

1. 前言：

随着信息通信技术的发展，信息化建设将网络普及到社会的方方面面，人们在随时随地享受 IT 带给人们的服务。正是由于现今人们对 IT 服务的高度依赖，传统的 IT 服务模式已经远远无法满足当下的信息交互需求，在此大背景下，云计算油然而生。

云计算具有自助按需服务、虚拟资源池、可度量服务、高速弹性架构和高宽带网络等五个关键特征。而云平台则是指通过互联网把高度扩展且抽象化的庞大 IT 资源作为服务提供给用户使用的一种计算形态，提出软件既服务（SaaS）、平台既服务（PaaS）和基础设施既服务（IaaS）的理念，随着虚拟化技术的不断发展与革新，一种以整合服务器或存储器等 IT 资源并合理运用的模式正逐步普及，因此“IT 既服务”的云平台理念必将成为未来的发展趋势。

云技术的应用都大大提高了工作效率并节约了成本，云技术是 IT 技术发展的必然趋势也是对时代进步的一个完美诠释，它构建了一个全新的世界：组件可以迅速调配、置备、部署和回收，还可以迅速地扩充或缩减，以提供按需的、类似于效用计算的分配和消费模式。从而完美解决了日益增长的 IT 服务需求。

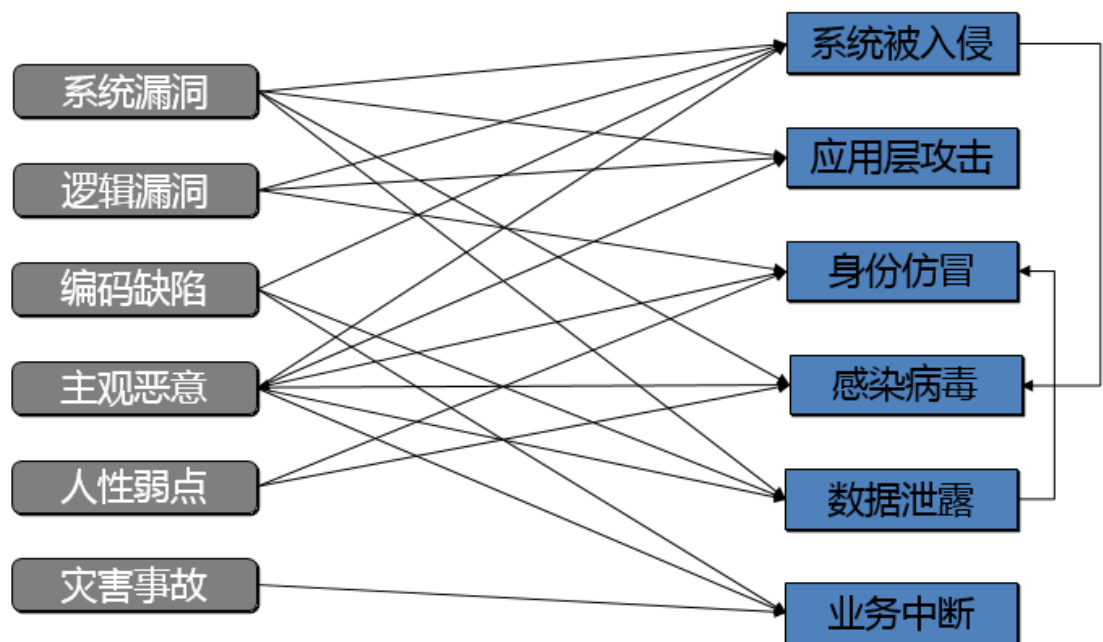
2. IDC 风险及需求分析

在运用云技术的 IDC 数据中心，由于在网络技术与协议上的开放性，使得整个云计算中心存在着各种类型的安全隐患和潜在的危险，黑客及怀有恶意的人员将可能利用这些安全隐患对网络进行攻击，造成严重的后果。因此如何保护重要信息不受黑客和不法分子的入侵，保证 IDC 数据中心系统的可用性、安全性和完整性等问题摆在我们面前。结合 IDC 数据中心信息环境的安全现状以及可能存在的安全问题，对网络中潜在的安全威胁与安全隐患进行分析。

2.1. 风险分类

2.1.1. 传统风险

云计算虽然传统架构有很多差异，但是继承了传统架构的网络协议，操作系统，数据系统，应用系统开发等技术。技术传统的安全风险依然存在，主要表现在系统漏洞、逻辑漏洞、编码缺陷、主观恶意、人性弱点、灾害事故等原因带来的系统被入侵、应用层攻击、身份仿冒、感染病毒、数据泄露、业务中断等问题。如下图所示：



2.1.1.1. 入侵风险

入侵分很多层次，从本质上说入侵是成功获取了入侵对象未经授权的权限，（权限访问、修改、执行等等；对象可以包括网络、主机文件、数据库等等），但是一般情况下默认为取得系统最高的权限为入侵系统。系统入侵一般是由于应用软件或操作系统软件在逻辑设计上的缺陷或错误、业务逻辑设计上的不足、编码缺陷、或者开发者主观上恶意留下后门等导致漏洞被不法者利用，通过网络植入木马、病毒等方式来攻击或控制整个主机，窃取主机中的重要资料和信息，甚至破坏系统。

2.1.1.2. 应用层攻击

应用层攻击通常并不依赖于在其下各层使用的攻击技术，尽管应用层攻击有时会使用这类技术（如 IP 欺骗或 TCP 会话劫持）来改变应用层攻击传递给目标系统的方式。应用层攻击之所以会存在，通常是因为程序员是在严格的期限压力下发布的代码，他们并没有足够的时间来发现并解决将会导致安全漏洞的错误。此外，许多程序员未考虑到使用某些特定语言结构将会导致应用程序暴露在隐式攻击下。最后，许多应用程序有着复杂的配置，缺乏经验的用户可能会在部署应用程序时启用了危险的选项，从而导致应用程序的安全性降低。

2.1.1.3. 身份仿冒

在用户身份假冒攻击中，攻击者与受害者有两种简单的关系：熟知和不知。熟知关系的攻击者可以轻易的盗取受害者的登录凭证(如：账号、密码、Cookie、USBKEY 等)，从而假冒受害者身份进行操作。不知关系的攻击者要进行攻击需要一定的攻击场景，如：处于同一个局域网环境，包括办公局域网、公共 WIFI 网络等，攻击者利用 ARP 或代理拦截等技术攻击获取用户登录凭证，假冒受害者身份进行操作。

2.1.1.4. 感染病毒

计算机病毒（Computer Virus）是编制者在计算机程序中插入的破坏计算机功能或者数据的代码，能影响计算机使用，能自我复制的一组计算机指令或者程序代码。计算机病毒具有传播性、隐蔽性、感染性、潜伏性、可激发性、表现性或破坏性。计算机病毒的生命周期：开发期→传染期→潜伏期→发作期→发现期→消化期→消亡期。计算机病毒是一个程序，一段可执行码。就像生物病毒一样，具有自我繁殖、互相传染以及激活再生等生物病毒特征。计算机病毒有独特的复制能力，它们能够快速蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上，当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。

2.1.1.5. 数据泄露

数据泄露是指私有数据在未经允许情况下盗取数据。在数据无所不在的世界里，企业保护机密信息比以往任何时候都要困难。复杂的异构 IT 环境让数据保护和威胁响应也变得相当困难。另外，随着企业移动办公人员不断的增加，当今的企业需要依靠自己的安全团队来确保他们协作和共享的安全性和可靠性。数据泄露的原因有以下三种：善意内部人员、目标性攻击和恶意内部人员。很多情况下，数据泄露是由上述几种原因共同引发的。

2.1.1.6. 业务中断

系统硬件故障、应用程序或操作系统出错、人为错误、电脑病毒/黑客入侵、自然灾害、正常的停机都有可能导导致业务中断。业务中断最大的问题是导致数据的丢失和错误以及业务的持续性。

2.1.1.7. 内部安全威胁

如果内部员工的计算机与 Internet 相连，其机器遭到黑客的攻击，黑客就可以再利用它作为跳板，攻击重要的服务器；而且来自于内部员工（或者内外勾结）的破坏行为，往往对整个系统的破坏作用将更大。因此 IDC 数据中心也同样面临来自内部人员的威胁。

内部安全威胁包括两个方面：一是内部员工的恶意攻击，由于在网络内部较网络外部更容易直接通过局域网连接到核心服务器等关键设备，尤其是管理员拥有一定的权限可以轻而易举地对内网进行破坏，造成严重后果。另外一方面是由于内部人员的误操作，或者为了贪图方便绕过安全系统等违规的操作从而对网络构成威胁。

2.1.2. 安全技术风险

依据云平台为租户提供不同服务内容，简要分析一下不同的安全风险。

2.1.2.1. DaaS 层安全风险

DaaS 层是存放数据，对数据进行归一化处理，进而交由 PaaS 层大数据分析平台进行进一步分类的基础。在信息安全方面的关注点在于数据在存储和传输过程中的保密性、完整性和可用性。

DaaS 层涉及到从 LVM（逻辑卷组）中的原始零散数据，到数据整合、数据管理进而成为元数据等各个流程。主要包括数据存储，数据传输，数据访问，数据审计以及数据容灾等五个方面的风险。

- 1) 数据存储风险：敏感数据（包括结构化和非结构化数据）在存储状态下可能存在被非法提权泄露，恶意破坏的风险。
- 2) 数据传输风险：敏感数据在传输状态下，存在被监听、篡改、泄露的风险。
- 3) 数据访问风险：数据被调用时，存在访问是否合法、合理的风险。
- 4) 数据审计风险：数据的各类活动过程在不进行审计的情况下，即使发生上述风险，也无法被探知，无法进行数据的容灾恢复工作。
- 5) 数据容灾风险：数据在存储时，限于其物理设备可能存在的风险，导致风险转嫁，造成数据失败；在数据传输时造成完整性破坏后，造成失败写入。都会影响数据的完整性和可用性，因此需要进行数据容灾保护。

2.1.2.2. PaaS 层安全风险

PaaS 层介于应用与资源之间，是两者的纽带和桥梁。在信息安全方面的关注点在于资源是否被合理、合法的被应用调用，并且调用的过程是否进行了周密的审计和监控。

PaaS 层通过中间件接口以及大数据平台的数据索引、调度、分类管理平台为应用和数据间做好代理人的工作；同时，通过虚拟化平台提供对虚拟化应用环境的管理。因此 PaaS 层的安全风险也主要在于其组件在与其他平台交互，运行时体现。

此外，**PaaS** 层也提供开源的开发环境，为扩展云的服务组件提供孵化环

境。

- 1) 中间件及接口安全风险：中间件是重要的协议过渡，指令传递组件；而接口是完成中间件获取和传递信息的出入口。因而面临着因软件代码自身具备的脆弱性带来的进程失败，信息损坏、泄露等风险。
- 2) 虚拟化平台风险：虚拟化平台是管理和实现各类资源池化的工具平台，虚拟主机、网络、存储所隐含着的风险，主要原因在于虚拟化平台自身存在的设计缺陷和安全漏洞。同时，因虚拟化技术主要源于国外，存在自主可控技术的风险。
- 3) 大数据分析平台风险：大数据分析平台直接面向各类应用和数据，将 DaaS 层整合的元数据资源借由调用各类中间件和接口，进行归类整合，成为数据仓库，方便应用直接调取；因此，也面临着临时数据泄漏和损坏的风险，对于数据调取的权限控制，审计措施也势在必行。
- 4) 开发环境安全风险：开发环境是重要的系统环境，最主要的威胁来自非法访问后，提权进行更深层次的系统资源调用或修改，甚至对源代码进行修改，导致基础性的业务损毁风险。其风险主要在于失效的身份鉴别、权限控制所引发的后续风险。

2.1.2.3. IaaS 层安全风险

IaaS 层是负责承载其上平台、数据和应用的基础设施层。包含各类 IT 设备，云化的资源池，各类计算主机和连接他们之间的网络。

IaaS 层是整个云数据中心的基础之所在，与该层的业务交互是通过 PaaS 层提供的合法接口来进行，同时存在与物理环境的交互。

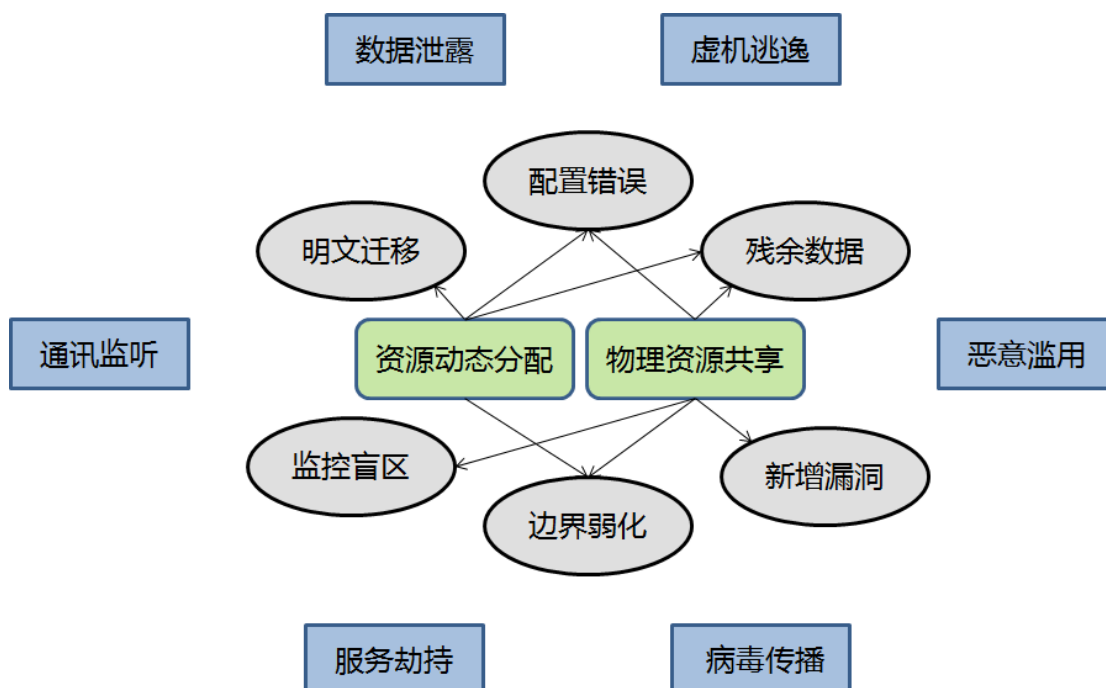
本层的风险主要体现在四个方面：

- 1) 基础设备安全：基础设施因与物理环境直接交互，所以面临着物理方面带来的安全风险，如火灾、温湿度、电力故障等等。此外，各类设备硬件组件因自身故障可能导致部分失败，也引发了故障风险。

- 2) 主机操作系统安全：无论是计算节点还是网络节点、安全设备等
都具备自身的操作系统，也因此带来天然存在的脆弱性，引入了
被渗透，被侵染的风险。
- 3) 网络安全：基于 TCP/IP 的以太网网络，是连接各类节点的道路。网
络链路可能会因恶意代码（如 DDoS 攻击）或带宽分配不合理等
原因导致的堵塞的风险；同时，网络内的流量可能承载着恶意入
侵行为流量，导致针对应用服务和数据的风险传递。
- 4) 虚拟化风险：依托于虚拟化技术的虚拟化主机、虚拟化网络有别
于传统 IT 基础设施，存在新环境下特有的安全风险。虚拟化网络
存在流量不可视，网络边界漂移模糊，多租户访问控制隔离等风
险；虚拟化主机存在恶意抢占资源，伪装正常业务访问进行嗅探
等风险。

2.1.3. 虚拟化引发的新风险

由于 IDC 数据中心采用了虚拟化和资源动共享和动态调度的技术，信息系统的架构比
以往更复杂，虚拟化层和动态共享等引入配置错误、残余数据、新型漏洞、边界弱化、监
控盲区、明文迁移等新的脆弱性。这些新的脆弱性有造成了数据泄露、虚机逃逸、恶意滥
用、病毒传播、服务劫持、通讯监听等威胁，如下图所示：



2.1.3.1. 数据泄漏

由于基于云计算的信息系统无法避免的资源共享和动态分配的过程，因此在这两个过程中都有可能出现数据泄漏的问题。例如原来被 A 用户租用的硬盘空间，分配给 B 用户使用，如果硬盘内容没有充分清除，B 用户则有可能读取 A 用户的数据。在例如当虚拟机采用明文方式动态迁移时，攻击者有可能通过监听获得虚拟机的数据。

2.1.3.2. 虚机逃逸

虚拟机逃逸是指利用虚拟机软件或者虚拟机中运行的软件的漏洞进行攻击，以达到攻击或控制虚拟机宿主操作系统的目的。在虚拟化环境与传统主机环境相比，多了一个虚拟机管理（VMM）层，如果 VMM 存在漏洞，虚拟机的拥有者则可以利用漏洞，摆脱 VMM 控制或者直接攻击同一个 VMM 下的其它虚拟主机。

2.1.3.3. 恶意滥用

攻击者可以租用虚拟机用于恶意目的。例如把虚拟机当作受控主机发送攻击数据包，对被攻击目标形成 DDoS 攻击。还可以用于对网页的虚假点击，从而获得不正当经济利益。

2.1.3.4. 病毒传播

云平台用户复杂，数据量大，边界弱化带来的东西流量控制难度大，使得病毒传播在云平台中更加容易，难以控制。

2.1.3.5. 服务劫持

恶意虚拟机与传统物理主机一样，也可以发送 ARP 欺骗数据包来实现对其它虚拟机的通讯劫持。

2.1.3.6. 通讯监听

在虚拟化环境中，通过同一物理主机上两个虚拟机通过虚拟交换机进行交换的数据，

原理上是通过共享内存来实现的。如果恶意虚拟机利用 VMM 漏洞，可以读取虚拟化层的内存，从而达到通讯监听的目的。

2.1.4. 管理风险

当云数据中心进入上线运营阶段后，相关安全管理人员在管理过程中可能会遭遇多种问题，引发安全管理风险。

2.1.4.1. 云环境下的特有安全管理风险

在云环境下，“资源池”管理技术主要实现对物理资源、虚拟资源的统一管理，并根据用户需求实现虚拟资源（虚拟机、虚拟存储空间等）的自动化生成、分配、回收和迁移，用以支持用户对资源的弹性需求。

这突破了传统的安全区域，使得传统基于物理安全边界的防护机制不能有效地发挥作用，削弱了云平台上各租户对重要信息的管理能力。另外，在传统网络环境中，网络中的各类资产通常由不同的管理员进行管理。但在虚拟化环境中，往往都由同一管理员负责，可能会出现管理员权限过于集中的风险。对管理员的操作审计和行为规范都提出了很高的要求。

2.1.4.2. 安全组织建设风险

要应对云数据中心进入运行阶段的各类问题，首先对进行安全管理运维的组织保障能力提出了挑战。

没有依据实际情况建设的安全组织，无法应对云平台复杂环境下的安全管理要求，无法顺利完成安全管理工作，无法保障各类云业务的顺利进行。而且鉴于本次云数据中心建设的实际情况：即迁入多租户的大量应用，所以在进行安全管理时，如何划分管理权限，明晰职责，也成为了需要解决的问题。

因此，需求合理的、务实的、专业的多类安全队伍来应对挑战，保障云数据中心业务顺利通畅的进行。

2.1.4.3. 人员风险

再安全的网络设备和安全管理系统也离不开人的操作和管理，再好的安全策略也最终要靠人来实现，因此人员也是整个网络安全中的重要一环。需要具备完备的信息安全意识，专业的信息安全素养，职业化的信息安全态度人才，来管理和维护云数据中心，保障业务顺利通畅的进行。

2.1.4.4. 安全策略风险

在应对云平台未来可能遇到的信息安全事件时，除了具备组织、人员外，还需要制定适合云平台系统复杂环境的安全制度和策略，让组织和人员可以有效的，合规的完成信息安全事件相关的各类工作，以保证信息安全管理可以高效，高质量的进行。

2.1.4.5. 安全审计风险

在云平台投入使用后，因业务系统和底层架构较为复杂，需要进行全方位的监控审计，以便及时发现各类可能和信息安全相关、业务状态相关的信息，并及时作出管理策略的响应和调整。

而具体由谁来监控审计，审计结果是否有效而客观，是否可以及时传达至相关责任人，这些问题都需要妥善解决，才能够实现全方位、及时，有效的审计。

2.1.5. 运维风险

云数据中心建设完成后，将引入租户的应用系统。所以在云数据中心投入使用后，运维人员、审计监控以及应急响应等都发生了职责、权限、流程的变化，引入了新型的，在云环境下特有的新型风险。

此外，还包括一些传统的安全运维风险，例如：环境与资产，操作与运维，业务连续性，监督和检查，第三方安全服务等风险。

2.1.5.1. 云环境下的特有运维风险

- 运维职权不明风险

在云数据中心投入使用后，基础设施由机房运维团队进行运维，而基于基础设施的各类应用由各租户的相关人员进行运维。但是当发生事故的时候，无法在第一时间确定事故的波及方；处理事故时，无法分配具体任务；事故追责时，无法确定到底由谁来负责。尤其是在云环境中，资源池内如果发生了安全事故，资源边界更加模糊。因此确定运维职责非常重要。

- 运维流程不明风险

因为运维参与者众多，属于不同的参与方，也导致在进行运维过程中，很多流程要涉及到不同参与方的多个部门。因此确定一个统一的，合理的安全运维制度是保障运维工作顺利进行的必要条件。

- 虚拟资源运维审计监控风险

在安全技术上，传统的运维审计手段缺乏对虚拟机的运维审计能力。流量不可视也带来了协议无法审计，虚拟机动态迁移带来审计策略中断等问题。

- 突发事件风险

再完备的安全保障体系，也无法阻止突然性事件的发生，这种风险也是信息系统固有的属性，无法避免。尤其是在云环境下，应急响应变得更为复杂，涉及范围广，恢复难度大。也因此需要在云数据中心，有可靠的应急响应队伍和机制，保障快速、妥善的应对各类突发性问题。

2.1.5.2. 环境与资产风险

信息系统依托于机房与周边环境，而业务系统则直接依托于基础设施。在云数据中心投入使用后，面临的最直接的风险就来自于环境和资产。因此为了保证各租户业务系统的正常运行，所以要求数据中心运维团队的运维管理能力具备较高的水平。

2.1.5.3. 操作与运维风险

人员是很难进行控制的，而对业务和基础设施进行操作和运维的人员，无论是通过现场还是远程进行操作，都可能因为误操作，为信息系统带来损失。如何规范人员的操作、运维流程，如何减少误操作的可能性，如何提高操作者的职业素养，这些都是需要解决的问题。

2.1.5.4. 业务连续性风险

信息系统的最终使命是运行业务，但是业务的连续性是否能够保证，关乎信息系统的多个层面，包括物理、网络、主机、应用以及数据等。在云计算环境下，还包括虚拟化平台，以及运行在其上的虚拟主机、虚拟网络。其中任何一环如果出现问题，都有可能影响业务的连续性。所以如何保护业务的连续性也给运维团队提出了难题。

2.1.5.5. 监督和检查风险

为了保障如此复杂的系统，需要许多安全技术、管理和运维的过程。这些过程是否符合法律、符合标准，在发生事故时，如何督促管理者有效跟踪事故，并快速解除故障。这些都需要进行监督和检查管理，否则容易使参与者承担法律风险。

2.1.5.6. 第三方服务风险

为保障云数据中心的正常运行和不断完善，需要进行很多运行维护工作，诸如：业务迁入，差距分析，安全加固，渗透测试等。但是这些工作都过于专业化，仍需要专业的第三方安全机构提供相应的服务，才可以有效的进行。

因此，如何选择第三方服务机构，如何监督评价第三方的服务质量，就需要妥善的第三方服务管理。

2.2. 需求分析

2.2.1. 传统网络的安全需求

2.2.1.1. 物理安全需求

云数据中心的机房，应符合等级保护中的物理安全的要求。

2.2.1.2. 网络安全的需求

网络边界防护的设计是将组织的网络，根据其信息性质、使用主体、安全目标和策略的不同来划分为不同的安全域，不同的安全域之间形成了网络边界，通过边界保护，严格规范系统内部的访问，防范不同网络区域之间的非法访问和攻击，从而确保各个区域的有序访问。一般来说边界防护采用的主要技术包括防火墙技术、入侵防御技术、过滤网关技术和接入认证技术。

■ 防火墙技术

防火墙是指设置在不同网络(如可信任的组织内部网和不可信任的公网)或网络安全域之间的一系列部件组合。防火墙通常位于不同网络或网络安全域之间信息的唯一连接处，根据组织的业务特点、行业背景、管理制度所制定的安全策略，运用包过滤、代理网关、NAT 转换、IP+MAC 地址绑定等技术，实现对出入网络的信息流进行全面的控制（允许通过、拒绝通过、过程监测），控制类别包括 IP 地址、TCP/UDP 端口、协议、服务、连接状态等网络信息的各个方面。防火墙本身必需具有很强的抗攻击能力，以确保其自身的安全性。

■ 入侵防御技术

网络入侵防御系统位于有敏感数据需要保护的网络上，通过实时侦听网络数据流，寻找网络违规模式和未授权的网络访问尝试。当发现网络违规行为和未授权的网络访问时，能够根据系统安全策略做出反应，包括实时报警、事件登录，或执行用户自定义的安全策略等。

■ 过滤网关技术

传统的防病毒解决方案主要是基于单机或服务器的方式，是一种被动的解

决方案。每当出现新的病毒，管理员往往会发现他们分身乏术，需要确保网络中的每台 PC 机、笔记本和服务器等都升级到了最新的病毒库。过滤网关技术是传统网络防病毒的有力补充，通过在网关部位部署过滤网关，能够在网关处过滤病毒和垃圾邮件等，把病毒和垃圾邮件挡在安全域外。

■ 接入认证技术

对接入终端接入网络进行接入认证，只有通过身份认证的用户才允许接入网络，把非法接入的漏洞彻底封死。

■ 加密技术

由于 TCP/IP 的开放性和网络嗅探工具的普及，网络中数据被非法窃听的可能性愈来愈大，造成未经授权的数据泄漏的风险越来越大，所以有必要对远程用户对云数据中心重要应用的访问进行数据加密，采用加密技术进行数据传输可以有效避免数据被非法窃听。

2.2.1.3. 主机安全的需求

一般来讲，安全的威胁主要来自于系统的弱点，针对主机中存在的安全隐患，很容易成为内部用户或外部非法入侵者进行攻击的对象，因此，有必要进行分析，发现存在的隐患或弱点后，进行修补。

同时还要设法提高整体网络的抗病毒能力，确保网络不受到病毒的侵害，从而降低系统层、应用层的安全威胁。一般来说系统加固采用的主要技术包括安全扫描技术和防病毒技术。

■ 安全扫描技术

安全扫描系统是现阶段最先进的系统安全评估技术，该系统能够测试和评价系统的安全性，并及时发现安全漏洞。

漏洞检测和安全风险评估技术，因其可预知主体受攻击的可能性，并具体指证将要发生的行为和产生的后果，而受到网络安全业界的重视。这一技术的应用可帮助识别检测对象的系统资源，分析这一资源被攻击的可能指数，了解支撑系统本身的脆弱性，评估所有存在的安全风险。

■ 网络防病毒技术

传统的网络防病毒技术已经不能满足主机防护的需求，病毒攻击、系统漏

洞等造成的破坏和损失原来越大，必须采用防病毒的手段来保障主机和网络的安全。在技术层面主动防御：采用防病毒技术、防火墙技术、IDP 技术、威胁扫描技术以及系统加固技术对主机进行主动实时的防护，抵御来自多方面的威胁和攻击。

■ 负载均衡技术

云数据中心有许多核心应用系统，如果这些应用系统有宕机、断网等现象会造成应用系统不可用，系统不能正常提供服务。负载均衡技术可以解决应用系统的单点故障。两台以上的应用服务器就可以组成一套带有冗余功能的应用系统，形成 AA 模式的冗余备份系统，多台设备同时处理业务请求，其中一台系统宕机或者断网不影响业务系统的正常运行。

2.2.1.4. 应用安全的需求

云数据中心将运行各部门及租户的多类应用，应用之间应进行授权访问隔离，每一位用户应根据其业务、职务来分配其授权范围，从而保护应用数据的最小授权。应通过建立统一的身份认证平台，配合静态账户+数字证书的方式完成对账号、认证、授权的管理。

维护应用正常运转的另一个必要条件是对应用及其数据进行全方位的审计，应成立专有的审计部门（隶属于运维团队）对应用服务进行审计。同时应采用集中日志审计系统，将审计数据从各应用系统收集，在专有的 LVM（逻辑卷组）中保存，并维护审计数据的真实性和完整性。

另外，云数据中心的应用系统主要通过 WEB 方式，将重要的信息和数据进行公开发布。而针对主页系统的攻击包括篡改、拒绝服务、恶意脚本、信息泄露等攻击，常见的防护手段是防火墙、入侵检测和防病毒来，在采纳上述三种技术之上，如果对主页内容进一步进行防护，那将大大降低攻击的成功率，进一步提升 WEB 应用的安全性，这种技术就是 WEB 防护系统。

WEB 服务器的安全防护需求包括：能够解决 WEB 服务器所面临的各类 WEB 应用攻击，包括已知攻击（如：注入攻击、跨站攻击、表单绕过等）、变形攻击及未知攻击等。

2.2.1.5. 数据安全的需求

■ 数据存储保护

加强关键业务数据的存储保护，保证数据不被非法授权查看。

■ 数据存储完整性校验

应采取措施检测应用系统信息的完整性，对信息传输过程中出现的变动记录日志。同时对应用系统区域中存储的信息进行监测，防止非授权的修改。

■ 抗抵赖

应采取数字签名、时间戳等技术防止参与通信的双方或一方对自己源发行为、交付行为以及所作的操作（如文档创建、信息发送、信息接收以及批示）进行部分或全部的否认。

■ 数据库安全

数据库的安全，主要从四个方面考虑：

- 1) 数据库的漏洞填补: 通过前置虚拟补丁库，在不影响数据库业务连续性的条件下完成数据库漏洞的填补；
- 2) 数据库攻击防护: 应配备专有的数据库防护系统，防护针对数据库的恶意攻击行为，如 **SQL** 注入，提权后拖库、盗库；
- 3) 数据库运维侧审计和防护: 数据库运维人员应经过有效的双向认证后，在审计监督的环境下对数据库进行运维操作；高危操作语句，如：**update no where**、**delete no where** 应从技术侧面禁止；
- 4) 数据库应用侧审计和防护: 应用对数据库的访问是固化在代码中的，具备一定的 **SQL** 语句模型，应对应用访问进行合法性认证，同时对其 **SQL** 语句进行建模，防止黑客可能的注入攻击。

■ 备份与恢复

应建立本地容灾中心，未来应建立异地容灾中心，当发生事件后能迅速恢复，不影响业务正常使用。

■ 应急响应

应急响应针对两种事件：影响系统稳定运行的事件和安全事件。

2.2.1.6. 安全管理和运维需求

一切安全保障活动的核心是符合安全管理的需求，安全技术的部署是为了达成组织安全策略、方针、制度的有效措施。

因此，云数据中心在信息安全管理和运维方面也应进行有效的实践。具体包括：

- 1) 建立专业云数据中心管理和运维的组织团队；
- 2) 配属具备信息安全素养和职业素质的安全管理人员；
- 3) 制定有效的，贴合实际的安全策略、方针、制度和规范；
- 4) 通过文档化的过程，颁布环境与资产保护策略、操作与运行维护规范、审计制度、业务连续性保障制度、监督和检查规定、第三方服务规范；
- 5) 通过领导的执行力，将这些文档化安全管理和运维制度落地到实处，并辅以有效追责，奖惩制度将制度有效推行。

2.2.2. 云平台安全需求

2.2.2.1. 适当的安全管理

不管是内部的安全自我评估，还是通过第三方对云数据中心的外部安全审计/认证，或者两者都有，都应该基于用户安全需求而建立。此外，应该定义适合的标准，以便提供对云服务平台和用户之间安全级别更好的理解。云数据中心也应该通过整合云用户的安全策略、正在谈判的 SLA 等来实施他自己的安全策略，并且给出几个不同的商业解决方案。

2.2.2.2. 安全的 Hypervisor

虚拟化技术是云计算的基础，在共享内存、CPU 和存储容量的环境下，必须保证虚拟机之间的有效隔离。在一个物理服务器上，Hypervisor 可以支撑多个虚拟机。如果 Hypervisor 被破坏，虚拟机之间严格的隔离可能会失败。对云服务平台来说，Hypervisor 必须提供标准，以确保其本身和虚拟机的安全。

2.2.2.3. 虚拟机安全需求

尽管在大多数情况下，云服务提供商不会对用户的虚拟机安全负责，云服务提供商只是提供用户所需要的虚拟硬件、平台和与之相关的软件应用使用环境，而对于用户如何使用虚拟机，如何确保虚拟机的安全并不负责，但是出于对安全层面的认真考虑，在此将虚拟机安全也作为分析内容。

云平台虚拟机主机安全主要指主机以及应用层面的安全风险与需求分析，包括：身份鉴别、访问控制、系统审计、入侵防范、恶意代码防范、软件容错、数据完整性与保密性、备份与恢复、资源合理控制、剩余信息保护、抗抵赖等方面，我们建议用户在使用虚拟机服务时考虑以下方面。

■ 身份鉴别

身份鉴别包括主机和应用两个方面。

用户在虚拟机上的主机操作系统登录、数据库登陆以及应用系统登录均必须进行身份验证。过于简单的标识符和口令容易被穷举攻击破解。同时非法用户可以通过网络进行窃听，从而获得管理员权限，可以对任何资源非法访问及越权操作。因此必须提高用户名/口令的复杂度，且防止被网络窃听；同时应考虑失败处理机制。

■ 访问控制

访问控制包括主机和应用两个方面。

访问控制主要为了保证用户对虚拟机的主机资源和应用系统资源的合法使用。非法用户可能企图假冒合法用户的身份进入系统，低权限的合法用户也可能企图执行高权限用户的操作，这些行为将给主机系统和应用系统带来了很大的安全风险。用户必须拥有合法的用户标识符，在制定好的访问控制策略下进行操作，杜绝越权非法操作。

■ 系统审计

系统审计包括主机审计和应用审计两个方面。

对于登陆虚拟机主机后的操作行为则需要进行主机审计。对于服务器和重要主机需要进行严格的行为控制，对用户的行为、使用的命令等进行必要的记录审计，便于日后的分析、调查、取证，规范主机使用行为。而对于应用系统同样提出了应用审计的要求，即对应用系统的使用行为进行审计。重点审计应

用层信息，和业务系统的运转流程息息相关。能够为安全事件提供足够的信息，

与身份认证与访问控制联系紧密，为相关事件提供审计记录。

■ 入侵防范

云平台里的虚拟机主机操作系统面临着各类具有针对性的入侵威胁，常见操作系统存在着各种安全漏洞，并且现在漏洞被发现与漏洞被利用之间的时间差变得越来越短，这就使得操作系统本身的安全性给整个系统带来巨大的安全风险，因此对于主机操作系统的安装，使用、维护等提出了需求，防范针对系统的入侵行为。

■ 恶意代码防范

病毒、蠕虫等恶意代码是对计算环境造成危害最大的隐患，当前病毒威胁非常严峻，特别是蠕虫病毒的爆发，会立刻向其他子网迅速蔓延，发动网络攻击和数据窃密。大量占据正常业务十分有限的带宽，造成网络性能严重下降、服务器崩溃甚至网络通信中断，信息损坏或泄漏。严重影响正常业务开展。因此必须部署恶意代码防范软件进行防御。同时保持恶意代码库的及时更新。

■ 软件容错

软件容错的主要目的是提供足够的冗余信息和算法程序,使系统在实际运行时能够及时发现程序设计错误,采取补救措施,以提高软件可靠性,保证整个计算机系统的正常运行。

■ 资源合理控制

资源合理控制包括主机和应用两个方面。

虚拟机主机系统以及应用系统的资源是有限的，不能无限滥用。系统资源必须能够为正常用户提供资源保障。否则会出现资源耗尽、服务质量下降甚至服务中断等后果。因此对于系统资源进行控制，制定包括：登陆条件限制、超时锁定、用户可用资源阈值设置等资源控制策略。

2.2.2.4. 安全的虚拟机迁移

必须确保在多个物理主机之间的虚拟机的迁移安全。包括虚拟机在迁移之前、之后，和迁移过程中的安全。可以通过控制台管理器或编程方式，维护一个日志文件和报告，以便确定：虚拟机所在的物理主机，虚拟机的状态（静止、还是迁移），如何控制虚拟机防止未授权的访问及修改。虚拟机迁移还要求提供安全策略协商功能，已迁移的虚拟机应该适应新的物理主机的安全策略。

2.2.2.5. 虚拟机镜像安全

虚拟机镜像是云计算环境中的特殊资产。应当执行合适的安全规则，用来保护虚拟机镜像在整个生命周期的安全。在虚拟机运行和休眠阶段，采用访问控制，防止虚拟机镜像被窃取和修改；在虚拟机镜像启动之前，进行安全检查，防止预先配置的虚拟机镜像的误配置和欺骗。

2.2.2.6. 存储隔离

云数据中心可以为用户提供灵活的、可扩展的存储功能。根据虚拟机的执行要求，它的存储需求是动态变化的。在数据中心，会部署不同的存储解决方案。各种存储技术互操作性和安全保护是一个重要的问题。必须确保它的存储系统的隔离是随时有效的，而不会受到实际方案选择的限制。

2.2.2.7. 网络保护

在云基础架构中，用了很多虚拟网络技术。相对于传统的网络，因为虚拟网络的隔离是逻辑的而非物理的，所以，云计算中的虚拟网络将出现更多的安全漏洞。当前为了实现网络区域划分，主要通过虚拟化防火墙来实现。另外，为了阻止云服务之间的影响，造成安全问题，应该实施网络边界控制机制。

为了响应云执行环境的动态演变，需要提供网络资源的弹性分配和快速供给，同时，也需要部署适应其的保护机制。为了使得多个租户同时动态使用共享的网络基础设施，云服务平台需要提供网络保护机制。有效的网络安全保护机制是云服务端到端安全的重要保证。

2.2.2.8. 受信任的资源池管理和多租户隔离

云计算允许虚拟机灵活地进行在线迁移。这种灵活性打破了已知的安全模型。在虚拟机迁移或其他虚拟机移动行为之前，虚拟机管理员需要负责要执行的虚拟机迁移的目标是可信赖的。

云计算通过资源共享可以带来潜在的成本节约，但也带来了一些潜在的安

全漏洞。云应该提供对数据的加密，保证造成数据泄漏的虚拟化层的袭击成为最小可能。

2.2.2.9. 数据的可追溯性

在共享的虚拟化基础架构中，用户失去的不仅是对数据的控制，还包括数据的定位和数据生命周期的管理。在任何时候，一个云管理平台应该需要准确的知道用户的数据和虚拟机的数据是在哪里存放、处理和被访问的。当前缺乏关注的是，在云中的数据是可以自由地在多个组织之间迁移的，甚至是可以跨国界的。在数据使用过程中，还是在使用之后，数据都应该不能被第三方访问。

2.2.2.10. 互操作性

一个数据中心经常通过一套异构的硬件和软件组成，包括服务器、磁盘阵列、交换机、Hypervisor、中间件、软件。关于异构性的解决方案依然是一个重要的关注点。作为云管理平台，应该分析这些异构性组件共存和合作的安全性。进一步说，多种安全策略和机制的协调和整合是一个重要的问题。云管理平台应该保证多个安全策略和他们实现的一致性。

2.2.2.11. 灾难恢复

可用性是 IT 系统的三个主要安全目标之一。在任何时刻，一个云系统应该保持可用。灾难恢复表示应对特大灾难和恢复到安全状态的能力。此机制可以保证提供服务的连续性。云环境下，资源作为一种服务对外提供，因此，相对于传统的 IT 环境来说，其可用性显得更加重要。

2.2.3. 数据安全需求

对于云来讲，用户的大量数据在云平台内存储并且传输，一旦用户的数据丢失或者被攻击者恶意利用，修改，删除，泄漏，那么对用户和云服务提供商来讲都将造成巨大的损失。因此数据安全对于云平台来讲至关重要。

■ 数据安全

主要指数据的完整性与保密性。数据是信息资产的直接体现。所有的措施最终无不是为了业务数据的安全。因此数据的备份十分重要，是必须考虑的问题。应采取措施保证数据在传输过程中的完整性以及保密性；保护鉴别信息的保密性。

■ 备份与恢复

数据是信息资产的直接体现。所有的措施最终无不是为了业务数据的安全。因此数据的备份十分重要，是必须考虑的问题。对于关键数据应建立数据的备份机制，而对于网络的关键设备、线路均需进行冗余配置，备份与恢复是应对突发事件的必要措施。

■ 剩余信息保护

对于正常使用中的主机操作系统和数据库系统等，经常需要对用户的鉴别信息、文件、目录、数据库记录等进行临时或长期存储，在这些存储资源重新分配前，如果不对其原使用者的信息进行清除，将会引起元用户信息泄漏的安全风险，因此，需要确保系统内的用户鉴别信息文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用户前得到完全清除

对于动态管理和使用的客体资源，应在这些客体资源重新分配前，对其原使用者的信息进行清除，以确保信息不被泄漏。

■ 抗抵赖

对于数据安全，不仅面临着机密性和完整性的问题，同样还面临着抗抵赖性（不可否认性）的问题，应采用技术手段防止用户否认其数据发送和接收行为，为数据收发双方提供证据。

3. 架构设计

3.1. 设计原则

■ 体系化原则

IDC 数据中心的架构设计应充分考虑到各个层面的安全风险，构建完整的

安全防护体系，充分保证系统的安全性。同时，应确保方案中使用的信息安全产品和技术方案在设计和实现的全过程中有具体的措施来充分保证其安全性。

■ 先进性原则

IDC 数据中心对所需的各类安全产品有着很高的要求，必须认真考虑各安全产品的技术水平、合理性、先进性、安全性和稳定性等特点，共同打好工程的技术基础。

■ 有序建设原则

IDC 数据中心的安全建设是一项长期的工程，并非一蹴而就解决所有安全问题。因此，在实际建设过程中要根据实际情况分轻重缓急，分期、分批的进行部署。

3.2. 依据的标准和规范

本方案重点参考以下的政策和标准：

国际标准和文件	CSA 云安全指南 V3.0.1
	CSA CCM 云控制矩阵 V3.0
	FedRAMP 云安全标准
	ITU-T X.ccsec：通信领域云计算安全指引
	ITU-T X.srfcts：基于云的通信服务环境安全要求和框架(X.srfcts)
指导思想	中办[2003]27 号文件（关于转发《国家信息化领导小组关于加强信息安全保障工作的意见》的通知）
	公通字[2004]66 号文件（关于印发《信息安全等级保护工作的实施意见》的通知）
	公通字[2007]43 号文件（关于印发《信息安全等级保护管理办法》的通知）
等级保护	GB 17859-1999 计算机信息系统安全保护等级划分准则
	GB/T 25058-2010 信息安全技术 信息系统安全等级保护实施指南
	GB/T 25070-2010 信息安全技术 信息系统等级保护安全设计技术要求
技术方面	GB/T 22080-2008 信息安全技术 信息安全管理体系要求
	GB/T 22081-2008 信息安全技术 信息安全管理体系实用规则

	GB/T 20270-2006 信息安全技术 网络基础安全技术要求
--	-----------------------------------

	GB/T 20271-2006 信息安全技术 信息系统通用安全技术要求 GB/T 20272-2006 信息安全技术 操作系统安全技术要求 GB/T 20273-2006 信息安全技术 数据库管理系统安全技术要求 GA/T671-2006 信息安全技术 终端计算机系统安全等级技术要求 GA/T 709-2007 信息安全技术 信息系统安全等级保护基本模型 GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求
管理方面	GB/T 22239-2008 信息安全技术 信息系统安全等级保护基本要求 ISO/IEC 27001 信息系统安全管理体系标准
方案设计	信息安全技术 信息系统等级保护安全建设技术方案设计规范
方案架构	IATF 信息保障技术框架

3.3. 安全技术架构（天融信）

IDC 数据中心从分层、纵深防御思想出发，根据层次分为物理设施安全、网络安全、主机安全、应用安全、虚拟化安全、数据安全、用户管理、安全管理等几个层面，安全技术架构如下图所示：

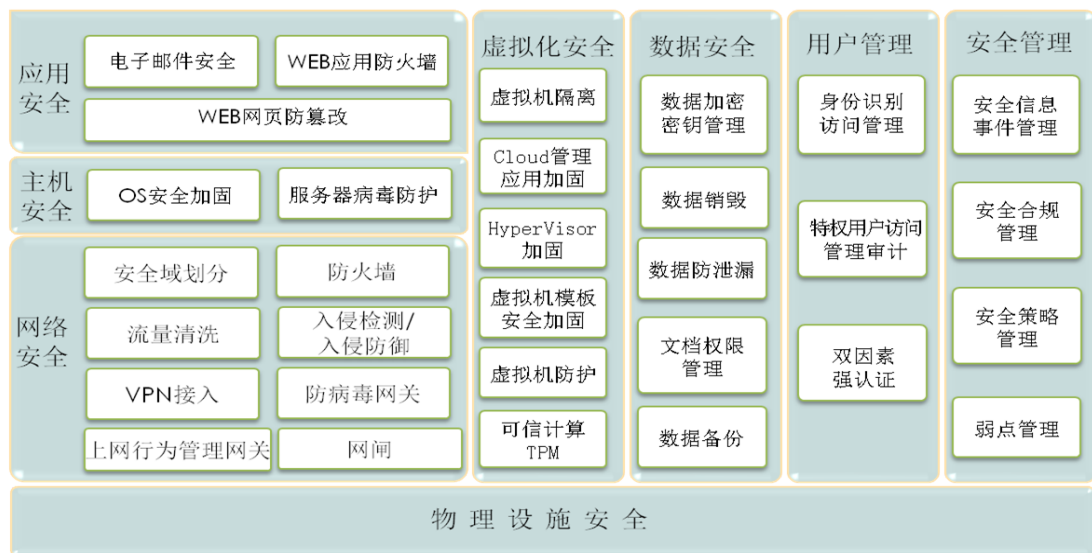


图 云数据中心安全技术架构

该架构中包含以下安全层面的能力：

- **物理设施安全**：通过门禁系统、视频监控、环境监控等实现数据中心环境、物理访问控制等确保物理设施层面的安全；
- **网络安全**：从防火墙、IPS、SSL VPN、Anti-DDoS、IDS/IPS、网闸等技术手段

确保 VDC 边界和 VDC 内部系统、数据和通信的隔离和安全，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

- **主机安全:** 保护主机层操作系统的安全，通过主机加固、防病毒软件、主机 IPS、主机补丁管理等技术手段确保主机免受攻击。

- **虚拟化安全:** 从虚拟机隔离、虚拟层加固、Cloud 管理应用加固、虚拟机防护、虚拟机可信计算等技术手段确保虚拟化的安全。

- **应用安全:** 从电子邮件防护、Web 应用防护等技术手段对应用层面的数据进行保护，保障用户的应用数据能够不受破坏、更改、泄漏、篡改。

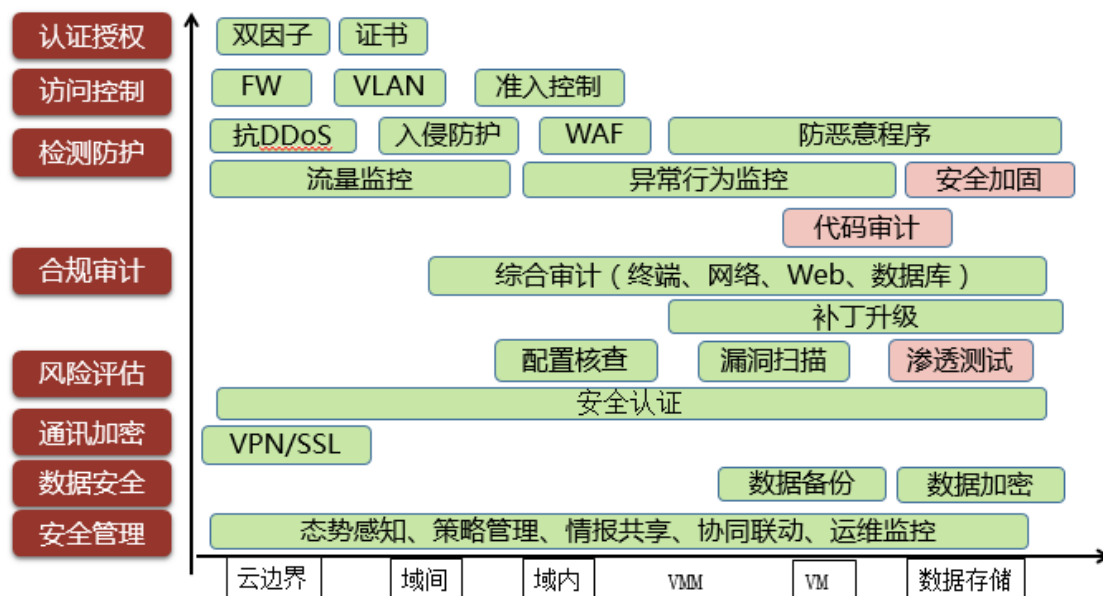
- **数据安全:** 从数据加密、数据销毁、数据防泄漏、数据备份等技术手段保障数据安全。

- **用户管理:** 通过统一认证、授权、访问控制、特权用户访问审计、双因素认证等保障用户管理安全。

- **安全管理:** 通过安全信息时间管理、安全合规审计、安全策略统一管理、弱点管理等进行统一安全管理。

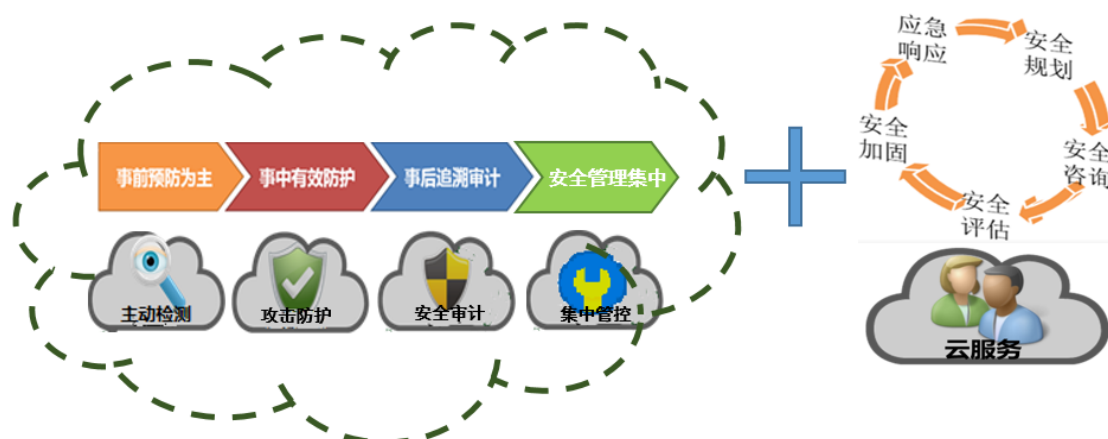
3.4. IDC 安全防护模型（安恒）

为了保证 IDC 安全建设方案的完整和全面，需要对安全防护措施建立理论模型，然后在理论模型的指导下指定具体的建设方案。通常安全防护可以从安全措施功能域以及安全措施部署的位置两个维度来考虑。这里给出云计算环境下，安全防护需求的参考模型。



按照云计算环境的拓扑架构，可以划分为云边界、专业（功能）域、域内、VMM、虚拟机、数据存储等几个层次。而安全措施功能可以划分为认证授权、访问控制、检测防护、合规审计、风险评估、通讯加密、数据安全、安全管理等八个功能类别。其中大部分可以通过部署安全产品来实现，图中用绿色方块表示。少数粉色方块代表安全服务。

3.5. 分阶段防护思路



主动检测：对云平台中数据采集、网络接入，信息接收等初始阶段开始跟踪监测，特别是网站的风险漏洞、敏感信息、系统漏洞、数据库弱点、配置信息，防护于未然，守住云平台的“第一道门”。

攻击防护: 保障数据在接入层、传输层、平台层、应用层、操作层的安全传输、交换和存储。全方位抵御各类攻击，保障云平台安全运转，最大限度的实现御敌于边界之外。计算内资源进行东西向流量管控，防虚拟机逃逸。

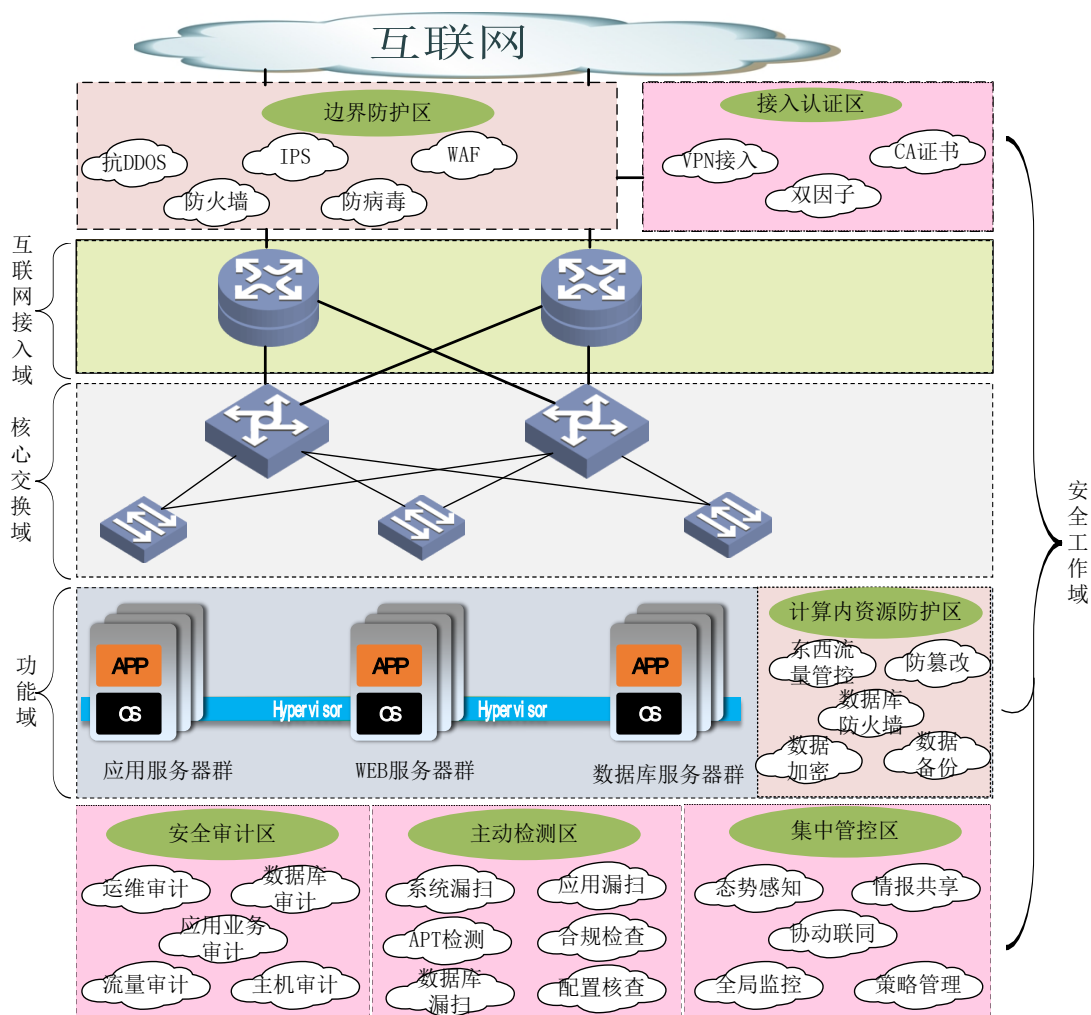
安全审计: 通过对云平台日志、数据库操作、运维动作、流量情况细粒度的访问行为审计和精细化操作规则的匹配，第一时间提供云平台非法行为的取证，确保安全事件爆发后的有据可查、有源可溯，形成云平台多角度、全方位的“监控系统”。

集中管控: 通过对平台运行情况的实时监控、数据汇总，把握云平台健康状态。制定周期性检查计划、及时发现安全弱点，及时整改。通过实施审计信息和边界防护设施回馈实时发现攻击行为，对安全事件快速响应。同时共享外界威胁情报，结合自身安全状态分析。

云服务: 通过专业的安全工具、白客级的专家团队，对云平台的应用系统进行常规渗透测试安全评估、全面的风险分析、及时的应急响应，对应用安全事件进行成因分析、应急修复，担当云平台实时响应的“专职医生”。

4. 解决方案

根据分阶段防护思路，在 IDC 数据中心中划分安全工作域，分为接入认证区、边界防护区、计算内资源防护区、安全审计区、主动检测区、集中管控区五大区域。如下图如示：



其中整个解决方案分为两部分进行介绍，一部分为天融信安全系统，天融信负责接入认证区和边界防护区，采用天融信安全云平台，负责互联网出口、核心区、业务接入区的边界防护管理。一部分为安恒安全系统，安恒负责内部资源防护、安全审计、主动检测、集中管控等区域。

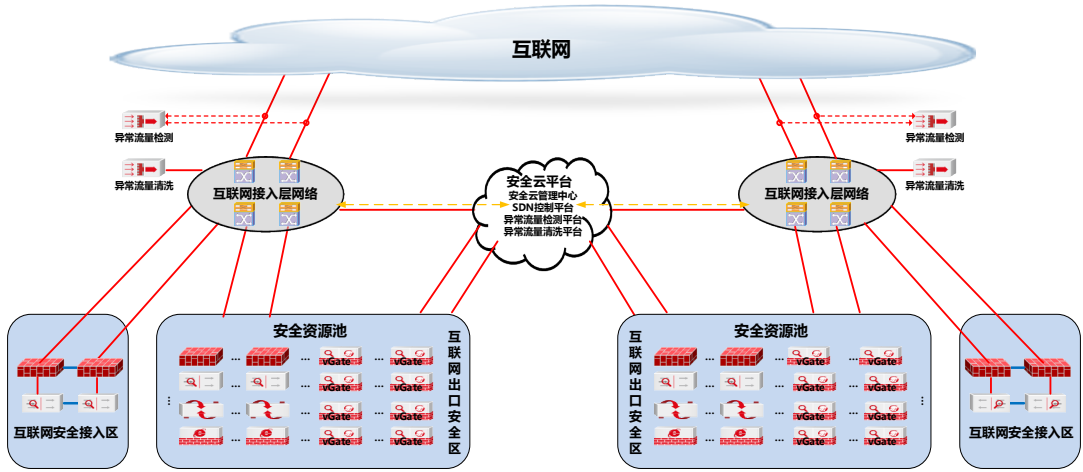
4.1. 天融信安全系统

4.1.1. 互联网接入层

互联网接入层是整个 IDC 业务的出口，承担着抵御 DDOS 攻击和保证带宽正常可用及 IDC 业务可正常访问的重任，重点需防治 DDOS 攻击造成的带

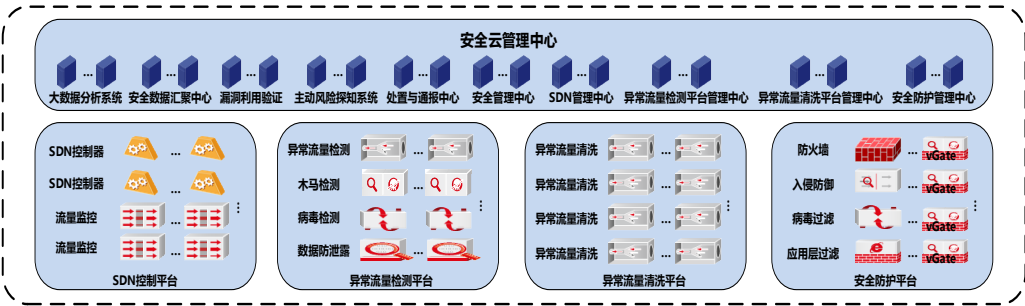
宽或主机资源被大量消耗。

通过对网络安全设施资源及业务能力进行云化，形成安全资源池，并为客户提供按需的网络安全服务，从而实现网络安全即服务的一种技术和业务模式。



4.1.1.1. 安全云平台

安全云平台由安全云管理中心、SDN 控制平台、异常流量检测平台、异常流量清洗平台、安全防护平台组成。



4.1.1.1.1. 安全云管理中心

安全云管理中心

以风险管理为视角，收集云数据中心互联网接入层的各类安全产品的审计信息和日志记录，通过事件关联分析，挖掘表面不相关信息之间的安全隐患或攻击行为。最终以图形化的方式展示系统安全态势，以各类统计信息、排名方式和工单下达的方式辅助安全管理人员进行安全管理活动。

SDN 管理中心

SDN 管理中心，同时管理多台 SDN 控制器。提供对不同类流量的监控，为运行在控制器上的物理网络和多个虚拟网络提供可视化。能够动态地创建基于策略的虚拟网络，这些虚拟的网络能够形成逻辑的网络资源池。

异常流量检测平台管理中心

异常流量检测平台管理中心，同时管理多台异常流量检测、木马检测、病毒检测、病毒检测、数据防泄露等设备。对流量实时监控，发现异常流量。将异常 IP 地址发送到异常流量清洗平台管理中心进行处置。

异常流量清洗平台管理中心

异常流量清洗平台管理中心，同时管理多台异常流量清洗设备。异常 IP 地址的数据流将通过异常流量清洗平台进行处置。

安全防护平台管理中心

安全防护平台管理中心，同时管理多台防火墙、入侵防御、病毒过滤、应用层过滤等硬件网关设备服务资源池，以及虚拟化(vGate 软件)网关服务资源池。

主动风险探知系统

采用各种主动探知技术，依托数据分析建模，结合各种安全情报机制，帮助用户全面、准确掌握自己的所辖网络中资产、应用的基本情况和安全状态。

- **构建基础资产信息库：**系统通过各种主动探测技术对数据中心的目标网络进行探测，发现目标网络中存在的资产并实时更新资产信息，包括但不限于开放的端口、开放的服务、操作系统类型、设备类型、厂商、型号、承载的各种应用以及漏洞信息等，构建并形成基础资产信息库。用户可以通过目标特征快速从基础资产信息库中找到所关注的资产，并了解其详情并掌握实时变化情况。
- **绘制信息安全底图：**系统能够基于基础资产信息库对用户所关注的安全问题绘制信息安全底图，帮助用户了解风险在网络中的影响情况。例如某个特定漏洞，用户缺少检测手段但却希望知道这些漏洞所影响

的资产特征时，就可以通过绘制信息安全底图，迅速检索到漏洞影响的所有资产，并给出对应的统计图表，供用户了解风险影响的资产数量、涉及的业务系统等。

漏洞验证与利用

对于目标网络中所发现的漏洞，判断其是否真实有效，可被利用。系统能够基于预置的各种漏洞利用验证模板，用户只需建立验证任务，系统便能对目标网络的漏洞进行自动化的验证，极大提高验证效率并降低对验证人员技能要求。

处置与通报中心

为数据中心运维人员、内部(自用)用户、重要服务对象（租户）用户，提供安全事件的处置与通报服务。

- 数据中心运维人员，可获取网络安全事件、网络安全信息通报。
- 内部(自用)用户，可通过平台来获取与其单位相关的网络安全事件、网络安全信息通报，并向平台提供安全事件处置结果反馈等。
- 重要服务对象（租户）用户，可通过平台来获取与其单位相关的网络安全事件、网络安全信息通报，并向平台提供安全事件处置结果反馈等。重要行业和服务对象用户包括但不限于电商、银行、政府等多个行业的具体用户。

安全数据汇聚中心

大数据基础架构为整个平台提供大数据的采集、存储、分布式分析框架等基础功能，其包含数据采集层、数据存储层、数据汇总层、预处理数据、计算框架等部分。

大数据分析系统

提供多种不同的数据分析方法，可实时分析与事后分析，此外还提供一套可视化的与存储无关的挖掘分析工具，可灵活调整分析过程，发现数据价值。平台采用分布式技术提升存储与分析性能的同时，提供一套数据展示平台及丰富的数据展示组件，便于管理者获取分析结果。

以上内容仅为本文档的试下载部分,为可阅读页数的一半内容。

如要下载或阅读全文, 请访问:

<https://d.book118.com/095040342132011341>