puresecurity™

Check Point®
SOFTWARE TECHNOLOGIES LTD.

Központi biztonságmenedzsment

A Check Point központi biztonságmenedzsment megoldásai egyesített szabálykezelést, megfigyelést és elemzést biztosítanak

SmartCenter

Az ideális választás a központosított biztonságmenedzsmentben

AZ ÖN FELADATA

Volt idő, amikor biztonságtechnika csúcsának számított, ha a rendszer tűzfallal volt körülvéve, és vírusirtó program futott a számítógépeken. Ez ma már nem igaz. Az internetes férgek és az egyre kifinomultabb támadások megjelenésével a hálózati biztonság sokkal összetettebb képet mutat, mint valaha. Ez az új környezet a biztonsági előírások megjelenésével és a távoli felhasználók és üzleti partnerek általi hozzáférés igényével együtt alaposabb biztonsági megoldást igényel. A többrétegű védelem a perimeteren a tűzfalakkal kezdődik, és mélyebbre nyúlik a hálózatba, hogy védje az érzékeny szervezeti egységeket, a szervereket, az alkalmazásokat, sőt a felhasználói számítógépeket és noteszgépeket. Sajnos ez a fajta többrétegű biztonság bonyolultabb alkalmazást igényel. A kihívás, hogy a biztonság folyamatos legyen több telephelyen és több platformon, hamar terhes feladattá válhat a korlátozott erőforrásokkal rendelkező informatikai osztály számára.

Hatékony kezelés nélkül a legösszetettebb biztonság megvalósítása is csak olyan erős, mint annak leggyengébb láncszeme. A biztonságkezelési megoldásoknak lehetővé kell tenniük a vállalatok számára, hogy nyomon kövessék a biztonság hatékony megvalósítását, részletes tájékoztatást nyújtsanak a biztonsági oknyomozó vizsgálatok számára, valamint lehetővé tegyék a biztonsági szabályok következetes alkalmazását és a proaktív frissítéseket az egész szervezetre kiterjedően.

A MI MEGOLDÁSUNK

SmartCenter™ lehetővé teszi a vállalatoknak, hogy központilag meghatározzák a hálózati, adatkezelési és végponti biztonsági szabályzataikat, összefüggésbe hozzák és fontossági sorrendbe állítsák a biztonsági eseményeket, valamint fejlett megfigyelést és jelentést valósítsanak meg, mindezt egyetlen konzolon keresztül. Könnyűvé válik a biztonsági szabályzat és a veszélyekkel szembeni védelem frissítéseinek továbbítása az összes átjáróhoz, ami biztosítja a szabályzat következetes érvényesítését és a legújabb fenyegetésekkel szembeni naprakész védelmet. Ennek eredményeként a vállalatok képesek lesznek megvédeni az üzleti szempontból kritikus eszközeiket, valamint a maximumra növelni a biztonsági befektetéseik megtérülését.

TERMÉKLEÍRÁS

A SmartCenter™ biztosítja az összes Check Point termék központi kezelését.

TERMÉKJELLEMZŐK

- Integrált hálózat-, adat- és végpontbiztonság kezelés
- A biztonsági szabályzat megjelenítése
- A szabályzatok és a szoftverek automatizált terítése
- A szabályzatok elérése webes portálon vagy kezelői konzolon keresztül
- Nagyfokú rendelkezésre állás és méretezhetőség

A TERMÉK ELŐNYEI

- Maximalizálja az üzemi hatékonyságot
- Lehetővé teszi a szabályzat következetes érvényesítését és ellenőrzését az egész hálózatra kiterjedően
- Megkönnyíti az előírásoknak való megfelelés bizonyítását
- Fenntartja a legaktuálisabb, preemptív biztonságot

NGX™

Az NGX platform egységes biztonsági architektúrát biztosít a Check Point számára.

ÁTFOGÓ BIZTONSÁGKEZELÉS

A Check Point különféle szintű kezelési funkciókat biztosít a SmartCenter UTM™ és a SmartCenter Power™ segítségével, hogy integrált és költséghatékony megoldásokat nyújtson a legmagasabb szintű ellenőrzés és biztonság érdekében egyetlen kezelőpult használatával.

A SmartCenter UTM központi kezelést biztosít az összes Check Point alkalmazás számára. Az alábbi részekből áll:

- SmartDashboard™: az a felület, amely lehetővé teszi az adminisztrátorok számára a biztonsági és VPN-szabályok központi meghatározását
- SmartView Tracker™: biztosítja az összes naplózott kapcsolat és adminisztrátori tevékenység valós idejű vizuális nyomon követését

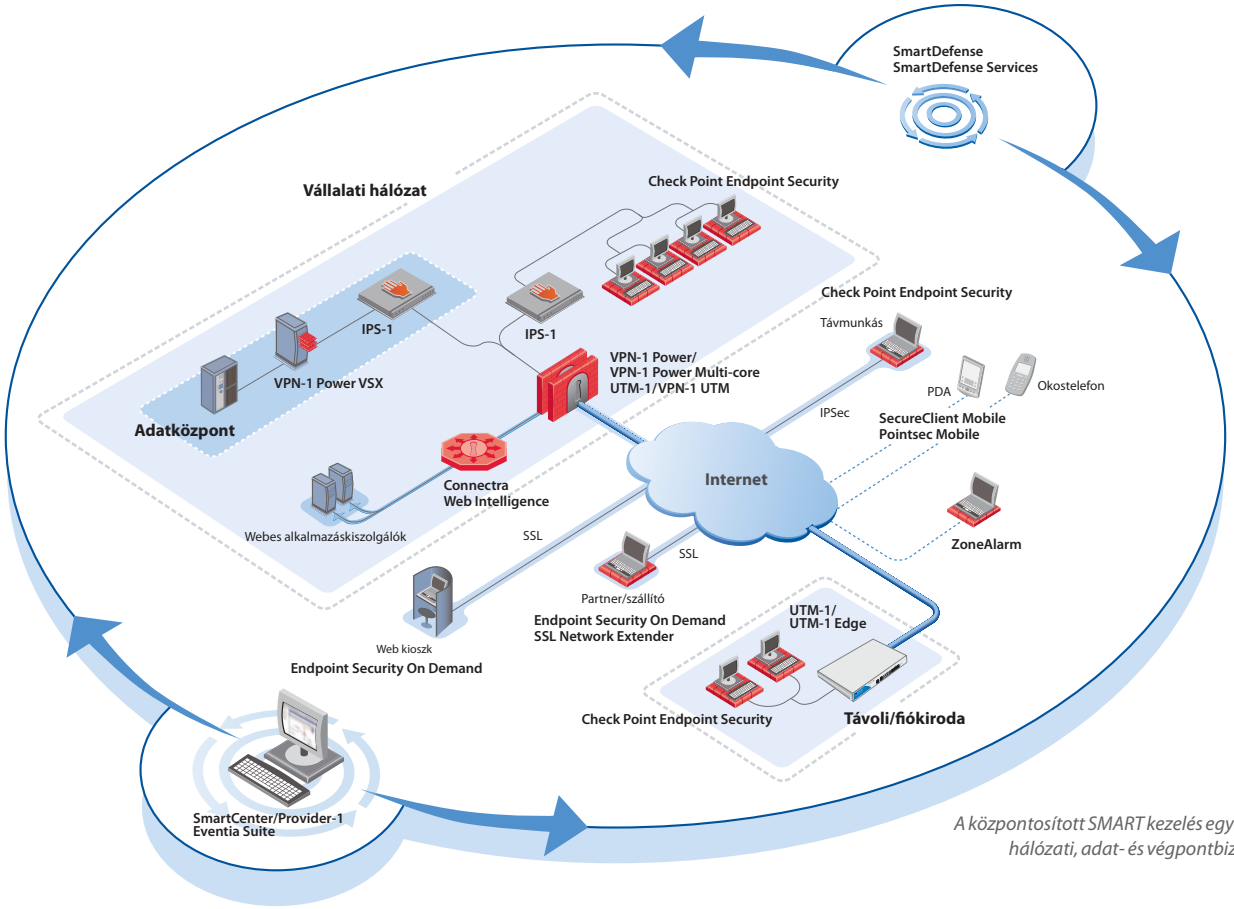
A SmartCenter Power a SmartCenter összes képességén túl további menedzsment funkciókkal is rendelkezik a legösszetettebb környezetek számára:

- SmartPortal™: kiegészíti a böngészőalapú hozzáférést a Smart Centerre
- SmartMap™: lehetővé teszi a biztonsági szabályzatok vizuális kezelését
- SmartView Monitor: lehetővé teszi a valós idejű hálózat, a VPN és a felhasználó figyelemmel kísérését
- SmartUpdate™: központosítja a szoftverek és a licencek terítését és nyilvántartását
- SmartLSM™: lehetővé teszi a távoli biztonsági eszközök nagyszámú kezelését
- SmartDirectory: integrációt biztosít az LDAP-alapú címtárakkal
- Management High Availability: biztosítja az összes menedzsment alkalmazás hibatűrését

Emellett az Eventia Reporter™ átfogó, könnyen érthető grafikus kimutatásokat készít, és az Eventia Analyzer™ biztosítja a Check Point átjárókból és több különböző biztonsági és hálózati eszközből származó naplóadatok eseményeinek valós idejű megfeleltetését. Az Eventia Reporter és az Eventia Analyzer a SmartCenter kiegészítőiként rendelhető.

Szabályzat-alapú VPN/tűzfalkezelés

A SmartCenter részét képező SmartDashboard kifinomult és könnyen használható. Az adminisztrátorok a biztonsági rendszer összes elemét tudják kezelni: a hálózati és asztali szabályzatokat, a VPN-eket, a hálózati címfordításokat (NAT-okat), a szolgáltatási minőséget (QoS), az olyan üzenetkezelési biztonságot, mint például a spam elleni műveletek, az olyan tartalomfigyelést, mint például a vírusvédelmet, a webes és távoli elérést és a SmartDefense frissítéseket. A biztonsági szabályzat részeként definiált hálózati „objektumok", végpontok, felhasználók, szolgáltatások, erőforrások és műveletek vizuálisan megjelennek, és kezelhetők a SmartDashboard segítségével. Az objektumok például SmartGroup-okba csoportosíthatók, a hálózati objektumok pedig könnyen klónozhatók a szabályzatmeghatározás egyszerűsítése érdekében. Mivel az egységes biztonsági architektúra részei szorosan integráltak, ugyanazok az objektumok megoszthatók az érvényesítési pontok és alkalmazások között, ami adminisztratív időt takarít meg, és biztosítja a szabályzat következetes kialakítását az egész hálózatra kiterjedően.



A központosított SMART kezelés egyesíti a Check Point hálózati, adat- és végpontbiztonság-kezelését.

A központi műszerfal mellett a SmartCenter megoldásai a szabályzatkezelési eszközök széles skáláját kínálják a szabályzatok hatékony létrehozásának érdekében. Az előre definiált globális szabályzatok lehetővé teszik a megfelelő kapcsolatokat az érvényesítési pontok és a különböző szolgáltatások között. A SmartCenter a szabályzatok több verzióját is tudja kezelni, ami lehetővé teszi, hogy az adminisztrátor visszatérjen a szabályzat régebbi verziójához.

Integrált biztonság

A SmartCenter biztosítja az összes Check Point termék központi kezelését. A SmartDashboardról az adminisztrátor definiálhatja és érvényesítheti a szabályzatot, nyomon követheti a naplókat, figyelemmel kísérheti a biztonsági és hálózati tevékenységet, megjelenítheti a hálózati és biztonsági tevékenység alakulásáról szóló kimutatásokat, és központilag terítheti a biztonsági és szoftverfrissítéseket. Ilyen funkciókkal a kezükben az adminisztrátorok jobb üzemi hatékonyságot érhetnek el, valamint fokozott rálátást kapnak az egész hálózat biztonsági helyzetére.

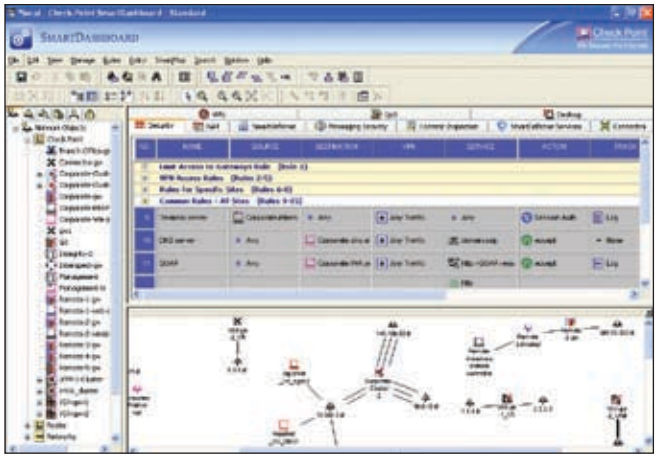
Integrált végponti biztonság

A Check Point Endpoint Security az első önálló, teljes körű végpontbiztonságot jelentő kliens, amely összekapcsolja a legkiválóbb minősítésű tűzfal, a hálózati hozzáférés-szabályozás (NAC), a programfelügyelet, a vírus- és kémprogram-szűrés, az adatbiztonság és a távoli hozzáférés előnyeit. Megvédi a számítógépeket és feleslegessé teszi több kliens telepítését és felügyeletét, ezzel csökkenti a tulajdonlási összköltséget.

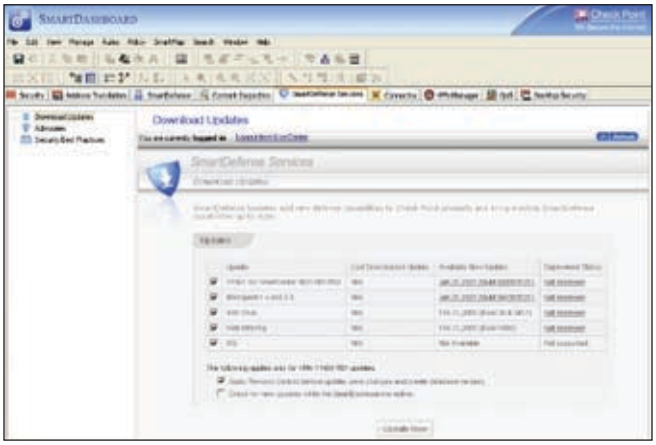
A SmartCenterbe integrált Check Point Endpoint Security más Check Point megoldásokkal együtt központilag kezelhető, ami hatékonyabbá teszi az egész vállalatra kiterjedő biztonságkezelést.

Globális biztonsági védelmi frissítések

A SmartDashboardba épített SmartDefense Services lehetővé teszi az adminisztrátorok számára, hogy központilag frissítsék a biztonsági konfigurációkat és védelmeket egy egyesített felületen keresztül, és ezáltal fenntartsák a legújabb preemptív biztonságot a Check Point biztonsági infrastruktúra számára. A SmartDefense lehetővé teszi különböző védelmi profilok hozzárendelését különböző átjárókhoz. Az átjárók és azok SmartDefense profiljainak hozzárendelése és kezelése központilag elvégezhető a SmartDashboardon keresztül.



A szabályzatok központi kezelését és megjelenítését biztosítja a SmartDashboard révén.



A biztonsági konfigurációs és védelmi frissítések központilag, a SmartDashboardon keresztül történnek.

A VPN egyszerű megvalósítása

A SmartDashboard lehetővé teszi az adminisztrátoroknak, hogy egyetlen műveletben elvégezzék a VPN közösségek definiálását és a biztonsági paraméterek beállítását az egész VPN topológiára kiterjedően, ideértve az intranetet, az extranetet és a távoli elérésű megvalósításokat. A biztonsági adminisztrátor egyszerűen egyetlen közösségbe csoportosítja a VPN-1 átjárókat, és a VPN-ek automatikusan létrejönnek az összes átjáró között vagy a távoli felhasználók és átjárók között. Amikor új helyszínek vagy felhasználók adódnak a közösséghez, azok automatikusan öröklik a megfelelő jellemzőket, és azonnal biztonságos munkameneteket tudnak létrehozni a VPN közösség többi részével együtt. A biztonsági adminisztrátorok így mentesülnek a titkosítási szabályok tervezésének és definiálásának ismétlődő feladatától. A SmartCenter számos hálózati topológiát támogat, ideértve a teljesen összekapcsolt „full mesh", csillag, „hub and spoke", valamint a hibrid topológiákat. A VPN objektumok és közösségek könnyen felvehetők a biztonsági szabályok adatbázisába.

Valós idejű hibakeresés

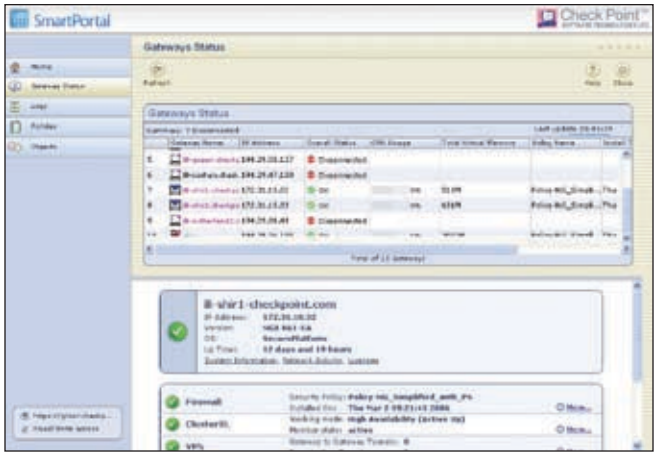
A SmartView Tracker biztosítja az összes naplózott kapcsolat és adminisztrátori tevékenység valós idejű vizuális nyomon követését. Az adminisztrátorok kiszűrhetik vagy megkereshetik az őket érdeklő eseményeket, és támadás vagy gyanús tevékenység észlelése esetén azonnal letilthatják vagy megszakíthatják a kapcsolatot meghatározott IP-címekkel. Ezek a funkciók jelentősen csökkentik a konfigurációs hibák kereséséhez szükséges időt.

SMARTCENTER POWER – FEJLETT BIZTONSÁGKEZELÉS ÖSSZETETT KÖRNYEZETEK SZÁMÁRA

A SmartCenter révén a vállalatot központilag meghatározhatja és figyelemmel kísérheti biztonsági szabályzatát. A SmartCenter Power és kezelési kiegészítő modulok, például az Eventia Reporter és az Eventia Analyzer, a biztonsági környezet még jobb megértését és ellenőrzését biztosítják számos fejlett, integrált funkció révén.

A SmartCenter webes elérése

A SmartPortallal a biztonsági csapat kiterjesztheti a SmartCenter böngészőalapú elérését a külső csoportokra, például a műszaki támogatási személyzetre vagy az auditorokra, miközben képes fenntartani a szabályzat érvényesítésének központi ellenőrzését. A SmartPortal felhasználók megtekinthetik a biztonsági szabályzatokat és a Check Point termékek állapotát, illetve az adminisztrátori ellenőrzési (audit trail)nyomvonalakat. A haladó szintű felhasználók adminisztrátori kezelési jogosultságokat kaphatnak. Ez a kibővített funkció elősegíti a



A SmartPortal webes kezelési portál a szervezeten belül több felhasználóra is kiterjeszti a biztonság láthatóságát.

csapat összehangolt munkáját a támadások mérséklése, illetve a hálózati és a biztonsági problémák megoldása során. A SmartPortal lehetővé teszi, hogy a biztonsági adminisztrátorok saját belátásuk szerint kiterjesszék a biztonsági szabályzathoz való hozzáférést más csoportokra, és ezáltal növeljék a biztonság láthatóságát a szervezeten belül.

A biztonság megjelenítése

A legtöbb szervezet összetett topológiával rendelkezik, amelyben az átjárók, a végpontok, a szerverek és a hálózatok több különböző gép között vannak szétosztva, és azokra sok különböző szabály és szabályalap vonatkozik. A SmartMap a biztonsági szabályzatokat vizuálisan jeleníti meg, ami megkönnyíti a szabályzatok megértését és a hibakeresést. Emellett lehetővé teszi a biztonsági vezetők számára, hogy ellenőrizzék a biztonsági szabályzataik integritását azok bevezetése előtt.

Valós idejű felügyelet

A SmartView Monitor biztosítja a biztonság, a hálózat, a VPN-alagút és a felhasználói tevékenységek valós idejű felügyeletét. Ez a megoldás lehetővé teszi, hogy az adminisztrátorok grafikusan megjelenítsenek olyan mutatókat, mint a sávszélesség, a megfordulási idő (RTT), a csomagveszteség és a VPN-alagút állapota. A SmartView Monitor által biztosított információkkal felvértezve az adminisztrátorok a maximumra növelhetik a hálózatok teljesítményét, és korlátozhatják a költségeket.

A szoftverek és licencek automatikus terítése

A SmartUpdate automatikusan teríti a szoftveres alkalmazásokat és a Check Point és OPSEC-tanúsítással rendelkező termékek frissítéseit, és kezeli a terméklicenceket. Centralizált eszközt biztosít, amely garantálja, hogy az egész hálózaton mindig naprakész a biztonság. Továbbá csökkenti az informatikai személyzet iránti igényt a fiókirodákban.

Nagy bonyolultságú VPN- és biztonságkezelés

A SmartLSM a nagy léptékű VPN/biztonsági telepítések kezelésének új megközelítését kínálja. A SmartLSM segítségével az adminisztrátorok előírhatnak egy egységes biztonsági szabályzatot (más néven profilt), és több száz átjáróra alkalmazhatják azt. Emellett a szabályzat telepítésével és frissítésével kapcsolatos automatizált folyamatok lehetővé teszik a gyors terítést, és a minimumra csökkentik a kezelési követelményeket. Ez csökkenti a több száz átjáró biztonságának megvalósítására és kezelésére fordított költségeket és időt.

Az új funkciók és a terméktámogatás dinamikus frissítései

A SmartCenter bővítmény architektúrája lehetővé teszi a felhasználók számára az új funkciók és új terméktámogatások dinamikus hozzáadását. Ezek a kezelői bővítménycsomagok könnyen feltölthetők, és csak az új átjáró termékek vagy konkrét funkciók kezeléséhez szükséges összetevőkből áll, így elkerülhető a következő kiadásra való teljeskörű frissítés.

Az infrastruktúra redundanciájának kezelése

A Management High Availability biztosítja a Check Point érvényesítési pontokhoz való folyamatos kapcsolódást. Több kezelési kiszolgáló csatlakoztatható másokhoz egy „idegrendszer" által, amely automatikusan szinkronizálja a felhasználói és az adminisztrátori adatokat. Ez kiküszöböli a dedikált, redundáns hardver és szoftver telepítésének szükségességét.

TÁMOGATOTT OPERÁCIÓS RENDSZEREK	
SmartCenter GUI konzol	Windows 2000/2003, ME, XP, Vista; Solaris 8/9/10
SmartCenter kiszolgáló	SecurePlatform™, Windows 2000/2003 Server, Solaris 8/9/10, Red Hat Linux Enterprise 3.0, Nokia IPSO

CHECK POINT ELÉRHETŐSÉGEK

Nemzetközi központ
5 Ha'Solelim Street, Tel Aviv 67897, Izrael | Tel.: 972-3-753-4555 | Fax: 972-3-575-9256 | E-mail: info@checkpoint.com

USA-központ
800 Bridge Parkway, Redwood City, CA 94065 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

2008. február 26. Cikksz.: 502841