KASPERSKY lab

KASPERSKY SECURITY FOR VIRTUALIZATION

Superior, flexible and efficient protection for the Nutanix Enterprise Cloud Platform

NUTANIX™
The Enterprise Cloud Company

Why Secure Virtualization?

As businesses continue to roll out virtualization across their IT estate, there is an increasing need both for reliable hardware and software, and for security designed specifically for virtual infrastructures.

Together, Nutanix and Kaspersky Lab deliver a secure, scalable compute and storage solution for virtualized applications. Virtual servers and virtual desktop infrastructures (VDI) running on Nutanix nodes are protected by powerful, intelligent security from Kaspersky Lab, while preserving all the performance benefits that virtualization brings. It's a winning combination for an optimized environment.

The world's most advanced enterprise data centers rely on Nutanix web-scale technology to power their mission-critical workloads, and on Kaspersky Lab's security solutions to protect them from the most advanced cyberthreats.

How You Benefit From Integration

The Nutanix Enterprise Cloud platform was built using web-scale technologies and architectures that originated in large internet and cloud companies. Kaspersky Security for Virtualization integrates with the platform's own security features, adding layers of intelligent, real time protection and VM controls to help customers meet the most stringent security requirements.

Security at Every Layer
Security is built into the Nutanix and Kaspersky Lab stack from platform through to workload. Kaspersky Security for Virtualization provides multi-layered security and additional visibility on top of Nutanix's hardened and self-healing platform, with SaltStack and STIG, resulting in a highly secure environment.

Simplified Management and Administration
Unified management consoles are a feature of both the Nutanix platform and Kaspersky Security for Virtualization. Virtual systems security is managed, together with security for physical and mobile endpoints, through a single user-friendly interface – Kaspersky Security Center.

Distributed Everything
Nutanix and Kaspersky Lab solutions are both built on an architecture that is 100% software-defined, distributing all data, security, and operational resources for web-scale extensibility and performance.

Securely Share Infrastructure
Kaspersky Security for Virtualization, coupled with compute and storage from Nutanix, enables enterprises to run and to control access to a raft of business-critical applications on one simplified platform.

The Nutanix enterprise cloud platform eliminates unpredictable user performance, burdensome operational costs and high capital costs. Nutanix web-scale architecture is ideal for VDI. It consolidates compute (server), storage and virtualization into a single, 100% software –defined appliance that comes ready to run VMware Horizon View, XenDesktop or Citrix XenApp. All of these can be secured by Kaspersky Lab's specialized solution for virtual infrastructures.

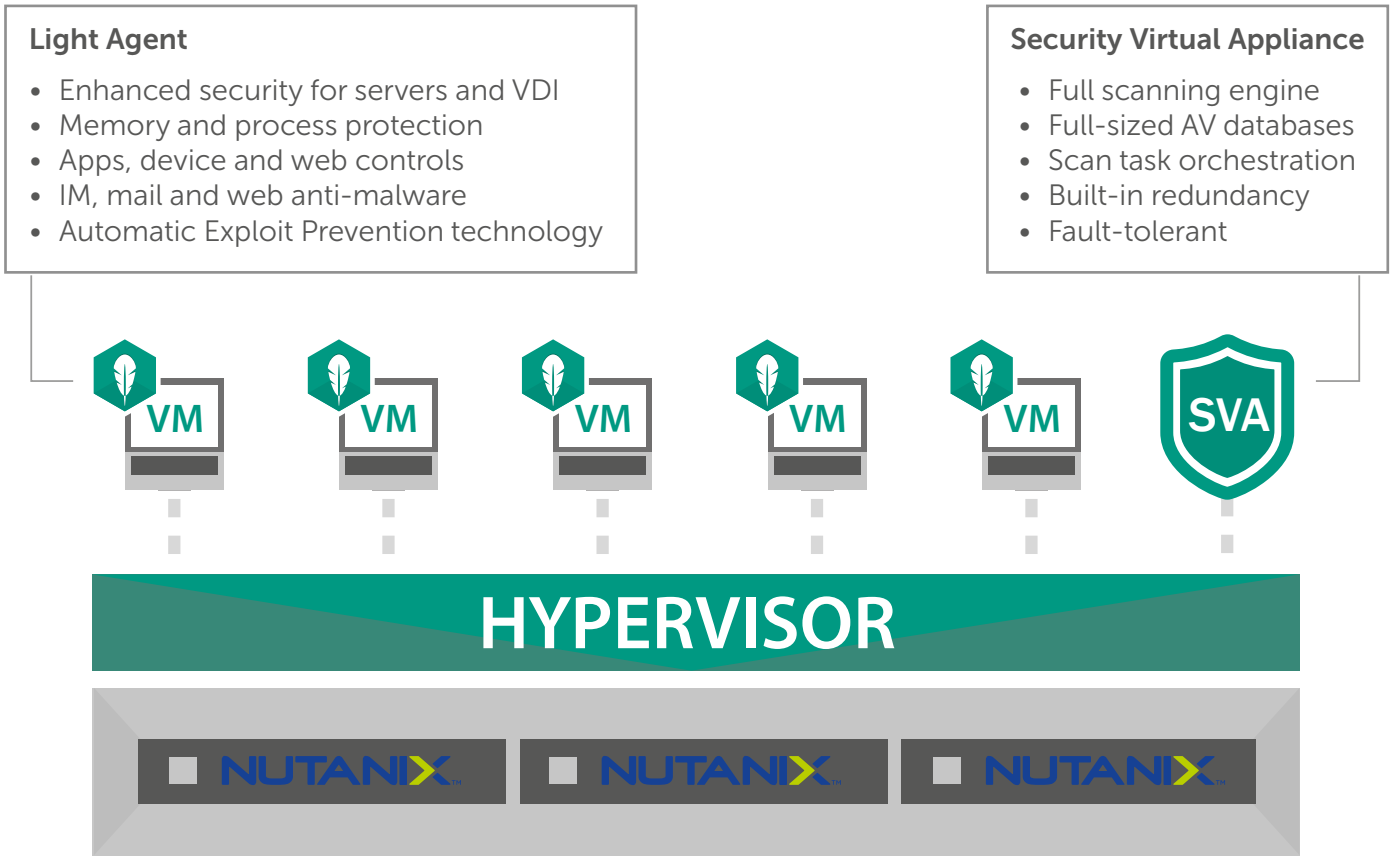
Kaspersky Security for Virtualization adds powerful multi-layered protection with the lightest of resource footprints, resulting in a significantly higher machine density than traditional anti-malware solutions can deliver. So you can effectively protect your systems and sensitive corporate data, while maintaining high consolidation ratios and quality of service for your users.

Unique Light Agent Technology: Multi-Layered Security for Superior Protection

For virtualized environments, maintaining security without affecting performance is critical. Kaspersky Security for Virtualization uses patented technologies to strengthen the protection of VDI and server platforms at individual VM (virtual machine) level, with minimal impact on performance.

Kaspersky's award-winning anti-malware engine provides automatic, real-time protection for every VM – on-access and on-demand – on most popular virtualization platforms including VMware vSphere and Microsoft Hyper-V.

How it Works and What it Does



A Security Virtual Appliance (SVA) on each host scans all VMs centrally, while a powerful but lightweight agent deployed on each VM allows advanced security features, including application, device and web controls, anti-malware protection for IM, mail and web, plus advanced heuristics, to be activated.

Kaspersky Security for Virtualization is tightly integrated with most popular platforms. Your business critical infrastructure benefits from optimized performance that fully exploits your hypervisor's own core technologies – complementing and enhancing security in, for example, VMware Horizon and Citrix XenDesktop VDI environments.

Key Security Benefits

Multi-layered security for VDI environments

Kaspersky Security for Virtualization delivers outstanding multi-layered, granular protection for VDI, including individual VM controls and mail/web/IM security. VMware, vSphere and Microsoft Hyper-V, virtualization platforms are all supported. Most popular VDI platforms, such as VMware Horizon and Citrix XenDesktop can be also protected with Kaspersky Security for Virtualization. Tight systems integration means that each hypervisor's own core technologies are fully exploited, enhanced by powerful, intelligence-led security from Kaspersky Lab.

Award-winning anti-malware engine for superior security

Kaspersky Lab's latest anti-malware engine combines signature-based, proactive and cloud-assisted technologies to deliver superior detection rates and powerful protection against known, unknown and advanced threats (including crypto-malware, zero-day exploits and unpatched vulnerabilities).

Optimized performance for virtualized infrastructures

Kaspersky Security for Virtualization has been specifically developed for virtual environments, delivering the lightest resource footprint through optimizing file-level scanning tasks, fine-tuning protection technologies and orchestrating scanning tasks. As a result, performance is maintained while update and scanning 'storms', as well as Windows of Vulnerability or 'instant-on' gaps, are eliminated.

Fast log-on and application responses for VDI

Our solution architecture dramatically enhances end-user experience, promoting improved VDI security without sacrificing performance or affecting important parameters like log-on time and boot time.

Supports the rapid provisioning of VDI machines

Kaspersky Security for Virtualization supports linked and full cloning. Thanks to the pre-installed lightweight agent, provisioning a new VM just involves cloning a template, which simplifies VDI management, eliminating the need to update security products on the VDI image.

Automatic Exploit Prevention (AEP)

To overcome the dangers posed by unpatched vulnerabilities, Kaspersky Lab offers Automatic Exploit Prevention (AEP) technology, which specifically monitors the most frequently targeted applications in VDI environments, delivering an extra layer of protection against unknown threats.

Reliability, redundancy and flawless operation

Advanced self-protective techniques constantly and autonomously monitor operations, while Security Virtual Appliance dual redundancy ensures continuous security for every VM in your infrastructure.

Easy-to-use unified management console

A single, unified administration console lets your IT team centrally manage the security of all your VMs and helps you roll out virtualization projects at your own pace.

Learn more at www.kaspersky.com/enterprise

KASPERSKY lab