华为云 PCI DSS 实践指南

文档版本 3.0

发布日期 2023-02-07

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 概述

1.1 适用范围

本文档提供的信息适用于华为云在官网上由华为云提供的产品和服务。

1.2 发布目的与目标读者

支付卡协会数据安全标准（Payment Card Industry Data Security Standard, 以下简称PCI DSS）作为广受国际认可的数据安全标准，致力于保护持卡人的数据安全。华为云目前已经通过PCI DSS标准认证，并希望为客户介绍依照标准要求华为云保护数据安全的主要措施。基于此背景，本文档主要面向希望在认证过程中将华为云上环境纳入PCI DSS 评估范围的客户，以及希望了解华为云数据安全政策的客户，帮助其了解：

- 华为云如何基于PCI DSS的要求进行数据安全保护；
- 华为云为客户提供了多种产品帮助其遵从PCI DSS标准要求。

1.3 文章前提

本文档中所有对于PCI DSS的标准及官方指引的版本皆以第六章引用资料中标识的为准，并且本文档不包含PCI DSS中所涉及的所有具体要求，仅供客户作为总体的思路参考之用，不作为其进行PCI DSS认证时的任何依据。

华为云的产品及服务介绍仅基于本文档发布时的内容，随着产品更新迭代，功能可能发生变化，具体应以华为云官网的产品说明为准。

1.4 基本定义

PCI安全标准协会：2006年由美国运通、发现金融、JCB 国际信用卡公司、万事达卡国际组织与 Visa公司共同创建的开放全球论坛。

持卡人数据（Cardholder Data，简称CHD）：由四部分组成的卡数据，包含：

- 主账户信息（PAN）：一般为银行卡号，大多数信用卡账户由16位字符串组成；
- 持卡人姓名：主账户中登记的归属人的姓名或任何授权使用卡的人；

- 失效日：银行卡的授权有效期；
- 业务码：3至4位数字的编码，用于定义服务属性、识别国际和国内的数据交换、识别使用限制等信息。

敏感验证数据（Sensitive Authentication Data，简称SAD）：主要由三部分组成，包含：

- 全磁道数据：信用卡背面磁条中存储的数据，每个磁条拥有三条磁道，分别记录了PAN、姓名、失效日、业务码、CVV、PVV等数据；
- 信用卡安全码：银行卡安全验证码，一般为3至4位，常见的安全码有CVV2（VISA）、CVC2（万事达卡）、CVN2（中国银联）、CID（美国运通卡）、CAV2（日本JCB）等；
- PIN/PIN数据块：一般为信用卡交易密码。

持卡人数据环境（Cardholder Data Environment，简称CDE）：存储、处理或传输持卡人数据或敏感验证数据的人员、流程或技术。

客户：指与华为云达成商业关系的注册用户。

服务提供商：PCI协会将直接参与持卡人数据的处理、存储和传输的除支付方以外的商业实体，或提供的服务影响持卡人数据的安全性的实体定义为服务提供商。

云供应商：云供应商是服务提供商的子类。由于在本文档中仅阐述使用华为云服务的情况，因此本文使用云供应商，即华为云，指代官方语境下的服务提供商。

2 PCI DSS 标准简介

2.1 标准介绍

PCI安全标准协会致力于账户数据安全标准的持续发展、完善、存储、普及与实施，迄今为止，共发布了支付卡行业数据安全标准 (PCI DSS)、支付应用程序数据安全标准 (PA-DSS) 和引入设备 (PED) 要求三份标准。

PCI DSS包含建立并维护安全的网络和系统、保护帐户数据、维护漏洞管理计划、实施强效访问控制措施、定期监控并测试网络、维护信息安全政策这六大领域内容，具体囊括12项具体安全标准要求，为保护持卡人数据及敏感验证数据的技术和操作提供基准。

建立和维护安全网络和系统	1. 安装和维护网络安全控制
	2. 安全配置应用于所有系统组件
保护帐户数据	3. 保护所存储账户数据
	4.在开放的公共网络上传输过程中使用强效加密法保护持卡人数据
维护漏洞管理计划	5.保护所有系统和网络免受恶意软件侵害
	6.开发和维护安全系统和软件
实施强效的访问控制措施	7.根据“必须知道”原则限制系统组件和持卡人数据的访问权限
	8.识别用户并验证系统组件的访问权限
	9.限制持卡人数据的实体访问权限
定期监控和测试网络	10.记录并监控系统组件和持卡人数据的所有访问权限
	11.定期测试系统和网络的安全性
维护信息安全政策	12.使用组织政策和计划支持信息安全

PCI DSS已成为全球企业作为彰显其数据安全能力的主要认证之一，最新版的标准为2022年发布的4.0版。

2.2 标准适用群体

PCI DSS适用于参与支付卡处理的所有实体，包括商户、处理商、收单机构、发卡机构和服务提供商。PCI DSS 还适用于存储、处理或传输持卡人数据或敏感验证数据的所有其他实体。

对于业务中不涉及持卡人数据的客户，也可参考PCI DSS的要求强化自身的数据保护能力，全面保护数据安全。

3 华为云对 PCI DSS 的遵循

3.1 华为云的认证情况

目前，华为云作为云产品及服务的提供者，已经取得了基于4.0版本的PCI DSS 认证，表明华为云的基础环境已经达到了PCI DSS的要求，可为客户提供高质量的数据安全保护。

同时，华为云在提供产品或服务过程中，不可避免地将收集、传输、存储客户的持卡人数据。为此，华为云运营中心，即处理客户持卡人数据的部门，同样通过了基于4.0版本的PCI DSS认证，表明华为云可有效地保护客户的持卡人数据。

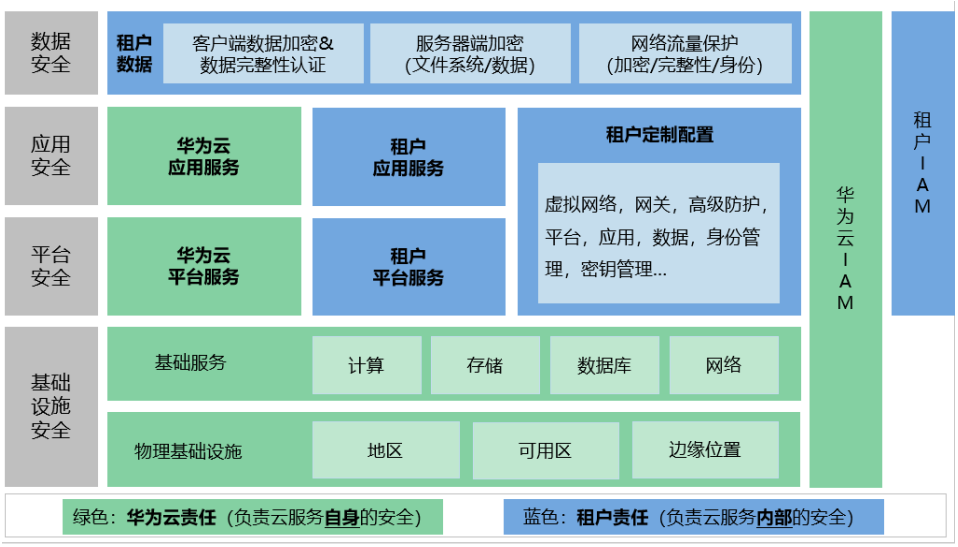
华为云布局全球，在29个区域（自营+合营）运营75个可用区，覆盖亚太、拉美、非洲、欧洲、中东等地域，为全球的客户提供产品及服务，可根据客户的需求支持其收集、传输、存储持卡人数据信息。

华为云PCI DSS的合规性认证范围包含了华为云官网上由华为云提供的所有云服务，详情可参见官网。

3.2 华为云安全责任共担

在复杂的云服务业务模式中，云安全不再是某一方单一的责任，需要租户与华为云共同努力。基于此，华为云为帮助租户理解双方的安全责任边界、避免出现安全责任真空区而提出了责任共担模型。在模型中租户与华为云具体负责的区域可参见下图。

图 3-1 华为云安全责任共担模型



基于责任共担模型，华为云与租户主要承担如下责任：

华为云：主要责任是研发并运维运营华为云数据中心的物理基础设施，华为云提供的各项基础服务、平台服务和应用服务，也包括各项服务内置的安全功能。同时，华为云还负责构建物理层、基础设施层、平台层、应用层、数据层和租户身份管（IAM）层的多维立体安全防护体系，并保障其运维运营安全。

租户：主要责任是在租用的华为云基础设施与服务之上定制配置并且运维运营其所需的虚拟网络、平台、应用、数据、管理、安全等各项服务，包括对华为云服务的定制配置和对租户自行部署的平台、应用、用户身份管理等服务的运维运营。同时，租户还负责其在虚拟网络层、平台层、应用层、数据层和IAM层的各项安全防护措施的定制配置、运维运营安全、以及用户身份的有效管理。

关于华为云与租户的安全责任详情，可参考华为云已发布的**《华为云安全白皮书》**。

3.3 华为云如何遵循 PCI DSS 标准要求

华为云严格遵循PCI DSS的要求，从制度到流程上设定了相应的数据保护措施以保护云环境及客户在华为云官网购买产品及服务时的持卡人数据的安全。

安全的网络和系统

本领域对应标准中的***要求1***及***要求2***，从安装和维护网络安全控制、安全配置应用于所有系统组件两个方面建立安全的系统和网络。

根据PCI DSS中网络隔离及要求1的内容，管理层面，华为云制定了安装和维护网络安全控制与应用的流程和机制；技术层面，华为云使用防火墙将CDE与内部其他功能的系统环境进行隔离，并使用负载均衡、DNS和Web应用防火墙过滤外部流量，未经授权的流量将被拦截。同时华为云使用其自研发的VPN构建了其自身的安全虚拟网络（SVN），仅允许通过IPSec、VPN方式连接的数据，进一步保障网络隔离的效果及安全。华为云还设置了Web上传白名单，防止未经授权的数据传入。

华为云明确要求数据库或其他系统组件禁止使用原厂商的缺省口令，且要求若存在多个默认账号，需将不适用的账号禁用或删除。

保护持卡人数据

保护持卡人数据领域对应标准中的***要求3***及***要求4***，主要通过存储保护机制与加密机制来实现。

华为云服务及产品本身不会在使用过程中收集任何持卡人数据。但在客户购买华为云的产品及服务时，需要在线支付系统或绑定支付银行卡进行支付，此时华为云会收集、传输、存储客户的持卡人数据。华为云高度重视该类型数据的安全，使用AES加密存储持卡人账号（PAN）并在需要展示时对其进行掩盖，只展示前六位及后四位号码，在持卡人数据不再需要或超过留存期限后将被自动删除，实现存储期限最小化。而敏感验证数据则在验证完成后立即删除，不进行存储。

依据标准，华为云使用加密技术对客户的持卡人数据进行加密传输及加密存储，保护个人数据在传输、存储过程中的安全；并且华为云在网络传输过程中使用了业界通用的TLS高版本安全传输层协议及IPSec协议，在非信任网络之间传输敏感数据时使用安全传输通道或AES强效加密算法进行严格加密。华为云还使用密钥管理系统对加密密钥进行加密管理，数据加密密钥（DEK）及密钥加密密钥（KEK）的强度均为AES强效加密算法，属于PCI协会定义的强效加密法。

漏洞管理计划

本领域内容对应标准中的***要求5***及***要求6***，主要通过部署杀毒软件、漏洞管理以及安全开发及变更保护数据安全。

华为云使用IPS入侵防御系统、Web应用防火墙、防病毒软件以及HIDS主机型入侵检测系统对系统组件及网络进行漏洞管理。IPS入侵防御系统可以检测并预防潜在的网络入侵活动；Web应用防火墙部署在网络边界以保护应用软件的安全，使其免于受到来自外部的SQL注入、CSS、CSRF等面向应用软件的攻击；防病毒软件提供病毒防护及Windows 系统内的防火墙； HIDS主机型入侵检测系统保护云服务器的安全，降低账户被窃取的风险，提供弱密码检测、恶意程序检测、双因子认证、脆弱性管理、网页防篡改等功能。另一方面，华为云定期对TCP/IP进行漏洞扫描，降低因可能存在未被发现的安全漏洞带来的风险。

华为云建立了安全漏洞管理流程，设置了漏洞管理员及相关安全角色为漏洞的评估负责，并要求了定期安全关键安全补丁，降低漏洞风险。

在华为云产品及服务的定义、设计、分析和测试阶段，将信息安全纳入开发的整个生命周期，并且产品的代码被审核员进行审核并批准才允许代码进入版本中。

实施强效访问控制措施

标准主要通过***要求7***、***要求8***及***要求9***，从识别用户访问、访问权限控制及物理访问权限控制三个方面建立访问控制措施。

在运营过程中，华为云基于员工的角色设置其对个人数据的访问权限，并使用身份认证系统限制非法访问、以权限最小化原则管理员工权限，避免员工违规修改、披露个人数据。

华为云也对员工的账号进行了严密的保护，对账号的密码长度、复杂长度进行了限制，及时清退非活动账号，限定了账号密码的尝试次数，超过指定次数后账号将被锁定，并强制通过多因素验证进行登陆。

在物理设备的防护方面，华为云基于谨慎小心的原则为数据中心选址，建立了专门的规范对建筑与结构的安防、物理安防边界进行规定。在数据中心内部署了安全管理系统、入侵报警系统、视频监控系统，限定现场运维人员、供应商及华为云员工的最小权限，对访客进行了严格的控制，并监控人员的出入。物理存储介质进出机房时均会

进行数据防泄漏管理，并对数据擦除、报废清退中流程进行规定，减少可能存在的数据泄露损失。

监控及网络测试

本领域由***要求10***与***要求11***组成，华为云对系统进行监控并定期检查监控的有效性两方面响应要求。

华为云使用CLS日志系统对系统组件进行监控，收集并存储和分析所有系统组件日志，以及自主研发的CIP集中化安全事件管理系统分析安全事件并实时告警，系统基于威胁模型和专家定义规则进行智能分析。华为云也会定期对日志及安全事件的处理进行复核。

华为云针对关键基础设施、网络进行监控，可及时监测可能的网络攻击，避免数据泄露事件的发生。华为云建立了应对网络安全事件的响应流程，多个部门进行协同合作，及时监控事件，迅速部署处置措施，降低事件带来的影响。

信息安全政策

信息安全政策领域对应***要求12***，建立并维护全面的安全政策。

华为云建立了一系列保障数据安全的政策与流程指引，并通过了多种数据安全标准类认证，如ISO 27001信息安全管理体系、ISO 27017云服务信息安全管理体系、ISO 20000信息技术服务管理体系认证、ISO 22301业务连续性管理体系、CSA STAR云安全国际金牌认证，以及多种地区性安全认证，如MTCS Level3多层云计算安全规范（新加坡）、云服务客户数据保护能力认证（中国）、网络安全等级保护（中国）、可信云金牌运维专项评估（中国）、网信办云计算服务安全评估（中国）。

在各产品、服务的业务团队中，明确规定了所有员工对应角色的信息安全责任，华为云设置专门负责安全及隐私保护的角色承担一定的信息安全管理职责。同时，华为云会严格筛选录用人员，并对员工定期举行安全意识、网络安全及隐私保护培训及测试，增强员工对数据安全的理解、提升数据保护能力并规范其日常行为。

对于服务供应商的数据安全管理，华为云与相关服务供应商签订了《供应商网络安全与数据处理协议》，要求供应商遵循个人数据保护相关的法律法规、建立安全保障体系及安全应急响应机制。

4 华为云助力客户响应 PCI DSS 的要求

4.1 PCI DSS 评估指引

客户可以通过华为云部署其寻求PCI DSS合规性的云环境。但是这不意味着客户使用华为云则默认满足了PCI DSS的合规要求，客户与华为云基于上文的责任矩阵共同承担数据安全责任，客户应根据其自身的类型，采取相应的措施。若客户希望通过PCI DSS的认证，则需要联系PCI安全标准协会授权的评估机构QSA对其进行评估，范围一般包含持卡人数据环境中包含或与之连接的所有系统组件。

4.2 标准要求与具体措施

当客户使用华为云部署其自身的云环境以处理账户数据时，客户往往需要同华为云共同承担数据安全保护责任。下面将阐述华为云作为服务提供商，如何协助客户满足PCI DSS的要求。

要求 1 安装和维护网络安全控制

PCI DSS建议使用防火墙控制内部网络和外部网络（不可信网络）之间的计算机访问流量以及内部网络中敏感区域的输入及输出流量，并对所有网络流量进行检查，阻止不符合已制定安全标准的传输，以避免系统组件受到来自不可信网络的非授权访问。

华为云部署了防火墙对于外部网络及华为云内部网络之间通讯的流量进行筛查，并对基础设施的网络设置负责，分离客户流量与管理流量，使得网络隔离与租户分离。

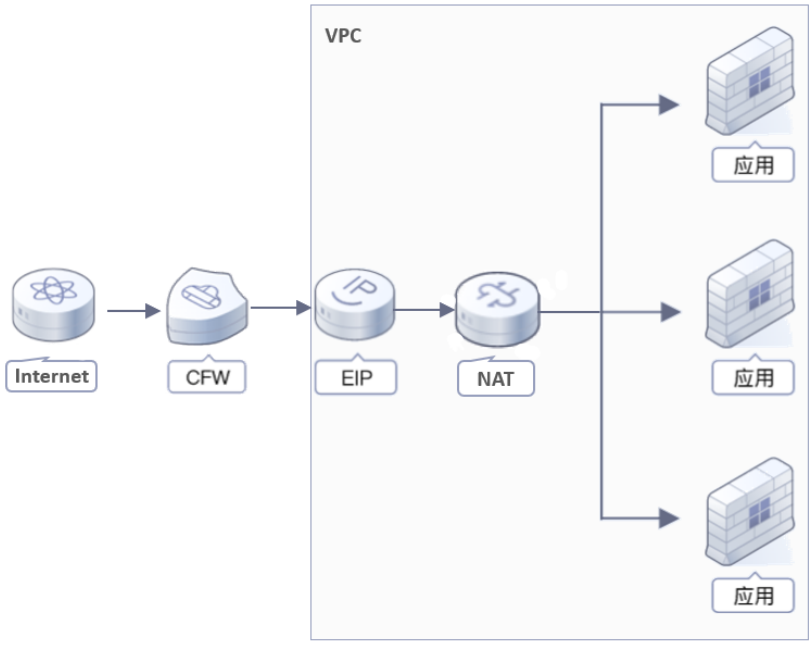
要求1	
客户类型	**客户实践指引**
IaaS	客户保护其自有环境中的网络安全，部署防火墙控制进出环境的流量，并识别其所有网络、设备、系统组件及持卡人数据环境及其他环境之间的网络，保证仅被可信的组件连接。
PaaS	客户仍需要在其平台内的环境部署防火墙以保证网络安全，并定期检查可进入其环境的服务、协议及接口的清单及设置。
SaaS	由华为云主要负责网络安全保护工作。

针对要求1，华为云为客户提供了**虚拟私有云VPC**、**云防火墙CFW**、**NAT网关**等产品。

IaaS及PaaS客户在可通过**虚拟私有云VPC**产品在云上建立隔离的、私密的虚拟网络环境，在流畅地访问的同时隔离租户，在此基础上支持灵活配置VPC之间的互联互通。VPC可适用于三种场景的应用，包含云端专属网络、Web服务、混合云内通过部署VPC隔离持卡人数据环境与其他业务环境、管理环境。实现持卡人数据环境持卡人数据环境内组件不可通过互联网直接公共访问，响应***要求1.3***中禁止互联网与持卡人数据环境间直接访问的规定。

云防火墙CFW产品提供云上互联网边界和VPC边界的防护，如下图所示，云防火墙置于外部互联网与云上VPC之间，可提供功能包括全局统一访问控制，全流量分析可视化，实时入侵检测与防御，日志审计与溯源分析等，同时支持按需弹性扩容。可响应***要求1.3*** 限制持卡人数据环境的网络访问权限，***要求1.4*** 控制可信网络和不可信网络之间的网络连接的要求。

NAT网关产品分为公网NAT网关和私网NAT网关。公网NAT网关支持将私网IP转换为公网IP，转换后，云上资源即可安全地访问公网或者对外提供服务，并且保护私有网络信息不直接对公网暴露。私网NAT网关提供私网地址转换的功能，实现VPC与VPC之间、VPC与本地数据中心（ IDC ）互访。可响应***要求1.4.5***内部IP地址和路由信息隐藏的规定。



要求 2 安全配置应用于所有系统组件

供应商提供的默认密码或默认设置可能被非法使用以威胁云环境、系统、软件的安全，因此需要在日常使用中注意更改默认密码，删除不必要的软件、功能和帐户，以及禁用或删除不必要的服务，减少潜在的攻击面。

华为云负责云环境的基础设施（仅IaaS用户）及系统（IaaS及PaaS用户）的管理账号的密码配置策略，并根据华为云密码政策控制密码的复杂程度、修改周期，同时为系统组件制定适用的系统配置标准。

要求2	
客户类型	**客户实践指引**
IaaS	客户需要对其部署在华为云的系统、应用及虚拟系统组件的安全配置负责。
PaaS	
SaaS	由华为云主要负责设备、系统及应用的安全配置。

针对要求2，华为云为客户提供了**统一身份认证服务IAM、企业主机安全HSS等产品**。

客户管理员在使用华为云**统一身份认证服务IAM**创建新用户时，可通过邮件发送一次性登陆链接给新用户，新用户使用链接进行登陆时需要设置密码，另外在客户管理员自定义新用户的密码可选择强制用户在激活后修改默认密码。两种方式均可避免IAM用户使用默认密码，响应***要求2.2***中管理供应商的默认帐户的规定。并且在客户的账号登陆IAM控制台的访问是由公网进行传输，使用HTTPS协议，响应***要求2.2***中要求使用强效加密法对所有非控制台的管理访问进行加密。

企业主机安全HSS服务是服务器的贴身安全管家，提供资产管理、漏洞管理、基线检查、入侵检测等功能，能够帮助企业更方便地管理主机安全风险，实时发现并阻止黑客入侵行为。HSS资产管理功能包括：提供账号、端口、进程、Web目录和软件等安全资产信息的管理和分析，响应***要求2.2***中检查是否只启用必要的服务、协议、守护程序和功能，删除或禁用所有不必要的功能。

要求 3 保护存储的持卡人数据

客户应最小限度的存储持卡人数据，并采取加密、掩码等方法保护持卡人数据，以降低持卡人数据被未授权的读取及披露的风险。

对于IaaS及PaaS客户，华为云主要保障所提供的基础设施或平台安全，以此辅助客户保护存储的持卡人数据。

要求3	
客户类型	**客户实践指引**
IaaS	客户负责管理数据的加密机制、存储方法及存储期限，对PAN进行一定的掩盖。
PaaS	
SaaS	需要依据客户使用到的华为云具体产品或服务进行判断。

针对要求3，华为云为客户提供**云数据库、数据加密服务DEW、数据安全中心DSC**等产品。

华为云为客户提供多种类型的**云数据库**，包含MySQL、PostgreSQL、SQL Server、分布式多模NoSQL数据库，并且已通过ISO 27001、CSA、可信云、等保三级等14项国内外安全合规认证。云数据库支持与VPC进行连接，保障存储持卡人数据的数据库与其他业务环境的隔离。客户可通过云数据库管理持卡人数据的存储时间， 并根据需要进行安全地数据删除，支持客户响应***要求3.1***关于数据保留、存储时间及数据删除的规定。云数据库产品的客户端及服务端密码认证时提供SHA256级别的加密，具有日志禁止打印密码等敏感信息的安全控制功能，响应***要求3.4***中PAN在显示时被掩盖的规定。

云数据库支持**数据加密服务DEW**托管密钥的服务端加密，通过使用硬件安全模块HSM保护密钥安全的托管，帮助客户轻松创建和控制加密密钥。客户密钥不会明文出现在HSM之外，避免密钥泄露。对密钥的所有操作都会进行访问控制及日志跟踪，提供所有密钥的使用记录，响应***要求3.5***中PAN不可读的规定。

数据安全中心DSC提供数据分级分类、数据安全风险识别、数据水印溯源和数据静态脱敏等基础数据安全能力，通过数据安全总览整合数据安全生命周期各阶段状态，对外整体呈现云上数据安全态势。DSC通过深度行为识别引擎，建立用户行为基线，实现基线外异常操作实时告警，风险事件关联识别，完善溯源审计链条，及时发现数据使用是否存在安全违规并及时告警，预防数据泄露。客户还可通过20+种预置脱敏规则或自定义规则对数据进行静态脱敏，同时，通过数据水印注入/提取功能对数据追踪溯源。响应***要求3***中保护所存储账户数据的要求。

要求 4 加密持卡人数据在开放式公共网络中的传输

持卡人数据及敏感信息在公共网络传输时必须进行加密，同时需要结合配置正确的无线网络及新版的加密及与验证协议以保护数据不被他人轻易获取。

对于IaaS客户需独自承担加密持卡人数据传输时的安全保护责任，而对于PaaS用户，华为云依据与客户签署的服务水平协议，主要承担客户环境之外的平台底层传输安全保障的责任。

要求4	
客户类型	**客户实践指引**
IaaS	客户负责指定持卡人数据的传输机制以及选择需使用的加密、传输技术，同样需关注在公共网络组件间的数据传输均应进行加密以保障数据安全，并确保传输持卡人数据或连接到持卡人数据环境的无线网络使用了强效加密。
PaaS	客户负责指定持卡人数据的传输机制以及选择需使用的加密、传输技术，同样需关注在公共网络组件间的数据传输均应进行加密以保障数据安全。
SaaS	需要依据客户使用到的华为云具体产品或服务进行判断。

针对要求4，华为云为客户提供**弹性负载均衡ELB、数据加密服务DEW、云专线DC**等产品。

弹性负载均衡ELB是将访问流量根据转发策略分发到后端多台弹性云服务器的流量分发控制服务，可以通过流量分发扩展应用系统对外的服务能力，提高应用程序的容错能力，针对加密传输场景，可为客户提供基于HTTPS监听器的安全策略配置，包含TLS协议版本和配套的加密算法套件。客户可以配置TLS1.2、TLS1.3版本的传输协议，增强数据传输的安全性，同时可响应***要求4.2***中使用强效加密法保护数据安全的规定。

在要求4.2中，还对密钥及证书的管理进行了规定，客户可通过**数据加密服务DEW**中的HSM组件来管理密钥及设置密钥强度，响应标准的要求。

客户可使用**云专线DC**产品构建客户本地数据中心与华为云上的虚拟私有云VPC之间高速、低延时、稳定安全的专属连接通道，保护数据中心与VPC之间的数据传输安全，响应***要求4.2***中不使用终端用户通讯技术，如电子邮件、即时通讯传送不被保护的银行账号的规定。

要求 5 保护所有系统和网络免受恶意软件侵害

恶意软件，如病毒、蠕虫、木马、间谍软件、勒索软件等可通过员工电子邮件（例如通过网络钓鱼）和使用互联网、移动计算机和存储设备进入企业网络中，从而利用系统漏洞造成损失。因此所有系统均应使用反恶意软件解决方案，保护系统免受当前和不断发展的恶意软件威胁。

华为云为其负责服务器或平台部署反恶意软件解决方案，并正确配置其设置，以维护反恶意软件的有效性。

要求5	
客户类型	**客户实践指引**
IaaS	客户负责保护其操作系统及其虚拟机的安全，需要在其操作系统中部署部署反恶意软件解决方案，以保护持卡人数据环境免于恶意软件攻击。
PaaS	客户需要在其操作系统中部署杀部署反恶意软件解决方案，以保护系统免于恶意软件攻击。
SaaS	由华为云主要负责持卡人数据环境的反恶意软件保护。

主机安全服务HSS采用先进的AI、机器学习等技术，并集成多种杀毒引擎，深度查杀主机中的恶意程序，可识别后门、木马、蠕虫等恶意程序，提供自动隔离查杀功能，同时，支持已知勒索病毒检测能力，帮助用户自动识别处理系统存在的安全风险。响应***要求5.2***中防止或检测并处理恶意软件的要求。

要求 6 开发并维护安全的系统和应用程序

安全漏洞可能使他人非法获得系统访问特权，所有系统组件必须具备所有适当的软件补丁，以防止恶意的个人和恶意软件对帐户数据的利用和威胁。对于定制软件，通过应用软件生命周期（SLC）流程和安全编码技术，可以避免许多漏洞。

华为云负责保护在客户云环境或平台下的设备维护及补丁安全，以及底层应用的开发安全。在PaaS及SaaS模式下，系统及应用的补丁安全及管理也将根据服务类型，分别由华为云负责。

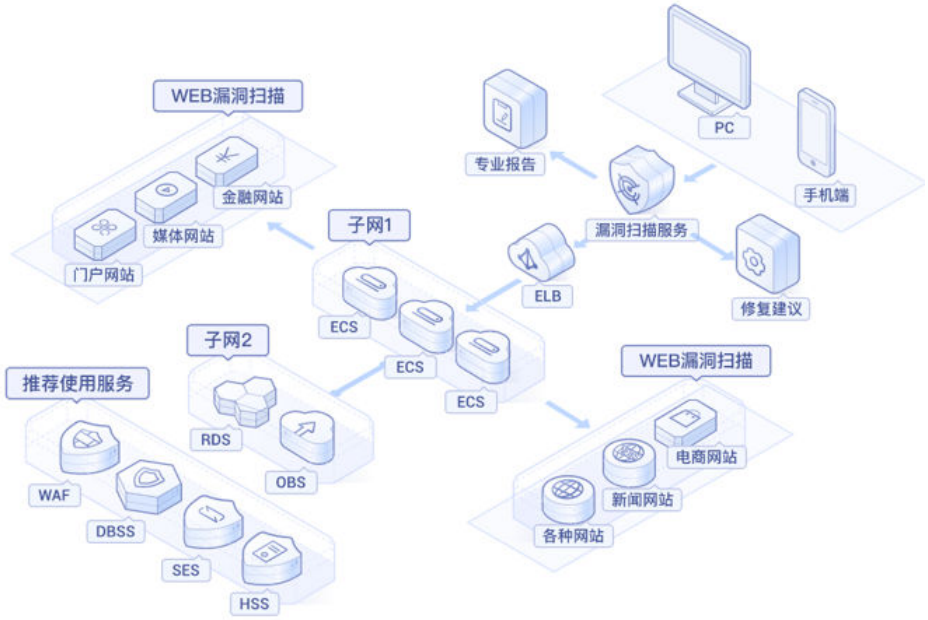
要求6	
客户类型	**客户实践指引**
IaaS	客户应保证操作系统及应用的补丁及更新及时被安装，并应对其安全的开发负责，维护适当的变更流程。
PaaS	
SaaS	客户应确保补丁或更新已及时安装。

针对要求6，华为云为客户提供**漏洞扫描服务VSS、数据库安全服务DBSS、Web应用防火墙WAF**等产品。

华为云为客户提供**漏洞扫描服务VSS**，集成了Web漏洞扫描、操作系统漏洞扫描、资产内容合规检测、配置基线扫描、弱密码检测五大功能，可以自动发现网站或服务器

暴露在网络中的安全风险，提供多种维度的安全检测服务。同时，华为云安全专家会第一时间针对紧急爆发的通用漏洞CVE进行分析并更新规则，提供快速、专业的CVE漏洞扫描。可响应***要求6.2***识别并解决安全漏洞要求。VSS还支持扫描前端漏洞，如SQL注入、XSS、CSRF、URL跳转等，可响应***要求6.1***中提及的注入攻击、XSS跨站脚本等漏洞的防护。

客户也可选用**数据库安全服务DBSS**，DBSS提供基于机器学习机制和大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能，同样可响应***要求6.1***中关于SQL注入防护及漏洞识别的要求。



PCI DSS标准要求在面向公众的 Web 应用程序前安装可检查和防范网页式攻击的自动化技术解决方案，不断检查所有流量。客户可通过购买**Web应用防火墙服务WAF**对网站业务流量进行多维度检测和防护，如上图所示，WAF可阻挡如SQL注入、跨站脚本等攻击，具有防数据泄露、漏洞修复、防CC攻击、防网页篡改四大功能，可响应标准***要求6.4***中面向公众的网络应用程序，部署自动技术解决方案，持续检测和防止Web应用程序受到攻击。

要求 7 根据“必须知道”原则限制系统组件和持卡人数据的访问权限

最佳实践需要根据知情及工作职责需要限定人员对于持卡人数据的访问权限，并通过适当的系统和流程保证权限的正确设置，以免非必要人员或非授权人员访问到核心、敏感数据。

各类型客户都需要同华为云一同协作来进行访问控制管理，其中华为云主要负责底层基础设施的访问控制。

要求7	
客户类型	**客户实践指引**
IaaS	客户应负责定义其不同员工对于持卡人数据访问的权限，以及对数据访问时的控制。
PaaS	
SaaS	客户应负责定义其不同员工对于持卡人数据访问的权限。

针对要求7，华为云为客户提供**统一身份认证服务IAM等服务**。

在客户注册华为云账号后，默认开通**统一身份认证服务IAM**，可以为客户提供身份认证和权限管理功能。IAM可通过配置联邦身份认证，在自身企业管理系统后即可直接访问华为云，降低管理复杂度。并且支持基于客户组的权限管理机制，可以基于项目授予个人某个资源的操作权限，可响应***要求7.2***中根据工作分类和职能及履行工作职责所需的最小权限分配权限的规定。

要求 8 识别用户并验证系统组件的访问权限

为有访问权限的每个人分配唯一标识符 (如ID)，确保每个人都能对自己的操作负责。实施这种责任制后，由已知被授权客户和流程对关键数据和系统执行操作和跟踪。

PCI DSS要求建立和管理用户和管理员的强效验证，如使用强效密码/口令，密码的有效性主要取决于验证系统的设计和实施，尤其是允许攻击者尝试密码的频率以及在输入点、传输过程和存储中保护客户密码的安全方法。标准还要求实施多因素验证（ MFA ），确保CDE的安全访问权限，并防止滥用。

华为云将负责在底层基础设施的管控中使用了强有效的验证机制，除IaaS模式外，华为云将保留对华为云系统服务器的访问控制管理权限。

要求8	
客户类型	**客户实践指引**
IaaS	客户应对所有账户的进行控制，以保证每个账户都拥有唯一的ID及强有效的验证机制。
PaaS	
SaaS	客户应为其员工分配唯一的ID并根据其活动状态调整、禁用其权限。

同要求7一致，华为云为客户提供**统一身份认证服务IAM等服务**管理客户人员的访问控制。

IAM还支持设定符合客户条件的账号锁定策略、账号停用策略及会话超时策略。在设置账号锁定策略后，在限定时间内登录失败次数到达设定值后，会将失败登录账号进行锁定，次数可在3~10次之间进行设置，响应***要求8.3.4***的不超过十次次失败登陆后锁定账户。IAM支持如果在限定时间长度内达到登录失败次数后，用户会被锁定一段时间，帐号锁定时长可在15~30分钟之间进行设置，响应***要求8.3.4***的锁定时间设置为至少 30分钟的要求。IAM支持设置1~240天的非活动天数，若账号在设置天数内未登录，则被停用，响应***要求8.2.6***中规定的禁用90天非活动账户的要求。并且在会话在设置时长范围内未进行操作，则需要重新登陆，IAM支持15分钟~24小时的会话超时时长设置，响应***要求8.2.8***中规定的用户会话闲置超过15分钟进行重新验证登陆的要求。此外IAM支持首次登录时需要修改密码，设置1~180天的密码有效期和密码复杂度，同时，支持新密码不能与历史密码相同响应***要求8.3.4***至***要求8.3.9***中关于密码复杂程度及密码更新规则的规定。

华为云IAM还支持使用多因素验证和虚拟MFA对账号进行验证，可响应***要求8.4***、***要求8.5***中与验证机制相关的规定。

要求 9 限制持卡人数据的实体访问权限

若可以实际接触持卡人数据或存储这些数据的系统，则有可能通过访问这些数据或系统删除或者泄露数据，因此PCI DSS中要求被审核人，应予以适当的物理限制以保护数据、系统及存储持卡人数据的媒介。

但由于云服务的特性，对于所有类型的客户，都无需对其持卡人数据的云环境的物理访问控制负责。华为云作为云服务提供商，会为其物理环境进行保护，控制华为云员工及外部人员对于华为云数据中心的物理访问，并保护所有媒介的存储、转移、处置时的数据安全。华为云的详细保护措施请参见本文档3.2章的“实施强效访问控制措施”部分内容。

要求 10 记录并监控系统组件和持卡人数据的所有访问权限

日志机制和跟踪用户活动的能力对于预防、检测或减少数据威胁的影响至关重要。日志存在于所有系统组件和持卡人数据环境（CDE），可以在出错时进行全面的跟踪、报警和分析。

华为云主要负责基础设施的监控与日志记录，对于SaaS客户来说，更多地需要依赖华为云的监控及日志来管理及跟踪访问活动。

要求10	
客户类型	**客户实践指引**
IaaS	客户负责其自身云环境的活动监控与系统组件日志记录。
PaaS	
SaaS	客户负责其应用层的日志设置及监控。

针对要求10，华为云为客户提供**云日志LTS、数据库安全服务DBSS、云监控服务CES、威胁检测服务MTD、态势感知服务SA**等服务。

云日志LTS提供对日志实时采集、实时查询、存储功能，可记录云环境中的活动，便于查询与追踪。结合云监控服务CES，可以对客户登录日志进行实时监控，当遇到恶意登陆行为，可触发告警并拒绝该IP地址的请求。数据库安全服务DBSS基于机器学习机制和大数据分析技术，提供数据库审计，SQL注入攻击检测，风险操作识别等功能。同时LTS及**数据库安全服务DBSS**可对系统组件的日志进行记录并保存，供客户进行日志审核，以响应***要求10.2***实施检查日志，以支持检测异常和可疑活动，以及对事件的取证分析的要求。

LTS中记录的日志支持转储到OBS，转储后可存储较长时间，可响应***要求10.5.1***中保留日志至少12个月的要求。

威胁检测服务MTD，通过接入目标区域中用户在华为云操作所产生的的IAM日志、DNS日志、CTS日志、OBS日志、VPC日志，持续检测日志中访问者的IP或域名是否存在潜在的恶意活动和未经授权行为，发现异常将及时告警。此服务集成了AI智能引擎、威胁情报、规则基线三种能力实现=检测多个云服务（包含IAM服务、DNS服务、CTS服务、OBS服务、VPC服务）日志数据中隐含的异常访问行为，主动发现潜在威胁，对可能存在威胁的访问行为生成告警信息。用户可通过告警描述对告警信息进行核查、处理，在未造成信息泄露等重大损失之前，及时对潜在威胁进行处理，对服务安全进行升级加固，从而保护用户的账户安全、保障服务稳定运行。可响应***要求10.4***中使用自动化机制来执行检查日志审核的要求。

态势感知SA，为用户提供统一的威胁检测和风险处置平台，帮助用户检测云上资产遭受到的各种典型安全风险，还原攻击历史，感知攻击现状，预测攻击态势，为用户提供强大的事前、事中、事后安全管理能力。SA支持结合云上ECS、VPC等核心资产安全状况做统计，扣分项分为“安全服务启用、威胁告警、基线异常、漏洞”四大维度，从资产遇到的已知威胁事件、脆弱性、可能面临的威胁等方面，全方位全天候地进行风险评估，集中呈现威胁告警事件、漏洞、基线检查异常结果数目及风险严重等级（致命、高危、中危等）分布，并支持下钻查看详情，快速处置。可响应***要求10.2***实施日志检查，以支持监测异常和可疑活动，以及对事件的取证分析。

要求 11 定期测试系统和网络的安全性

应经常测试系统组件、流程和自定义软件，以确保安全控制适用于不断变化的环境。

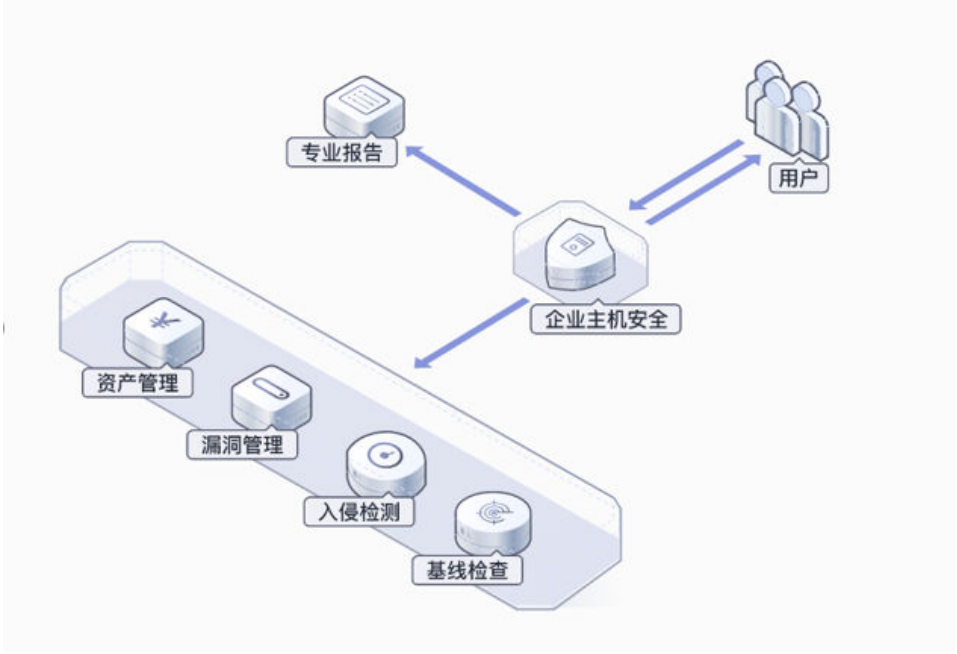
底层设施及SaaS服务的漏洞扫描及穿透测试由华为云定期组织运营，客户仅需负责其云环境的系统及流程测试。

要求 11	
客户类型	**客户实践指引**
IaaS	客户应与华为云协商对于入侵检测、穿透测试等功能的支持性；但客户需要定期或在系统或控制发生重大变更后，重新进行安全测试。
PaaS	
SaaS	由华为云负主要责系统及流程的安全测试。

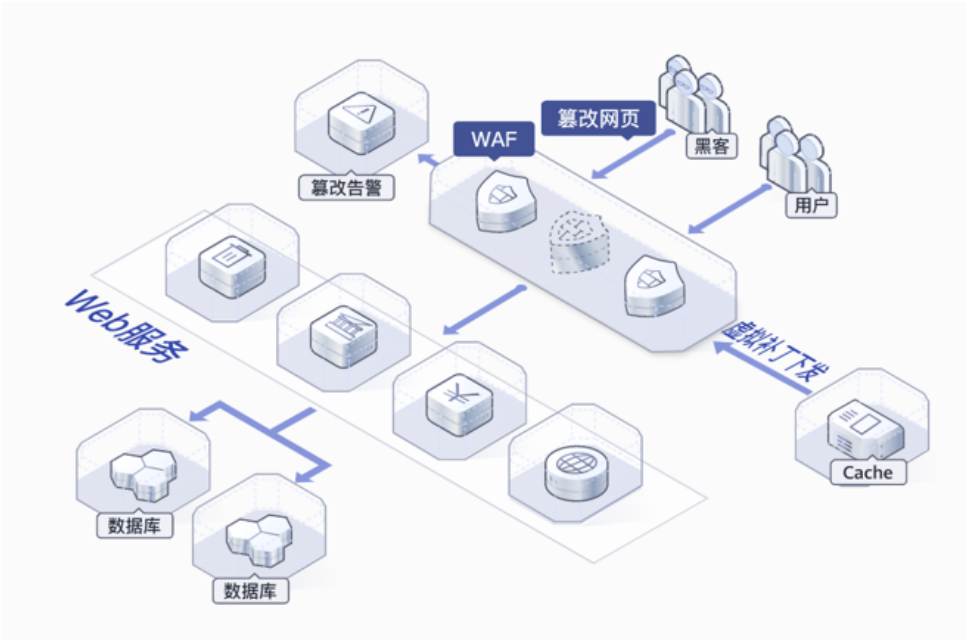
针对要求11，华为云为客户提供**漏洞扫描服务VSS、企业主机安全服务HSS、Web应用防火墙WAF**等服务。

标准***要求11.2***规定至少每个季度开展一次由PCI DSS认证的授权扫描提供商执行的外部漏洞扫描以及一次内部漏洞扫描，客户可使用**华为云漏洞扫描服务VSS**执行定期内部的漏洞扫描工作。通过VSS可识别网站与系统内的漏洞，以便及时发现并解决漏洞，降低漏洞被他人利用而导致的系统组件或持卡人数据被破坏的可能性。

客户也可选用**企业主机安全服务HSS**对主机系统进行安全评估，将现有系统存在的账户、端口、软件漏洞、弱口令风险进行展示，提示客户进行加固，消除安全隐患，提升主机整体的安全性。HSS还提供入侵检测功能，在发现账户暴力破解、进程异常、异常登陆等事件后快速进行告警，客户可通过事件管理全面了解告警事件，帮助客户及时发现资产中的安全威胁、实施掌握资产的安全状态，可响应***要求11.5***中对于使用入侵检测技术检测和防止入侵网络的规定。



同时，客户可选用**Web应用防火墙WAF**防止网页被篡改。WAF支持挂马检测，检测恶意攻击者在网站服务器注入的恶意代码，保护网站访问者安全，支持页面不被篡改，保护页面内容安全，避免攻击者恶意篡改页面，修改页面信息或在网页上发布不良信息，影响网站品牌形象，配合HSS的网页防篡改功能，可响应***要求11.6.1***支付页面部署变更和篡改检测机制的要求。



要求 12 使用组织政策和计划支持信息安全

健全有效的安全政策可以更为全面地保护信息安全，员工了解公司的安全政策将有效降低因安全意识不足及操作不规范带来的风险。所有员工均应了解持卡人数据的敏感性及对此类数据的保护责任。

华为云负责制定其自身的信息安全政策，并为员工提供定期的培训，以增强员工对于数据保护的意识与能力。在实际运营过程中，华为云还需要根据与客户实际签署的服务水平协议调整职责范围。

要求12	
客户类型	**客户实践指引**
IaaS	客户应建立并维护其自身的安全政策及内部流程体系，定义负责安全控制的角色及职责，为员工提供数据安全培训。
PaaS	
SaaS	

客户应根据自身的业务及规模大小制定适合的安全政策及流程指引，华为云不为客户提供相关的服务或文件。客户可参考ISO 27001信息安全体系、ISO 27018云隐私保护认证等标准建立自身的信息及数据安全体系。

4.3 适用的产品清单

下表总结了前文提到的华为云产品及服务，以及其可响应的主要PCI DSS标准要求条款。

产品名	功能简介	对应的标准要求
虚拟私有云VPC	为云服务器、云容器、云数据库等资源构建隔离的、客户自主配置和管理的虚拟网络环境。	1.4、6.5
云防火墙CFW	提供云上互联网边界和VPC边界的防护，包括：实时入侵检测与防御，全局统一访问控制，全流量分析可视化，日志审计与溯源分析等.	1.2、1.3、1.4、10.3
NAT网关	为虚拟私有云内的云主机或者通过云专线/VPN接入虚拟私有云的本地数据中心的服务器，提供网络地址转换服务。	1.4
企业主机安全 HSS	可全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为。	2.2、5.2、5.3、6.1、11.5、11.6、10.3
云数据库（MySQL, PostgreSQL, SQL Server, GeminiDB）	云数据库拥有即开即用、稳定可靠、安全运行、弹性伸缩、轻松管理、经济实用等特点	1.4.4、3.2、3.4
弹性负载均衡ELB	将访问流量分发到后端多台服务器的流量分发控制服务，可以通过流量分发扩展应用系统对外的服务能力。	2.2.7、4.2

产品名	功能简介	对应的标准要求
数据加密DEW	综合的云上数据加密服务，可以提供专属加密、密钥管理、密钥对管理等服务。	3.3、3.5、3.6、3.7、4.2
云专线DC	为客户搭建本地数据中心与云上VPC之间的专属连接通道，实现安全可靠的混合云部署。	1.4、4.2
漏洞扫描服务VSS	对服务器或网站进行漏洞扫描的安全检测服务，提供通用漏洞检测、漏洞生命周期管理、自定义扫描等服务。	2.2.1、6.1、6.2、6.3、6.4.1、10.3、11.3
数据库安全服务 DBSS	提供旁路模式数据库安全审计服务功能，对风险行为和攻击行为进行实时告警。	6.1、10.2
Web应用防火墙 WAF	通过对HTTP(S)请求进行检测，识别并阻断恶意攻击，保护Web服务安全稳定。	6.4、10.3、10.7、11.6
统一身份认证服务 IAM	提供身份认证和权限管理功能，可以管理客户账号，并且可以控制这些客户对资源的操作权限.	7.2、7.3、8.2、8.3、8.4、8.5
云日志服务LTS	提供日志收集、实时查询、存储等功能，无需开发即可利用日志做实时决策分析。	10.2、10.5、10.7
云监控服务 CES	提供一个针对弹性云服务器、带宽等资源的立体化监控平台。	10.7
威胁检测服务MTD	威胁检测服务持续发现恶意活动和未经授权的行为，从而保护账户和工作负载。	10.2、10.4、10.7、10.5、11.5、11.6
云堡垒机CBH	提供主机管理、权限控制、运维审计、安全合规等功能，支持Chrome等主流浏览器随时随地远程运维。	3.4.2、7.3、8.4、8.5、8.6
数据安全中心服务 DSC	提供数据分类分级，敏感数据扫描，数据安全体检，数据水印溯源，数据脱敏等基础数据安全能力。	3.2.1、3.4.1、3.5
态势感知SA	帮助用户检测云上资产遭受到的各种典型安全风险，还原攻击历史，感知攻击现状，预测攻击态势，为用户提供强大的事前、事中、事后安全管理能力。	2.2、10.2、10.4、10.5、10.7、11.5、11.6
云证书管理服务 CCM	CCM是一个为云上海量证书颁发和全生命周期管理的服务。目前它可以提供SSL证书管理和私有证书管理服务。	4.2

5 结语

华为云始终秉持着华为公司“以客户为中心”的核心价值观，为此华为云构建了信息安全管理体系，应用业界通用的数据安全保护技术，致力于保护客户的数据安全。

同时，为帮助客户应对日益复杂和开放的网络环境及日益发展的信息安全技术，华为云不断开发各种数据保护领域的工具、服务和方案，支持客户提升数据保护能力，降低风险。

本白皮书仅供参考，不具备任何法律效力或构成法律建议，也不作为客户在华为云的持卡人数据环境一定合规的依据。客户应酌情评估自身业务和认证需求，选择适合的云产品及服务，并正确的进行配置。

6 引用资料

序号	发布人	资料名
1	PCI 安全标准协会	支付卡行业（PCI）数据安全标准 要求和安全评估程序 4.0版
2	PCI 安全标准协会	PCI安全标准协会云计算指引2018年4月发布版本

7 版本历史

日期	版本	描述
2023年2月	3.0	合规要求更新
2022年4月	2.0	合规要求更新
2020年7月	1.0	首次发布