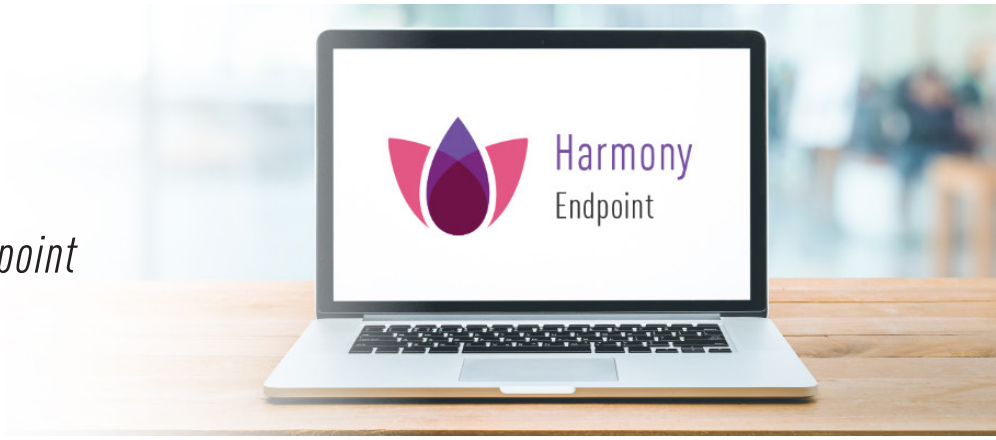
CHECK POINT

Harmony Endpoint

Tutta la protezione per gli endpoint di cui hai bisogno



Harmony Endpoint è una soluzione completa per la sicurezza degli endpoint creata per proteggere il personale remoto dal complesso panorama delle minacce odierne. Previene le minacce più imminenti sugli endpoint, come ransomware, phishing o malware drive-by, riducendo al minimo l'impatto della violazione con il rilevamento e la risposta autonomi.

In questo modo, la tua organizzazione ottiene tutta la protezione necessaria per gli endpoint, con la qualità che merita, in un'unica soluzione efficiente ed economica.

VANTAGGI PRINCIPALI DEL PRODOTTO

Protezione completa degli endpoint: prevenzione delle minacce più imminenti sugli endpoint

Ripristino più rapido: 90% di automazione delle attività di rilevamento, indagine e correzione degli attacchi

Migliore TCO: tutta la protezione per gli endpoint di cui hai bisogno, in un'unica soluzione efficiente ed economica

FUNZIONALITÀ ESCLUSIVE DEL PRODOTTO

Gli algoritmi avanzati di analisi comportamentale e apprendimento automatico arrestano il malware prima che provochi danni

I tassi di cattura elevati e i bassi falsi positivi garantiscono sicurezza e prevenzione efficaci

L'analisi dei dati forensi automatizzata offre informazioni dettagliate sulle minacce

Contenimento completo degli attacchi e correzione per ripristinare rapidamente qualsiasi sistema infetto

Soluzione per la sicurezza degli endpoint leader di mercato

Harmony Endpoint è stato riconosciuto come prodotto di punta nella protezione degli endpoint aziendali da AV-TEST

PER SAPERNE DI PIÙ

Forrester Wave attribuisce a Check Point il riconoscimento di leader nella sicurezza degli endpoint

PER SAPERNE DI PIÙ

Harmony Endpoint di Check Point ha ottenuto la valutazione prodotto AA durante il test di protezione avanzata degli endpoint di NSS Labs 2020

PER SAPERNE DI PIÙ

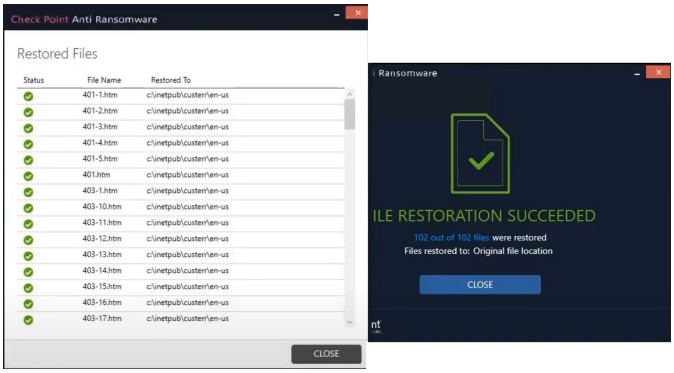
Come funziona

Protezione completa degli endpoint

Prevenzione delle minacce più imminenti sugli endpoint

- **Blocca il malware** proveniente dalla navigazione web o dagli allegati e-mail prima che raggiunga l'endpoint, senza influire sulla produttività degli utenti. Ogni file ricevuto via e-mail o scaricato da un utente tramite un browser web viene inviato alla sandbox di emulazione delle minacce per verificare la presenza di malware. I file possono anche essere ripuliti attraverso un processo di estrazione delle minacce (tecnologia di disarmo e ricostruzione dei contenuti) per fornire contenuti sicuri e puliti in pochi millesimi di secondi

- **Ottieni una protezione runtime contro ransomware, malware e attacchi file-less, con una correzione immediata e completa,** anche in modalità offline. Una volta rilevata un'anomalia o un comportamento dannoso, Endpoint Behavioral Guard blocca e corregge l'intera catena di attacco senza lasciare tracce dannose. L'anti-ransomware identifica i comportamenti ransomware come la crittografia dei file o i tentativi di compromissione dei file di backup del sistema operativo e ripristina automaticamente i file crittografati dal ransomware in modo sicuro. Harmony Endpoint utilizza un unico spazio a volta locale sul computer, accessibile solo ai processi con firma Check Point. Nel caso in cui il malware tenti di eseguire l'eliminazione di una copia shadow, il computer non perderà nessun dato.



- **Protezione contro il phishing** - Previeni il furto di credenziali con la tecnologia Zero-Phishing® che identifica e blocca l'utilizzo dei siti di phishing in tempo reale. I siti vengono ispezionati e, se ritenuti dannosi, l'utente non potrà inserire le credenziali. Zero-phishing® protegge anche da siti di phishing precedentemente sconosciuti e dal riutilizzo delle credenziali aziendali.

Il miglior tasso di rilevamento di malware noti e zero-day del settore

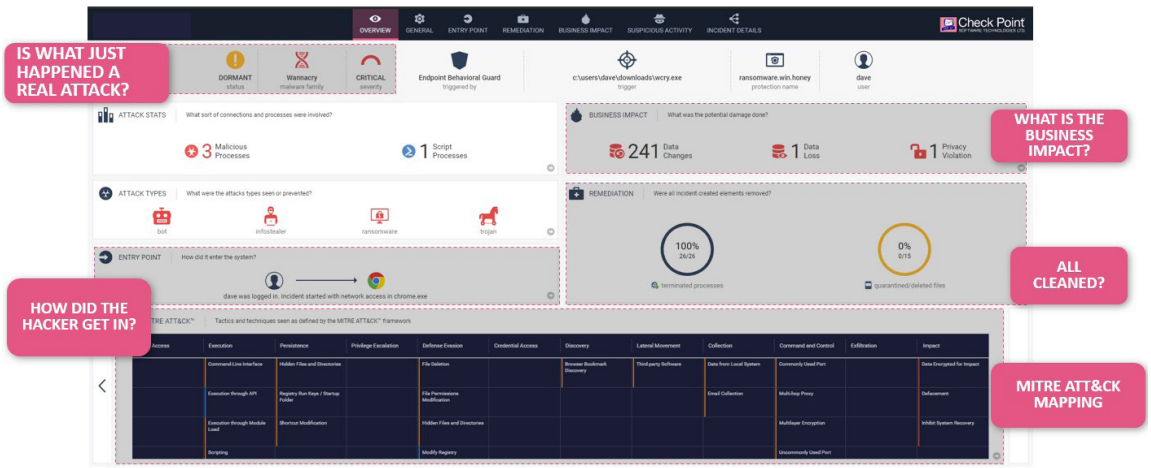
Leader riconosciuto del settore, come si evince dai test di laboratorio AV-TEST Corporate Endpoint Protection e NSS Advanced Endpoint Protection del 2020, Harmony Endpoint è potenziato da oltre 60 motori di prevenzione delle minacce e alimentato da Check Point ThreatCloud™, la più potente intelligence sulle minacce al mondo, per offrire il più alto tasso complessivo di cattura delle minacce sul mercato.

Ripristino più veloce

90% di automazione delle attività di rilevamento, indagine e correzione degli attacchi

- **Contenimento e correzione automatizzati degli attacchi:** l'unica soluzione di protezione per gli endpoint che corregge automaticamente e totalmente l'intera catena cyber kill. Una volta rilevato un attacco, il dispositivo infetto può essere messo automaticamente in quarantena per prevenire movimenti laterali di infezione ed essere ripristinato a uno stato di sicurezza.

- **Report forensi generati automaticamente:** forniscono una visibilità dettagliata delle risorse infette, flusso di attacco, correlazione con il framework MITRE ATT&CK™. La funzionalità Forensics monitora e registra automaticamente gli eventi degli endpoint, inclusi i file interessati, i processi avviati, le modifiche al registro di sistema e all'attività di rete, e crea un rapporto forense dettagliato. La solida diagnostica degli attacchi e la visibilità supportano gli interventi di correzione, consentendo agli amministratori di sistema e ai team di risposta agli incidenti di classificare e risolvere gli attacchi in modo efficace.

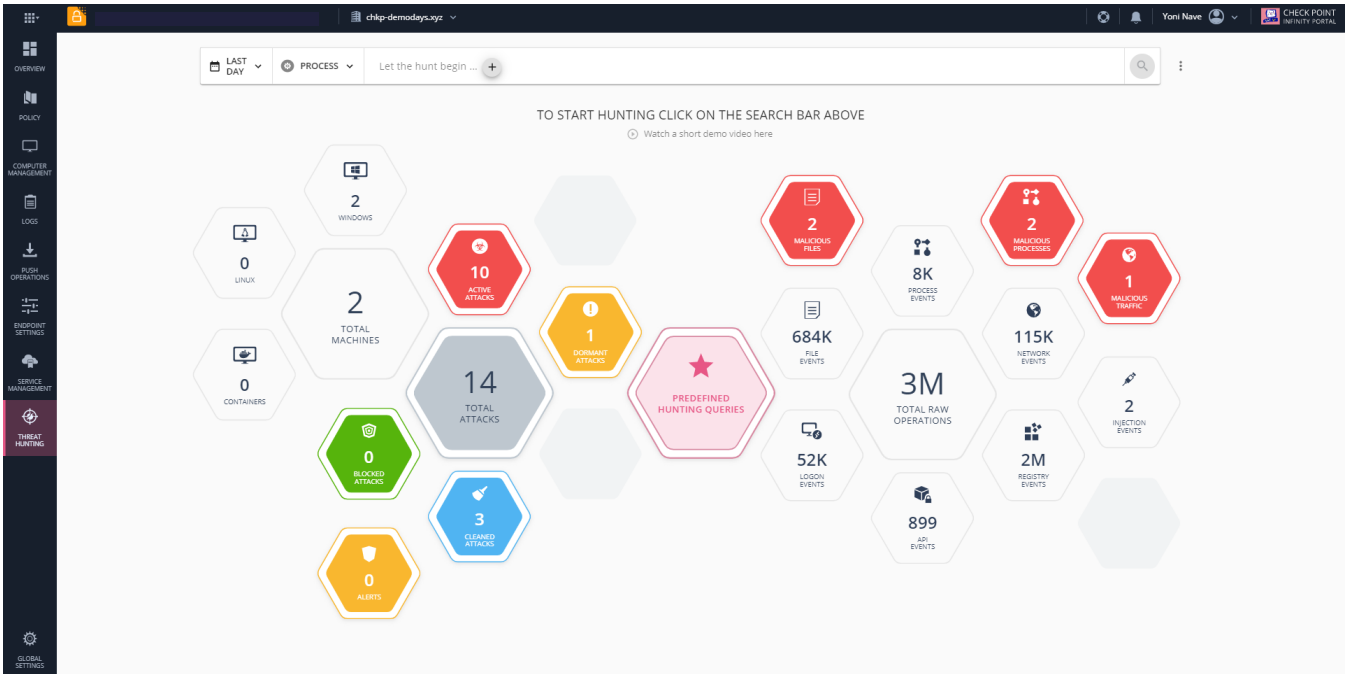


Rapporto forense di Harmony Endpoint

"Il vantaggio principale di Harmony Endpoint di Check Point è che non dobbiamo preoccuparci degli attacchi ransomware che colpiscono il nostro ambiente. Garantisce la massima tranquillità, e questo non ha prezzo. Sappiamo che sarà pronto a proteggere i nostri dati e farci sentire al sicuro."

David Ulloa, Direttore della sicurezza delle informazioni, IMC Companies

- **Threat Hunting:** è alimentata dalla visibilità a livello aziendale e potenziata dall'intelligence sulle minacce condivisa a livello globale da centinaia di milioni di sensori, raccolti da ThreatCloud™. Con la funzionalità Threat Hunting, è possibile impostare query o utilizzare quelle predefinite per identificare ed esaminare in dettaglio incidenti sospetti e intraprendere azioni correttive manuali.

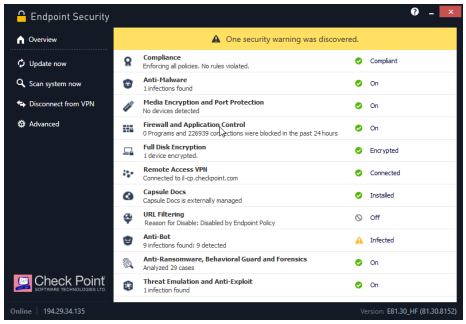


Harmony Endpoint - Threat Hunting

> *"Da quando abbiamo implementato Harmony Endpoint, non abbiamo riscontrato nemmeno un incidente di malware o ransomware avanzato in quasi un anno."*
> Russell Walker, Responsabile della tecnologia, Segretario di Stato del Mississippi

Il migliore costo di gestione per un'azienda

Tutta la protezione per gli endpoint di cui hai bisogno in un'unica soluzione efficiente ed economica



Un agente unico e unificato per la protezione EPP, EDR, VPN, NGAV, dati e navigazione web, in modo che la tua organizzazione possa semplificare i processi e ridurre il TCO.

Massima flessibilità per soddisfare i requisiti specifici di sicurezza e conformità.

- Harmony Endpoint è gestito localmente o sul cloud e offre funzionalità solide e facili da utilizzare, nonché un'implementazione rapida per soddisfare le tue esigenze
- Supporta i sistemi operativi Windows, macOS e Linux
- Funzionalità VDI (emulazione di istanza desktop su un server remoto), supporto di VMWare Horizon, Citrix PVS/MCS
- L'Harmony Endpoint Installer aggiornato di recente consente aggiornamenti senza interruzioni, rollback senza riavvii o interruzioni per gli utenti finali.
- Supporto per la protezione degli sviluppatori: per aiutare a proteggere gli sviluppatori senza introdurre un'integrazione continua/recapito continuo (CI/CD) o un ambiente di sviluppo integrato (IDE).

Si basa su Check Point Infinity, la prima architettura di sicurezza consolidata, progettata per risolvere le complessità della crescente connettività e della sicurezza inadeguata che offre protezione completa e intelligence sulle minacce su reti, cloud, endpoint, dispositivi mobili e IoT.

CHECK POINT INFINITY

> *"Harmony Endpoint di Check Point: l'unica e sola protezione avanzata per gli endpoint. Harmony Endpoint ha rappresentato per noi la migliore protezione avanzata per endpoint. È stato implementato rapidamente all'interno della nostra organizzazione in tutto il mondo. La console di gestione è dotata di un'interfaccia intuitiva e facile da usare"*
>
> Analista di sicurezza senior, grande impresa di infrastrutture globale

Specifiche tecniche

PACCHETTI HARMONY ENDPOINT	
Pacchetti	• **Protezione dei dati:** include la crittografia dell'intero disco e dei supporti rimovibili, tra cui il controllo degli accessi e la protezione delle porte • **Harmony Endpoint Basic:** include anti-malware, anti-ransomware, phishing zero-day, prevenzione avanzata delle minacce e rilevamento e risposta agli endpoint (EDR) • **Harmony Endpoint Advanced:** include Harmony Endpoint Basic, più Threat Emulation e Threat Extraction • **Harmony Endpoint Complete:** include Harmony Endpoint Advanced, più Data Security (crittografia completa del disco e dei supporti) **Nota: Endpoint Compliance** viene fornito con tutti i pacchetti
SISTEMI OPERATIVI	
Sistema operativo	• Windows Workstation 7, 8 e 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, Estensione del browser Chrome per Mac)
Disarmo e ricostruzione dei contenuti (CDR) tramite e-mail e web	
Threat Extraction	Rimuove i contenuti sfruttabili, ricostruisce i file per eliminare potenziali minacce e fornisce contenuti ripuliti agli utenti in pochi secondi
Threat Emulation	• Capacità di sandboxing contro le minacce per rilevare e bloccare malware nuovi e sconosciuti e attacchi mirati trovati negli allegati e-mail, nei file scaricati e negli URL dei file contenuti nelle e-mail. • Fornisce protezione su una vasta gamma di tipi di file, tra cui MS Office, Adobe PDF, Java, Flash, in formato eseguibile e archivio, nonché su più ambienti di sistemi operativi Windows. • Individua le minacce nascoste nelle comunicazioni crittografate SSL e TLS.
Gestione centralizzata	
Gestione cloud e locale	• Harmony Service (ospitato sul cloud Check Point) • Harmony Appliance (ospitato in modalità locale)
NGAV: Rilevamento e protezione runtime	
Anti-ransomware	• Prevenzione delle minacce: monitora costantemente il comportamento specifico del ransomware e identifica la crittografia illegittima dei file, riducendo la firma. • Rilevamento e quarantena: tutti gli elementi di un attacco ransomware vengono identificati mediante analisi forense e quindi messi in quarantena. • Ripristino dei dati: i file crittografati vengono ripristinati automaticamente dalle snapshot per garantire la continuità aziendale completa.
Anti-exploit	• Fornisce protezione contro gli attacchi basati su exploit che compromettono le applicazioni legittime, garantendo l'inutilizzo di tali vulnerabilità. • Rileva gli exploit identificando le manipolazioni di memoria sospette in fase di runtime. • Chiude il processo sfruttato quando ne rileva uno, corregge l'intera catena di attacco
Behavioral Guard	• Rileva e blocca in modo adattivo le mutazioni malware in base al loro comportamento in tempo reale. • Identifica, classifica e blocca le mutazioni del malware in tempo reale in base alle somiglianze minime con l'albero di esecuzione del processo.
Protezione Web	
Zero-Phishing	• Protezione in tempo reale da siti di phishing sconosciuti • Rilevamento statico ed euristico di elementi sospetti nei siti web che richiedono informazioni private
Protezione delle credenziali aziendali	Rilevamento del riutilizzo delle credenziali aziendali in siti esterni
Filtraggio URL	• Plug-in leggero per browser, consente/blocca l'accesso ai siti web in tempo reale • Applica i criteri dell'organizzazione per una connessione Internet sicura a beneficio degli utenti che lavorano in sede e fuori sede, è conforme alle normative, migliora la produttività dell'organizzazione • Visibilità completa del traffico HTTPS
THREAT HUNTING	
Threat Hunting	Raccolta di tutti gli eventi non elaborati e rilevati sull'endpoint, consente query avanzate, drill-down e pivoting per la ricerca proattiva delle minacce e un'indagine approfondita degli incidenti

Perché utilizzare Harmony Endpoint?

Oggi più che mai, la sicurezza degli endpoint riveste un ruolo fondamentale nell'abilitazione del personale remoto. Con il 70% degli attacchi informatici che si verificano sugli endpoint, la protezione completa degli endpoint al massimo livello di sicurezza è fondamentale per evitare violazioni della sicurezza e compromissione dei dati.

Harmony Endpoint è una soluzione completa per la sicurezza degli endpoint creata per proteggere il personale remoto dal complesso panorama delle minacce odierne. Previene le minacce più imminenti sugli endpoint, come ransomware, phishing, o malware drive-by, riducendo al minimo l'impatto della violazione con il rilevamento e la risposta autonomi.

In questo modo, la tua organizzazione ottiene tutta la protezione necessaria per gli endpoint, con la qualità che merita, in un'unica soluzione efficiente ed economica.

Harmony Endpoint fa parte della suite di prodotti Harmony di Check Point, la prima soluzione di sicurezza unificata del settore per utenti, dispositivi e accessi. Harmony consolida sei prodotti per fornire a tutti sicurezza e semplicità senza compromessi. Protegge i dispositivi e le connessioni Internet dagli attacchi più sofisticati garantendo al contempo l'accesso zero-trust alle applicazioni aziendali, il tutto in un'unica soluzione facile da usare, gestire e acquistare.

Maggiori informazioni su: https://www.checkpoint.com/products/advanced-endpoint-protection/

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

Headquarter Stati Uniti
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com