云数据中心安全解决方案

www.huawei.com

HUAWEI

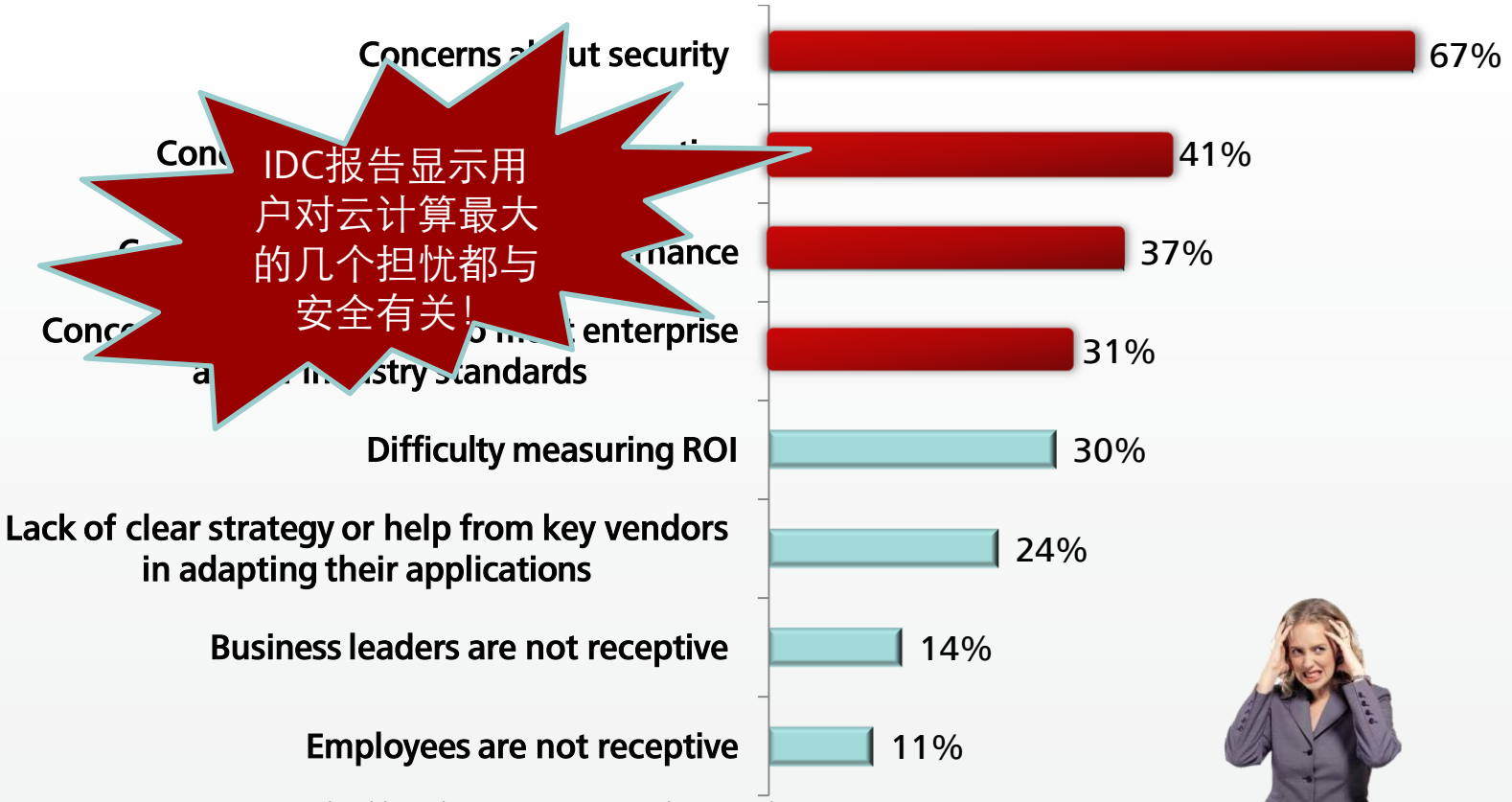
课程描述与目标

- 这门课程将会介绍数据中心安全解决方案的相关内容，面向已经完成数据中心课程的学员，课程内容包括应用安全，主机安全，网络安全，虚拟化安全，数据安全，物理设施安全，用户管理，安全管理等9个模块。
- 学完本课程后，您应该能：
  - 了解云计算技术之下数据中心安全的特殊要求
  - 了解数据中心安全解决方案子模块的特性，规格，主要设备

目 录

HUAWEI

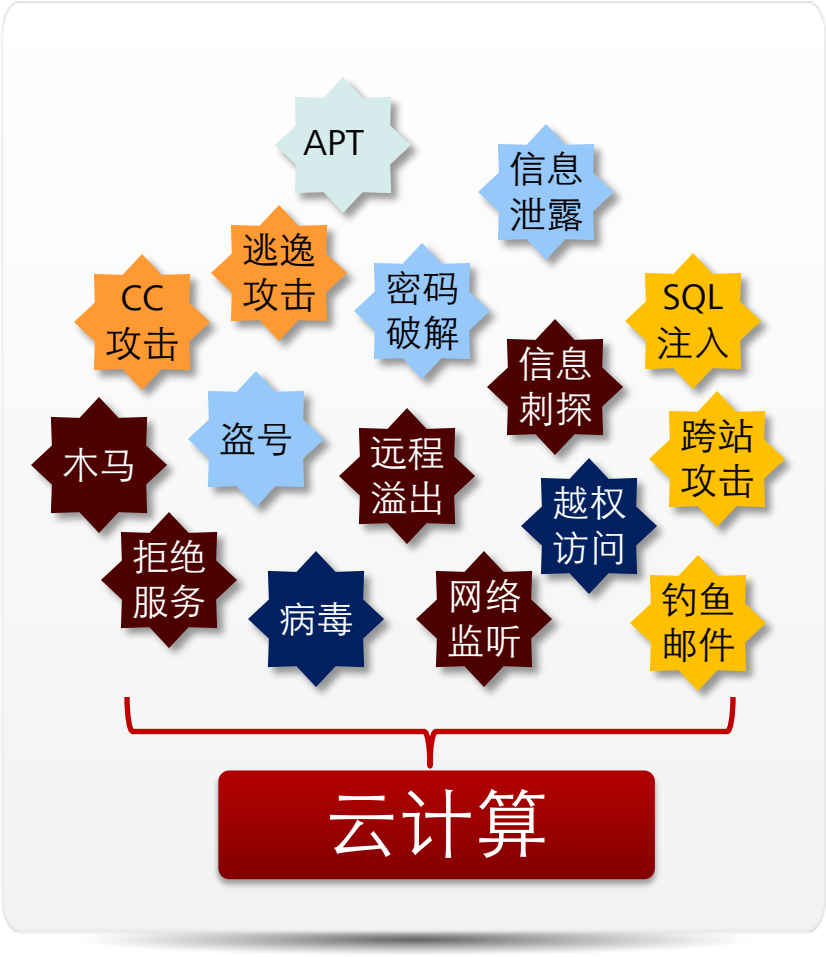
安全是云计算最大的担忧



Source: 2010 IDG Enterprise Cloud-based Computing Research, November 2010

云计算大潮已经到来，安全问题成为云计算发展的焦点

传统安全威胁在云计算下同样存在



◆应用威胁

SQL注入、跨站等针对应用层的攻击已经成为安全最大的威胁。

◆主机威胁

病毒蠕虫等将占用系统资源、破坏文件和数据。恶意用户也会利用本地漏洞和配置错误来获取额外权限。

◆数据安全

破坏数据的机密性、完整性和可用性。

◆网络威胁

针对网络层的攻击组要有拒绝服务、远程溢出、信息探测、网络监听等。

云计算环境下还存在新的威胁

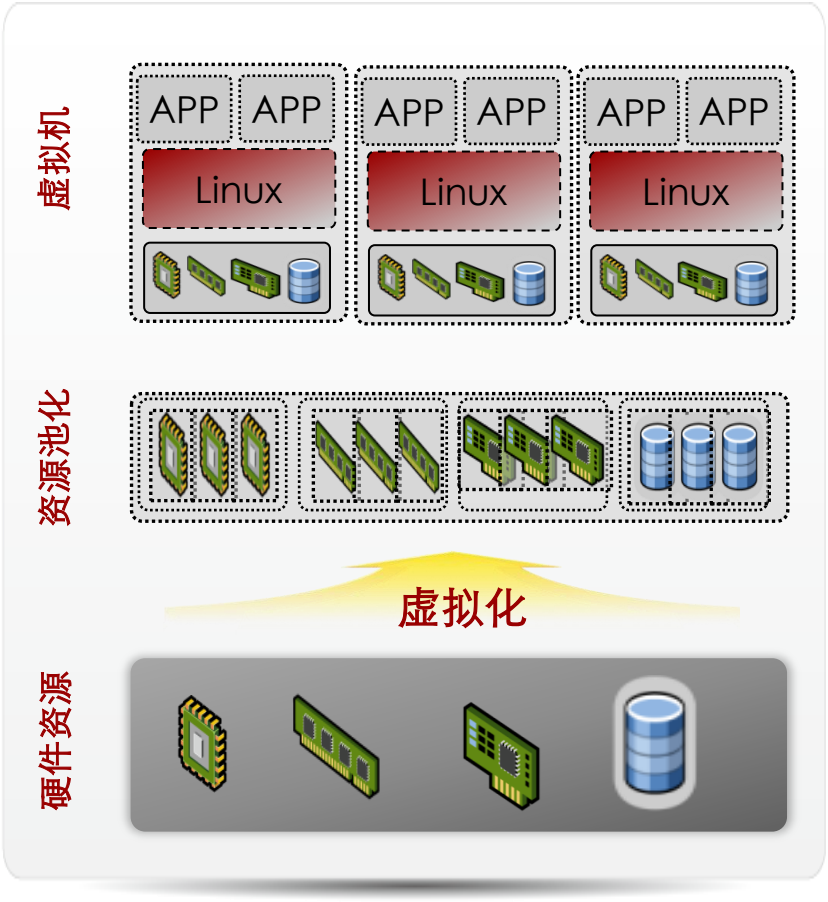
◆虚拟化平台引入新的威胁：
虚拟化平台运行在操作系统与物理设备之间，其设计和实现中出现的漏洞，将成为新的威胁。

◆多租户安全威胁：
不同安全需求的租户可能运行在同一台物理机上，传统安全措施难以处理这种情况。

◆特权用户问题：
应用系统和资源所有权的分离，导致云平台管理员可能访问用户数据，从而对数据机密性、完整性、可用性造成破坏。

除传统威胁外，虚拟化、多租户和特权用户问题使得云计算面临更大风险！

云计算面临的新威胁-虚拟化安全威胁



◆ **Hypervisor及管理系统会引入新的威胁**

在CVE的数据库中，虚拟化软件的漏洞累计超过超过700条，其中主要是vmware系统的。

◆ **Hypervisor层的漏洞将影响所有的虚拟机**

作为虚拟机的底层系统，一旦存在漏洞，将危及运行其上的所有虚拟机。

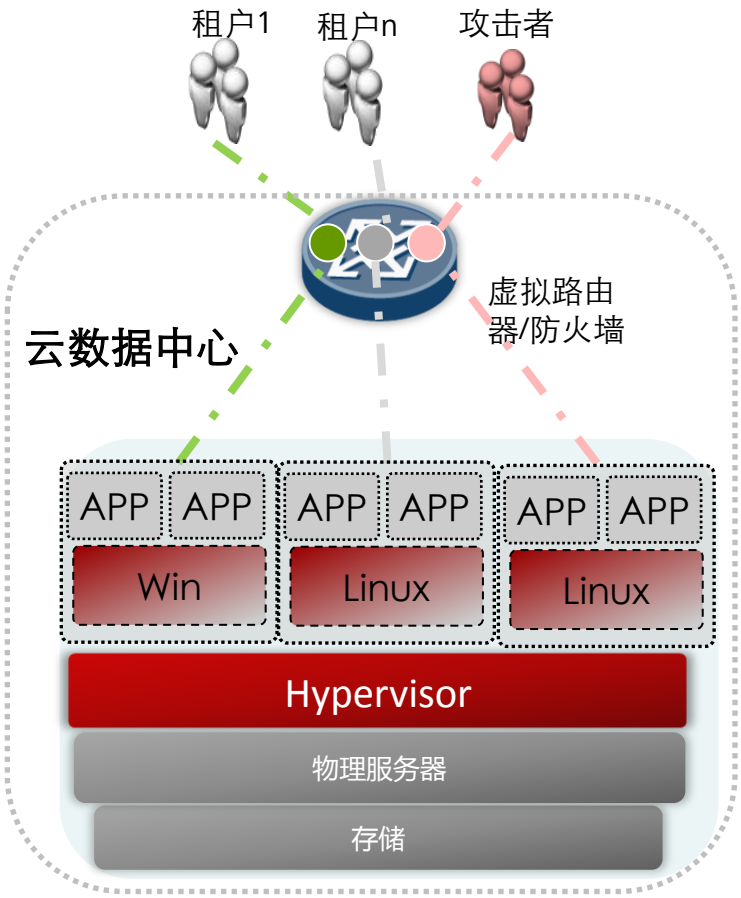
◆**网络虚拟化安全威胁**

- 同一物理机机上不同虚拟机之间的流量对传统网络安全设备不可见；
- 安全策略无法随网络调整而动态迁移。

◆**虚拟机镜像被修改的风险**

虚拟机镜像在休眠时是数据文件形式存储的，有被修改的风险。

云计算面临的新威胁-多租户安全威胁



◆网络边界模糊

不同的租户应用运行在同一物理机上，使网络的物理边界消失，只存在逻辑的边界。

◆恶意租户威胁

恶意用户可以付费获得对虚拟机访问的权限，从而可以利用漏洞对Hypervisor或其它虚拟机进行攻击。

◆数据重用风险

磁盘释放给其他租户使用，原有数据未被彻底清除的话，可能被新用租户获取。

云计算面临的新威胁 - 特权用户问题

◆云计算特权用户也可以访问数据

云计算环境下，除了租户访问自己的数据外，云管理员由于需要对资源进行管理，因此也可以接触数据，从而可能造成数据泄露、损坏或被修改。

◆可能存在多个特权用户

SaaS提供商可能会利用其它PaaS、IaaS的服务，因此可能会有多个特权用户。

问 题

- 云计算面临的新安全威胁有哪些?
- 简述云计算面临的传统威胁有哪些?

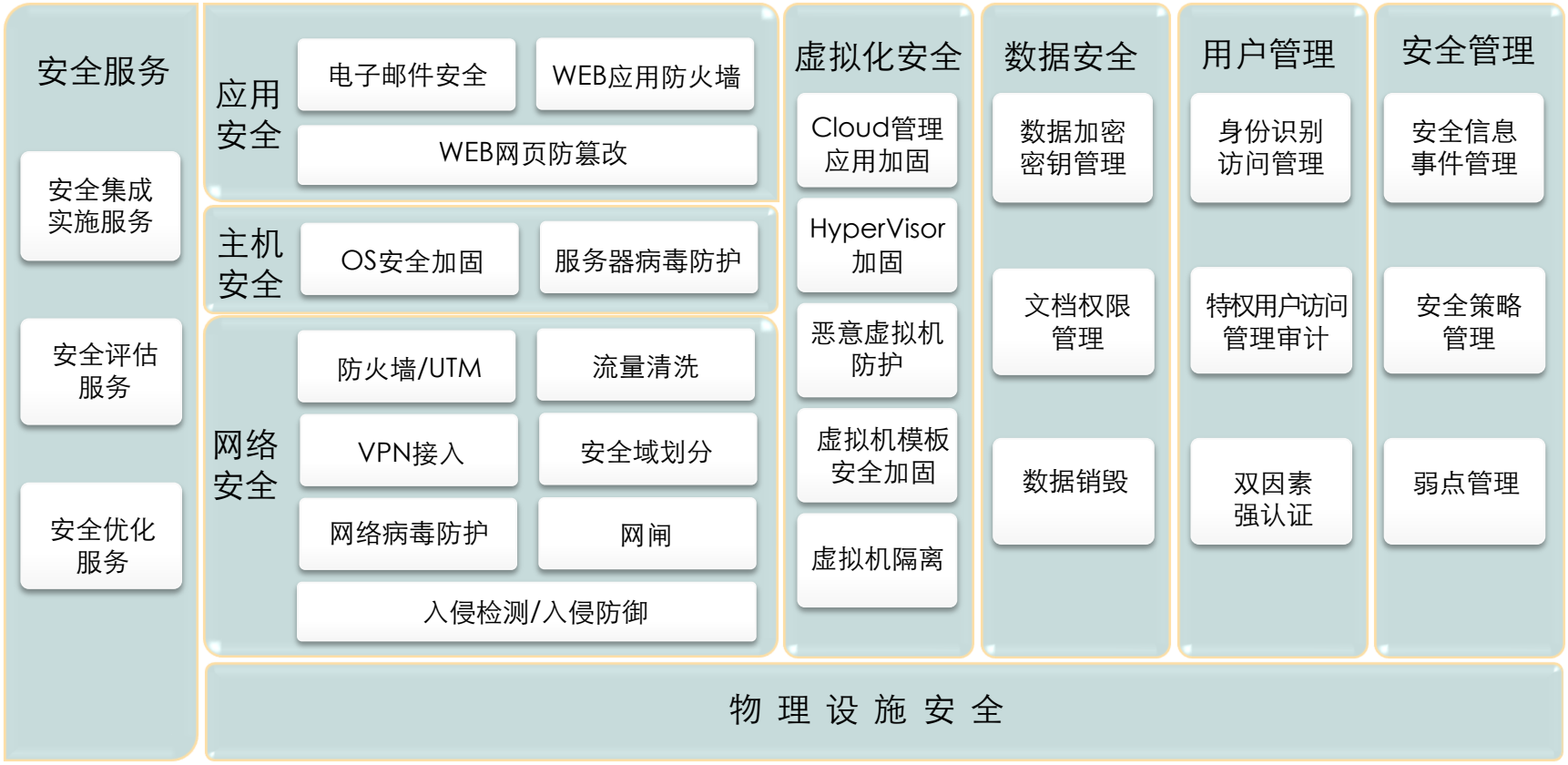
总 结

- 本章主要介绍云计算面临的威胁，包含传统威胁和云计算带来的新威胁。

目 录

HUAWEI

华为云数据中心安全解决方案框架

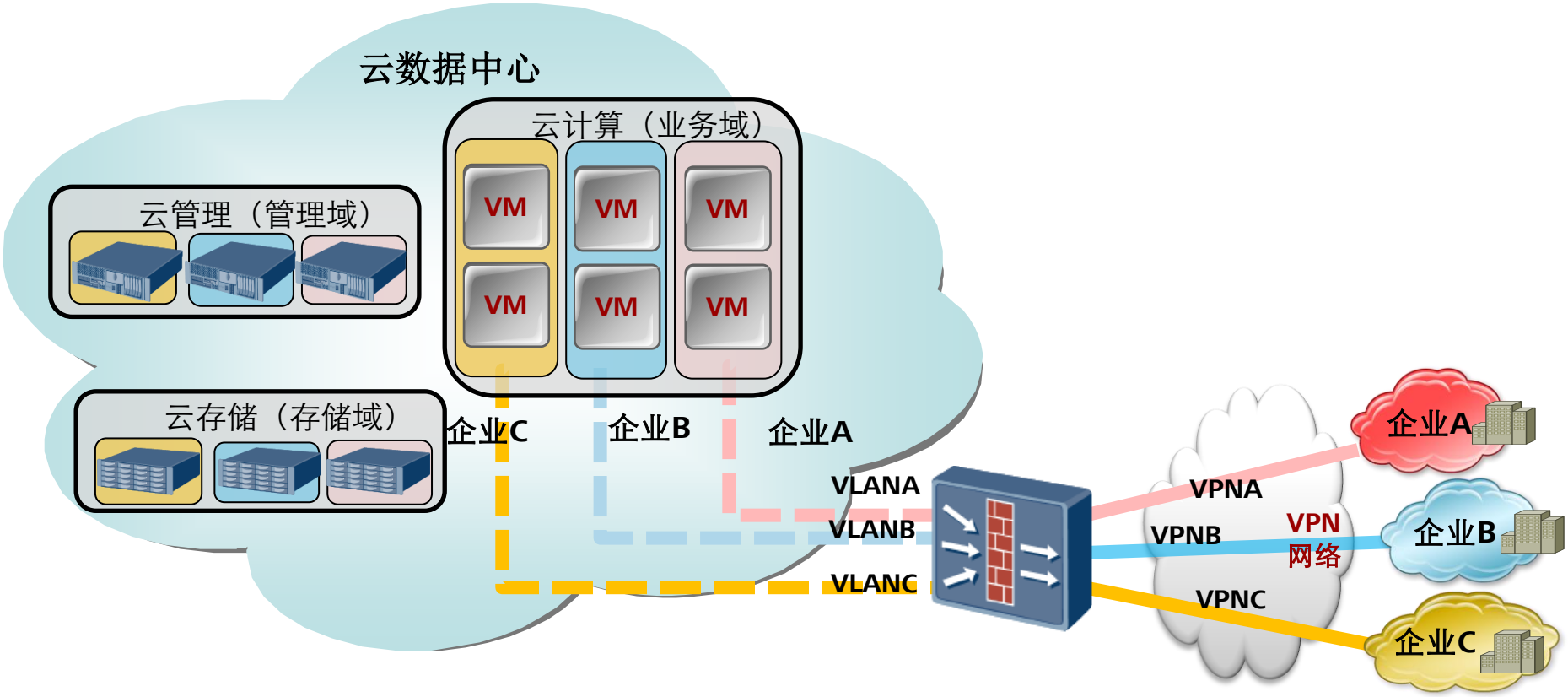


针对云计算数据中心面临的各种威胁，华为提出了全面安全解决方案框架

网络安全

安全域划分	安全域的划分从规划和设计上将不同用户的不同安全等级要求网络进行划分，为部署和实施隔离措施提供了依据。
防火墙	在网络边界对网络进行隔离和访问控制。
流量清洗	对DDoS等恶意流量进行清洗，保护网络的可用性。
VPN接入	通过传输加密措施，保护数据传输的机密性、完整性。
入侵检测与防御	对网络上的攻击行为进行实施检测、防御并响应。
网络防病毒	在网络上对病毒进行拦截。
网闸	实现不同安全等级网络间的隔离。

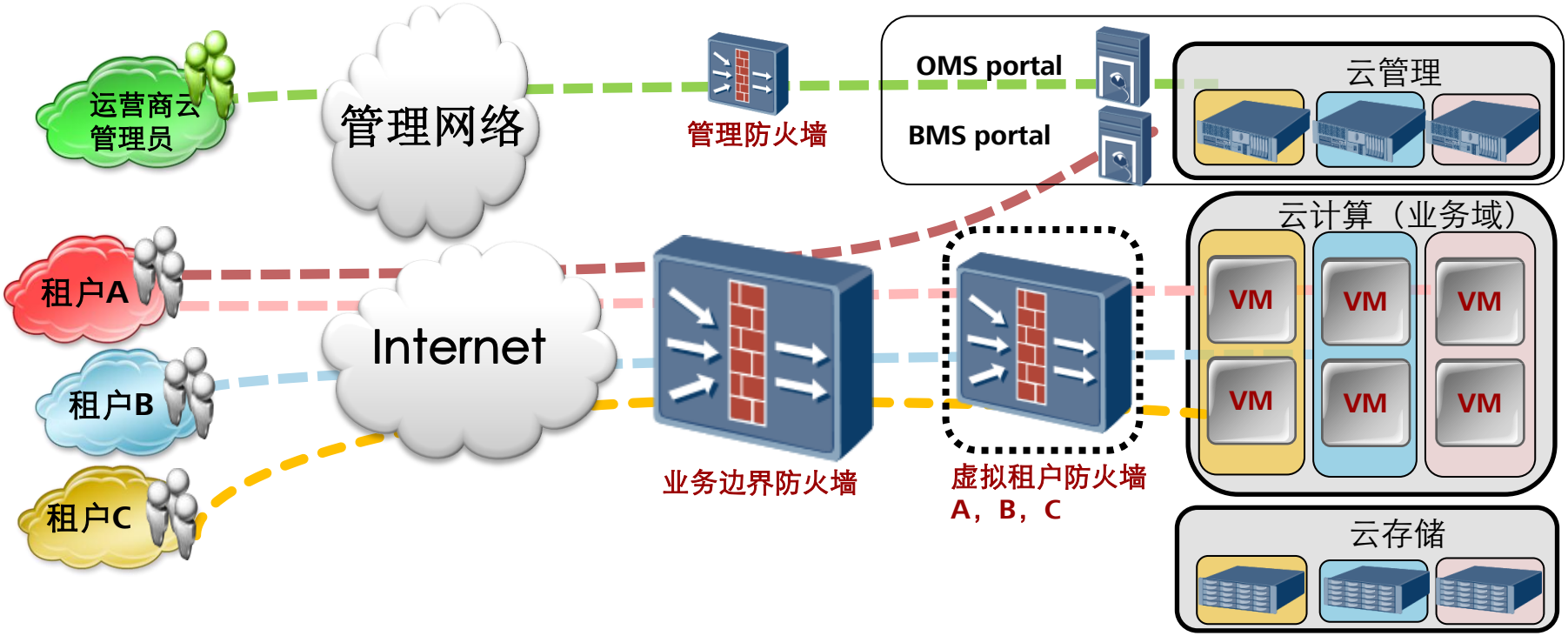
网络安全-安全域划分



◆根据业务情况和服务类型进行安全域划分

- 根据安全要求等级及服务类型等因素进行安全域划分；
- 采用防火墙、网闸、虚拟机安全组、IPS等产品实现不同安全域的隔离和访问控制。

网络安全-防火墙



◆管理防火墙

部署在数据中心云管理设备和云管理网络边界，完成两者之间的隔离和防护，是运营商的基础设施。

◆业务防火墙

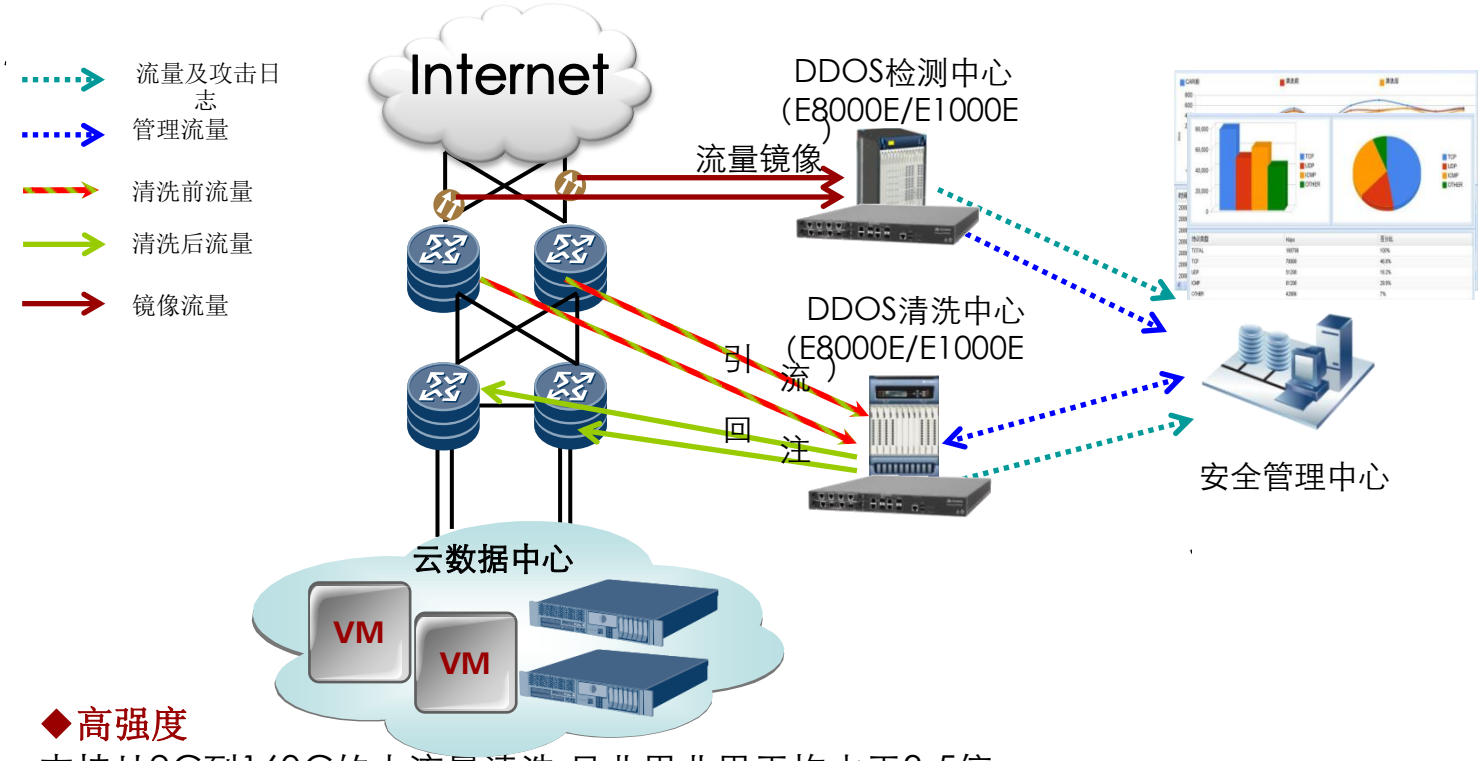
部署在数据中心和外网(如Internet)的边界，完成两者之间的隔离和防护，是运营商的基础设施。

◆虚拟防火墙

部署在企业出租虚拟机的边界，主要租赁给企业完成各个租户网络和外部网络的隔离和防护，企业根据自己的策略定制防火墙规则。

HUAWEI

网络安全-流量清洗



◆高强度

支持从2G到160G的大流量清洗,是业界业界平均水平3-5倍。

◆高精度

- 有效识别流量型攻击、应用型攻击、扫描窥测型攻击和畸形包攻击等类型；
- 支持小流量应用层攻击防范/支持低速攻击防范。

◆灵活部署

可直路、旁路、集中式、分布式部署。

◆系列化

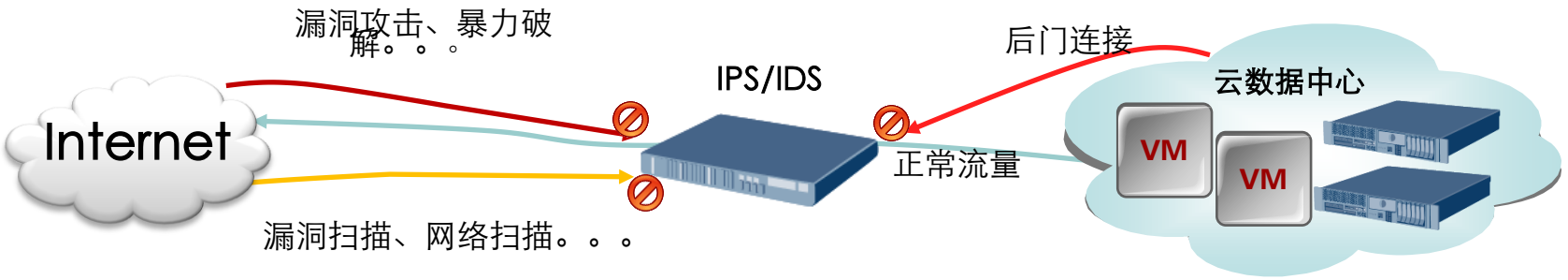
针对不同的数据中心规模，用不同的产品组合。

网络安全-VPN接入

◆数据中心传输安全由以下几个方面保证：

- 管理面信任域与非信任域之间全部SSL加密；
- 用户管理接入支持HTTPS，安全性要求高的提供SSL VPN接入用户访问虚拟机支持SSH。

网络安全- 入侵检测与防御



◆实时检测与拦截网络攻击

对网络流量进行实时检测，拦截各种网络攻击及维护网络安全的行为。

◆产生报警并提供统计分析数据

对攻击行为产生实时报警，并存储历史报警数据，通过统计历史数据进行统计分析，提供各种维度的数据报表，供决策使用。

网络安全-网络防病毒

◆在网络上拦截病毒

•无需占用主机系统资源；

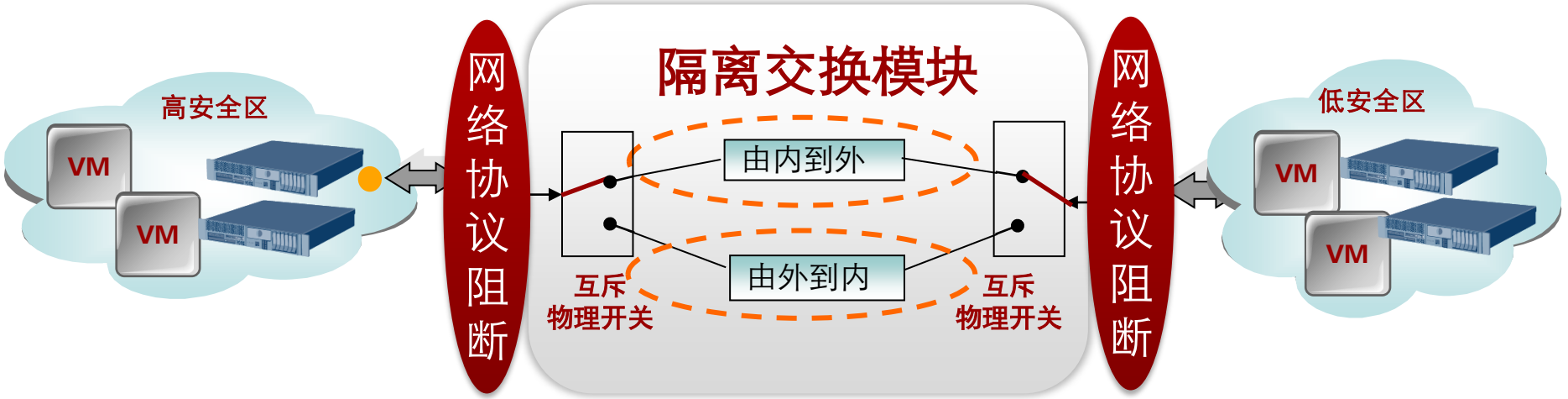
•只需要网络防病毒设备升级即可保护所有主机。

◆与主机防病毒产品异构

利用不同厂家各自对病毒研究能力的不同和反应速度，可提高病毒的识别率和病毒库更新速度。

HUAWEI

网络安全-网闸



◆网闸实现不同等级网络的安全隔离

数据只能以专有数据块方式静态地在两个网络间进行“摆渡”，从而切断了不同安全等级网络之间的所有直接连接，保证数据能够安全、可靠地交换。

主机安全

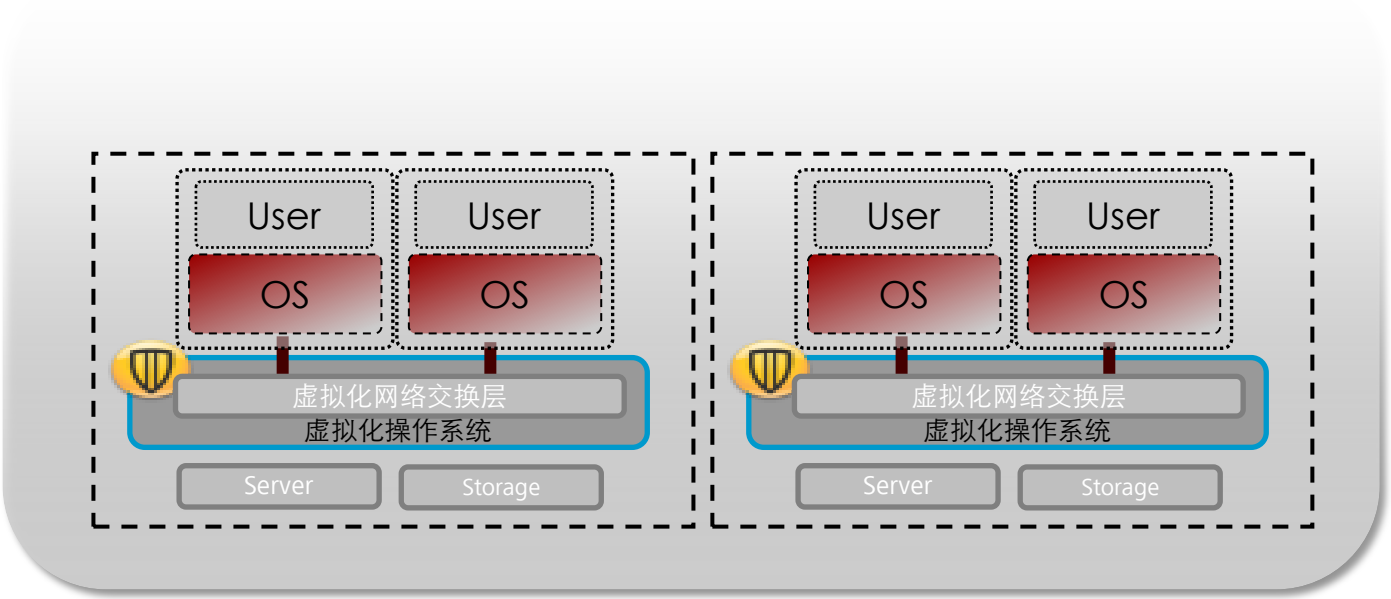
主机恶意软件防护

- 如病毒、蠕虫、特洛伊、间谍软件、恶意软件、零日威胁和rootkit等。
- 同一个VLAN的虚拟主机网络可达，当一个虚拟主机感染了恶意程序后，会对同一个VLAN内的主机进行攻击。

主机安全系统加固

默认安装的操作系统存在无用的服务、未考虑安全防护的默认配置。

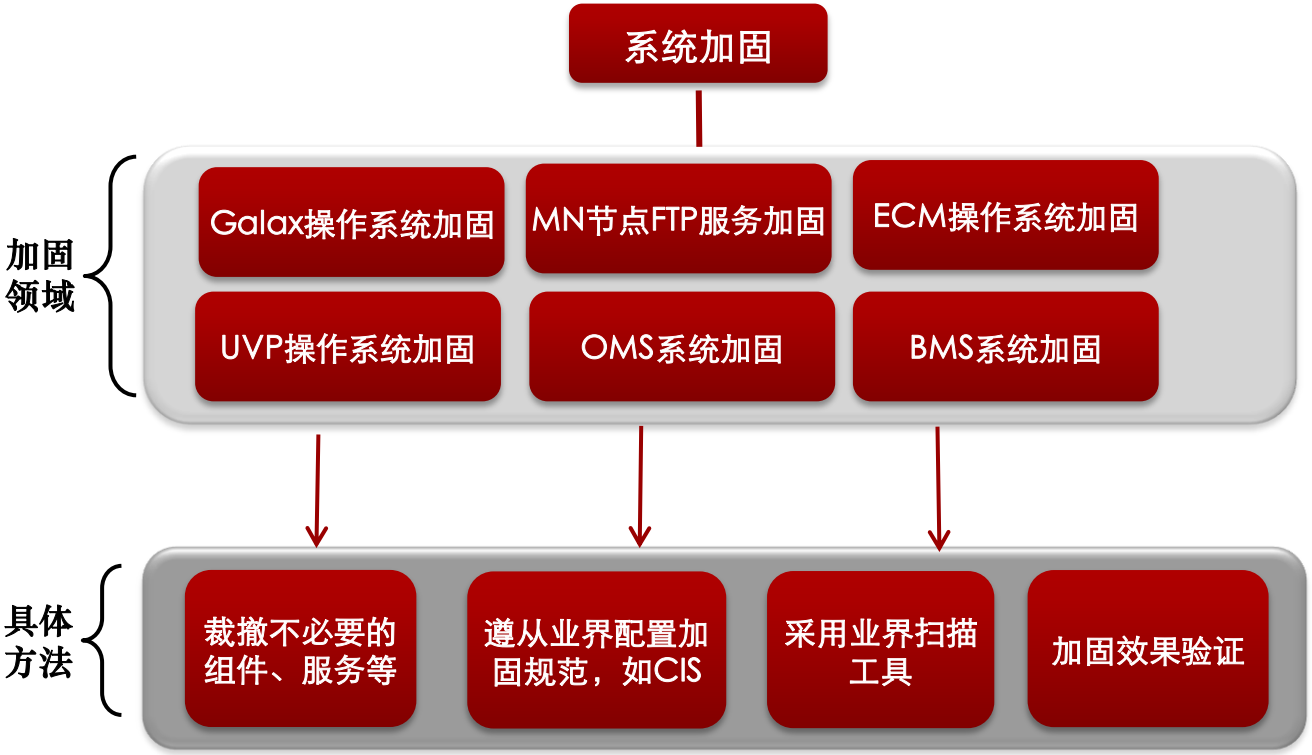
主机安全- 病毒防护



◆针对Host操作系统进行优化

- Host操作系统病毒防护，能够对病毒、蠕虫、特洛伊木马、间谍软件、恶意软件、零日威胁和rootkit等提供安全防护；
- 简单集中管理。

主机安全- 系统加固



◆通过合理配置相应系统参数、降低程序运行权限等手段，达到增强系统安全能力的目的，保护租户的业务数据和资产安全。

应用安全

WAF

Web应用防火墙可提供专门针对Web服务器及应用系统相关的防护，防止针对web应用的各种攻击。

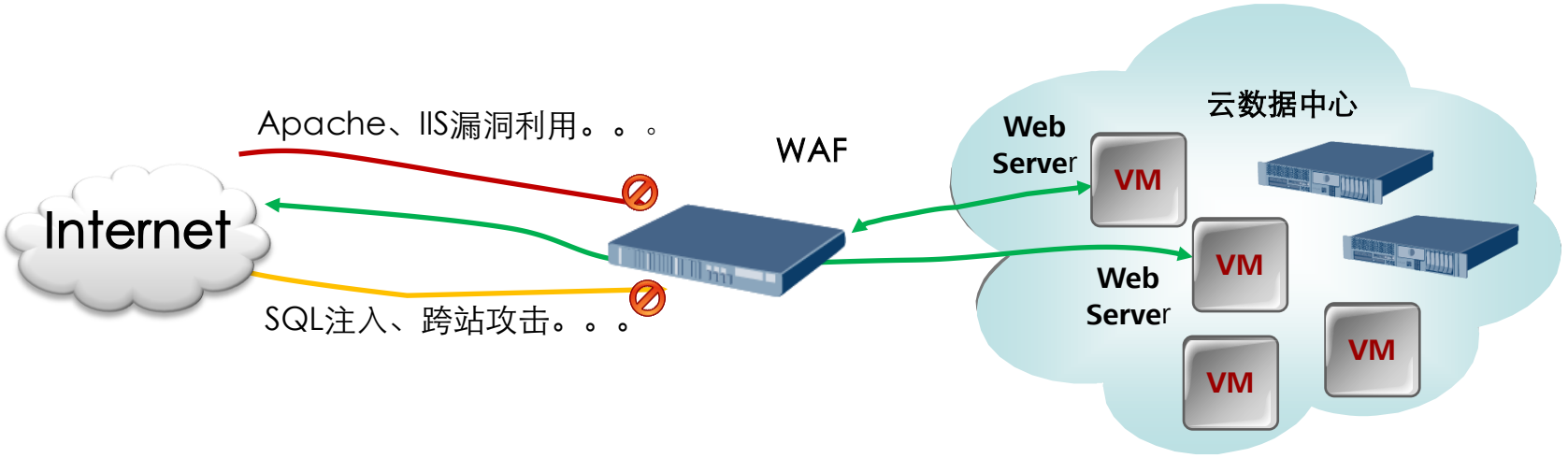
邮件安全

邮件是最主要的办公应用系统，大量的垃圾邮件不仅占用系统资源，还会降低员工工作效率，钓鱼邮件和带病毒、后门等的恶意邮件更会对系统安全造成威胁。

网页防篡改

Web化的业务系统不仅是信息发布的渠道，更是业务的入口，网页防篡改系统在网页遭非授权修改时进行恢复。

应用安全 – Web应用防火墙



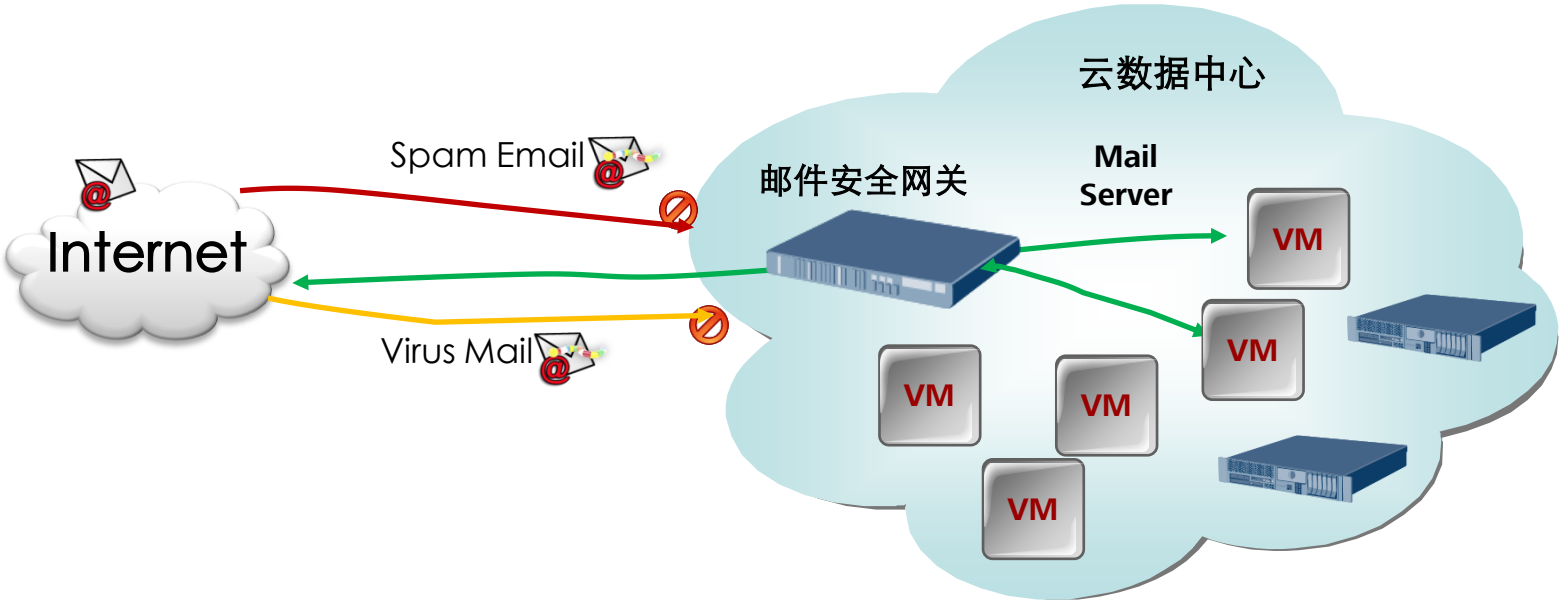
◆防御针对Web系统的攻击

保护Web Server及应用程序，阻断针对Web Server的漏洞和配置错误的攻击，阻断SQL注入、XSS攻击等针对应用程序的攻击。

◆提供SSL加解密、负载均衡、应用加速等能力

专门针对Web Server提供一系列的能力提高可交付性。

应用安全-邮件安全



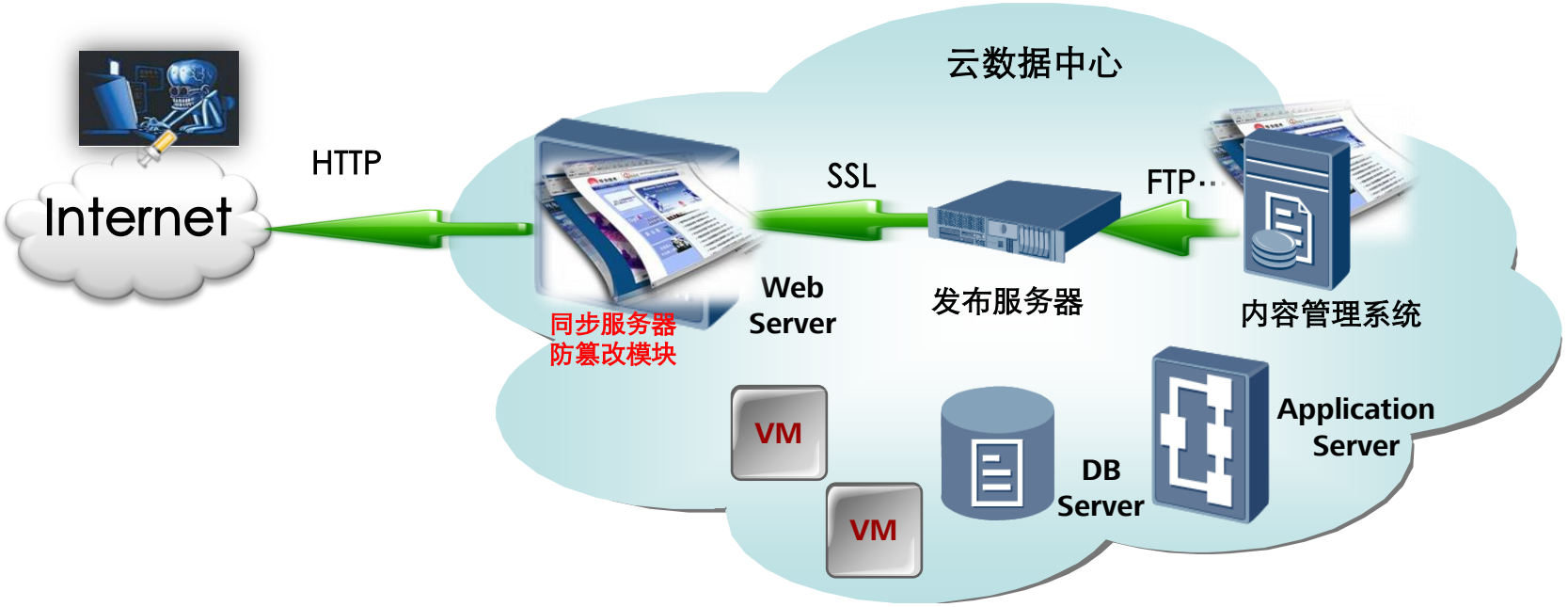
◆垃圾邮件防护

利用信誉库、统计分析、黑白名单等方式阻止垃圾邮件进入收件箱，防止欺骗、钓鱼邮件等影响系统及用户。

◆提供客户自定义能力

用户可自行根据自身情况（邮件流量等）进行设置，阻止威胁，防止针对目录收割攻击（DHA）和邮件退信攻击等。

应用安全-网页防篡改



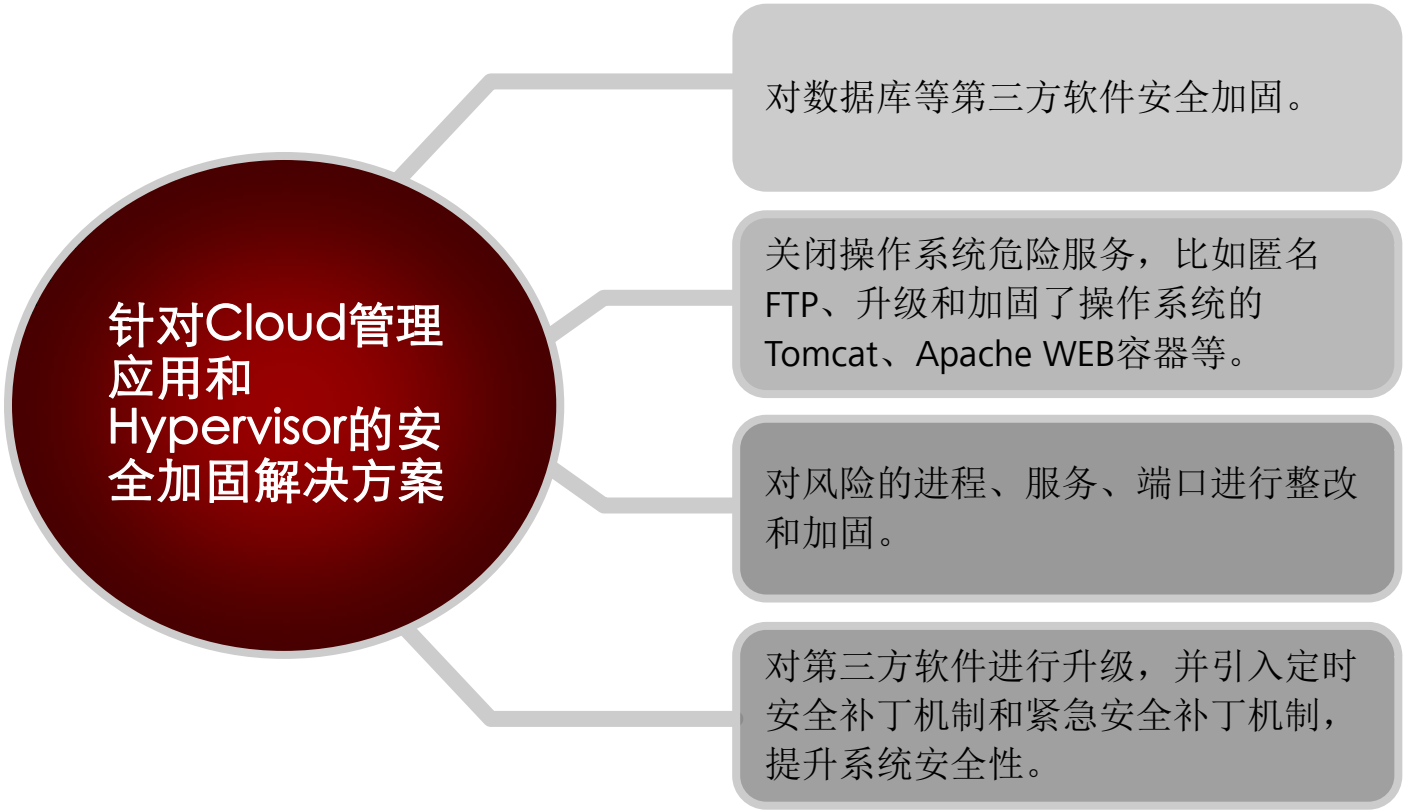
- ◆网页防篡改系统运行在web服务器上，监测网页状态。
- ◆网页被修改时，启动恢复机制。
- ◆结合发布服务器来完成合法的网页内容更新。

HUAWEI

虚拟化安全

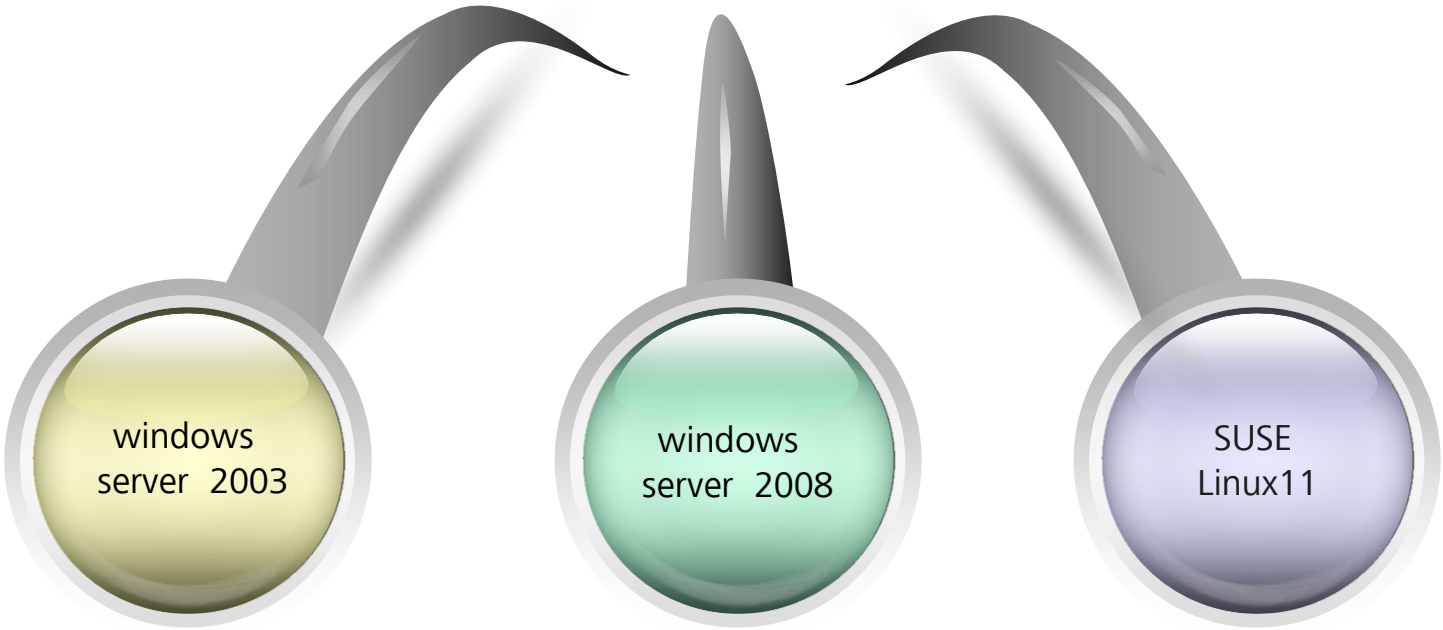
云平台安全加固	提供针对Cloud管理应用和HyperVisor的安全加固解决方案。
虚拟机模板加固	提供基于业界最佳实践的云主机加固模板。
恶意虚拟机防护	提供基于虚拟机的IPS解决方案，弥补了传统网络层入侵检测和入侵防御措施的不足，及时发现入侵威胁，并进行有效处理。
安全隔离	有完善的虚拟机隔离机制，同时，提供虚拟安全组解决方案， 满足租户为确保对所租用的虚拟机自身的安全而进行安全隔离的需求 。

虚拟化安全-云平台安全加固

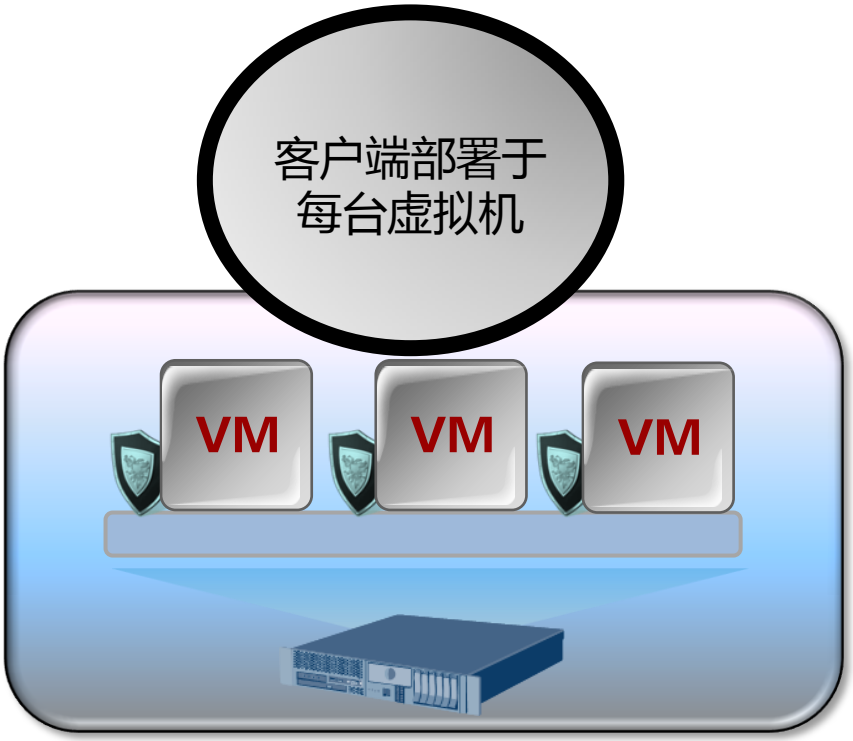


虚拟化安全-虚拟机加固模板

提供基于业界最佳实践的云主机加固模板，虚拟机加固模板支持多种操作系统



虚拟化安全-恶意虚拟机防护



◆主要安全防护

- 入侵探测/防御 (IDS/IPS)；
- 应用控制；
- 网络应用保护；
- 完好性监测。

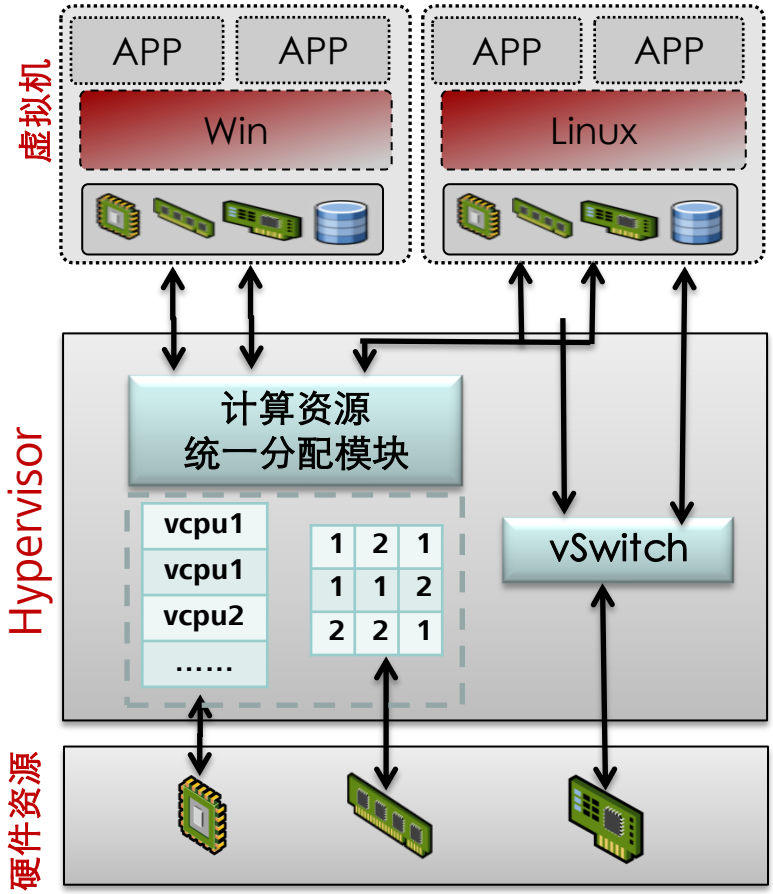
◆受保护的主机平台有

- Windows® 客户端平台 2000, XP, Vista；
- Windows® 服务器平台 2003, 2008；
- Linux RHEL 3,4,5, SUSE 9,10。

◆恶意虚拟机安全防护

通过基于虚拟机的IDS、IPS、完整性检测等深度安全防护技术，实现针对恶意虚拟机的有效防护。

虚拟化安全-虚拟机隔离



◆物理资源与虚拟资源的隔离

• Hypervisor统一管理物理硬件资源，保证每个虚拟机都能获得相对独立的资源；

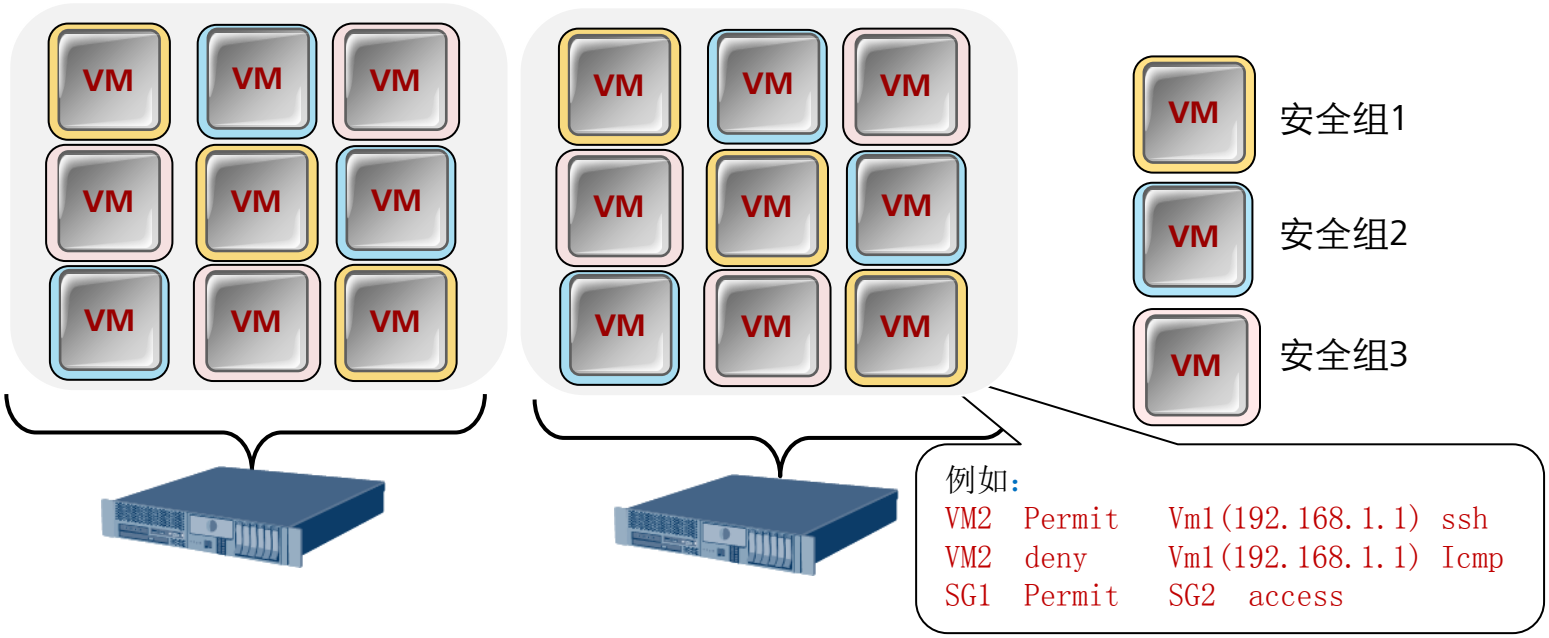
• 屏蔽虚拟资源故障，虚拟机崩溃不影响Hypervisor。

◆虚拟机之间的隔离

• Hypervisor从物理层面隔离虚拟机各类资源，使得虚拟机在整个生命周期内互不可见，避免虚拟机之间的数据窃取或恶意攻击；

• 支持定制每个虚拟机的资源配额，保证虚拟机的资源使用不受周边虚拟机的影响。

虚拟化安全-虚拟安全组



◆虚拟机实例可以动态地加入和退出安全组，实现虚拟机间的访问控制。

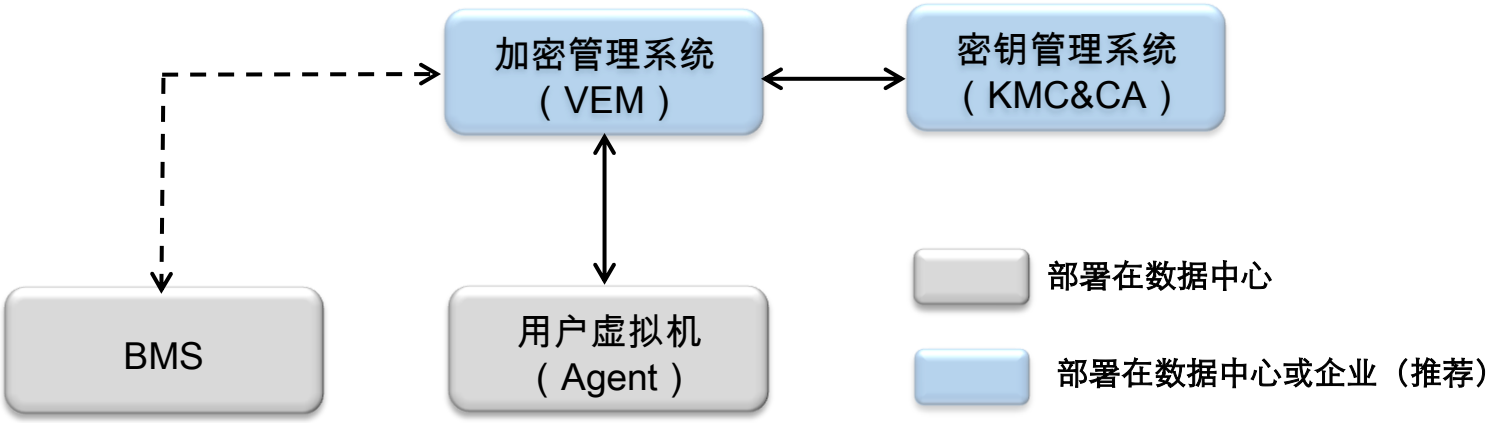
◆可以实现在同一个安全组的虚拟机之间、在不同安全组的虚拟机之间的访问控制。

◆安全组规则可以随虚拟机动态迁移。

数据安全

防止数据被窃取	提供虚拟机数据卷加密的解决方案，确保云主机上的数据机密性，防止被窃取。
文档权限管理	提供文档权限解决方案，确保不同权限的用户只能访问相应权限的文档。
数据销毁	提供数据销毁机制，防止用户敏感信息泄露。

数据安全-VM卷加密防止数据被窃取



◆ **VM卷加密系统由三部分组成：**

加密管理系统（VEM）、密钥管理系统（KMC&CA）、安装用户虚拟机的Agent。

◆ **Agent中过滤驱动实现了磁盘的透明加密。**

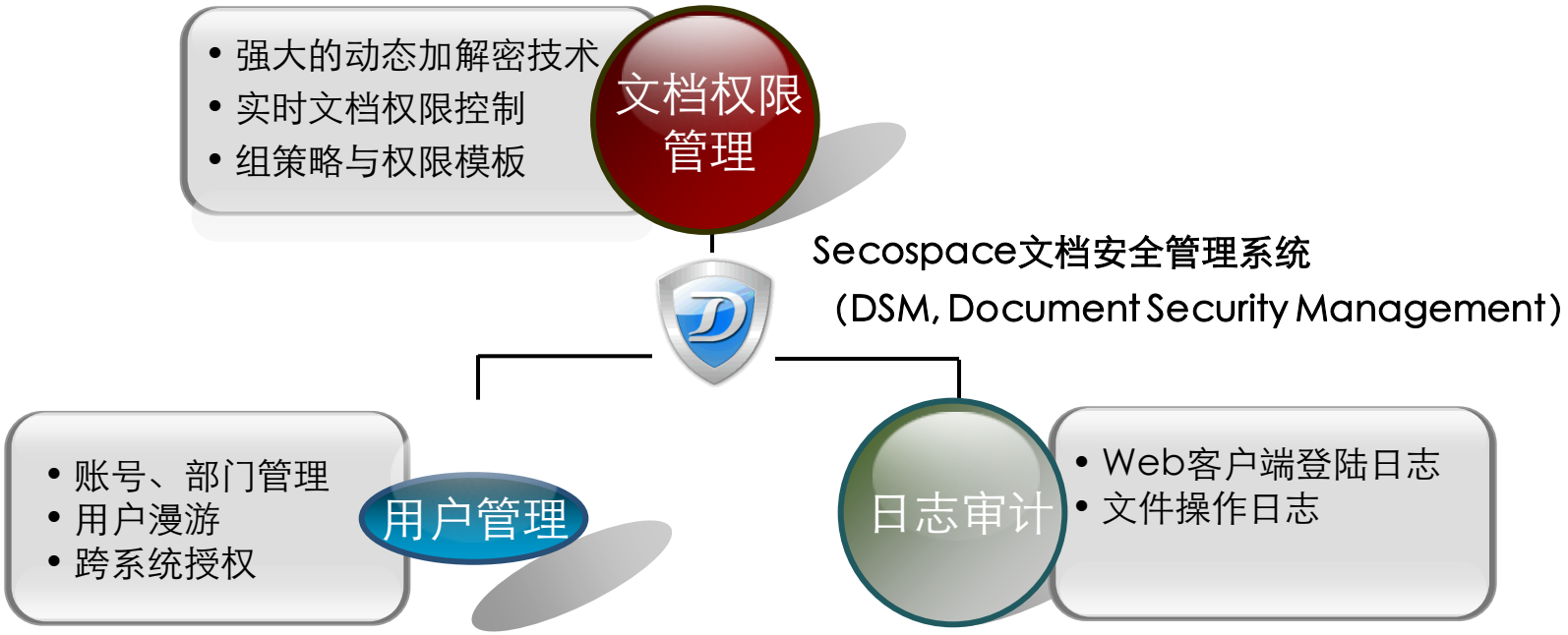
◆ **VEM负责加密虚拟机的管理**

包括开通/关闭加密服务、下发加密/解密指令、更新密钥、查看虚拟机加密状态等。另外， VEM负责从密钥管理系统给用户申请证书、更新证书、吊销证书、丢失证书后找回证书等。

◆**密钥管理系统负责用户证书的管理**

包括相应VEM的用户申请、更新、吊销、找回等操作。

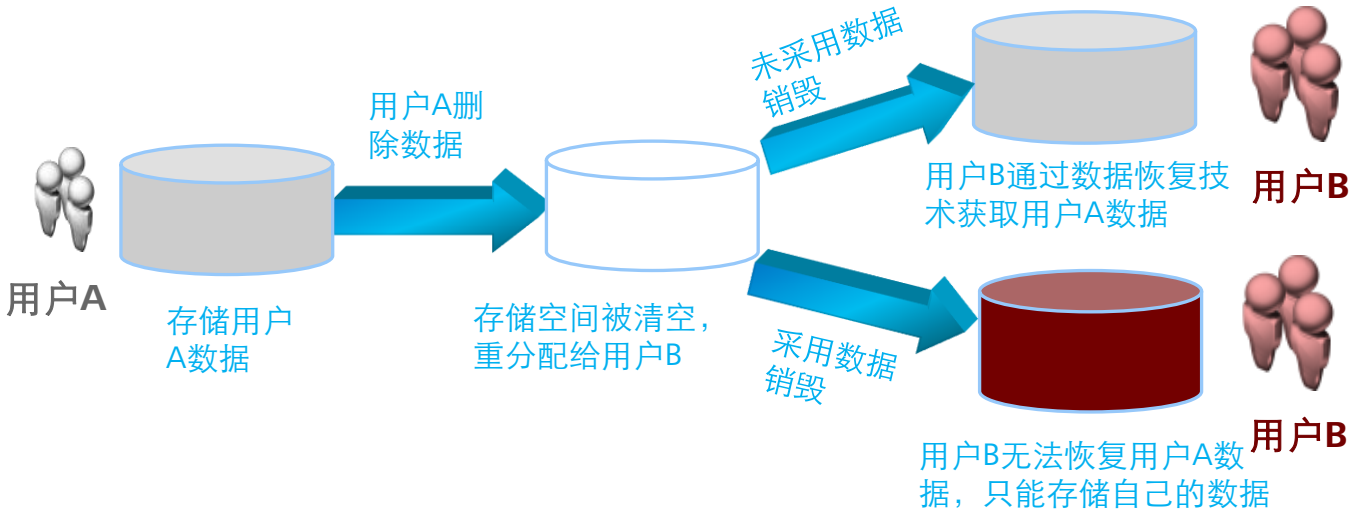
数据安全-文档管理安全



◆ **Secospace 文档安全管理助力企业构建安全可控的文档安全管理平台**

通过实时权限控制，提供安全授权下的机密信息共享，使信息所有者能够定义信息的访问者、访问方式和时间等，并记录文档操作日志。

数据安全-数据销毁



◆ **SingleCLOUD确保原用户敏感信息安全性**

完善的数据销毁机制，确保用户敏感数据（系统管理数据、用户鉴权数据、重要业务数据等敏感数据）所使用的存储空间在被重新分配给其他用户使用前要被彻底擦除。

用户管理

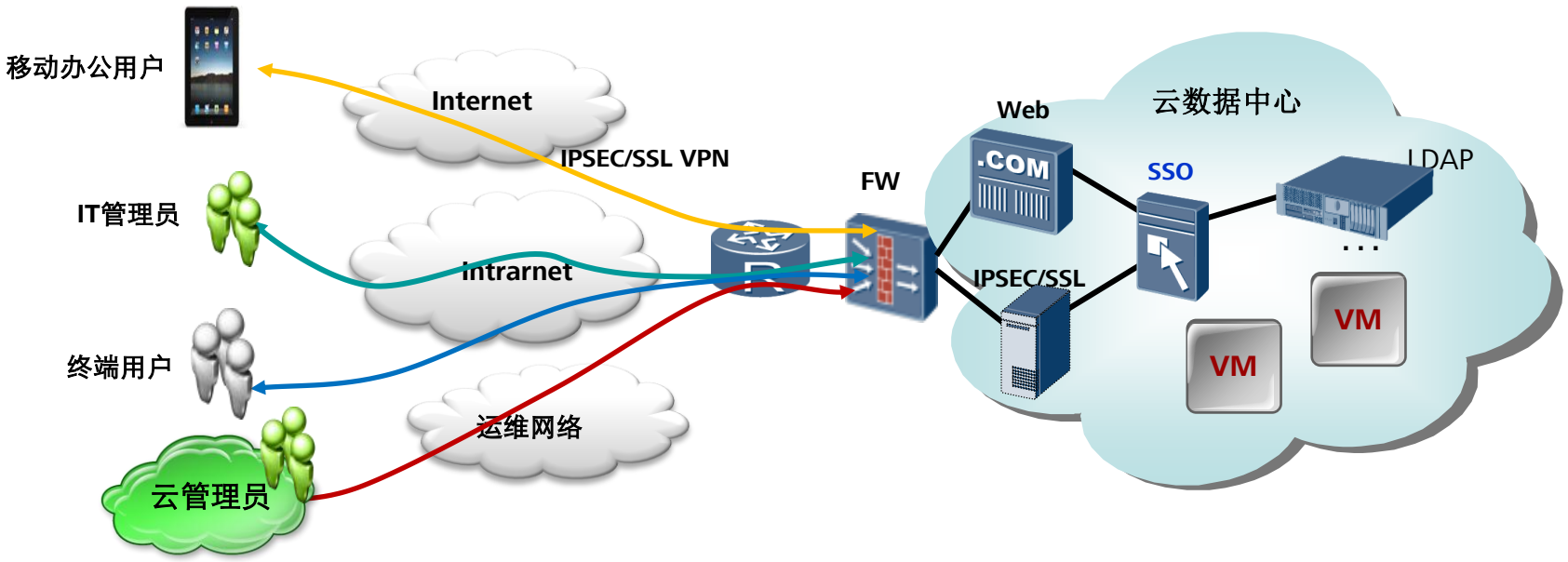
强认证与单点登录方案

结合数据中心众多业务系统，避免信息孤岛问题，同时结合双因子认证等方式避免口令泄漏导致系统遭受破坏。

运维账户分权分域管理

通过运维管理系统对用户运维操作进行分权分域控制，避免多个业务系统用户独立登录各个系统，解决了口令维护和易用性问题。

身份认证与管理-强认证与单点登录解决方案



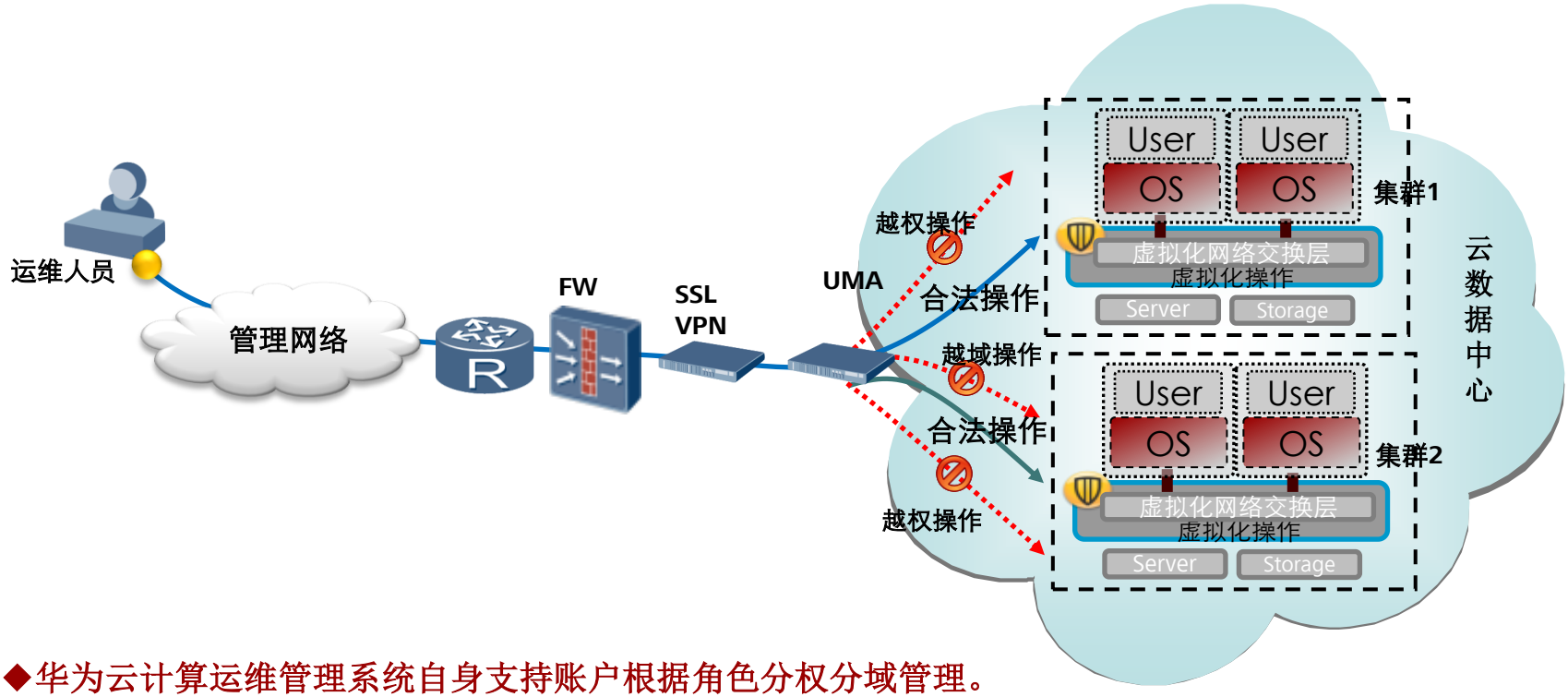
◆支持多种强认证方式

可支持各种强认证系统，如指纹认证、USB Key认证、动态密码认证;
良好的兼容性：可对接第三方认证系统，如微软AD、Novell NDS。

◆单点登录方式

可以给第三方SaaS系统提供身份认证服务，快速推出新的业务。

身份认证与管理-运维账户分权分域管理



◆华为云计算运维管理系统自身支持账户根据角色分权分域管理。

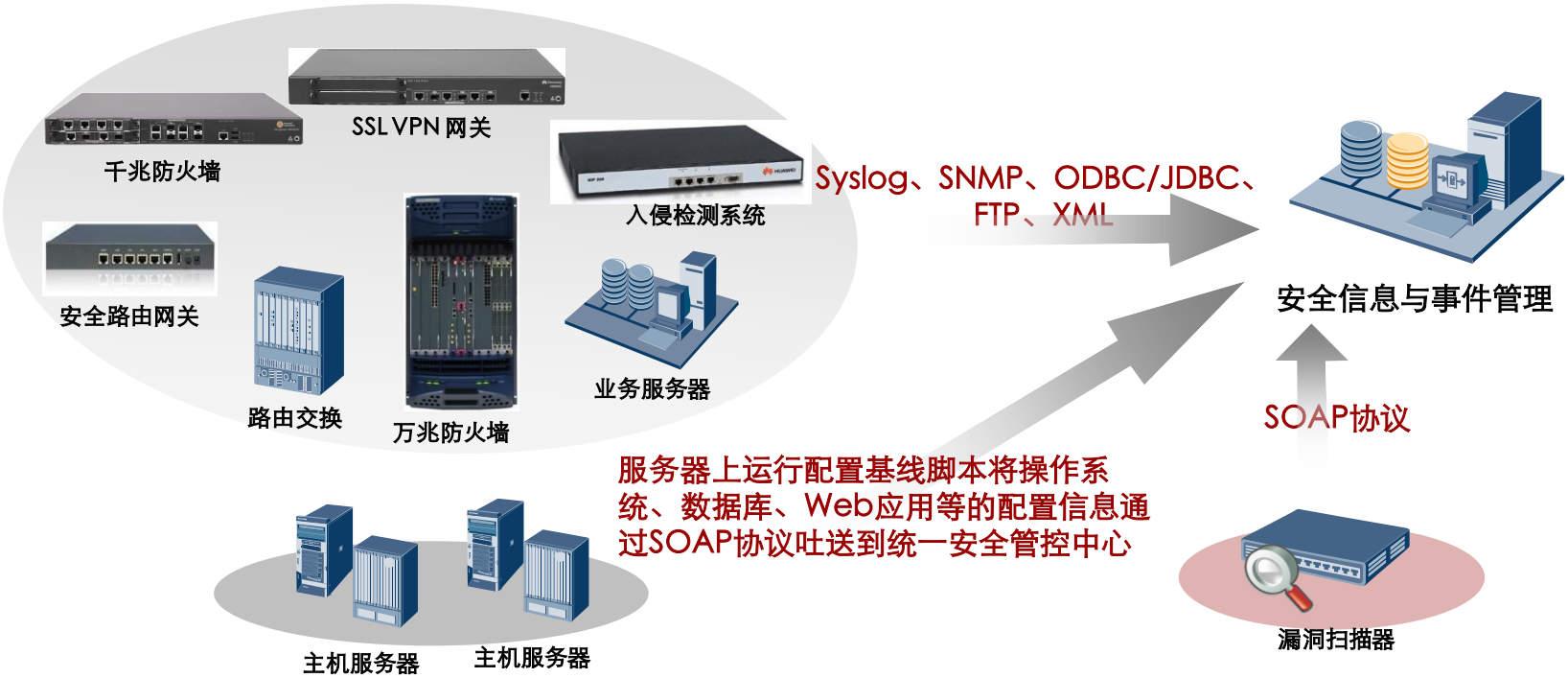
◆运维堡垒机结合SSL VPN提供更加安全的运维通道

SSL VPN提供远程访问通道安全，运维堡垒机提供运维权限管理，完善的日志审计功能，支持对图形终端、字符终端、数据库应用、文件传输等。 提供实时视频监控录屏，对高危的操作（删除或重启等）可以实时的截断。

安全管理

安全信息与事件管理	各种设备产生大量的日志信息需要进行同一管理和存储，并进行关联分析以发现可能的威胁。
安全策略管理	设备间的策略必须有一致性，并可统一管理。
弱点管理	需要提前了解系统中存在的弱点，在被恶意利用前进行修补。

安全管理-安全信息与事件管理



◆日志统一管理与关联分析

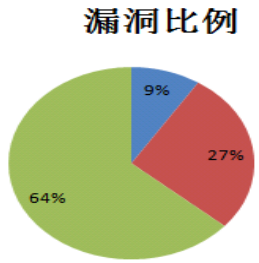
集中日志存储，提供统一的日志备份、管理，并对不同设备的日志进行关联分析，发现可能存在的攻击。

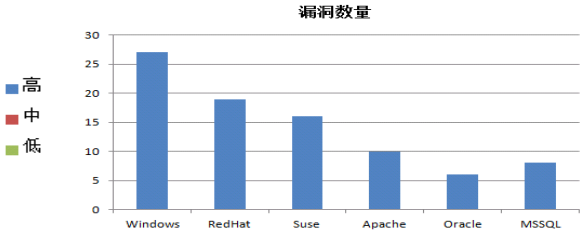
◆对合规提供支持

根据不同的合规要求提供报表模板，根据日志内容自动化分析合规满足程度。

安全管理-安全策略管理

安全管理-弱点管理





序号	IP地址	漏洞总数	高危险	中危险	低危险
1	192.168.13.1	1	0	0	1
2	192.168.13.2	4	0	1	3
3	192.168.13.3	81	10	22	49
4	192.168.13.4	2	0	0	2
5	192.168.13.5	0	0	0	0
6	192.168.13.6	19	0	4	15
7	192.168.13.7	2	0	0	2
8	192.168.13.8	0	0	0	0

◆漏洞扫描

主动探知数据中心中从网络到应用的各种漏洞，形成分析报表。

◆提供漏洞及补丁信息

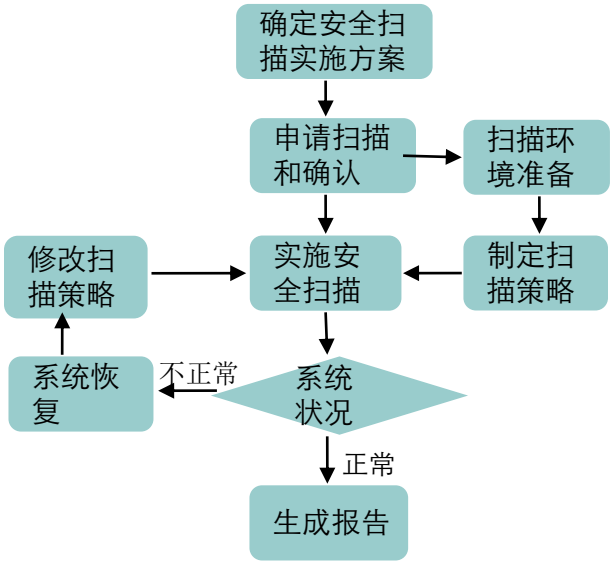
提供漏洞相关说明、补丁下载信息等，形成漏洞相关知识库。

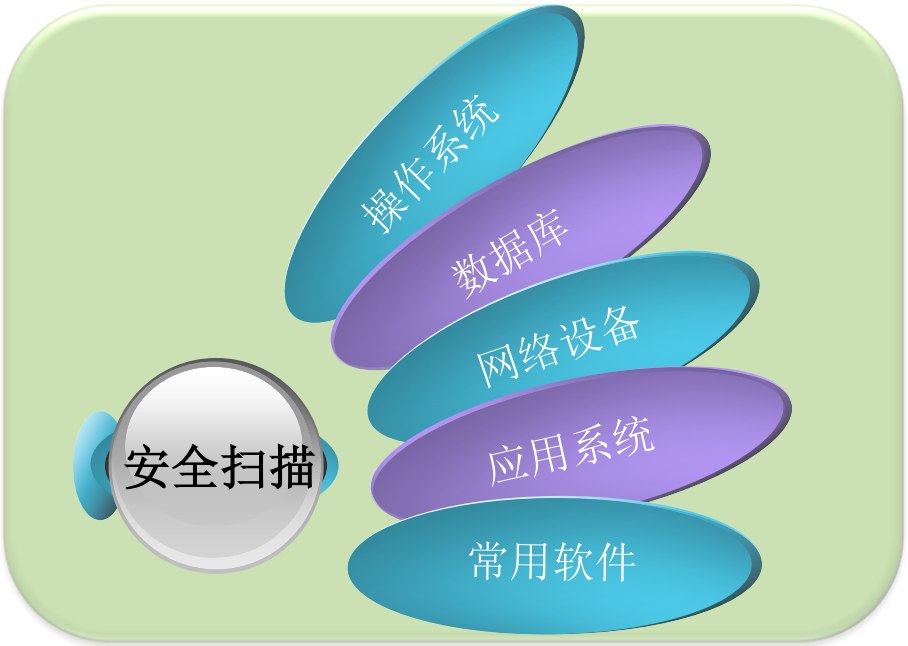
HUAWEI

安全服务

安全评估服务	针对云安全场景，提供面向数据中心的信息安全风险扫描，生成风险评估报告，识别云数据中心存在的安全风险。
优化与安全加固服务	基于评估结果，进行安全优化设计，提供安全解决方案建议；制定安全加固方案，通过一系列的安全加固措施，消除或转移数据中心系统中存在的高、中级别安全风险。
安全集成实施服务	从安全域划分、安全管理系统、应用与数据安全、IT基础设施安全和物理安全等层面，集成并实施安全基础设施。

安全评估服务





◆安全扫描

利用带有安全漏洞知识库的安全脆弱性扫描与管理工具，对云数据中心信息系统资产进行基于网络或主机层面的安全扫描，检测信息系统所存在的安全隐患和漏洞。

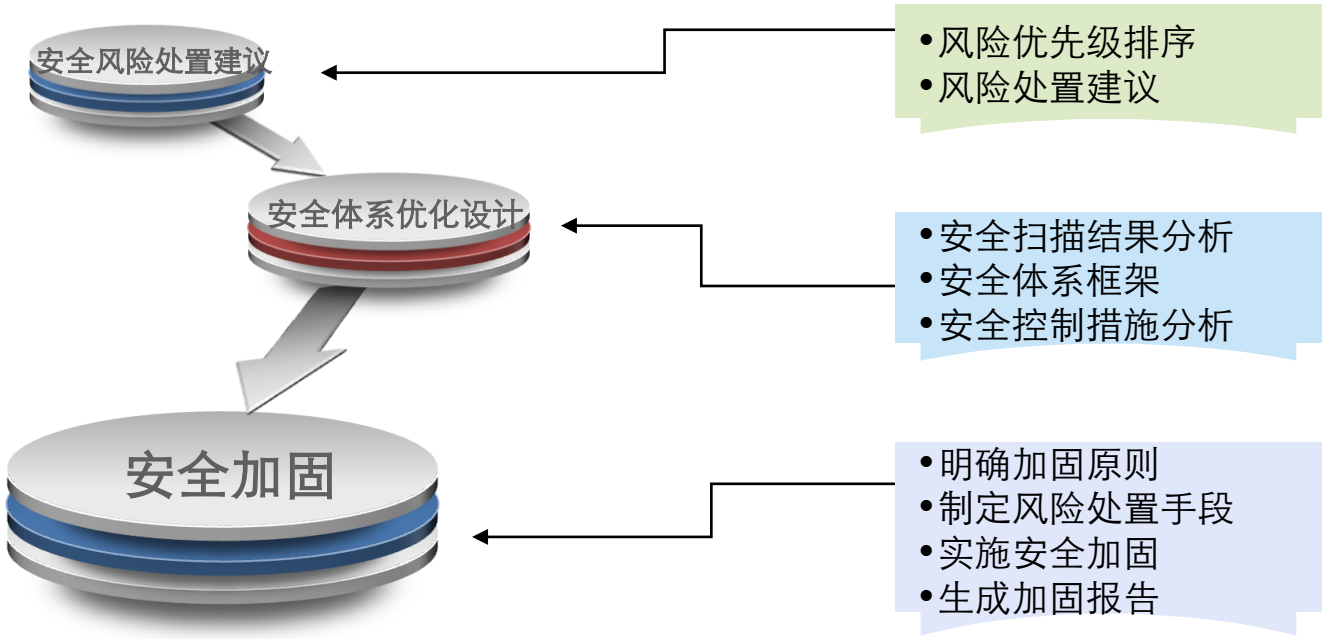
◆风险控制措施

选取适当的扫描策略、适当的扫描时间，提前做好系统备份和系统恢复措施，遵循单点试扫，主备分开的原则进行安全扫描。

◆扫描主要内容

版本及补丁维护、系统开放服务、账号及密码策略、文件和目录权限、日志配置、认证授权等方面。

安全优化与加固服务



◆安全优化设计

根据安全扫描得到的结果，针对不同风险等级和优先级的风险，给出安全风险处置意见，并提供安全体系结构优化建议，整体降低数据中心面临的安全风险。

◆安全加固

制定合理的加固方案，实施安全加固，消除信息系统存在的主要风险点。经加固后的评估对象不应再存在高风险漏洞和中风险漏洞。

安全集成实施服务

安全层次	具体范围	安全功能	服务类型
物理安全	物理安全	门禁系统	基础
		管理措施	基础
IT基础设施安全	网络安全	多租户之间的VPC隔离	基础
		防火墙	基础
		安全隔离	基础
		VPN接入服务	增值
		网络IDS/IPS	增值
		虚拟安全组/弹性IP	增值
		运维堡垒主机	增值
		安全域划分	基础
	主机安全	操作系统加固	基础
		防病毒	基础
		用户虚拟机模板加固	增值
		用户终端病毒防护	增值
	虚拟化安全	VM隔离	基础
		防止虚拟机之间的攻击	基础
应用与数据安全	应用安全	网页防篡改	增值
		Web应用防火墙	增值
		邮件安全	增值
	数据保护	主机存储与对像存储	基础
		数据加密和密钥管理	增值
安全管理	安全管理	安全信息与事件管理	基础
		安全策略管理	增值
		弱点管理	增值

◆ **IT基本架构基础安全设计**

描述了物理安全、安全域划分、网络安全隔离、主机安全保护、虚拟化安全、数据保护、安全信息与事件管理等基本安全措施的集成实施。

◆ **IT基本架构增值安全设计**

描述了远程接入安全、安全入侵防范、虚拟安全组、虚拟机安全加固、应用安全、数据保护、安全管理等增值安全措施的集成实施。

HUAWEI

安全产品全景图

网络安全设备

防火墙

Eudemon200E

<1G

Eudemon1000E

1G-8G

Eudemon8000E

10G-160G

Anti-DDoS 防分布式拒绝服务攻击

Eudemon1000E-I/D

1-2G

Eudemon8000E

10G-80G

ATIC

管理中心

安全路由网关

Eudemon200E-X

<350KPPS

Eudemon1000E-X

350K-1500KPPS

SSL VPN

SVN 3000

2000 users

IDS 入侵检测系统

NIP200

100M-200M

NIP1000

200M-1G

软安件全

端点安全管理

TSM

终端安全管理

DSM

文档安全管理

安全管理系统

eLog

Log日志管理与审计

VSM

统一安全网管

HUAWEI

问 题

- 数据中心安全解决方案包括了哪几个模块?
- 列举数据中心安全解决方案涉及的设备

总 结

- 本章主要介绍数据中心安全解决方案。
- 它包括了安全服务，应用安全，主机安全，网路安全，虚拟化安全，数据安全，用户管理，物理设施安全以及安全管理等9个子模块。

谢谢

www.huawei.com