

★完全公开

奇安信网神零信任 环境感知系统(TESS) 产品彩页

地址：北京市西城区西直门外南路26号院1号

邮编：100044

1 产品简介

1.1 产品定位

奇安信网神零信任环境感知系统 (TESS: Trust Environment Sensor System) 是基于“零信任架构”，基于云计算、大数据成为业务新载体这一趋势，针对威胁离业务越来越近的现状，推出的一款终端零信任产品。通过多维度的终端感知与风险度量，并结合业务访问控制手段，能够实现对终端唯一身份的识别、风险的动态感知与度量，将终端威胁对业务的影响面降到最低。

奇安信网神零信任环境感知系统 (TESS) 的功能是通过多维度的终端感知方式采集和分析终端安全环境，包括设备环境、系统环境及应用环境等，并对采集数据进行风险度量，结合设备可信技术、应用可信技术和身份可信技术以确保主体可信。奇安信网神零信任环境感知系统 (TESS) 还将环境可信评估结果返回给可信访问控制中心以实现动态授权策略的判定，并结合可信代理实现对业务的安全隔离，对风险的动态响应，对人员的动态鉴权和授权。

奇安信网神零信任环境感知系统 (TESS) 拥有设备级的可信标识、可信密钥与可信证书，优先采用国产可信芯片，并支持白盒加密技术、沙箱技术等安全技术，保证设备身份的可信。

奇安信网神零信任环境感知系统 (TESS) 是零信任产品家族中新的一员，可以通过跟奇安信网神零信任身份服务系统 (TAC)、奇安信网神零信任应用代理系统 (TAP)、奇安信网神零信任 API 代理系统 (TIP)、奇安信网神零信任身份分析系统 (IDA)、智能手机令牌联动，形成完整的零信任解决方案，共同解决设备可信任、人员可信任、应用可信任，最终实现业务安全访问的结果。

1.2 关键技术

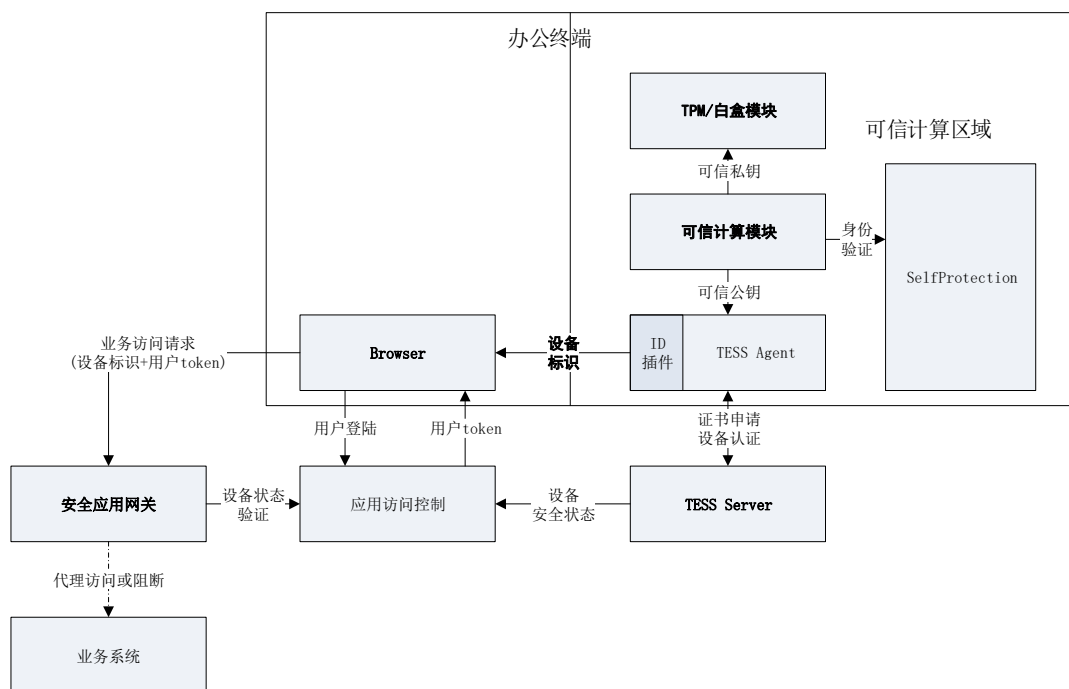
(1) 终端可信标识技术

终端可信标识技术里最重要的是设备标识技术，目前市面上的设备标识技术中，都是直接使用硬件信息做为设备标识，未解决终端标识的被恶意窃取、仿冒等问题。做为零信任体系中关键技术之一，需要能够唯一、延续性标识一个终端设备，因此必须要引入终端可信标识的概念和技术。

终端可信标识需要满足如下需求：

- **可用**: 此标识应该可以被计算出来, 不会由于攻击或终端用户有意而导致无法计算, 或对于无法计算的情况, 应作为异常情况处理。
- **可信**: 此标识不能被仿冒, 包括不能被掌握终端的全部权限的人仿冒, 以及不能被网络层攻击者 (如 sniff) 仿冒。
- **不变**: 此标识需要防止被破坏, 如果试图破坏此标识, 应该能够探测到并恢复原本的标识; 在设备的关键硬件和操作系统等没有发生变化的时候, 此标识不应该改变; 需要考虑云桌面等虚拟环境下, 此标识对于实质上的同一套硬件应该不变。
- **唯一**: 此标识对于不同的设备应该是不同的, 对于同一系统的关键硬件 (如硬盘等) 发生变化之后, 或终端操作系统重装后, 设备标识应该发生变化。
- **稳定性**: 即使设备发生临时性故障如磁盘的磁道损坏、临时增加外设等情况, 设备的标识不应该快速变化; 不应由于实现本身的 BUG 导致标识频繁变化。

终端可信标识的逻辑架构如下图所示:



组件与功能说明:

- **TESS**: Trust Environment Sensor System, 奇安信网神零信任环境感知系统。
- **TESS Agent**: TESS 的 agent 程序。
- **TESS Server**: TESS 的服务器端。
- **TPM**: Trusted Platform Module, 可信平台模块。

- TPM 安全芯片：符合 TPM 标准的安全芯片。
- 白盒模块：TESS 的白盒加密模块，用于没有 TPM 芯片的场景下白盒化存储设备可信私钥。
- 可信计算模块：TESS Agent 的核心模块，提供私钥的安全存储和数字签名的安全运算。
- SelfProtection：驱动级的程序保护组件，包括对程序的进程、文件、注册表的保护。
- 设备硬件 ID：定义的使用设备核心硬件信息计算所得的 ID，目前为 cpuid、硬盘序列号、第一块物理网卡的 MAC 地址计算所得。
- 设备可信私钥：TESS Agent 身份认证用到的私钥，后续的设备 ID 获取、核心信息上报需要用到。
- 设备可信证书：用和终端可信私钥配合使用的公钥颁发的公钥证书，还附加了设备硬件 ID、设备使用人等额外信息。
- TESS 服务端公钥：用于认证 TESS 服务端身份的公钥证书，安装 TESS 服务端软件时自动生成。
- TESS 服务端私钥：安装 TESS 服务端软件时生成的私钥。
- 设备可信标识：用于标识设备的唯一标识，目前为设备硬件 ID 用可信私钥签名，再用 TESS 服务端公钥加密后的字符串。

(2) 终端风险度量技术

奇安信网神零信任环境感知系统 (TESS) 提供基于终端风险的度量技术，该技术包括两部分内容：风险评分和风险报告。风险评分主要目的是提供快速终端可信鉴定能力，所有业务安全访问策略可以基于分数的高低来进行设置；风险报告主要目的是提供深度终端可信鉴定能力，所有业务可以基于报告中的具体属性进行细粒度的业务访问控制。

● 风险评分

奇安信网神零信任环境感知系统 (TESS) 采用“可信加权”原则，将所有风险项产生的权值进行相加，以百分制提供给策略方，策略方再根据不同的权值制定相应的安全策略。

目前奇安信网神零信任环境感知系统 (TESS) 采用“感知模板”的方式来定义终端的可信程度，该模板由管理者根据自身的情况进行自定义。

奇安信网神零信任环境感知系统 (TESS) 对所有感知项进行三种等级划分：潜在风险、一般风险、严重风险，这三类风险的含义与扣分标准如下表所示：

| 风险设定 | 说明 | 扣分标准 |
|------|----|------|
|------|----|------|

| | | |
|------|-------|-------|
| 潜在风险 | 风险系数低 | 0-100 |
| 一般风险 | 风险系数中 | 0-100 |
| 严重风险 | 风险系数高 | 0-100 |

表：风险设定表

奇安信网神零信任环境感知系统 (TESS) 采用初始 100 分制，每发现一个风险项则扣除设置的分数，管理员可以根据业务需要设置不同的策略模板和度量标准。奇安信网神零信任环境感知系统 (TESS) 从基础安全感知、系统安全感知、应用合规感知、健康状态感知等四个方面对终端的安全状况进行全面感知和度量。

- 风险报告

奇安信网神零信任环境感知系统 (TESS) 会将识别出的风险种类及属性形成风险报告传递给访问控制中心，访问控制中心可以根据将具体属性与业务进行绑定，实现更加细粒度的访问控制策略。

(3) 终端接口开放技术

奇安信网神零信任环境感知系统 (TESS) 为开放平台架构，能够提供对应的标准接口能力，用以与其它产品形成解决方案，支持的接口类型如下：

- 身份认证系统。能够对接第三方身份认证系统。
- 应用访问控制系统。能够对接第三方 ACL 控制系统。
- 终端安全防护类产品的标准化调用接口。如防病毒/漏洞模块等。
- 可信环境感知的属性可标准化接口输出。输出对应的感知属性或终端分数提供给第三方平台进行访问控制。
- 在完成调试后，提供第三方软件测试报告以及安全评估报告。

2 控制中心功能介绍

奇安信网神零信任环境感知系统 (TESS) 分为客户端和服务端两部分。服务端负责接收客户端上传的信息，下发客户端的策略配置。

控制中心可支持国产化环境部署，需要配置 1 台接入服务器、一台 Web 服务器。每台服务器 CPU 最少 16 核 2.4Ghz、32GB 内存、1TB 硬盘，采用国产化中间件、数据库和操作系统。

2.1 终端管理

能够对安装了奇安信网神零信任环境感知系统 (TESS) 客户端的电脑进行统一管理, 能够对所有终端进行统一分组管理、查看所有终端的状态、并针对终端进行策略统一下发等。支持国产化客户端、windows 客户端 (windows7、windows10)、国产化客户端 (中标麒麟、银行麒麟、通信 UOS 等) 等环境;

能够对安装了奇安信网神零信任环境感知系统 (TESS) 的所有终端进行密码保护策略设置、升级策略设置; 能够配置与控制中心的通讯策略、网络流量策略、终端数据上报接口频率设置, 并对终端的外观进行自定义。

终端身份标识由环境感知服务结合终端属性生成, 具备唯一、永久、防篡改、不可伪造等特性。环境感知服务能够基于终端身份标识来管理环境中的可信终端, 包括其应用的感知策略、环境感知得分、应用合规感知、健康状况感知等, 终端的身份及感知项属性也用于应用访问控制策略和风险决策。

在奇安信网神零信任环境感知系统关于终端的详情信息包括如下:

- 终端的概览信息, 包括: 终端名称、终端 IP 责任人、资产组、安全评分;
- 终端攻击访问关系图;
- 终端性能资源监控信息;
- 终端漏洞风险信息;
- 终端风险事件概览信息;
- 终端合规信息概览;
- 终端安装软件信息概览;
- 终端进程运行快照;
- 终端系统服务信息;
- 终端资源监控信息;

可支持的终端列表信息查询如下：

- 终端列表的基础信息包括：终端名称、终端 IP、终端类型、责任人、主机信息、系统资源占用信息、上下行速率、在线状态、防护状态、合规策略、EDR 策略、诱捕策略、采集策略等；
- 提供自定义资产名称、责任人等信息，可提供基于资产名称、主机信息、责任人等条件的终端分组管理；
- 提供对终端详情的查看功能；

终端接入管理：

- 提供对不同种类如 PC、服务器、虚拟主机，不同操作系统如 Windows、Linux、国产化操作系统的终端进行统一管理，可根据业务需求对终端进行资产分组；
- 提供对指定终端上的客户端软件进行更新、禁用、卸载等操作，对已识别风险的主机一键隔离；
- 提供对安装了违规软件的终端，能够向其推送警告或提示消息，能够编辑消息标题和内容；
- 满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中环境感知服务要求；
- 满足电子政务外网《政务外网终端一机两用安全管控技术指南》中环境感知服务要求；

2.2 环境感知内容分类

- 1) 提供终端基础环境感知信息

- 终端基本属性信息：终端名称、终端 IP、终端 mac 地址、CPU 基础信息、操作系统基本信息，内存信息、硬盘信息等；
- 不同种类终端环境及应用信息：主机信息、资源信息、共享信息、防火墙配置信息、注册表变化感知信息、账户密码配置感知信息、用户权限配置感知信息、用户组信息、用户信息、启动项信息、程序包信息、补丁信息、应用程序信息、系统服务信息、登录信息、应用服务信息、系统事件信息、进程运行信息、文件操作信息、网络连接信息、USB 插入行为信息等；
- 供用户根据实际需求配置环境信息采集策略，包括定义采集周期和采集内容；
- 满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中环境感知服务要求；
- 满足电子政务外网《政务外网终端一机两用安全管控技术指南》中环境感知服务要求；

2) 风险环境感知信息

风险环境感知信息是基于基础环境感知信息进行关联分析判定，确定为相应的风险环境信息时，环境感知客户端以威胁事件的方式上报的风险环境感知事件，包括：

- 物理环境安全风险信息；
- 终端身份标识变化风险信息；
- 网络环境变化风险信息；
- 文件操作行为信息；
- 恶意网络连接信息；
- 异常/风险行为信息；

- 恶意样本信息；
- 漏洞信息；
- 系统配置安全风险信息；
- 应用环境风险信息，如软件合规风险感知、服务合规风险感知、注册表合规风险感知等；
- 性能故障信息等；

满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中环境感知服务要求，

满足电子政务外网《政务外网终端一机两用安全管控技术指南》中环境感知服务要求。

2.3 环境感知内容的接入

环境感知信息的接入采集通过 syslog 或者 Webservice 等接口方式或通道实现相应的环境感知信息日志的接入，感知公安安全 U 盘、公安 PKI_U_key 拔插及使用情况，支持基于 PKI 拔插认证的网络准入机制；满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中环境感知服务要求和电子政务外网《政务外网终端一机两用安全管控技术指南》中环境感知服务要求。

2.4 环境感知内容的监控分析

环境感知信息的分析模块是环境感知报告和环境感知大屏呈现的基础数据。包含：

终端网络访问的分析，确定异常网络访问行为，包括，异常终端外联，异常横向攻击，恶意攻击域名，异常被攻击 IP 等；

终端运行监控统计，确定终端的异常运行状态，包括 CPU/内存/磁盘 IP 等的性能告警；

异常用户行为监控信息统计，可疑行为监测（可疑凭证获取、可疑权限控制、可疑日志清理行为、可疑文件操作行为、系统高危命令、可疑远程操作行为、异常进程创建行为、异常用户操作行为、可疑 USB 操作行为等）；

提供对接入终端的安全态势分析及可视化展示，包括攻击链统计、网络访问统计、威胁事件类型统计、攻击诱捕统计、弱点统计、事件列表、事件趋势统计等，支持系统整体评分，接入容量占比和月事件总数等。

满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中环境感知服务要求和电子政务外网《政务外网终端一机两用安全管控技术指南》中环境感知服务要求。

2.5 终端风险感知信息监控分析

奇安信网神零信任环境感知系统 (TESS) 的功能是通过多维度的终端感知方式采集和分析终端安全环境, 其主要分析的内容如下:

- 物理环境的风险感知信息分析;
- 终端及网络环境风险变化感知信息分析;
- 应用环境风险感知变化信息统计分析;
- 漏洞信息统计分析;
- USB 异常行为统计分析;
- 恶意样本信息统计分析;
- 异常服务、进程统计分析;
- 异常远程连接分析;
- 异常文件操作分析;
- 合规配置风险感知信息统计, 包括系统安全配置风险分析、软件合规风险感知分析、服务合规风险感知分析、注册表合规风险感知分析等;
- 弱口令分析;
- 威胁攻击行为分析, 包括入侵攻击分析、攻击诱捕分析等;
- 满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中环境感知服

务要求和电子政务外网《政务外网终端一机两用安全管控技术指南》中环境感知服务要求。

2.6 环境感知策略管理

环境感知策略管理能够提供基于终端风险度量技术的度量自定义,形成风险评分和风险报告。风险评分采用“可信加权”原则,将所有风险项产生的权值进行相加,以百分制提供给策略方,策略方再根据不同的权值制定相应的安全策略,主要目的是提供快速终端可信鉴定能力,所有业务安全访问策略可以基于分数的高低来进行设置;风险报告主要目的是提供深度终端可信鉴定能力,所有业务可以基于报告中的具体属性进行细粒度的业务访问控制。

- 允许管理员自定义感知策略、感知内容、风险等级、评分规则等;
- 可配置多个感知策略模板并应用到不同终端,允许管理员自定义终端执行策略的频率;
- 提供环境感知策略模板管理,可选择应用合规感知、健康状态感知、脆弱性安全感知等不同模块的启停;
- 提供为某个模块配置细粒度策略,包括:感知项启停、扣分标准、检测名单等;
- 提供应用合规感知项细粒度策略配置,包括:违规端口、违规网络连接、违规服务配置,并且支持分别的名单定义如端口黑名单、违规网络连接黑名单、违规服务黑名单、违规文件黑名单;
- 提供健康状态感知项配置包括:用户共享目录检测、屏保时间检测、防病毒软件安装检测、主机命名规范、补丁更新检测、加密文件存储检测、系统防火墙检测、违规软件检查等;
- 提供脆弱性安全感知项配置包括:资产漏洞检测,漏洞黑名单配置;

- 提供全局违规软件配置、提供内置违规软件列表展示，可自定义违规软件信息；
- 提供按照不同操作系统、IP 等条件下发环境感知策略，感知任务中可设置使用的环境感知模板，用于对应目标的环境感知检测；
- 提供环境感知策略列表展示、策略启停、查看、编辑、删除等操作；
- 满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中环境感知服务要求和电子政务外网《政务外网终端一机两用安全管控技术指南》中环境感知服务要求。

2.7 环境感知报告

根据终端的环境感知数据，对终端环境风险进行评估，得出终端安全环境感知的报告：

- 日志报表：能够对当前终端数量情况统计。能够对当前感知风险项统计。能够对终端感知结果分布进行统计。能够将风险项按照类别进行统计。
- 能够针对风险项做不同排名统计；
- 提供环境感知检查结果列表展示，以主机粒度展示各主机 IP、主机名、不合规项数目、已检测项数目、检查时间等；
- 提供主机检查详情下钻，点击可查看具体主机的极限合规情况详情，给出检查项名称、安全要求、用户当前实际设置值、检查结果情况（合规、不合规等），并支持主机基本软硬件信息、端口服务信息、进程信息等基本采集信息展示；
- 提供检查项的下钻展示，可对检查项类别、合规情况、风险值、配置方法等进行查看；
- 满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中环境感知服

务要求和电子政务外网《政务外网终端一机两用安全管控技术指南》中环境感知服务要求。

2.8 云桌面联动管理

环境感知服务应能关联同一个访问中所使用的云桌面和物理终端上的身份标识,具备联动感知功能:

- 感知云桌面环境信息及风险状况变化,包括但不限于云桌面基础属性信息,应用信息,风险信息;
- 确定当前的敏感信息访问方式是否为云桌面访问;
- 若为虚拟桌面访问,需要基于云桌面的环境感知信息分析确定当前虚拟桌面的风险状况及可信分数;
- 同时基于环境感知信息确定启动当前云桌面的的终端,并这个终端的环境感知信息确定当前终端的风险状况及可信分数;
- 通信加密:客户端和服务端通信使用 https 加密。管理端访问使用 https 通信加密。
- 外部联动:客户端支持执行访问控制传递的命令,包括:展示感知结果、启动云桌面客户端;

满足《GA/DSJ351-2020 公安大数据安全零信任体系技术设计要求》中环境感知服务要求和电子政务外网《政务外网终端一机两用安全管控技术指南》中环境感知服务要求。

2.9 数据库加密

对服务器控制中心的数据库的用户表与策略表进行加密处理，防止数据库被黑客篡改。

3 客户端功能介绍

奇安信网神零信任环境感知系统 (TESS) 分为客户端和服务端两部分。客户端安装在用户电脑、手机上，收集用户的环境信息，然后上传到服务端。具有自我保护功能，保证客户端程序目录下的相关文件均是不可以被篡改、注入、拦截、恶意终止，保证客户端程序本身的可信

3.1 基础安全感知

基础安全感知项包括病毒 APT 环境感知、系统漏洞环境感知等，采用“可信加权”原则，将所有风险项产生的权值进行相加，以百分制提供给策略方，策略方再根据不同的权值制定相应的安全策略；。

3.2 系统安全感知

系统安全感知包括登录失败限制、登录交互约束、本地身份防盗用、密码维护要求、账户管理审核、登录注销审核、对象访问审核、配置更改审核、系统事件审核、审核日志管理、其他补充审核、网络安全访问控制、数据泄密控制、账户访问控制、账户权限控制、服务资源控制、功能组件控制、设备资源控制、网络配置入侵防范、应用安全配置入侵防范、系统配置安全风险，从身份鉴别、资源控制和入侵防范。

3.3 应用合规感知

应用合规感知包括软件环境感知、服务环境感知、注册表合规等，感知是否存在非合规的软件、进程、注册表键值等风险，支持针对终端是否安装违规的软件，运行违规的进程、存在违规的注册表和服务项行为进行感知，保证终端安全合规的运行。

3.4 健康状态感知

健康状态感知是指拥有感知是否存在与浏览器相关、文件操作相关、桌面相关的终端健康相关风险能力。

健康状态感知包括 IE 主页相关项目、IE 菜单项、IE 核心配置、IE 外观配置、IE 常规设置、IE 浏览器图标配置、Internet 选项、用户样式表、重置 web 设置、About 协议、常用文件关联项、磁盘及文件夹配置、系统常用组件、系统启动配置、系统图标配置、任务栏及开始菜单、系统重要服务组件、组策略、显示属性、Web 桌面、网络驱动器、打印机设置、域名解析文件 Hosts、收藏夹快捷方式、桌面图标快捷方式、开始菜单快捷方式、桌面及资源管理器、快速启动栏快捷方式。

3.5 物理环境感知

奇安信网神零信任环境感知系统 (TESS) 客户端可以通过各种物理环境感知设备来识别操作终端的人，从而识别如 UKEY 插拔、网络切换、屏幕拍照、多人围观、授权人离席等物理环境风险的能力。

3.6 多环境感知

奇安信网神零信任环境感知系统 (TESS) 通过物理机客户端和云桌面客户端，能够同时感知物理机环境的可信状态和云桌面环境的可信状态，并通过安全策略来决定不同可信等级的终端的访问行为，可采集硬件信息，包括 CPU、内存、磁盘、ip、mac 操作系统等信息，采用应用监控技术，可感知到应用的启动信息，并上报至控制中心。