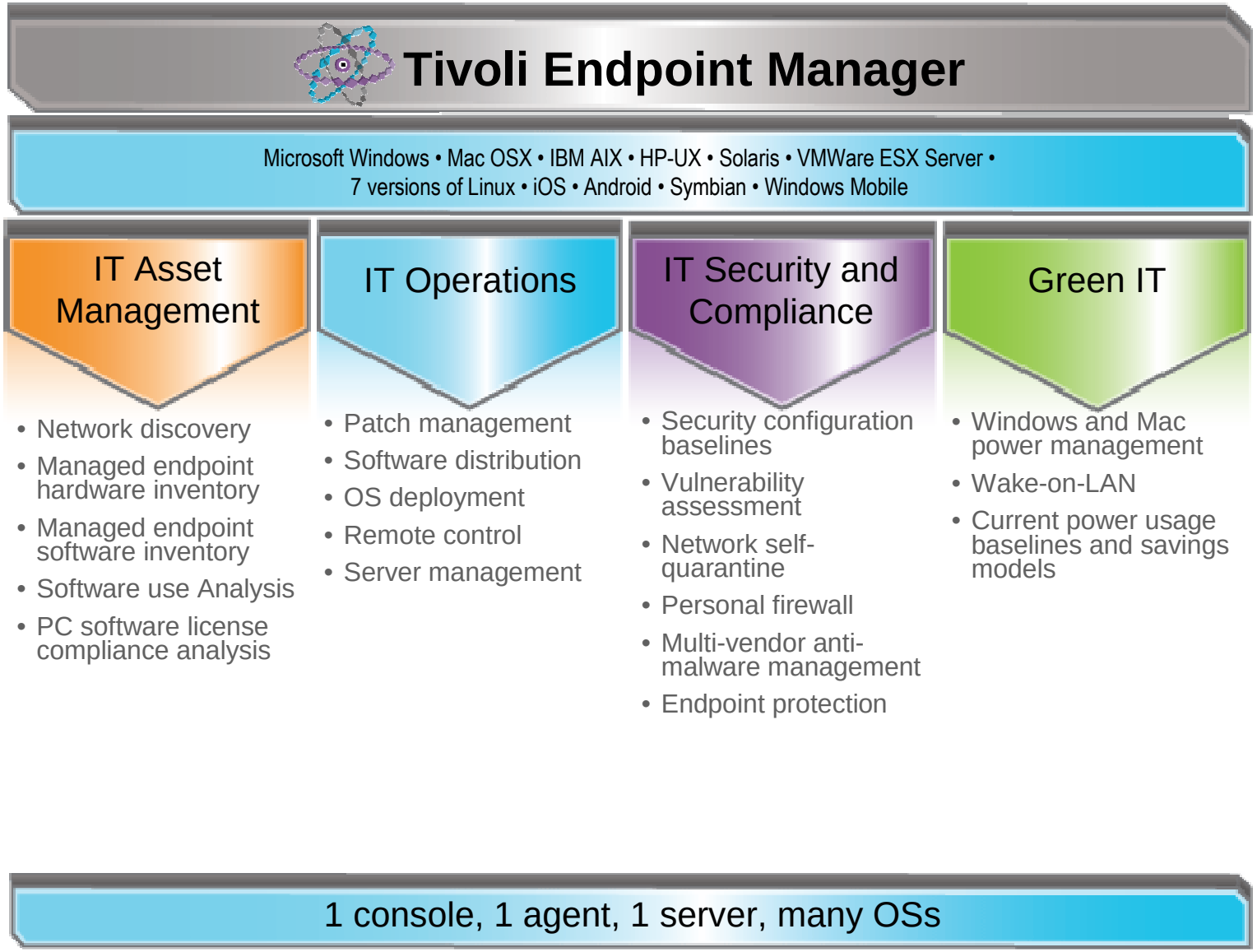
Egyenszilárd biztonság

... avagy Tivoli Endpoint Manager a Unixoktól a mobiltelefonokig

A termékcsalád funkcionális áttekintése



Tivoli Endpoint Manager: alacsony TCO, **valódi** megtakarítás

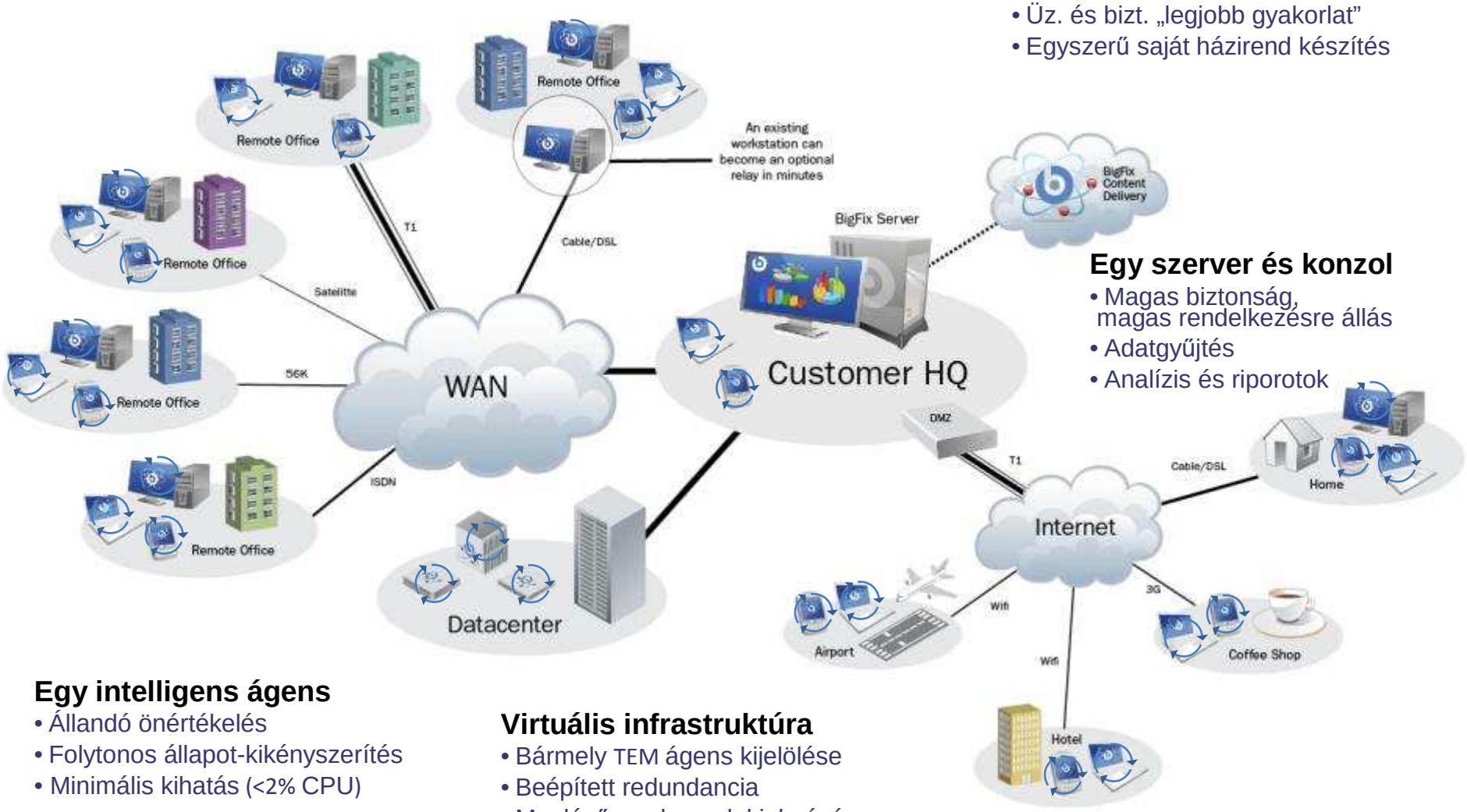
	Korábbi megközelítés	TEM megközelítés
Bevezetés 90 000 eszközre	6 hónap	1 hét
Felügyeleti szerverek darabszáma	25	1
Éves áramfelvétel (USA árak)	$6.9M	$4M
Javítási ciklus	7 nap	5 perc
Szoftver leltári ciklus	3 hét	20 perc
Sebezhetőség-vizsgálati ciklus	6 hónap	3 nap
Biztonság-konfigurációs ciklus	5 hónap, 6 FTE	2 hét, 1 FTE

„[...] Gondoltam, megosztom Veled és a srácokkal [...] A Microsoft javítások terítése reggel 5:00-kor indult április 20-án, összességében 579 047 terítendő javítással, ami nálunk ebben a pillanatban az eddigi legnagyobb ilyen jellegű vállalkozás volt. Ebből délután 3:00-ig 527 916 darab került végrehajtásra. Ez azt jelenti, hogy 10 óra leforgása alatt az érintett javítások 91,17%-a sikeresen lefutott!

Nem hiszem, hogy lenne még egy olyan termék, amely ehhez hasonló eredményt tudott volna nálunk produkálni. [...]”

Zárt ciklusú, kliens oldali házirend-kikényszerítés

Fixlet üzenetek
- Készen kapott szabályok
- Üz. és bizt. „legjobb gyakorlat”
- Egyszerű saját házirend készítés



Egy szerver és konzol
- Magas biztonság, magas rendelkezésre állás
- Adatgyűjtés
- Analízis és riportok

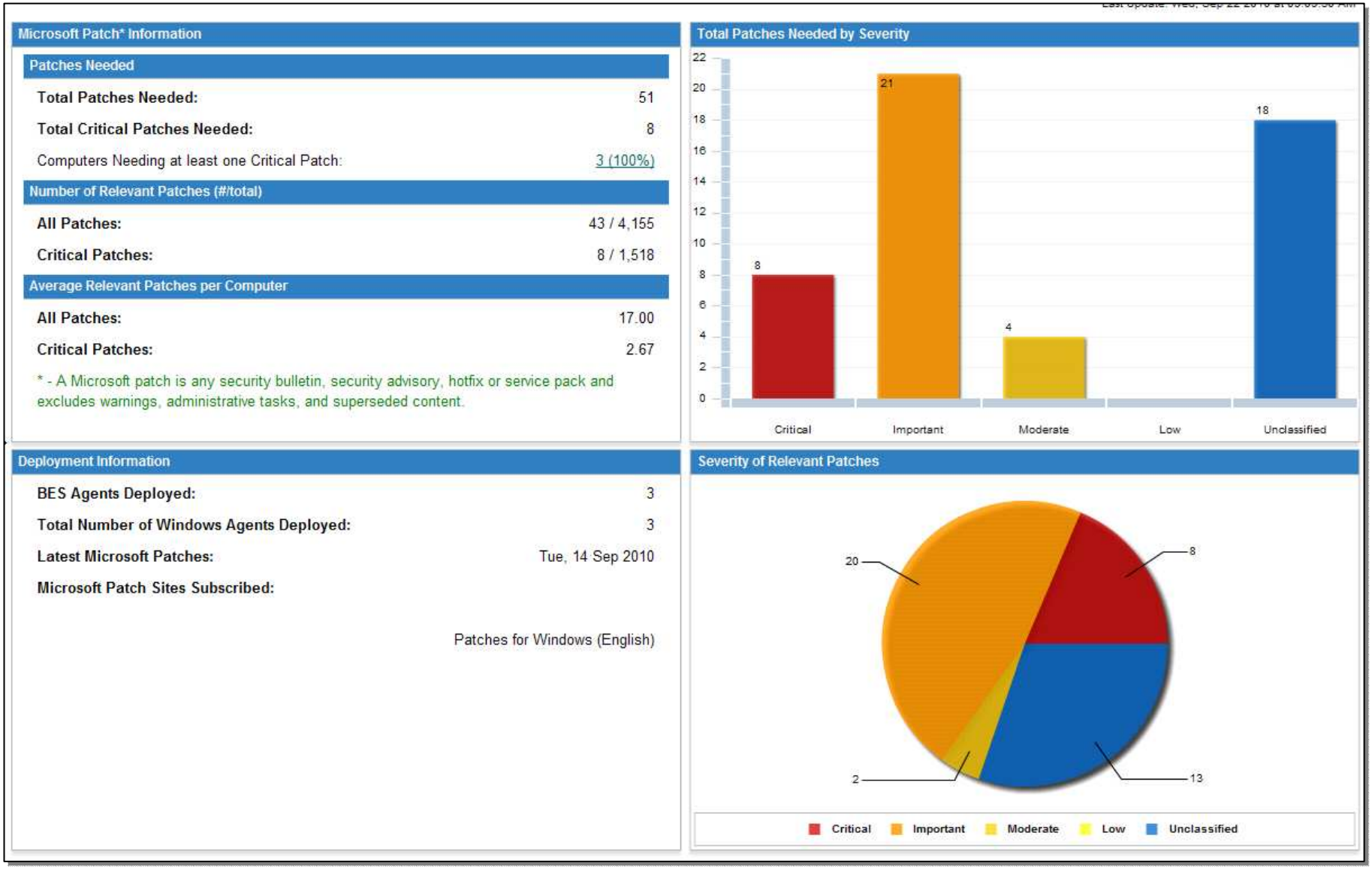
Egy intelligens ágens
- Állandó önértékelés
- Folytonos állapot-kikényszerítés
- Minimális kihatás (<2% CPU)

Virtuális infrastruktúra
- Bármely TEM ágens kijelölése
- Beépített redundancia
- Meglévő rendszerek kiaknázása

Folytonos javítás-megfelelőség ellenőrzés és kikényszerítés

• Automatizált patch-kezelés sokféle operációs rendszerhez és alkalmazáshoz
• Biztonsági és megfelelőségi kockázatok csökkentése a javítási ciklusok heti nagyságrendről napi/órás nagyságrendre való csökkentésével
• Patch-szintek átláthatósága flexibilis, valós idejű monitorozással és riportozással
• Helytelen javítások automatikus megakadályozása a téves végpontokon

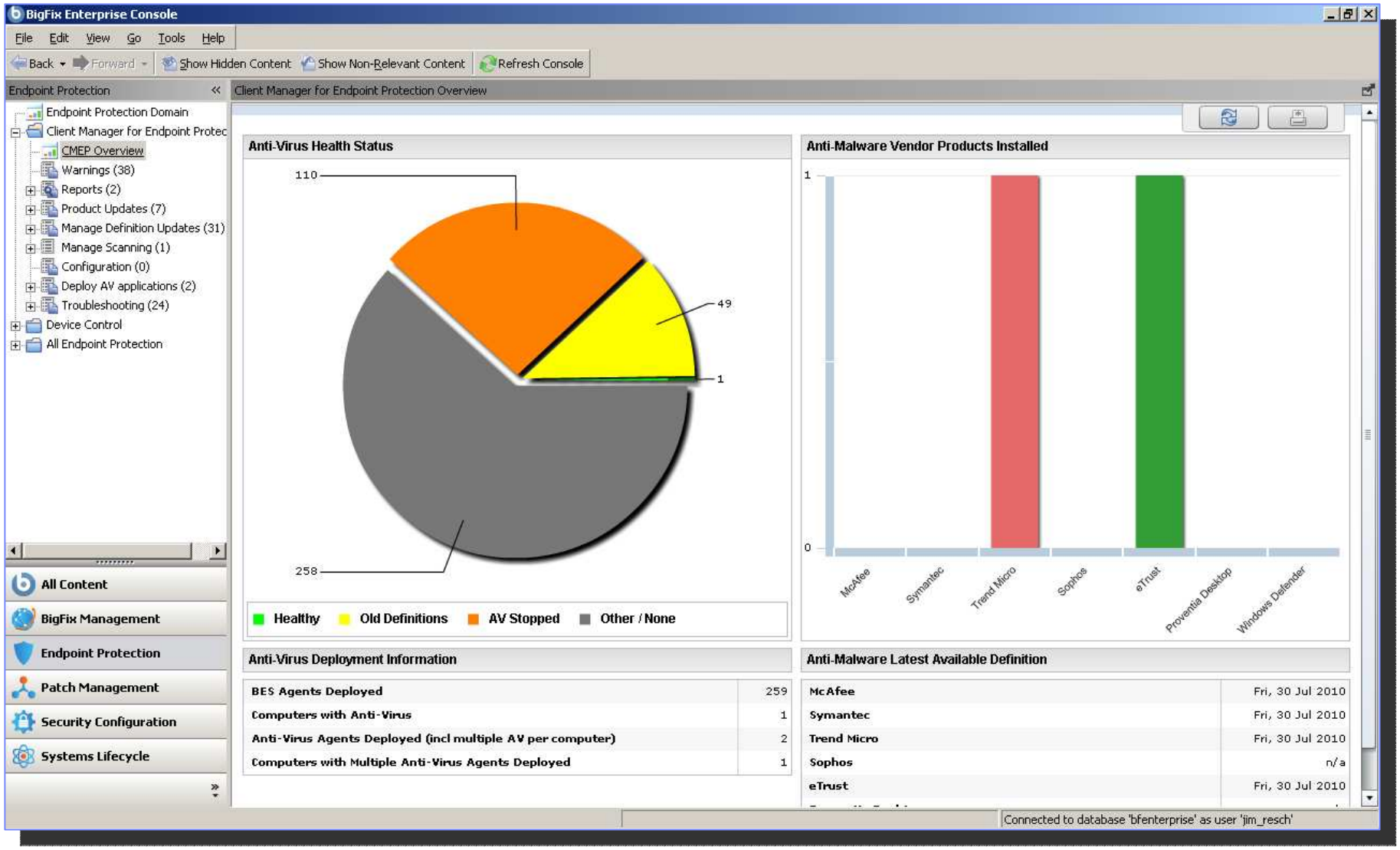
Valós idejű monitorozás és riportozás



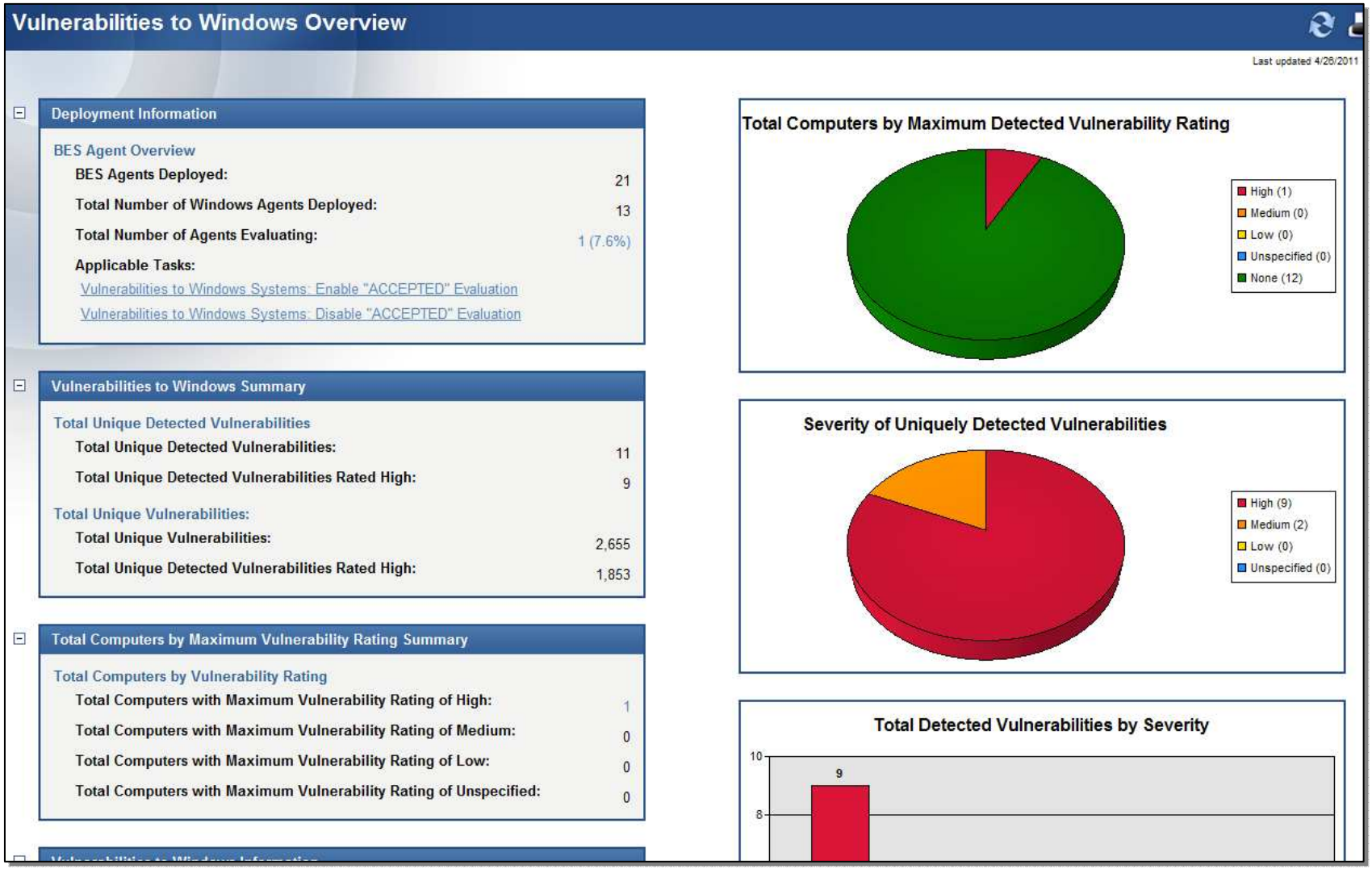
Egyetlen megoldásban megvalósított vállalati végponti biztonság-felügyelet

- Biztonsági beállítások és javítások folytonos kikényszerítése
- Patch-szintek átláthatósága flexibilis, valós idejű monitorozással és riportozással
- Más gyártóktól származó anti-malware és tűzfal-védelem központosított felügyelete
- Készen kapott „legjobb gyakorlatok” a szabályozások által megkívánt állapotok eléréséhez
- Trendfelismerést és analízist biztosító biztonsági változás riportozás
- A vállalat által potenciálisan nem ismert végpontok felderítése
- Hálózati ön-karanténozás

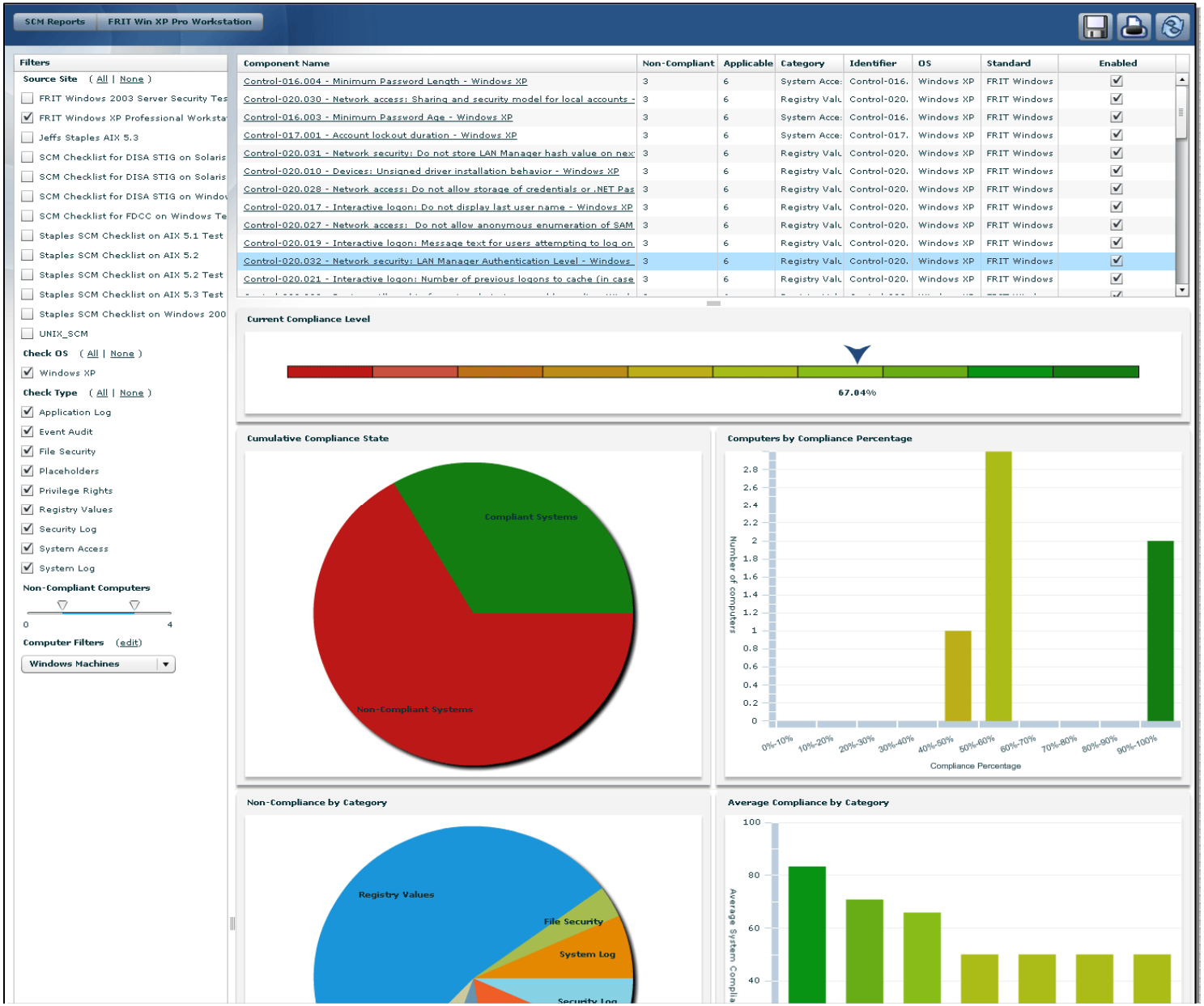
Megfelelőség: antivírus, anti-malware



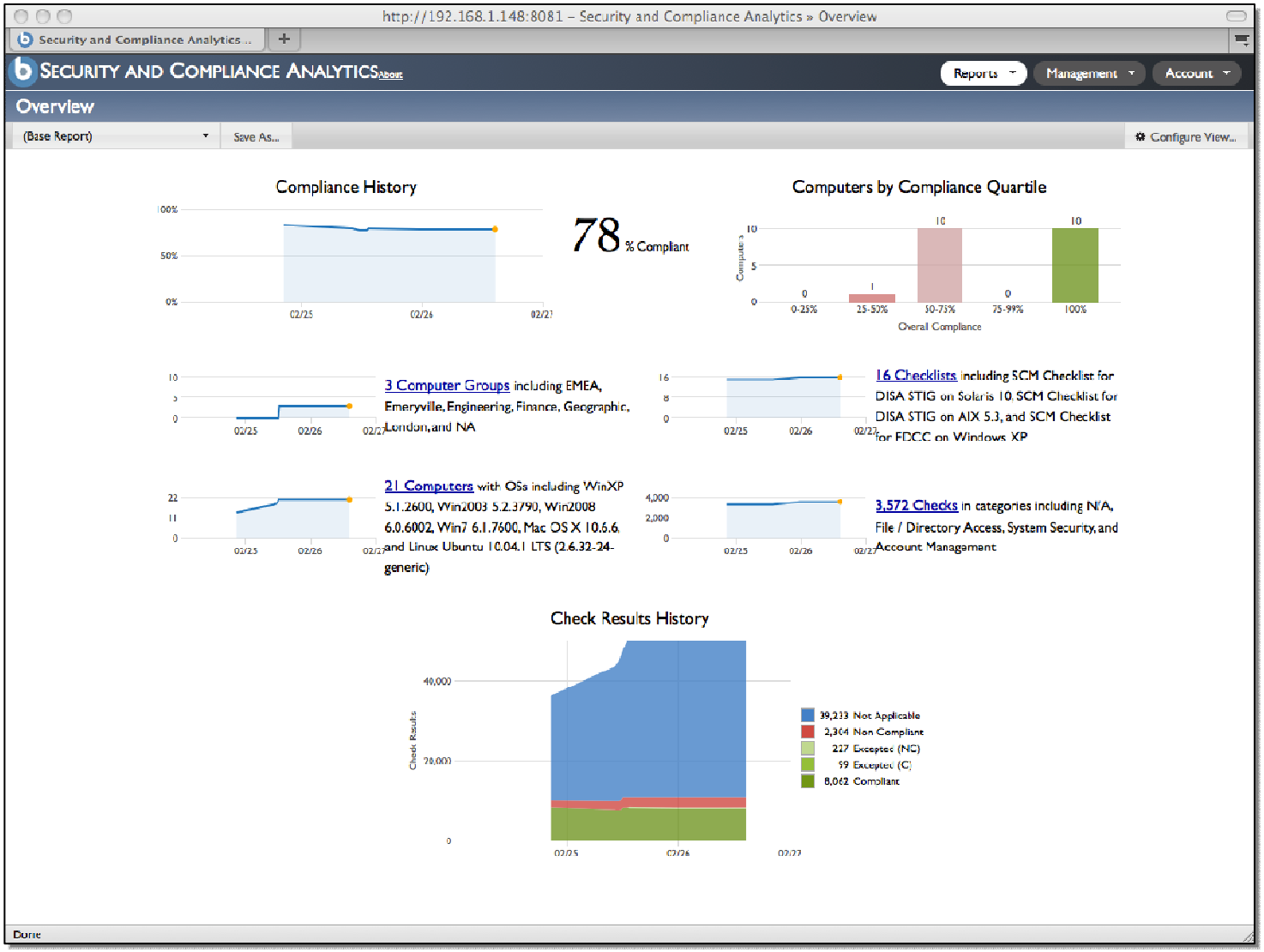
Sérülékenység-kezelés



Biztonsági és megfelelőségi riportok



Trendfelismerés és analízis riportozással



Valós idejű malware és sebezhetőség elleni védelem

- Vírusok, trójaiak, vírusférgek, kémprogramok, rootkitek, webes támadások és ezek variánsainak károkozása elleni védelem fizikai és virtuális végpontokon
- Valós idejű végpont-védelem biztosítása állomány és web ismeretség, viselkedés-monitorozás, virtualizáció-tudatosság és személyes tűzfal alkalmazásával
- Automatikus malware törlés és végpont sérülékenységek javítása a támadások előtt
- Az antivírus szolgáltatások telepítettségének, frissességének és futó állapotának folyamatos biztosítása
- Virtualizáció-tudatosság a virtuális infrastruktúrák erőforrás-versengési jelenségének minimalizálására

Eszköz-korlátozások

- X Port letiltás
- X Tiltott kulcsszó
- X Hozzáférés-tiltás
- X Állományméret-tiltás

- X Nem engedélyezett USB sorozatszám
- X Tiltott kulcssszó
- X Gyanús adattartalom – minta-restrikció

- X Nyomtatás-védelem
- X Tiltott kulcsszó
- X Gyanús adattartalom – minta-restrikció
- X Port letiltás

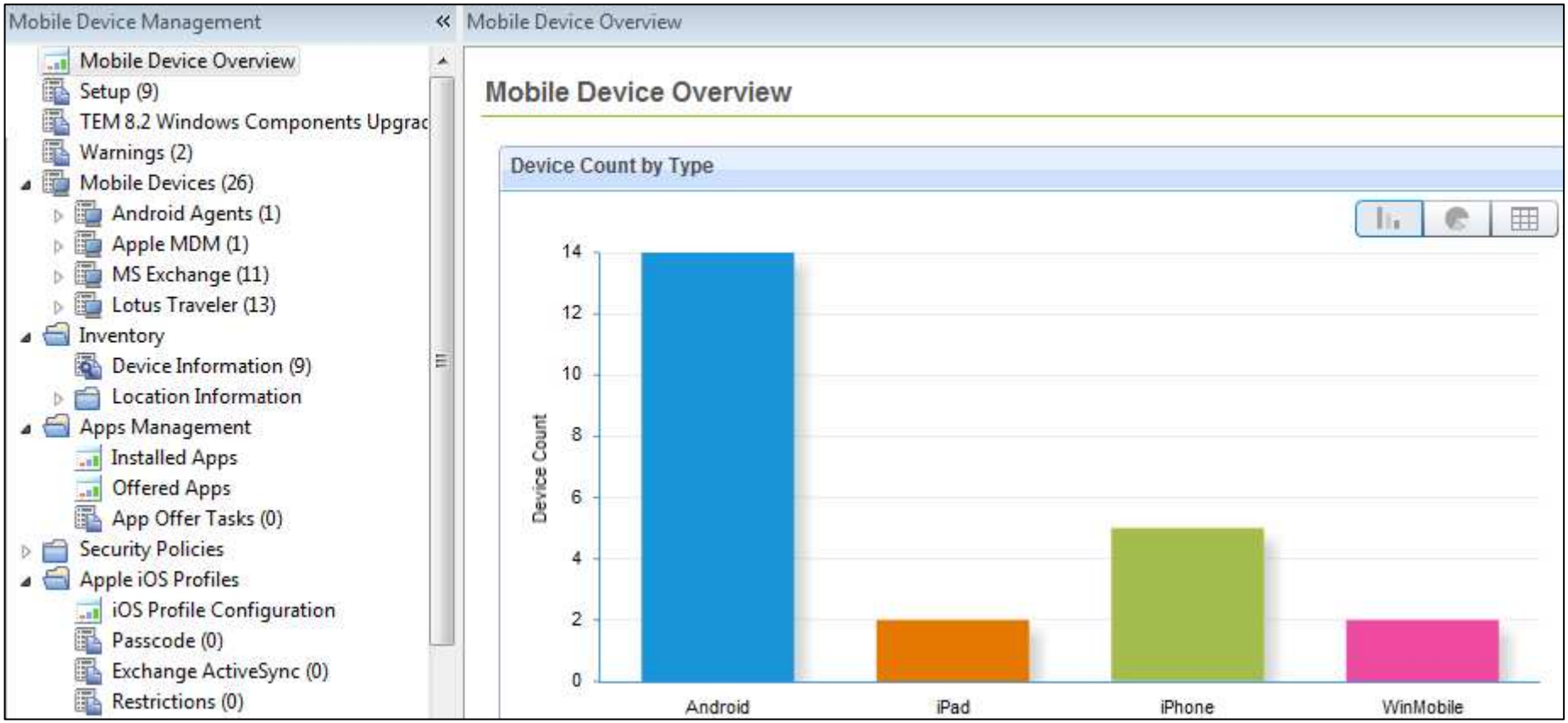
Mobil eszközök felügyelete

- Biztonsági alapelvek kikényszerítése
  - jelszavak
  - eszköztitkosítás
  - titkosított mentés
  - távoli törlés
  - levelezés- és vállalati adathozzáférés-kontroll
- Jailbreak és root detektálás
- Szoftver és hardver nyilvántartás
- Szoftverterítés
- Támogatott rendszerek: Windows Phone, Android, Symbian, iOS
- Agent alapú + email alapú

Microsoft Exchange Server

Lotus Notes

Endpoint Manager for Mobile Devices Dashboard



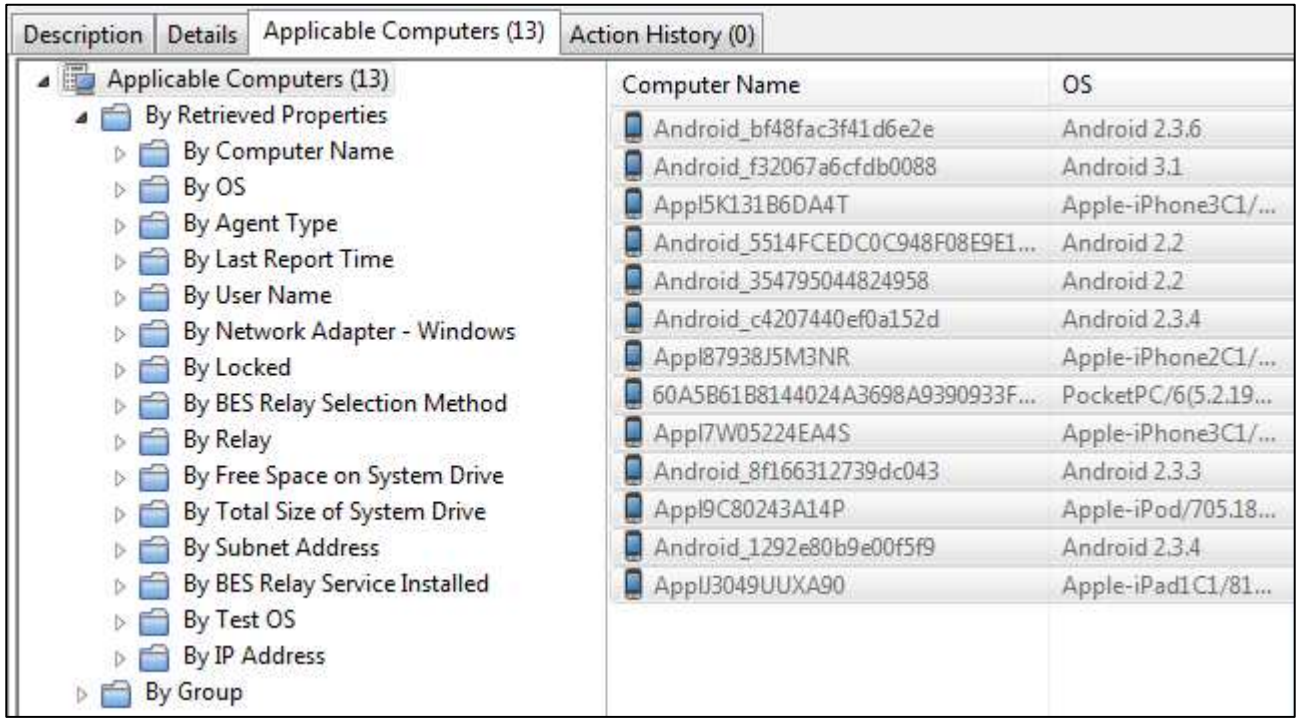
„Deny Email Access” szabály

Description

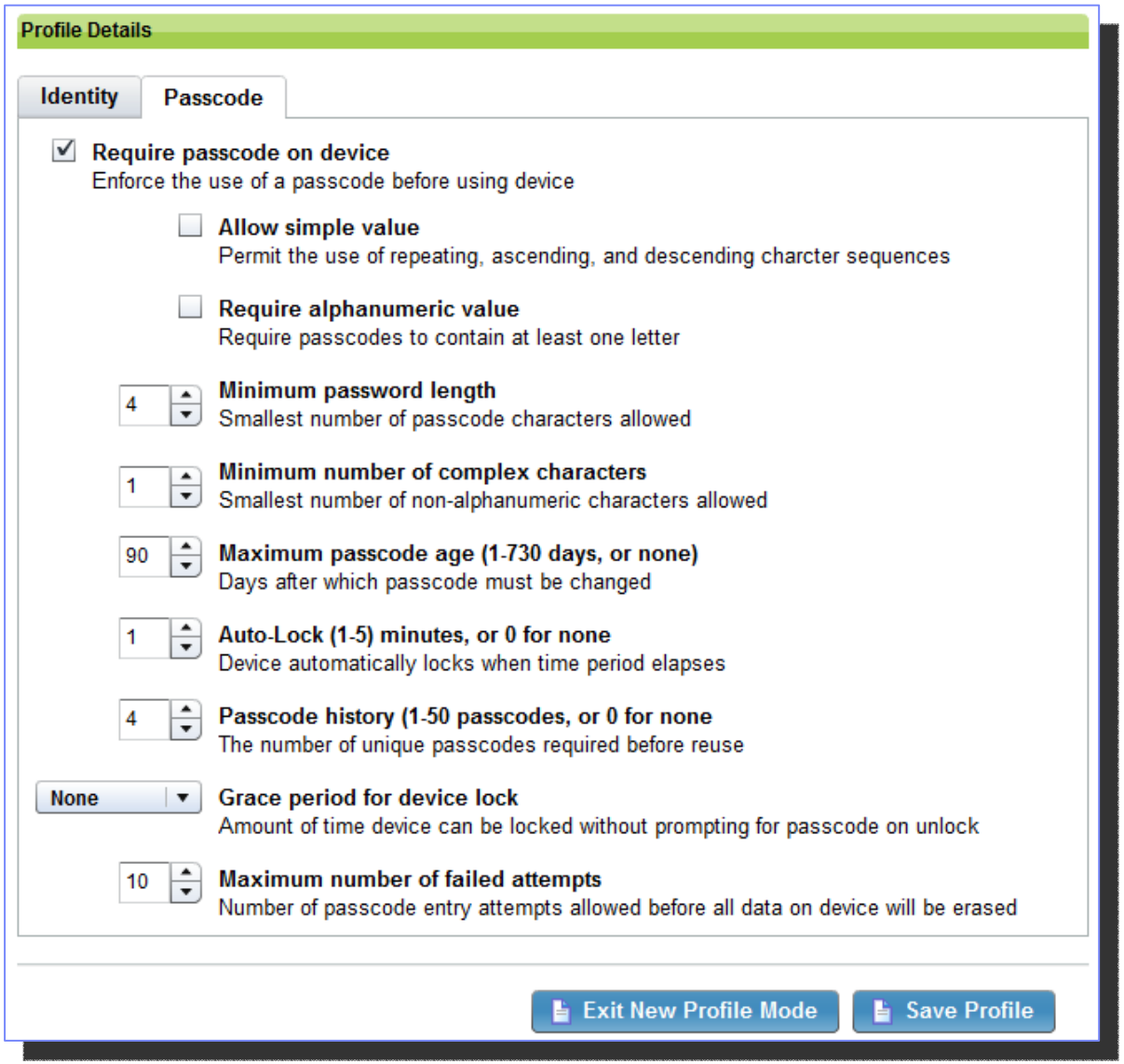
This task will deny targeted mobile devices access to their email server (Lotus Traveler or Microsoft Exchange). Use Allow Email Accessto restore access.

Actions

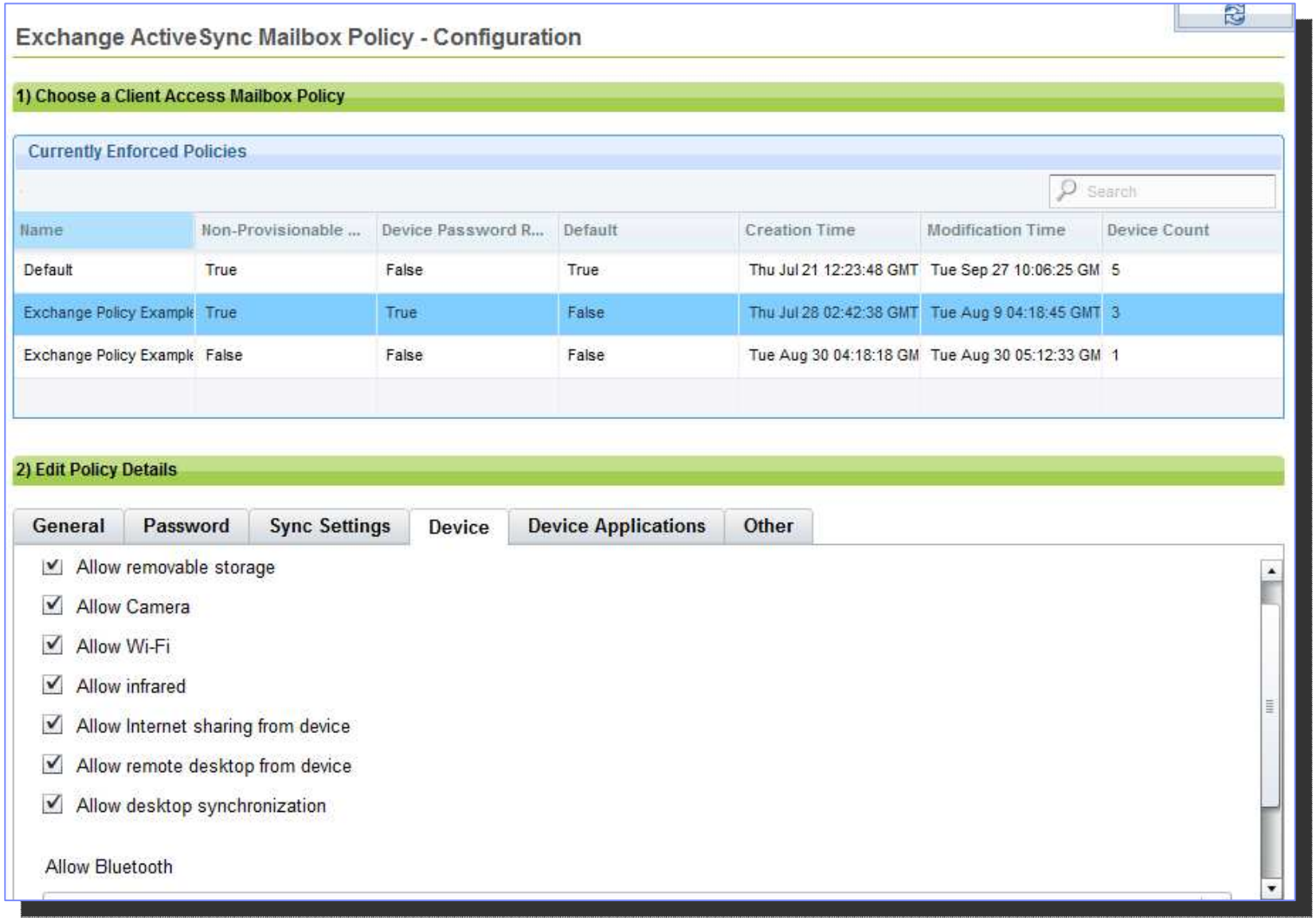
- Click here to deny email access.



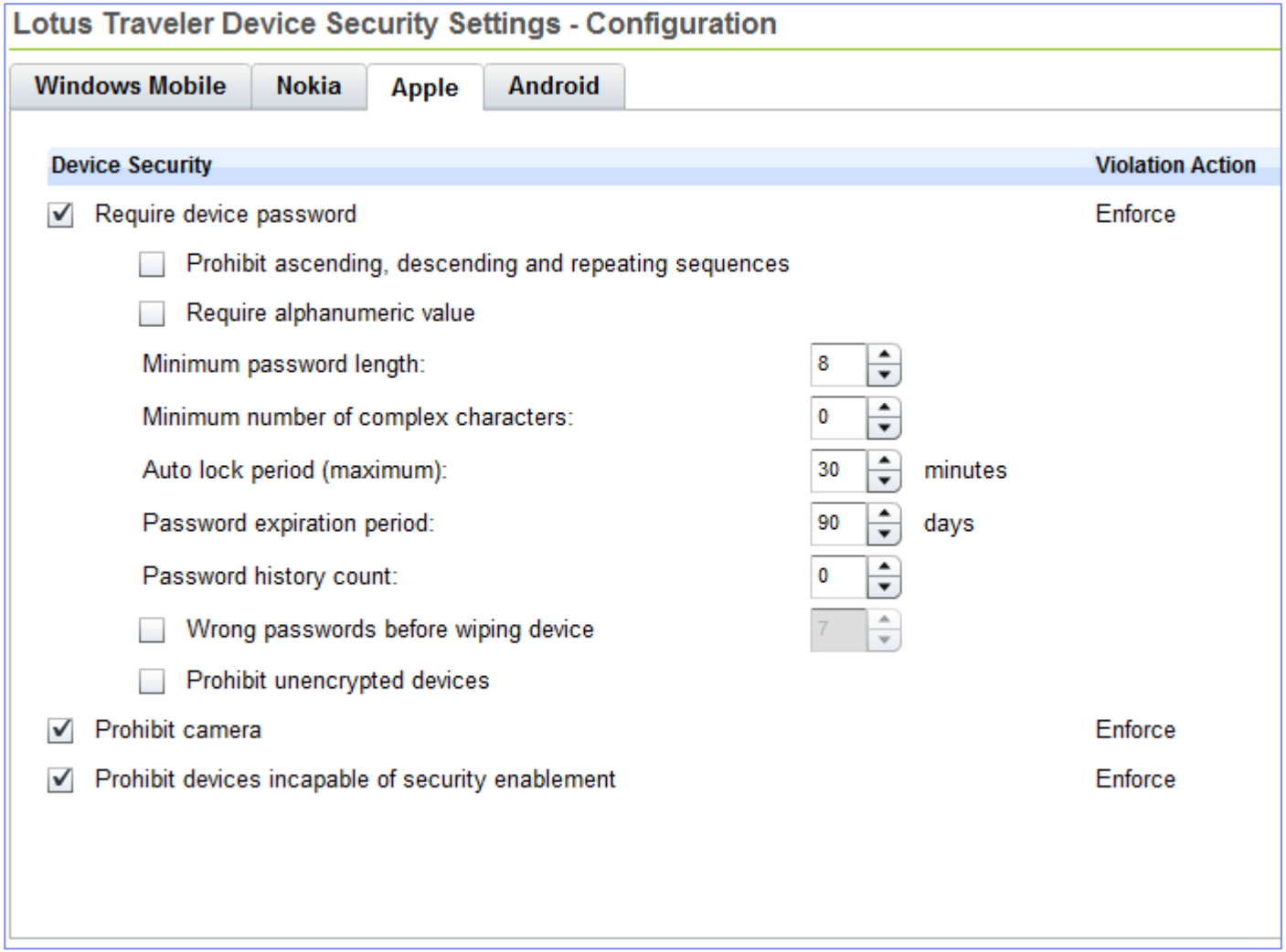
Felhasználóbarát iOS profilbeállítási varázsló az Apple MDM API-hoz



Exchange szabályok beállítása és kiküldése TEM konzolról



Lotus Traveler szabályok beállítása és kiküldése TEM konzolról



Köszönöm a figyelmet!