Introducing Kaspersky Security for Virtualization

Be Ready for What's Next

What is Driving Virtualization?

Business Needs

- **Greater Efficiency**
- **Higher Productivity**
- **Increased Agility**
- **Reduced Costs**
- **Competitiveness**
- **Improved IT Control**

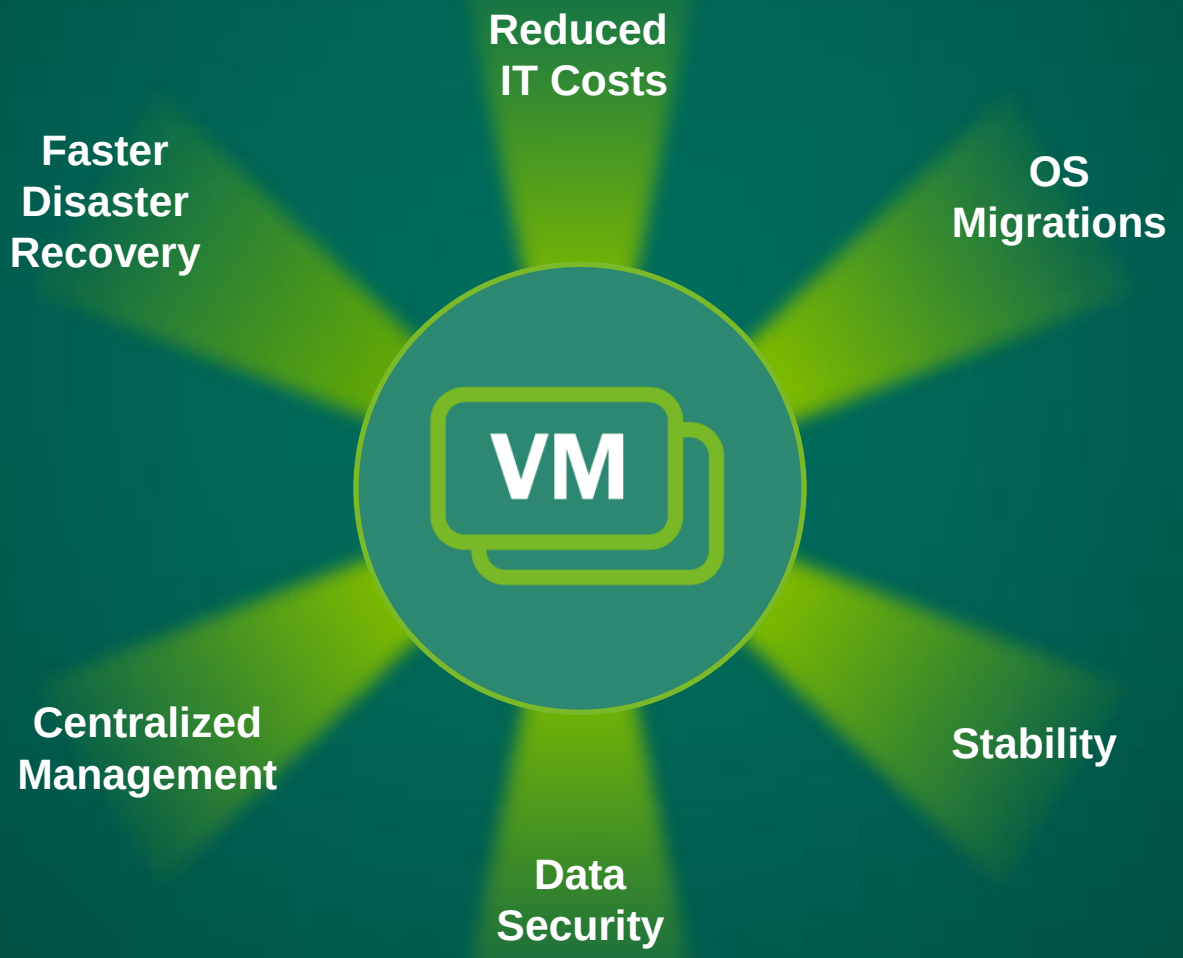
Virtualization Adoption Rates

Source: Small Business Server Virtualization Roadmap, CDW, August 31 2011

KASPERSKY lab

Expected Benefits

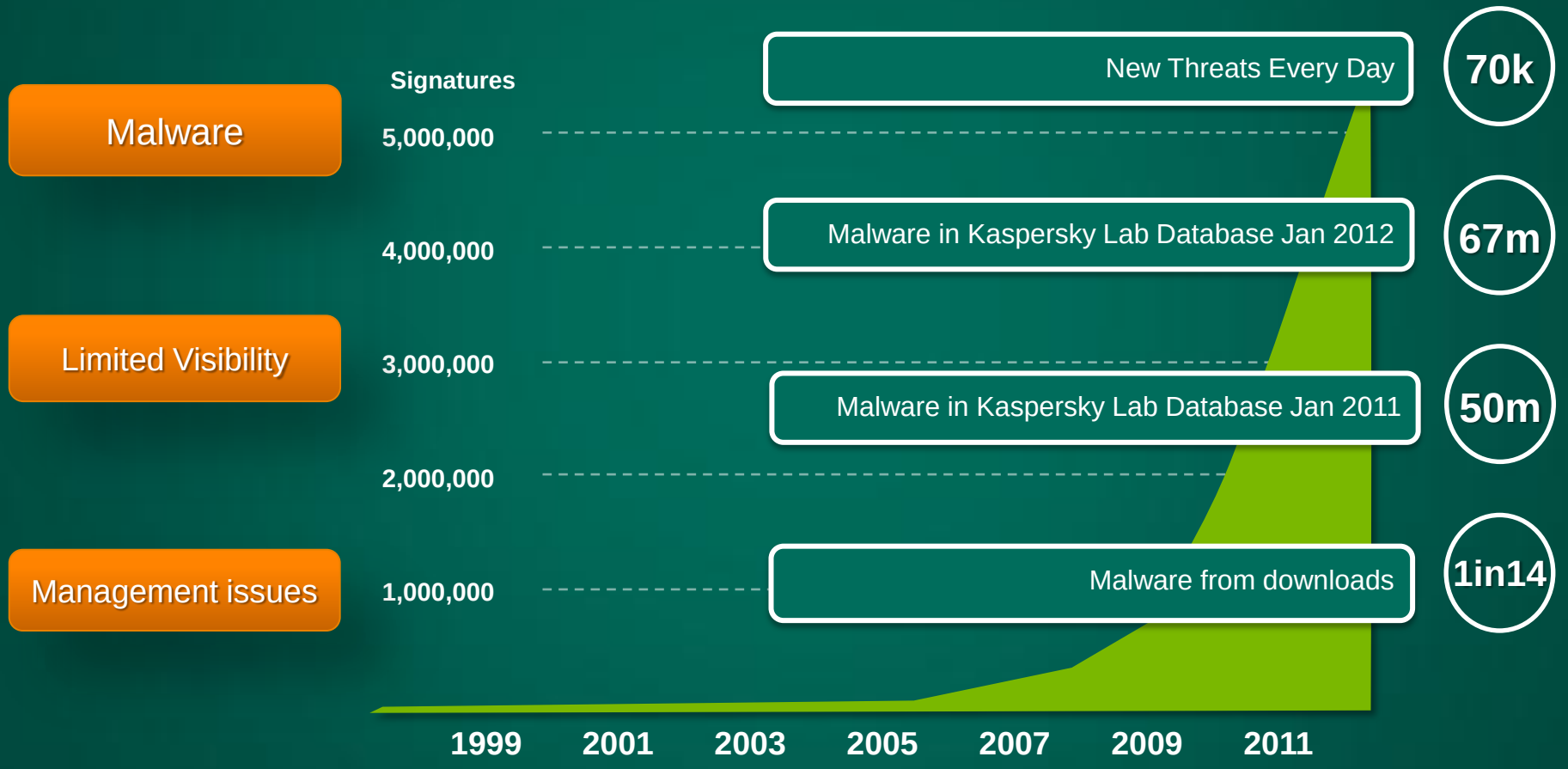
What is Virtualization Supposed to Bring?



KASPERSKY lab

Threats and risks

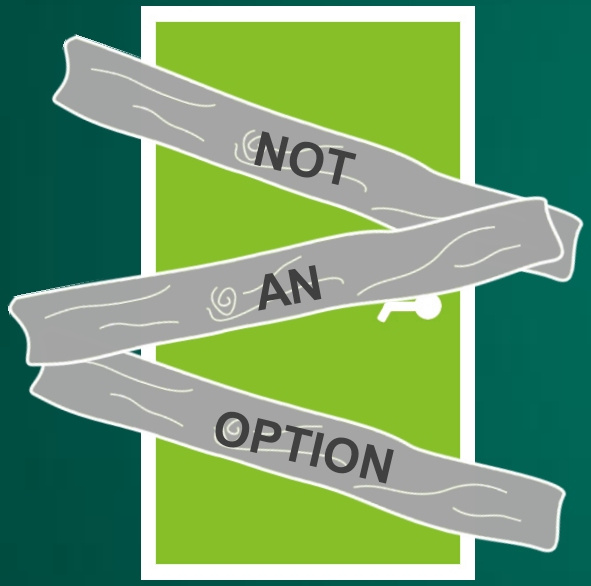
The same as for physical machines



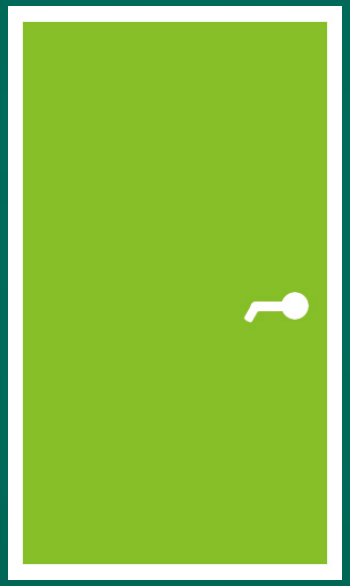
KASPERSKY lab

Options for Virtual Protection

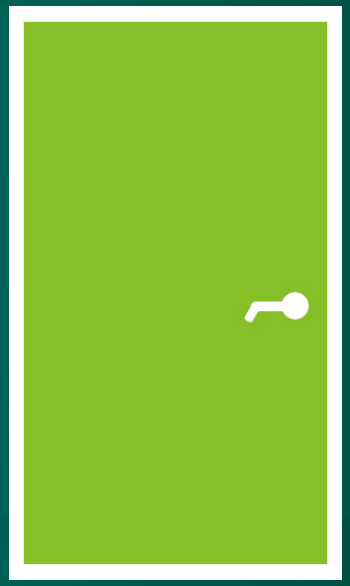
Option 1
No Protection



Option 2
Agent-based



Option 3
Agentless



KASPERSKY lab

No Protection – Not an Option

- Virtual Infection and spread
- Virtual eavesdropping
- Target of cybercriminals
- Malware can survive “tear-down” of non-persistent machines

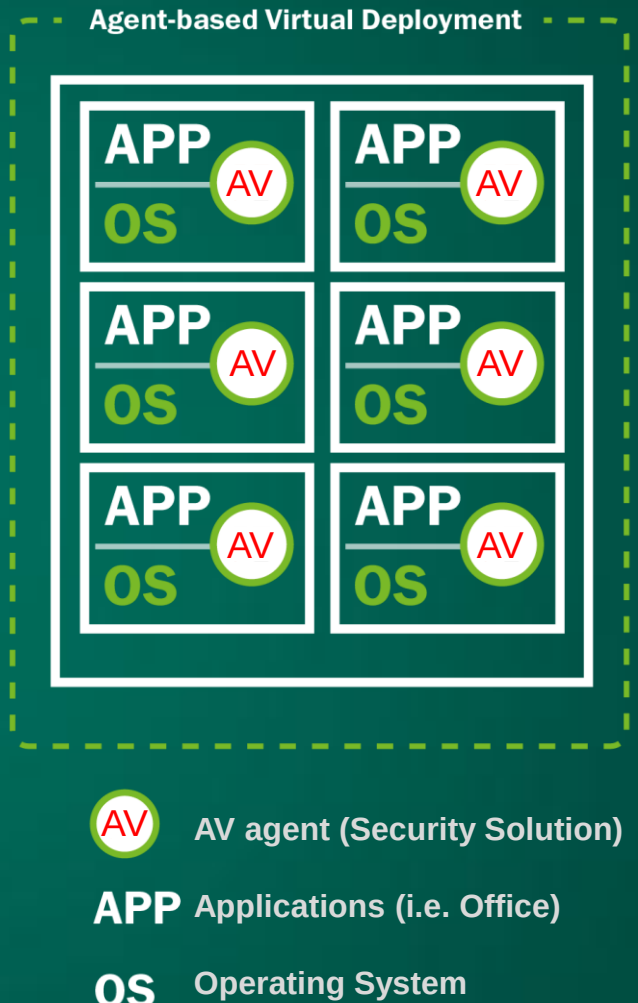
“A single compromised virtual machine impacts the entire virtual infrastructure.”

Guide to Security for Full Virtualization Technologies
National Institute of Standards & Technology

Agent-based Protection

Traditional Protection methods applied to VM

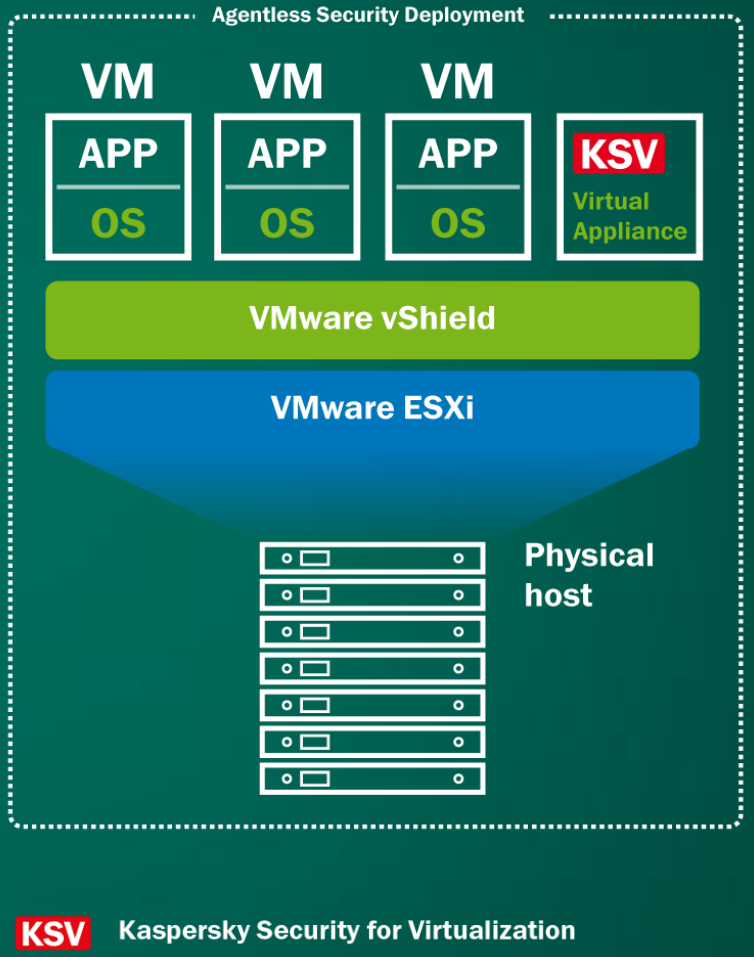
- AV-Storm
- Redundant anti-malware and signature files
- Instant On Gap
- VM's in Motion
- Reduced consolidation ratios



KASPERSKY lab

Agentless Protection
Kaspersky Security for virtualization

- Works with VMware's vShield Endpoint
- Anti-malware functions offloaded
- Managed component of Kaspersky Security Center 9.0

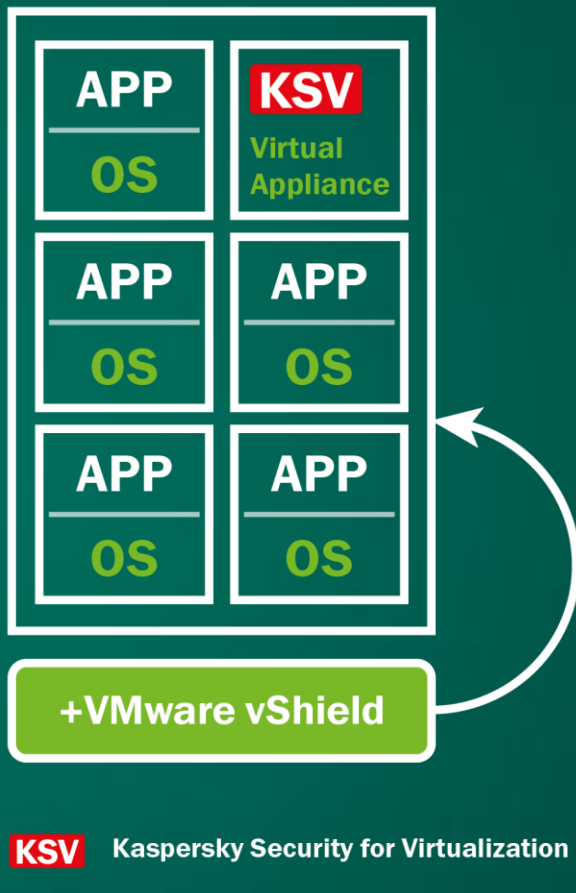


Kaspersky Security for Virtualization

Key benefits

Superior Protection, High Performance

- Award-winning anti-virus engine
- Unified management
- No Anti-virus Storm issues
- Immediate protection
- Higher density ratios
- Superior ROI

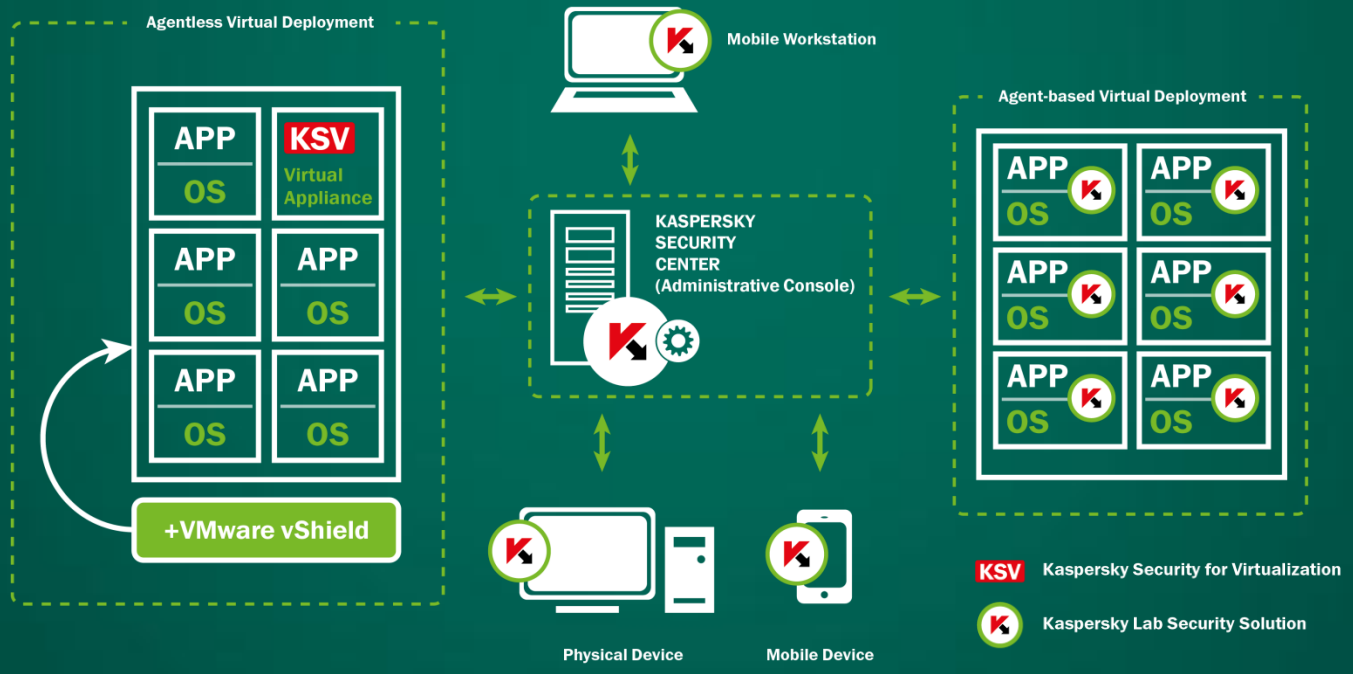


KASPERSKY lab

Kaspersky Security Center

Centralized Management of combined environment

- “Single-Pane” for administrators
- Automatic recognition
- Physical, Virtual, Mobile
- Broad platform coverage
- Intuitive deployment, management and reporting



Protection for infrastructures of any size and complexity

Simplified Management

Unified Under a "Single-Pane"

Solid Policy Enforcement

Intuitive

Robust Reporting

Virtual Protection

Immediate Protection

High Performance

Maximized Density

Virtual Aware

Physical Protection

Real Time Protection

Powerful Controls

Broad Platform Support

Mobile Protection

Protects Lost Devices

Android, BlackBerry, Windows, Symbian

Existing agentless offerings can be limited

- Multiple Administrative Consoles (different for virtual and physical infrastructures)
- Low detection rates
- Complex and long technical support procedure

Recommendations

- Don’t underestimate **manageability**
- **Choose unified solutions** to protect both physical and virtual environment
- Find the **right balance** of security and performance
- **Combine** «agent-based» and «agentless» protection methods
- **Don’t cherish illusions** that virtual environments are more secure than physical ones

Get the right balance with Kaspersky

Kaspersky Security for Virtualization provides agentless anti-malware security for virtual machines, without compromising performance.

Get the right balance with Kaspersky.

Security for Virtualization.
Be Ready for What's Next.

kaspersky.com/beready

KASPERSKY lab

Thank You!