360 网神虚拟化安全管理系统 V7.0

（无代理）

技术白皮书

企 业 安 全 领 军 者

版本信息

文档名称	密级	创建人	创建日期

修订记录

修订日期	修订内容	修订人
2017.11.09	新建	政企云事业部
2018.04.08	更新功能	政企云事业部

目录

1. 云计算安全防护面临的新问题

随着云计算技术的日趋发展，越来越多的政府、企业正不断地把业务迁移到云计算平台中，但与此同时也带来了诸多新的安全防护问题：

1.1. 边界消失带来的安全防护盲点

由于云计算边界消失的问题，数据中心内部“东西向”威胁成为主要的安全问题。传统的安全设备更偏向“南北向”内外网的防护，无法保障数据中心安全。

1.2. 层出不穷的“未知威胁”

由于数据中心的数据集中存放，成为黑客“高价值”的猎物。攻击者为了获取数据，针对数据中心的安全漏洞，不断变换攻击方法，现有的“基于特征库”的安全软件对此失效。

1.3. 安全运维困难

根据等保规范，配置了许多不同厂商的安全产品。由于产品间缺乏联动和统一管理，管理成本很高，但收效甚微。

1.4. 安全软件部署成本过高

沿用传统的有代理模式，在每个虚拟机上安装安全软件耗费了大部分的系统资源，造成虚拟机密度极具降低，大幅度的增加了数据中心的建设成本。

2. 360 网神虚拟化安全解决方案

360 企业安全集团针对虚拟化环境下诸多安全问题提供全新的安全防护方案。360 网神虚拟化安全解决方案采用创新的无代理防护模式，即在宿主机的虚

拟化层对文件、网络和系统数据进行检测，避免了安全软件在同一主机上的重复部署，显著的降低了安全系统对资源的占用。经测算，采用新的防护方式，可将虚拟机部署数量提升 3 倍以上，大幅度的降低云计算数据中心的建设成本。系统提供中央控管的全方位云安全管理平台，集成了防恶意软件、进程管控、防火墙、应用控制、入侵防御、DDoS 防护等多个安全模块，以确保应用及数据安全。除此之外，系统提供可视化的安全管理，通过对海量访问日志数据的分析，找到异常行为、定位未知的安全威胁，帮助用户快速制定应对的安全策略。

3. 360 网神虚拟化安全管理系统介绍

3.1. 产品架构与部署

360 网神虚拟化安全管理系统无代理型有安全组件和管理中心两部分组成：

3.1.1. 管理中心

在每个数据中心内部安装一个管理中心，可以对异构的私有云、公有云和物理平台进行统一安全管理，配置每个虚拟机或物理终端的安全策略。

管理中心接收安全组件上传的安全事件和网络流量日志，通过多维度、细粒度的大数据分析，并以可视化的形式展现给用户，从而帮助用户对已知威胁进行溯源，并对未知威胁进行预警。

3.1.2. 安全组件

安全组件安装在数据中心每个计算节点、物理服务器上，接收管理中心配置的安全策略，对虚拟机或物理终端进行文件、网络和系统的安全防护，并将安全事件及行为日志上传到管理中心进行分析。

对于不同的虚拟化平台，安全组件以无代理的方式部署在虚拟化平台的虚拟化层，或者以安全虚拟机的形式进行部署，无需在虚拟机中部署安全软件的客户端。所有的安全功能包括文件扫描和网络流量扫描都在虚拟化层或者安全虚拟机中进行。

对于非虚拟化平台中的终端，如物理主机、云主机等，安全组件可以通过有代理的方式部署在其中，并对文件、网络及系统进行安全防护。

3.2. 产品优势

3.2.1. 防护新的云端威胁

- 防护在同一个数据中心、甚至是在同一主机上的两个虚拟机之间的攻击这种新的威胁。采用传统的网络安全设备无法检测。
- 应用防火墙，全文解析网络数据的内容，根据内容制定灵活的安全策略。
- 自动检测虚拟机的系统和应用，并调整入侵检测的规则。使得虚拟机无需安装补丁即可防护利用系统漏洞的新的威胁。
- 未知威胁的防护，通过对海量访问日志数据的分析，找到异常行为、定位未知的安全威胁。

3.2.2. 广泛的云平台的支持及统一管理

- 支持主流的虚拟化平台，包括 VMware、Xen、KVM 等。
- 与 OpenStack 的深度集成，支持绝大部分的国产云计算平台。
- 对异构的虚拟化平台进行统一安全管理。
- 支持虚拟化平台无代理部署和非虚拟化平台有代理部署的统一安全管理。

3.2.3. 提升云计算投资回报率

- 采用无代理部署的模式，即在云服务器的外部虚拟层进行安全检测及防护，极大地提高了安全防护的效率。
- 虚拟机内部无需安装安全检测软件，极大地降低了安全检测对资源的消耗。
- 高效的缓存机制，系统自动规避重复数据的检测，提供无与伦比的安全防护的性能。
- 根据主机的资源使用状况，系统动态的调节安全检测的系统开销，使得安全检测对系统性能的影响微乎其微。

3.2.4. 更低运营成本

- 管理中心采用中央控管的管理方式，集中的配置每一台虚拟机的安全策略，提供了便捷的管理、更高的灵活性。
- 采用多租的架构，使得系统不仅适合私有云的部署，也适合提供租赁服务的公有云。通过管理中心，可以为每个用户配置不同的安全策略。
- 安全特征库的自动升级，避免用户频繁升级系统补丁而引起的服务中断，降低了管理成本。

3.2.5. 可视化的安全管理

- 海量访问日志的、安全日志的分析及处理，及时找到异常行为、定位未知的安全威胁。
- 网络流量、安全威胁地图。
- 多维度的安全数据分析，支持数据挖掘，便于用户监控整个安全事件发生的整个过程。
- 灵活的分析图表及报表系统。

3.2.6. 安全态势全方位感知-网络态势大数据可视化

- 对安全威胁进行可视化呈现，全方位感知安全态势。
- 基于支持地理空间分布，对全网主机及关键节点的综合安全信息进行网络态势监控。
- 提供全面的网络威胁安全分析功能，深入分析网络流量信息，对全网各节点进行实时监测，并支持多种图表的威胁告警方式，让威胁一目了然。
- 根据安全威胁事件的来源信息和目标信息，结合 GIS 技术将虚拟的网络威胁和现实世界生动的结合起来，实现网络安全态势的可视化。

3.3. 主要功能

3.3.1. 恶意软件防护

- 无需在虚拟机内部安装杀毒软件，防止其受病毒、间谍软件、木马和其他恶意软件的侵害。
- 支持文件系统的实时防护、定期全盘检测、以及快速和全盘两种手工文件检测方式。
- 感染的文件删除、修复、隔离以及恢复。

- 指定目录和文件类型的检测。
- 文件和目录的检测白名单。
- 高效的缓存机制，避免不同虚拟机内部的相同文件被重复检测，极大的提高了文件检测的性能。
- 优化安全操作的资源调度，以避免全系统扫描时出现常见的防病毒风暴。
- 恶意代码特征库的自动更新。
- 指定隔离文件最大容量配置、后台扫描最大并发数。

3.3.2. 进程管控

- 支持根据进程路径和进程名制定规则，并预置操作系统信任进程列表。
- 支持白名单和黑名单方式，可针对不同的用户场景灵活配置管控规则。
- 未被允许的进程将无法使用，彻底阻止勒索软件或其他恶意软件执行。

3.3.3. 完整性监控

- 完整性监控功能可以扫描并检测对计算机文件，目录，注册表项和值等的更改，这些更改将记录为管理中心的事件，供管理员分析查看。
- 系统默认根据操作系统推荐完整性监控规则。

3.3.4. 防火墙

- 对虚机进行微隔离，不但能控制南北向流量，还可以控制云平台内部虚拟机之间的东西向流量。
- 按照 IP 地址、端口、流量类型以及流量方向来配置防火墙规则。

3.3.5. 应用控制

- 2300 多种国内主要网络应用协议的内容解析及精确识别。
- 上网行为管理，可以针对每个虚拟机用户统一配置管理策略，阻止、放行特定的应用程序，提高工作效率。
- 对应用协议进行分类，可以针对分类配置阻断、放行策略，对于新增的应用，能自动应用分类的配置策略。
- 自动更新应用解析的规则库，不断增加新应用的支持，及时识别更新后的网络应用。

3.3.6. 入侵防御

- 支持 8000 多种针对系统、应用漏洞的入侵防御规则。
- 对已知的漏洞进行虚拟修补，在虚拟机系统及应用不进行安全补丁升级的情况下，防御针对漏洞的攻击。
- 防护 SQL 注入，跨站脚本攻击及其他的利用 Web 应用程序漏洞的攻击。
- 系统自动侦测虚拟机系统的内容，动态的调整用于检测的入侵检测的规则库，提高检测的效率。
- 自动更新功能，及时防御针对最新漏洞的攻击。

3.3.7. DDoS 防护

- 支持对 TCP、UDP 和 ICMP Flood 攻击的防护。
- 支持针对每台虚拟机单独进行流量清洗。

3.3.8. 可视化分析

- 支持海量安全日志数据的分析及查询。

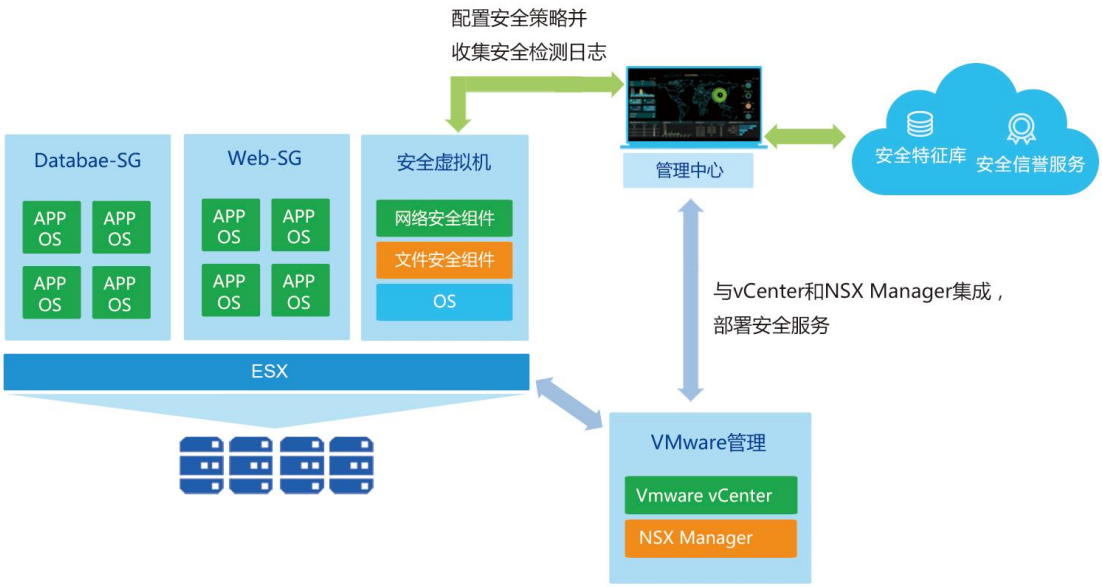
- 安全威胁地图，描述安全威胁发生的地理位置。
- 网络流量地图，对网络的新增连接、数据流量、地理位置的分析及数据挖掘。
- 以虚拟机、操作系统、应用程序、攻击类型、恶意代码类型、地理位置、时间等多个维度
- 对文件、网络的海量安全数据进行关联性分析，并辅以多种图表形式，对同一数据进行描述，便于用户理解。
- 支持安全事件的数据挖掘，便于管理人员及时准确的找到攻击源，阻断安全威胁。

3.3.9. 安全态势感知

- 数据中心威胁态势感知，大屏动态显示安全运维的状况。
- 实时的网络分析，包括流量、连接统计。
- 安全威胁及流量的地理位置分析。
- 数据中心流量及威胁的统计数据。

4. 支持平台及部署方案

360 企业安全集团是国内少数领先的虚拟化云计算安全解决方案提供商，也是目前国内唯一能提供多平台混合云的统一管理的云计算安全厂商。我们支持国内主流的云计算平台，并提供丰富多样的部署方式，防护私有云、公有云及物理环境。

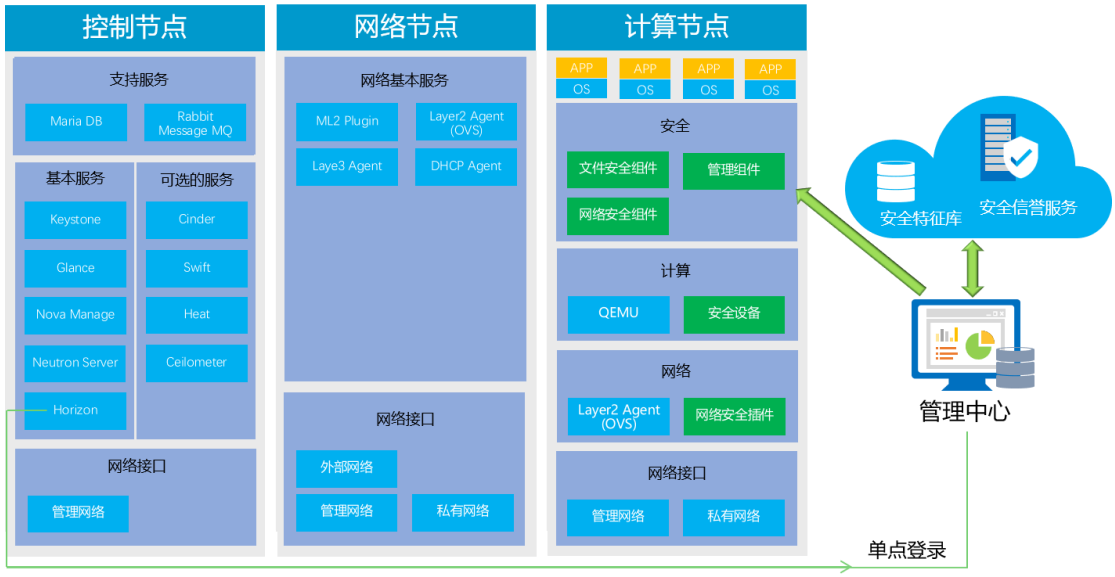


4.1. VMware 支持

通过在每台vSphere主机中部署安全虚拟机对其中的虚拟机进行无代理安全防护。该方案依赖于 VMware 的 vShield EndPoint 或者 NSX EndPoint 和 NetX 组件。

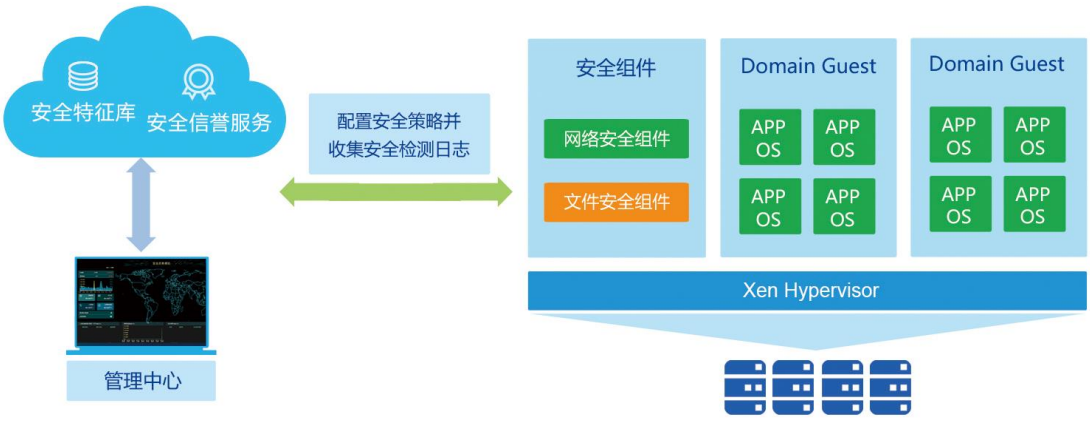
安全虚拟机集成了 VMware 的安全组件，对同一台 vSphere 主机的中虚拟机进行文件和网络的安全防护，通过接收管理中心配置的安全策略，对不同的虚拟机应用不同的安全策略，并将产生的安全事件和网络流量日志上传给管理中心。

4.2. Openstack 支持



安全组件部署在 OpenStack 计算节点中，在 OpenStack 网络组件中部署网络安全插件，并对每台虚拟机添加安全设备，即可以对虚拟机进行无代理的文件和网络安全防护。通过管理组件获取管理中心的安全配置，并上传安全事件和网络流量日志到管理中心。

4.3. Citrix XenServer 支持



安全组件部署在 XenServer 的 Dom0 中，即可以对虚拟机进行无代理的文件和网络安全防护。

4.4. 其它虚拟化平台支持

支持的其他虚拟化平台（持续更新中）：

华为 FusionSphere 云管理平台

H3C 云计算管理平台

中兴通讯云计算虚拟化桌面

浪潮 InCloud Sphere

浪潮云海 OS

QingCloud 青云

CNware WinCenter

品高云

oCloud 东方通虚拟化平台

CloudManager 云管理平台

乾云云管理平台

机敏云

普天云

斯坦德云

oVirt 管理平台

易思捷云管理平台

4.5. 有代理部署

对于非虚拟化平台中的终端，如物理主机或公有云中的云主机，可以通过部署有代理安全组件进行安全防护。目前支持几乎所有的 Windows 操作系统和主流的 Linux 操作系统。

4.6. 操作系统支持

下面是虚拟化安全支持的操作系统。

Windows 操作系统：

- Windows XP
- Windows XP Embedded
- Windows Vista
- Windows 7
- Windows 8
- Windows 10
- Windows 2000 (32 位)
- Windows 2003
- Windows 2008
- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016

Linux 操作系统：

- SUSE Enterprise 9，10，11，12
- Red Hat Enterprise Linux Server 5.0，6.0，6.5，7.0，7.2
- CentOS 5.0，6.0，6.5，7.0，7.2
- Ubuntu
- BC Linux
- 中标麒麟通用服务器操作系统(NeoKylin Linux)
- 深度 Deepin
- Oracle linux5、6、7