeräte Ihres Unternehmens in einer einzigen, effizienten und kostengünstigen Lösung den gesamten Schutz, den es benötigt, in der Qualität, die es verdient.

HAUPTVORTEILE DES PRODUKTS

Umfassender Schutz für Endgeräte: Vermeidung unmittelbarer Bedrohungen für Endgeräte

Schnellste Wiederherstellung: Automatisierung von 90 % der Angriffserkennungs-, Untersuchungs- und Behebungsaufgaben

Beste Gesamtbetriebskosten: Der Schutz für Endgeräte, den Sie benötigen, in einer einzigen, effizienten und kostengünstigen Lösung

EINZIGARTIGE PRODUKTFUNKTIONEN

Fortschrittliche Verhaltensanalysen und Algorithmen für maschinelles Lernen legen Malware lahm, bevor sie Schäden verursacht

Hohe Erkennungsraten und niedrige Zahl an Fehlalarme gewährleisten Sicherheitseffizienz und effektive Prävention

Automatisierte forensische Datenanalyse bietet detaillierte Einblicke in Bedrohungen

Vollständige Eindämmung und Behebung von Angriffen, um infizierte Systeme schnell wiederherzustellen

Marktführende Lösung für Endgerätesicherheit

AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS 10/2020 av-test.org TOP PRODUCT

Harmony Endpoint von AV-TEST als eines der besten Produkte im Bereich Endgeräteschutz für Unternehmen anerkannt

MEHR ERFAHREN

FORRESTER®

Forrester Wave erkennt Check Point als führenden Anbieter von Endgerätesicherheit an

MEHR ERFAHREN

AA NSS Labs

Check Point Harmony Endpoint erhält AA-Produktbewertung im NSS Labs 2020 Advanced Endpoint Protection Test

MEHR ERFAHREN

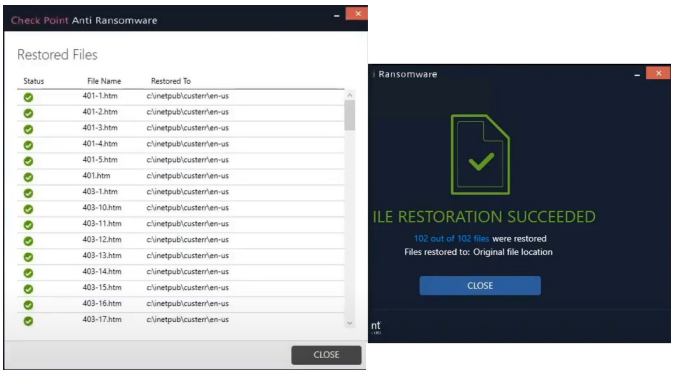
Funktionsweise

Vollständiger Schutz für Endgeräte

Verhindern Sie unmittelbare Bedrohungen für Endgeräte

- **Blockieren Sie** Malware, die aus dem Internet oder aus E-Mail-Anhängen kommt, bevor sie Endgeräte erreicht, ohne die Produktivität der Benutzer zu beeinträchtigen. Jede per E-Mail empfangene oder von einem Benutzer über einen Webbrowser heruntergeladene Datei wird an die Threat Emulation-Sandbox gesendet, um sie auf Malware zu untersuchen. Die Dateien können auch mit einem Bedrohungsbereinigungsprozess (Content Disarm & Reconstruction-Technologie) bereinigt werden, um innerhalb von Millisekunden sichere und gereinigte Inhalte zu liefern.

- **Sichern Sie sich einen Laufzeitschutz vor Ransomware, Malware und dateilosen Angriffen mit sofortiger und vollständiger Behebung,** selbst im Offline-Modus. Sobald eine Anomalie oder ein böswilliges Verhalten erkannt wird, blockiert und behebt Endpoint Behavioral Guard die gesamte Angriffskette, ohne schädliche Spuren zu hinterlassen. Anti-Ransomware identifiziert Ransomware-Verhaltensweisen wie die Verschlüsselung von Dateien oder Versuche, Betriebssystem-Backups zu kompromittieren, und stellt Ransomware-verschlüsselte Dateien automatisch sicher wieder her. Harmony Endpoint verwendet einen eindeutigen, lokal auf dem Computer liegenden Speicherplatz, der nur für von Check Point signierte Prozesse zugänglich ist. Falls die Malware versucht, eine Schattenkopie zu löschen, gehen auf dem Computer keine Daten verloren.



- **Phishing-Schutz**- Verhindern Sie den Diebstahl von Anmeldedaten mit der Zero-Phishing®-Technologie, die die Nutzung von Phishing-Websites in Echtzeit identifiziert und blockiert. Die Websites werden inspiziert und wenn sie als bösartig erkannt werden, wird der Benutzer daran gehindert, Anmeldeinformationen einzugeben. Zero-Phishing® schützt sogar vor bisher unbekannten Phishing-Websites und der Wiederverwendung von Unternehmensanmeldeinformationen.

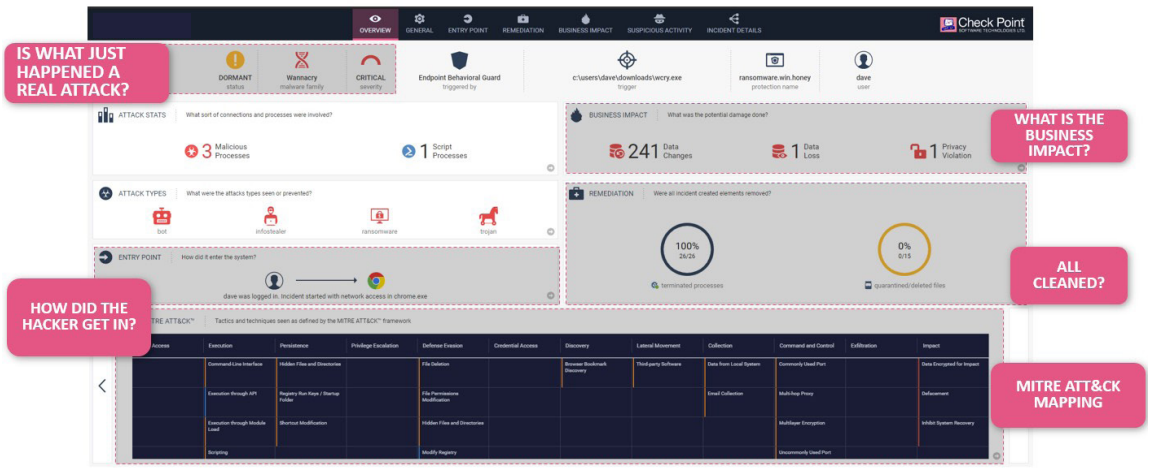
Die branchenweit beste Abfangrate bekannter und Zero-Day-Malware

Harmony Endpoint ist ein anerkannter Branchenführer, der in den AV-TEST Corporate Endpoint Protection- und NSS Advanced Endpoint Protection-Labortests von 2020 zu finden ist. Harmony Endpoint verfügt über mehr als 60 Engines zur Abwehr von Bedrohungen und wird von Check Point ThreatCloud™ unterstützt, der weltweit leistungsstärksten Bedrohungsintelligenz, um die höchste Bedrohungsabwehrrate auf dem Markt zu liefern.

Schnellste Wiederherstellung

Automatisierung von 90 % der Aufgaben zur Erkennung, Untersuchung und Behebung von Angriffen

- **Automatisierte Eindämmung und Behebung von Angriffen:** die einzige Lösung für Endgeräteschutz, die die gesamte Cyber-Kill-Chain automatisch und vollständig beseitigt. Sobald ein Angriff erkannt wurde, kann das infizierte Gerät automatisch unter Quarantäne gestellt werden, um eine Bewegung der lateralen Infektion zu verhindern und wieder einen sicheren Zustand herzustellen.
- **Automatisch generierte forensische Berichte:** detaillierte Sichtbarkeit infizierter Assets, Angriffsfluss, Korrelation mit dem MITRE ATT&CK™-Framework. Die Forensics-Funktion überwacht und zeichnet automatisch Endgeräteereignisse auf, einschließlich betroffener Dateien, gestarteter Prozesse, Systemregistrierungsänderungen und Netzwerkaktivitäten, und erstellt einen detaillierten forensischen Bericht. Robuste Angriffsdiagnosen und Transparenz unterstützen Abhilfemaßnahmen und ermöglichen es Systemadministratoren und Incident-Response-Teams, Angriffe effektiv zu diagnostizieren und zu beheben.

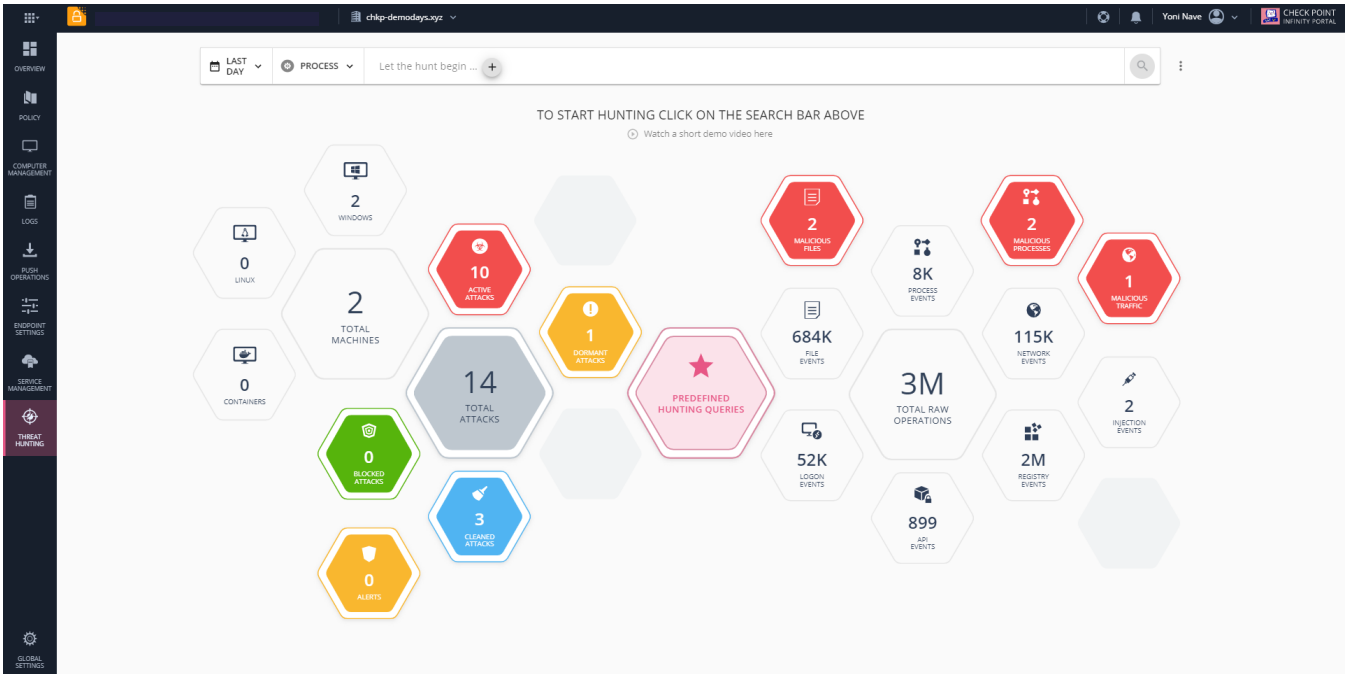


Harmony Endpoint Forensischer Bericht

„Der größte Vorteil der Verwendung von Check Point Harmony Endpoint ist, dass wir uns keine Gedanken über Ransomware-Angriffe auf unsere Umgebung machen müssen. Es bietet absolute Sicherheit und die ist unbezahlbar. Wir wissen, dass unsere Daten sicher bleiben."

David Ulloa, Chief Information Security Officer, IMC Companies

- **Threat Hunting:** Basierend auf unternehmensweiter Sichtbarkeit, ergänzt durch global geteilte Bedrohungsdaten von Hunderten von Millionen von Sensoren, erfasst durch ThreatCloud™. Mit der Threat Hunting-Funktion können Sie Abfragen festlegen oder vordefinierte verwenden, um verdächtige Vorfälle zu identifizieren und zu untersuchen und manuelle Abhilfemaßnahmen zu ergreifen.

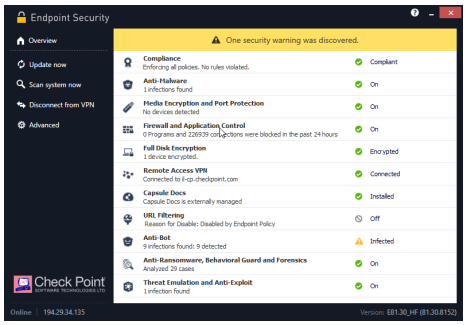


Harmony Endpoint – Bedrohungssuche

> *„Seit wir Harmony Endpoint implementiert haben, hatten wir in fast einem Jahr keinen einzigen fortgeschrittenen Malware- oder Ransomware-Vorfall.“*
> Russell Walker, Chief Technology Officer, Secretary of State von Mississippi

Beste Gesamtbetriebskosten

Der Schutz für Endgeräte, den Sie benötigen, in einer einzigen, effizienten und kostengünstigen Lösung



Ein einziger, einheitlicher Anbieter für EPP-, EDR-, VPN-, NGAV-, Daten- und Web-Browsing-Schutz, damit Ihr Unternehmen Prozesse rationalisieren und die Gesamtbetriebskosten senken kann.

Volle Flexibilität, um Ihre spezifischen Sicherheits- und Compliance-Anforderungen zu erfüllen.

- Harmony Endpoint wird entweder vor Ort oder über einen Cloud-Service verwaltet und bietet einfach zu bedienende, robuste Funktionalität und schnelle Bereitstellung, um Ihre Anforderungen zu erfüllen
- Unterstützt Windows, macOS, Linux-Betriebssysteme
- VDI-Fähigkeit (Desktop-Instanz-Emulation auf einem Remote-Server), Unterstützung von VMWare Horizon, Citrix PVS/MCS
- Der kürzlich aktualisierte Harmony Endpoint Installer ermöglicht nahtlose Upgrades und Rollbacks ohne Neustarts oder Unterbrechungen für Endnutzer.
- Unterstützung des Entwicklerschutzes – zum Schutz von Entwicklern ohne Integration der kontinuierlichen Integration/kontinuierlichen Bereitstellung (CI/CD) oder integrierten Entwicklungsumgebung (IDE).

Bauen Sie auf Check Point Infinity auf, der ersten konsolidierten Sicherheitsarchitektur, die entwickelt wurde, um die Komplexität der wachsenden Konnektivität und unzureichenden Sicherheit zu lösen und umfassenden Schutz und Bedrohungsinformationen über Netzwerke, Clouds, Endgeräte, Mobilgeräte und das IoT zu liefern.

CHECK POINT INFINITY

> *„Check Point Harmony Endpoint – der einzige erweiterte Endgeräteschutz. Harmony Endpoint war für uns der am besten geeignete erweiterte Schutz für Endgeräte. Er wurde schnell in unserer weltweiten Organisation eingesetzt. Die Management-Konsole verfügt über eine intuitive Benutzeroberfläche und ist einfach zu bedienen“*
>
> Sr. Sicherheitsanalyst, großes globales Infrastrukturunternehmen

Technische Daten

HARMONY ENDPOINT VERPACKUNGEN	
Pakete	• **Datenschutz –** umfasst vollständige Festplattenverschlüsselung und Verschlüsselung von Wechseldatenträgern, einschließlich Access Control und Port Protection • **Harmony Endpoint Basic –** umfasst Anti-Malware, Anti-Ransomware, Zero-Day-Phishing, Advanced Threat Prevention und Endpoint Detection and Response (EDR) • **Harmony Endpoint Advanced –** umfasst Harmony Endpoint Basic sowie Threat Emulation und Threat Extraction • **Harmony Endpoint Complete –** umfasst Harmony Endpoint Advanced plus Datensicherheit (Full Disk und Media Encryption) **Hinweis: Endpoint Compliance** wird mit allen Paketen geliefert
BETRIEBSSYSTEME	
Betriebssystem	• Windows Workstation 7, 8 und 10 • Windows Server 2008 R2, 2012, 2012 R2, 2016 • MacOS Sierra 10.12.6, MacOS High Sierra 10.13.4 (Threat Emulation, Threat Extraction, Anti- Ransomware, Chrome für Mac Browser-Erweiterung)
Inhaltsentschärfung und -rekonstruktion (CDR) über E-Mail und Web	
Threat Extraction	Entfernt ausnutzbare Inhalte, rekonstruiert Dateien, um potenzielle Bedrohungen zu eliminieren, und liefert den Benutzern in wenigen Sekunden bereinigte Inhalte
Threat Emulation	• Sandboxing-Funktion für Bedrohungen, um neue, unbekannte Malware und gezielte Angriffe in E-Mail-Anhängen, heruntergeladenen Dateien und URLs auf Dateien in E-Mails zu erkennen und zu blockieren. • Bietet Schutz für eine Vielzahl von Dateitypen, einschließlich MS Office, Adobe PDF, Java, Flash, ausführbare Dateien und Archive sowie mehrere Windows-Betriebssystemumgebungen. • Erkennt Bedrohungen, die in SSL- und TLS-verschlüsselter Kommunikation versteckt sind.
Zentralisierte Verwaltung	
Cloud- und On-Prem-Management	• Harmony Service (gehostet auf der Check Point-Cloud) • Harmony Appliance (gehostet vor Ort)
NGAV: Laufzeiterkennung und -schutz	
Anit-Ransomware	• Bedrohungsprävention – überwacht ständig auf Ransomware-spezifisches Verhalten und identifiziert eine illegitime Dateiverschlüsselung ohne Signatur. • Erkennung und Quarantäne – Alle Elemente eines Ransomware-Angriffs werden durch forensische Analyse identifiziert und dann unter Quarantäne gestellt. • Datenwiederherstellung – Verschlüsselte Dateien werden automatisch aus Snapshots wiederhergestellt, um eine vollständige Geschäftskontinuität zu gewährleisten.
Anit-Exploit	• Bietet Schutz vor Exploit-basierten Angriffen, die legitime Anwendungen kompromittieren, und stellt sicher, dass diese Schwachstellen nicht genutzt werden können. • Erkennt Exploits, indem verdächtige Speichermanipulationen während der Laufzeit identifiziert werden. • Beendet den ausgenutzten Prozess, sobald er erkannt wird, und behebt die gesamte Angriffskette
Behavioral Guard	• Erkennt und blockiert Malware-Mutationen entsprechend ihrem Echtzeitverhalten. • Identifiziert, klassifiziert und blockiert Malware-Mutationen in Echtzeit, basierend auf minimalen Ähnlichkeiten der Prozessausführungsstruktur.
Webschutz	
Zero-Phishing	• Echtzeitschutz vor unbekannten Phishing-Websites • Statische und heuristische Erkennung verdächtiger Elemente auf Websites, die private Informationen anfordern
Schutz von Unternehmensanmeldeinformationen	Erkennung der Wiederverwendung von Unternehmensanmeldeinformationen auf externen Websites
URL Filterung	• Leichtes Browser-Plugin, Zugriff auf Websites in Echtzeit zulassen/verweigern • Unternehmensrichtlinien für sicheres Internet für Benutzer innerhalb/außerhalb des Unternehmensgeländes durchsetzen, Einhaltung von Vorschriften durchsetzen, Unternehmensproduktivität verbessern • Vollständige Transparenz für HTTPS-Datenverkehr
THREAT HUNTING	
Threat Hunting	Erfassung aller unformatierten und erkannten Ereignisse auf Endgeräten, wodurch erweiterte Abfragen, Drilldowns und Pivots für die proaktive Bedrohungssuche und tiefgreifende Untersuchung der Vorfälle ermöglicht werden

Warum Harmony Endpoint?

Heutzutage spielt Endgerätesicherheit eine entscheidende Rolle bei der Ermöglichung von Remote-Arbeit. Da 70 % der Cyber-Angriffe auf Endgeräten beginnen, ist ein vollständiger Schutz von Endgeräten auf höchstem Sicherheitsniveau entscheidend, um Sicherheitsverstöße und Datenverletzungen zu vermeiden.

Harmony Endpoint ist eine umfassende Sicherheitslösung für Endgeräte, die Remote-Mitarbeiter vor der komplexen Bedrohungslandschaft von heute schützt. Es verhindert unmittelbare Bedrohungen für Endgeräte wie Ransomware, Phishing oder Drive-by-Malware und minimiert gleichzeitig die Auswirkungen von Sicherheitsverletzungen durch autonome Erkennung und Reaktion.

Auf diese Weise erhalten die Endgeräte Ihres Unternehmens in einer einzigen, effizienten und kostengünstigen Lösung den gesamten Schutz, den es benötigt, in der Qualität, die es verdient.

Harmony Endpoint ist Teil der Check Point Harmony-Produktsuite, einer branchenweit ersten einheitlichen Sicherheitslösung für Benutzer, Geräte und Zugriff. Harmony vereint sechs Produkte für kompromisslose Sicherheit und Anwenderfreundlichkeit. Geräte und Internetverbindungen werden vor den raffiniertesten Angriffen geschützt. Gleichzeitig wird ein Zero-Trust-Zugang zu Unternehmensanwendungen gewährleistet – alles in einer einzigen Lösung, die einfach in der Bedienung, der Verwaltung und in der Anschaffung ist.

Erfahren Sie mehr: https://www.checkpoint.com/products/advanced-endpoint-protection/

Headquarter (weltweit)
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: +972 3-753-4555 | Fax: 972-3-624-1100 | E-Mail: 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