360云安全管理平台

——产品白皮书

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | █文档编号 | █密级 内部公开 | | █版本编号 V1.0 | █日期 2016-7-11 | |



|  |
| --- |
| █ **版权声明** |
| 本文中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，所有版权均属360企业安全集团所有，受到有关产权及版权法保护。任何个人、机构未经360企业安全集团的书面授权许可，不得以任何方式复制或引用本文的任何片断。 |

|  |
| --- |
| █ **版本变更记录** |
| |  |  |  |  | | --- | --- | --- | --- | | **时间** | **版本** | **说明** | **修改人** | | 2016-7-11 | V1.0 | 创建 | 任子骙 | |  |  |  |  | |

|  |
| --- |
| █ **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

[1 前言 5](#_Toc448419074)

[2 为什么需要网站监控 5](#_Toc448419075)

[2.1 攻与防的博弈 5](#_Toc448419076)

[2.2 安全思路的转变 6](#_Toc448419077)

[3 传统网站安全监控的弊端 6](#_Toc448419078)

[3.1 单一的探测源头 7](#_Toc448419079)

[3.2 钓鱼网站探测盲区 7](#_Toc448419080)

[3.3 漏洞探测技术陈旧 7](#_Toc448419081)

[3.4 违规资产难以发现 7](#_Toc448419082)

[4 360网站群监测系统介绍 8](#_Toc448419083)

[4.1 产品概述 8](#_Toc448419084)

[4.2 产品架构 8](#_Toc448419085)

[4.3 产品原理 9](#_Toc448419086)

[4.3.1 多引擎扫描技术 9](#_Toc448419087)

[4.3.2 沙箱检测技术 9](#_Toc448419088)

[4.3.3 特有搜索检测技术 10](#_Toc448419089)

[4.3.4 最新漏洞舆情推送手段 10](#_Toc448419090)

[4.3.5 可用性监控技术 11](#_Toc448419091)

[4.3.6 DDOS攻击检测技术 11](#_Toc448419092)

[4.4 产品主要功能 12](#_Toc448419093)

[4.4.1 安全趋势监控 12](#_Toc448419094)

[4.4.2 有效跟踪通报处理进度 12](#_Toc448419095)

[4.4.3 态势感知 13](#_Toc448419096)

[4.4.4 报表管理 14](#_Toc448419097)

[4.4.5 配置管理 16](#_Toc448419098)

[5 产品优势 17](#_Toc448419099)

[5.1 产品优势 17](#_Toc448419100)

[5.1.1 立体多维，监控服务更周到 17](#_Toc448419101)

[5.1.2 持续监测，反复跟踪无死角 18](#_Toc448419102)

[5.1.3 威胁情报，助安全一臂之力 18](#_Toc448419103)

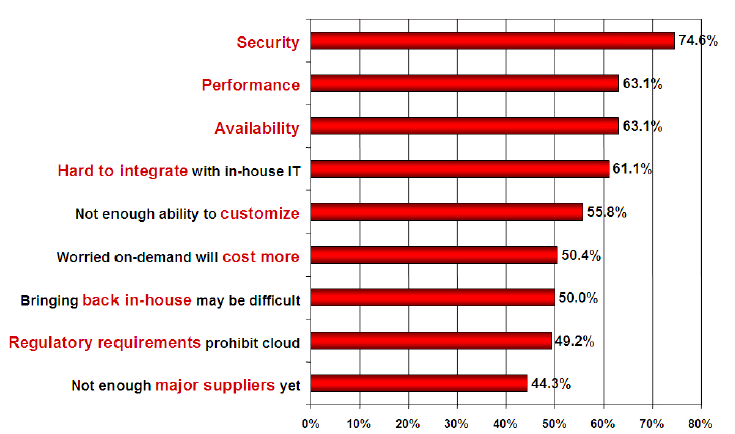
[5.1.4 集中力量，造网站安全护甲 19](#_Toc448419104)

# 前言

云计算的迅猛发展，大大改变了今天的商业环境。一方面，企业享受到云计算带来的种种益处：节省成本开支、增强计算能力、灵活的业务应用扩展等。

而另一方面，高整合、高竞争、高淘汰的新商业环境，也让企业的生存和发展高度依赖于两个核心要素，即“云”自身的可用性和企业核心数据的安全。正是基于应对云环境新的安全挑战，更好地保护企业业务发展，360企业安全将云安全技术进行了革命性的进化，推出全新云安全解决方案。

IDC在一次关于“您认为云计算模式的挑战和问题是什么？”的调查中，安全以74.6%的比率位居榜首，可见安全是人们对云计算最大的担心。实际上，由于云时代的企业，其自身的业务应用和云环境高度关联，哪怕是短短一分钟的停机，对于依赖“云应用”的企业而言，其后果都是灾难性的。因此，企业在将重要业务和基础设  
 实施向云端迁移时，首先要关注云平台本身的可靠性和安全防护。



此外，存放于云环境中的企业数据信息，同样是关系到企业在“云”时代取得竞争优势的核心资源，调查显示，对于大部分企业和组织机构来说，风险防范、数据隐私和遵从法规要求，成为其实施“云”服务的另一个重要顾虑。

# 云安全框架

云计算中的主要组成部分包括了：

* 云的基础设施，这部分是实现云计算的基础；
* 云数据，是指存储在云计算中的数据；
* 云应用，是指通过B/S结构的方式实现外部应用的云计算服务。

## 云基础设施

云计算的基础设施划分为3个类别：服务器、存储和网络连接。 服务提供商可能会提供虚拟服务器实例，在这些实例上，用户可以安装和运行一个自定义的映像。持久性的存储是一种单独的服务，客户可以单独购买。最后，还会有一些用于扩展网络连接的产品。基础架构服务可全面虚拟化服务器、存储设备和网络资源，聚合这些资源，并基于业务优先级将资源准确地按需分配给应用程序。

* 服务器实际上代表了随着计算资源一起分配的最小存储空间和输入/输出信道的资源集合。
* 存储通常提供与位置无关的虚拟化数据存储，这样促进了对通过弹性机制制造无限容量存储的期望，而且高度的自动化水平使得用户能非常容易地使用。

大多数基础设施层的组件最终是通过虚拟化技术供应商的设施进行管理的。而虚拟化实现后，其安全的考虑发生了质的变化，完全打破了传统安全防护的概念。

## 云中数据

随着云计算技术的逐步成熟，它给IT应用带来的商业价值越来越明显的表现出来，相对于传统的软件架构，云计算运营和支持方面的成本更低廉，但同时又能够获得更快速的部署能力，近乎无限的伸缩性等收益。然而，尽管云计算带来的价值是如此之巨大，但是仍然有诸多企业在云计算和传统软件架构中选择了后者，其原因很大程度上在于云计算领域中，有关企业数据的安全问题没有得到妥善的解决。一些分析机构的调查结果显示出，数据安全问题是企业应用迁移到云计算过程中的最大障碍之一。

怎样保证存储在云中的数据，不被其他人看到、不被其他人使用、删除后没有备份存在等等，云中的数据安全是个很大的课题。

## 云应用

云应用使用很普遍，如在线办公系统、在线CRM等等，而这些服务往往都使用B/S的方式进行公布。在Web安全中，由于网站是开放给所有用户的，它在开放业务给用户的时候，也把自己暴露给了黑客，对网站的入侵相比其他的安全领域降低了门槛，那么在防御体系终究会被打破的预估下，如何快速、精确的发现安全影响将成为所有安全厂商面临的安全问题。

从以上的分析看，云计算下需要进行安全考虑的部分主要是：虚拟化、云中数据和云应用四个部分，下文会主要从这些方面进行安全阐述。

# 360云安全管理系统产品介绍

## 产品概述

为了应对云环境带来的新的安全挑战，更好的保护云上业务的发展，360公司通过大数据分析、可视化分析、威胁情报等手段建立了协同防御系统，全面整合了360独有的虚拟化漏洞挖掘与安全防御能力，推出了360云安全管理平台。

360云安全管理平台是全球首个全面解决专有云安全问题的一站式综合性解决方案。产品整体设计由原来“防范”为中心的，基于边界防御的传统网络安全，升级为由“监测——发现——防御”一体的解决思路，深入云计算内部，全面覆盖了云环境中的网络层、宿主机层、虚拟化层、云主机层、应用层、数据层等多层防护。

## 产品架构

从技术上来说，对云安全应该以全方位的视角去审视，按照物理层、主机层、网络层、应用层、数据层的多层次去建设。由于云环境与传统环境的差异性，又将主机层划分为了物理服务器层、虚拟化层和虚拟机层三个层面，并且在网络层重点关注虚拟网络层的安全。本产品采取一个平台进行所有层次安全问题的管理，即方案中涵盖的所有内容，除服务相关的内容以外，全部以统一管理平台的方式进行展现，能够在一个平台上对云安全平台进行统一管理，兼顾职责划分，并且实时监控，对云平台的状态实现内外部结合的云安全态势感知。方案设计了防御系统与安全态势感知系统两个子系统，分别对应各个层次的多个防御点与审计检测点，实现云安全的一站式解决方案。



## 产品主要功能

### 网络层安全监测与防护

通过云安全管理平台虚拟网络可视化界面，实现对网络层进行安全检测。云安全管理平台通过与云平台结合，生成虚拟机交换机流量镜像，所以可以提供云平台环境中虚拟网络的结构和变化。日常网络层安全检测包括：网络拓扑的可视化和网络分析的可视化

网络层安全防护通过虚拟防火墙，有效划分云平台安全域。完善的双向状态防火墙为所有网络通讯协议（包括 TCP、UDP 和 ICMP）提供全面支持。防火墙规则是完全可配置的，以每个网络接口为基础允许或拒绝网络通信，以及限制对允许的 IP 或 MAC 地址的通信。

### 物理机层安全监测与防护

针对日常系统文件，可通过云安全管理平台核心文件完整性检测，及时的发现核心系统文件的变化，帮组管理员发现攻击者的入侵。云安全管理平台使用预设的完整性检查规则可对文件和目录针对多方面的更改进行监控，包括：内容、属性（如所有者、权限和大小）以及日期与时间戳，还可监控对 Windows 注册表键值、访问控制列表以及日志文件进行的添加、修改或删除操作，并提供警报。完整性检查检测Config目录，保存的是需要监控的文件和目录。在运行完整性检测时，会生成新的签名信息，通过和基线数据库比较，找出被篡改的文件。

核心文件签名扫描通过收集核心文件的版本，创建时间，文件大小，md5等信息。帮助及时分辨出那些文件被修改。

### 虚拟化层安全监测与防护

云安全管理平台负责监控云平台中虚拟化层安全威胁，针对虚拟化层出现新的攻击层面，通过安全漏洞扫描工具，定时扫描发现虚拟化层漏洞并处理，避免因黑客攻击造成的虚拟机逃逸现象，针对突发漏洞情况，通过安全厂商提供工具进行防护。云安全管理平台虚拟化层漏洞扫描引擎通过虚拟化系统的符号特征、版本信息等条件匹配相应的平台漏洞，检测虚拟化漏洞信息。扫描完成后对所有的漏洞进行汇总分析，提供漏洞排名、漏洞分布情况、漏洞发生趋势等信息展示，并通过报表形式向管理员展示主机存在的系统脆弱性风险。

其中云安全管理平台针对宿主机层分析虚拟机的底层I/O操作，形成独有的安全基线行为准则，运维管理员无需配置，针对专网X中或特定服务器，可直接通过云安全管理平台下发匹配任务，从而发现和拦截各种已知和未知的虚拟机逃逸攻击，并能对未知攻击进行溯源。对服务器进行免疫保护，免招病毒传染和激活。

对于云平台中特殊文件与进程（包括误报、误删在内），统一通过云安全管理平台白名单进行控制。 云安全管理员在虚拟化层中安装驱动组件，在控制中心显示可被管理的主机数量。在宿主机列表中，选择被检测的物理主机，下发扫描任务。当扫描完成后，云安全管理中心显示发现漏洞，针对漏洞信息，安全管理员可以查看对应主机的漏洞信息详情。

### 虚拟机层安全监测与防护

#### 文件安全监测与防护

对于日常云主机运行中文件安全防护，由云安全管理平台配置实时防御策略。虚拟机开启实时防护后，进行主动防御，系统中进行每一个动作时（修改文件，启动进程，变更服务），主动防御模块都进行安全检查。可以有效避免常驻内存型病毒和服务型木马的攻击，还可以避免恶意黑客所利用0day漏洞进行的网络渗透和攻击。

#### 系统及应用监测与防护

360云安全管理平台包括入侵检测和虚拟补丁、Web 应用程序防护和应用程序控制，DPI 规则通过保护漏洞不受已知和未知攻击来提供入侵检测和阻止防护。此类防护也称为虚拟补丁，实现方式是每个规则定义预期的应用程序数据并根据其内容阻止恶意数据。 此外，DPI 规则通过一组 Web 应用程序防护规则来保护 Web 应用程序中的漏洞（如跨站点脚本 (XSS) 和 SQL 注入）。 通过检测已知的应用程序流量（在企业环境中可能需要限制），DPI 规则还可以用于向计算机提供应用程序控制。本系统规则更新会自动提供最新的全面防护，以抵御已知和未知攻击。

#### 账户安全监测与防护

账号作为云主机的入口，各运维人员需要保证各自云平台中的账户安全，需要保证内容包括身份唯一标识、密码的安全性（口令复杂性、定期更换等）及账号的生命周期管理，防止暴力破解、未知账号等风险，

云安全管理平台账号安全主要功能：

1. 检查是否存在root之外UID为0的用户
2. 检查用户口令设置是否为空
3. 限制使用root账号远程登录虚拟机进行操作，防止root账号特权被滥用

### 应用层安全监测与防护

#### 应用漏洞扫描与防护

针对云主机中的Web应用，进行定期安全扫描，并保存记录扫描报告。对于扫描所暴露漏洞，需要通过云平台管理软件或原厂商补丁进行修复，修复完成后，再次扫描并记录完成结果。

云安全管理平台针对应用层Web漏洞,提供应用层安全检测。漏洞扫描主要依靠带有安全漏洞知识库的网络安全扫描工具对信息资产进行基于安全扫描，能够全面反映主机系统、网络设备、应用系统所存在的网络安全问题和面临的网络安全威胁。云安全管理平台中Web漏洞扫描器通过在部署在交换机的镜像监听端口，完整记录下Web应用攻击行为，具备漏洞感知、入侵检测和全流量镜像存储三个主要功能。

针对We你防护主要通过本地防御虚拟集群，即使在云平台中划分部分虚拟机资源，并将这些虚拟机资源集群化处理，部署web防护软件，将该区域划分为公有云内部的web安全防护中心。所有公有云上的网站可自行选择是否需要使用，如需使用，则需修改DNS（CNAME）指向到web安全防护中心。Web安全防护中心提供DDoS防护、CC防护、漏洞攻击防护、SQL注入防护、流量负载均衡等功能。当公有云内部的web安全防护中心不足以应对大规模DDoS攻击时，可自动切换至外部云端防护。本地防御虚拟集群业务流程示意如下：

### 数据层安全监测与防护

#### 镜像安全监测与防护

多数云主机由镜像生成，所以镜像安全至关重要，如果镜像出安全问题，会导致创建云主机都有安全风险。通过云安全平台，主要对镜像源进行安全检测，由运维人员下发定时扫描或实时检测任务，云安全管理平台对镜像漏洞合规检测。镜像发布监测包括记录所有云平台镜像发布的信息，包括发布者,发布时间,镜像信息等。系统审计所有的镜像发布行为，防止未授权的镜像发布和发布不安全的镜像。

# 产品优势

## 先进的云安全理念

产品完美诠释了先进的设计理念：

* 一个核心安全理念：

“数据驱动安全”，提升安全能力

* 两大创新：

体系创新： “动态安全闭环运营体系”“云管端”安全防护体系

技术创新：大数据安全分析、威胁情报，等

* 三大突破：

建立及时减损的安全运营体系

深化和延伸“纵深防御”体系

建立基于“威胁情报”的全新监测体系

* 四大转变：

从传统合规安全转变到“及时减损+合规”

从传统注重“网络和系统”的防护转变中心到“业务+数据”的保护

从基于设备的对抗转变到基于“人的智力”的对抗

从被动安全响应向主动安全管控的转变

* 五大提升：

提升信息安全风险管控能力

提升信息安全技术水平

提升信息安全防御能力

提升信息安全监测感知水平

提升信息安全可看见能力

## 全日志审计系统

云安全管理平台对云环境进行了全面的审计日志记录，通过这些审计日志能够对网络通信行为进行还原，以供安全人员进行取证分析。

可提供至少6个月的日志数据实时查询，流量日志至少应包括：TCP会话记录、Web访问记录、SQL访问记录、DNS解析记录、文件传输行为、LDAP登录行为；

## 大数据分析审计引擎

能够对至少3个月的日志数据检索具备秒级查询速度，可对TB级日志做到快速搜索，搜索时间小于30s；具有APT攻击溯源能力，过去半年中公开发布过业界知名 APT攻击分析报告（例如：海莲花）。可以对记录数据的全部字段进行全文检索。

## 自动化的攻击感知系统

通过部署轻量化的Agent(探针程序)检测目标操作系统的关键行为，准确的判断云中可能出现的攻击行为，具体感知情况如下：通过部署Agent监测服务器的网站程序异常变更，通过自动化审计相关访问日志及文件准确判断服务器是否被上传webshell(网页后门)，自动通告管理员进行下一步的安全分析或安全处置工作。

通过部署Agent记录服务器的shell命令行操作感知系统是否被成功入侵，自动通告管理员在安全运营中心针对可以服务器发起分析或安全处置工作。

## 可视化安全监测系统

通过云安全管理平台收集的审计日志，结云平台的资产情况以及外部的威胁情报输入，通过可视化的形态直观呈现云平台的威胁安全态势，对云平台的整体安全进行实时展示。

# 总结

通过360云安全管理平台的建设，达到以下实施效果：

通过可视化监测系统可以直观的了解云平台遭受的安全威胁以及正在发生的安全现状。

通过大数据运营可以预知并防范安全威胁，真正做到“预防为主”的安全建设。同时可以提高对未知威胁的抵御能力，建设成与安全运营相结合的信息安全应急保障工作体系。

可以提高安全事件分析的反应速度与效率。并且可以为安全事件发生后的事后处理提供更加强大的追踪溯源基础。

通过威胁情报与全日志检索，可以发现如“海莲花”的APT级攻击。使网络对于APT有一定的发现与防御能力。