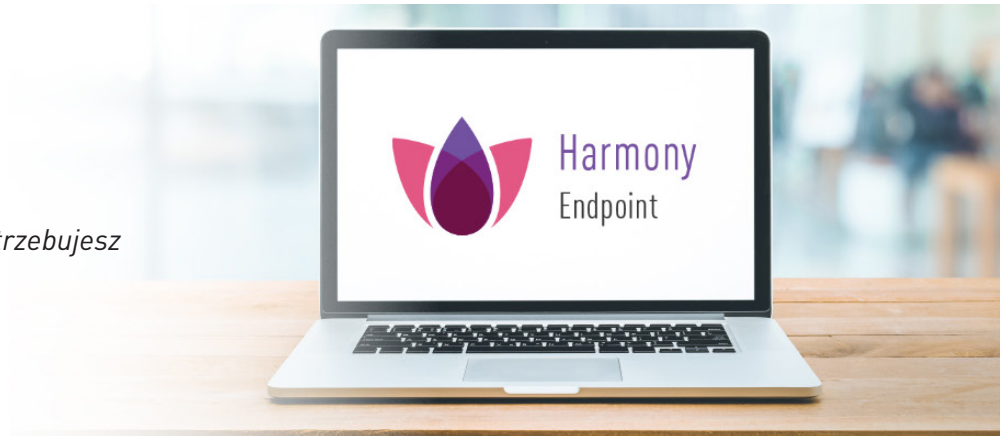
CHECK POINT

Harmony Endpoint

Ochrona punktów końcowych, której potrzebujesz



Harmony Endpoint to kompleksowe rozwiązanie do zabezpieczania punktów końcowych, stworzone w celu ochrony zdalnych pracowników przed dzisiejszym złożonym środowiskiem zagrożeń. Zapobiega bezpośrednim zagrożeniom, takim jak oprogramowanie ransomware, phishing lub złośliwe oprogramowanie typu drive-by, jednocześnie szybko minimalizując wpływ naruszeń poprzez autonomiczne wykrywanie i reagowanie.

W ten sposób cała organizacja otrzymuje pełną ochronę punktów końcowych, której potrzebuje – w jakości, na jaką zasługuje, w postaci jednego, wydajnego i opłacalnego rozwiązania.

NAJWAŻNIEJSZE ZALETY

Pełna ochrona punktów końcowych:
zapobieganie najbardziej bezpośrednim zagrożeniom, jakie dotykają punktów końcowych

Najszybsze odzyskiwanie:
automatyzacja 90% zadań związanych z wykrywaniem i badaniem ataków oraz usuwaniem ich skutków

Najlepszy całkowity koszt posiadania (TCO):
kompleksowa ochrona punktów końcowych w postaci jednego, wydajnego i opłacalnego rozwiązania

UNIKATOWE MOŻLIWOŚCI

Zaawansowana analiza behawioralna i algorytmy uczenia maszynowego neutralizują złośliwe oprogramowanie, zanim wyrządzi ono szkody.

Wysoka wykrywalność i niski współczynnik fałszywych alarmów (false-positive) zapewnia skuteczną i wydajną ochronę.

Zautomatyzowane raporty „Forensics" oferują szczegółowy wgląd w wykryte zagrożenia.

Całkowite powstrzymywanie wykonywanych ataków i usuwanie ich skutków w celu szybkiego przywracania sprawności zainfekowanych systemów.

Najlepsze na rynku rozwiązanie do ochrony punktów końcowych

APPROVED CORPORATE ENDPOINT PROTECTION WINDOWS TOP PRODUCT
AV-TEST av-test.org 04/2021

Harmony Endpoint uznany przez AV-TEST jako „Top Product" w kategorii korporacyjnej ochrony punktów końcowych.

DOWIEDZ SIĘ WIĘCEJ

MITRE ENGENUITY
A Foundation for Public Good

Oceny MITRE ATT&CK® podkreślają czołową pozycję firmy Check Point w dziedzinie bezpieczeństwa punktów końcowych.

DOWIEDZ SIĘ WIĘCEJ

AA
NSS Labs

Check Point Harmony Endpoint uzyskało ocenę AA w badaniu 2020 Advanced Endpoint Protection Test firmy NSS Labs.

DOWIEDZ SIĘ WIĘCEJ

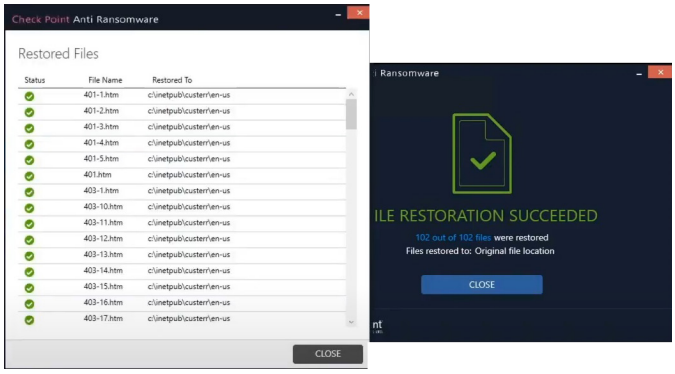
Jak to działa?

Kompleksowa ochrona punktów końcowych

Zapobieganie najbardziej bezpośrednim zagrożeniom na punktach końcowych

- **Blokowanie złośliwego oprogramowania** pochodzącego z przeglądanych witryn internetowych lub załączników e-mail, zanim dotrze do punktu końcowego – bez wpływu na produktywność użytkowników. Każdy plik otrzymany za pośrednictwem poczty elektronicznej lub pobierany przez użytkownika przy użyciu przeglądarki jest wysyłany do środowiska Threat Emulation (Sandbox) w celu sprawdzenia pod kątem obecności złośliwego oprogramowania.
Pliki można również oczyszczać za pomocą funkcji Threat Extraction (technologia Content Disarm & Reconstruction), aby dostarczać bezpieczne treści w czasie liczonym w milisekundach.

- **Ochrona wczasie rzeczywistym przed ransomware, złośliwym oprogramowaniem i atakami typu file-less – wraz z natychmiastowym i pełnym usuwaniem ich skutków**, nawet w trybie offline. Po wykryciu anomalii lub złośliwego zachowania Endpoint Behavioral Guard blokuje cały łańcuch ataku oraz usuwa wszystkie jego ślady i skutki. Moduł Anti-Ransomware wykrywa szkodliwą aktywność ransomware, w tym szyfrowanie plików lub próby naruszenia kopii zapasowych systemu operacyjnego, a także bezpiecznie i automatycznie przywraca pliki zaszyfrowane przez ransomware.



Harmony Endpoint wykorzystuje unikatową wydzieloną przestrzeń lokalną na komputerze, do której dostęp mają tylko procesy podpisane przez Check Point – w przypadku gdy złośliwe oprogramowanie spróbuje usunąć kopię zapasową, żadne dane nie zostaną utracone.

Ochrona przed phishingiem zapobiega kradzieży poświadczeń dzięki technologii Zero-Phishing ®, która wykrywa i blokuje korzystanie z witryn phishingowych w czasie rzeczywistym.
Witryny są aktywnie skanowane, a jeśli zostaną uznane za złośliwe, użytkownik nie będzie mógł wprowadzić w nich swoich danych i poświadczeń. Zero-phishing® chroni nawet przed nieznanymi wcześniej witrynami phishingowymi i ponownym wykorzystaniem poświadczeń firmowych.

Najlepszy w branży wskaźnik wykrywania zarówno znanych zagrożeń, jak i zagrożeń zero-day

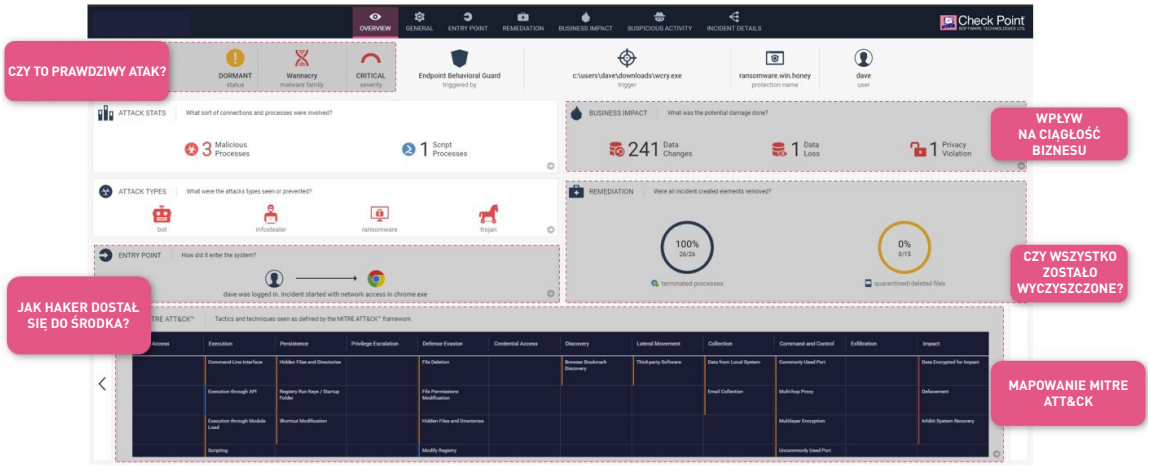
Harmony Endpoint, rozwiązanie czołowe w branży według badań AV-TEST Corporate Endpoint Protection oraz NSS Advanced Endpoint Protection z 2020 roku, korzysta z ponad 60 silników zapobiegających zagrożeniom oraz z Check Point ThreatCloud™ – najpotężniejszej na świecie usługi threat intelligence, która zapewnia najwyższy ogólny wskaźnik wykrywalności zagrożeń na rynku.

Najszybsze odzyskiwanie

Automatyzacja 90% zadań związanych z wykrywaniem i badaniem ataków oraz usuwaniem ich skutków

- **Automatyczne powstrzymywanie ataków i usuwanie ich skutków**: jedyne rozwiązanie do ochrony punktów końcowych, które automatycznie i kompleksowo usuwa skutki całego łańcucha cyberataku. Po wykryciu ataku zainfekowane urządzenie może zostać automatycznie poddane kwarantannie, aby zapobiec rozprzestrzenianiu się infekcji, a następnie przywrócone do bezpiecznego stanu.

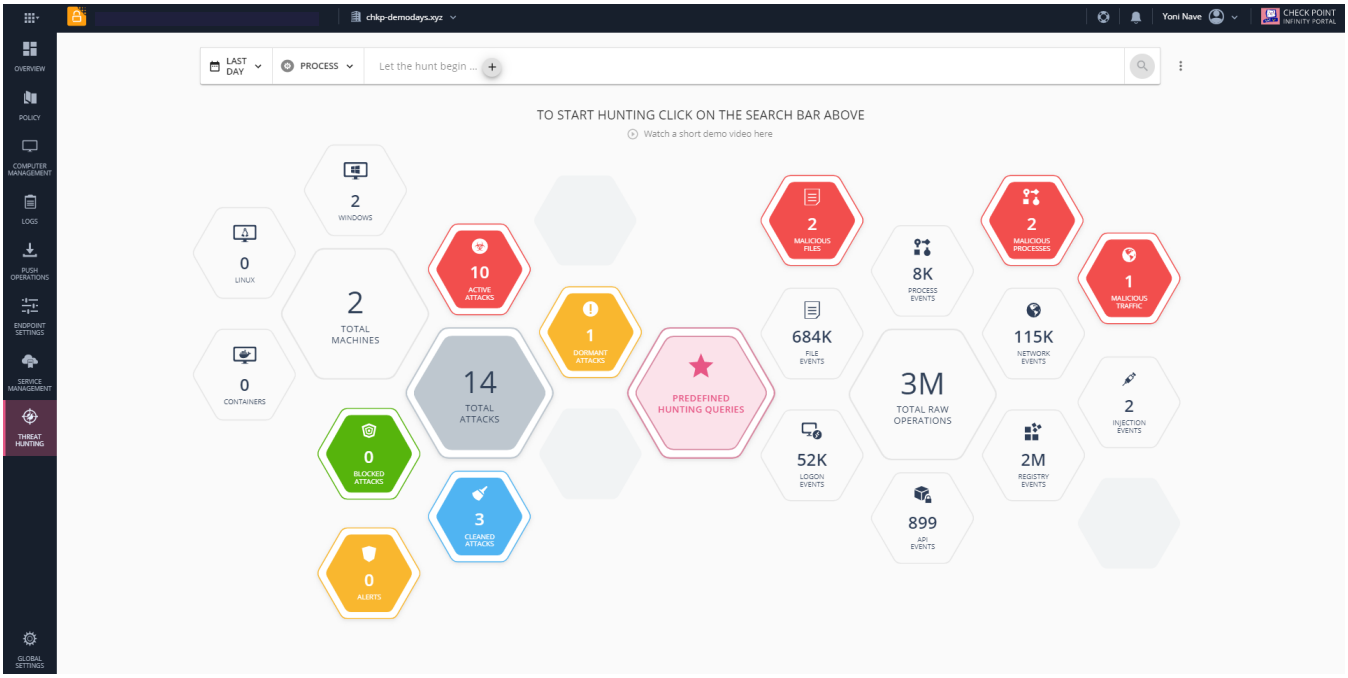
- **Automatycznie generowane raporty typu forensic**: zapewniają szczegółowy wgląd w zainfekowane zasoby, przebieg ataków oraz korelację z MITRE ATT&CK™ Framework. Proces Forensics automatycznie monitoruje i rejestruje zdarzenia na punktach końcowych, w tym naruszone pliki, uruchomione procesy, zmiany w rejestrze systemu i aktywność sieciową, a następnie tworzy szczegółowy raport typu forensic. Niezawodna diagnostyka ataków i widoczność wspierają działania naprawcze, umożliwiając administratorom systemu i zespołom SOC skuteczne podejmowanie działań.



Harmony Endpoint Forensic Report

> *„Największą zaletą korzystania z Check Point Harmony Endpoint jest to, że nie musimy się martwić o ataki ransomware na nasze środowisko. Rozwiązanie zapewnia całkowity spokój, który nie sposób przeliczyć na pieniądze. Wiemy, że zawsze nas ochroni i że nasze dane będą bezpieczne".*
>
> David Ulloa, główny specjalista ds. bezpieczeństwa informacji, IMC Companies

- **Threat Hunting:** to proces oparty na widoczności całego przedsiębiorstwa i wzbogacony o globalnie współdzielone dane na temat zagrożeń, zebrane przez ThreatCloud™ z setek milionów sensorów. Threat Hunting pozwala tworzyć zapytania lub korzystać z predefiniowanych zapytań, aby wykrywać i analizować podejrzane incydenty oraz podejmować ręczne działania naprawcze.



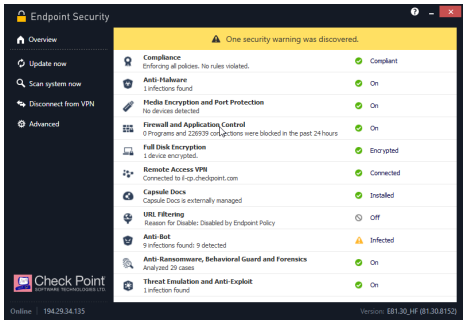
Harmony Endpoint – Threat Hunting

> *„Odkąd wdrożyliśmy Harmony Endpoint, od blisko roku nie mieliśmy ani jednego zaawansowanego złośliwego oprogramowania oraz ani jednego incydentu związanego z oprogramowaniem ransomware".*
>
> Russell Walker, dyrektor ds. technicznych, biuro Sekretarza Stanu Missisipi

Najlepszy całkowity koszt posiadania (TCO)

Kompleksowa ochrona punktów końcowych w postaci jednego, wydajnego i opłacalnego rozwiązania

Jeden ujednolicony agent, który zawiera: EPP, EDR, VPN, NGAV, ochronę danych i przeglądania witryn internetowych sprawia, że cała organizacja może usprawnić procesy i zmniejszyć całkowity koszt posiadania (TCO).



Pełna elastyczność pozwala spełnić wymagania organizacji w zakresie bezpieczeństwa i zgodności ze standardami compliance.

- Zarządzanie lokalnie lub z konsoli chmurowej sprawia, że Harmony Endpoint zapewnia łatwą obsługę, solidną funkcjonalność i szybkie wdrożenie.
- Wsparcie dla systemów z rodziny Windows, macOS, Linux
- Wsparcie dla VDI, -obsługa VMWare Horizon, Citrix PVS/MCS
- Zaktualizowany Harmony Endpoint Installer umożliwia bezproblemowe aktualizacje, rollbacki bez restartów lub zakłóceń dla użytkowników końcowych.
- Moduł Developer Protection – zapewnia ochronę bez konieczności stosowania praktyki ciągłej integracji/ciągłego wdrażania (CI/CD) lub zintegrowanego środowiska programistycznego (IDE).

Wykorzystaj potencjał Check Point Infinity, pierwszej skonsolidowanej architektury bezpieczeństwa zaprojektowanej w celu rozwiązania problemów rosnącej skali łączności i niewystarczających zabezpieczeń. Ujednolicona konsola chmurowa zapewnia pełną ochronę i analizę zagrożeń w sieciach, chmurach, punktach końcowych, urządzeniach mobilnych i IoT.

CHECK POINT INFINITY

> *„Check Point Harmony Endpoint to najlepsze rozwiązanie do zaawansowanej ochrony punktów końcowych. W naszym przypadku okazał się najlepiej dopasowanym produktem zabezpieczającym, który szybko wdrożyliśmy w naszej ogólnoświatowej organizacji. Konsola zarządzania ma intuicyjny interfejs użytkownika i jest łatwa w obsłudze”.*
>
> Starszy analityk ds. bezpieczeństwa w dużym globalnym przedsiębiorstwie infrastrukturalnym

Dane techniczne

PAKIETY HARMONY ENDPOINT	
Pakiety	• **Data Protection** – obejmuje moduły Full Disk Encryption i Removable Media Encryption oraz moduły Access Control i Port Protection • **Harmony Endpoint Basic** – obejmuje moduły Anti-Malware, Anti-Ransomware, Zero-day Phishing, Advanced Threat Prevention oraz Endpoint Detection and Response (EDR) • **Harmony Endpoint Advanced** – zawiera w sobie pakiet Harmony Endpoint Basic, a także dodatkowo moduły Threat Emulation i Threat Extraction • **Harmony Endpoint Complete** – zawiera w sobie pakiety Harmony Endpoint Advanced oraz Data Security (Full Disk and Media Encryption). Uwaga: moduł Endpoint Compliance jest zawarty we wszystkich pakietach.
SYSTEMY OPERACYJNE	
System operacyjny	• Windows 7, 8, 10 i 11 • Windows Server 2008 R2, 2012, 2012 R2, 2016, 2018, 2019, 2022 • MacOS Catalina 10.15, MacOS BigSur 11.x, MacOS Monterey 12, MacOS Ventura 13 • Linux Ubuntu (16.04, 18.04, 20.04), Debian (9.12-10.10), RHEL (7.8-8.4, CentOS (7.8-8.4, Oracle (7.9-8.4, Amazon Linux (2)
Content Disarm & Reconstruction (CDR) w wiadomościach e-mail i Internecie	
Threat Extraction	Usuwa aktywną zawartość możliwą do wykorzystania w ataku (np. skrypty oraz makro), rekonstruuje pliki w celu wyeliminowania potencjalnych zagrożeń i dostarcza wyczyszczone treści użytkownikom w ciągu kilku sekund.
Threat Emulation	• Sandboxing, który umożliwia wykrywanie i blokowanie nowego, nieznanego złośliwego oprogramowania i ataków ukierunkowanych, które znajdują się w załącznikach do wiadomości e-mail, pobranych plikach i adresach URL do plików w treściach wiadomości e-mail. • Zapewnia ochronę najszerszego zakresu typów plików, w tym MS Office, Adobe PDF, Java, Flash, plików wykonywalnych i archiwów. • Wykrywa zagrożenia ukryte w komunikacji szyfrowanej przez SSL i TLS.
Centralne zarządzanie	
Zarządzanie lokalne (On-Premise) i w chmurze (Check Point Infinity Portal)	• Usługa Harmony (hostowana w chmurze Check Point) • Appliance Harmony (hostowane lokalnie)
NGAV: Ochrona i wykrywanie w czasie rzeczywistym	
Anti-Ransomware	• Threat Prevention – stale monitoruje zachowania specyficzne dla ransomware i wykrywa niepożądane szyfrowanie plików bez użycia sygnatur. • Wykrywanie i kwarantanna – wszystkie elementy ataku ransomware są wykrywane za pomocą analizy forensic, a następnie poddawane kwarantannie. • Przywracanie danych – zaszyfrowane pliki są automatycznie przywracane ze snapshotów, aby zapewnić pełną ciągłość biznesową.
Anti-Exploit	• Zapewnia ochronę przed atakami, wykorzystującymi luki w zabezpieczeniach (exploit), które zagrażają normalnym aplikacjom. • Wykrywa exploity, identyfikując podejrzane manipulacje pamięci w czasie rzeczywistym. • Wyłącza proces wykorzystywany do ataku po jego wykryciu i usuwa cały łańcuch ataku
Behavioral Guard	• W sposób adaptacyjny wykrywa i blokuje mutacje złośliwego oprogramowania zgodnie z ich zachowaniem w czasie rzeczywistym. • Wykrywa, klasyfikuje i blokuje mutacje złośliwego oprogramowania w czasie rzeczywistym w oparciu o minimalne podobieństwa drzewa wykonywania procesów.
Ochrona sieci Web	
Zero-Phishing	• Ochrona w czasie rzeczywistym przed nieznanymi witrynami phishingowymi • Statyczne i heurystyczne wykrywanie podejrzanych elementów witryn internetowych, które wyłudzają prywatne informacje
Corporate Credential Protection	Wykrywanie ponownego wykorzystania poświadczeń korporacyjnych w zewnętrznych serwisach i witrynach
URL Filtering	• Lekka wtyczka do przeglądarki umożliwia/blokuje dostęp do witryn internetowych w czasie rzeczywistym • Egzekwowanie polityk organizacji dotyczących bezpiecznego korzystania z Internetu przez użytkowników na terenie organizacji i poza nią, egzekwowanie zgodności z regulacjami compliance oraz poprawa produktywności organizacji • Pełna widoczność ruchu HTTPS
THREAT HUNTING	
Threat Hunting	Zbiór wszystkich surowych i wykrytych zdarzeń zebranych na punktach końcowych pozwala generować zaawansowane zapytania i przeprowadzać analizy w celu proaktywnego wyszukiwania zagrożeń i szczegółowego badania incydentów.

Dlaczego Harmony Endpoint?

Dziś bezpieczeństwo punktów końcowych odgrywa kluczową rolę we wspieraniu pracy zdalnej bardziej niż kiedykolwiek wcześniej. 70% cyberataków rozpoczyna się od punktów końcowych, dlatego ich pełna ochrona na najwyższym poziomie bezpieczeństwa ma kluczowe znaczenie w celu unikania naruszeń bezpieczeństwa organizacji i jej danych.

Harmony Endpoint to kompleksowe rozwiązanie do zabezpieczania punktów końcowych, stworzone w celu ochrony zdalnych pracowników przed dzisiejszym złożonym środowiskiem zagrożeń. Zapobiega bezpośrednim zagrożeniom, takim jak oprogramowanie ransomware, phishing lub złośliwe oprogramowanie typu drive-by, jednocześnie szybko minimalizując wpływ naruszeń poprzez autonomiczne wykrywanie i reagowanie.

W ten sposób cała organizacja otrzymuje pełną ochronę punktów końcowych, której potrzebuje – w jakości, na jaką zasługuje, w postaci jednego, wydajnego i opłacalnego rozwiązania.

Harmony Endpoint jest częścią pakietu produktów Check Point Harmony – pierwszego w branży zunifikowanego rozwiązania do ochrony użytkowników, urządzeń i dostępu. Harmony łączy w sobie sześć produktów, aby zapewnić wszystkim bezkompromisowe bezpieczeństwo i prostotę. Zabezpiecza urządzenia i połączenia internetowe przed najbardziej wyrafinowanymi atakami, zapewniając jednocześnie dostęp do aplikacji korporacyjnych na zasadzie Zero Trust w ramach jednego rozwiązania, które jest proste we wdrożeniu, obsłudze i zarządzaniu.

Więcej informacji: https://www.checkpoint.com/products/advanced-endpoint-protection/

CLICO Sp. z o.o.
ul. Oleandry 2, 30-063 Kraków
Informacje i pomoc techniczna: ps@clico.pl
www.clico.pl, www.checkpoint.clico.pl

Centrala ogólnoświatowa
5 Ha'Solelim Street, Tel Awiw 67897, Izrael | Tel.: 972-3-753-4555 | Faks: 972-3-624-1100 | E-mail: info@checkpoint.com
Centrala w USA
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel.: 800-429-4391; 650-628-2000 | Faks: 650-654-4233
www.checkpoint.com