

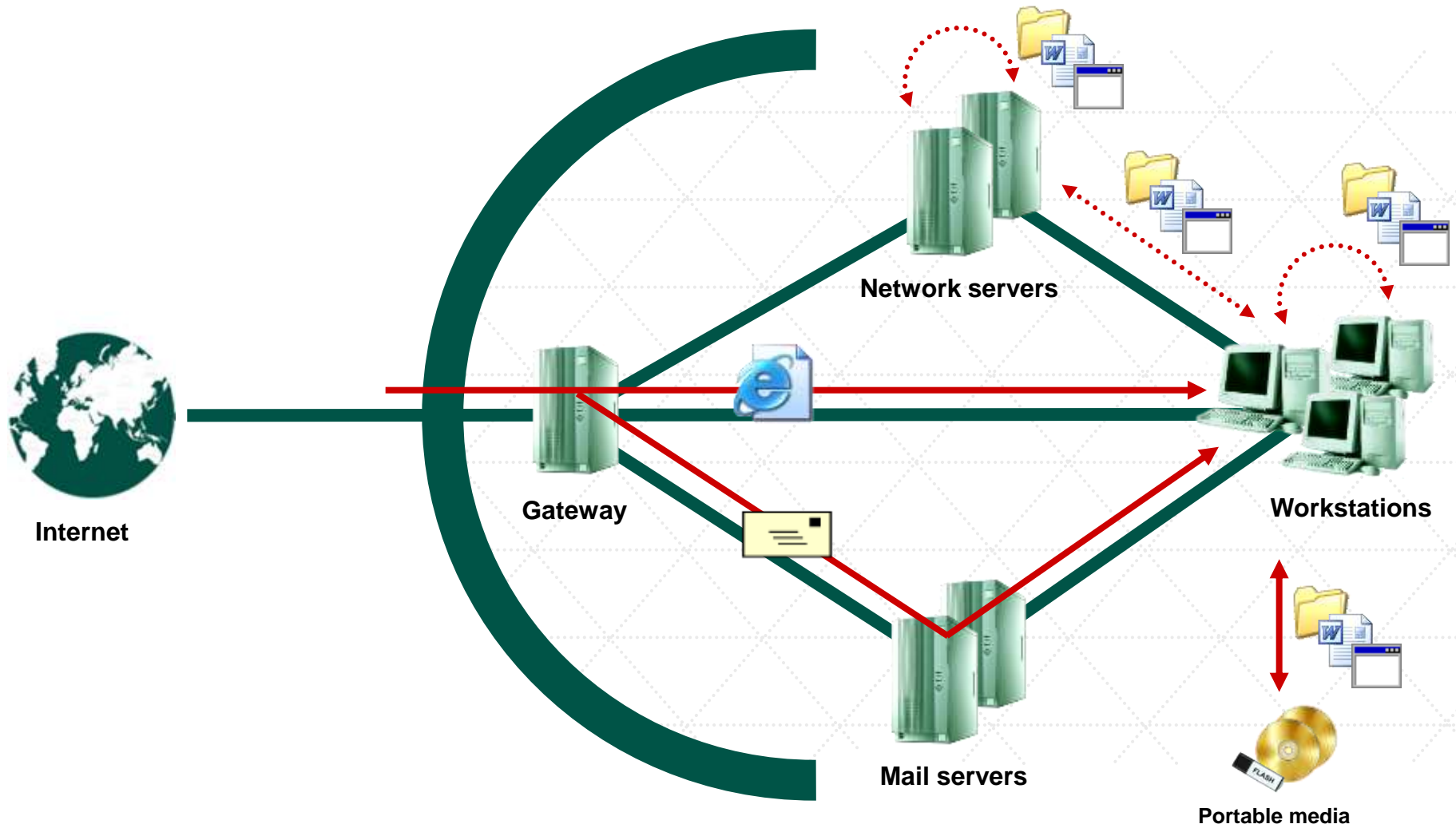


Kaspersky Endpoint Security 10 for Windows

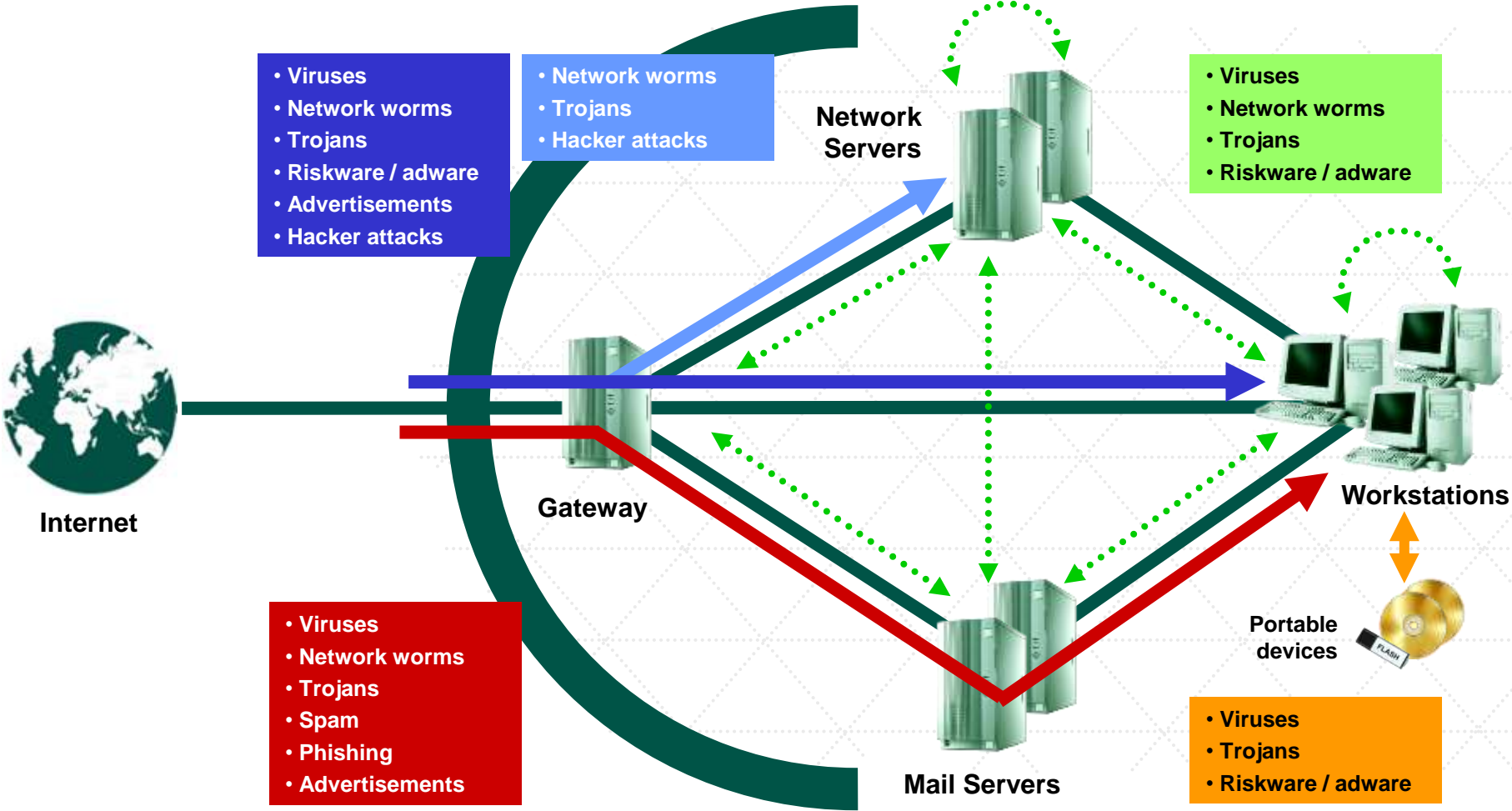
Deployment guide

Introduction

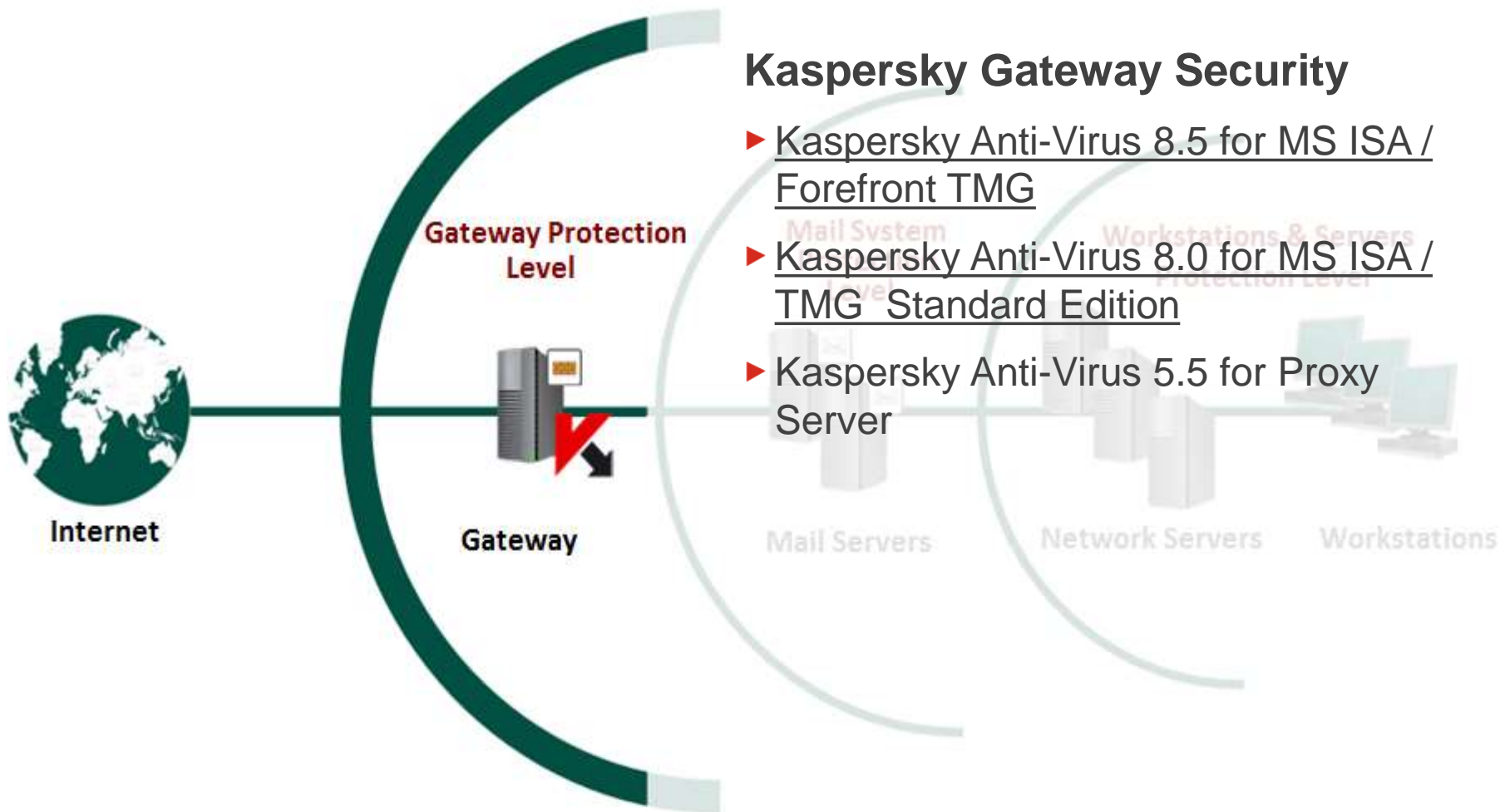
Typical Corporate Network



Malware Intrusion Routes



Gateway protection (KL 1004)



Kaspersky Gateway Security

- ▶ Kaspersky Anti-Virus 8.5 for MS ISA / Forefront TMG
- ▶ Kaspersky Anti-Virus 8.0 for MS ISA / TMG Standard Edition
- ▶ Kaspersky Anti-Virus 5.5 for Proxy Server

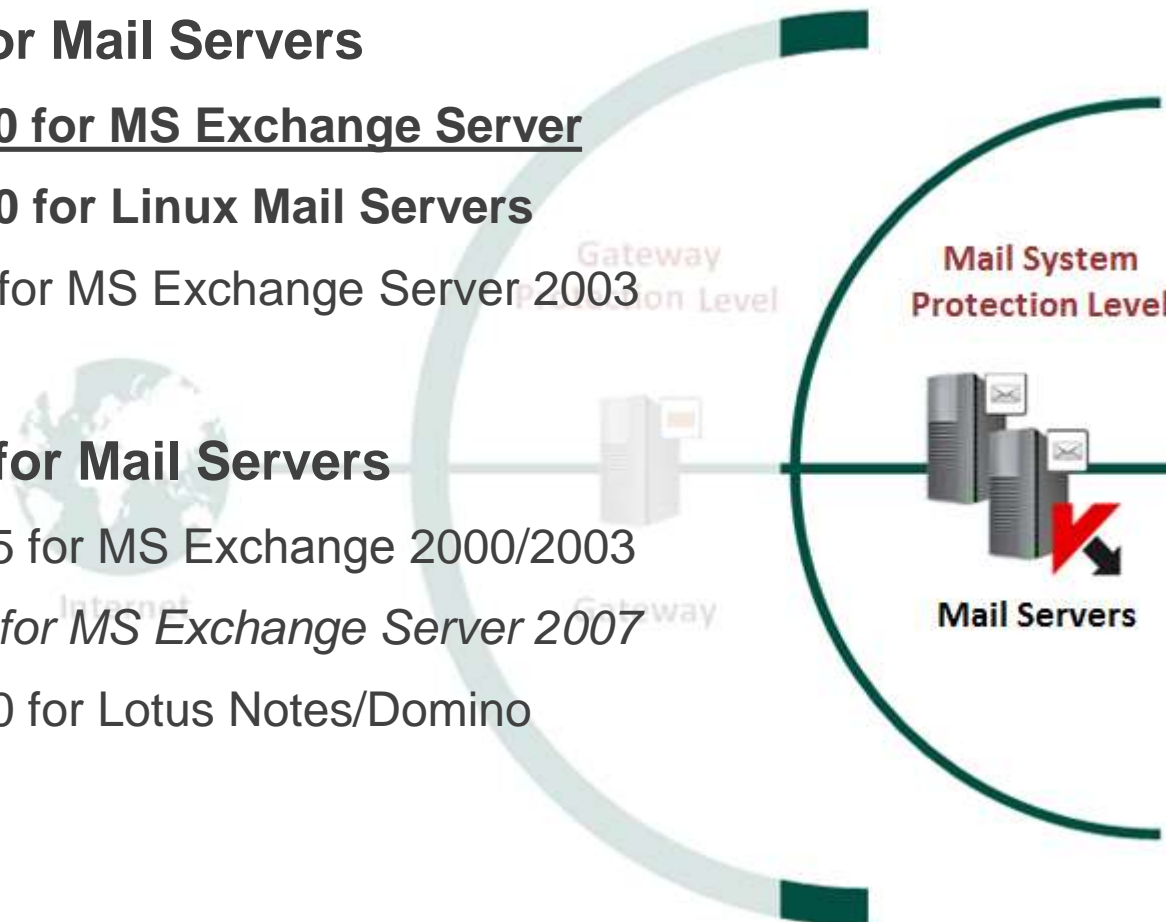
Mail Systems Protection (KL 1003)

Kaspersky Security for Mail Servers

- ▶ Kaspersky Security 8.0 for MS Exchange Server
- ▶ **Kaspersky Security 8.0 for Linux Mail Servers**
- ▶ Kaspersky Security 5.5 for MS Exchange Server 2003

Kaspersky Ant-Virus for Mail Servers

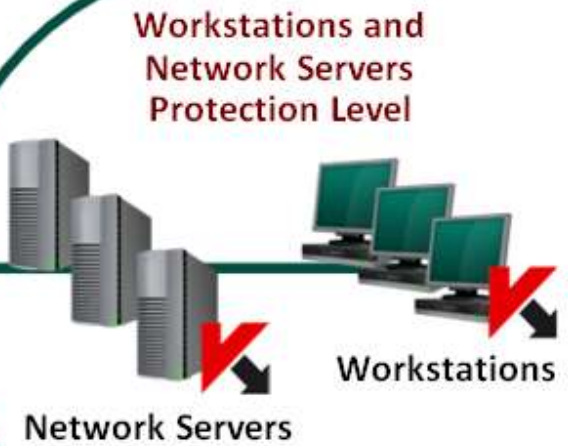
- ▶ Kaspersky Anti-Virus 5.5 for MS Exchange 2000/2003
- ▶ *Kaspersky Security 6.0 for MS Exchange Server 2007*
- ▶ Kaspersky Anti-Virus 8.0 for Lotus Notes/Domino



Workstations and Servers protection (KL 1302)

Kaspersky Endpoint Security

- ▶ Kaspersky Endpoint Security 10 for Windows
- ▶ Kaspersky Endpoint Security 8.0 for Linux
- ▶ Kaspersky Endpoint Security 8.0 for Mac
- ▶ Kaspersky Security 10 for Mobile
- ▶ Kaspersky Anti-Virus 8.0 for Windows Servers Enterprise Edition
- ▶ Kaspersky Anti-Virus 8.0 for Linux File Servers
- ▶ Kaspersky Anti-Virus 5.7 for Novell NetWare



Management Server

- ▶ Kaspersky Security Center 10

Product Line Renewal

Product Line Renewal


Windows Workstations and Servers protection

- ▶ Kaspersky Endpoint Security 10 for Windows


Management Server

- ▶ Kaspersky Security Center 10

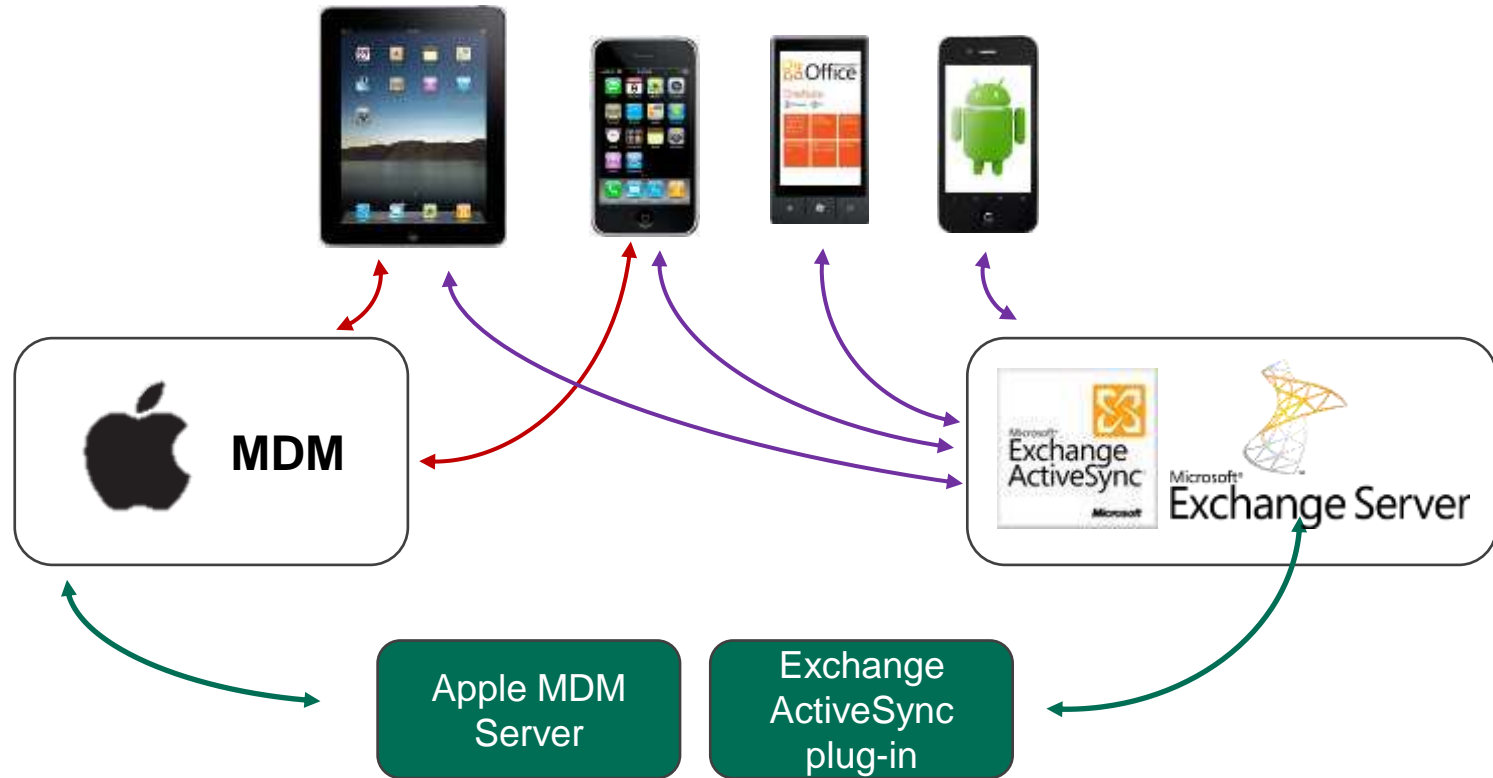
Management Server. What's new?

Kaspersky Security Center 10	
Capturing and deployment of operating system images	✓
License restrictions control functionality has been added	✓
Controlling devices' access to the organization's network – NAC	✓
Exchange ActiveSync Mobile devices server	✓
iOS MDM Mobile devices server	✓
Feature of sending SMS messages to mobile devices users	✓
Centralized remote installation of applications to managed mobile devices	✓
Automatic fixing of application vulnerabilities	✓
Support of data encryption for Kaspersky Endpoint Security 10 for Windows	✓
Publishing arbitrary stand-alone packages on a web server integrated with Administration Server	✓


Management Server. What's new?

Kaspersky Security Center 10	
Information panel displaying the statuses of update agents	✓
Management of the centralized list of users	✓
Specifying distributed content in the settings of an update agent has been added: installation packages, updates, or both	✓
Display of information about the full volume of data stored in the Administration Server database and about the volume of events stored in the database	✓
Feature of specifying an existing blank database as the Administration Server database during installation	✓
Option of managing Kaspersky Security Center tasks and policies via web-console	✓
Feature of excluding selected subdivisions from search through Active Directory	✓

Mobile Device Management



Endpoint protection. What's new?

Kaspersky Endpoint Security 10	
File Level Encryption (FLE)	✓
Encryption of files on local computer drives	✓
Encryption of files on removable storage drives	✓
Encryption of files created or modified by specific applications	✓
Management of rules of application access to encrypted files	✓
Full Disk Encryption (FDE)	✓
Encryption of hard drives	✓
Encryption of removable storage drives	✓
Manage user rights to boot an OS on computers with encrypted hard drives	✓
Restoration of encrypted devices	✓

Anti-Virus protection implementation

The background consists of a grey gradient with abstract, flowing white lines. At the bottom, there is a series of white vertical bars of varying heights, resembling a bar chart or a stylized city skyline.

Prerequisites

Microsoft Network Security Enhancements (KL 1001)

- ▶ Use Active Directory
 - Central management
 - Group policy mechanism (GPO)
 - Update system
 - Easy to deploy antivirus complex
- ▶ Disable Autorun functionality for all drives
- ▶ Limit external devices (data storages, modems, smart phones,..)
- ▶ Enforce password policy (length, complexity, lifetime, uniqueness)
- ▶ Limited accounts for users
- ▶ Limited shared folders (quantity, privileges)

Corporate Update System (KL 1001)

Corporate Update System

- ▶ Microsoft Products (Windows, Exchange, Office, ISA, MS SQL)
 - WSUS (Microsoft Windows Server Update Services)
 - Kaspersky Security Center 10

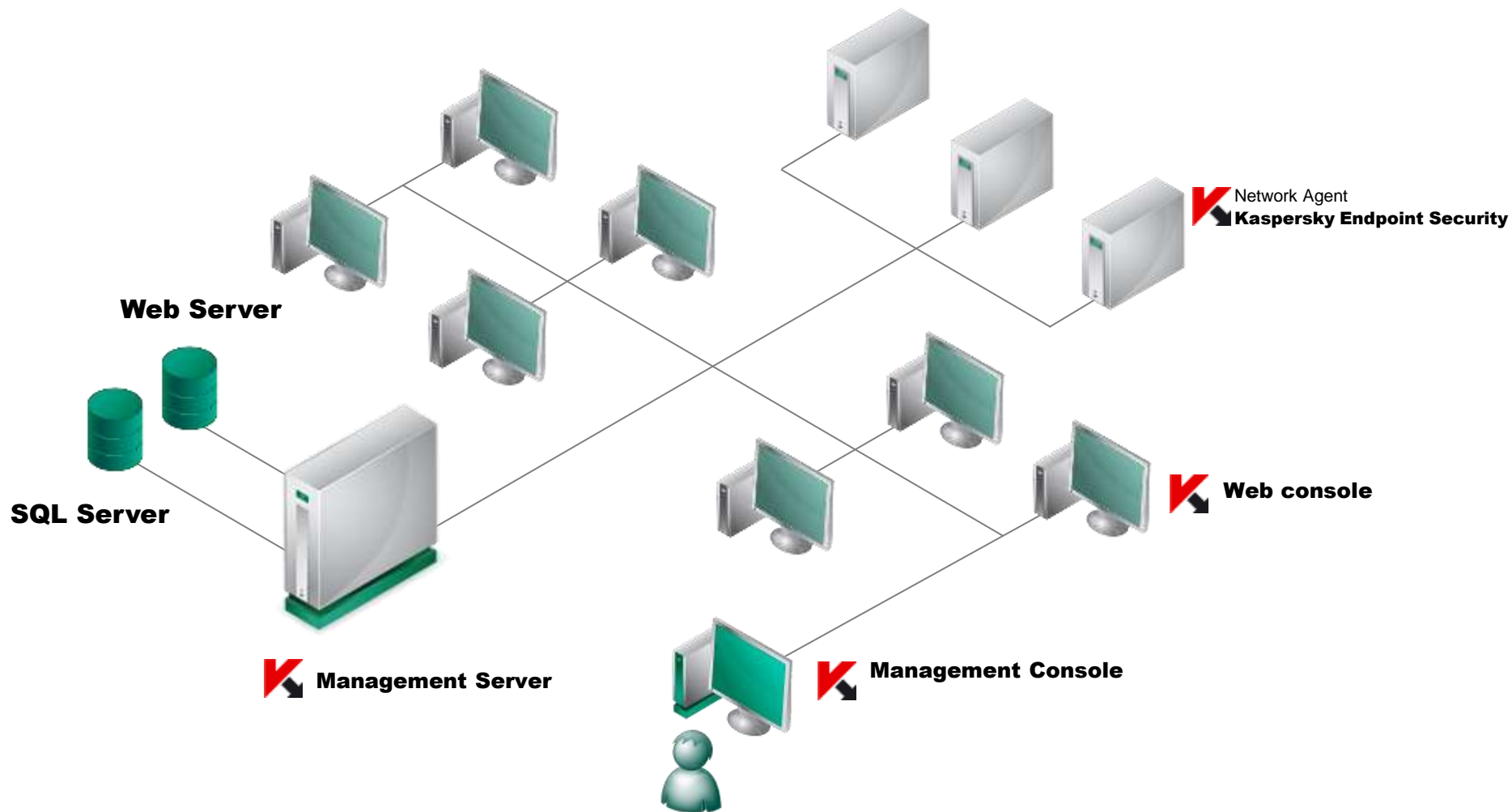
- ▶ Software of other Vendors
 - Built-in Update tools

 - Using GPO facilities (semi-automatically)
 - Implement corporate legalized software list
 - Watch the patch news
 - Download timely update packages
 - Deploy via GPO (Software install)

 - Using Kaspersky Security Center 10
 - Regular vulnerability scan by Kaspersky Endpoint Security
 - Download update packages
 - Deploy remotely via Security Center

Kaspersky AV-Complex Deployment

Kaspersky AV-Complex Scheme



Action plan

1. Network examination
2. Administration server installation
 - » **Kaspersky Security Center 10**
3. Logical network creation
4. Client applications deployment
 - » **Network Agent 10**
 - » **Kaspersky Endpoint Security 10 for Windows**
5. Administration Server configuring

Network examination

What information to collect

- ▶ Hardware platforms

- ▶ Operating systems
 - Security policies
 - Access permissions

- ▶ Network topology
 - Workgroup
 - Active Directory

- ▶ Firewall
 - Local
 - Network

- ▶ Deployment tools (Microsoft System Center, Tivoli, ...)

Kaspersky Security Center Installation

Security Center Installation Steps

- ▶ Administration server
- ▶ Management console
- ▶ Web-management console

Security Center Installation Requirements

- ▶ SQL server installed

- ▶ Compliance with system requirements

- ▶ Appropriate account privileges
 - Local administrator (workgroup)
 - Domain administrator (active directory)

- ▶ No Kaspersky Network Agents installed

Supported Types of SQL Server

- ▶ Microsoft SQL Server 2005
Standard/Enterprise/Express(freeware) Edition
- ▶ Microsoft SQL Server 2008 (x32/x64)
Standard/Enterprise/Express(freeware) Edition
- ▶ Microsoft SQL Server 2008 R2 (x32/x64)
Standard/Enterprise/Express(freeware) Edition
- ▶ Microsoft SQL Server 2012 (x32/x64)
Standard/Enterprise/Express(freeware) Edition
- ▶ MySQL Enterprise Server 5.0.32, 5.0.70

SQL Server. Enterprise or free edition?

- ▶ MS SQL 2005/2008 Express Edition
 - Maximum database size : 4 GB
 - Hardware limitations : 1CPU, 1 GB RAM
- ▶ MS SQL 2008R2/2012 Express Edition
 - Maximum database size : 10 GB
 - Hardware limitations : 1CPU, 1 GB RAM

Due to above limitations it is not recommended to use free SQL servers for more than 1000 clients

Security Center: software requirements

Operating systems

- ▶ Microsoft Windows XP Professional SP2+ *
- ▶ Microsoft Windows Server 2003 *
- ▶ Microsoft Windows Vista (SP1+) *
- ▶ Microsoft Windows Server 2008 (SP1+) * / R2 (Core)
- ▶ **Microsoft Windows Server 2012**
- ▶ Microsoft Windows 7 *
- ▶ Microsoft Windows 8 *

* 32/64 bit editions

Additional software

- ▶ Microsoft.NET Framework 2.0 SP1*
- ▶ Microsoft Data Access Components (MDAC) 2.8* or higher
- ▶ Windows DAC 6.0*
- ▶ Microsoft Internet Explorer 8.0 or higher
- ▶ Windows Installer 4.5 for Windows Server 2008/ Windows Vista

*Software is installed automatically

OS Type: Server or Client?

▶ Microsoft Windows XP / Vista / 7 / 8

- Connections limitation:
 - Win XP: 10
 - Win 7, 8: 20
- Client OS: designed for usability and appearance not best performance

▶ Microsoft Windows Server 2003 / 2008 / R2 / 2012

- Designed for Server operations (high performance and reliability)
- Number of redundant processes and modules is minimal

Security Center: Hardware Requirements

▶ Minimum

- Intel Pentium 1.4 GHz processor
- 4 GB of RAM
- 10 GB of free hard drive space

▶ Sufficient for 1000 client computers

- Intel Pentium 2.8 GHz processor
- +1 GB of extra RAM

*See deployment guide for detailed information

Security Center Installation Steps

- ▶ Administration server
- ▶ Management console
- ▶ Web-management console

Management console: software requirements

Operating systems

- ▶ MS Windows XP Professional (SP 2+) *
- ▶ MS Windows Server 2003 (SP 1+) *
- ▶ Microsoft Windows Vista (SP1+) *
- ▶ Microsoft Windows Server 2008 (SP1+) * / R2 (Core)/ 2012
- ▶ Microsoft Windows 7 *
- ▶ Microsoft Windows 8 *

* 32/64 bit editions

Additional software

- ▶ Microsoft.NET Framework 2.0 SP1*
- ▶ Microsoft Management Console 2.0 or higher
- ▶ Microsoft Internet Explorer 8.0 or higher
- ▶ Windows Installer 4.5 for Windows Server 2008/ Windows Vista

*Software is installed automatically

Management console: Hardware Requirements

▶ Minimum

- Intel Pentium 1.4 GHz processor
- 512 MB of extra RAM
- 1 GB of free hard drive space

Security Center Installation Steps

- ▶ Administration server
- ▶ Management console
- ▶ Web-management console

Web console: software requirements

▶ Server side

- Web server
 - Apache 2.2.9 or higher, 32 bit (Windows)
 - Apache 2.2.9 or higher, 32/64 bit (Linux)

▶ Client side

- Operating system
 - Any system with supported type of web browser
- Web browser
 - Microsoft Internet Explorer 7 or higher
 - Mozilla Firefox 16 or higher
 - Apple Safari 4 or higher

Demo: Security Center Installation

Quick Start Wizard

Quick Start Wizard

- ▶ License add
- ▶ KSN agreement
- ▶ Network scan
- ▶ Notification settings
- ▶ Vulnerability scan and fixing
- ▶ Initial Kaspersky Endpoint Security configuration
 - Group policies
 - Group tasks
 - Kaspersky Security Center tasks
- ▶ Proxy server settings

Demo: Quick Start Wizard

Kaspersky Security Center Logical Network Implementation

Logical Network Implementation

- ▶ Administration groups creation
 - Group structure wizard
 - Manual

- ▶ Computer assignment
 - Automatic
 - Manual

Demo: Logical Network Implementation

Anti-Virus Applications Remote Installation

KES 10: Hardware Requirements

▶ Windows 7/ 8 /Vista / 2003/ 2008/ 2008R2/ 2012

- Processor Intel Pentium 2.0 GHz or equivalent
- 1024 MB of available memory
- 1GB of available disk space

▶ Windows XP

- Processor Intel Pentium 2.0 GHz or equivalent
- 512 MB of available memory
- 1GB of available disk space

Applications Deployment Steps

- ▶ Installation packages creation
- ▶ Network Agents remote installation
- ▶ Compatibility check
 - Incompatible applications report
 - Detected applications uninstall
 - Remote from Security Center (recommended)
 - Automatic by installation package
- ▶ Kaspersky Anti-Virus remote installation
- ▶ Encryption module installation
- ▶ License distribution

Remote Installation Methods

- ▶ Push installation methods
 - Using Windows tools (RPC-based)
 - Using Network Agents

- ▶ Additional (delayed) installation methods
 - Active-directory-based methods
 - Installation using Active Directory policies

 - Employing users' help
 - Using stand-alone installation packages

Installation Using Windows (RPC) tools

- ▶ Installation files are copied to the Admin\$ (\\target\admin\$) share
- ▶ Installation is being launched via RPC
- ▶ Installation success depends on a number of factors

This method is fully automated in Kaspersky Security Center

RPC Installation Requirements

- ▶ Windows NT-like operating system (except for Home Editions)

- ▶ Network availability
 - Physical
 - Check LAN

 - Logical
 - Firewall (Windows)
 - » Turn off
 - » Allow file sharing (TCP 139, 445, UDP 137, 138)

- ▶ Access to the Admin\$ folder
 - File sharing service (server) is enabled

 - Local administrator privileges

 - Guest access disabled (Workgroups problem)
 - “Simple file sharing” disabled
 - Local security policies (secpol.msc)
 - » Network access: Sharing and security model for local accounts (Classic)

 - Blank passwords
 - Accounts: Limit local account use of blank passwords to console logon only (Disabled)

 - Windows Vista, 7, 8, 2008/R2, 2012
 - User account control (UAC) disabled or built-in Administrator account is used (workgroups)
 - Enable file and printer sharing for current network profile (work\home, public, domain)

- ▶ Administrative privileges to perform installation

Demo: Anti-Virus Applications Remote Installation

Security Center Configuring

Administration Server Configuring

▶ Policies

- Kaspersky Endpoint Security
 - Full Disk Encryption
 - Application startup control
 - Web control

- Network Agents

▶ Tasks

- Update
 - Kaspersky Endpoint Security
 - Kaspersky Security Center

- Full Scan for Kaspersky Endpoint Security

- Kaspersky Security Center Backup

Demo: Security Center Configuring

Thank You