

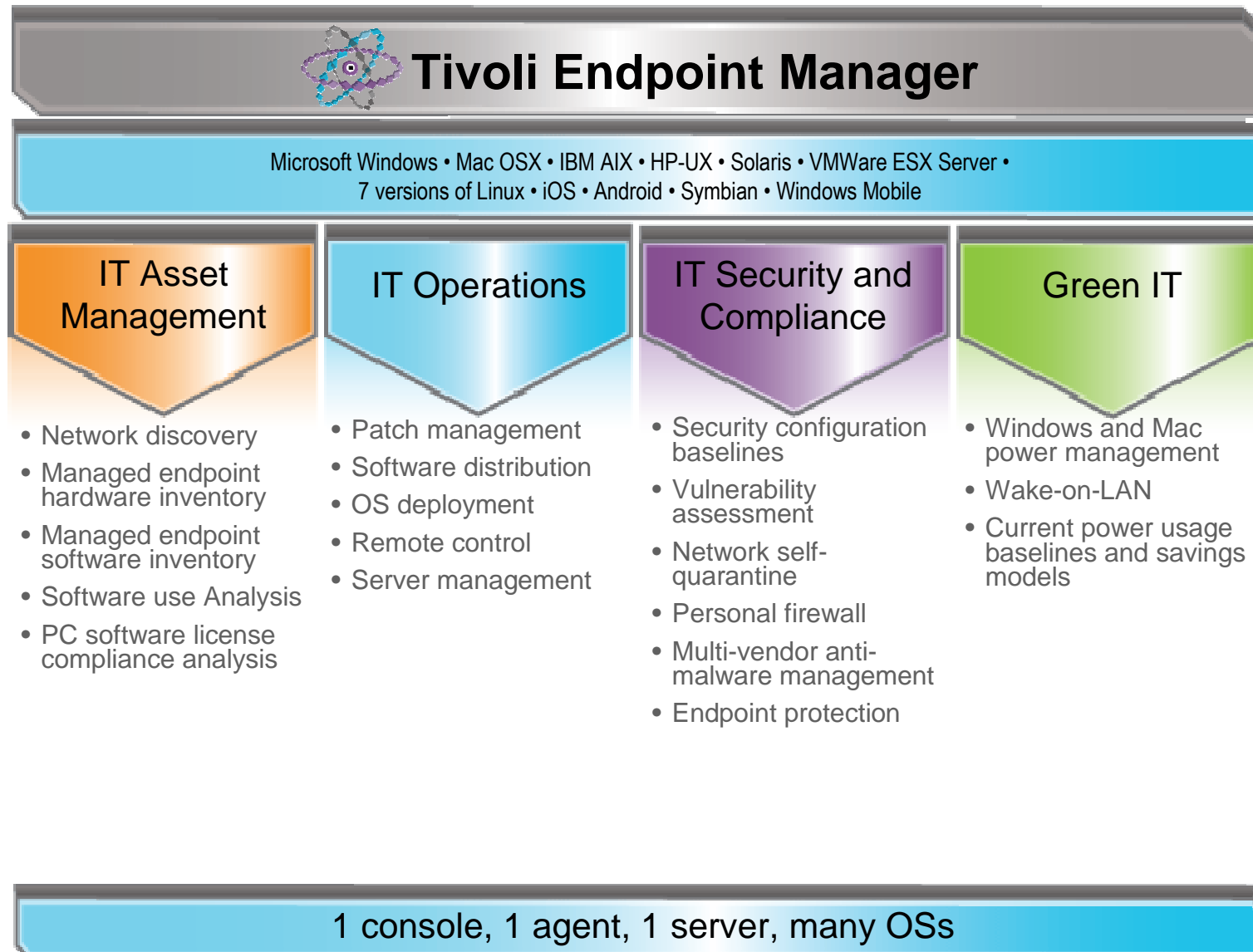
Egyenszilárd biztonság



... 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

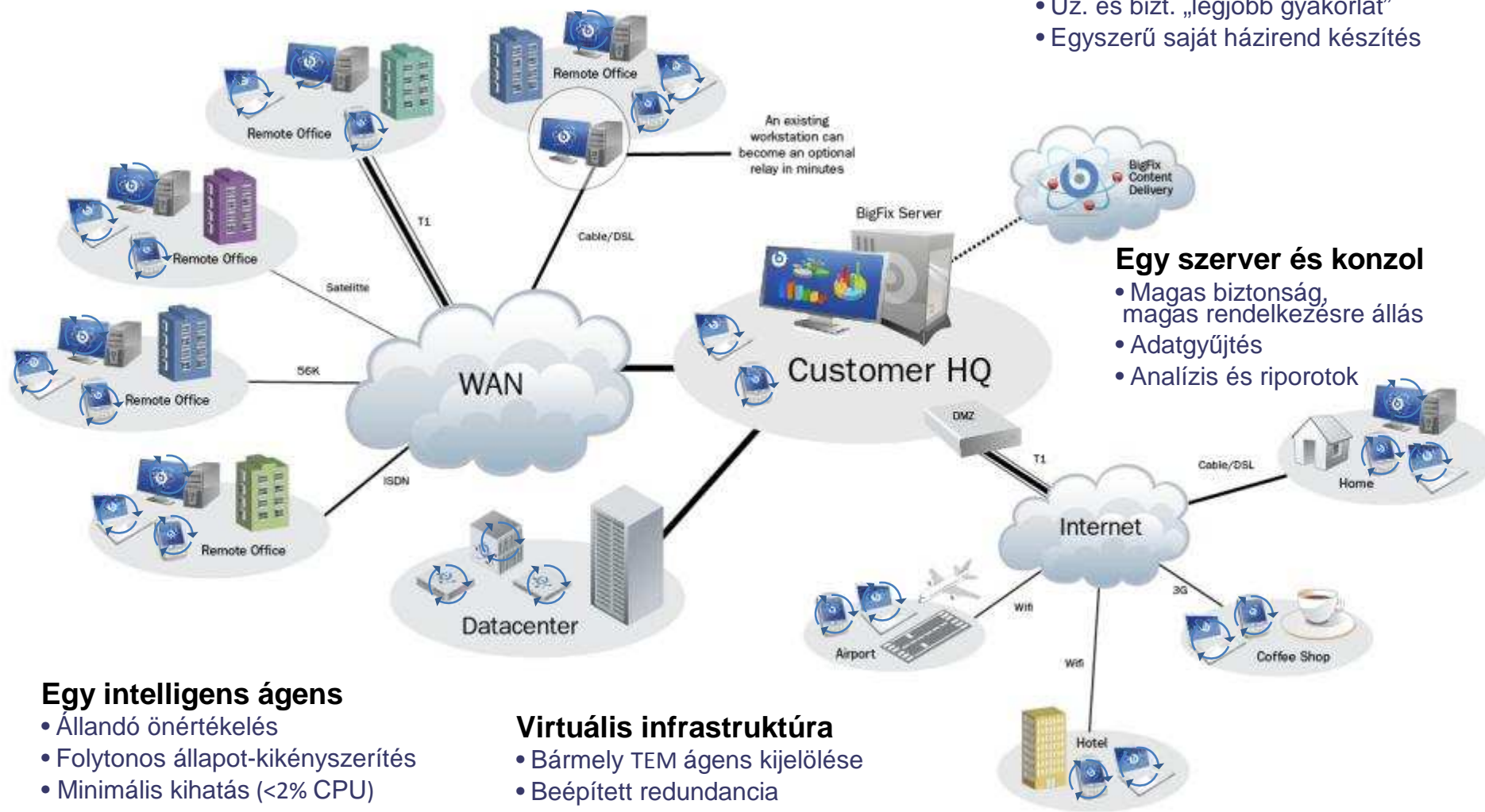
„[...] Gondoltam, megosztom Veled és a srácokkal [...] A Microsoft javítások terítése reggel 5:00-kor indult április 20-án, összességében 579 047 terítendő javítással, ami nálunk ebben a pillanatban az eddigi legnagyobb ilyen jellegű vállalkozás volt. Ebből délután 3:00-ig 527 916 darab került végrehajtásra. 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 szervert és konzolt

- 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

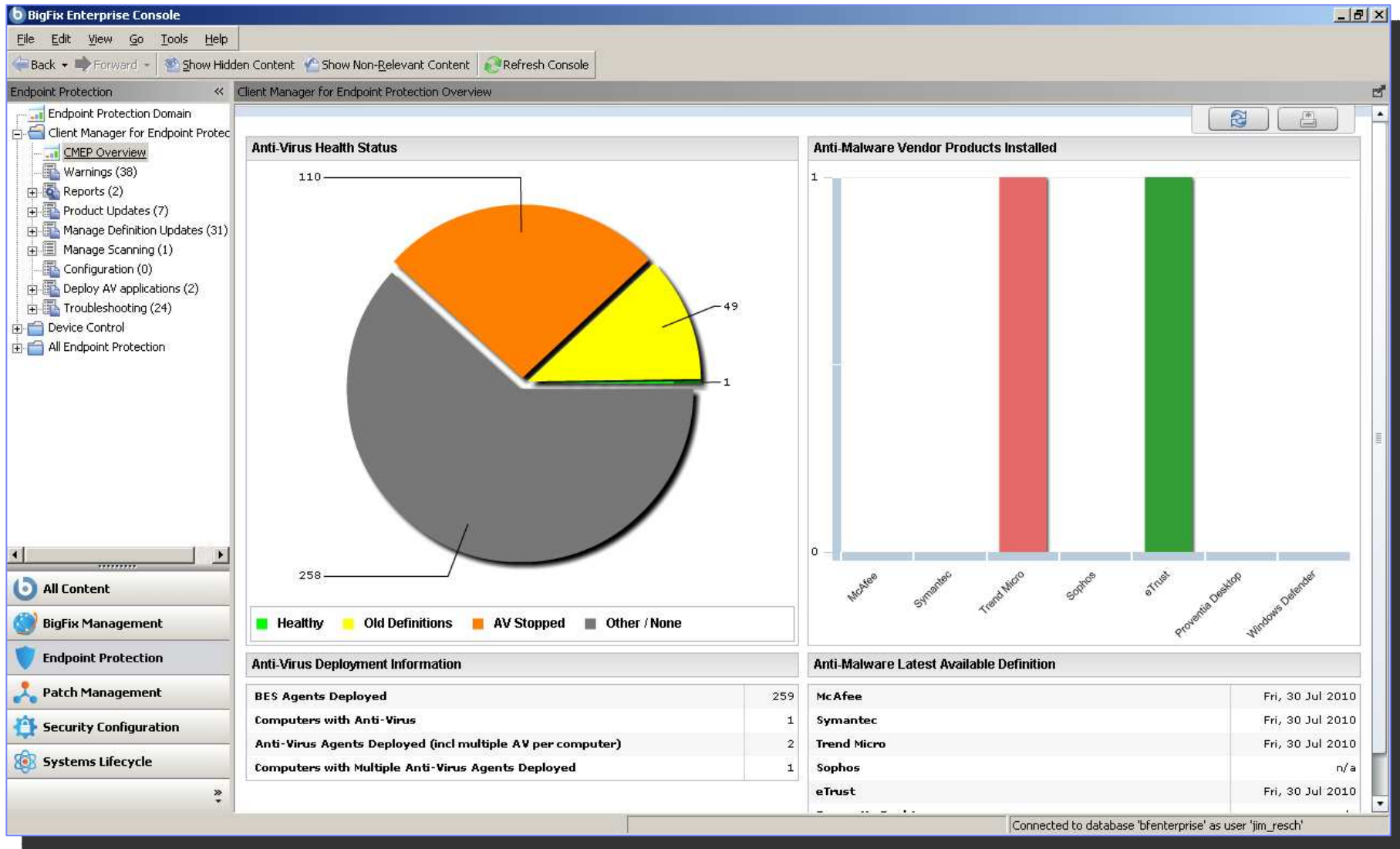
Microsoft Patch* Information		Total Patches Needed by Severity	
Patches Needed		Total Patches Needed by Severity	
Total Patches Needed:	51		
Total Critical Patches Needed:	8		
Computers Needing at least one Critical Patch:	3 (100%)		
Number of Relevant Patches (#/total)			
All Patches:	43 / 4,155		
Critical Patches:	8 / 1,518		
Average Relevant Patches per Computer			
All Patches:	17.00		
Critical Patches:	2.67		
* - A Microsoft patch is any security bulletin, security advisory, hotfix or service pack and excludes warnings, administrative tasks, and superseded content.			
Deployment Information		Severity of Relevant Patches	
BES Agents Deployed:	3		
Total Number of Windows Agents Deployed:	3		
Latest Microsoft Patches:	Tue, 14 Sep 2010		
Microsoft Patch Sites Subscribed:	Patches for Windows (English)		



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

Vulnerabilities to Windows Overview
Last updated 4/26/2011

Deployment Information

BES Agent Overview

BES Agents Deployed: 21

Total Number of Windows Agents Deployed: 13

Total Number of Agents Evaluating: 1 (7.6%)

Applicable Tasks:

[Vulnerabilities to Windows Systems: Enable "ACCEPTED" Evaluation](#)

[Vulnerabilities to Windows Systems: Disable "ACCEPTED" Evaluation](#)

Vulnerabilities to Windows Summary

Total Unique Detected Vulnerabilities

Total Unique Detected Vulnerabilities: 11

Total Unique Detected Vulnerabilities Rated High: 9

Total Unique Vulnerabilities: 2,655

Total Unique Detected Vulnerabilities Rated High: 1,853

Total Computers by Maximum Vulnerability Rating Summary

Total Computers by Vulnerability Rating

Total Computers with Maximum Vulnerability Rating of High: 1

Total Computers with Maximum Vulnerability Rating of Medium: 0

Total Computers with Maximum Vulnerability Rating of Low: 0

Total Computers with Maximum Vulnerability Rating of Unspecified: 0

Total Computers by Maximum Detected Vulnerability Rating

High (1)
Medium (0)
Low (0)
Unspecified (0)
None (12)

Severity of Uniquely Detected Vulnerabilities

High (9)
Medium (2)
Low (0)
Unspecified (0)

Total Detected Vulnerabilities by Severity

High: 9

© 2011 IBM Corporation

Biztonsági és megfelelőségi riportok

SCM Reports
FRIT Win XP Pro Workstation

Filters

Source Site (All | None)

FRIT Windows 2003 Server Security Test

FRIT Windows XP Professional Workstation

Jeffs Staples AIX 5.3

SCM Checklist for DISA STIG on Solaris

SCM Checklist for DISA STIG on Solaris

SCM Checklist for DISA STIG on Windows

SCM Checklist for FDCC on Windows Test

Staples SCM Checklist on AIX 5.1 Test

Staples SCM Checklist on AIX 5.2

Staples SCM Checklist on AIX 5.2 Test

Staples SCM Checklist on AIX 5.3 Test

Staples SCM Checklist on Windows 2003

UNIX_SCM

Check OS (All | None)

Windows XP

Check Type (All | None)

Application Log

Event Audit

File Security

Placeholders

Privilege Rights

Registry Values

Security Log

System Access

System Log

Non-Compliant Computers

0 4

Computer Filters (edit)

Windows Machines

Component Name	Non-Compliant	Applicable	Category	Identifier	OS	Standard	Enabled
Control-016.004 - Minimum Password Length - Windows XP	3	6	System Acce	Control-016.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>
Control-020.030 - Network access: Sharing and security model for local accounts -	3	6	Registry Val.	Control-020.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>
Control-016.003 - Minimum Password Age - Windows XP	3	6	System Acce	Control-016.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>
Control-017.001 - Account lock-out duration - Windows XP	3	6	System Acce	Control-017.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>
Control-020.031 - Network security: Do not store LAN Manager hash value on nex	3	6	Registry Val.	Control-020.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>
Control-020.010 - Devices: Unsigned driver installation behavior - Windows XP	3	6	Registry Val.	Control-020.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>
Control-020.028 - Network access: Do not allow storage of credentials or .NET Pas	3	6	Registry Val.	Control-020.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>
Control-020.017 - Interactive logon: Do not display last user name - Windows XP	3	6	Registry Val.	Control-020.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>
Control-020.027 - Network access: Do not allow anonymous enumeration of SAM	3	6	Registry Val.	Control-020.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>
Control-020.019 - Interactive logon: Message text for users attempting to log on	3	6	Registry Val.	Control-020.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>
Control-020.032 - Network security: LAN Manager Authentication Level - Windows	3	6	Registry Val.	Control-020.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>
Control-020.021 - Interactive logon: Number of previous logons to cache (in case	3	6	Registry Val.	Control-020.	Windows XP	FRIT Windows	<input checked="" type="checkbox"/>

Current Compliance Level

67.04%

Cumulative Compliance State

Computers by Compliance Percentage

Compliance Percentage	Number of computers
0%-10%	0
10%-20%	0
20%-30%	0
30%-40%	0
40%-50%	1
50%-60%	2.8
60%-70%	0
70%-80%	0
80%-90%	0
90%-100%	2

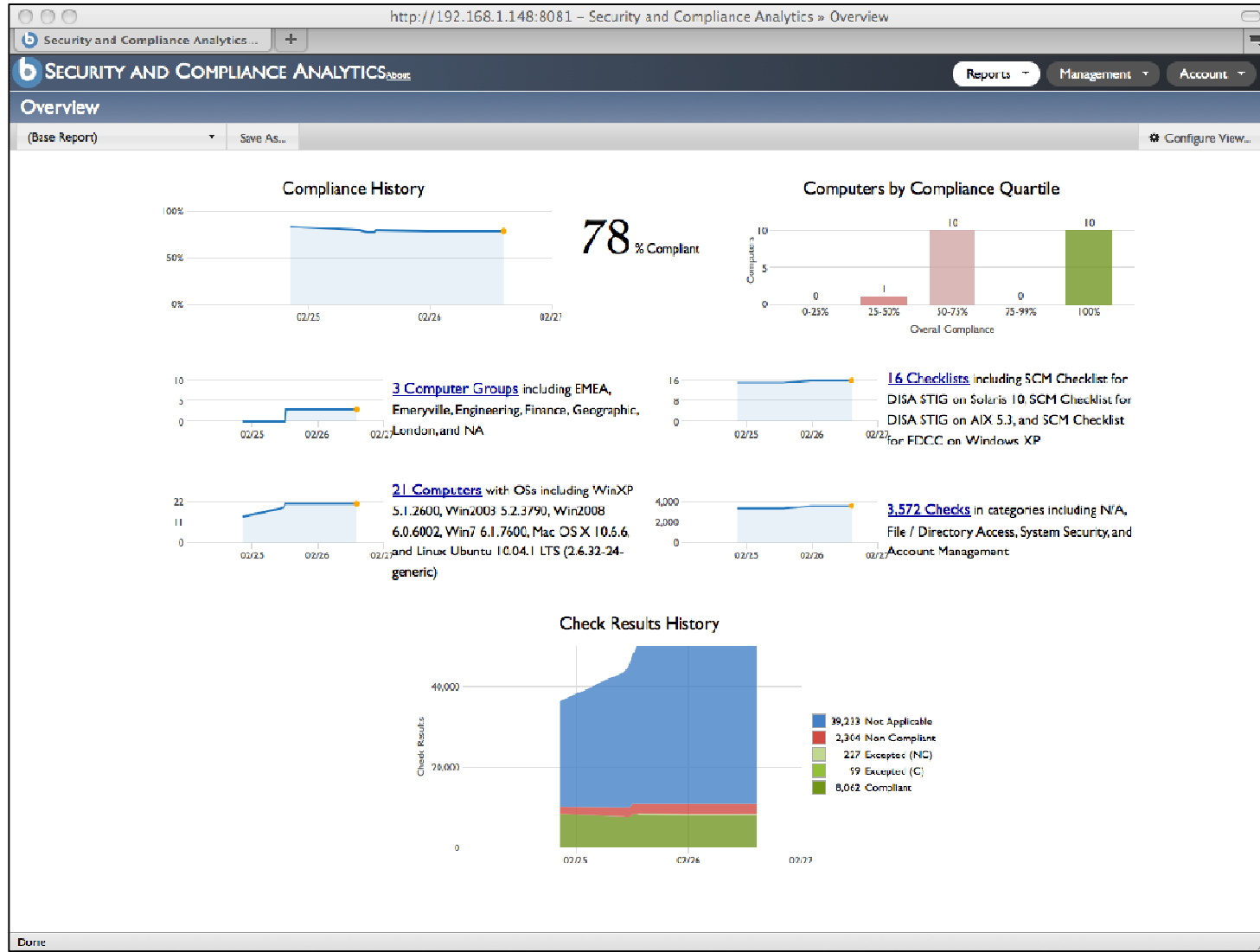
Non-Compliance by Category

Average Compliance by Category

Category	Average System Compliance
Registry Values	85
File Security	75
System Log	70
Security Log	55
Application Log	55
Event Audit	55
Placeholders	55
Privilege Rights	55

© 2011 IBM Corporation

Trendfelismerés és analízis riportozással

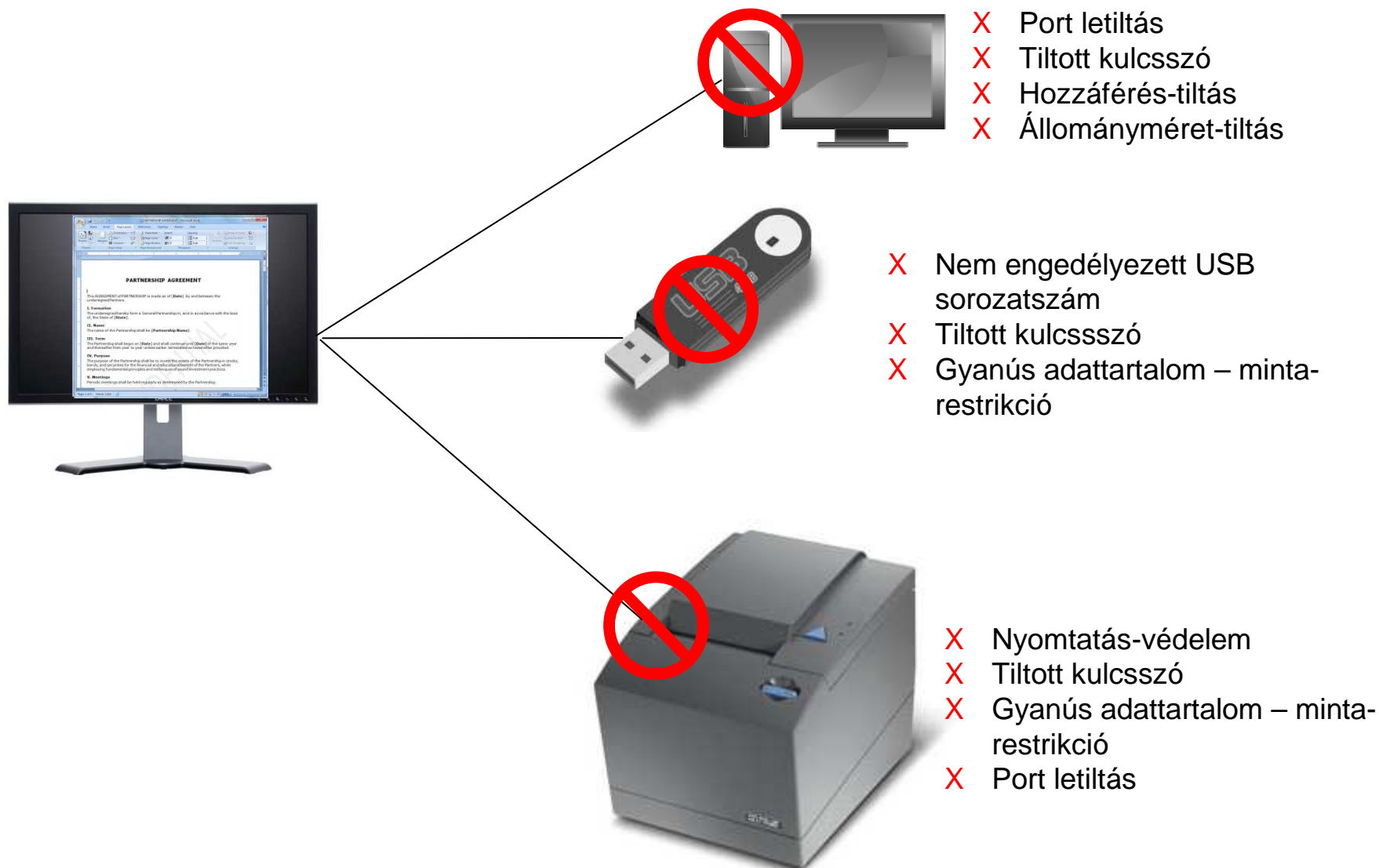




Valós idejű malware és sebezhetőség elleni védelem

- 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



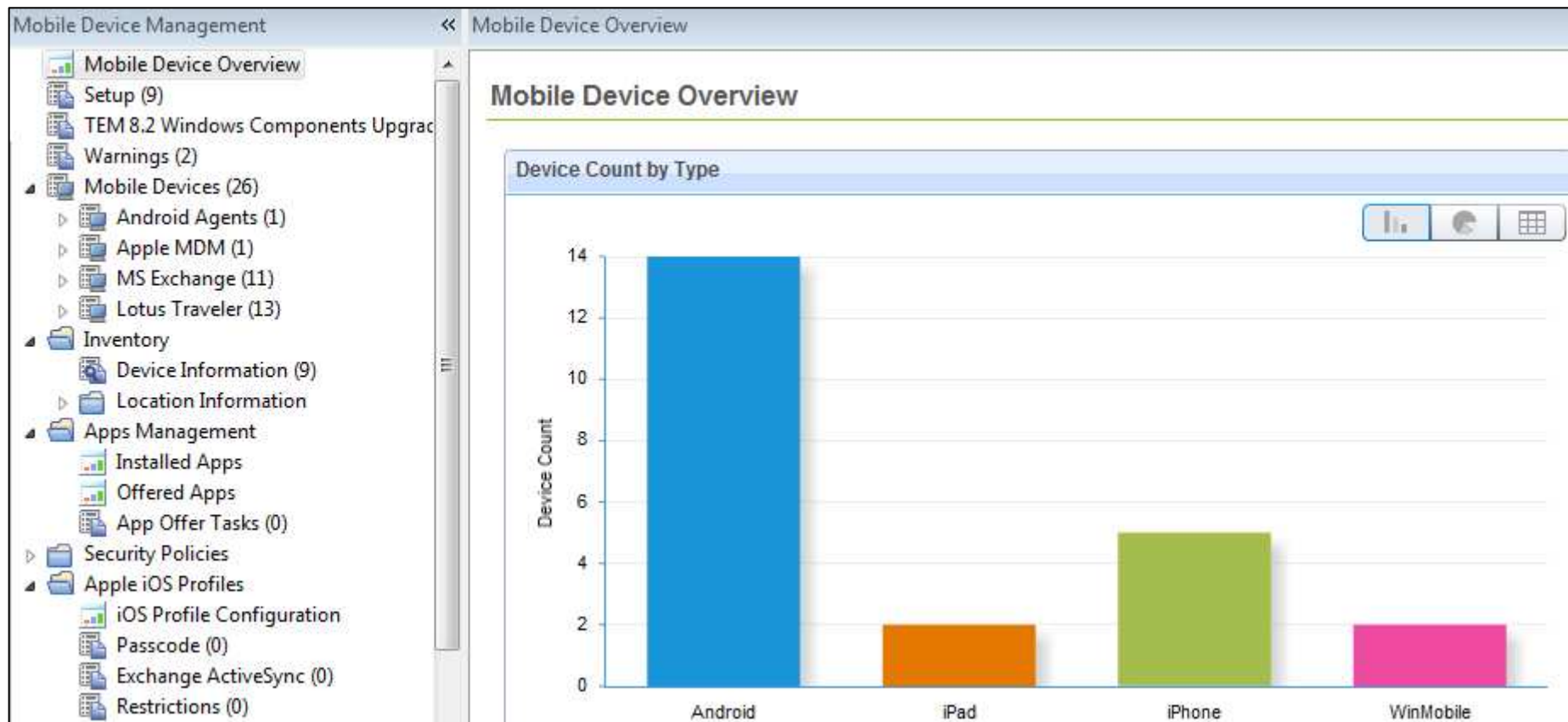


Mobil eszközök felügyelete

- 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



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 Access to restore access.

Actions
<input checked="" type="radio"/> Click here to deny email access.

Description	Details	Applicable Computers (13)	Action History (0)																												
<ul style="list-style-type: none"> Applicable Computers (13) <ul style="list-style-type: none"> By Retrieved Properties <ul style="list-style-type: none"> By Computer Name By OS By Agent Type By Last Report Time By User Name By Network Adapter - Windows By Locked By BES Relay Selection Method By Relay By Free Space on System Drive By Total Size of System Drive By Subnet Address By BES Relay Service Installed By Test OS By IP Address By Group 		<table border="1"> <thead> <tr> <th>Computer Name</th> <th>OS</th> </tr> </thead> <tbody> <tr><td>Android_bf48fac3f41d6e2e</td><td>Android 2.3.6</td></tr> <tr><td>Android_f32067a6cfdb0088</td><td>Android 3.1</td></tr> <tr><td>AppI5K131B6DA4T</td><td>Apple-iPhone3C1/...</td></tr> <tr><td>Android_5514FCEDC0C948F08E9E1...</td><td>Android 2.2</td></tr> <tr><td>Android_354795044824958</td><td>Android 2.2</td></tr> <tr><td>Android_c4207440ef0a152d</td><td>Android 2.3.4</td></tr> <tr><td>AppI87938J5M3NR</td><td>Apple-iPhone2C1/...</td></tr> <tr><td>60A5B61B8144024A3698A9390933F...</td><td>PocketPC/6(5.2.19...</td></tr> <tr><td>AppI7W05224EA4S</td><td>Apple-iPhone3C1/...</td></tr> <tr><td>Android_8f166312739dc043</td><td>Android 2.3.3</td></tr> <tr><td>AppI9C80243A14P</td><td>Apple-iPod/705.18...</td></tr> <tr><td>Android_1292e80b9e00f5f9</td><td>Android 2.3.4</td></tr> <tr><td>AppIj3049UUXA90</td><td>Apple-iPad1C1/81...</td></tr> </tbody> </table>	Computer Name	OS	Android_bf48fac3f41d6e2e	Android 2.3.6	Android_f32067a6cfdb0088	Android 3.1	AppI5K131B6DA4T	Apple-iPhone3C1/...	Android_5514FCEDC0C948F08E9E1...	Android 2.2	Android_354795044824958	Android 2.2	Android_c4207440ef0a152d	Android 2.3.4	AppI87938J5M3NR	Apple-iPhone2C1/...	60A5B61B8144024A3698A9390933F...	PocketPC/6(5.2.19...	AppI7W05224EA4S	Apple-iPhone3C1/...	Android_8f166312739dc043	Android 2.3.3	AppI9C80243A14P	Apple-iPod/705.18...	Android_1292e80b9e00f5f9	Android 2.3.4	AppIj3049UUXA90	Apple-iPad1C1/81...	
Computer Name	OS																														
Android_bf48fac3f41d6e2e	Android 2.3.6																														
Android_f32067a6cfdb0088	Android 3.1																														
AppI5K131B6DA4T	Apple-iPhone3C1/...																														
Android_5514FCEDC0C948F08E9E1...	Android 2.2																														
Android_354795044824958	Android 2.2																														
Android_c4207440ef0a152d	Android 2.3.4																														
AppI87938J5M3NR	Apple-iPhone2C1/...																														
60A5B61B8144024A3698A9390933F...	PocketPC/6(5.2.19...																														
AppI7W05224EA4S	Apple-iPhone3C1/...																														
Android_8f166312739dc043	Android 2.3.3																														
AppI9C80243A14P	Apple-iPod/705.18...																														
Android_1292e80b9e00f5f9	Android 2.3.4																														
AppIj3049UUXA90	Apple-iPad1C1/81...																														

Felhasználóbarát iOS profilbeállítási varázsló az Apple MDM API-hoz

Profile Details

Identity | **Passcode**

Require passcode on device
Enforce the use of a passcode before using device

Allow simple value
Permit the use of repeating, ascending, and descending character sequences

Require alphanumeric value
Require passcodes to contain at least one letter

Minimum password length
Smallest number of passcode characters allowed

Minimum number of complex characters
Smallest number of non-alphanumeric characters allowed

Maximum passcode age (1-730 days, or none)
Days after which passcode must be changed

Auto-Lock (1-5) minutes, or 0 for none
Device automatically locks when time period elapses

Passcode history (1-50 passcodes, or 0 for none)
The number of unique passcodes required before reuse

Grace period for device lock
Amount of time device can be locked without prompting for passcode on unlock

Maximum number of failed attempts
Number of passcode entry attempts allowed before all data on device will be erased

Exchange szabályok beállítása és kiküldése TEM konzolról

Exchange ActiveSync Mailbox Policy - Configuration

1) Choose a Client Access Mailbox Policy

Currently Enforced Policies

Search

Name	Non-Provisionable ...	Device Password R...	Default	Creation Time	Modification Time	Device Count
Default	True	False	True	Thu Jul 21 12:23:48 GMT	Tue Sep 27 10:06:25 GM	5
Exchange Policy Exampk	True	True	False	Thu Jul 28 02:42:38 GMT	Tue Aug 9 04:18:45 GMT	3
Exchange Policy Exampk	False	False	False	Tue Aug 30 04:18:18 GM	Tue Aug 30 05:12:33 GM	1

2) Edit Policy Details

General Password Sync Settings Device Device Applications Other

- Allow removable storage
- Allow Camera
- Allow Wi-Fi
- Allow infrared
- Allow Internet sharing from device
- Allow remote desktop from device
- Allow desktop synchronization
- Allow Bluetooth

Lotus Traveler szabályok beállítása és kiküldése TEM konzolról

Lotus Traveler Device Security Settings - Configuration		
Windows Mobile Nokia Apple Android		
Device Security		Violation Action
<input checked="" type="checkbox"/> Require device password		Enforce
<input type="checkbox"/> Prohibit ascending, descending and repeating sequences <input type="checkbox"/> Require alphanumeric value Minimum password length: <input type="text" value="8"/>		
Minimum number of complex characters:	<input type="text" value="0"/>	
Auto lock period (maximum):	<input type="text" value="30"/>	minutes
Password expiration period:	<input type="text" value="90"/>	days
Password history count:	<input type="text" value="0"/>	
<input type="checkbox"/> Wrong passwords before wiping device <input type="checkbox"/> Prohibit unencrypted devices	<input type="text" value="7"/>	
<input checked="" type="checkbox"/> Prohibit camera		Enforce
<input checked="" type="checkbox"/> Prohibit devices incapable of security enablement		Enforce

Köszönöm a figyelmet!

