卡巴斯基®
虚拟化安全解决方案

为虚拟服务器和VDI提供灵活、高效的出色保护

随着越来越多企业受益于软件定义数据中心，企业愈发需要一款能够完美兼顾出色保护与高效性能的解决方案。卡巴斯基虚拟化安全解决方案与大部分常用的虚拟化平台和技术紧密集成，包括VMware vSphere with NSX、Microsoft Hyper-V、Citrix XenServer和KVM以及VMware Horizon和Citrix XenDesktop，可为VDI和虚拟服务器环境提供出色、多层级、细粒度的增强保护。

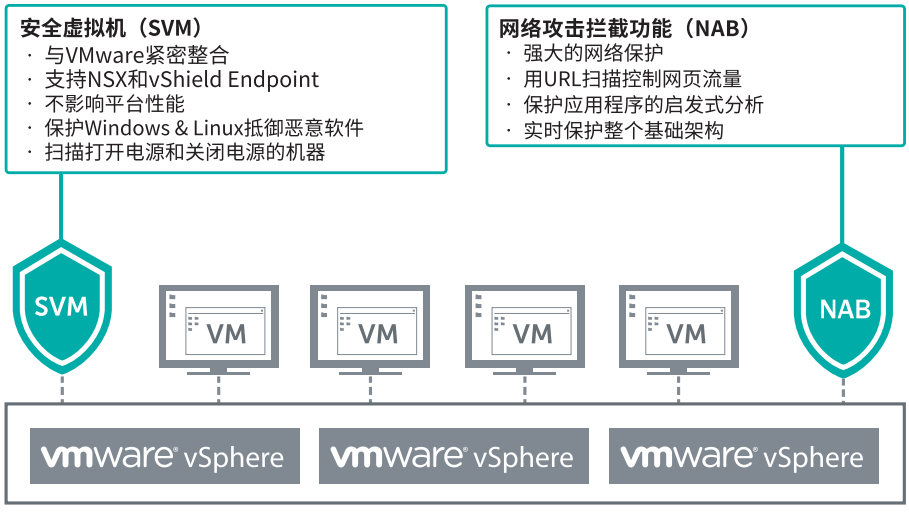
卡巴斯基虚拟化安全解决方案提供无代理和轻代理两种安全选择，重新定义了软件定义数据中心与其安全解决方案的交互方式，使彼此变得更加智能、快速和高效。

本地集成无代理安全解决方案的优势：

- 根据适用于系统管理程序主机上每一台受保护虚拟机的安全策略，**全自动配置安全虚拟机**——一种基于安全策略的专业安全设备。
- **与NSX安全策略集成，**让每一台受保护的虚拟机获得精确的细粒度安全，从而使管理员能对没有边界的公司软件定义数据中心进行调整。
- **与NSX安全标签集成，**让企业软件定义数据中心能够实时监测到最新威胁，并做出响应，甚至在必要时重新配置整个基础架构。
- **全面的基础架构扫描**可保护所有联机或离线虚拟机，扩大网络安全的覆盖范围，甚至覆盖企业的整个虚拟化基础架构。
- 通过基于云的卡巴斯基安全网络**主动防御网络威胁。**

VMware NSX 无代理安全解决方案

卡巴斯基虚拟化安全解决方案——无代理与VMware NSX紧密整合。无需为每台虚拟机上额外安装代理，即可实时保护整个基础架构的所有虚拟机，同时系统对虚拟平台性能的影响近乎于零，管理任务仅消耗少量资源。



卡巴斯基虚拟化安全解决方案——无代理不仅提供恶意软件防护，还使用专门的虚拟网络IDS/IPS（网络攻击拦截功能，NAB）保护整个基础架构抵御网络攻击。

支持的平台和操作系统：

VMware虚拟化：

- VMware NSX 6.3、6.2
- VMware vSphere 6.5、6.0、5.5、5.1
- VMware Horizon View 7

微软虚拟化：

- MS Windows Server 2016 Hyper-V
- MS Windows Server 2012 R2 Hyper-V
- 通过SCVMM 2016、2012 R2部署

Citrix虚拟化：

- Citrix XenServer 7.0、6.5 SP1
- Citrix XenDesktop 7.12、7.11、7.9
- Citrix PVS 7.12、7.11、7.9

KVM（基于内核的虚拟机）：

- RHEL Server 7 patch 1
- Ubuntu Server 14.04 LTS
- CentOS 7

MS Windows操作系统：

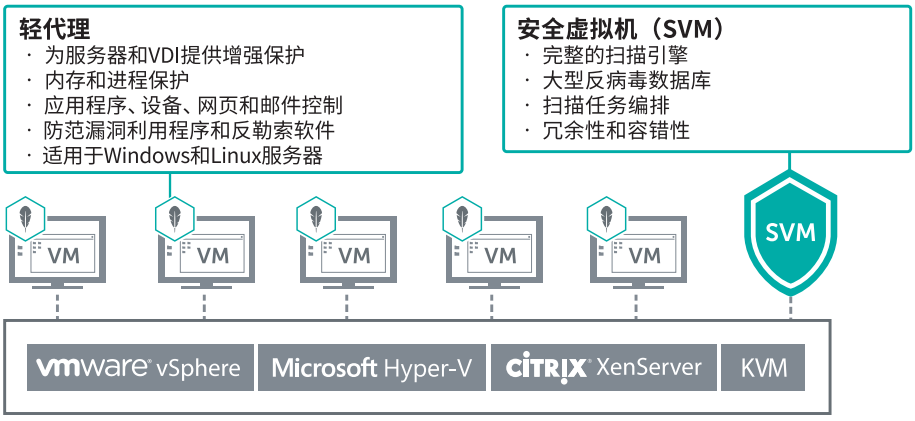
- Windows 10（包括RS1）、8.1、7
- Windows Server 2016、2012 R2、2012、2008 R2、2008（完整或服务器核心模式）

Linux操作系统：

- Debian GNU/Linux 8.5
- Ubuntu Server 16.04 LTS、14.04 LTS
- CentOS 7.2、6.8
- RHEL 7.2、6.7
- SUSE LES 12 SP1

轻代理提供更多安全层级

卡巴斯基虚拟化安全解决方案——轻代理支持包括VMware vSphere、Citrix XenServer、Microsoft Hyper-V和KVM在内的大部分主流平台，可同时为虚拟服务器和VDI提供可靠保护，是混合软件定义数据中心的理想之选。强大的轻量级安全代理支持诸如Citrix XenDesktop和VMware Horizon等行业领先的VDI平台，在为各虚拟机提供强大保护的同时，还能确保虚拟机的性能。

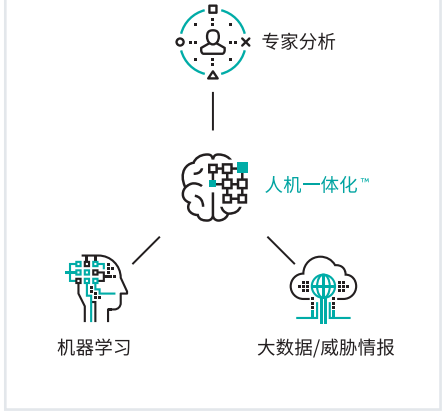


每台主机上的安全虚拟机（SVM）可集中扫描所有虚拟机。同时，部署在每台虚拟机上的强大轻量级代理可以激活高级安全保护功能，包括应用程序、设备和网页控制、邮件和网页流量的反恶意软件保护，以及先进的启发式分析技术。通过智能扫描任务编排，对多台受保护虚拟机的扫描任务进行分组和优先化排序，从而进行自动编排，降低最高资源消耗。

- **系统监视技术**使用行为流签名保持各VDI的一致性，预防加密病毒和勒索软件。
- **应用程序启动和权限控制，**包括默认拒绝，控制用户活动，确保受保护的虚拟机上只运行受信任的应用程序。
- **通过主机入侵防御系统的网络攻击拦截功能，**保护虚拟环境免于遭受网络攻击。
- **URL保护**可保护每台虚拟机远离可能实施破坏或不符合企业安全策略的恶意软件以及恶意互联网资源。
- **邮件和网页流量保护**确保企业环境内部的所有通信安全，避免其成为恶意软件的攻击通道。
- **设备控制**可确保安全访问与虚拟桌面连接的虚拟化设备。

无论企业使用哪一种虚拟化平台，卡巴斯基虚拟化安全解决方案及其完善的技术和独有的架构，均能提供强大的安全保护。该方案支持VMware vSphere以及NSX、Microsoft Hyper-V、Citrix XenServer和KVM。无论企业的平台如何配置和组合，无论是本地还是外部平台，均通过统一的控制平台进行所有安全管理，并且确保系统的高效运行。

卡巴斯基虚拟化安全解决方案将轻代理和无代理两种模式合二为一。这两种安全解决方案由卡巴斯基实验室独有的人机智能提供支持，均能实现出色的保护。



卡巴斯基实验室

企业网络安全：www.kasperksy.com.cn/enterprise

网络威胁新闻：www.securelist.com

IT安全新闻：https://www.kaspersky.com.cn/blog/b2b/

真正的网络安全

人机一体化

www.kaspersky.com.cn

©2017 AO卡巴斯基实验室保留所有权利。注册商标与服务商标归其各自所有者所有。