第5章 云安全

本章主要介绍云计算中产生的安全问题，首先介绍什么是云安全及云安全的相关术语；其次向读者展示目前有哪些常见的云安全威胁，以便及时防范；再次说明实现云安全的防护策略；最后提到4个典型的云安全应用及要实现云应用需要解决的问题。通过对本章的学习，读者应能够对云安全有详细的了解，并且对其应用有一定的认识。

5.1 基本术语与概念

虽然虚拟化和云计算可以帮助企业打破IT基础设施与其用户之间的黏合性，但随之带来的安全威胁也严重影响了这种新的计算模式得到用户的认可。云计算资源共享的特性促使人们尤其关心安全问题，例如，云计算中心本身安全不安全、如何获得安全的云服务、云计算为改善安全能做出什么贡献等，都已成为云计算研究中关于安全的热点话题。如图5.1所示为云安全。

对SaaS提供商尤其如此。例如，在云计算中，用户在某些方面失去了对资源的控制，因此必须重新评估用户自身的安全模式。

图5.1 云安全

和云计算的定义一样，关于云安全也没有统一的定义，但基本上都差不多。总而言之，云安全就是确保用户在稳定和私密的情况下在云计算中心上运行应用，并保证存储于云中的数据的完整性和机密性。

云安全是我国企业提出的概念，在国际云计算领域独树一帜。“云安全”(cloud security)计划是网络时代信息安全的最新体现，它融合了并行处理、网格计算、未知病毒行为判断(通过网状的大量客户端对网络中软件行为的异常监测，获取互联网中木马、恶意程序的最新信息，传送到Server端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端)等新兴技术和概念。

未来杀毒软件将无法有效地处理日益增多的恶意程序。来自互联网的主要威胁正在由计算机病毒转向恶意程序及木马，在这样的情况下，采用特征库判别法显然已经过时。在云安全技术应用后，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络

服务，实时进行采集、分析以及处理。整个互联网就是一个巨大的“杀毒软件”，参与者越多，每个参与者就越安全，整个互联网就会更安全。

在云安全的概念提出后，曾引起广泛的争议，许多人认为它是伪命题。但事实胜于雄辩，瑞星、趋势、卡巴斯基、McAfee、Symantec、江民科技、Panda、金山、360 安全卫士等都推出了云安全解决方案。瑞星基于云安全策略开发的产品，每天拦截数百万次木马攻击，其中在 2009 年 1 月 8 日更是达到了 765 万余次。趋势科技云安全已经在全球建立了 5 大数据中心、几万部在线服务器。其云安全可以支持平均每天 55 亿条点击查询，每天收集、分析 2.5 亿个样本，资料库第一次命中率就可以达到 99%。而且借助云安全，趋势科技现在每天阻断的病毒感染最高达 1000 万次。

5.2 云安全威胁

在将应用和数据迁移到云端这件事上，对安全问题需要加以密切关注。最小化云端安全风险的第一步就是要认清那些顶级安全威胁。

云安全联盟（Cloud Security Alliance，CSA）指出，云服务天生就能使用户绕过公司范围内的安全策略，建立起自己的影子 IT 项目服务账户。新的安全控制策略必须被引入。下面是云安全联盟列出的 11 项云安全威胁。

1. 数据泄露

云环境面对的威胁中有很多与传统企业网络面对的威胁相同，但由于有大量数据存储在云服务器上，云提供商便成为黑客很喜欢下手的目标。万一受到攻击，潜在损害的严重性取决于所泄露数据的敏感性。个人财务信息泄露事件或许会登上新闻头条，但涉及健康信息、商业机密和知识产权的数据泄露却有可能更具毁灭性的打击。图 5.2 是 2018 年数据安全泄露事件行业占比，从图中可以看出，涉及个人敏感信息泄露情况涵盖了各个行业。其中个人信息泄露涉及的 Top 5 的行业为互联网公司、金融机构、电商、政府机构、医疗，占全部信息泄露事件的 66%，成为个人敏感信息泄露的重灾区。这些行业基本上都涉及企业和公民的身份信息、社交信息、资金和财务信息，数据价值较高，泄露之后造成的危害和影响也特别大。其中，互联网行业之所以会成为敏感信息泄露最严重的行业，根本原因在于互联网行

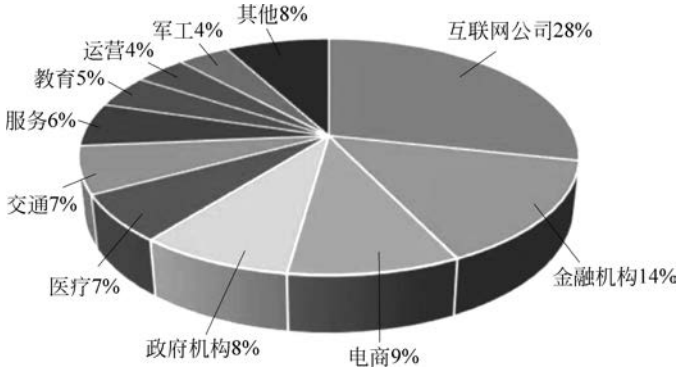

图 5.2　2018 年数据安全泄露事件行业占比

业面对的用户最多最广，网络访问也最为开放。而多数互联网公司在数据及客户群发展壮大以后才发现数据安全问题，而此时海量数据已经形成，且还在持续不断地增长，面对海量数据及复杂的应用环境，互联网公司没有重视并积极应对数据安全问题。

云服务提供商通常都会部署安全控制措施来保护云环境，但最终保护自身云端数据的责任还是要落在使用云服务的公司自己身上。

2. 凭证被盗和身份验证

数据泄露和其他攻击通常都是由于身份验证不严格、弱密码横行、密钥或凭证管理松散的结果。企业在试图根据用户角色分配恰当权限的时候，通常都会陷入身份管理的泥潭，更糟糕的是，他们有时还会在工作职能改变或用户离职时忘了撤销相关用户的权限。

多因子身份验证系统，如一次性密码、基于手机的身份验证、智能卡等，可以有效地保护云服务。因为有了多重验证，攻击者想要靠盗取的密码登进系统就难多了。在美国第二大医疗保险公司 Anthem 的数据泄露事件中，超过 8000 万客户记录被盗，就是用户凭证被窃的结果。Anthem 没有采用多因子身份验证，因此一旦攻击者获得了凭证，进出系统如入无人之境。

将凭证和密钥嵌入源代码里，并留在面向公众的代码库（如 GitHub）中，也是很多开发者常犯的错误。

3. 界面和 API 被黑

基本上，现在每个云服务和云应用都提供应用编程接口（API）。IT 团队使用界面和 API 进行云服务的管理与互动，服务开通、管理、配置和监测都可以借助这些界面和接口完成。

从身份验证和访问控制到加密和行为监测，云服务的安全和可用性依赖于 API 的安全性。由于企业可能需要开放更多的服务和凭证，建立在这些界面和 API 基础之上的第三方应用的风险也就随之增加。弱界面和有漏洞的 API 将使企业面临很多安全问题，如机密性、完整性、可用性和可靠性都会受到考验。API 和界面通常都可以从公网访问，也就成为系统最暴露的部分。如图 5.3 所示，攻击者可通过 App 的各种 API 接口入侵云平台服务器。

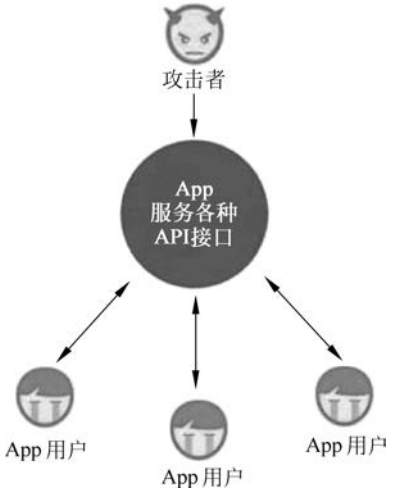

图 5.3　接口入侵云平台服务器

4. 系统漏洞

系统漏洞或程序中可供利用的漏洞是人们司空见惯的。但是，随着云计算中多租户的出现，这些漏洞的问题也随之增大。企业共享内存、数据库和其他资源，也催生出了新的攻击方式。最佳实践包括定期漏洞扫描、及时补丁管理和紧跟系统威胁报告。如图 5.4 所示的是 360 安全卫士正在快速修复系统漏洞。

图 5.4　360 安全卫士快速修复系统漏洞

修复系统漏洞的花费与其他 IT 支出相比要少一些，部署 IT 过程来发现和修复漏洞的开销比漏洞遭受攻击的潜在损害要小很多。

5. 账户劫持

如图 5.5 所示，网络钓鱼、诈骗、利用软件漏洞是目前很普遍的攻击方式，而云服务的出现又为此类威胁增加了新的难度，因为攻击者可以利用云服务窃听用户活动、操纵交易、修改数据。利用云应用发起其他攻击也不无可能，常见的深度防护保护策略能够控制数据泄露引发的破坏。

图 5.5　网络钓鱼

6. 恶意内部人士

现员工或前雇员、系统管理员、承包商、商业合作伙伴的恶意行为可以从单纯的数据偷盗到报复公司。根据 Verizon 的 2020 数据泄露调查报告，在金融和保险行业中，内部攻击的占比相对较大，尽管报告中显示“滥用权责”的比例大幅度下降，但并不表示现实中这类现

象有所缓和，依然需要引起重视。

7. 高级持续性威胁(APT)寄生虫

APT 通常在整个网络内逡巡，混入正常流量中，因此它们很难被侦测到。主要云提供商应用高级技术阻止 APT 渗透进他们的基础设施，客户也必须像在内部系统里进行的那样，勤于检测云账户中的 APT 活动。

常见的切入点包括鱼叉式网络钓鱼、直接攻击、U 盘预载恶意软件和通过已经被黑的第三方网络。

8. 永久的数据丢失

随着云服务的成熟，由提供商失误导致的永久数据丢失已经极少见了，但恶意黑客会永久删除云端数据来危害云安全，而且云数据中心跟其他任何设施一样对自然灾害无能为力。

云服务提供商建议多地分布式部署数据和应用，以增强防护，足够的数据备份措施和灾难恢复是最基本的防范永久数据丢失的方法。

预防数据丢失的责任并非全部在云服务提供商身上。如果客户在上传数据到云端之前先把数据加密，那保护好密钥的责任就落在客户自己身上了。一旦密钥丢失，数据丢失就在所难免。

合规策略通常都会规定企业必须保留审计记录和其他文件的时限。此类数据若丢失，会产生严重的监管后果。在新的欧盟数据保护规定中，数据损毁和个人数据损坏也被视为数据泄露，需要进行恰当的通知。

9. 云服务滥用

云服务可能被用于支持违法活动，例如，利用云计算资源破解密钥、发起分布式拒绝服务(distributed denial of service，DDoS)攻击、发送垃圾邮件和钓鱼邮件、托管恶意内容等。

提供商要能识别出滥用类型，例如，通过检查流量识别出 DDoS 攻击，还要为客户提供监测他们的云环境是否健康的工具。客户要确保提供商拥有识别服务滥用的报告机制。尽管客户可能不是恶意活动的直接猎物，云服务滥用依然可能造成服务可用性问题和数据丢失问题。

10. 拒绝服务(DoS)攻击

如图 5.6 所示，拒绝服务(Denial of Service，DoS)攻击的方式之一是向一个子网的广播地址发一个带有特定请求(如 ICMP 回应请求)的包，并且将源地址伪装成想要攻击的主机地址。子网上的所有主机都回应广播包请求而向被攻击主机发包，使该主机受到攻击。

DoS 攻击通常会影响系统可用性，系统响应会被大幅度拖慢甚至直接超时，能给攻击者带来很好的攻击效果。

DoS 攻击消耗大量的处理能力，最终都要由用户买单。尽管高流量的 DDoS 攻击如今更常见，企业仍然要留意非对称的、应用级的 DoS 攻击，保护好自己的 Web 服务器和数据库。

在处理 DoS 攻击上，云服务提供商一般都比用户更有经验、准备更充分，关键在于攻击

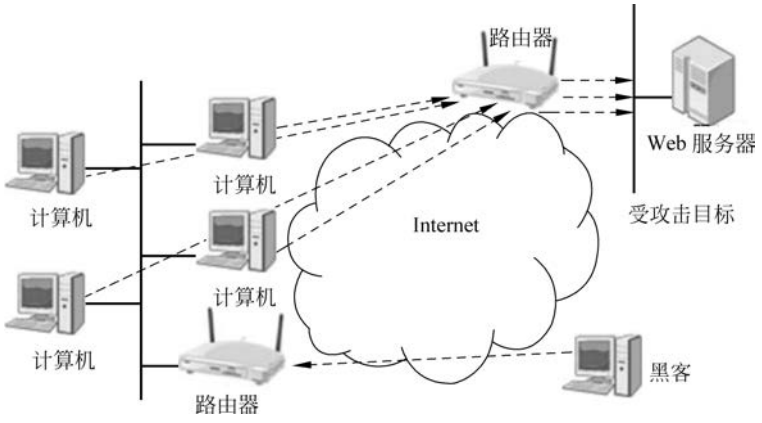

图 5.6　DoS 攻击方式

发生前要有缓解计划，这样管理员才能在需要的时候访问到这些资源。

11. 共享技术，共享危险

共享技术中的漏洞给云计算带来了相当大的威胁。云服务提供商共享基础设施、平台和应用，一旦其中任何一个层级出现漏洞，每个人都会受到影响。一个漏洞或错误配置可能导致整个提供商的云环境遭到破坏。

若一个内部组件被攻破，如一个管理程序、一个共享平台组件或一个应用，则整个环境都会面临潜在的宕机或数据泄露风险。

5.3　云安全防护策略

云安全涉及的关键技术及风险应对策略包括基础设施安全、数据安全、应用安全和虚拟化安全 4 方面。

5.3.1　基础设施安全

云计算模式的基础是云基础设施，承载服务的应用和平台等均建立在云基础设施上，确保云计算环境中用户数据和应用安全的基础是要保证服务的底层支撑体系（即云基础设施）的安全和可信。表 5.1 为分别在传统环境下和云计算环境下对云基础设施安全性的相关服务特性进行的对比。

表 5.1　云基础设施安全性的相关服务特性的对比

分 析 角 度	传统环境下的情况	云计算环境下的情况
网络开放程度	网页服务器、邮件服务器等接口暴露在外，设置访问控制、防火墙等防护措施，维护安全	用户部署的系统完全暴露在网络中，任何节点都可能遭受攻击
平台管理模式	部署的系统通过内部管理员管理	利用多样化网络接入设备远程管理，涉及网络通信协议、网页浏览器、SSH 登录等服务

续表

分析角度	传统环境下的情况	云计算环境下的情况
资源共享方式	一台物理主机对应一个用户	多个用户同时共享IT资源，用户之间需要进行有效的隔离
服务迁移要求	不存在服务迁移问题	单个云提供商提供给用户的服务应当可灵活迁移，以达到负载均衡并有效利用资源。同时，用户希望在多个云提供商之间灵活地迁移服务和数据
服务灵活程度	一旦拥有，便一直拥有，容易造成资源浪费	按需伸缩的服务，保证服务随时可用、可终止、可扩展、可缩减

如何确保基础设施层的安全，可以从以下几方面进行考虑。

1. 数据可控及数据隔离

对于数据泄露风险而言，解决此类风险主要通过数据隔离方法，可以通过以下途径来实现数据隔离。

(1) 让客户控制他们需要使用的网络策略和安全。

(2) 从存储方面来说，客户的数据应该存储在虚拟设备中。由于实际上虚拟存储器位于更大的存储阵列上，所以采取虚拟存储，可以在底层进行数据隔离，保证每个客户只能看到自己对应的数据。

(3) 在虚拟化技术实现中，可以考虑大规模地部署虚拟机以实现更好的隔离及使用虚拟的存储文件系统，如VMware的VMFS文件系统。

2. 综合考虑数据中心的软/硬件部署

在软/硬件的选用中，考虑品牌厂商，硬件的选择要综合考虑质量、品牌、易用性、价格、可维护性等一系列因素，并选择性价比高的产品。

3. 建立安全的远程管理机制

根据定义，IaaS资源在远端，因此用户需要远程管理机制。最常用的远程管理机制如下。

(1) VPN：提供一个到IaaS资源的安全连接。

(2) 远程桌面、远程Shell：最常见的解决方案是SSH。

(3) Web控制台UI：提供一个自定义远程管理界面，通常是由云服务提供商开发的自定义界面。

对应的安全策略如下。

(1) 缓解认证威胁的最佳办法是使用双因子认证，使用动态共享密钥或缩短共享密钥的共享期。

(2) 不要依赖于可重复使用的用户名和密码。

(3) 确保安全补丁及时打上。

(4) 对于自身无法保护传输数据安全的程序而言，应该使用VPN或安全隧道(SSL/TLS或SSH)，推荐首先使用IPSec，然后是SSLv3或TLSv1。

4. 选择安全的虚拟化厂商及成熟的技术

选择有持续的支持及对安全长期关注的厂商，定期更新虚拟化安全补丁，并关注虚拟化安全。成熟的虚拟化技术不仅能够预防风险，在很大程度上还能增强系统安全性，如VMware对有问题虚拟机的隔离、DRS系统动态调度等。

5. 建立、健全IT行业法规

在云计算环境下，用户不知道自己的数据放在哪里，因而会有一定的焦虑，如数据的位置、安全性等疑问。

在IaaS环境下，由于虚拟机具有漂移特性，用户在很大程度上不知道数据到底存放在哪个服务器。另外，由于数据的独有特点，一旦为别人所知，价值便会急剧降低。这需要从法律、技术两个角度来规范。

（1）建立、健全法律，对数据泄露、IT从业人员的不道德行为进行严格约束，从人为角度防止出现数据泄露等不安全现象。

（2）开发虚拟机漂移追踪技术、IaaS下数据独特加密技术，让用户可以追踪自己的数据，感知到数据存储的安全。

6. 针对突然的服务中断等不可抗拒因素采取异地容灾策略

服务中断等风险存在于任何IT环境中，在部署云计算数据中心时，最好采取基于异地容灾的策略，进行数据与环境的备份。在该环境下，一旦生产中心发生毁坏，可以启用异地灾备中心对外服务，由于数据需要恢复，用户感觉到服务中断，但短时间内会恢复，不会造成严重事故。

5.3.2 数据安全

企业数据安全和隐私保护是云用户最关心的安全服务目标，无论是云用户还是云服务提供商，都应避免数据丢失和被窃，不管使用哪种云计算的服务模式（SaaS/PaaS/IaaS），数据安全都变得越来越重要。从数据安全生命周期和云应用数据流程综合考虑，针对数据传输安全、数据存储和数据残留等云数据安全敏感阶段进行关键技术的分析。

1. 数据传输安全

当云用户或企业把数据通过网络传到公有云时，数据可能会被黑客窃取和篡改，数据的保密性、完整性、可用性、真实性受到严重威胁，给云用户带来不可估量的商业损失。

数据安全传输防护策略是首先对传输的数据进行加密，其次使用安全传输协议SSL和VPN进行数据传输。

2. 数据存储

云用户在云服务提供商存储数据时存在数据滥用、存储位置隔离、灾难恢复、数据审计等安全风险。

（1）对于IaaS应用而言，可以采用静止数据加密的方式防止被云服务提供商、恶意邻

居租户及某些应用滥用，但对于 PaaS 或者 SaaS 应用，数据是不能被加密的，密文数据会影响应用索引和搜索。如图 5.7 所示是同态加密安全的方案之一，到目前为止还没有可商用的算法实现数据同态加密。

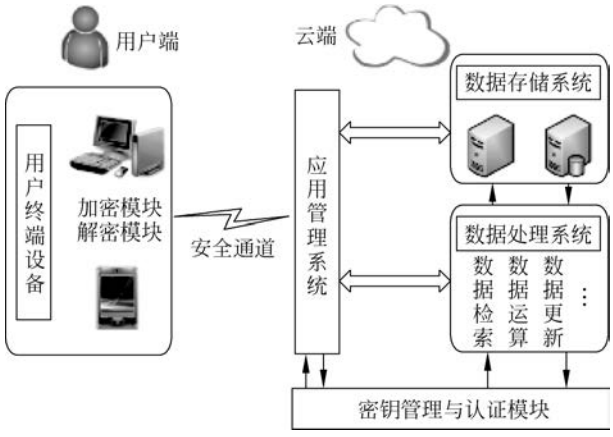

图 5.7　同态加密安全的方案之一

(2) 对于数据存储位置而言，云用户要坚持一个关于数据具体位置的基本原则，确保有能力知道存储的地理位置，并在服务水平协议 SLA 和合同中约定。在地理位置定义和强制执行方面，需要有适当的控制来保证。

(3) 采用“数据标记”、单租户专用数据平台实现数据隔离，防止数据被非法访问，但 PaaS 和 SaaS 应用为了实现可扩展、可用性、管理及运行效率等方面的“经济性”，云服务提供商基本上都采用多租户模式，无法实现单租户专用数据平台，唯一可行的办法是建立私有云，不要把任何重要的或者敏感的数据放到公有云中。

(4) 采用数据多备份的方式实现数据恢复，通过外部审计和安全认证实现数据完整性和可用性。

3. 数据残留

数据残留是数据在被以某种形式擦除后所残留的物理表现，存储介质被擦除后可能留有一些物理特性使数据能够被重建。在云计算环境中，数据残留有可能会无意地泄露敏感信息。

因此，云服务提供商应通过销毁加密数据相关介质、销毁存储介质、磁盘擦拭、内容发现等技术和方法来保证数据的完整清除。

5.3.3　应用安全

云环境的灵活性、开放性及公众可用性等特性给应用安全带来了很多挑战，因此云提供商在云主机上部署的 Web 应用程序应当充分考虑来自互联网的威胁。

1. 终端客户安全

为了保证云应用安全，云客户端应该保证自己的计算机安全，防护措施如下。

（1）在云客户端上部署反恶意软件、防病毒、个人防火墙及IPS类型安全软件，并开启各项防御功能。

（2）云用户应该采取必要措施保护浏览器免受攻击，在云环境中实现端到端的安全。云用户应使用自动更新功能，定期完成浏览器的打补丁和更新工作。

（3）对于企业客户来说，应该从制度上规定连接云计算应用的计算机禁止安装虚拟机，并且对计算机进行定期检查。

2. SaaS应用安全

SaaS应用提供给用户的是使用服务商运行在云基础设施之上的应用，用户使用各种客户端设备通过浏览器来访问应用。用户并不管理或控制底层的云基础设施，如网络、服务器、操作系统、存储甚至其中单个的应用能力。

在SaaS服务模式下，提供商应最大限度地确保提供给客户的应用程序和组件的安全，客户端只负责用户与访问管理安全，所以在选择SaaS提供商前要从如下几方面对其进行安全评估。

（1）根据保密协议，要求SaaS提供商提供包括设计、架构、开发、黑盒与白盒应用程序安全测试和发布管理有关的安全实践的信息，甚至有必要请第三方安全厂商进行渗透测试（黑盒安全测试），以获得更为翔实的安全信息。

（2）特别要注意SaaS提供商提供的身份验证和访问控制功能，它是客户管理信息风险唯一的安全控制措施。用户应该尽量了解云特定访问控制机制，并采取必要措施，保护在云中的数据；应实施最小化特权访问管理，以消除威胁云应用安全的内部因素。同时，要求云服务提供商能够提供高强度密码；定期修改密码，时间长度必须基于数据的敏感程度；不能使用旧密码等。

（3）用户应理解SaaS提供商使用的虚拟数据存储架构和预防机制，以保证多租户在一个虚拟环境中所需要的隔离。SaaS提供商应在整个软件生命开发周期过程中加强软件安全性上的措施。

3. PaaS应用安全

PaaS云提供商提供给用户的能力是在云基础设施之上部署用户创建或采购的应用，这些应用使用服务商支持的编程语言或工具开发，用户并不管理或控制底层的云基础设施，包括网络、服务器、操作系统、存储等，但是可以控制部署的应用以及应用主机的某个环境配置。PaaS应用安全包含两个层次，即PaaS平台自身的安全和客户部署在PaaS平台上应用的安全。

（1）PaaS应提供负责包括运行引擎在内的平台软件及其底层的安全，用户只负责部署在PaaS平台上应用的安全。PaaS提供商采取可能的办法来缓解SSL攻击，避免应用被暴露在默认攻击之下，客户必须有一个变更管理项目，在应用提供商指导下进行正确的应用配置或打补丁，确保SSL补丁和变更程序是最新的。

（2）如果PaaS应用使用了第三方应用、组件或Web服务，那么第三方应用提供商需要负责这些服务的安全。用户需要了解自己的应用到底依赖于哪个服务，在采用第三方应用、组件或Web服务时，用户应对第三方应用提供商做风险评估，应尽可能地要求云服务提供

商增加信息透明度，以利于风险评估和安全管理。

（3）在多租户 PaaS 的服务模式中，用户应确保自己的数据只能由自己的企业用户和应用程序访问，要求 PaaS 服务商提供多租户应用隔离，负责维护 PaaS 平台运行引擎的安全，在多租户模式下提供“沙盒”架构，集中维护用户部署在 PaaS 平台上应用的保密性和完整性；负责监控新的程序缺陷和漏洞，以避免这些缺陷和漏洞被用来攻击 PaaS 平台和打破“沙盒”架构。

（4）用户部署的应用安全需要 PaaS 应用开发商配合，开发人员需要熟悉平台的 API、部署和管理执行的安全控制软件模块；必须熟悉平台被封装成安全对象和 Web 服务的安全特性，调用这些安全对象和 Web 服务实现在应用内配置认证和授权管理；必须熟悉应用的安全配置流程，改变应用的默认安装配置。

5.3.4　虚拟化安全

如图 5.8 所示，虚拟化对于云计算是至关重要的，而基于虚拟化技术的云计算主要存在两方面的安全风险，一个是虚拟化软件的安全；另一个是使用虚拟化技术的虚拟服务器的安全。

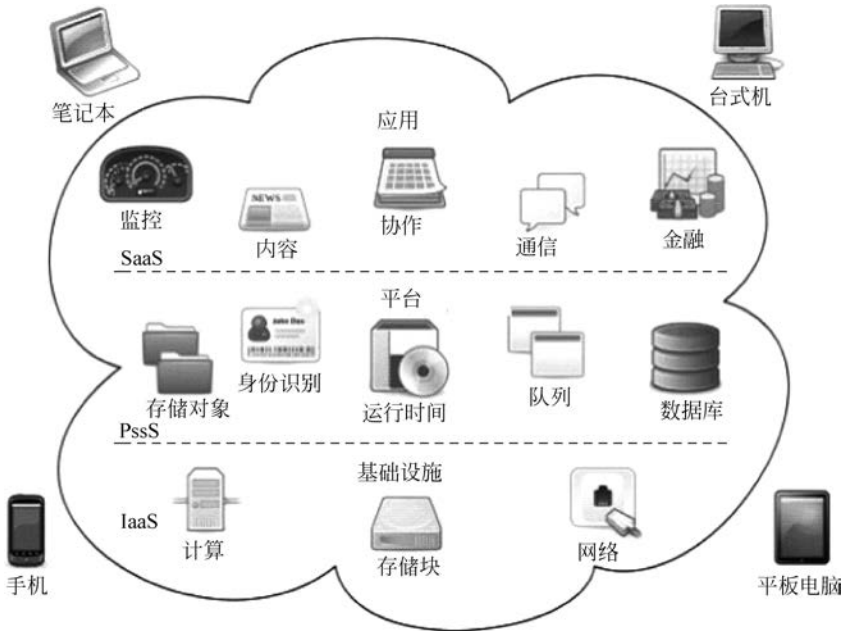

图 5.8　云计算的资源虚拟化

1. 虚拟化软件安全

虚拟化软件层直接部署于裸机之上，提供能够创建、运行和销毁虚拟服务器的能力。虚拟化软件层的完整性和可用性对保证基于虚拟化技术构建的公有云的完整性和可用性是最重要的，也是最关键的。

（1）选择无漏洞的虚拟化软件，一个有漏洞的虚拟化软件会暴露所有的业务域给恶意

的入侵者。

（2）必须严格限制任何未经授权的用户访问虚拟化软件层。云服务提供商应建立必要的安全控制措施，限制对于管理程序和其他形式的虚拟化层的物理和逻辑访问。

2. 虚拟服务器安全

虚拟服务器位于虚拟化软件之上，对物理服务器的安全原理与实践也可以被运用到虚拟服务器上，当然需要兼顾虚拟服务器的特点。以下将从物理服务器选择、虚拟服务器安全和日常管理3方面对虚拟服务器安全进行阐述。

（1）选择具有TPM安全模块的物理服务器，TPM安全模块可以在虚拟服务器启动时检测用户密码，如果发现密码及用户名的Hash序列不对，不允许启动此虚拟服务器；选用多核并支持虚拟技术的处理器，保证CPU之间的物理隔离，这样会减少许多安全问题。

（2）在构建服务器时，应为每台虚拟服务器分配一个独立的硬盘分区，以便将各个虚拟服务器从逻辑上隔离开来。虚拟服务器系统还应安装基于主机的防火墙、杀毒软件、IPS(IDS)以及日志记录和恢复软件，以便将它们相互隔离，并与其他安全防范措施一起构成多层次防范体系。

（3）虚拟服务器之间及其物理主机之间通过VLAN和IP进行网络逻辑隔离，服务器之间通过VPN进行网络连接。

（4）对虚拟服务器的运行状态进行严密的监控，实时监控各虚拟机中的系统日志和防火墙日志，以此来发现存在的安全隐患。另外，不需要运行的虚拟机应当立即关闭。

5.3.5 身份识别和访问管理

身份识别和访问管理系统(Identity and Access Management，IAM)能够对服务和资源的访问及权限进行管理。在一个租户下，通过IAM可以控制组织内不同用户及用户组对资源和访问的控制权限，从而保证数据和信息的安全性。那么对于云计算平台的IAM，主要从以下几方面体现其管理和控制。

（1）用户管理。管理用户及其访问权限，包括创建用户、为用户分配单独的安全凭证(如访问密钥、密码和多重身份验证设备)或要求提供临时安全凭证，以便为用户提供服务和资源的访问权限。通常可以管理各种权限，以便控制用户可以执行的操作。创建用户的步骤为创建用户→设置用户访问凭证→将用户设定用户组。使用用户组(用户集合)实现轻松管理，可以通过组向多个用户分配权限。例如，可以设置一个用户组，并向该组授予管理员通常需要的权限类型，该组中的任何用户均自动具有分配给该组的权限，如果有新用户加入该组，并且要具有管理员权限，则可将该用户添加到该组，分配相应的权限；同样，如果该组中有人改变工作，则不必编辑该用户的权限，只需从旧组中将其删除，然后将其添加到新组即可。

（2）角色管理。可通过IAM角色为通常没有权限访问组的资源的用户或产品授予访问权限。IAM用户或服务在担任角色之后可以获得用于调用API的临时安全凭证，因此不必为需要访问资源的每个实体提供长期凭证或定义权限。在跨租户/账户访问时，在某些情况下，一个账户的用户可能需要访问另一个账户/租户中的资源，因此需要该用户拥有每个账户的凭证，但势必会提升管理的复杂性，可以使用角色来解决这个问题。

(3) 权限管理。能够指定对资源的访问权限。权限授予用户、组和角色，在被授予前默认没有任何权限。也就是说，除非授予需要的权限，否则用户、组和角色无法进行任何操作。如果要为用户、组和角色提供权限，可以附加一条指定访问类型、可以执行的操作以及可以操作的资源的策略。此外，还可以针对允许访问或拒绝访问指定必须设置的条件。在策略中可以指定需要哪些操作、访问哪些资源、在什么条件下该策略生效等。

(4) 安全凭证管理。包括密码、访问密钥、密钥对、X.509 证书等，在通过 UI 访问或者 API 以及命令行访问时，会采用不同的凭证方式。在有些系统中，还可以通过强制使用多重身份验证(MFA)来进一步提高 IAM 用户访问的安全性，它能够在用户名称和密码之外再额外增加一层保护。当用户登录系统时，系统将要求其输入用户名和密码(第一安全要素，用户已知)以及来自其 MFA 设备的身份验证代码(第二安全要素，用户已有)。这些多重要素结合起来将为云平台账户设置和资源提供更高的安全保护。

5.3.6　操作系统安全

在云平台中的操作系统，为了避免病毒及黑客攻击，需要及时更新系统补丁，以保护和防止数据泄露。对于公有云来说，云平台可以提供操作系统安全补丁服务；对于私有云来说，则需要管理员借助自动化方式集中对补丁进行分级分发。云平台的自动化补丁功能具备以下能力。

(1) 支持在线及离线补丁下载模式，自动化完成补丁的下载及分类，提供过滤器过滤要下载的补丁类型。

(2) 用户在使用资源的过程中，可以选择需要的补丁进行自动化部署。

(3) 提供补丁分析能力，可以结合当前系统补丁集自动推荐补丁版本。

(4) 可以根据管理员自建的补丁黑名单或白名单来部署补丁。

(5) 能够自动发现补丁之间的依赖关系。

5.3.7　操作审计

审计是一项支持用户进行监管、合规性检查、操作审核和风险审核的模块。审计功能可以记录日志、持续监控，并保留与整个基础设施中的操作相关的账户活动。它提供账户活动的事件历史记录，这些活动包括通过管理控制台、命令行工具和其他服务执行的操作。这一事件历史记录可以简化安全性分析、资源更改跟踪和故障排除工作。审计具有以下功能。

(1) 合规更加简化：借助审计，可以自动记录和存储账户中已执行操作的事件日志，从而简化合规性审核。有些平台直接将审计数据记录到日志中，可以方便地搜索所有日志数据、识别不合规事件、加快事故调查速度并加快响应审核员请求的速度。

(2) 用户与资源活动的可见性：可通过记录管理控制台操作和 API 调用来提高用户和资源活动的可见性。

(3) 安全性分析和故障排除：借助审计，可以通过捕捉特定时段内账户中所发生更改的全面历史记录发现并解决安全性和操作性问题。

(4) 安全自动化：借助审计，可以跟踪并自动应对威胁云平台的资源安全性的账户活动。

5.4 典型的云安全应用

5.4.1 金山私有云安全平台

金山私有云安全平台是金山安全软件有限公司耗时三年研发的，基于智慧的云计算构架，可为客户提供专属的私有云安全定制化服务平台。金山私有云安全平台的技术和应用来自于百万企业级客户的成功应用实践，在全球首次将私有云技术引入客户端进行IT生产环境全面管控，是企业级客户信息数据的传输、应用、交互、存储等在内的数字化环境的安全管理平台、安全服务平台和安全应用扩展平台。借助这一平台及相关扩展应用，可为企业级客户提供整合的一体化的信息安全管理和服务。

金山私有云安全平台是一种完全的私有安全云。公有云安全技术必然存在信息与云端的交互和流动，这一过程中，还潜藏着新的安全风险。金山私有云平台将云安全技术引入企业级应用时，充分认识到这一问题，直接将公有云端平台的核心技术推进企业内部，变成企业私有云安全中心，有效避免了企业级用户机密信息泄露的潜在风险，并最大程度解决了企业对云技术的种种安全顾虑。

金山毒霸“云安全”有以下几个特点。

1. 掌控

私有云安全平台能够对用户内网环境中的所有文件进行安全标记，并以此为基础，确定IT环境的安全基线。根据安全基线知识库，管理员可以掌控对内部网络中的所有数据文件的安全属性，以此搭建可信可控的金山私有云安全基线。

2. 洞察

对任意计算机上出现的IT环境变化，私有云终端软件都会及时作出响应，并反馈至私有云中心平台，使得管理员能够洞察内部网络中所有文件的变化及安全属性的变化。

3. 提升

大量的计算量和内容资源都来自云网络，这使得安全客户端的资源消耗得到极大的降低。由于对抗手段的云端化，因此可以在云端构建很多鉴定技术，多角度、多素材、数据挖掘等方法可以使用，而这一切对病毒作者和黑客来说是“隐藏”的和快速变化的，这大大提高了对抗的门槛。对于新兴恶意攻击的快周期发布，只有云安全才可以做到秒级响应最新威胁，这样绝大部分用户都可以处于被保护之中。而传统的安全软件需要按天来等待厂商发布解决方案。

4. 优化

对内部网络计算机上出现的IT环境变化，私有云终端软件都会及时作出审计，并反馈至私有云中心平台，使得管理员能够根据审计报表，及时了解内部网络安全性状态，并以此为依据，调整基线安全策略，确保内网低风险平稳运行。

5.4.2　卡巴斯基的全功能安全防护

卡巴斯基实验室(Kaspersky Labs)是国际著名的信息安全领导厂商。其卡巴斯基安全软件主要针对家庭及个人用户,能够彻底保护用户计算机不受各类互联网威胁的侵害。图 5.9 是卡巴斯基 PURE 的主界面,其中包括数据备份和恢复、计算机保护、上网管理三大功能模块。

图 5.9　卡巴斯基 PURE 的主界面

卡巴斯基的全功能安全防护旨在为互联网信息搭建一个无缝、透明的安全体系。

1. 信息安全软件的功能平台化

针对互联网环境中类型多样的信息安全威胁,卡巴斯基实验室以反恶意程序引擎为核心,以技术集成为基础,实现了信息安全软件的功能平台化。系统安全、在线安全、内容过滤和反恶意程序等核心功能可以在全功能安全软件的平台上实现统一、有序和立体的安全防御。

2. 卡巴斯基安全网络

在强大的后台技术分析能力和在线透明交互模式的支持下,卡巴斯基全功能安全软件 2009 可以在用户"知情并同意"(awareness & approval)的情况下在线收集、分析(online realtime collecting & analysing)用户计算机中可疑的病毒和木马等恶意程序样本,并且通过平均每小时更新 1 次的全球反病毒数据库进行用户分发(instant solution distribution),从而实现病毒及木马等恶意程序的在线收集、即时分析及解决方案在线分发的"卡巴斯基安

全网络”，即云安全技术。

卡巴斯基安全网络是首个为满足个人和家庭需求而量身打造的安全服务解决方案。由于采用了获得专利的自适应性技术，该服务能够根据用户行为进行自我设置，不管用户使用何种设备。除了能够自适应跨平台情景外，这项服务还采用了卡巴斯基实验室屡获大奖的保护技术，能够全面抵御恶意程序和恶意网站，消除用户的隐私和在线支付风险，利用 VPN 对网络流量进行加密，通过密码管理器创建和存储高强度密码，保护用户在线安全。

3. 实现用户与技术后台的零距离对接

通过扁平化的服务体系实现用户与技术后台的零距离对接。卡巴斯基拥有全球领先的恶意程序样本中心及恶意程序分析平台，每小时更新的反病毒数据库能够保障用户计算机的安全防御能力与技术后台的零距离对接。在卡巴斯基的全功能安全防御体系中，所有用户都是互联网安全的主动参与者和安全技术革新的即时受惠者。

卡巴斯基混合云安全为用户使用云服务的任何阶段或场景提供统一的安全性。它适用于云迁移和原生云场景，可保护物理和虚拟化工作负载，无论是在本地、数据中心还是公共云中运行。因为它的应用程序是在考虑虚拟化和服务器功能的细节的情况下创建的，所以它可以提供完美平衡的保护来抵御当前和未来最先进的威胁，而不会影响系统性能。

5.4.3 瑞星“云安全”

2021 年瑞星“云安全”系统共截获病毒样本总量 1.19 亿个，病毒感染次数 2.59 亿次，病毒总体数量比 2020 年同期下降了 19.66%。报告期内，新增木马病毒 8050 万个，为第一大种类病毒，占到总体数量的 67.49%；排名第二的为蠕虫病毒，数量为 1652 万个，占总体数量的 13.85%；后门、灰色软件、感染型病毒分别占到总体数量的 8.75%、5.47% 和 3.76%，位列第三、第四和第五，除此以外还包括漏洞攻击和其他类型病毒。

1. 安全云终端软件

瑞星安全云终端软件的定位是政府及企业单机环境、互联网小企业以及个人家庭群组用户，秉承着企业级产品功能严谨、测试严格、升级慎重、安全性、稳定性以及绝对无捆绑无广告无弹窗、绝对不收集用户信息的原则，同时又在用户体验上做足了功夫。超轻的客户端、极低资源占用、亲切友好的操作界面、极好的防护效果等都是为此类用户群体量身定做。

产品主要由主程序、计算机监控系统、主动防御系统、安装升级卸载程序四部分组成。它是一款无捆绑无推送的纯粹干净的安全软件，用户在此防护体系下能够安全地进行文件访问，浏览 Internet 和收发电子邮件等操作，为用户提供了全方位的保护，保证用户的数据安全，同时防止计算机被病毒侵害。

2. 虚拟化恶意代码防护系统

瑞星虚拟化恶意代码防护系统是瑞星公司推出的国内首家企业级云安全防护解决方案，支持对虚拟化环境与非虚拟化环境的统一管控，包括 VMware vSphere、VMware NSX、HUAWEI FusionSphere、浪潮 InCloud Sphere、Windows 系统与 Linux 系统等，可以有效保障企业内部虚拟系统和实体网络环境不受病毒侵扰。

如图 5.10 所示，瑞星虚拟化恶意代码防护系统的完整防护体系由管理中心、升级中心、日志中心、扫描服务器、安全虚拟设备、安全终端 Linux 杀毒和安全防护终端等子系统组成，各个子系统均包括若干不同的模块，除承担各自的任务外，还与其他子系统通信，协同工作，共同完成企业内部的安全防护。

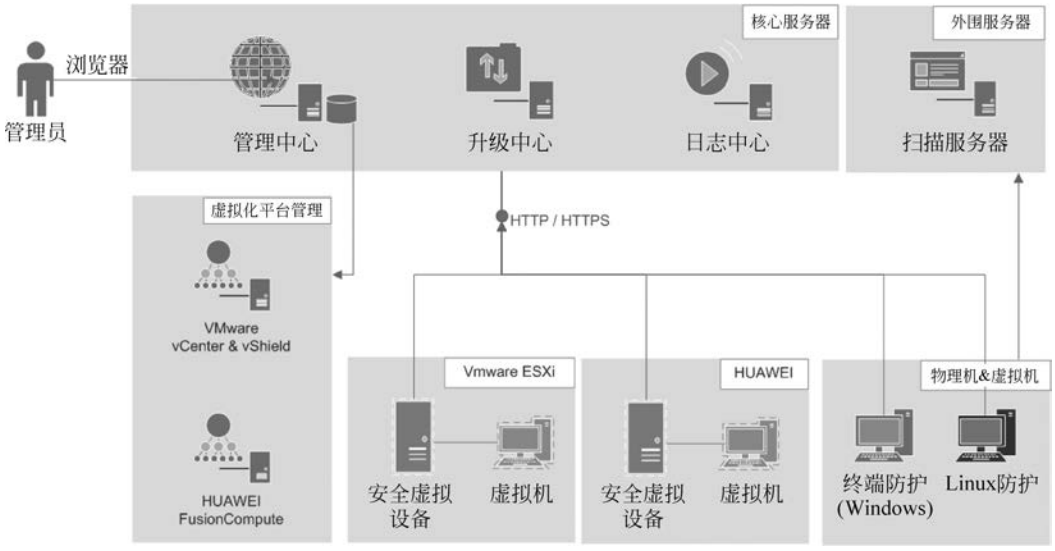

图 5.10　瑞星虚拟化恶意代码防护系统

瑞星建立“云安全”系统面临以下四大问题。

(1) 需要海量的客户端(“云安全”探针)。只有拥有海量的客户端，才能对互联网上出现的病毒、木马以及挂木马的网站等有最灵敏的感知能力。目前瑞星有一亿多自有客户端，如果加上迅雷等合作伙伴的客户端，则能够完全覆盖国内的网民，无论哪个网民的机器中毒、访问挂木马网站，都能在第一时间作出反应。

(2) 需要专业的反病毒技术和经验。瑞星公司拥有 20 多年的反病毒技术积累，有数百名工程师组成的研发队伍，技术实力稳居世界前列。大量专利技术、虚拟机、智能主动防御、大规模并行运算等技术的综合运用，使得瑞星的“云安全”系统能够及时处理海量的上报信息，并将处理结果共享给“云安全”系统的每个成员。

(3) 需要大量的资金和技术投入。目前瑞星“云安全”系统在服务器、带宽等硬件上的投入已经超过几亿元人民币，而相应的顶尖技术团队、未来数年持续的研究花费将数倍于硬件设施投资。

(4) 系统必须是开放的，而且需要大量合作伙伴的加入。瑞星“云安全”是一个开放性的系统，其“探针”与所有软件完全兼容，即使用户使用其他的杀毒软件，也可以安装瑞星卡卡助手等带有“探针”功能的软件，享受“云安全”系统带来的成果。

5.4.4　趋势科技“云安全”

趋势科技“云安全”的核心在于超越了拦截 Web 威胁的传统方法，转而借助威胁信息汇总的全球网络。该网络采用了趋势科技的云安全技术，在 Web 威胁到达网络或者计算机之

前即可对其拦截。

通过推出在云中的快速实时安全状态“检测”，趋势科技降低了对端点上传/下载传统特征码文件的依赖性，同时减少了在公司范围内部署特征码有关的成本和管理费用。

趋势科技已经将云安全技术架构融入公司的全线产品中，例如，网关安全设备 IWSA、客户端产品 OfficeScan、中小企业产品 Worry-Free SME 10.0 以及个人消费类产品网络安全专家（TIS）等。图 5.11 是趋势科技“云安全”软件全功能增强版的界面。

图 5.11　趋势科技“云安全”软件全功能增强版 2013

目前，趋势科技“云安全”已经在全球建立了 5 个数据中心、几万部在线服务器，拥有 99.9999%的可靠性。借助“云安全”，趋势科技现在每天阻断的病毒感染高达 1000 万次。借助其 Web 威胁保护战略，趋势科技率先界定了一种主张，即仅靠传统的扫描安全解决方案将不能够针对恶意 Web 威胁提供有效的保护，现在需要的是多层、多组件、灵活的可适应技术。

趋势科技“云安全”有如下特点。

1. 自动反馈机制

趋势科技“云安全”的一个重要组件就是自动反馈机制，以双向更新流方式在趋势科技的产品及公司的全天候威胁研究中心和技术之间实现不间断通信。通过检查单个客户的路由信誉来确定各种新型威胁，趋势科技广泛的全球自动反馈机制的功能很像现在很多社区采用的“邻里监督”方式，实现实时探测和及时的“共同智能”保护，将有助于确立全面的最新

威胁指数。单个客户常规信誉检查发现的每种新威胁都会自动更新趋势科技位于全球各地的所有威胁数据库，防止以后的客户遇到已经发现的威胁。

由于威胁资料将按照通信源的信誉而非具体的通信内容收集，所以不存在延迟的问题，而客户的个人或商业信息的私密性也得到了保护。

2. 电子邮件信誉服务

趋势科技的电子邮件信誉服务按照已知垃圾邮件来源的信誉数据库检查 IP 地址，同时利用可以实时评估电子邮件发送者信誉的动态服务对 IP 地址进行验证。信誉评分通过对 IP 地址的“行为”和“活动范围”及之前的历史进行不断的分析而加以细化。按照发送者的 IP 地址，恶意电子邮件在云中即被拦截，从而防止“僵尸”或“僵尸网络”等 Web 威胁到达网络或用户的计算机。

3. Web 信誉服务

借助全球最大的域信誉数据库之一，趋势科技的 Web 信誉服务按照恶意软件行为分析所发现的网站页面、历史位置变化和可疑活动迹象等因素来指定信誉分数，从而追踪网页的可信度。然后通过该技术继续扫描网站，并防止用户访问被感染的网站。为了提高准确性、降低误报率，趋势科技的 Web 信誉服务为网站的特定网页或链接指定了信誉分值，而不是对整个网站进行分类或拦截，因为通常合法网站只有一部分受到攻击，而信誉可以随时间不断变化。

通过信誉分值的比对，就可以知道某个网站潜在的风险级别。当用户访问具有潜在风险的网站时，就可以及时获得系统提醒或阻止，从而帮助用户快速地确认目标网站的安全性。通过 Web 信誉服务，可以防范恶意程序。由于防范是基于网站的可信程度而不是真正的内容，所以能有效预防恶意软件的初始下载，用户在进入网络前就能够获得防护能力。

4. 行为关联分析技术

趋势科技“云安全”利用行为分析的“相关性技术”把威胁活动综合联系起来，确定其是否属于恶意行为。Web 威胁的单一活动似乎没有什么害处，但如果同时进行多项活动，就可能会导致恶意结果。因此，需要按照启发式观点来判断是否实际存在威胁，可以检查潜在威胁不同组件之间的相互关系。通过把威胁的不同部分关联起来并不断更新其威胁数据库，使得趋势科技获得了突出的优势，即能够实时做出响应，针对电子邮件和 Web 威胁提供及时、自动的保护。

5. 文件信誉服务

趋势科技“云安全”包括文件信誉服务技术，它可以检查位于端点、服务器或网关处的每个文件的信誉。检查的依据是已知的良性文件清单和已知的恶性文件清单，即所谓的防病毒特征码。高性能的内容分发网络和本地缓冲服务器将确保在检查过程中使延迟时间降到最短。由于恶意信息被保存在云中，所以可以立即到达网络中的所有用户。与占用端点空

间的传统防病毒特征码文件下载相比，这种方法降低了端点内存和系统消耗。

6. 威胁信息汇总

来自美国、菲律宾、日本、法国、德国和中国等地研究人员的研究将补充趋势科技的反馈和提交内容。在趋势科技防病毒研发暨技术支持中心 TrendLabs，各个国家的员工将提供实时响应、全天候威胁监控和攻击防御，以探测、预防并清除攻击。

5.5 小结

若把云计算比作在互联网浪潮中遨游的战舰，那么云安全就是战舰的动力装置，如果动力装置够强、够稳健，战舰就可以快速前行，劈风斩浪；反之会止步不前，直到沉没。

在学习了云计算的相关概念、相关技术后，读者应该对云计算包含的安全问题有所了解。本章对云安全做了详细的介绍，包括威胁、防护策略及典型的安全应用。通过对本章的学习，读者在使用云计算服务的同时要密切关注并避免可能出现的安全问题。

5.6 习题

一、选择题

1. 典型的云安全应用除了金山毒霸、卡巴斯基、趋势科技以外，还有哪个应用？（　　）

A. 淘宝　　B. 京东

C. 瑞星科技　　D. 微信

2. 云服务提供商除了应通过销毁加密数据相关介质、磁盘擦拭、内容发现等方法来保证数据的完整清除，还有哪个操作可以实现？（　　）

A. 销毁存储介质　　B. 定期修改密码

C. 选择无漏洞的软件　　D. 强化用户管理

3. 在部署云计算数据中心时，最好采用什么策略进行数据与环境的备份？（　　）

A. 数据传输控制计划　　B. 基于异地容灾

C. 数据审计于安全传输　　D. 安全数据储存位置

4. 瑞星云安全计划的核心是什么？（　　）

A. 木马/恶意软件自动分析系统　　B. 虚拟化软件

C. 身份识别与访问　　D. 安全数据储存位置

5. 趋势科技的云安全核心在于超越了传统方法，转而借助了什么的帮助？（　　）

A. 腾讯　　B. 文件信誉

C. 瑞星科技　　D. 威胁信息汇总的全球网络

6. 卡巴斯基 2012 特设了什么功能？（　　）

A. 无云安全功能　　B. 不嵌入对象使用

C. 对象应用　　D. KSN 云安全连接功能

7. 卡巴斯基实验室以(　　)为核心,以技术集成为基础,实现了信息安全软件的功能平台化。

A. 反恶意程序引擎　　B. 系统安全

C. 在线安全　　D. 内容过滤

8. 对于 PaaS 和(　　)应用来说,信息是不能被加密的。

A. IaaS　　B. kis

C. SaaS　　D. cpus

9. 金山毒霸将近十年的积累的数据存储到(　　)。

A. 水平平台　　B. 水银平台

C. 水弹平台　　D. 人人平台

10. 通过(　　)的比对,就可以知道一个网站是不是危险。

A. 蚂蚁信任积分　　B. Web 信任积分

C. 其他公司的担保　　D. 其他网友的评价

二、判断题

1. 通过 Web 信誉服务分值的比对,就可以知道某个网站的潜在的风险等级。(　　)

2. 云用户在云服务提供商存储数据时存在数据滥用、存储位置隔离、灾难恢复、数据审计等安全风险。(　　)

3. 审计是一项支持用户进行监管、合规性检查、操作审核和风险审核的模块。(　　)

4. APT 通常在整个网络内逡巡,混入正常流量中,因此它们很难被侦测到。客户也必须像在内部系统里进行的那样,勤于检测云账户中的 APT 活动。(　　)

5. 随着运服务的成熟,永久数据丢失这样的案例已经不可能再发生了。(　　)

6. 只有拥有海量的客户端,才能对互联网上出现的病毒木马,以及挂木马的网站等有最敏感的感知。(　　)

7. 瑞星云安全不是一个开放的网站,用户的杀毒软件不能使用带有探针功能的软件。(　　)

8. 趋势云安全的杀毒服务器拥有百分百的成功率。(　　)

9. 卡巴斯基的安全工能旨在为互联网搭建一个无缝透明的安全系统。(　　)

10. 将凭证和秘钥嵌入源代码,也是很多开发者常犯的错误。(　　)

三、填空题

1. 瑞星建立云安全系统面临的四大问题是海量的客户端、专业的反病毒技术和经验、_____、_____。

2. 趋势科技云安全的特点有自动反馈机制、_____、_____、行为关联分析技术、文件信誉服务技术和威胁信息汇总。

3. 金山毒霸的云安全平台结构包括可支撑海量计算与存储的水银平台、_____和_____。

4. _____对保证基于虚拟技术的公有云的完整性和可用性是最重要也是最关键的。

5. 典型的云安全应用有金山毒霸、趋势科技、_____、_____。

6. 数据泄漏通常都是由于身份验证不严格、弱密码横行、_____、_____。

7. 审计具有合规更加简化、用户与资源活动的可见性、_____、_____。

8. 安全凭证管理包括密码、访问密钥、_____、_____，在通过 UI 访问或 API 及命令访问时，会采用不同的凭证方式。

9. 最常用的远程管理机制有 VPN、_____、_____。

10. 常见的切入点包括_____、_____、U 盘预载恶意软件和通过已经被黑的第三方网络。

四、问答题

1. 相比于传统环境，云计算面临哪些安全问题？

2. 数据安全主要包括哪些方面？