态势感知

常见问题

文档版本	18
发布日期	2020-10-10

华为技术有限公司

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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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。

目 录

1 产品咨询

1.1 态势感知可以为我提供什么服务?

态势感知是可视化威胁检测和分析平台。态势感知能够检测出超过20+的云上安全风险，包括DDoS攻击、暴力破解、Web攻击、后门木马、漏洞攻击、僵尸主机、异常行为、命令与控制等。利用AI大数据分析技术，态势感知可以对威胁告警和攻击源头进行分类统计和综合分析，为用户呈现出全局安全攻击态势。

详细基础版和专业版功能特性请参见**功能介绍**。

1.2 为什么没有看到攻击数据或者看到的攻击数据很少?

态势感知支持检测云上资产遭受的各类攻击，并进行客观的呈现。但是，如果您的云上资产在互联网上的暴露面非常少（所谓“暴露面”是指资产可被攻击或利用的风险点，例如端口暴露和弱口令都可能成为风险点），那么遭受到攻击的可能性也将大大降低，所以态势感知可能会显示您的系统当前遭受的攻击程度较低。

如果您认为态势感知未能真实反映系统遭受攻击的状况，欢迎您向客服反馈问题，我们会尽快给您答复。

详细说明请参见**态势感知工作原理**和**功能介绍**。

1.3 态势感知的数据来源是什么?

态势感知基于云上威胁数据和华为云服务采集的威胁数据，通过大数据挖掘和机器学习，分析并呈现威胁态势，并提供防护建议。

- 一方面采集全网流量数据，以及安全防护设备日志等信息，通过大数据智能AI分析采集的信息，呈现资产的安全状况，并生成相应的威胁告警。
- 另一方面汇聚DDoS高防（Advanced Anti-DDoS，AAD）、企业主机安全（Host Security Service，HSS）、漏洞扫描服务（Vulnerability Scan Service，VSS）、Web应用防火墙（Web Application Firewall，WAF）等安全防护服务上报的告警数据，从中获取必要的安全事件记录，进行大数据挖掘和机器学习，智能AI分析并识别出攻击和入侵，帮助用户了解攻击和入侵过程，并提供相关的防护措施建议。

态势感知通过对多方面的安全数据的分析，为安全事件的处置决策提供依据，实时为呈现完整的全网攻击态势。

详细说明请参见**态势感知工作原理**。

1.4 如何获取风险程度最高的资产信息?

通过查看资产风险排名，可以获取风险程度最高的资产信息，并可进一步了解该资产遭受的威胁告警统计信息。

用户可在**专业版**的“资产管理 > 主机”主机列表页面，以及“华为云主机安全态势”页面的“TOP5风险云主机”模块查看风险主机。**基础版**不支持查看攻击者排名信息。

详细说明请分别参见**主机安全管理**和**主机安全态势**。

前提条件

- 已购买态势感知**专业版**。
- IAM用户已获取**Tenant Administrator**或**Tenant Guest**权限。

操作步骤

步骤1 登录管理控制台。

步骤2 选择“安全 > 态势感知 > 资产管理”，进入态势感知服务主机资产安全管理页面。

单击“安全状况”或“被攻击次数”列排序按钮，排序当前主机资产风险排名。

图 1-1 主机资产风险排序

步骤3 选择“安全 > 态势感知 > 综合大屏”，单击“主机安全态势”，查看华为云主机安全态势大屏。

查看“TOP5风险云主机”窗口，如图1-2。可查看TOP5风险主机主机的名称、主机系统和安全风险等级，并按照风险等级从高到低的依次排序。TOP5风险云主机最多展示5条。安全风险等级由高到低分别是“致命”、“高危”、“中危”、“低危”和“提示”。

图 1-2 风险云主机

----结束

1.5 如何获取攻击者的信息?

如需了解攻击者（即攻击源）的相关信息，可以查看攻击者排名列表。

用户可在**专业版**的“安全看板”页面“攻击者排名”模块，以及“综合态势感知”页面的“威胁源主机TOP5”模块查看攻击者信息。**基础版**不支持查看攻击者排名信息。

详细说明请分别参见**攻击者排名**和**威胁源主机TOP5**。

前提条件

- 已购买态势感知**专业版**。
- IAM用户已获取**Tenant Administrator**或**Tenant Guest**权限。

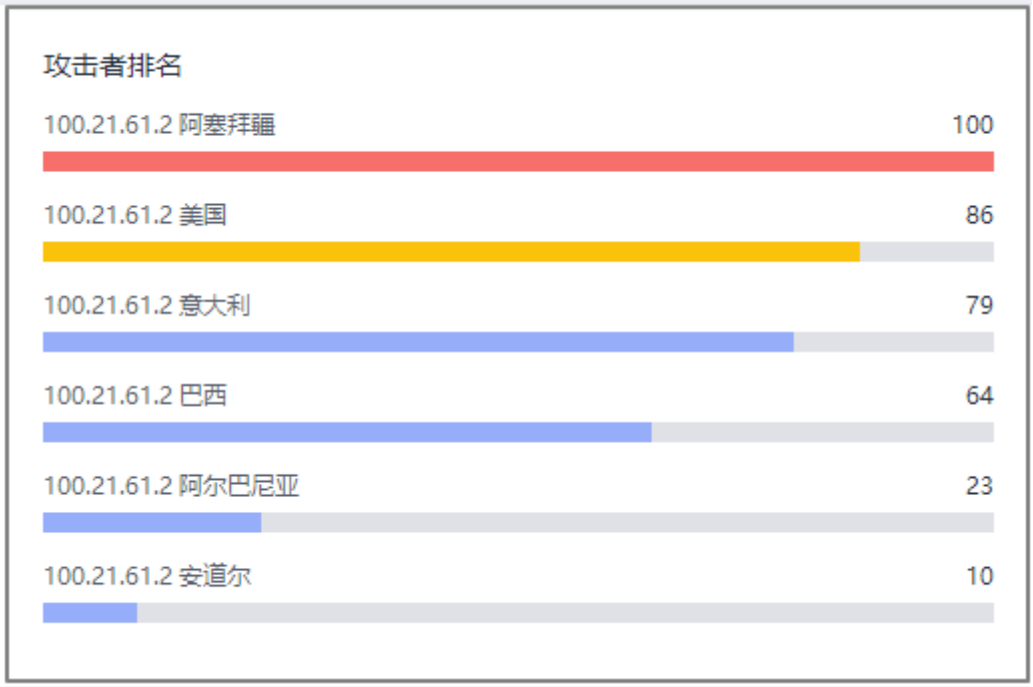
操作步骤

步骤1 登录管理控制台。

步骤2 选择“安全 > 态势感知”，进入态势感知“安全看板”页面。

攻击者排名列表如**图1-3**。列表中展示攻击次数最多的6个攻击者的相关信息，包括攻击者的IP地址、所在地域和攻击次数，并按照攻击次数从高到低的次序进行排列。

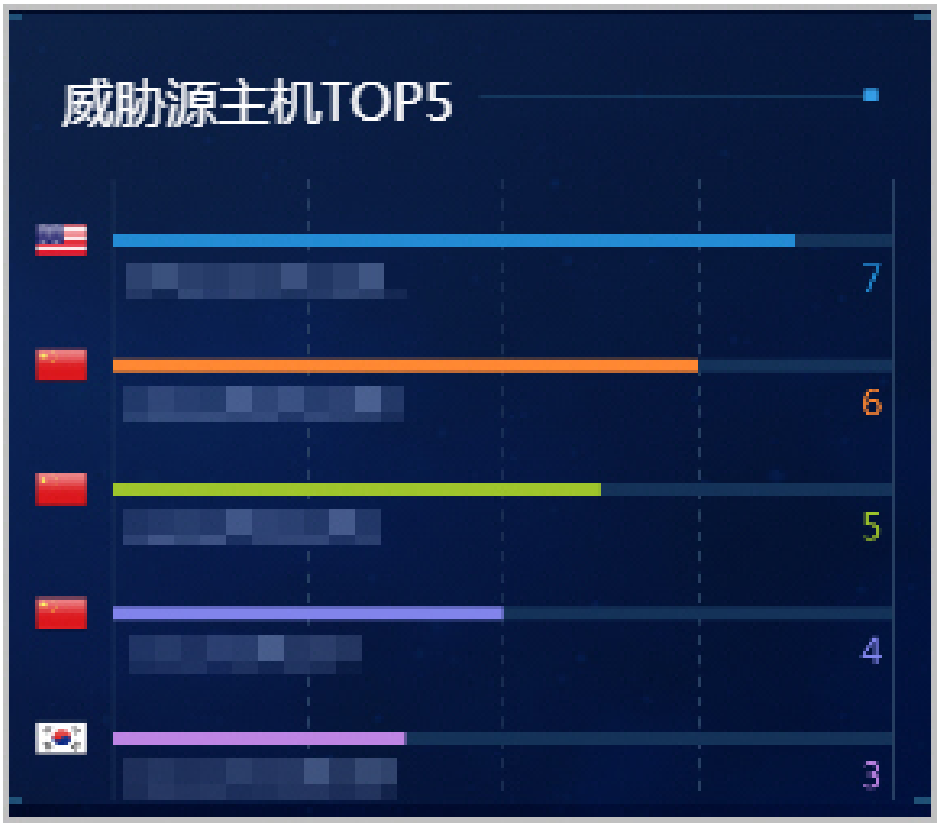
图 1-3 攻击者排名



步骤3 选择“安全 > 态势感知 > 综合大屏”，单击“综合态势感知”，查看综合态势感知大屏。

查看“威胁源主机TOP5”窗口，如图1-4。可查看攻击者主机的IP地址、所属国家/地区和攻击次数，并按照攻击次数从高到低的依次排序。

图 1-4 威胁源主机 TOP5



----结束

1.6 态势感知与其他安全服务之间的关系与区别?

华为云提供多种安全防护和管理服务，其中态势感知（Situation Awareness，SA）是可视化威胁检测和分析的安全管理平台，通过从Anti-DDoS流量清洗（Anti-DDoS）、DDoS高防（Advanced Anti-DDoS，AAD）、企业主机安全（Host Security Service，HSS）、漏洞扫描服务（Vulnerability Scan Service，VSS）、Web应用防火墙（Web Application Firewall，WAF）、数据库安全服务（Database Security Service，DBSS）等安全防护服务中获取必要的安全事件记录，进行大数据挖掘和机器学习，智能AI分析并识别出攻击和入侵，帮助用户了解攻击和入侵过程，并提供相关的防护措施建议。

态势感知作为安全管理服务，依赖于安全防护服务提供威胁检测数据，进行安全威胁风险分析，呈现全局安全威胁态势，并提供防护建议，但是态势感知不实施具体安全防护动作，需与其他安全服务搭配使用。

SA与其他安全防护服务区别，详细内容如**表1-1**。

表 1-1 SA 与其他服务的区别

服务名称	服务类别	关联与区别	防护对象	功能差异
态势感知（SA）	安全管理	SA着重呈现全局安全威胁攻击态势，统筹分析多服务威胁数据和云上安全威胁，并提供防护建议。	呈现全局安全威胁攻击态势。	**SA功能介绍**
Anti-DDoS流量清洗（Anti-DDoS）	网络安全	Anti-DDoS集中于异常DDoS攻击流量的检测和防御，相关攻击日志、防护等数据同步给SA。	保障企业业务稳定性。	**Anti-DDoS功能特性**
DDoS高防（AAD）	网络安全	AAD将公网流量引流至高防IP，聚焦于大流量的DDoS攻击的检测和防御，相关攻击日志、防护等数据同步给SA。	保障企业重要业务连续性。	**AAD产品介绍**
企业主机安全（HSS）	主机安全	HSS着手于保障主机整体安全性，检测主机安全风险，执行防护策略，相关告警、防护等数据同步给SA。	保障主机整体安全性。	**HSS功能特性**
漏洞扫描服务（VSS）	应用安全	VSS通过启动扫描Web类、应用类安全漏洞，发现网站或服务器的风险，并修复漏洞。相关历史漏洞和修复记录同步给SA。	保障网站整体安全性。	**VSS功能特性**
Web应用防火墙（WAF）	应用安全	WAF服务对网站业务流量进行多维度检测和防护，防御常见攻击，阻断攻击进一步威胁。相关入侵日志、告警数据等同步给SA，呈现全网Web风险态势。	保障Web应用程序的可用性、安全性。	**WAF功能特性**
数据库安全服务（DBSS）	数据安全	DBSS着力于数据库访问行为的防护和审计，相关审计日志、告警数据等同步给SA。	保障云上数据库安全和资产安全。	**DBSS产品介绍**

1.7 为什么主机最大配额不能小于主机数量?

主机最大配额是授权检测主机的最大数量。在购买态势感知时，选择的最大配额需等于或大于当前账户下主机总数量，且不支持减少。若购买的最大配额小于主机数量，可能会造成如下影响：

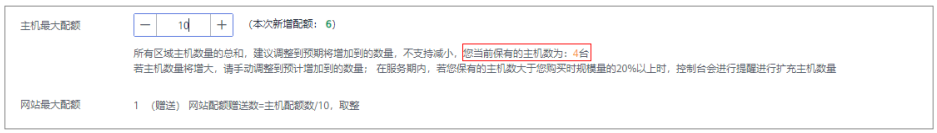
- 未授权检测的主机被攻击后，不能及时感知威胁，造成数据泄露等风险。

操作步骤

登录华为云安全中心，单击“购买态势感知”。根据规划或现有主机数量，配置主机最大配额。

更多购买操作说明，请参见**购买态势感知专业版**。

图 1-5 配置最大配额



说明

在态势感知使用期间，当账号下主机数量的总和超过主机最大配额时，您需及时扩充主机最大配额，变更版本规格，详情请参见**如何变更专业版规格?**

1.8 态势感知支持跨区域使用吗?

支持。

目前态势感知面向中国大陆用户，为全局服务。不需要切换区域，用户即可使用态势感知服务。

1.9 态势感知支持跨账号使用吗?

不支持。

态势感知服务暂不支持跨账号使用，用户仅能获取和管理当前账号下资源的威胁风险信息。

但一个账号下所有用户，即该账号及该账号下所有授权的IAM用户，可共享该账号的全局威胁风险信息。

1.10 什么是区域和可用区?

什么是区域、可用区?

我们用区域和可用区来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图1-6阐明了区域和可用区之间的关系。

图 1-6 区域和可用区

目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。不过，在基础设施、BGP网络品质、资源的操作与配置等方面，中国大陆各个区域间区别不大，如果您或者您的目标用户在中国大陆，可以不用考虑不同区域造成的网络时延问题。

  中国香港、曼谷等其他地区和国家提供国际带宽，主要面向非中国大陆地区的用户。如果您或者您的目标用户在中国大陆，使用这些区域会有较长的访问时延，不建议使用。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“亚太-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“南非-约翰内斯堡”区域。
  - 在欧洲地区有业务的用户，可以选择“欧洲-巴黎”区域。

- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。

2 购买咨询

2.1 态势感知如何变更版本规格?

购买态势感知后，当用户资产数量增加，或追加**综合大屏**功能，则需要变更版本规格，即需扩充“主机最大配额”或新增“安全大屏”。

变更包周期专业版规格

步骤1 登录管理控制台。

步骤2 单击页面的上方的“服务列表”，选择“安全 > 态势感知”，进入态势感知管理控制台。

步骤3 单击“增加配额”，跳转到态势感知购买页面。

步骤4 查看当前配置。

图 2-1 查看当前配置

步骤5 选择计费模式，“计费模式”选择“包年/包月”，按配置周期计费。

图 2-2 选择包周期计费

步骤6 添加需要增加的“主机最大配额”或勾选“安全大屏”，确认“购买时长”。

说明

- 变更为增加“主机最大配额”规格时，选择的“购买时长”为新增配额的使用时长，不影响已购买配额的使用时长。
- 新开通综合大屏的“配置费用”根据大屏的使用时长计算。已有资产配额不会重复计费，请放心购买。
- 增加资产配额的“配置费用”根据新增资产的配额数和使用时长计算。已有资产配额不会重复计费，请放心购买。

步骤7 配置完成后，单击“立即购买”。

步骤8 进入“订单确认”页面，确认订单无误并阅读《态势感知服务免责声明》后，勾选“我已阅读并同意《态势感知服务（SA）免责声明》”，单击“去支付”。

步骤9 在支付页面完成付款后，返回态势感知控制台页面，即可在版本管理窗口查看规格变化。

----结束

变更按需专业版规格

步骤1 登录管理控制台。

步骤2 单击页面的上方的“服务列表”，选择“安全 > 态势感知”，进入态势感知管理控制台。

步骤3 单击“增加配额”，跳转到态势感知购买页面。

步骤4 查看当前配置。

图 2-3 查看当前配置

步骤5 选择计费模式，“计费模式”选择“按需计费”，按小时计费。

从开通开始到取消结束，按实际防护时长（小时）计费。

图 2-4 选择按需计费

步骤6 添加需要增加的“主机最大配额”或勾选“安全大屏”。

步骤7 配置完成后，单击“立即购买”。

步骤8 进入“订单确认”页面，确认订单无误并阅读《态势感知服务免责声明》后，勾选“我已阅读并同意《态势感知服务（SA）免责声明》”，单击“确认开通”。

步骤9 返回态势感知控制台页面，即可在版本管理窗口查看规格变化。

----结束

2.2 态势感知如何收费?

态势感知服务提供包年/包月和按需计费的计费模式。

- 包年/包月

  购买1年，在总价基础上享受83折优惠，购买2年享受7折优惠，购买3年享受5折优惠。对于长期用户，推荐购买更实惠的包月/包年计费模式。

- 按需计费

  按小时计费，根据实际使用时长（小时）计费。先使用后付费，使用方式灵活，可以即开即停。

详细计费信息请参见**SA产品价格详情**。

2.3 态势感知支持退订吗?

若用户不再使用态势感知防护功能，可执行退订或一键取消操作。

- 包周期（包年/包月）计费模式：预付费方式。新购5天内的资源，支持每年10次5天无理由“退订”；使用超过5天的资源，“退订”需要收取手续费。
- 按需计费模式：按小时计费方式。资源即开即停，支持一键“取消”释放资源。

更多费用和订单说明信息，请参见**费用中心**。

退订包周期专业版

步骤1 登录管理控制台。

步骤2 单击“服务列表”，选择“安全 > 态势感知”，进入态势感知管理控制台。

步骤3 单击右上角“专业版”，显示版本管理窗口。

步骤4 针对包周期购买的资产配额或综合大屏，单击“退订”，进入“退订管理”列表页面。

步骤5 在需要退订的实例所在行，单击“操作”列中的“退订资源”，进入“退订资源”页面。

步骤6 确认待退订资源信息，选择退订原因，并勾选退订确认。

步骤7 单击“退订”，在退订管理页面确认退订。

步骤8 退订成功后，返回版本管理窗口，包年/包月计费的资产配额或综合大屏资源已取消。

----结束

退订按需专业版

步骤1 登录管理控制台。

步骤2 单击“服务列表”，选择“安全 > 态势感知”，进入态势感知管理控制台。

步骤3 单击右上角“专业版”，显示版本管理窗口。

步骤4 针对按需购买的资产配额或综合大屏，单击“取消”，一键释放按需计费的资产配额。

步骤5 返回版本管理窗口，按需计费的资产配额或综合大屏资源已取消。

----结束

2.4 态势感知即将到期，如何续费?

态势感知续费是在原已购买的版本规格的基础上，延长使用时间。续费操作不能变更版本规格，即不能改变“主机最大配额”和“安全大屏”选择。

续费操作仅针对包周期版本。

- 包周期（包年/包月）模式为预付费方式。当购买的包周期资产配额到期时，用户需通过“续费”延长使用期。
- 按需计费为按小时计费，即开即用。在账户余额充足前提下，不涉及过期情况，即无需续费操作。

手动续费

步骤1 登录管理控制台。

步骤2 单击“服务列表”，选择“安全 > 态势感知”，进入态势感知管理控制台。

步骤3 单击右上角“专业版”，显示版本管理窗口。

步骤4 单击“续费”，系统跳转至费用中心“续费管理 ”页面。

步骤5 在态势感知专业版实例所在行，单击“续费”，跳转至“续费”页面。

步骤6 配置“选择续费时长”，如选择“一年”。

步骤7 单击“去支付”，跳转至支付页面，完成付款。

步骤8 返回续费管理页面，可查看态势感知已续费成功，确认到期日期和倒计时天数。

----结束

开通自动续费

在账户余额充足前提下，已配置“自动续费”后，包周期版本将自动续费，延长使用周期。

自动续费的相关注意事项，请参见**自动续费规则说明**。

步骤1 登录管理控制台。

步骤2 单击“ 费用 > 续费管理”，跳转至费用中心“续费管理 ”页面。

步骤3 在“手动续费项”页签，选择态势感知专业版实例，单击“开通自动续费”，跳转至自动续费配置页面。

步骤4 选择配置“自动续费周期”和勾选“预设自动续费次数”。

步骤5 单击“开通”，完成自动续费配置。

步骤6 返回续费管理页面，在“自动续费项”页签，可查看态势感知已开通自动续费。

后续将根据配置，自动续费延长使用期。

----结束

2.5 态势感知到期后，会继续收费吗?

态势感知到期后，不会继续收费。

若到期后，未及时续费，会根据“客户等级”和“订购方式”定义不同的保留期时长，保留期内服务可继续使用，不收取费用。若保留期到期后，仍未及时续费，专业版会变为基础版。

2.6 如何取消态势感知自动续费?

态势感知开通自动续费后，支持取消自动续费操作。关闭自动续费后，版本到期将恢复为手动续费。

详细取消操作指导，请参见**取消自动续费**。

2.7 如何修改态势感知自动续费?

态势感知开通自动续费后，支持修改续费配置，包括修改续费设定、修改自动续费周期、重置自动续费次数等。

详细修改操作指导，请参见**修改自动续费**。

2.8 态势感知可以免费使用吗?

可以。

态势感知提供基础版和专业版两个服务版本。

- 用户可长期免费使用基础版；
- 专业版按需计费，且**综合大屏**功能需额外购买。

基础版与专业版在功能上的差异，请参见**功能介绍**。

有关**专业版**价格参考，请参见**态势感知价格计算器**。

A 修订记录

发布日期	修改记录
2020-10-10	第十八次正式发布。 本次更新说明如下： ● 修改了**为什么主机最大配额不能小于主机数量？** 问答； ● 修改了**态势感知如何变更专业版规格？** 问答。
2020-08-28	第十七次正式发布。 本次更新说明如下： ● 修改了**态势感知如何变更专业版规格？** 问答； ● 修改了**态势感知支持退订吗？** 问答； ● 修改了**态势感知即将到期如何续费？** 问答。
2020-07-09	第十六次正式发布。 本次更新说明如下： ● 新增了**态势感知到期后，会继续收费吗？** 问答； ● 新增了**如何取消态势感知自动续费？** 问答； ● 新增了**如何修改态势感知自动续费？** 问答； ● 修改了**态势感知如何变更专业版规格？** 问答； ● 修改了**态势感知如何收费？** 问答； ● 修改了**态势感知支持退订吗？** 问答； ● 修改了**态势感知即将到期如何续费？** 问答。
2020-03-30	第十五次正式发布。 本次更新说明如下： ● 新增了**态势感知支持跨区域使用吗？** 问答； ● 新增了**态势感知支持跨账号使用吗？** 问答； ● 修改了**如何获取风险程度最高的资产信息？** 问答。

发布日期	修改记录
2020-03-20	第十四次正式发布。 本次更新说明如下： • 新增了**为什么最大配额数不能小于主机数量？**问答； • 修改了**态势感知与其他安全服务之间的关系与区别？**问答。
2020-03-13	第十三次正式发布。 本次更新说明如下： • 新增了**态势感知可以免费使用吗？**问答； • 修改了**态势感知的数据来源是什么？**问答； • 修改了**态势感知即将到期如何续费？**问答； • 修改了**如何获取攻击者的信息？**问答； • 修改了**态势感知与其他安全服务之间的关系与区别？**问答。
2020-01-10	第十二次正式发布。 本次更新说明如下： • 新增了**态势感知如何变更专业版规格？**问答。
2019-09-26	第十一次正式发布。 本次更新说明如下： • 新增了**态势感知与其他安全服务之间的关系与区别？**问答。
2019-09-06	第十次正式发布。 本次更新说明如下： • 新增了**什么是区域和可用区？**问答。
2019-08-09	第九次正式发布。 本次更新说明如下： • 新增了**态势感知如何收费？**问答； • 新增了**态势感知支持退订吗？**问答； • 新增了**态势感知支持续费吗？**问答。
2019-07-11	第八次正式发布。
2019-02-20	第七次正式发布。
2019-02-01	第六次正式发布。
2018-11-06	第五次正式发布。
2018-10-16	第四次正式发布。
2018-09-06	第三次正式发布。
2018-08-06	第二次正式发布。

发布日期	修改记录
2018-04-24	第一次正式发布。

