数据安全网关

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2019-08-29 15:11:05

概述

堡垒机（数据安全网关）是集用户（Account）管理、授权（Authorization）管理、认证（Authentication）管理和综合审计（Audit）于一体的集中运维管理系统。

堡垒机主要特点：

- 为企业提供集中的管理平台，减少系统维护工作。
- 为企业提供全面的用户和资源管理，降低企业维护成本。
- 帮助企业制定严格的资源访问策略，并且采用强身份认证手段，全面保障系统资源安全。
- 详细记录用户对资源的访问及操作，达到对用户行为审计的需要。

系统架构

堡垒机采用层次化、模块化设计，产品整体架构包括：资源层、接口管理层、核心服务层和统一展示层。

- 资源层：负责提供各种类型资源的资源管理交互。
- 接口管理层： 主要是实现核心层与外部产品、用户资源系统之间的数据交互，包括账号类、认证类、授权类和审计类接口。
  - 账号和角色管理接口：实现资源从账号的收集和同步管理。
  - 认证接口：实现与第三方强身份认证产品的联动和主账号认证。
  - 访问控制策略接口：实现访问控制策略的下发。
  - 审计接口：接收外部系统产生的各类日志。通过数据接口层完成与各种应用系统的相关接口通信。
- 核心服务层：完成系统各功能模块的业务处理，包括身份管理，行为管理，审计管理以及协议代理等服务，每个模块再细分若干子模块完成各自的管理功能。核心层具体的功能模块有：账号管理、授权管理、认证管理和审计管理。
- 统一展示层：负责用户交互部分的展现，一方面可对用户身份进行认证，并将可访问资源及自服务信息展示给操作人员，另一方面，可供管理人员进行管理配置和审计查看，并将管理人员的输入传递到核心服务层。

产品优势

最近更新时间：2019-08-29 15:11:28

AI 与运维管理的高效结合

从时间、命令语句、下载上传操作、访问 IP、服务器、用户名等多个维度对审计记录进行分析，将异常行为筛选并告警，确保内部恶意事件提前有效预防。

强解释性的 AI 报表

AI 引擎具备逻辑链、上下文梳理、异常情况详情等可视化模块，能够从异常行为相关事件、时间前后事件、异常原因等多个角度解释 AI 所发现的内部隐患，避免纯粹通过打分来展示异常事件，确保管理员能够理解 AI 告警，并追溯 AI 告警。

强大的资源管理能力

- 资源数量统计：支持柱形图方式查看系统中不同资源所占比例。
- 资源类型：支持主流资源类型丰富，包含 Linux 资源、Windows 资源等其他常见资源类型。

全面的账号管理机制

- 主账号支持分组管理，分组可以采用树形方式展现，不限制分组层级数量。
- 完整的用户账号集中管理：生命周期管理，实现账号的创建、维护、修改、删除的集中管理。
- 用户类型：自定义用户类型，基于用户类型进行用户地址策略。
- AD 域同步：平台与 AD 域数据同步，将 AD 域中 OU 或域用户数据作为堡垒机系统组织结构和主账号，实现数据统一，无需重复创建数据。
- 从账号管理：支持资源从账号的管理，系统具有各种资源类型驱动器，能够将资源上的账号进行自动收集、推送、抽取、同步及属性的变更等。

超强的授权管理功能

- 角色管理：系统支持自定义角色来进行权限管理。角色可按照组节点进行定义，从而实现分层分级管理模式。

- 岗位授权：资源授权模式基于岗位授权，岗位授权即是建立岗位，岗位上绑定资源账号。此方式授权可进行迁移、授权粒度更细，并可针对岗位设置相关安全策略。

单点登录 SSO

- 支持收藏夹功能：运维人员可将经常访问的资源添加到收藏夹，而且支持批量单点登录资源，体现平台运维便捷性，易用性。
- 一键式快速登录，将目标资源的登录配置信息保存为默认后，即可支持一键快速登录目标资源。
- 支持 su 用户角色自动切换操作并代填密码。

增强的计划管理功能

- 自动改密计划：支持所有被管设备的密码自动变更计划。管理员可以设置密码策略，变更密码需要符合密码策略中关于密码强度的要求。
- 密码拨测计划：定期检查平台存储的设备账号密码与设备实际密码是否匹配，以便进行校验密码一致性，提高设备的安全性，避免密码混乱发生无法登录现象。

审计管理

- 用户图形资源访问时，支持键盘、剪切板、文件传输记录，并且对图形资源的审计回放时，可以从某个键盘、剪切板、文件传输记录的指定位置开始回放。
- 支持 Windows 图形审计的监控，管理员可以随时查看运维人员的操作，并且可以发送告警信息进行会话锁定和解锁。
- 图形审计支持画质如灰度、真彩、伪真彩的设置，帧间隔，压缩比等设置，可以大大缩减图形审计产生录像文件的大小，每十分钟真彩模式下的审计录像大小为0.5M左右。

更专业的安全管理功能

- 提供认证服务器组件，所有对资源的访问都是认证服务器提供的临时会话号，即使会话号被截获，也无法通过此会话号再次访问资源，提高资源访问的安全性。
- 审计开关：根据不同设备审计安全需求，客户可自定义审计范围。例如，字符（命令、内容、录像）、图形（录像、键盘、上下行剪切板、上下行文件传输）。
- 服务端口变更：很多用户为了提高设备的安全性，不采用标准的协议端口。平台支持 FTP、telnet、ssh、远程桌面等协议服务端口变更。

- 产品自带基础的病毒检测功能，在通过堡垒机进行文件传输时，自动对传输的文件进行防病毒检测，并阻止带病毒文件的传输，有限防护服务器的安全。

应用场景

最近更新时间：2019-08-29 15:11:39

互联网+业务

互联网+业务云上资源众多，大量运维服务暴露在公网，且由于服务高度公开，容易被外部攻击者盯上。
堡垒机在业务资源远程运维时，通过隐藏真实运维端口与真实管理账户，解决远程运维安全问题。同时产品提供云上服务器运维日常审计，通过运维规则库梳理不良运维习惯，减少运维事故，帮助业务系统长期稳定运行。

企业

企业内部通常存在大量经营数据等敏感信息，这些信息在行业中具有一定价值，且容易泄密。
堡垒机为账号与岗位进行细颗粒度的权限划分，确保运维人员无法越权操作。

金融

金融行业具有大量金融、个人信息数据，且存在大量第三方代维机构，代维机构是否违规操作是金融企业需要重点关注的一个问题。
堡垒机为账号与岗位进行细颗粒度的授权控制，严格落实岗位规范，确保运维人员无法越权操作。通过 AI 引擎对运维行为进行深度分析，挖掘内部异常操作，防止金融数据被非法利用。

政务民生

政务民生在互联网化过程中，需要大量第三方机构进行建设和运维。
堡垒机可将运维方与管理方的权责分明，通过操作审计对运维问题进行追溯，确保安全事故有效定责。通过 AI 引擎对运维行为进行深度分析，挖掘内部异常操作，对民生政务数据（医疗、教育、社保、税务等信息）泄露进行预警。