# 360 虚拟化安全管理系统产品白皮书

## 版权声明



## 适用性说明

本模板用于撰写 360 企业安全集团中各种正式文件，包括技术手册、标书、白皮书、会议通知、公司制度等文档使用。

# 目 录 | Contents

# 一. 引言

云计算安全（cloud security）是指云计算模式中的安全能力，是网络时代信息安全的最新体现，在云计算的架构下，云计算开放网络和业务共享场景更加复杂多变，安全性方面的挑战更加严峻，一些新型的安全问题变得比较突出，如多个虚拟机租户间并行业务的安全运行、虚拟化底层的稳定和延续性等。由于云计算采用了云服务模式，其基础 IT 架构发生了本质的变化，传统的 IT 安全方案无法对云计算环境提供有效的安全防护能力，因此企业应以新的思路来实现云计算环境的安全。

# 二. 云计算安全

## 2.1 云计算安全范畴

针对云计算安全，需要考虑整体安全状况态势，以安全控制的手段在云计算建立过程中一层或多层上实现，包括 IT 设备的物理与网络安全、系统安全、虚拟化安全、上层应用安全等方面，此外，还包括人员、管理层面的安全控制。而虚拟化作为云计算的核心支撑技术，在考虑云计算安全的时，虚拟化的安全就成了优先考虑的重点。

## 2.2 虚拟化现状与安全挑战

虚拟化软件作为云计算的基础架构为虚拟化管理与虚拟化安全提供了一个良好的平台，如著名的 Xen、vSphere、 Hyper-V 等产品。上述虚拟化软件利用运行在物理服务器和操作系统之间的中间软件层 Hypervisor，协调访问服务器上的所有物理设备和虚拟设备。Hypervisor 也叫虚拟机监视器（Virtual Machine Monitor），是这些虚拟化管理软件的虚拟化技术核心。随着互联网的飞速发展，越来越多的企业意识到 Hypervisor 安全是虚拟数据中心安全的首要条件。

针对传统安全防火墙技术不能有效监控虚拟机流量的问题。业界有些公司使用 VMware 公司的 API 开发了虚拟安全分析器，以检测虚拟交换机流量——在虚拟层之上的网络层流量。相应地也出现了虚拟网络防火墙，这种防火墙基于虚拟机管理器，可认证有状态的虚拟防火

墙，检查所有通过虚拟机的数据分组，组织所有未经批准的连接和允许对数据分组进行更深层次的检查，确保了虚拟机间部分通信的安全，但是对于虚拟机之间的攻击流量的特殊性，使用虚拟化厂商的网络流量分析已经无法解决这样的问题。

虚拟化技术是生成一个和真实系统行为一样的虚拟机器，虚拟机像真实操作系统一样，同样存在软件漏洞与系统漏洞。必须像对待真正的操作系统一样加固虚拟机，给程序不断地及时打补丁升级，以此来保证虚拟机的安全，同时宿主机的安全需要得到同等的关注。

传统杀病毒安全软件可以部署在虚拟机中解决虚拟机防病毒的问题，但传统的防病毒技术依靠已知病毒特征样本对所有文件进行详细的扫描与分析，准确率依赖于病毒样本库的覆盖面和规模，其效率受限于技术方案的局限性，往往会占用过多的物理机 CPU、内存、网络资源，效果差强人意。

传统的防病毒软件可以一定程度的解决已知病毒、木马的威胁，但对于越来越多的 APT 攻击却束手无策。APT 很多攻击行为都会利用 0day 漏洞进行网络渗透和攻击，且具有持续性及隐蔽性。此种持续体现在攻击者不断尝试各种攻击手段，以及在渗透到网络内部后长期蛰伏，不断收集各种信息，直到收集到重要情报。更加危险的是，这些新型的攻击和威胁主要针对大型企业、国家重要的基础设施或者具有核心利益的网络基础设施。由于 APT 特种木马的免疫行为，所以传统的防病毒软件以及安全控管措施和理念很难有效应对 APT 攻击。

由于云计算与虚拟化环境自身的特性，企业需要充分考虑虚拟化的引入为企业带来的相应的风险，根据各个风险点带来的问题及威胁建设针对性的防护方案，以保障企业数据的安全及业务系统的平稳运行。

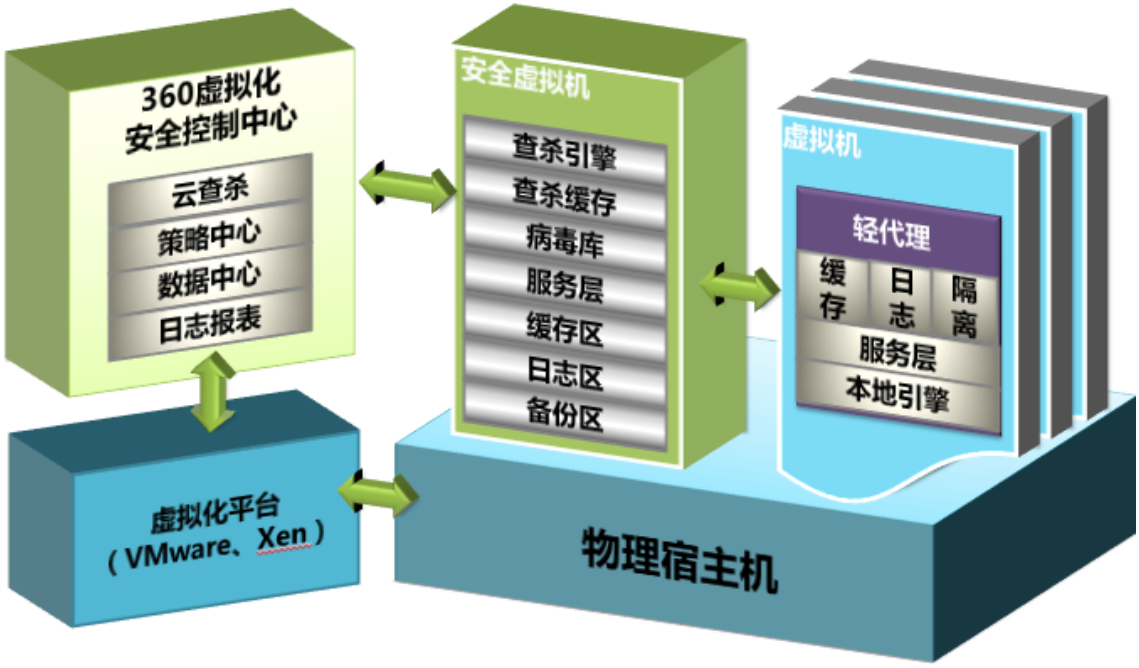
# 三. 360 虚拟化安全管理系统简介

## 3.1 产品概述

360 虚拟化安全管理系统是一款针对于云数据中心的虚拟化安全管理系统，可对物理资源池、虚拟资源池、云资源池进行统一的安全防护与集中管理，对宿主机、虚拟机、虚拟机应用提供三层防护安全架构，具备对混合虚拟化平台、混合操作系统、混合系统应用环境的兼容防护能力。在虚拟化环境中出现的病毒风暴、安全域混乱、宿主机安全、虚拟机之间攻击等问题，360 虚拟化安全管理系统都可提供行之有效的解决办法。最终为用户提供一套可跨多种平台、防护无死角的综合虚拟化安全解决方案。

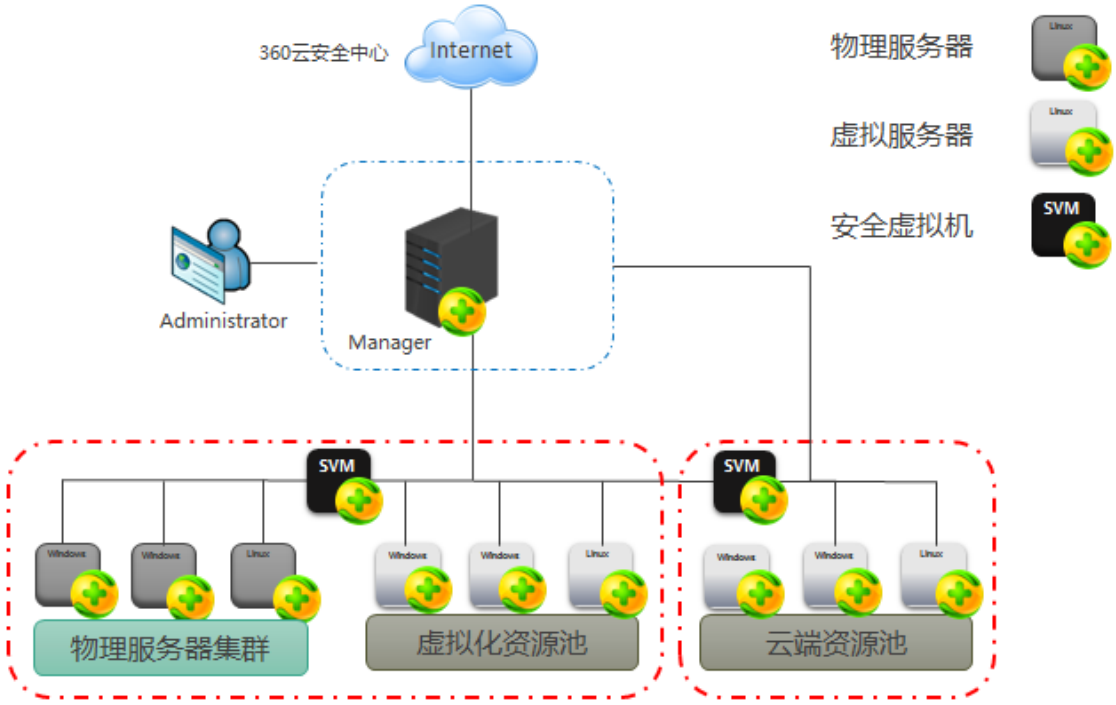
## 3.2 产品架构

360 虚拟化安全管理系统主要由 360 管控中心、安全虚拟机及轻型代理客户端组成，产品架构图如下图所示：



## 3.3 部署拓扑

360 安全管理系统部署拓扑图如下所示：




# 四. 主要功能

## 4.1 多引擎病毒查杀

360 依靠多年在杀毒领域的技术积累，自主开发出了 QVM 人工智能引擎、云查杀引擎、AVE 文件修复引擎、QEX 宏病毒检测引擎四大杀毒引擎，其中，QVM 人工智能引擎依托于 360 云端超过 100 亿条病毒样本，进行家族类可视化分析，可对未知变种病毒实现精准的查杀与隔离。四大杀毒引擎在运行时可进行数据交互，对虚拟机及服务器进行扫描结果缓存共享，在整个数据中心进行增量扫描从而提高扫描效率。

## 4.2 虚拟补丁

补丁管理一直是企业关注的核心问题，由于企业内部的 IT 环境多种多样，在进行补丁管理的时候面临的风险也日益严峻，如 XP 系统的补丁管理、热补丁带来的物理服务器重启风险、

补丁空窗期等问题。360 虚拟化安全管理系统可以通过虚拟补丁的方式对存在漏洞的企业服务器操作系统及应用进行修复，由于虚拟漏洞修复模块无需对操作系统及应用进行代码修改，只是对于来自外部的攻击行为进行识别和过滤，无需重启虚拟机或服务器，企业既无需担心兼容性问题也无需重启系统中断业务，因此虚拟补丁可以在保障企业业务系统连续运行的情况下对攻击行为进行有效防护。

## 4.3 虚拟化防火墙

360 虚拟化安全管理系统在虚拟机内部植入了轻量化的防火墙守护程序，该模块可以通过管理中心进行统一访问控制策略管理，对每台虚拟机下发个性化访问控制策略，且该策略会与虚拟机进行适配绑定，无论虚拟机在资源池中如何漂移都不会造成策略失效，甚至管理员可以根据原有安全域进行虚拟安全域划分，将不同的物理服务器与虚拟服务器进行安全域划分，从根本上解决企业在虚拟化进程中经常遇到的安全域无法划分的问题。

## 4.4 威胁情报联动防御

360 虚拟化安全管理系统可以与 360 威胁感知平台智能联动，接收威胁情报及全球威胁态势，智能调整数据中心安全防御策略。结合 360 虚拟化安全在终端上的精确防御能力，实现对虚拟化终端的攻击防御。

天眼威胁感知系统在检测出网络攻击行为之后，一方面会采用页面报警、邮件报警的方式对攻击行为进行实时报警，同时，天眼威胁感知系统还会将报警信息实时发送给部署在终端之上的 360 虚拟化安全终端安全管理系统进行有效联动。终端在接收到报警信息之后，会及时根据报警信息所提供的文件标识对终端文件进行更新查杀，实现“边界发现、终端防御”的防御效果。

## 4.5 宿主机防护

当前业界安全厂商都将安全防护的核心聚焦虚拟机安全，随着互联网的飞速发展，越来越多的企业开始将注意力集中在提供虚拟化服务的 Hypervisor 层，360 结合多年的安全防护经验，并深入研究 Hypervisor 层系统架构与脆弱性分析，大胆提出在 Hypervisor 层中植入

轻型代理的方式来防护宿主机安全，为虚拟化环境提供自上而下，由内而外的整体安全防护方案。

# 五. 优秀特性

## 5.1 强大的跨平台防护能力

360 虚拟化安全管理系统支持 VMware vSphere、Microsoft Hyper-V、H3C CAS、Huawei FusionCompute、Citrix XenServer、Redhat Enterprise Virtualization 等多种国内、国外虚拟化平台，并可以对虚拟资源池以外的物理资源池或者云端资源池进行统一的安全管理，形成威胁统一管理平台，简化运维成本，提高安全运维水平。

## 5.2 智能的虚拟机查杀策略

360 虚拟化安全管理系统在进行病毒查杀时会进行缓存化处理，由同一虚拟机模板生成的虚拟机在进行一次全盘扫描后，将会记录扫描过的安全文件的特征，多台虚拟机轻代理会共享扫描缓存，在扫描下一台虚拟机时会仅仅扫描虚拟机中的差异化文件部分，此扫描方式将会大大提高扫描的速度并降低扫描的资源及时间消耗。并且在扫描多台虚拟机时能够自动根据待扫描虚拟机集群进行序列化查杀，只有在结束一台虚拟机扫描时才会开始下一台，因此可以有效避免全盘扫描导致的查杀风暴等问题。

## 5.3 灵活的虚拟机漂移绑定

在虚拟化资源池中由于虚拟机资源的弹性可变，因此经常发生由于资源枯竭等原因导致的虚拟机从不同的安全域之间反复漂移的情况，而使用无代理方式无法保障整体资源池中都部署安全防护策略，因此无法保障在漂移后的虚拟机安全策略随虚拟机绑定。360 虚拟化管理系统采用独有的轻代理部署方式，在虚拟机中植入轻型代理，轻代理安全策略和虚拟机无缝绑定，无论虚拟机漂移至虚拟化资源池中的任何宿主机均可保证虚拟机防护策略稳定有效，提供全时的坚实防护。

## 5.4 有效的虚拟机访问控制

企业在虚拟化的过程中，得到了一个高效资源利用率的 IT 环境，这依靠的是虚拟机漂移这一优质特性，但是，客户原本的安全域划分将随着虚拟机漂移将被完全打破，而传统的安全设备无法对这一问题束手无策。360 虚拟化安全管理系统具有虚拟防火墙功能，它根植于轻代理中，可依据用户业务的需要，制定防火墙访问控制策略，根据安全域规格批量下发给虚拟主机后，无论虚拟机漂移到任何位置，虚拟机访问控制策略不变，原有安全域稳定继承，极大方便了业务主机的安全管控工作。

## 5.5 领先的 Hypervisor 防护

360 拥有东半球第一支专业的虚拟化平台漏洞研究团队，已发现多个带有 CVE 编号的虚拟化平台漏洞，具有深厚的虚拟化安全研究底蕴，在发现虚拟化平台安全漏洞时，可在第一时间完成对虚拟化平台漏洞的研究和防护。除此之外，通过对 Hypervisor 层系统架构与脆弱性分析，研发出了一套针对 Hypervisor 层独有的序列化检测引擎，可有效预防 Hypervisor 层的零日漏洞，完善宿主机的安全防护体系。

# 六. 客户价值

## 6.1 混合环境统一管理

在虚拟化的演变过程中，客户的 IT 环境会经历从物理环境向虚拟化环境乃至云端环境演变，而且部署环境错综复杂。360 虚拟化安全管理系统采用轻代理的部署方式，可对物理资源池、虚拟资源池、云端资源池进行统一的安全防护与管理，并且具备对混合虚拟化平台、混合操作系统、混合系统应用环境的兼容能力，降低企业运维成本。

## 6.2 完善的立体防御体系

基于多年互联网安全防护的技术积累，融合了 360 虚拟化攻防团队的研究成果，360 虚拟化安全管理系统提出了宿主机、虚拟机、虚拟机应用的三层防护安全架构，从虚拟机资源池

中的底层安全，到虚拟机的系统安全，到虚拟机内部的应用安全，为企业提供自内至外、自上之下的立体防御体系。

## 6.3 降低补丁修复成本

补丁管理对于企业至关重要，长时间的漏洞空窗期会使企业面临业务系统中断等安全风险，但是企业中的 IT 环境错综复杂，操作系统多种多样，在进行补丁管理时遇到了诸多问题：例如 Windows XP 及 Server2003 等操作系统厂商已经不再提供技术支持；甚至有的系统在漏洞修复完毕后重启系统发现业务系统无法正常运行，而 360 虚拟化管理系统提供给用户的虚拟补丁功能，可以在漏洞出现后第一时间联合云端进行规则更新，直接应用到轻代理中，企业无需重启系统或应用，兼容性及稳定更好，及时封堵了漏洞空窗期，大大降低了运维难度。

## 6.4 全面防护零日漏洞

360 补天平台是全球最大的漏洞响应平台，可以让厂商最快发现漏洞。360 虚拟化安全管理系统通过和 360 补天平台进行有机联动，可在第一时间获取零日漏洞信息，并且形成虚拟补丁对操作系统及应用进行加固。另外，360 安全管理系统依靠 360 虚拟化研究团队的研究成果，研发了独有的序列化检测引擎，此引擎依托于虚拟化平台内部的检测机制，根植于 Hypervisor 层，可实现全面检测各种虚拟化平台的零日漏洞。

# 七. 结语

云计算是基于互联网的相关服务的增加、使用和交付模式，通常涉及通过互联网来提供动态易扩展且经常是虚拟化的资源，云计算安全的根本，便是虚拟化安全。随着时间的推进，越来越多的企业意识到虚拟化的优势，开启了数据中心的虚拟化进程，这无疑是时代的选择，虚拟化带来了弹性可变的高利用率形态，同时，也引入了相对应的虚拟化安全风险。

虚拟化安全究竟是什么？虚拟化使 IT 环境发生了巨变，我们不妨探究一下虚拟化安全的本质，在虚拟化之前，我们一直在考虑的安全范畴包括数据安全、应用安全、网络安全、系统安全等，而在引入虚拟化之后，我们要考虑的不仅仅是虚拟化引入的宿主机安全、虚拟机互相攻击等虚拟化相关问题，更要考虑依托于虚拟化形态的数据安全、应用安全、网络安全、系统安全等，那么，如何融入虚拟化这一形态将是虚拟化安全的首要考量标准。而传统的硬

件安全设施伴随着虚拟化进程将无法完全融入，这时候，就需要一套完全适应于虚拟化形态的解决方案。

360 虚拟化安全管理系统应需而生，它采用轻代理的部署方式，以低消耗的形态切合于虚拟化环境中，全面兼容各种虚拟化平台、各种虚拟机操作系统、各种系统应用，依托于 360 专业的虚拟化安全研究团队与大数据分析平台，大胆提出了虚拟化防护三层架构体系，广泛的应用于政府、教育、金融、能源等各个行业之中，为用户的云数据中心保驾护航。