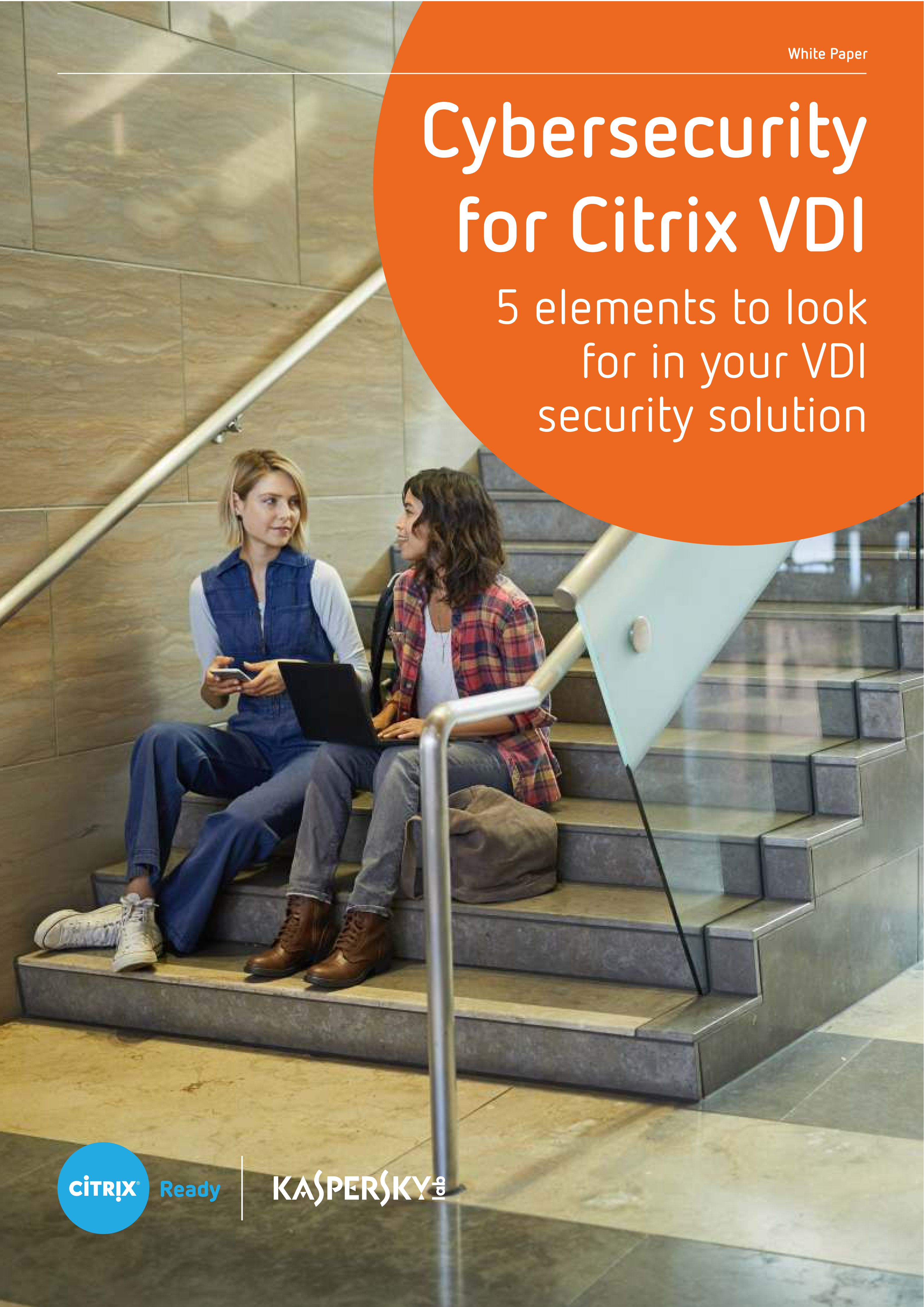
White Paper

Cybersecurity for Citrix VDI

5 elements to look for in your VDI security solution



CITRIX Ready | KASPERSKY lab

What Matters Most in VDI Cybersecurity

Businesses worldwide are taking operational efficiency to the next level and becoming truly borderless through desktop and application virtualization. These technologies deliver remote access to your business environment from any device, over any network. But as data becomes increasingly free-ranging, there's a clear need for effective security designed specifically to complement the agility and performance of leading VDI platforms.

Kaspersky Lab and Citrix are together addressing this by introducing a joint solution – a complete tool set of advanced cybersecurity capabilities available in Kaspersky Security for Virtualization and built around the Citrix XenDesktop and XenApp platforms. Kaspersky Security for Virtualization delivers multi-layered protection using the latest security technologies, without eating into resources or compromising performance, resulting in significantly higher consolidation ratios than can be achieved using traditional anti-malware solutions.

Our joint solution ensures that all components of your virtual desktop and application environments interoperate in a fully secured landscape, delivering precise protection for end-users and the data they work with from any kinds of cyber threats, including malware, ransomware, cryptors, and network attacks. Our ability to understand and respond to the specific security needs of XenDesktop installations is recognized by enterprise users worldwide.

75% of business users responding to our latest survey have already adopted virtualization [1]

[1] Based on "IT Security Risks Report 2016" by Kaspersky Lab

Anti-Ransomware & Exploit Prevention

People and applications are the two greatest areas of vulnerability in most IT environments. An effective security solution needs to incorporate technologies specifically designed to monitor and prevent cybercriminals from exploiting these two vectors.

Anti-Ransomware for VDI

Ransomware is one of the fastest growing classes of malicious software. Attackers don't even have to bother stealing and selling your critical data – they just encrypt it and demand a ransom, often using malicious links in emails to introduce malware and initiate attacks.

'System Watcher' technology built into Kaspersky Security for Virtualization monitors the behavior of applications running inside each virtual desktop. If any form of suspicious behavior, such as cryptor or locker activity, is detected, the activity is blocked and any malicious changes are automatically rolled back, so critical data remains secure. Your users won't even be aware that anything's happened.

Automatic Exploit Prevention (AEP)

The exploitation of unpatched vulnerabilities in applications is a common method of introducing most forms of malware, including ransomware, into VDI environments.

To overcome the dangers posed here, Kaspersky Security for Virtualization includes a technology called Automatic Exploit Prevention (AEP). This specifically monitors the most frequently targeted applications – including Adobe Reader, Internet Explorer, Microsoft Office, Java and many more – delivering an extra layer of security monitoring and protection against unknown threats.

Kaspersky Security for Virtualization

- Multi-layered security for hybrid infrastructures
- Security for all leading virtualization platforms
- Protects Windows and Linux-based virtual servers
- Powerful yet lightweight security for VDI platforms including XenDesktop
- Application and Device controls with advanced HIPS
- Perfectly balanced protection with no impact on performance

System Hardening

Kaspersky Security for Virtualization delivers security capabilities and controls enabling you to reduce your attack surface while preserving efficiency, so your end-users can work comfortably and uninterruptedly on business tasks in a safe corporate environment.

Application Control

Application Startup and Privilege Control, including a Default Deny approach, ensures control over system resources and personal data by allowing only trusted applications to be launched on the protected VM.

Device Control

This technology regulates access to virtualized USB devices connected to a VM. It's easy to apply control policies to a range of devices, including removable drives, printers and non-corporate network connections.

Web Control

URL and web-traffic protection shields virtual desktops from malware and malicious web-based resources which might harm corporate security or which don’t meet your cybersecurity policy requirements.

Mail Control

This feature allows the scanning of inbound and outbound email traffic, ensuring all communications are safe and malware-free.

38% of attacks, including ransomware threats, are initiated through the, often quite unintentional, actions of internal users [1]

51% of businesses admit that IT infrastructure complexity directly affects their ability to maintain appropriate levels of cybersecurity

1) Based on “IT Security Risks Report 2016” by Kaspersky Lab

Intrusion Detection and Prevention

While file-level protection is crucial, it's only one aspect of VDI security: protecting virtualized networks is also critical.

Multi-layered protection for your network
Kaspersky Security for Virtualization protects against external and internal network attacks – including threats that may be hidden in non-transparent virtual traffic. Every VM is protected by host-based network security which includes Kaspersky Lab's HIPS, firewall and Network Attack Blocker technologies.

Host-based Intrusion Prevention System (HIPS) and personal firewall
Working together with Kaspersky Lab's two-way firewall, HIPS controls both inbound and outbound traffic on your network. Flexible tools let you control security according to a wide choice of parameters, including settings for an individual port, individual IP addresses or a specific application's network activity.

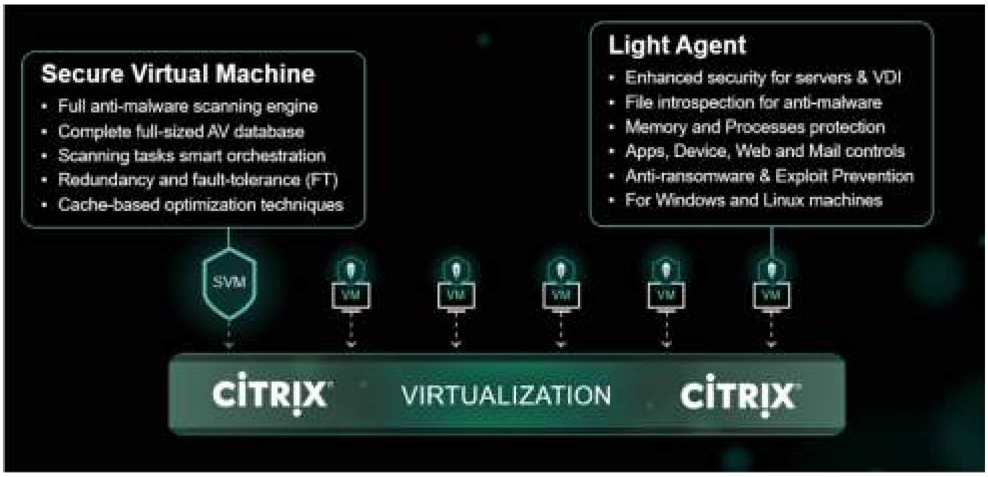
75% of businesses say that cybersecurity is their major concern

52% of companies understand the specific risks of virtualization

HuMachine® Intelligence

Based on the most highly awarded security engine in the business, Kaspersky Security for Virtualization helps fight the most advanced threats and vulnerabilities, right across your entire virtualized IT landscape.

Kaspersky Security for Virtualization is more than just 'designed for' virtualization platforms: it utilizes the core technologies of those platforms to optimize the security capabilities of both platform and security solution. Our perfectly balanced, award-winning cybersecurity is empowered by HuMachine® Intelligence - a seamless blend of global threat intelligence big data, robotic Machine Learning capabilities and the ingenuity and experience of Human Experts. The cloud-based threat intelligence big data environment identifies new threats and provides automatic updates to security solutions installed worldwide, identifying new malware in as little as 0.02 seconds, enabling Kaspersky Security for Virtualization to protect your VDI environment and your business against emerging and even zero-day threats.



Secure Virtual Machine

- Full anti-malware scanning engine
- Complete full-sized AV database
- Scanning tasks smart orchestration
- Redundancy and fault-tolerance (FT)
- Cache-based optimization techniques

Light Agent

- Enhanced security for servers & VDI
- File introspection for anti-malware
- Memory and Processes protection
- Apps, Device, Web and Mail controls
- Anti-ransomware & Exploit Prevention
- For Windows and Linux machines

Architecture of Kaspersky Security for Virtualization Light Agent

Resource-Efficiency

The lightweight architecture of Kaspersky Security for Virtualization supports end-user satisfaction, promoting improved VDI security without compromising performance or important parameters like log-on and boot time for increased responsiveness.

Typical resource-intensive tasks are offloaded from individual Virtual Desktops to a security appliance, called a Security Virtual Machine (SVM) that holds an always up-to-date database of malware definitions. Meanwhile, small Light Agents on every VM maintain protection by checking the virtual RAM and processes for rootkits and memory-based malware.

VDI environments tend to include many similar VMs, each accessing identical files, so some security products waste time and resources running multiple scans of the same file. Kaspersky Lab’s Shared Cache feature effectively shares the results of file scans, helping to minimize the overall load on your IT infrastructure.

Thanks to integration capabilities, Kaspersky Security for Virtualization ensures that your infrastructure and its security solution work in harness for optimum efficiency.

A Symbiotic Security Solution

It's a dangerous world. More than ever before, it's crucial that all systems, both physical and virtual, are protected with comprehensive security solutions. So, the means of protection, and the resultant impact on system management and usability, is important. Careless selection can result in problems that resonate far beyond issues of security.

When selecting a security solution for virtual desktops and servers, adequate protection is of course important. But it's equally important to select solutions that will not prevent the achievement of the very goal that prompted the move toward virtualization – cost savings through increased efficiency.

For Citrix XenDesktop and XenServer customers, Kaspersky Security for Virtualization offers a single solution for protecting both virtual servers and desktops. In perfect symbiosis, Kaspersky Security for Virtualization maximizes the protection so vital in today's world without diminishing the performance benefits that make Citrix so popular.

To learn more about how Kaspersky Security for Virtualization can provide superior protection for your VDI environment, visit www.kaspersky.com/enterprise-security/virtualization, or find a Kaspersky Lab partner or sales representative near you at www.kaspersky.com/partners.

Protects Your Investment

- Preserves the Return on Investment
- Adaptive & Automated Security
- Security Cost Optimization

Gives Full Visibility

- Seamless integration into VDI
- Transparent, user protection
- Scalability and Control
- Unified Management

About Citrix Ready

Citrix Ready identifies recommended solutions that are trusted to enhance the Citrix Delivery Center infrastructure. All products featured in Citrix Ready have completed verification testing, thereby providing confidence in joint solution compatibility. Leveraging its industry-leading alliances and partner ecosystem, Citrix Ready showcases select trusted solutions designed to meet a variety of business needs. Through the online catalog and Citrix Ready branding program, you can easily find and build a trusted infrastructure. Citrix Ready not only demonstrates current mutual product compatibility, but through continued industry relationships also ensures future interoperability. Learn more at citrixready.citrix.com.