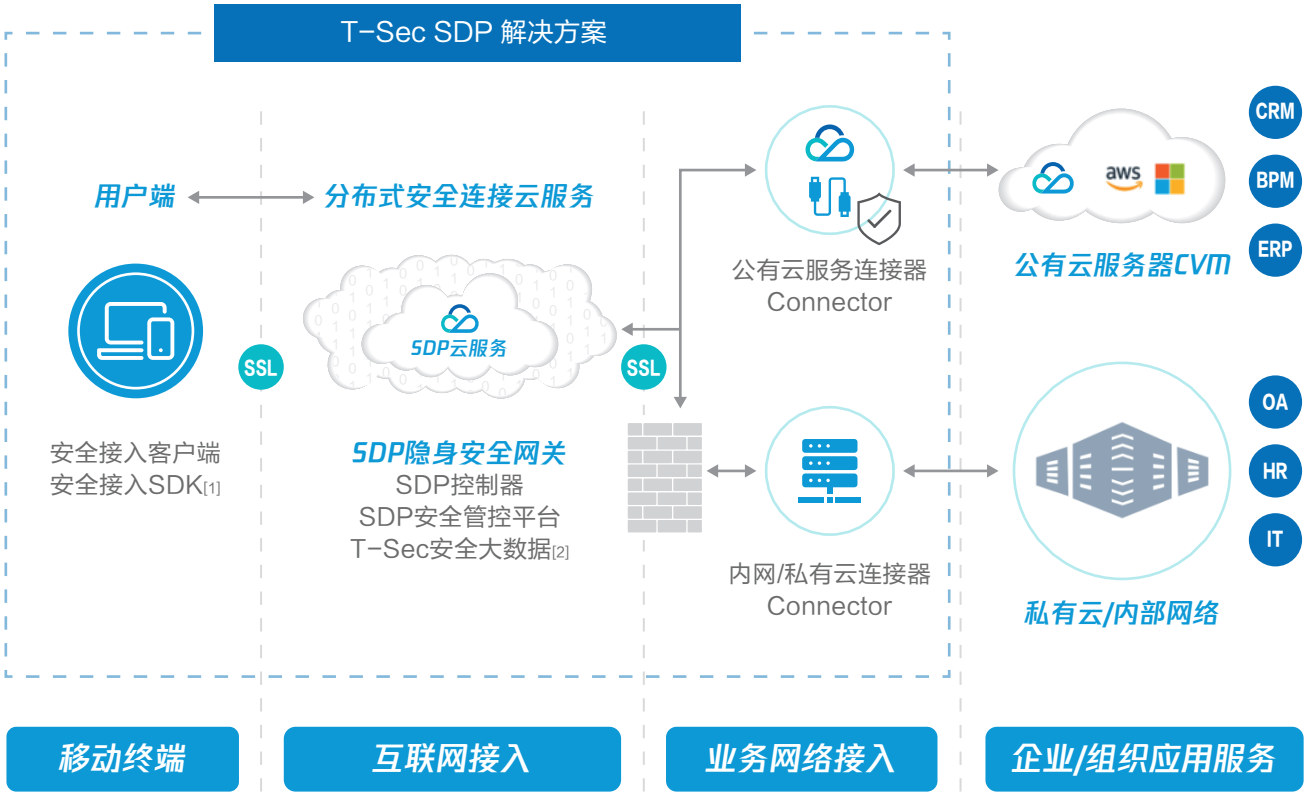
零信任轻量版（T-Sec-SDP）

腾讯T-Sec SDP（零信任轻量版）安全接入系统是采用国际云安全联盟CSA SDP架构设计的新一代终端安全访问控制方案，基于用户身份提供特定应用的最小访问权限以及清晰可见的细粒度访问控制策略，并通过网络隐身以及可信终端、可信身份、可信应用的持续性认证，实现用软件定义安全边界，保障终端用户在任意网络环境中安全、高效、稳定地访问企业资源和数据。

产品模块及架构

T-Sec SDP主要包含六个部分，分别是客户端、隐身安全网关、SDP控制器、SDP连接器、SDP安全管控平台。



[1] 开发中：包含流量转发模块、SPA模块、终端感知模块。

[2] 腾讯提供的公有云服务，SaaS版本自带。

典型应用场景

远程办公免VPN → 替代传统VPN

通过隐身网关，细粒度的访问控制，多因子身份认证等多种手段大幅提高安全性，保障在多网络环境下随时随地快速、稳定地访问企业资源，大幅优化提升企业远程接入办公内网环境，进行办公、开发和运维体验与效率。

企业内网安全加固→重保，防扫描

通过隐身网关隐藏企业内部应用，收敛关键资产互联网暴露面，不给潜在攻击者任何扫描和攻击的机会，自动化解来自外部的网络漏洞扫描和入侵。以及缓解恶意DDOS攻击，防止数据泄漏。

企业应用访问控制

根据用户身份与访问需求进行差异化、极细粒度的动态访问控制，确保公有云/私有云应用的安全访问。

多云环境的统一安全访问

支持混合云场景下企业资源的统一访问业务管理，保障企业的云上业务安全。

终端设备的基础安全防护

终端的安全检测与防护，确保只有合法的设备可接入。

自动化安全管理

通过统一的身份管理、认证及授权，收拢传统的多系统管理模式减少IT人员工作量；公有云vPC部署低成本运维，避免安全架构的重复建设。

安全监测

实时监控、分析用户的访问行为，识别异常。

产品价值和优势

腾讯安全能力

腾讯20年安全防护经验及腾讯的品牌能力，拥有国内首个互联网安全实验室矩阵，并汇聚国际最顶尖白帽黑客。

业务服务隐身，基础设施安全

T-Sec 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，保证企业业务服务的隐身性。

差异化、细粒度的访问控制引擎

T-Sec 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、设备、网络、风险及可访问应用程序等。

易于部署

公有云VPC部署和私有化部署，均无需软硬件升级，T-Sec SDP可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，不依赖任何物理或虚拟设备。

终端安全检测确保设备可信

基于腾讯安全大数据积累下来的强大终端设备安全检测及修复能力，利用设备信誉库、智能人机识别、设备环境检测、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、系统环境的安全及可信。

简单高效的访问体验

对无论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。

落地案例

案例一：某运营商省级公司远程运维接入

背景

本项目主要用于运营商应急响应中心远程运维场景，该公司有百量级的抗拒绝服务等安全产品管理系统，在非办公时间需要通过公网接入进行监控。

客户诉求

- 系统分布在运营商云的各节点，传统VPN无法统一接入管理；
- 应用系统数繁多，需要有快速接入能力；
- 需支持ssh、远程桌面等运维接入。

应用效果

- 在不同网段配置连接器，实现跨网段的应用系统访问；
- 两天内完成50+抗拒绝服务管理系统接入；
- SDP支持所有基于TCP协议，可使用各种基于TCP的远程C/S远程管理工具。

案例二：某政府信息中心远程运维安全保障

背景

某政务业务系统部署在云环境上，日常运维人员登录堡垒机是通过VPN接入，但VPN存在端口暴露，在某次HW攻防中被攻破，导致内网穿透。客户寻求新的接入方案以增强安全性。

核心诉求

- 缩小系统公网暴露面，减少被攻击风险；
- 最小化授权，杜绝内网穿透导致其他系统受攻击；
- 需支持堡垒机、ssh、远程桌面等运维使用。

应用效果

- 业务系统通过SDP安全网络加固，不对公网开放，减少了绝大部分的来自互联网的攻击；
- 控制接入者访问权限，最小化授权，接入者仅允许访问特定的堡垒机资源及端口；
- 高可用部署，保证了在重点保障时间段业务的稳定性。

案例三：某地图测绘服务提供商众包人员远程接入作业

背景

2021年初，国内某市疫情有爆发趋势(石家庄封城)，客户启动了灵活地点办公，由于人员众多且原VPN老旧，无法扩容，需要有便捷方案快速实现远程接入。

业务特点

- 接入作业人员众多（数百人），且业务应用特殊，访问时会并发大量请求，传统VPN作业卡慢，无法正常使用；
- 接入时间急，要求一天内完成应用接入，实现远程办公；
- 过程中，众包服务提供商数不断提升，需要快速实现扩容，且作业人员职能各有不同，需做访问权限控制。

应用效果

- 客户通过SAAS版SDP接入业务系统，在作业人员增加的情况下，弹性扩容得到等同于内网访问的体验，操作无延迟；
- 1天内完成作业系统接入及人员导入，短信验证码验证提升安全性；
- 按业务场景及角色制定访问策略，先认证后连接。

案例四：业内某知名第三方支付公司远程接入

背景

公司的内部办公应用均部署在企业内部数据中心，如OA、财务、客服等。针对部分高敏业务，企业使用VPN及远程桌面方式接入，体验差，成本高；普通办公应用则直接开放公网权限，存在较大安全风险。

业务特点

- 金融支付类行业，安全性要求极高；
- 分公司较多有较大的远程接入应用系统需求；
- 客服等部门有外包员工，需要控制访问权限。

应用效果

- 业务系统接入SDP网络，通过隐身网关实现应用系统隐身；
- 按业务场景及角色制定访问策略，先认证后连接；
- 两周内完成第一批12个应用接入，试运行。

案例五：在线教育/远程教学/校园网接入

背景

在线教育系统为云+本地混合环境部署，系统部署在公有云/本地数据中心。学生分布范围广（国内外），疫情原因无法在校学习，绝大部分教学系统直接公网开放给学生使用，VPN安全性/扩展性较差。

核心需求

- 教师/学生人员多角色安全访问教学系统；
- 全球学生在线接入云+本地混合部署的在线教育平台；
- 对核心内部教研管理系统端口隐藏，提升系统安全性。

应用效果

- 学生在终端安装轻量级的agent实现远程校园网安全接入；
- 收拢了原外网开放的业务系统，业务系统不在公网暴露；
- 教研、教学、在线教育系统分权限管控，身份认证接入。