

# Rendszerüzemeltetés új perspektívája

**Greff Zsolt**

Rendszermérnök

**KASPERSKY** Certified Professional

**SOPHOS** Certified Engineer



## System Management – Kinek lesz a barátja... ???

### Ahol az IT üzemeltetési feladatok

- egyáltalán nem vagy kevésbé támogatottak
  - vegyes eszközökkel megvalósítottak
  - jól kezelhető, egységes, folyamatorientált megoldás szükséges
- + speciális területek és igények...



## System Management – Üzemeltetési eszközkészlet

- Software and Hardware Asset Management
- License Management
- Microsoft Patch and Update Management
- 3rd Party Vulnerability Management
- 3rd Party Remote Installation
- OS Deployment
- Network Access Control (NAC)



# Rendszerkomponensek

**Kaspersky Security Center**

File Action View Help

Administration Server SRV01KSC10

- Managed computers
  - Servers
  - Workstations
- Administration Server tasks
- Tasks for specific computers
- User accounts
- Reports and notifications
  - Events
  - Computer selections
  - Anti-virus database usage report
  - Applications registry report
  - Errors report
  - Incompatible applications report
  - Kaspersky Lab software version report
  - Key usage report
  - Most infected computers report
  - MyReport-Applications changes
  - MyReport-Configuration changes
  - MyReport - License monitoring Notepa...
  - Protection deployment report
  - Protection status report
  - Report on blocked runs
  - Report on Device Control events
  - Report on hardware registry
  - Report on users of the computers
  - Software updates report
  - Users of infected computers report
  - Viruses report
  - Vulnerabilities report
  - Web Control report
- Applications and vulnerabilities
- Remote installation
- Encryption and data protection
- Mobile devices
- Unassigned computers
- Repositories

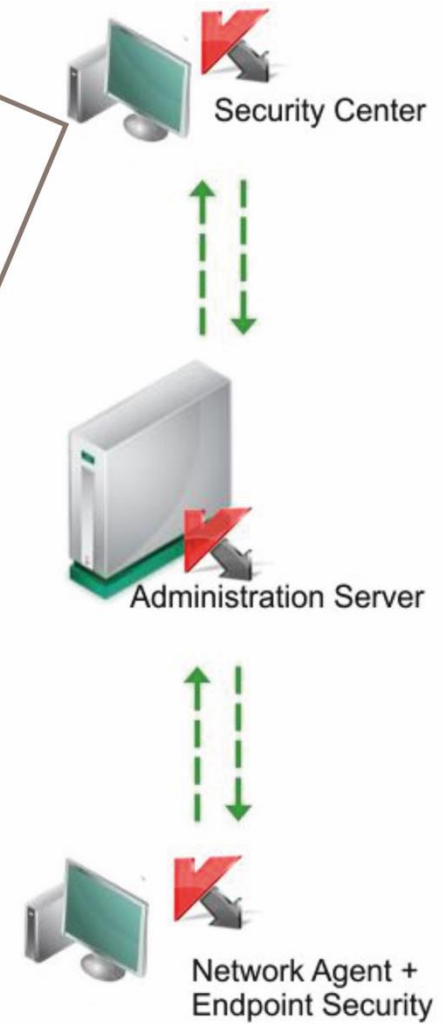
**Client computers**

- + Add computers
- Configure parameters of computer status discovery
- Add/Remove columns
- Refresh

Name	OS type	Domain	Agen...	Visible	Last
W5001KES10	Microsoft Wind...	TEST	+ / +	1 minute ago	4 ho
W5002KES10	Microsoft Wind...	TEST	+ / +	1 minute ago	4 ho

Kimutatások, események, dinamikus csoportok

Funkciók



## System Management – Rendszerkövetelmények

azonos a Kaspersky Administration Server követelményeivel

- + 100 GB a funkciók részére (pacth-ek, image-k, stb...)
- külön licence szükséges



<http://support.kaspersky.com/ksc10#requirements>

# Hardware Inventory

# Hardverelemek naprakész lekérdezése

**Kaspersky Security Center**

**Report on hardware registry**  
Monday, October 27, 2014 11:46  
The report contains information about motherboards, CPUs, RAM, and hard drives for all groups

**Device:**

- Intel(R) Core(TM)2 Quad CPU Q8400 @ 2.66GHz: 4
- XENSRC PVDISK SCSI Disk Device: 1
- XENSRC PVDISK SCSI Disk Device: 1
- Általános nem PnP-képernyő: 1
- Generic Non-PnP Monitor: 1
- HVM domU: 2
- Citrix PV Network Adapter: 2
- QEMU QEMU DVD-ROM ATA Device: 1
- QEMU QEMU DVD-ROM ATA Device: 1
- Physical Memory: 2
- Standard VGA Graphics Adapter: 1

**Summary:**

Device type	Device name	Manufacturer	Numl
CPU	Intel(R) Core(TM)2 Quad CPU Q8400 @ 2.66GHz	Intel	4
Memory device	XENSRC PVDISK SCSI Disk Device	(Standard disk drives)	1
Memory device	XENSRC PVDISK SCSI Disk Device	(Szabványos lemez meghajtó)	1
Monitor	Általános nem PnP képernyő	(Szabványos monitortípusok)	1
Monitor	Generic Non-PnP Monitor	(Standard monitor types)	1
Motherboard	HVM domU	Xen	2
Network adapter	Citrix PV Network Adapter	Citrix Systems Inc.	2
Optical drive	QEMU QEMU DVD-ROM ATA Device	(Normál CD-ROM-meghajtók)	1
Optical drive	QEMU QEMU DVD-ROM ATA Device	(Standard CD-ROM drives)	1
RAM	Physical Memory		2
Video adapter	Standard VGA Graphics Adapter	(Standard display types)	1
Video adapter	Szabványos VGA grafikus adapter	(Szabványos képernyőtípusok)	1

**All devices: 18**

# Hardver-konfigurációs változások nyomon követése

**Kaspersky Security Center**

**Report on configuration changes** Monday, October 27, 2014 10:42:57 AM

The report contains information about changes in computer configuration and devices connected to computer for specific computers  
 Period: from Monday, October 27, 2014 to Monday, October 27, 2014

**Details 2 of 2**

Virtual Server	Group	Client computer	Event	Detection time
	Workstations	WS001KES10	Device 'Physical Memory' removed.	Monday, October 27, 2014 10:12:50 AM
	Workstations	WS001KES10	Device 'Physical Memory' added.	Monday, October 27, 2014 10:12:50 AM

# Application Distribution

# System Management – Application Distribution

## Távtelepítési lehetőségek

- Network Agent
- Microsoft eszközök

## Telepíthető állományok

- **Kaspersky Lab** alkalmazások
- **Egyéni telepítő állományok** (exe, msi, msp, bat, cmd)
  - Parancssori kapcsolók használata
- Előre definiált **harmadik feles csendes** telepítőkészletek
- Operációs rendszer **lemezképek**

# Application Inventory

# Részletes alkalmazásinformációk

**Kaspersky Security Center**

Getting started > Applications and vulnerabilities > Applications registry

## Applications registry

Applications registry contains detailed information about the applications installed on managed computers.

- Show applications registry properties window
  - View report on applications installed in the network
  - Add/Remove columns
  - Refresh

Number of days:   Group applications by name  Display installed application only

Name	Version
Windows Driver Package - Citrix Systems Inc. (xenbus) System (05/09/201...	05/09/201...
Total Commander (Remove or Repair)	8.01
ThinkPad UltraNav Driver	16.2.19
SoundMAX	6.10.1...
Sophos SSL VPN Client 2.1	2.1
Skype™ 6.21	6.21.10
Skype Click to Call	7.3.169
Remote Desktop Connection Manager	2.2.04
MSXML 4.0 SP3 Parser (KB973685)	4.30.2...
MSXML 4.0 SP3 Parser (KB2758694)	4.30.2...
Mozilla Maintenance Service	32.0.3
Mozilla Maintenance Service	17.0.1
Mozilla Firefox 32.0.3 (x86 hu)	32.0.3
<b>Mozilla Firefox 17.0.1 (x86 hu)</b>	<b>17.0.1</b>
Microsoft SQL Server VSS Writer	10.52.4...
Microsoft SQL Server Browser	10.52.4...
Microsoft SQL Server 2008 Setup Support Files	10.1.2...
Microsoft SQL Server 2008 R2 Setup (English)	10.52.4...
Microsoft SQL Server 2008 R2 Native Client	10.52.4...

Applications in database: 53

# Telepített alkalmazások listája és visszakövetése

The screenshot displays the Kaspersky Security Center interface. The 'Computers' tab is selected in the top navigation bar. In the left-hand tree view, 'Managed computers' is expanded, and 'Workstations' is highlighted. The main pane shows the 'Applications registry' for computer 'WS001KE510'. A list of installed applications is shown, with 'Microsoft Silverlight 5.1.30214.0' and 'Microsoft Windows QFE' highlighted by a green box. Below the list, the 'History' button is highlighted with a red box. An 'Events' window is open in the foreground, showing a log of application removal and installation events.

Time	Description
Thursday, October 23, 2014 1:15:47 AM	'Microsoft Silverlight' has been removed
Thursday, October 23, 2014 1:15:47 AM	'Microsoft Silverlight' has been installed
Thursday, October 23, 2014 1:13:50 AM	'Microsoft Silverlight' has been removed
Thursday, October 23, 2014 1:13:50 AM	'Microsoft Silverlight' has been installed
Wednesday, October 22, 2014 6:28:51 AM	'Microsoft Windows QFE' has been installed
Wednesday, October 22, 2014 5:51:30 AM	'Microsoft Windows QFE' has been removed
Wednesday, October 22, 2014 3:58:07 AM	'Microsoft Silverlight' has been installed

# Szoftverkörnyezet változásainak követése

**Kaspersky Security Center**

File Action View Help

Kaspersky Security Center Administration Server SRV01KSC10

- Managed computers
  - Servers
  - Workstations
- Administration Server tasks
- Tasks for specific computers
- User accounts
- Reports and notifications**
  - Events
  - Computer selections
  - Anti-virus database usage report
  - Applications registry report
  - Errors report
  - Incompatible applications report
  - Kaspersky Lab software version report
  - Key usage report
  - Most infected computers report
  - MyReport-Applications changes**
  - MyReport-Configuration changes
  - Protection deployment report
  - Protection status report
  - Report on blocked runs
  - Report on Device Control events
  - Report on hardware registry
  - Report on users of the computer
  - Software updates report
  - Users of infected computers report
  - Viruses report
  - Vulnerabilities report
  - Web Control report
- Applications and vulnerabilities
- Remote installation
- Mobile devices
- Unassigned computers
- Repositories

**Report on applications registry history** Monday, October 27, 2014 2:37:28 PM

Applications installation/removal report for a group "Workstations"

Period: from Saturday, September 27, 2014 to Monday, October 27, 2014

**Applications:**

- Microsoft Silverlight installed: 1
- Microsoft Silverlight removed: 1
- Microsoft Silverlight removed: 1
- Microsoft Silverlight installed: 1
- Microsoft Silverlight installed: 1
- Microsoft Windows QFE installed: 1
- Microsoft Windows QFE removed: 1

**Summary:**

Event	Application	Version number	Manufacturer	Total events	Number of computers	Number of
Application has been installed	Microsoft Silverlight	5.1.10411.0	Microsoft Corporation	1	1	1
Application has been installed	Microsoft Silverlight	5.1.20513.0	Microsoft Corporation	1	1	1
Application has been installed	Microsoft Silverlight	5.1.30214.0	Microsoft Corporation	1	1	1
Application has been installed	Microsoft Windows QFE	N/A	N/A	1	1	1
Application has been removed	Microsoft Silverlight	5.1.10411.0	Microsoft Corporation	1	1	1
Application has been removed	Microsoft Silverlight	5.1.20513.0	Microsoft Corporation	1	1	1
Application has been removed	Microsoft Windows QFE	N/A	N/A	1	1	1
<b>Events (total): 7</b>				<b>Installations: 4</b>	<b>Removals: 3</b>	

**Details 7 of 7**

Event	Application	Version number	Manufacturer	Detected on	Virtual Server	Group	Client computer	Description	IP address	Visible	Last connecti Administ Server

# Futtatható állományok nyilvántartása

The screenshot displays the Kaspersky Security Center interface. On the left, the 'Applications and vulnerabilities' section is expanded, with 'Executable files' highlighted. The main pane shows a list of executable files, with 'firefox.exe' selected. A 'Properties: firefox.exe' dialog box is open, showing the following details:

General	
File name:	firefox.exe
File version:	17.0.1
Application name:	Firefox
Application version:	17.0.1
Copyright:	Mozilla Corporation
Trust level:	Trusted
Discovered in network:	10/27/2014 3:44:21 PM
First start in the network:	10/27/2014 3:30:45 PM
<a href="#">View description on Kaspersky Lab website</a>	
File categories:	Browsers\Web Browsers

At the bottom of the dialog box, there are buttons for 'Add to category', 'Properties', and 'Computers'. The status bar at the bottom of the application window indicates 'Executable files: 128'.

# Futtatható állományok lekérdezése - Application Advisor

Kaspersky Application Advisor - Kaspersky Whitelist - Windows Internet Explorer

http://whitelist.kaspersky.com/advisor#search/5744FFF8E72D105C138DAE9E17BB29FE

**Kaspersky Application Advisor** - always the most complete information about your file or program

5744FFF8E72D105C138DAE9E17BB29FE Or Upload a file to calculate the hash sum...

What is a hash sum? Upload limited to 5 MB.

**Security** Safe

**User confidence** of 21 889 359 people

100%

Trusted Low Restricted High Restricted Do not trust

**Geographic range**

- Other - 49%
- Germany - 15%
- Russian Federation - 14%
- USA - 11%
- Vietnam - 6%
- India - 6%

**Certificate** Trusted

Details →

**Number of users**

- 2 860 last 24 hours
- 10 211 last week
- 27 553 last month

**File**

Original file name: firefox.exe  
 Vendor: Mozilla Corporation  
 Application: Firefox

Name: **firefox.exe**  
 Type: EXE: Windows executable  
 Size: 895.17 KB

MD5: 5744FFF8E72D105C138DAE9E17BB29FE  
 SHA1: 7C6586E3B8503EE6682D1DB0B0E4BE901618C8

# System Management – Application Categories

**Kaspersky Security Center**

File Action View Help

Getting started > Applications and vulnerabilities > Application categories

## Application categories

Categorizing applications allows you to enhance applications start management.

- + Create a category...
- Add/Remove columns
- Refresh

**Create User Category Wizard**

**Create User Category Wizard**

**Category type**

- Category with content added manually. Data of executable files are manually added to the category.
- Category with content added automatically. Executable files of applications copied to the specified folder are automatically processed, their metrics are added to the category.
- Category which includes executable files from selected computers. Such files are processed automatically and their metrics are added to the category.

Cancel

Application categories: 2

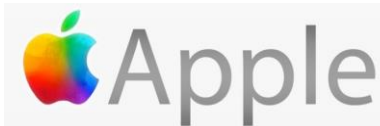
# Patch & Update Management

# System Management – Patch & Update Management

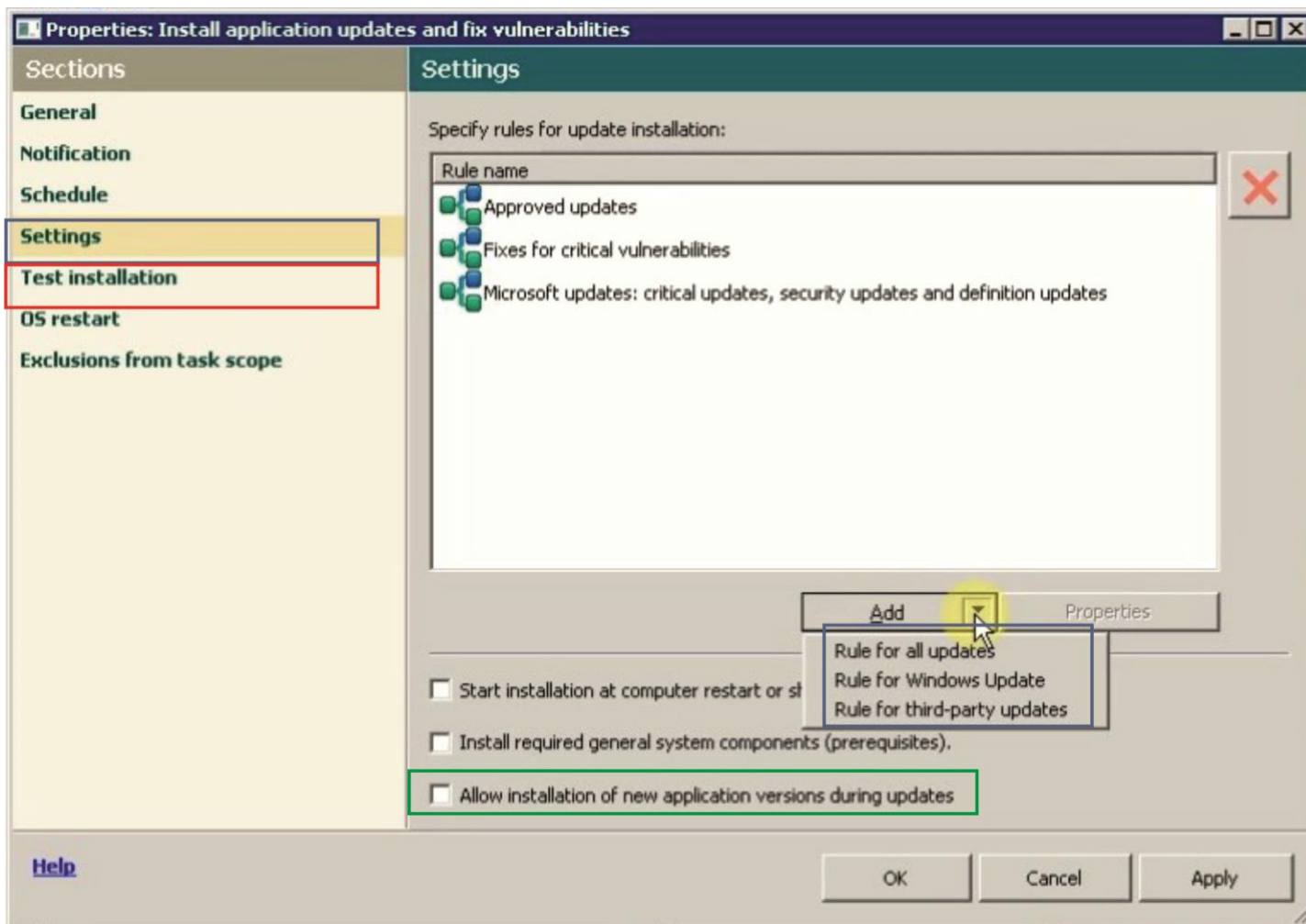
Minden kliensen, ahol a Network Agent telepítve van

- Microsoft és Adobe termékek automatizálható javítása (Patch Management)
- Frissítések 100+ támogatott alkalmazáshoz

Támogatott szoftverek teljes listája: <http://support.kaspersky.com/9327#>



# System Management – Patch & Update Management



# OS Deployment

# System Management – OS Deployment

## OS tömeges telepítése és rendszerkövetelményeik

1. Előtelepített OS (pl.: OS upgrade)
2. Bare-metal telepítés

### 1. Előtelepített OS követelmények

Kliens oldalon: KES10 **Network Agent** komponens

Szerver oldalon: KSC10, **Windows Automated Installation Kit (WAIK)**

### 2. Bare-metal követelmények

Kliens oldalon: -

Szerver oldalon: **PXE Boot Server és DHCP Server**

KSC10, **Windows Automated Installation Kit (WAIK)**

Microsoft források:

[http://technet.microsoft.com/en-us/library/ee523217\(v=ws.10\).aspx](http://technet.microsoft.com/en-us/library/ee523217(v=ws.10).aspx)

<http://www.microsoft.com/en-us/download/details.aspx?id=5753>

# Network Access Control

# System Management – Network Access Control

## Szabályok szerinti hálózat-hozzáférés korlátozás

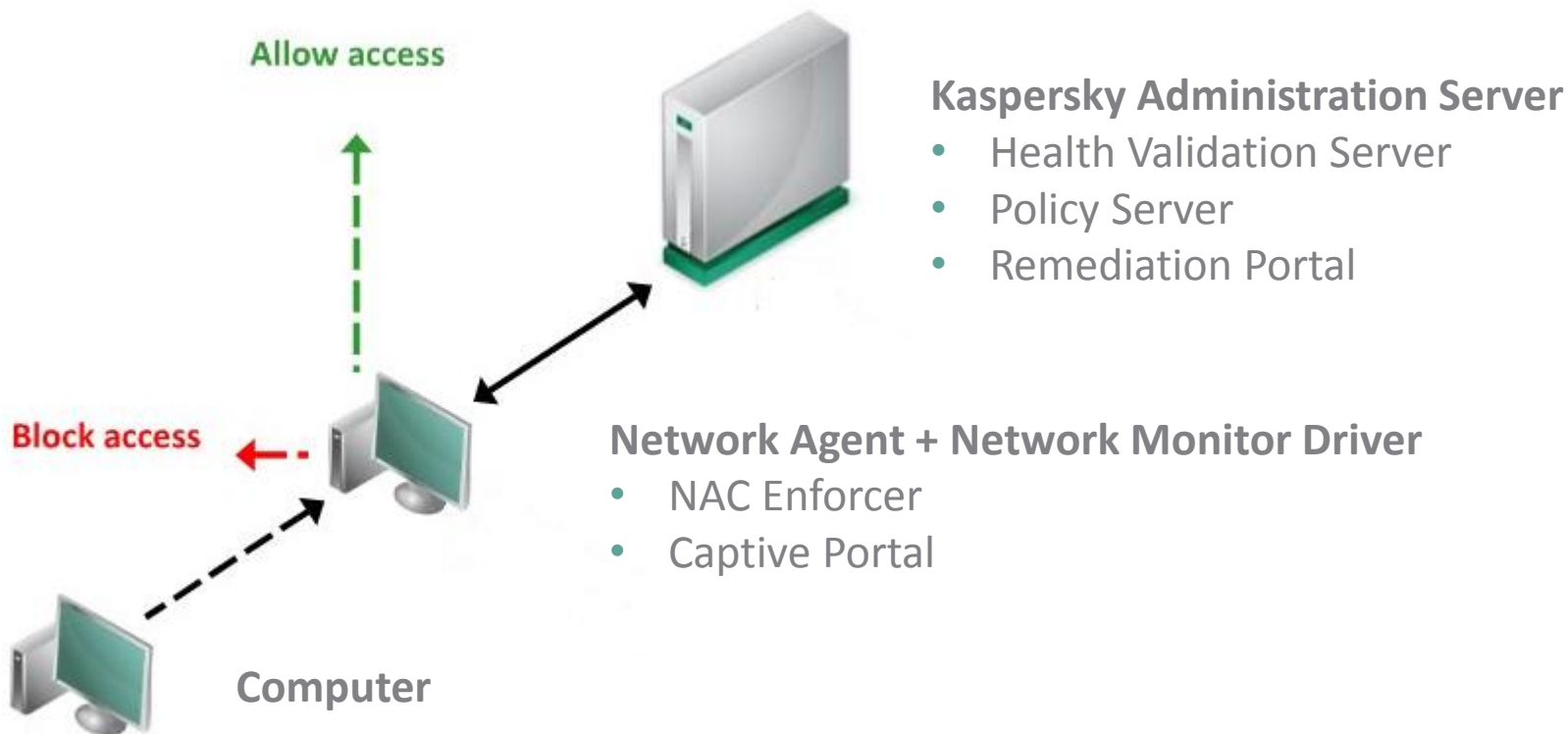
### Lehetséges forgatókönyvek

- Illetéktelen eszközök használatának megakadályozása
- Felügyelet nélküli és új végpontok kontrollált hálózati hozzáférése
- Nem megfelelő végpontok kizárása a hálózathoz
- ...

### Korlátozási lehetőségek

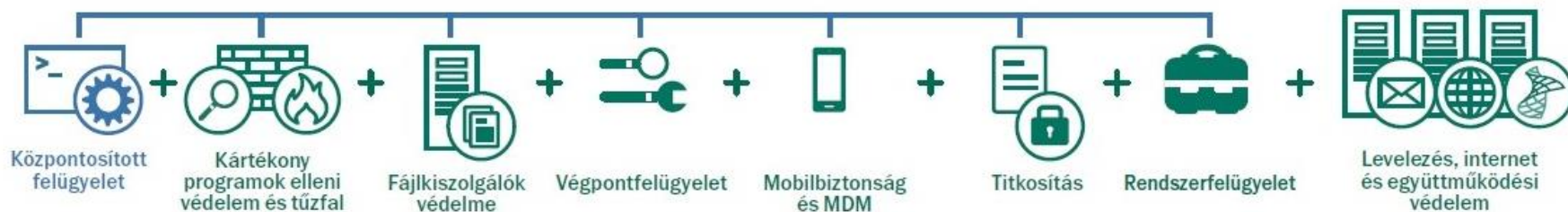
- Hozzáférés megakadályozása
- Korlátozott hálózati hozzáférés biztosítása
  - Izolált hálózat használata
  - Internet hozzáférés tiltása
- Ideiglenes hozzáférés biztosítása (Captive Portal)

# System Management – Network Access Control



## System Management – Licencsomagok

- Kaspersky **System Management**
- Kaspersky Endpoint Security for Business **ADVANCED**
- Kaspersky **TOTAL** Security for Business



## System Management – Összegzés

Nem csodafegyver, nem oldódik meg minden problémánk egy csapásra, de **hatékony üzemeltetési eszközkészlettel dolgozhatunk!**

- Egy **központosított felületen** minden funkció elérhető
- **Egyszerű telepítés és kezelhetőség**
  - Előre definiált eszközkészletek
  - Automatizált üzemeltetési folyamatok
- **Vállalati biztonság fokozása**
  - 3rd Party Patch Management
  - Teljes átláthatóság és kontrol

# Köszönöm a figyelmet!

**Greff Zsolt**

+ 36-30-465-0815

[zsgreff@newcotrading.hu](mailto:zsgreff@newcotrading.hu)

[www.newcotrading.hu](http://www.newcotrading.hu) | [mail@newcotrading.hu](mailto:mail@newcotrading.hu)

