软件定义边界

产品简介

产品文档

腾讯云

文档目录

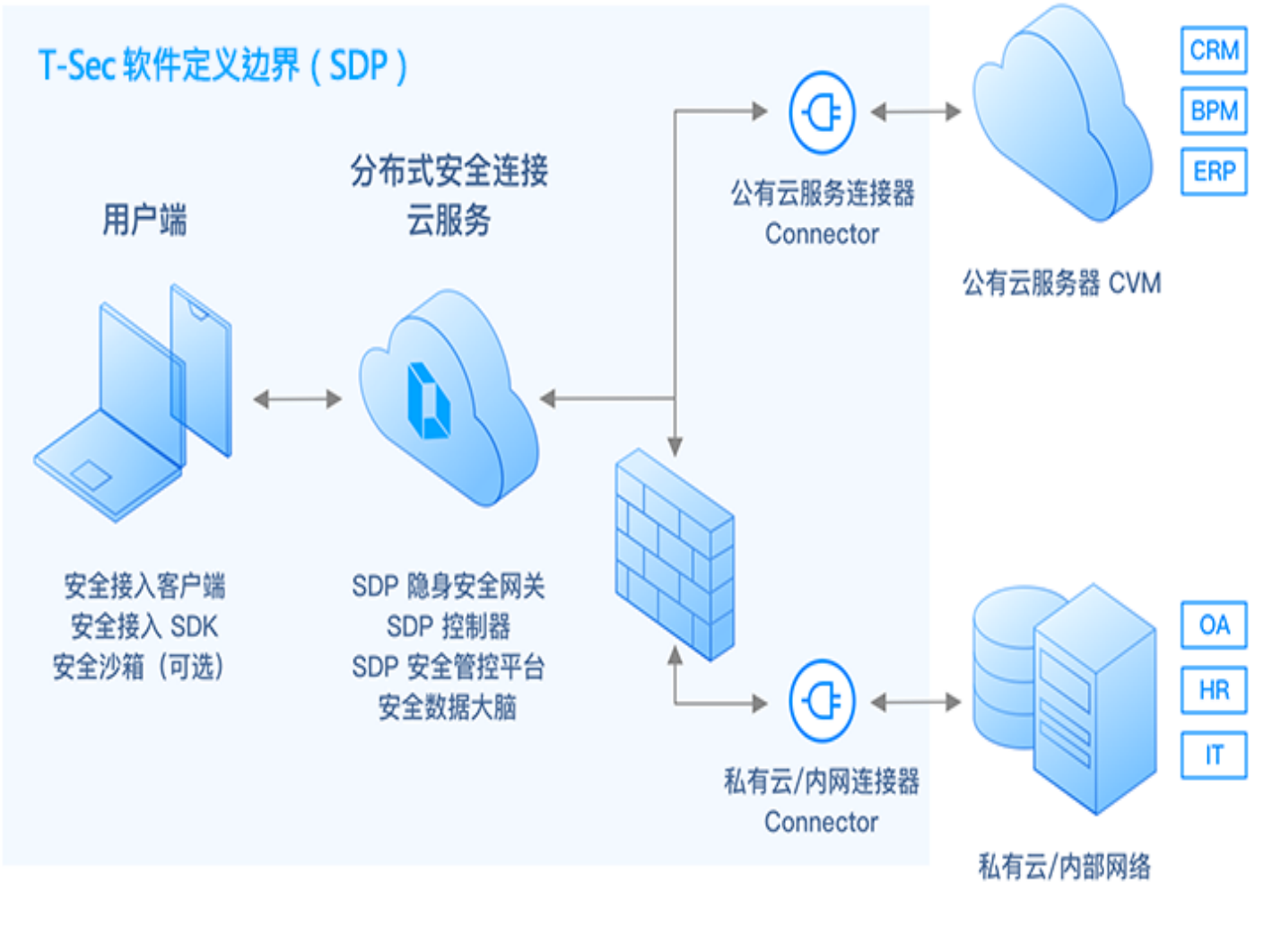
产品简介

产品概述

最近更新时间：2022-11-29 10:41:11

什么是软件定义边界

腾讯软件定义边界（Software Defined Perimeter，SDP）产品解决方案是一个遵循零信任原则，采用 云安全联盟（CSA）SDP 架构设计的新一代安全接入解决方案。SDP 主要包含六个部分，分别是 SDP 客户端、SDP 隐身网关 、SDP 控制器、SDP 连接器 、SDP 安全管控平台及安全数据大脑。

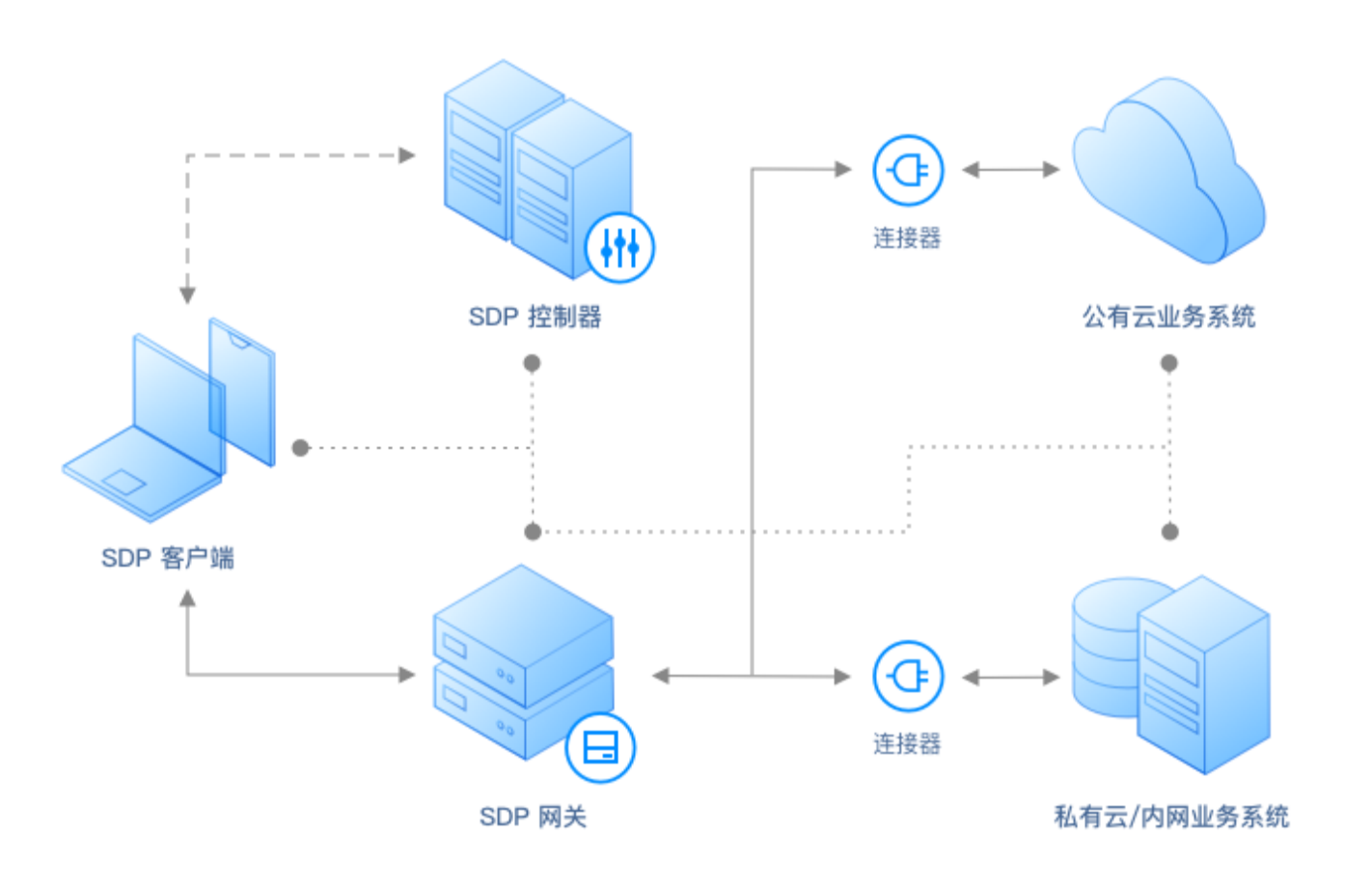


- **SDP 客户端：**
  - SDP 客户端在终端用户的设备上运行，用于与 SDP 控制器通信以请求连接，并向控制器发送设备或软件信息等数据。

  - SDP 客户端实时地对终端设备进行 App 安全、网络安全及系统安全检测以及多重用户身份验证，以确保用户身份和终端设备可信。
- **SDP 隐身安全网关**：SDP 隐身安全网关可对访问请求进行验证和过滤，还可以对已授权的访问连接进行监视、记录和报告。隐身安全网关对外不开放任何固定端口，使业务服务器仅对授权的设备可见，从而保障企业服务的隐身性。
- **SDP 控制器**：
  - SDP 控制器可对所有访问请求进行认证和动态授权，是产品架构中策略判定点。
  - SDP 控制器可对所有的访问请求进行权限判定，且不再是基于简单的静态规则，而是基于上下文属性、信任等级和安全策略进行动态判定。
  - SDP 控制器动态权限判定依据企业身份库、安全策略库、设备信誉库等数据，这些数据来源于 SDP 安全管控平台或安全数据大脑的分析结果。
- **SDP 连接器**：
  - SDP 连接器在企业应用程序所在服务器和 SDP 隐身网关之间，提供经过身份验证的安全接口。它们在运行时不需要任何入站开放端口，且企业应用程序仅通过 SDP 连接器与网关连接，无需对公网开放，以保证业务服务器仅对授权的设备可见。
  - SDP 连接器可以部署至客户私有云环境或公共云环境中。
- **SDP 安全管控平台**：
  - 管理员可以通过 SDP 安全管控平台对所有的 SDP 客户端和企业应用程序进行管理，创建并定义安全策略，为不同用户或用户组设置权限级别。
  - SDP 安全管控平台还可以与企业已有的身份管理系统对接。
- **安全数据大脑**：
  - 安全数据大脑基于腾讯安全大数据库，持续接收 SDP 访问控制的日志信息，结合身份库、策略库及数据，基于大数据和人工智能技术，对身份进行持续画像，并对访问行为和信任等级进行持续评估，最终生成和维护信任库，为 SDP 控制器及网关提供决策依据。
  - 安全数据大脑汇聚各个隐身安全网关以及所有 SDP 客户端发送过来的日志及审计信息，对汇聚信息进行大数据智能统计分析，以满足企业运维及安全需求。
  - 安全数据大脑也可以接收外部安全分析平台的分析结果，包括：终端可信环境感知、持续威胁检测等安全分析平台，这些外部风险源可以很好的补充身份分析所需的场景数据，从而进行更精准的风险识别和信任评估。

工作原理

SDP 工作原理如下：



1. 安装在用户设备上的 SDP 客户端，使用 单数据包授权（SPA）向 SDP 控制器发出访问请求，并发送设备或软件等信息。
2. SDP 控制器验证用户信息及设备信息，检查上下文，并将实时授权通过加密的 Token 传递给 SDP 客户端。
3. SDP 客户端使用 SPA 技术并附带实时授权信息，向 SDP 网关发出请求，SDP 网关根据请求信息和安全策略进行验证和匹配，然后允许或拒绝用户的访问请求。
4. SDP 网关为被允许的访问请求建立双向加密连接，客户端通过加密隧道和 SDP 连接器访问 SDP 网关所指定的企业应用服务或资源。
5. 持续动态地监控用户信息和访问行为，实时调整授权状态。

产品优势

最近更新时间：2022-04-14 10:55:28

简单高效的访问体验

SDP 是腾讯提供的一项云服务，无论对内网用户还是外网用户，都提供一致的访问体验，并与企业常用的身份验证服务商集成实现单点登录，简化终端用户操作，进而提高工作效率。

易于部署无需软硬件升级

SDP 是通过轻量级软件在用户与企业应用或资源之间建立安全连接，不依赖任何物理设备，客户只需在应用服务器之前部署SDP 连接器、开通连接器访问隐身网关权限，以及在用户终端安装 SDP 客户端，便可快速建立 SDP 安全访问体系。

更细粒度的访问控制引擎

SDP 可以使客户获得以身份为中心的更细粒度访问控制策略，控制条件包括用户群、地理位置、时间、网络及可访问应用程序等，客户可以根据其特定安全性要求动态地设置个性化网络边界和访问权限。

多重安全技术实现安全连接

SDP 采用单包授权（SPA）、动态端口机制及双向加密通信等多重安全策略实现安全连接。其中，SDP 通过 SPA 技术实现 “先认证后连接”模型，弥补了 TCP/IP 中开放且不安全的缺陷。

行为安全和态势感知

SDP 安全数据大脑可以汇聚各个 SDP 隐身安全网关以及所有客户端发送过来的日志及审计信息，对汇聚信息进行大数据智能统计分析，如用户访问趋势、资源访问分析及非法请求统计等，以满足企业运维及安全需求。

支持多场景安全接入

终端用户可在终端一键切换使用场景，从而执行不同等级安全策略，以满足不同场景及不同安全访问策略的需求。场景设置灵活、可扩展，客户可以根据业务需要扩展多种场景，终端用户可以根据访问需求选择适合的场景接入。

例如，企业财务人员需经常进入财务系统处理事务时，由于该类访问要求较高的安全性，企业可以针对该类访问，设置只面向财务人员的高安全要求的访问控制策略，财务人员必须通过此访问策略的安全检测和链路才能访问企业财务系统。而当财务人员进行普通线上办公时，使用普通场景安全接入即可。这样做到了既细粒度、高安全地保障企业资源，又提高了用户使用效率和使用体验。

可视化资源管理及控制

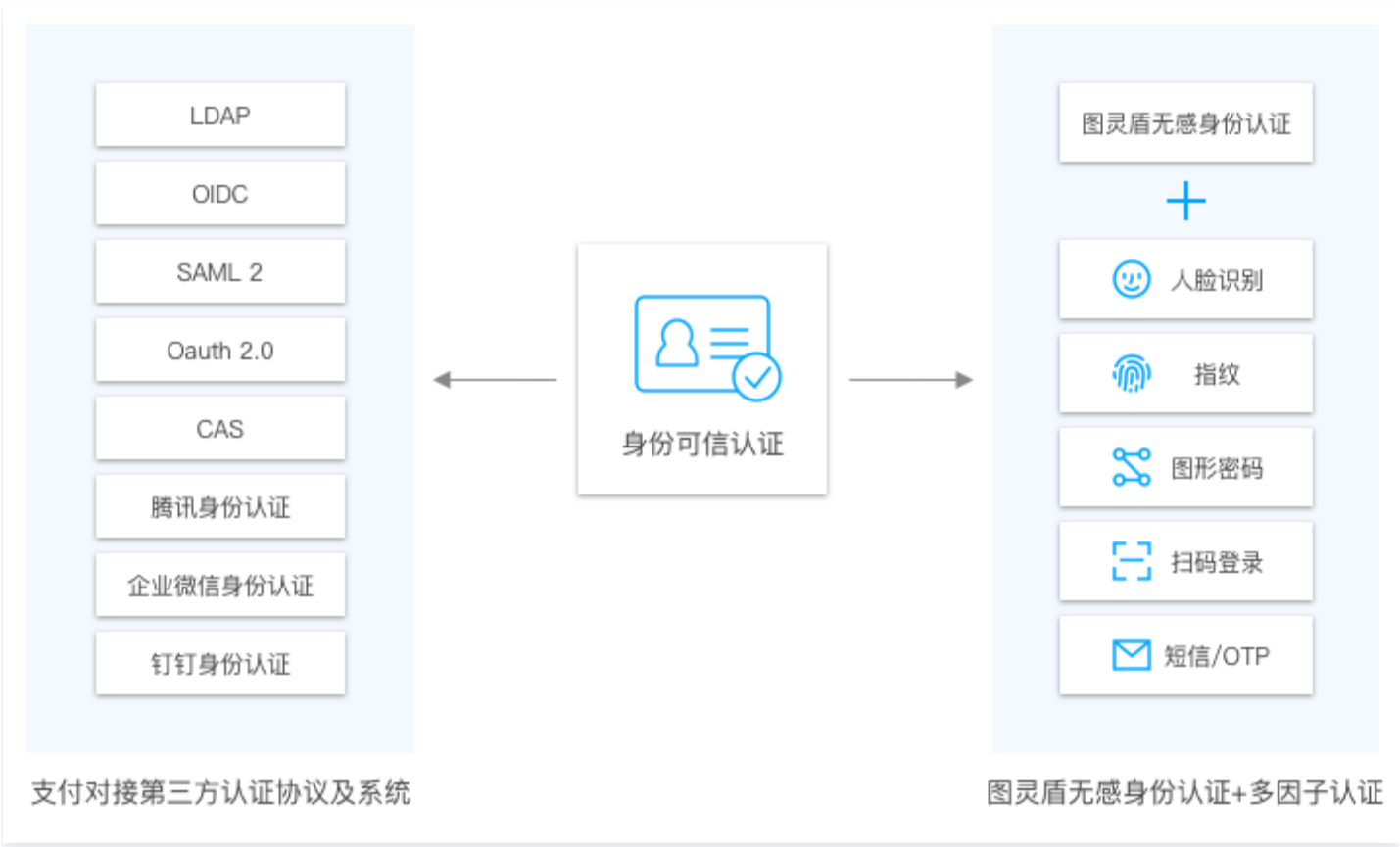
企业管理员可以在 SDP 安全管控平台上便捷地管理和控制网关、连接器及应用等资源信息，安全管控平台通过可视化的展示和操作，帮助管理员更加直观地了解到网络架构及节点运行情况。

业务服务隐身基础设施安全

SDP 安全隐身网关对外不开放任何固定端口，业务服务器仅对授权的设备可见。企业应用仅通过连接器与网关连接，无需对公网开放，保证企业业务服务的隐身性。

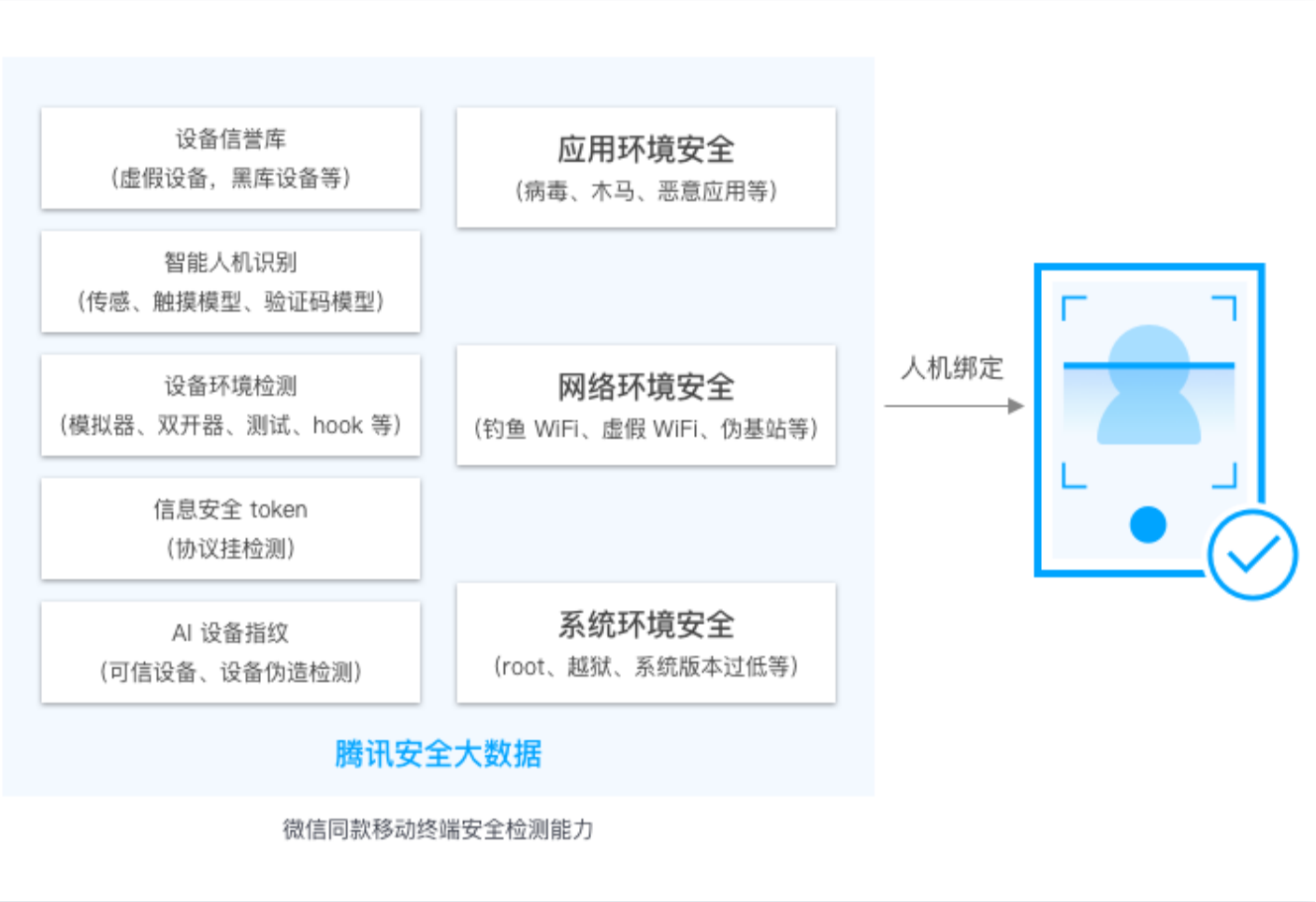
多重认证确保身份可信

SDP 集成腾讯独有的图灵盾无感身份认证 MFA 多因子认证 能力，支持人脸识别、指纹、图形密码、扫码登录、短信/OTP（一次性密码）等身份认证方式。同时 SDP 支持快速对接第三方身份认证系统，如 LDAP、OIDC、SAML2.0、Qauth2.0、CAS、腾讯身份认证、企业微信身份认证及钉钉身份认证等系统。



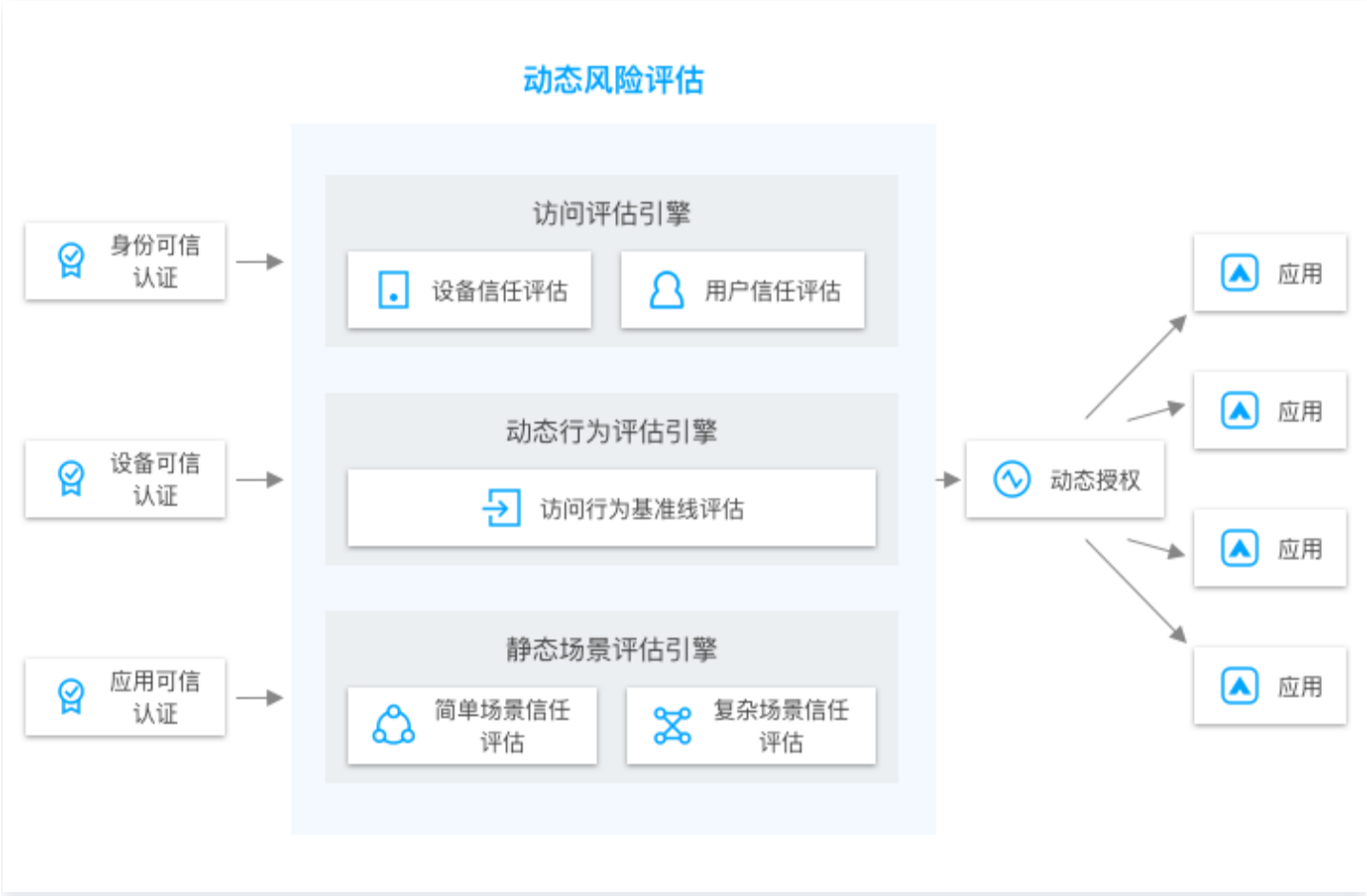
终端安全检测确保设备可信

SDP 集成基于腾讯安全大数据的终端安全检测能力，利用设备信誉库、智能人机识别、设备环境检测、信息安全 token、AI 设备指纹等安全检测能力，多维度确保企业应用环境、网络环境及系统环境的安全可信。



基于零信任的持续动态评估

SDP 遵循“零信任”安全理念，通过访问评估引擎、动态行为评估引擎及静态场景评估引擎，对用户身份、设备、行为及流量等进行动态信任等级计算，并据此进行动态授权，实现基于身份及设备信息的持续可信认证。


动态风险评估
身份可信认证
设备可信认证
应用可信认证
访问评估引擎
设备信任评估
用户信任评估
动态行为评估引擎
访问行为基准线评估
静态场景评估引擎
简单场景信任评估
复杂场景信任评估
动态授权
应用
应用
应用
应用

应用场景

最近更新时间：2022-11-29 10:41:11

企业业务安全上云

客户企业在业务上云的过程中会出现： 云上用户及信息资源的高度集中、访问人员身份复杂、公网访问应用暴露面广、终端分散、设备杂乱、网络复杂、上云应用安全级别不可控、多云访问及无统一边界等问题。

接入 SDP 产品：可以帮助客户在公有云上构建可信的、软件定义的虚拟内网，只对授权用户可见。做到业务系统隐身，减少系统暴露面，免受攻击威胁。保证只有身份及设备验证合法的授权用户才能正常访问业务系统，同时实现多因子认证以保证身份安全。

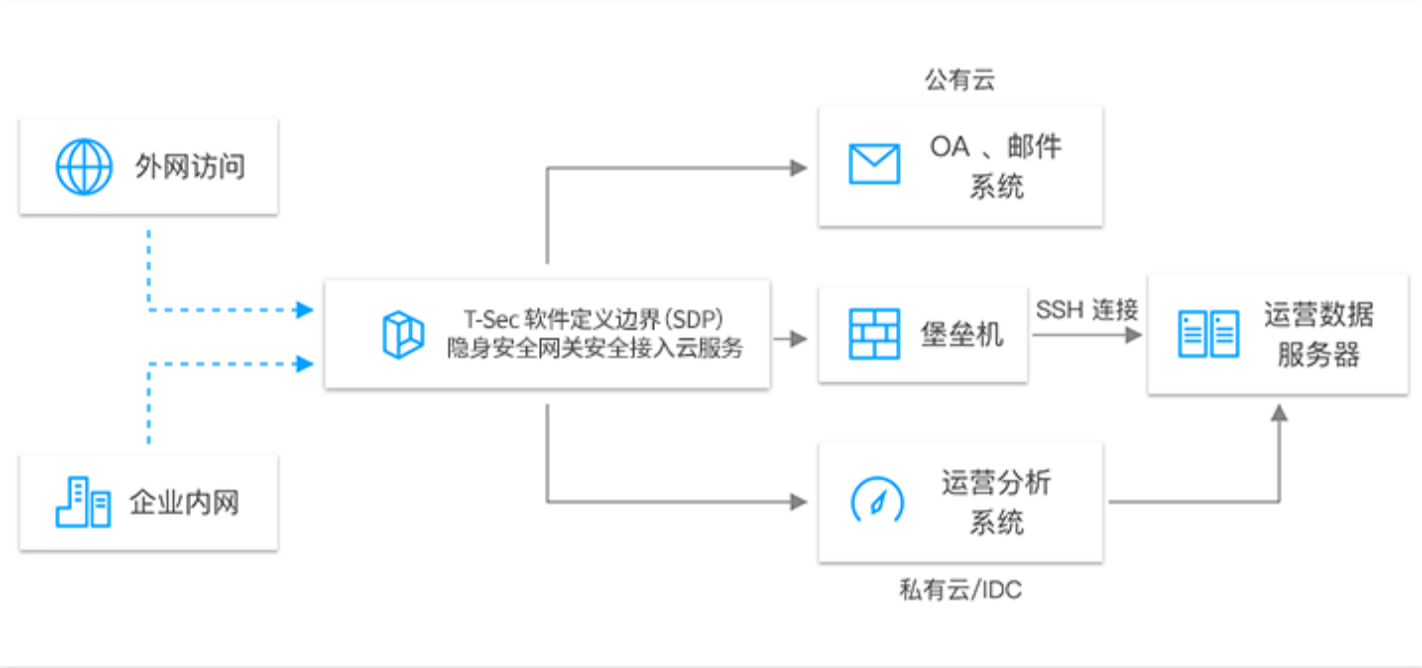
零信任远程访问

与传统的远程接入方案相比，SDP 能够解决数据泄漏、内部人员恶意威胁、DDoS 等应用和身份的安全性问题，同时做到更细粒度的访问控制、更方便的运维管理，并为终端用户提供更快速、更易用的使用体验，即可替代 VPN 进行远程办公，实现零信任远程访问。

产品	SDP	传统 VPN
用户体验	更快速、更稳定、更易用。	慢且易掉线，常莫名
应用安全	让应用“隐身”，使黑客无法扫描到受保护应用，消除各种网络攻击风险。	仍会暴露端口，黑客
访问控制	能做到细粒度访问控制。	暴露整个内网资源，
身份安全	支持多因子身份认证。	只能依靠应用自身认
运维管理	运维容易，数据可视化。	难以扩展，难以维护

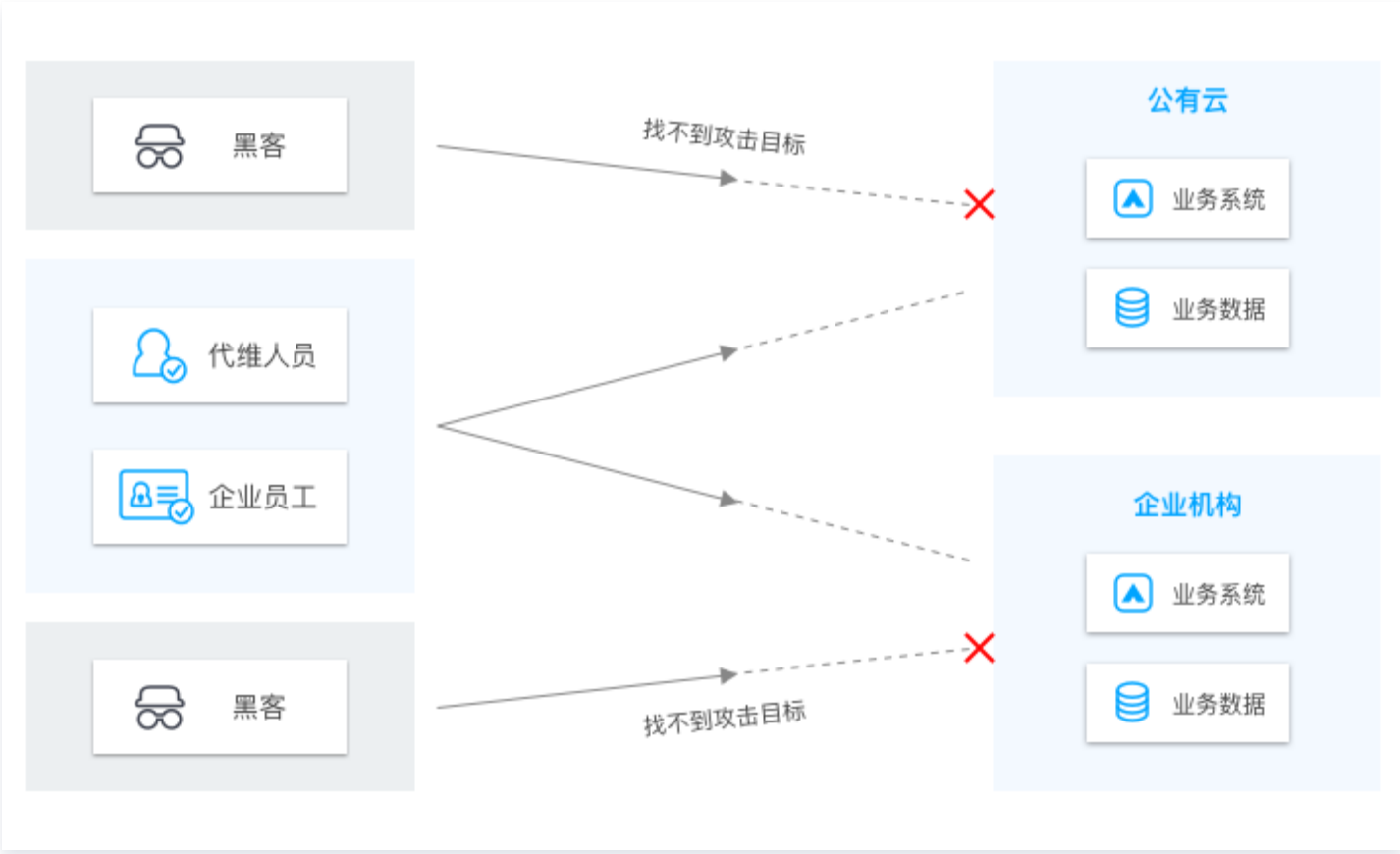
基于零信任的新职场建设

- **无边界接入**：企业内外网使用体验一致，保证远程办公、开发及运维服务。
- **攻击面缩减**：通过 SDP 隐身网关，大规模缩减企业应用的攻击面。
- **最小化授权**：基于身份持续验证与权限分级，让用户通过最小权限访问企业内的资源。
- **多云资产统一管控**：SDP 提供混合云场景下，企业资源统一访问业务管理。



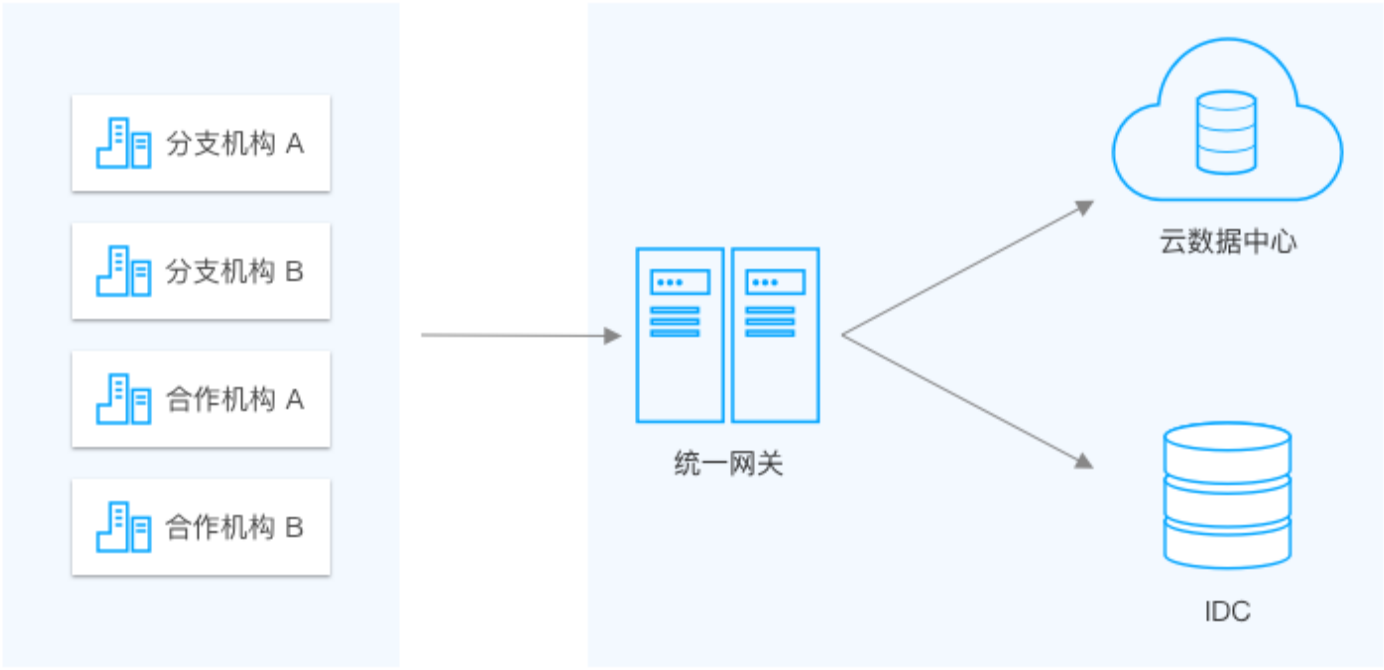
企业内网安全加固

- SDP 可以隐藏企业内部应用，企业边界无需暴露，自动化解来自外部的全天候网络漏洞扫描和入侵。
- 企业可以通过 SDP 实现统一的接入用户可视化、应用可视化及威胁可视化。
- SDP 可缓解恶意 DDoS 攻击，防止数据泄漏。



分支机构远程接入企业内部系统

- SDP 可以保障企业合并的员工数量大增，仍然可以平滑快速接入访问企业资源。
- SDP 可以极大降低企业网络边界重新规划的复杂性和时间成本（数月变为数天 ）。
- SDP 可以简化业务合并和管理，统一的安全访问和策略快速扩展到所有企业云端和数据中心的资源。
- SDP 支持全球多节点接入，保障跨地域大量的员工快速和安全接入。
- SDP 可以审计和分析所有未知流量，识别可信的用户和设备。


分支机构 A
分支机构 B
合作机构 A
合作机构 B
统一网关
云数据中心
IDC

产品价值

最近更新时间：2022-04-14 10:56:08

提升业务系统安全性

- SDP 通过最小化攻击面降低安全风险，并通过分离访问控制和数据信道来保护关键资产和基础架构，使其中的每一个都看起来是 “隐身”的，从而阻止潜在的基于网络的攻击。
- SDP 根据预先验证哪些用户和设备可以连接（从哪些设备、哪些服务、基础设施和其他参数）来控制所有连接，如果没有预先认证和预先授权，以及携带正确的 SPA 数据信息，SDP 隐身网关会默认拒绝来自恶意终端的网络连接请求，以防止因账号劫持带来的数据泄露。

综上所述， SDP 可以帮助企业建立高安全性网络架构，在边界防护、入侵防范、通信传输、身份鉴别、数据保密等方面，进一步收窄企业业务系统暴露面，更细粒度地保障业务系统的边界安全。

降低企业安全成本，提升办公效率

- **节省企业安全成本及人力**：
  - SDP 以公有云的方式为客户提供安全接入云服务。客户原有的应用无需做改造，仅需在业务服务端部署轻量级连接器实现安全访问，因此使用 SDP 替换传统网络安全组件，可降低采购和支持成本。
  - SDP 还可以通过减少或替换 MPLS（多协议标签交换）和租用线路利用率降低成本，因此企业可以减少或消除对专用主干网的使用，并降低企业安全管理人员的操作复杂度。
- **保障企业安全迁移上云**：SDP 通过降低所需安全架构的成本和复杂性，支持公有云、私有云、数据中心和混合环境中的应用程序，SDP 可以帮助企业快速、可控和安全地采用云架构。
- **提高企业用户办公效率和体验**：SDP 通过一键式的访问操作、集成企业身份认证系统实现单点登录及主动性安全检测等，降低用户学习成本，提高用户协同办公的效率。