

云安全风险巡检服务

产品简介



腾讯云

【 版权声明 】

©2013–2024 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【 商标声明 】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【 服务声明 】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【 联系我们 】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或 95716。

文档目录

产品简介

产品概述

产品优势

应用场景

产品简介

产品概述

最近更新时间：2023-11-29 17:16:51

云安全风险巡检服务（XSPM）是一款云安全风险巡检平台，监测云环境安全状态，提供云身份权限检查、云安全风险评估、云暴露面发现、云攻防矩阵视图等功能，帮助企业更好地理解和管理云基础设施服务，发现潜在的安全风险和威胁。

主要功能

云身份权限检查

提供云基础设施权利管理（CIEM）功能，帮助客户检测身份配置错误，审查云端用户和角色的访问权限，避免过度授权的安全隐患，有效降低云基础设施风险。

云安全风险评估

将云资源配置、身份权限、互联网暴露面等多种安全维度的风险评估整合到云安全风险巡检服务，通过关联云资源上下文，精准评估风险优先级，帮助客户减轻警报疲劳聚焦关键事项，高效识别云上资产的安全风险。

云攻防矩阵视图

攻击者视角呈现云安全风险分布，为客户提供完整且结构化的威胁模型，识别云环境中的安全风险，深入评估安全防御覆盖范围及潜在差距，借此优化安全防御策略，提升云端业务的安全防护能力。

产品优势

最近更新时间：2023-10-16 14:27:32

云原生优势

产品具备云原生优势，实现云资产自动发现、统一管理和实时监控，提供云安全保障，助力企业轻松应对云环境下的安全挑战。

云身份权限分析

- 提供云基础设施权利管理 (CIEM) 功能，检测身份权限配置错误。
- 识别过度特权身份，这些身份拥有高比例的未使用访问权限和强大的基础设施权限。

上下文风险评估

- 云资源关联、访问、权限等上下文信息评估安全风险，筛选有效风险。
- 全局展示可利用攻击路径，降噪风险告警，提高客户运营处置效率。

云攻防矩阵视图

- 矩阵视图呈现攻击各阶段风险分布，聚合风险维度提供用户更清晰的全局可视性。
- 评估安全防御覆盖范围及潜在差距，借此优化安全防御策略。

应用场景

最近更新时间：2023-11-29 17:16:52

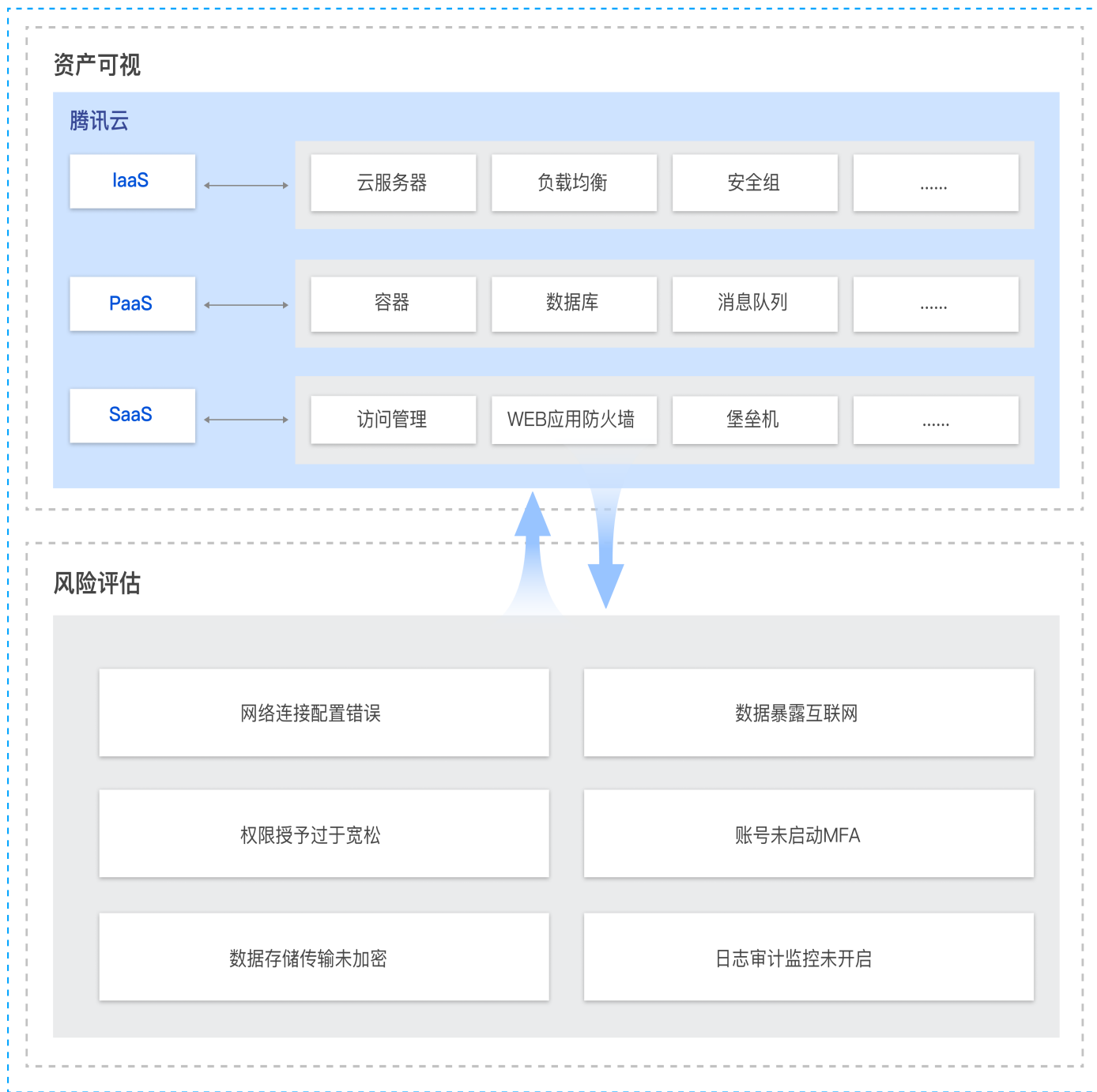
云安全风险巡检

适用场景

随着企业业务逐步迁移到云环境，云服务配置的复杂性和不断变化可能带来安全风险。企业面临缺乏云安全经验、人力资源不足等挑战，需要加强云安全风险发现和管理能力，保障业务安全。

解决方案

云安全风险巡检服务可为客户监测云环境安全状态，提供云身份权限检查、云安全风险评估、云暴露面发现、云攻防矩阵视图等功能，帮助企业更好地理解和管理云基础设施服务，发现潜在的安全风险和威胁。



多账号管理

适用场景

企业采购多个云账号部署业务服务，跨账号的安全管理变得越来越重要。企业需要在多个云账号统一管理安全策略和监控的能力，以及确保各个账号下的云资源配置符合安全要求。

解决方案

云安全风险巡检服务为客户提供多账号管理的功能，帮助企业统一管理多个云账号的安全策略和监控。