ICS xx.xxx
L xx

团 体 标 准

T/ISEAA XXX-2019

信息安全技术
网络安全等级保护云计算测评指引

Information security technology—

Testing and evaluation guideline of cloud computing for

classified production of cybersecurity

（征求意见稿）

20XX -XX-XX 发布　　20XX -XX-XX 实施

中关村信息安全测评联盟 发布

目　次

前　言

为配合国家网络安全等级保护制度2.0全面推进，更好的指导等级测评机构在云计算环境下开展等级测评工作，加强、规范云计算安全等级测评工作的独立性、客观性、合规性及有效性，依据网络安全等级保护2.0相关系列标准，制定网络安全等级保护云计算安全等级测评指引，本指引遵从下列标准规范：

—— GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求；

—— GB/T 28448—2019　信息安全技术　网络安全等级保护测评要求；

—— GB/T 28449—2018　信息安全技术　网络安全等级保护测评过程指南。

本标准由中关村信息安全联盟提出并归口。

本标准起草单位：公安部第三研究所（公安部信息安全等级保护评估中心）、阿里云计算有限公司、深信服科技股份有限公司、电力行业信息安全等级保护测评中心、国家信息技术安全研究中心、国家网络与信息系统安全产品质量监督检验中心、中国金融电子化公司测评中心、交通运输信息安全中心有限公司、信息产业信息安全测评中心、公安部第一研究所、中国信息通信研究院、国家信息中心、教育部信息安全等级保护测评中心、国家计算机网络与信息安全管理中心、安徽省信息安全测评中心、广西网信信息安全等级保护测评有限公司、中国电信集团系统集成有限责任公司、成都市锐信安信息安全技术有限公司。

本标准主要起草人：张振峰、张志文、王睿超、伊玮珑、廖智杰、张　乐、沈锡镛、陈立峰、陈妍、王理冬、冯伟、王建峰、祁志敏。

网络安全等级保护云计算测评指引

1　范围

本标准规定了测评机构开展云计算等级测评的方法以及应遵循的程序规则。

本标准适用于指导网络安全等级测评机构（以下简称测评机构）开展客观公正、科学规范的云计算等级测评工作。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239—2019　信息安全技术　网络安全等级保护基本要求

GB/T 28448—2019　信息安全技术　网络安全等级保护测评要求

GB/T 28449—2018　信息安全技术　网络安全等级保护测评过程指南

GB/T 25069 信息安全技术　术语

GB/T 31167—2014　信息安全技术　云计算服务安全指南

GB/T 31168—2014　信息安全技术　云计算服务安全能力要求

网络安全等级保护XXX系统测评报告模板[2019版]

3　术语和定义

3.1　云计算

通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式。

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

[GB/T 31167—2014，定义3.1]

3.2　云计算服务

使用定义的接口，借助云计算提供一种或多种资源的能力。

注：[GB/T 31167—2014，定义3.2]

3.3　云服务商

为个人、组织提供云计算服务的企事业单位。云服务商管理、运营支撑云计算服务的计算基础设施及软件，通过网络将云计算服务交付给客户。

注：[GB/T 31168—2014，定义3.2]

3.4　云服务客户

为使用云计算服务同云服务商建立业务关系的参与方。

注：[GB/T 31167—2014，定义3.4]

3.5 云基础设施

云基础设施包括硬件资源层和资源抽象控制层。硬件资源层包括所有的物理计算资源，主要包括服务器（CPU、内存等）、存储组件（硬盘等）、网络组件（路由器、防火墙、交换机、网络链接和接口等）及其他物理计算基础元素。资源抽象控制层由部署在硬件资源层之上，对物理计算资源进行软件抽象的系统组件构成，云服务商用这些组件提供和管理物理硬件资源的访问。

注：[GB/T 31168—2014，定义3.5]

3.6 云计算环境

包括由云服务商提供的云基础设施，及客户在云基础设施之上部署的软件及相关组件的集合。

注：[GB/T 31168—2014，定义3.7]

3.7 云计算平台

云服务商提供的云基础设施及其上的服务层软件的集合。

3.8 云服务客户业务应用系统

包括云服务客户部署在云计算平台上的业务应用和云服务商为云服务客户通过网络提供的应用服务。

3.9 云计算技术构建的业务应用系统

业务应用和为此业务应用独立提供底层云计算服务、硬件资源的集合，此类系统中无云服务客户。

3.10 云产品（服务）

使用云计算服务提供的包括软、硬件产品或服务。

3.11 虚拟机监视器

运行在基础物理服务器和操作系统之间的中间软件层，可允许多个操作系统和应用共享硬件。

3.12 宿主机

运行虚拟机监视器的物理服务器。

4 概述

网络安全等级保护云计算测评是指等级保护测评机构（下称“测评机构”）依据国家网络安全等级保护制度规定，受有关单位委托，对采用了云计算技术构建的信息系统等级保护状况进行的检测评估活动，是网络安全等级保护工作中的重要环节。采用了云计算技术构建的信息系统（下称“云计算平台/系统”）包括云计算平台、云服务客户业务应用系统以及使用了云计算技术构建的业务应用系统。

云计算平台/系统的网络安全等级保护测评工作较传统的网络信息系统测评，在安全通

用要求之外额外增加云计算安全扩展要求。云计算安全扩展要求主要涉及的控制点包括基础设施位置、网络架构、网络边界的访问控制、网络边界的入侵防范、网络边界的安全审计、集中管控、计算环境的身份鉴别、计算环境的访问控制、计算环境的入侵防范、镜像和快照保护、数据安全性、数据备份恢复、剩余信息保护、云服务商选择、供应链管理和云计算环境管理。

云计算平台/系统在测评时，应遵循下列两个基本原则：

- 责任分担原则

区别于传统信息系统，云计算环境中涉及一个或多个安全责任主体，各安全责任主体应根据管理权限的范围划分安全责任边界。

- 云服务模式适用性原则

云计算环境中可能承载一种或多种云服务模式，每种云服务模式下提供了不同的云计算服务及相应的安全防护措施，在对云计算平台/系统测评时，应仅关注每种特定云服务模式下，与其提供的云服务相对应的安全防护措施有效性。

5 云计算等级测评实施

5.1 系统调研

测评机构人员在编制等级保护测评方案前，对云计算平台/系统的调研阶段应至少明确以下内容：

(一) 云计算形态，即被测系统属于云计算平台/系统中的哪一类；

1) 被测对象为云计算平台时，需明确以下内容：
   a) 云计算平台的定级情况；
   b) 云部署模式：公共云、私有云（社区云）、混合云；
   c) 云基础设施物理机房地点/逻辑位置信息及运维地点；
   d) 云计算服务模式：
      - 基础设施即服务（Infrastructure-as-a-Service，IaaS），即云服务商将计算、存储和网络等资源封装成服务供客户使用；
      - 平台即服务（Platform-as-a-Service，PaaS），即云服务商为客户提供软件开发、测试、部署和管理所需的软硬件资源；
      - 软件即服务（Software-as-a-Service，SaaS），即云服务商将应用软件功能封装成服务，使客户能通过网络获取服务。
   e) 云计算平台服务基本安全功能<参见附录2>。
2) 被测对象为云服务客户业务应用系统，需明确以下内容：
   a) 所部署的云计算平台定级情况及等级测评情况，包括云计算平台的等级测评报告编号、等级测评结论以及等级测评主要问题及整改情况(主要内容包括云计算平台等级测评报告中的总体评价、主要安全问题及整改建议（可以以图片形式提供）和云服务商针对安全问题的整改情况)；
   b) 云服务客户业务应用系统部署的云服务模式，云服务客户业务应用系统可根据业务

选择，选用某一个或多个云服务商的单一或多种混合的服务模式，系统调研时，应明确云服务客户业务应用系统所选用的云服务模式。

3) 被测对象为使用了云计算技术构建的业务应用系统

a) 系统定级情况；

b) 云基础设施物理机房地点/逻辑位置信息及运维地点；

c) 业务应用系统独占的独立的底层服务和硬件资源情况。

(二) 调研被测系统基本信息情况<参见附录1>。

5.2 测评对象选取

测评机构在方案编制阶段选取测评对象时，应遵循重要性、安全性、共享性、全面性和符合性的原则，除包括网络互联与安全设备操作系统、应用软件系统、主机操作系统、数据库管理系统、安全相关人员、机房、介质以及管理文档外，还需针对云计算平台/系统的服务模式考虑下列内容：

(一) 虚拟设备，包括虚拟机、虚拟网络设备、虚拟安全设备；

(二) 云操作系统、云业务管理平台、虚拟监视器、云产品（服务）；

(三) 云服务客户网络控制器、云应用开发平台等。

针对被测系统为云计算平台时，测评机构在选取测评对象时可参照：

服务模式	安全层面	测评对象
SaaS	安全计算环境	云产品（服务）
		云产品（服务）数据
PaaS	安全计算环境	虚拟机、数据库服务、中间件、容器、云应用开发平台、云产品（服务）等
IaaS	安全计算环境	云操作系统、虚拟机监视器、云业务管理系统、云产品（服务）
		虚拟网络/安全设备、虚拟机镜像
		云产品（服务）服务器（虚拟机）、宿主机、终端、云管平台服务器
		网络设备、安全设备
		管理数据（配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据、个人信息）
	安全通信网络	网络架构、物理链路、通信数据
	安全区域边界	物理网络边界、虚拟网络边界
	安全管理中心	云管理平台、云平台监控系统
	安全管理[1]	安全相关人员、机房、介质以及管理文档
	安全物理环境	物理机房、云计算基础设施部署的相关机房及基础设施

针对被测系统为云服务客户业务应用系统时，测评机构在选取测评对象时可参照：

服务模式	安全层面	测评对象
IaaS	安全计算环境	云服务客户业务应用系统
		业务数据

服务模式	安全层面	测评对象
		虚拟机、数据库、中间件等
		虚拟网络设备、虚拟安全设备
	安全通信网络	虚拟网络架构
	安全区域边界	虚拟网络边界防护服务
	安全管理中心	安全管理平台
	安全管理[1]	安全相关人员、介质以及管理文档
	平台侧安全	云计算平台等级测评结论/云服务符合性评价
PaaS	安全计算环境	容器、数据库
		业务应用系统
		业务数据
	安全管理中心	安全管理平台
	安全管理[1]	安全相关人员、介质以及管理文档
	平台侧安全	云计算平台等级测评结论/云服务符合性评价
SaaS	安全计算环境	业务数据
		业务应用系统
	安全管理[1]	安全相关人员、介质以及管理文档
	平台侧安全	云计算平台等级测评结论/云服务符合性评价

注：[1]安全管理包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。

针对被测系统为使用云计算技术构建的业务应用系统时，测评机构在选取测评对象时可参照：

安全层面	测评对象
安全计算环境	业务应用系统、业务数据
	云操作系统、虚拟机监视器、云业务管理系统、云产品（服务）、虚拟机、数据库、中间件、容器
	云产品（服务）服务器（虚拟机）、宿主机、终端、云管平台服务器
	网络设备、安全设备、虚拟网络/安全设备
	管理数据（配置文件、鉴别信息、系统数据、审计数据、镜像文件、快照数据、个人信息）
安全通信网络	网络架构、物理链路、通信数据
安全区域边界	物理网络边界、虚拟网络边界
安全管理中心	云管理平台、云平台监控系统
安全管理[1]	安全相关人员、机房、介质以及管理文档
安全物理环境	物理机房、云计算基础设施部署的相关机房及基础设施

5.3 测评指标选取

云计算是一种共享技术模式，云服务商与云服务客户会承担实施和管理不同部分的责任，云计算平台/系统在不同服务模式和部署模式下，云服务商和云服务客户分担的安全职责有所不同。测评机构在编制测评方案时，应明确云服务商和云服务客户所承担的责任，基于“权

责一致”、“安全管理责任不变，数据归属关系不变”的原则，即对数据有什么管理权就应负相应的责任，具体责任划分建议如下：

服务模式	云服务商安全责任	云服务客户安全责任
IaaS	网络设备、安全设备、云产品（服务）服务器(虚拟机)、宿主机、终端、云管平台服务器； 云操作系统、云产品（服务）； 虚拟机监视器、虚拟网络/安全设备、虚拟机镜像； 鉴别数据、系统数据、审计数据、快照数据、个人信息	虚拟机、数据库、中间件、业务应用和数据的安全防护、云服务安全策略配置
PaaS	网络设备、安全设备、云产品（服务）服务器(虚拟机)、宿主机、终端、云管平台服务器、虚拟机； 云操作系统、云产品（服务）、数据库； 虚拟机监视器、虚拟网络/安全设备、虚拟机镜像； 鉴别数据、系统数据、审计数据、快照数据、个人信息	软件开发平台中间件以及应用和数据的安全防护、云服务安全策略配置
SaaS	网络设备、安全设备、云产品（服务）服务器(虚拟机)、宿主机、终端、云管平台服务器； 云操作系统、云产品（服务）； 虚拟机监视器、虚拟网络/安全设备、虚拟机镜像； 虚拟机、数据库、中间件、业务应用； 鉴别数据、系统数据、审计数据、快照数据、个人信息	业务应用相关的安全配置、用户访问、用户账户以及数据安全的防护、云服务安全策略配置

对云计算平台/系统进行测评时，应同时使用安全通用要求部分和云计算安全扩展要求部分的相关要求，不能仅使用云计算安全扩展要求。云计算安全扩展要求测评项内容本身为全局能力要求，不作为对某一测评对象或设备的要求，应作为云计算测评的整体指标。

测评机构在测评指标选取时，首先确定云计算平台/系统的保护等级，针对被测系统为云计算平台和云服务客户业务应用系统时，在级别控制点的基础上根据云服务商和云服务客户分担的安全责任、云计算的服务模式、云计算技术的实现方式以及测评对象在云计算环境中的角色进行等级测评指标选取；针对被测系统为使用云计算技术构建的业务应用系统时，在级别控制点的基础上根据云计算技术的实现方式和测评对象在云计算环境中的角色进行等级测评指标的选取。

5.4 工具测试对象选取

测评人员应与被测的云计算平台/系统有关人员明确选用的测评工具，确定工具测试环境与方法，查看、分析这些行为的结果，输出工具测试结论，针对云计算平台/系统的工具测试，具体测试目标对象选取可参考下表：

测评系统	服务模式	工具测试（漏扫）对象
云计算平台	IaaS	物理服务器、网络设备（物理+虚拟）、云产品（服务） 服务器（虚拟机）、云产品（服务）
	PaaS	物理服务器、网络设备（物理+虚拟）、云产品（服务） 服务器（虚拟机）、虚拟机镜像、数据库、云产品（服务）
	SaaS	物理服务器、网络设备（物理+虚拟）、云产品（服务） 服务器（虚拟机）、业务应用系统所在的虚拟机、数据库、云产品（服务）

测评系统	服务模式	工具测试（漏扫）对象
云服务客户业务应用系统	IaaS	业务应用系统服务器<虚拟机>、数据库、云服务客户业务应用系统
	PaaS	云服务客户业务应用系统
	SaaS	云服务客户业务应用系统
使用云计算技术构建的业务应用系统	——	物理服务器、网络设备（物理+虚拟）、云产品（服务）服务器（虚拟机）、业务应用系统所在的虚拟机、数据库、云产品（服务）、业务应用系统

6 云计算等级测评问题分析

云计算平台云安全服务能力评价是对云计算平台提供的云服务安全能力进行描述，同时比对网络安全等级保护基本要求，评价云计算平台是否能够提供相应的安全能力，若存在不符合项应着重进行阐述。

在完成现场测评活动后，测评机构人员应对等级测评中发现的安全问题进行安全风险分析，核查系统风险情况，制定整改方案，便于系统责任方落实整改措施，规避风险隐患，针对网络安全等级保护云计算安全扩展要求中，可能引发高安全风险的情况可参照下表：

安全层面	控制点	安全问题	风险级别
安全物理环境	基础设施位置	云计算基础设施不全位于中国境内。	高
安全通信网络	网络结构	虚拟网络间隔离措施或手段失效。	高
		云服务商未提供开放接口或开放的安全服务，第三方安全产品（服务）无法接入。	高
安全区域边界	访问控制	虚拟网络边界处未部署访问控制设备或设置的访问控制策略无效。	高
	入侵防范	无法检测到虚拟机与宿主机、虚拟机与虚拟机的攻击行为。	高
安全计算环境	访问控制	同一宿主机虚拟机间的隔离机制失效或不同宿主机虚拟机间未设置隔离措施。	高
	入侵防范	云计算环境中不具备防病毒能力。	高
	镜像和快照保护	未采取任何的防护措施对虚拟机镜像完整性防护，同时未对保密性进行安全防护。	高
	剩余信息保护	云服务资源被释放时，云服务客户数据未采取任何的数据清除机制对数据进行完全性清除。	高
安全建设管理	云服务商选择	云服务客户选择了未通过安全等级测评或不具备相应等级安全能力要求的云服务商。	高
		云服务商与云服务客户未签订服务水平协议。	高

7 云计算等级测评结论分析

等级测评报告是等级测评工作的最终产物，在输出云计算平台/系统等级测评报告应注意：

1) 云计算平台等级测评结论包括两部分内容：等级测评结论和云计算系统测评结论扩展信息表；
2) 针对测评系统为云服务客户业务应用系统时，云计算系统测评结论扩展信息表中应填写云服务客户业务应用系统所在云计算平台的等级测评报告编号和云计算平台服务符合性评价，云计算平台服务符合性评价引用云计算平台的等级测评报告中云计算平台服务符合性评价，若业务应用系统选用多种云服务模式组合，需引用相关云计算平台的服务符合性评价；
3) 使用了云计算技术构建的业务应用系统等级测评结论仅包括等级测评结论，不包括云计算系统测评结论扩展信息表；
4) 在对测评系统整体测评结果分析时，应充分考虑通用要求与扩展要求间的安全问题进行综合性分析；
5) 在对被测系统安全问题风险分析时，当被测系统为云服务客户业务应用系统时，应充分考虑云计算平台提供的不符合性服务对客户业务应用系统的风险影响。

针对云计算平台等级测评结论，应综合云计算平台面临的风险等级及综合得分：

1) 云计算平台存在的问题中无中、高风险项，且得分高于90分（含90分），判定云计算平台等级测评结论为优；
2) 云计算平台存在的问题中无高风险项，且得分高于80分（含80分），判定云计算平台等级测评结论为良；
3) 云计算平台存在的问题中无高风险项，且得分高于70分（含70分），判定云计算平台等级测评结论为中；
4) 云计算平台存在的问题中存在高风险项，或得分低于70分，判定云计算平台等级测评结论为差。

针对云服务客户业务应用系统等级测评结论，应综合考虑云计算平台和云服务客户业务应用系统的符合性：

1) 云计算平台等级测评结论为优，云服务客户业务应用系统存在的问题中无中、高风险项，且得分高于90分（含90分），判定云服务客户业务应用系统等级测评结论为优；
2) 云计算平台等级测评结论为良，云服务客户业务应用系统存在的问题中无高风险项，当得分高于80分（含80分），判定云服务客户业务应用系统等级测评结论为良；
3) 云计算平台等级测评结论为中，云服务客户业务应用系统存在的问题中无高风险项，当得分高于70分（含70分），判定云服务客户业务应用系统等级测评结论为中；
4) 云计算平台等级测评结论为优、良、中，云服务客户业务应用系统存在的问题中存在高风险项，或得分低于70分，判定云服务客户业务应用系统等级测评结论为差；
5) 云计算平台等级测评结论为差，无需考虑云服务客户业务应用系统安全符合性，直接判定云服务客户业务应用系统等级测评结论为差。

针对使用了云计算计算构建的业务应用系统等级测评结论，应综合考虑系统面临的风险等级及综合得分：

1) 使用了云计算计算构建的业务应用系统存在的问题中无中、高风险项，且得分高于90分（含90分），判定云计算平台等级测评结论为优；
2) 使用了云计算计算构建的业务应用系统存在的问题中无高风险项，且得分高于80分（含80分），判定云计算平台等级测评结论为良；
3) 使用了云计算计算构建的业务应用系统存在的问题中无高风险项，且得分高于70分（含70分），判定云计算平台等级测评结论为中；
4) 使用了云计算计算构建的业务应用系统存在的问题中存在高风险项，或得分低于70分，判定云计算平台等级测评结论为差。

附录 A 被测系统基本信息表（样例）

<table>
<tr><th colspan="4">云计算平台测评基本信息调研表</th></tr>
<tr><td>云计算形态</td><td>云计算平台</td><td>云服务模式</td><td>IaaS
PaaS
SaaS</td></tr>
<tr><td>运维所在地</td><td>XXXXXX</td><td>云部署模式</td><td>公有云
私有云
混合云</td></tr>
<tr><td rowspan="14">云计算平台基本信息</td><td>调研信息</td><td colspan="2">基本情况</td></tr>
<tr><td>定级情况</td><td colspan="2" rowspan="13">具体调研信息,参照网络安全等级保护系统调研表。</td></tr>
<tr><td>网络结构</td></tr>
<tr><td>网络设备</td></tr>
<tr><td>安全设备</td></tr>
<tr><td>服务器</td></tr>
<tr><td>云操作系统</td></tr>
<tr><td>云产品（服务）</td></tr>
<tr><td>虚拟机镜像</td></tr>
<tr><td>虚拟机</td></tr>
<tr><td>数据库</td></tr>
<tr><td>容器</td></tr>
<tr><td>中间件</td></tr>
<tr><td>SaaS 应用系统</td></tr>
</table>

注：IaaS 服务模式下，调研对象为 部分；

PaaS 服务模式下，调研对象为 两部分；

SaaS 服务模式下，调研对象为 三部分。

<table>
<tr><th colspan="4">云服务客户业务应用系统测评基本信息调研表</th></tr>
<tr><td>云计算形态</td><td>云服务客户业务应用系统</td><td>云服务模式</td><td>IaaS
PaaS
SaaS</td></tr>
<tr><td>运维所在地</td><td>XXXXXX</td><td>云部署模式</td><td>公有云
私有云
混合云</td></tr>
<tr><td>云计算平台测评报告编号</td><td>XXXXXXXXXXX-XXXXX-XX-XXXXXX-XX</td><td>云计算平台测评得分</td><td>XX.XX</td></tr>
<tr><td rowspan="10">云计算平台/系统基本信息</td><td>调研信息</td><td colspan="2">基本情况</td></tr>
<tr><td>虚拟网络结构</td><td colspan="2" rowspan="9">具体调研信息，参照网络安全等级保护系统调研表。</td></tr>
<tr><td>虚拟网络设备</td></tr>
<tr><td>虚拟安全设备</td></tr>
<tr><td>虚拟机镜像</td></tr>
<tr><td>虚拟机</td></tr>
<tr><td>数据库</td></tr>
<tr><td>中间件</td></tr>
<tr><td>业务应用系统</td></tr>
<tr><td>定级情况</td></tr>
</table>

注： SaaS 服务模式下，调研对象为 部分；

PaaS 服务模式下，调研对象为 两部分；

IaaS 服务模式下，调研对象为 三部分。

附录 B 云计算平台服务 （样例）

<table>
<tr><th colspan="6">云计算平台服务信息表</th></tr>
<tr><td>云计算形态</td><td>云计算平台</td><td>云部署模式</td><td>公有云
私有云
混合云</td><td>云服务模式</td><td>IaaS
PaaS
SaaS</td></tr>
<tr><td colspan="3">云计算平台服务</td><td colspan="3">安全功能简述</td></tr>
<tr><td colspan="3">虚拟主机服务</td><td colspan="3">虚拟主机服务主要是增加硬件的利用以及提高生产率，为构建云计算基础架构奠定了重要的技术基础。</td></tr>
<tr><td colspan="3">虚拟网络隔离服务</td><td colspan="3">帮助用户基于云平台构建出一个隔离的网络环境，用户可以完全掌控自己的虚拟网络，包括选择自有 IP 地址范围、划分网段、配置路由表和网关等。</td></tr>
<tr><td colspan="3">虚拟防火墙服务</td><td colspan="3">虚拟防火墙通过状态检测包过滤功能进行安全域划分，并基于虚拟防火墙实现三层网络的访问控制。</td></tr>
<tr><td colspan="3">虚拟主机入侵检测服务</td><td colspan="3">主机入侵检测服务通过在服务器上部署的客户端进行信息搜集和检测，实时检测专有云环境中所有物理服务器主机/虚拟机，并及时发现文件篡改、异常进程、异常网络连接、可疑端口监听等行为，帮助用户及时发现服务器安全隐患。</td></tr>
<tr><td colspan="3">云服务客户系统安全审计服务</td><td colspan="3">安全审计服务是基于云计算平台的一体化解决方案。安全审计服务从物理服务器层面、网络设备层面、云计算平台应用层面分别进行，实现了行为日志的收集、存储、分析、报警等功能。</td></tr>
<tr><td colspan="3">云服务客户系统防恶意代码服务</td><td colspan="3">……</td></tr>
<tr><td colspan="3">……</td><td colspan="3">……</td></tr>
</table>