## 产品介绍

浏览器作为用户与网络交互最主要的平台，已经成为终端攻防的关键环节。恶意链接、网络钓鱼、水坑攻击、跨站攻击等普遍是通过诱导用户在终端设备的浏览器上执行了真正带来危害的攻击动作，通过浏览器平台来完成木马植入、勒索软件植入、盗取敏感数据等恶意行为。因此，管控好终端的浏览器入口对于终端安全防护至关重要，传统的终端DLP产品、上网行为管理产品、安全Web浏览器、VDI虚拟桌面产品、SWG安全Web网关（一般含在SASE中）等安全产品均具备对终端Web访问行为进行安全管控的能力，各类产品的防护技术原理和产品定位也不尽相同，只有安全Web浏览器聚焦解决Web浏览器环节的安全风险，其他产品防护定位更加宽泛（不局限于浏览器安全风险）。

本次测评的钛星终端威胁隔离产品（TS-AI）也是聚焦解决终端Web浏览器的安全风险问题，其原理是为每个终端构建一个远端的浏览器，执行所有用户的浏览会话，和本地终端隔离开来，这样即使浏览器被感染，恶意软件也无法侵害终端用户的系统。能够解决由Web浏览器漏洞利用导致的勒索软件、网络钓鱼、0Day攻击、高级木马和APT等恶意威胁和攻击，防止业务中断，保障其业务连续性，实现“实时”安全防护，杜绝因黑客利用浏览器漏洞发起攻击的安全问题。

产品典型部署场景描述

1.对于大型企业，如果企业已有 SWG，则可以与企业的 SWG 集成，通过企业的 SWG 将流量发送至钛星隔离云进行访问。如果企业没有 SWG，则可以在企业的网 络内部署 SWG，网络内的 SWG 将流量发送至钛星隔离云上。对于企业外出的员 工，可以在员工终端上安装客户端，通过客户端隔离上网。

2.对于中小型企业，提供 Saas 化服务，客户可以通过钛星隔离云上的 SWG 进 行隔离上网。

产品技术原理描述

产品核心功能清单

勒索软件防护 、恶意脚本防护 、文件上传防泄露 、防护浏览器 0Day 攻击 、钓鱼防护 、偷渡式下载 、文档在线预览和在线下载 、精准的文件类型识别与灵活的下载策略 、SSL 加密流量的监测 、匿名访问 、无客户端的安全保护模式 、用户原生体验

## 测评目的

本次测试聚焦在产品部署、产品维护、用户使用、平台管理等方面的真实表现，以评估产品在实际客户场景中的交付成熟度、功能完备性、使用效果、易用性、安全性等指标，据此来判断产品的综合能力水平。

由于缺乏行业通用标准或规范，本次测评以用户角度评估为主，辅以简单的纯技术能力评估和性能评估。

## 测评维度

为了评估产品的综合能力表现，测评工作将重点评估4大类测评内容：对照产品资料的功能测试、针对几种典型场景的产品综合测试、针对重点关注的单项指标测试、与相关品类产品的功能对照分析。

* **产品下限：对照产品资料的功能测试**

根据钛星提供的产品资料（《钛星终端上网威胁隔离防护产品白皮书V2.1》、《钛星数安 终端上网威胁隔离产品介绍》、《终端隔离防护云平台部署须知-AIC-PE01(基础版)》、《终端隔离测试方案模板V2.0-2020407》、《远程浏览器隔离管理平台用户须知》、《终端隔离管理平台用户须知》、《终端隔离云防护控制平台用户须知center》、《终端隔离云防护控制平台用户须知center》、《钛星终端威胁隔离平台部署手册》）进行产品部署操作、用户功能操作、管理功能操作等，重点测试产品实际功能与产品资料描述是否一致。

* **产品价值：针对几种典型场景的产品综合测试**

由于暂时无法在多种实际场景中进行产品实际部署使用评估，因此我们根据内部梳理的几种典型应用场景，在测试环境中效仿类似用户业务行为，来评估产品的综合使用效果。比较典型的场景为：财务法务等职能部门办公场景、HW（高安全等级）的内网办公场景、长亭日常办公场景。

* **产品上限：针对重点关注的单项指标测试**

（性能、功能、安全性）

重点关注的单项指标可分为关键性能指标、重点功能、产品安全性三方面。关键性能指标有并发能力与资源开销（影响成本与系统规模）、响应延迟（影响用户体验）；重点功能指标有“灰名单”防护效果（影响产品核心竞争力）、无探针部署能力（影响产品易用性）、防护控制策略的灵活性与精细度（影响防护能力）。

* **产品边界：与相关品类产品的功能对比**

由于相关品类产品具备了全部或大部分产品功能，因此需要将测评产品与存在功能重叠的其他常见产品进行功能对比，以便更好的划清产品的能力定位边界。据过往经验，建议与终端DLP产品、上网行为管理产品、钓鱼邮件防护产品、SWG安全Web网关产品进行对比，选择行业占有率较高的典型产品进行对照功能对比分析。

## 测试环境

客观描述产品安装部署的机器配置、客户端配置、网络拓扑、产品部署模式、产品版本信息、产品授权功能信息。

## 测试内容

### 5.1 对照产品资料的功能测试

#### 5.1.1 安装部署测试

部署软件环境为centos7.9

系统配置8 vCPU 16 GB 1 Mbps

部署、卸载文档优化完成，对照文件操作即可



#### 5.1.2 标准功能测试

- 徐丛然已有测试结果整理

测试时间：2022.4.26

|  |  |
| --- | --- |
| 测试内容 | 疑似钓鱼策略（用户访问非可信网站的页面，如果需要输入密码，将被视为疑似钓鱼） |
| 防护前 | 访问网址可以输入密码创建账号注册 |
| 防护后 | 1.设置策略禁止输入密码，网址无法输入密码    2.设置策略提示风险，输入密码提示风险 |
| 测试内容 | 文件下载策略    （可禁止文件下载功能，对于在打开页面中的下载文件，配置其处置策略） |
| 防护前 | 钓鱼网址可以下载文件 |
| 防护后 | 1.网址对白名单内对网址可以进行下载，其他的不可以    添加白名单后可以下载    2.允许下载，可执行文件提示下载 |
| 测试内容 | 压缩文件检测开关策略   （ 下载压缩文件时，是否需要检测压缩文件，配置处置策略） |
| 防护前 | 压缩文件可以随意下载 |
| 防护后 | 开启策略后下载压缩文件，会在沙箱里跑一遍，之后风险提示。（策略关闭和开启终端接收不是很快，需刷新几次浏览器） |
| 测试内容 | 文件上传策略    （根据文件上传策略，用户访问不在白名单中的未知链接时，决定是否允许上传文件） |
| 防护前 | 可以任意上传图片、文件等 |
| 防护后 | 1.开启禁止上传策略后，访问百度贴吧进行上传，防护成功    2. 用户在访问白名单网站时允许上传文件，其他网站不允许上传    添加白名单后可以上（防护的盾牌没有了，但是防护效果在，判断为兼容性显示问题）    3. 用户访问所有网站均不允许上传（防护的盾牌没有了，但是防护效果在，判断为兼容性显示问题） |
| 测试内容 | 操作权限控制策略    （浏览网页时，是否需要禁止/允许复制粘贴，配置处理策略） |
| 防护前 | 浏览网页可以复制粘贴 |
| 防护后 | 开启防护后浏览网页无法复制粘贴 |
| 测试内容 | 广告拦截策略    （浏览网页时，是否拦截广告） |
| 防护前 | 默认访问网址有广告 |
| 防护后 | 开启防护后访问网页无广告 |
| 测试内容 | 白名单策略配合防护策略对某个终端或部门生效 |
| 防护前 | 设置白名单生效范围，仅对某个终端生效，不在白名单内的终端无法上传。 |
| 防护后 | 白名单生效范围策略设置    自定义白名单内的终端根据策略可以上传 |
| 测试内容 | 登录安全性（密码3次以上错误会进行双因子认证或禁用或锁定一段时间） |
| 测试效果 | 1. 双因子模式：输入错误三次以上会强制进入双因子认证（发送邮箱或短信验证）短信验证配置较繁琐，由于是内网环境无法连接短信网关（研发提了需求如果管理平台没有配置可以把短信相关功能去掉）测试了邮箱验证会发送验证码到创建用户时填写的邮箱，可以登录。 2. 禁用模式：输入密码错误3次会禁用账户，管理平台可以启用，但是还是无法更改密码，只能远程后台更改，内网环境无法更改目前只能删除账户重新添加，删除会导致对应账户的终端软件、防护日志清空（感觉功能易用性不好，用户密码忘记了被禁用了启用后还是不知道密码） |
| 测试内容 | 白名单策略管理（自定义添加白名单） |
| 测试效果 | 1.白名单只能添加域名无法添加url，如www.baidu.com可以，但是www.baidu.com/html无法添加    2.白名单没有失效时间，添加都是永久添加。 |
| 测试内容 | 终端安装探针是否可以快速安装 |
|  |  |
|  |  |

### 5.2 针对几种典型场景的产品综合测试

#### 5.2.1 敏感职能部门办公场景

#### 5.2.2. HW内网办公场景

#### 5.2.3 长亭日常办公场景

### 5.3 针对重点关注的单项指标测试

#### 5.3.1 关键性能测试

##### 5.3.1.1 并发与开销

终端配置：2 vCPU, 8GB RAM, 1 Gbps 网络

**性能测试 - 白名单站点**

测试本地 HTTP 中间人代理性能。后端为 HTTP 站点，nginx 静态页面。

最大并发：< 300

| 并发 | 发送 QPS | 实际 QPS | 延迟 | 备注 |
| --- | --- | --- | --- | --- |
| 10 | 100 | 100.08 | 6.7ms |  |
| 100 | 100 | 100.09 | 7.39ms |  |
| 200 | 100 | 100.06 | 13.17ms |  |
| 300 | 100 | - | - | 部分连接超时 |

最大 QPS：< 650

| 并发 | 发送 QPS | 实际 QPS | 延迟 | 备注 |
| --- | --- | --- | --- | --- |
| 100 | 100 | 100.09 | 7.39ms |  |
| 100 | 500 | 497.88 | 17.16ms |  |
| 100 | 600 | 585.55 | 60.11ms |  |
| 100 | 1000 | 619.99 | 1.93s |  |

简评：单机基本够用，无 Agent 模式（接入多台终端）需要更换实现方案。

**性能测试 - 远程浏览器**

测试远程浏览器处理性能。

TODO，测试环境准备中

##### 5.3.1.2 响应延迟

#### 5.3.2 重点功能测试

##### 5.3.2.1 “灰名单”防护效果

##### 5.3.2.1 无探针部署能力

##### 5.3.2.1 防护控制策略

#### 5.3.2 安全性测试

- 引用萌神的测试结论？？

### 5.4 与相关品类产品的功能对比

相关品类产品清单如下。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 产品 | 典型场景 | 防护侧重 | 功能类型 | 典型产品 |
| CASB | 当企业员工接入从固定环境转向BYOD，企业IT服务从集中数据中心转向云环境和SAAS服务时，CASB成为员工到企业IT服务的接入访问代理，实现对企业IT服务的有效保护。 | 企业资产 | 安全、管控 | 国内：  EnCASB（易安联）  国外：  Forcepoint |
| SASE | 在CASB基础上，融合了网络接入和优化加速能力。 | 企业资产 | 安全、管控、网络接入 | 国内：  亿格云  国外：  Zscaler |
| SWG | 当员工访问Web服务（包括其他协议）时，分析和过滤掉有安全风险内容（请求、响应、数据内容等）。  可作为单独产品，也可以集成在CASB或SASE。 | 企业员工（独立产品时）  企业资产（整合到CASB/SASE时） | 安全、管控 | 国内：  国外：  Forcepoint |
| 上网行为管理 | 对员工在企业内网环境下日常办公上网的行为进行监控和管控，避免访问违规网站，避免使用违规联网应用。 | 企业员工 | 管控 | 国内：  华域数安  国外： |
| 终端DLP | 对员工办公终端进行监控和管控，主动扫描文件/数据内容，防止违规的数据外发、数据拷贝，防止违规应用安装与运行，并进行调查取证。 | 企业员工 | 管控 | 国内：  天空卫士  国外：  Symantec |
| 安全浏览器 | 要求员工安装和使用专用Web浏览器上网，可以避免页面截图、无授权打印、文件下载、文本复制、访问违规网站等高风险行为（页面水印覆盖、落盘数据加密储存、截图保护、禁止下载等）。 | 企业员工 | 管控 | 国内：  360企业安全浏览器  国外： |
| 钓鱼邮件防护（邮件安全网关） | 综合运用特征库、指纹库、恶意网址库、沙箱等技术对于邮件进行分析和过滤，分离垃圾与威胁邮件。 | 企业员工 | 安全 | 国内：  SQR邮件安全网关（守内安）  国外：  Cisco Secure Email（Cisco ） |
| RBI技术类产品 | 主要基于RBI技术进行隔离防护的安全产品 | 企业员工 | 安全 | 国内：  北京方向标 邮件链接隔离系统  国外：  Cloudflare for Teams零信任安全和安全Web浏览服务套件的一项附加服务（Cloudflare） |

#### 5.4.1 终端DLP产品

#### 5.4.2 上网行为管理产品

#### 5.4.3 钓鱼邮件防护产品

#### 5.4.4 SWG

## 测评结论