TSM终端安全管理系统

华为技术有限公司

HUAWEI

来自终端安全管理的挑战

根据加利福尼亚州旧金山的计算机安全协会(CSI)的观点，大约60%到80%的网络滥用事件起源于内部网络。在企业网络中，任何一台终端的安全状态都将直接影响到整个网络的安全，这些问题极大地困扰着企业高层管理人员和IT部门。

1) 员工安全意识薄弱，企业安全策略难以实施，网络病毒泛滥
2) 非授权用户接入网络，重要信息泄漏
3) 网络资源的不合理使用，工作效率下降
4) 内网管理存在法律法规遵从的风险

华为终端安全管理系统介绍

TSM（Terminal Security Management，终端安全管理）系统是华为公司推出的企业终端安全管理产品，通过网络身份识别、接入控制、终端安全加固、行为管理、网络防护、数据保护、桌面管理等技术，帮助企业提升终端安全防御能力从而降低病毒、木马、间谍软件以及其他恶意软件感染入侵机会、降低企业信息泄密风险、确保员工合法使用网络资源、提升员工办公效率、节约IT预算、保证遵从性。同时以技术手段降低部署成本和复杂性、为内网终端安全管理提升效率并减轻压力。

TSM终端安全管理系统由终端安全管理服务器、安全接入控制设备和终端安全代理组成。其中安全接入控制设备支持安全接入网关、802.1X交换机、华为系列交换机、华为系列AC/AP设备和防火墙等设备。

产品特性

全面的网络准入控制

一体化接入控制：提供基于接入层、汇聚层网络设备（交换机、Wlan、防火墙等）联动的准入控制方案，适应无线、有线、VPN、拨号等各种复杂接入环境，无需调整现有网络拓扑，部署简便

多种认证方式：提供802.1x认证、Portal认证、MAC认证等多种认证方式，接入用户可通过客户端、Web、Web Agent发起认证，灵活适应企业雇员、合作伙伴、访客等各种网络接入用户的认证需要

自适应自修复：客户端准入认证方式自适应、对不合规终端自动或引导式修复，在保证企业网络接入安全性的同时，兼顾了终端用户的友好体验。

方便的系统管理能力

快速部署：提供基于portal交换机或防火墙提供客户端下载页面推送，实现客户端快速部署。

集中化管理配置：提供基于Web的配置管理界面，集中对网络接入控制、终端安全管理、桌面运维管理进行管理配置，方便日常维护管理

设备自动发现：自动识别IP打印机、IP电话、IP扫描仪、部门专用服务器等非PC类设备，免除在NAC部署前后需要对该类设备逐一采集登记和维护的麻烦。

通过匿名认证和访客管理，实现对于访客或合作方人员使用内部资源的合理管理，最大限度降低管理员的工作量。

提供终端违规自动提醒、一键自动或引导式修复，实现终端自我管理。自动识别终端用户所处的场所，自动选择相应安全策略，方便员工外出和企业内异地接入办公。

提供基于用户的管理和终端遵从性打分，量化评估终端安全状况，系统安全状态和趋势一目了然。

灵活扩展，云知识库更新

支持给部门或分支机构追加日志数据库，满足超大规模日志审计需要。
支持自定义检查策略，指定检查项，定制终端提示信息和违规上报信息，定制自动修复动作，免升级快速响应新需求，如清除恶意代码、给应用程序打补丁、配置应用程序、修复软件或环境异常等。
系统预制了大量安全策略和日常管理需要的报表，同时用户还可自定义或从公司云安全中心获取丰富的策略库和报表库，满足个性化和持续演进的安全要求。通过智能分析和深度挖掘，辅助各领域清晰了解企业内网状况，为IT管理提供足够的运维和决策支持。

功能全面，涵盖终端安全管理所有方面

将网络准入控制、终端安全加固、办公和上网行为管理、网络防护、信息泄密防护、资产管理、软件部署、远程协助等功能高度集成，为企业建立一体化、完整的终端安全管理方案。
可整合文档安全和移动存储设备管理，形成业界最完善的、端到端的安全解决方案。
丰富的行为审计功能：提供全面的用户行为审计功能，对用户使用网络和计算机资源的行为进行管控，包括USB设备监控、非法外联管理、进程与服务监控、ARP防护等。

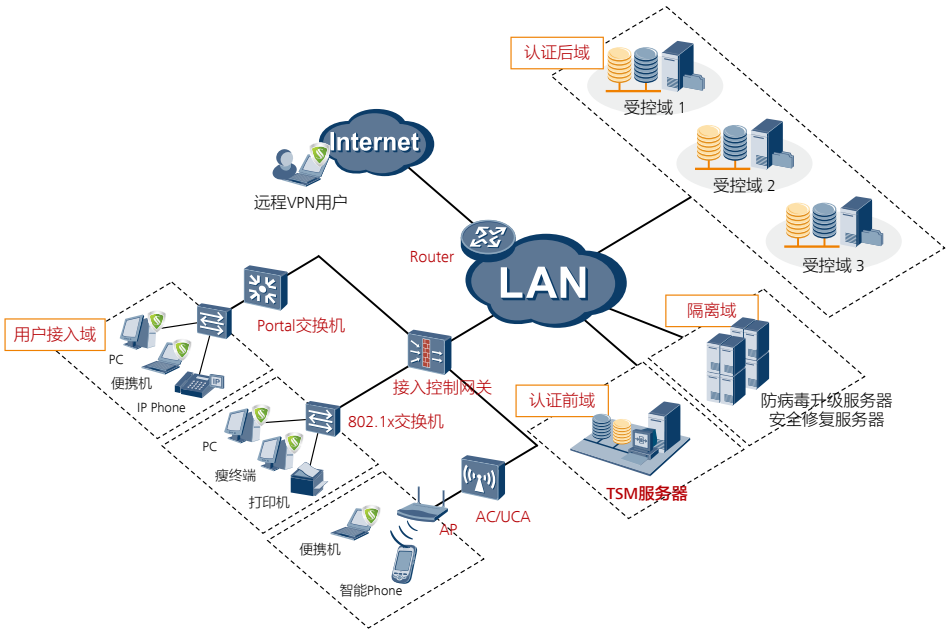
产品规格

功能	规格
网络身份识别	匿名认证：管理员可在指定网络区域开放匿名认证，终端用户选择匿名认证时无需输入密码
	基于系统的内建帐号认证
	Windows活动目录 (AD) 认证
	第三方LDAP联动认证
	移动证书认证 (PKI/CA)
网络准入控制	合规性检查：包括安全评估、系统配置等，限制不满足合规性要求的终端访问受保护资源
	自动隔离不合规终端，一键自动修复终端问题
	基于用户授权访问范围，杜绝非授权访问
安全管理	安全加固：包括静态配置检查 (防病毒、补丁、可疑注册项、可疑进程、非法软件安装等) 和动态审查
	(端口使用、开启最小服务、外设接入、ARP检测、流量监控等)，识别并修复潜在威胁
	办公行为管理：包括WEB访问、媒体下载、非办公软件等
	信息外泄防护：包括外设和移动存储设备管理、非法外联行为控制、网络程序控制等多重防护手段
桌面管理	补丁管理：一站式补丁自动检查和修复，基于设备和补丁维度展示补丁部署情况，支持与WSUS联动
	IP资产自发现：自动发现IP打印机、IP Phone、智能手机、收银机、条形码扫描仪等不可管理设备
	资产生命周期管理：防止企业软硬件资产流失，实时掌控企业资产情况
	软件分发：对于企业内大文件下发采用分布式存放和子网快速转发技术，低带宽占用、高效率分发软件
	远程桌面协助
	消息公告：对指定用户/部门推送公告消息，并可设置公告信息有效期
策略管理	分权分域：支持不同的管理员管理不同部门的不同业务
	策略模板：在策略模板内集中配置策略和参数，不同用户或不同部门间可以引用同一策略模板
	场景切换：支持基于终端所处不同的场所应用不同的安全策略
	支持自定义或从安全中心获取策略
可运维报表	预置常用报表模板
	预置常用趋势报表
	支持自定义或从安全中心获取报表
系统管理	系统运行状态监控：当服务器出现异常时，提供服务器告警功能，包括对话框告警、邮件告警等
	客户端在线故障诊断，集中处理客户端故障
	远程数据备份
组网模式	集中式组网：适用于终端规模较小，网络层次较清晰的环境
	分布式组网：适用于存在多个分支机构或终端规模相当大的环境
	分级管理：适用于网络规模超大，需要部署多套TSM系统的环境

应用场景

企业NAC（网络准入控制）场景

TSM系统提供丰富的网络准入控制技术方案，完美解决企业内网的网络准入控制需求。

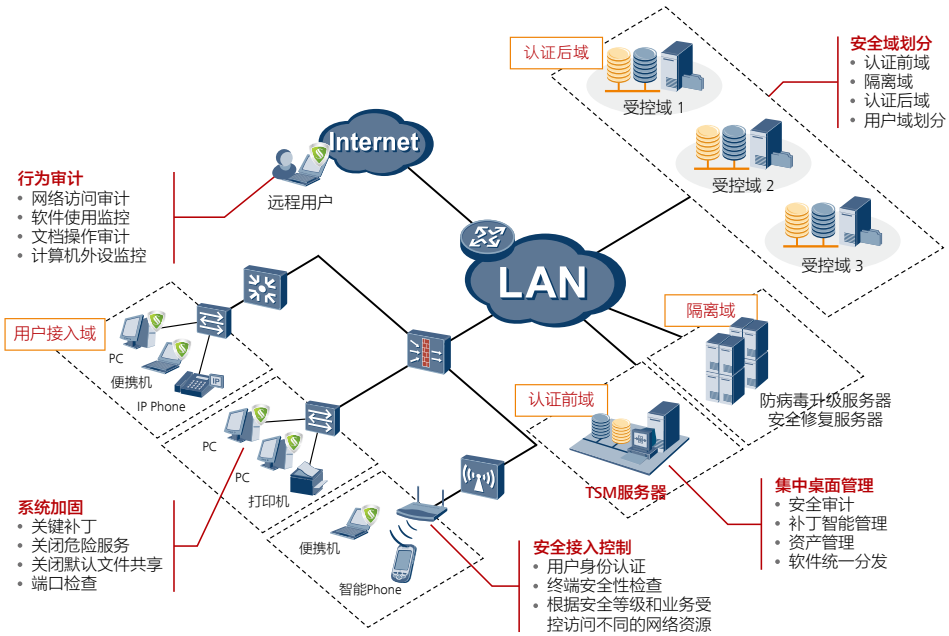


TSM系统支持与交换机、路由器、防火墙、Wlan等网络设备联动，根据终端用户身份认证和安全检查的结果进行网络准入控制，并根据用户角色授权用户相应的网络访问权限，保证企业内网的接入安全。

客户价值：通过部署NAC解决方案，提高终端准入安全性，同时支持与交换机联动的802.1x/portal网关方案、与USG防火墙联动的网关方案，适应无线、有线、VPN、拨号等各种复杂接入环境，客户无须对网络升级即可部署，有效减少客户投资。

企业终端安全场景

TSM系统提供丰富的终端安全管理功能，如网络访问控制、主机健康性检查、外设管理、行为管理、补丁管理、资产管理、软件分发、远程协助等功能，全方位、一体化解决企业在终端安全管理方面遇到的问题。



TSM系统对企业内网的网络资源基于“最小授权”和“业务相关性”原则划分为不同的认证域，基于终端用户的角色进行授权访问；并且在用户使用企业网络资源和计算机资源的工程中，对用户的行为进行监管；同时，为管理员提供桌面统一运维功能，能够远程、统一进行软件分发、补丁分、发远程协助等，提高企业的桌面运维能力。
客户价值：客户可建立一个一体化、完整的终端安全管理体系，有效提升终端安全性，降低内网安全事故，同时提高企业的桌面运维能力，降低企业桌面运维成本。

订购信息

项目	描述
功能服务端费用	提供接入控制模块控制项、安全策略管理模块控制、资产管理模块控制项、软件分发模块控制项、补丁管理模块控制项、员工行为管理模块控制项、USB移动存储介质管理模块控制项7大功能模块，根据客户需求选择相应的功能模块。
终端Licenses费用	每个功能模块均对应一种终端Licenses。Licenses数为现网实际终端数，所有功能模块的Licenses必须保持一致。
安全接入控制设备	根据安全接入控制方案选择相应的准入控制设备及其型号。
外购件	可以选购服务器整机，操作系统，数据库等，也可以自备。
服务	系统安装调试服务，安全设备适配。

免责声明

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺。华为可能不经通知修改上述信息，恕不另行通知。

华为技术有限公司

深圳市龙岗区坂田华为基地

电话: (0755) 28780808

邮编: 518129

版本号: M3-035027-20121106-C-1.0

www.huawei.com