SPN沙盒

安全上网解决方案

CNSINDA 深信达

关于深信达

CNSINDA深信达

深信达成立于2008年，专注于数据安全，在数据加密、防泄露、反病毒领域，有深入研究，推出了SDC沙盒防泄露、SPN安全上网，MCK主机加固、CBS赛博锁等系列产品。

公司业务已涉及各大行业，是国内领先的数据安全、环境安全及安全服务三大业务提供商，是国内第一个把沙盒应用于数据防泄露的厂家。

本部位于苏州市高新区。
技术团队精通windows/Linux/MacOS等操作系统底层技术，在数据安全领域深耕15年，积累了丰富的产品经验和项目经验。

产品资质

CNSINDA深信达

中华人民共和国国家版权局

计算机软件著作权登记证书

软件名称：深信达机密数据保护系统 [简称：SDC] V3.0

著作权人：苏州深信达信息技术有限公司

开发完成日期：2010年10月15日

首次发表日期：2010年10月15日

权利取得方式：原始取得

权利范围：全部权利

登记号：2011SR002251

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，经中国版权保护中心审核，对以上事项予以登记。

检测报告

国保测 2018C06546

产品名称：深信达身份鉴别系统

规格型号：V4.0

送测单位：苏州深信达网络科技有限公司

送测日期：2018年4月23日

国家保密科技测评中心

（盖章）

2018年5月28日

涉密信息系统

产品检测证书

编号：国保测 2018C06546

兹证明：苏州深信达网络科技有限公司

研制生产的 深信达身份鉴别系统 V4.0

经国家保密科技测评中心检测，符合国家保密标准《涉及国家秘密的信息系统身份鉴别产品技术要求》（暂行）的要求。

本证书有效期自 2018 年 5 月 28 日至 2021 年 5 月 27 日

批准人：

国家保密科技测评中心

CNAS L0653

我信编号：公计检110399

检验报告

样品名称：深信达数据保护系统

型号规格：V3

产品类别/级别：访问控制（网络-基本级）

受检单位：苏州深信达信息技术有限公司

检验类别：委托检验

公安部信息安全产品检测中心

公安部计算机信息系统安全产品质量监督检验中心

目 录

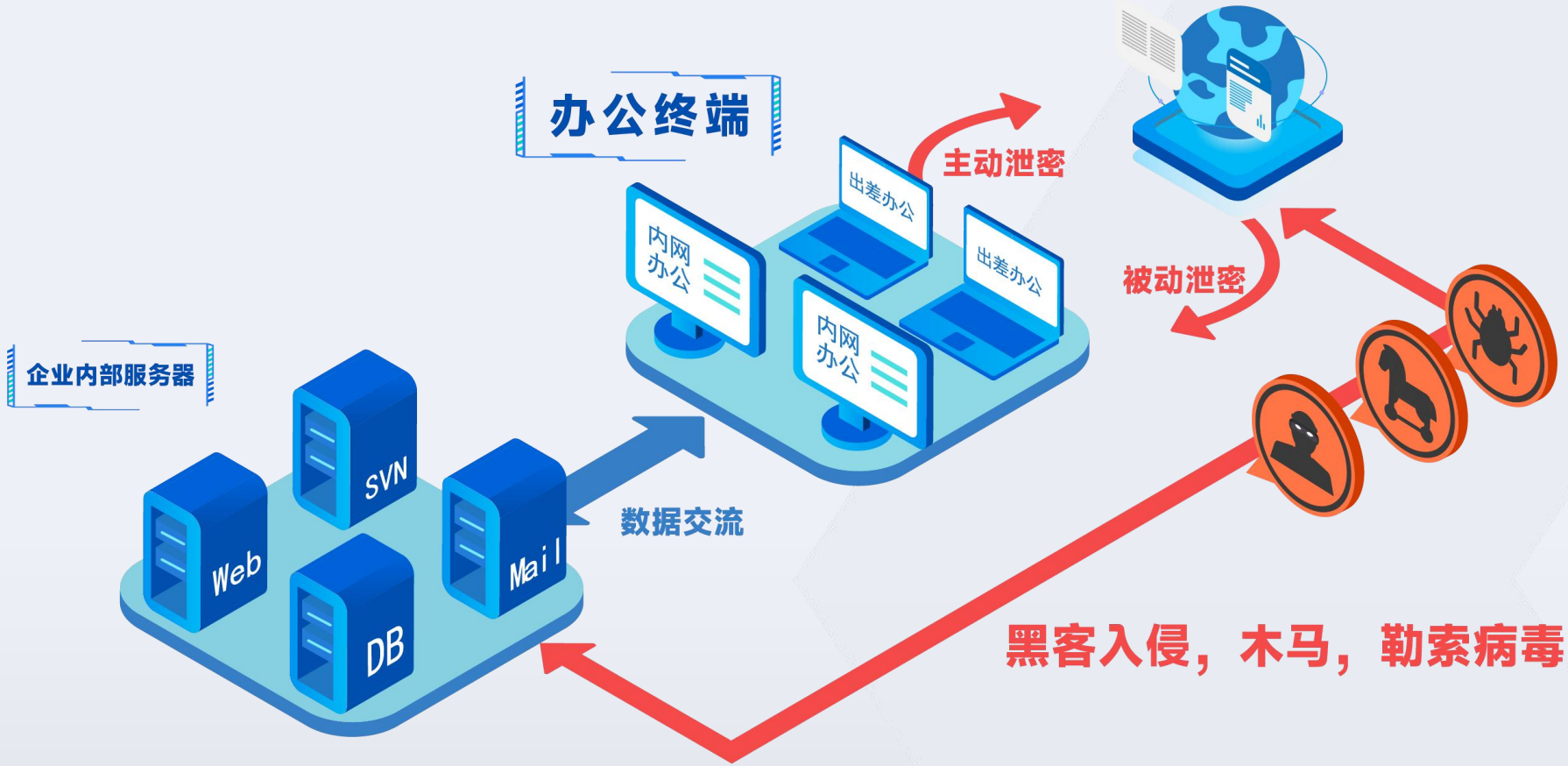
CONTENTS

01 前言介绍

前言

CNSINDA深信达

随着信息化的发展，企业日常办公越来越依赖互联网。终端以及普通PC终端在访问互联网过程中，会遇到各种各样不容忽视的风险，例如员工主动故意的数据泄漏，后台应用程序偷偷向外部发信息，木马间谍软件的外联，以及各种挖矿、病毒运行。



联网后的风险举例（一）

CNSINDA深信达

下图是某公司的网络监测日志，从日志上可以看出，到外联的木马以及挖矿病毒非常多，表面平静，但暗潮汹涌。

23-04-17 09:39:57	10.80.10.26	185.22.152.139	10.80.10.26	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:57	10.80.23.100	45.135.135.164	10.80.23.100	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:57	172.20.144.53	45.135.135.164	172.20.144.53	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:56	172.20.160.180	39.106.26.135	172.20.160.180	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:56	10.80.13.22	45.135.135.164	10.80.13.22	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:56	172.20.24.35	39.106.26.135	172.20.24.35	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:56	10.80.6.72	185.22.152.139	10.80.6.72	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:56	172.20.61.81	185.22.152.139	172.20.61.81	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:56	172.20.145.191	185.22.152.139	172.20.145.191	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:56	172.21.101.96	45.135.135.164	172.21.101.96	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:56	10.80.28.69	45.135.135.164	10.80.28.69	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:56	172.20.24.21	45.135.135.164	172.20.24.21	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:55	172.21.101.212	45.135.135.164	172.21.101.212	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:55	10.80.25.37	185.22.152.139	10.80.25.37	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:55	172.21.104.83	45.135.135.164	172.21.104.83	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:39:31	8.8.8.8	139.59.109.18	8.8.8.8	恶意软件	挖矿病毒	LifeCalendarWorm挖矿	失陷	高危
23-04-17 09:21:49	172.21.100.106	45.135.135.164	172.21.100.106	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:18:15	219.146.1.66	139.59.109.18	219.146.1.66	恶意软件	挖矿病毒	LifeCalendarWorm挖矿	失陷	高危
23-04-17 09:17:31	10.80.13.88	39.106.26.135	10.80.13.88	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:16:57	172.20.133.72	39.106.26.135	172.20.133.72	恶意软件	远控木马	普通远控木马活动事件	失陷	高危
23-04-17 09:14:45	8.8.8.8	63.251.235.76	8.8.8.8	恶意软件	挖矿病毒	LifeCalendarWorm挖矿	失陷	高危

联网后的风险举例（二）

CNSINDA深信达

打开自己的可以联网的电脑，进入CMD命令行下，输入“netstat - aon”,可以列出该主机联网的通信连接，这些都是在应用在后台连接网络发信息，他们发了什么，你知道吗?

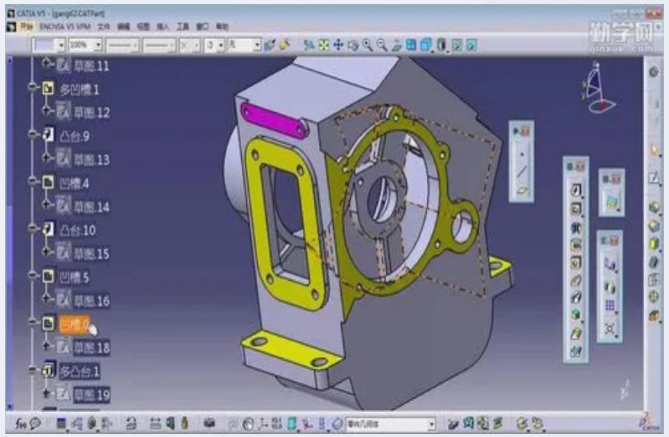
```
C:\Users\liyf>netstat -aon

活动连接

  协议   本地地址          外部地址        状态           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       856
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       7180
  TCP    192.168.100.89:49888   14.116.241.17:443      CLOSE_WAIT      12120
  TCP    192.168.100.89:49891   183.47.99.22:443       CLOSE_WAIT      12120
  TCP    192.168.100.89:49894   183.47.99.22:443       CLOSE_WAIT      12120
  TCP    192.168.100.89:49897   183.47.99.22:443       CLOSE_WAIT      12120
  TCP    192.168.100.89:49920   14.116.241.17:443      CLOSE_WAIT      12120
  TCP    192.168.100.89:49921   183.47.99.22:443       CLOSE_WAIT      12120
  TCP    192.168.100.89:49936   180.101.153.73:443     CLOSE_WAIT      12120
  TCP    192.168.100.89:50006   183.60.15.102:443      ESTABLISHED     4556
  TCP    192.168.100.89:50193   101.226.142.171:443    ESTABLISHED     10976
  TCP    192.168.100.89:50221   14.116.241.17:443      CLOSE_WAIT      12120
  TCP    192.168.100.89:50222   14.116.241.17:443      CLOSE_WAIT      12120
  TCP    192.168.100.89:50224   183.47.99.22:443       CLOSE_WAIT      12120
  TCP    192.168.100.89:50238   47.96.122.18:443       ESTABLISHED     12544
  TCP    192.168.100.89:50417   183.47.104.75:443      CLOSE_WAIT      12120
  TCP    192.168.100.89:50422   122.228.253.10:443     CLOSE_WAIT      12120
  TCP    192.168.100.89:50490   183.60.15.102:443      ESTABLISHED     3564
```

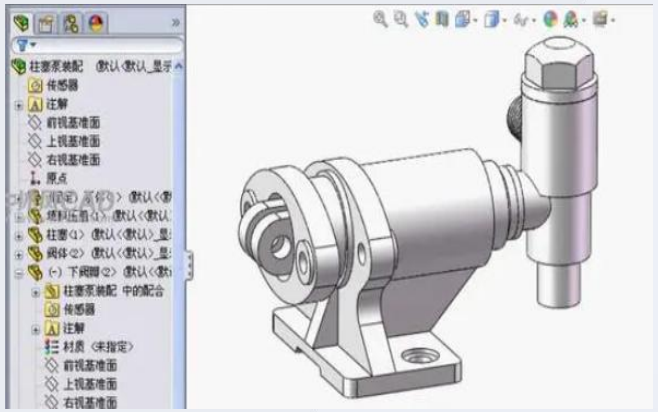
联网后的风险举例（三）

CNSINDA深信达

有的公司被查盗版的人带着公安人员登门索赔，他们可以直接说出您公司装了多少套盗版软件，什么时候安装的，安装在哪里，主机名、IP地址、谁在用都说得清清楚楚，这些信息是怎样被对方收集走的呢?

更有甚者，被国外敌对势力直接渗透，成为被攻击对象。





目前常用的措施

CNSINDA深信达

措施1：完全物理隔离断网，不访问互联网。

缺点：互联网是最大的知识库，不能访问外部网络工作效率大大降低，属于因噎废食。

措施2：部署防火墙或上网行为管理

缺点：由于互联网的不确定性，无法使用网址、IP、端口、协议白名单，只能用黑名单方式管控，效果很差；来自终端的https请求是员工浏览器发出的，还是盗版间谍软件发出的，无法辨别，只能放行！

在终端访问互联网时，需要有一种安全访问互联网方案

CNSINDA深信达

能自由访问互联网

每个访问都是受控的

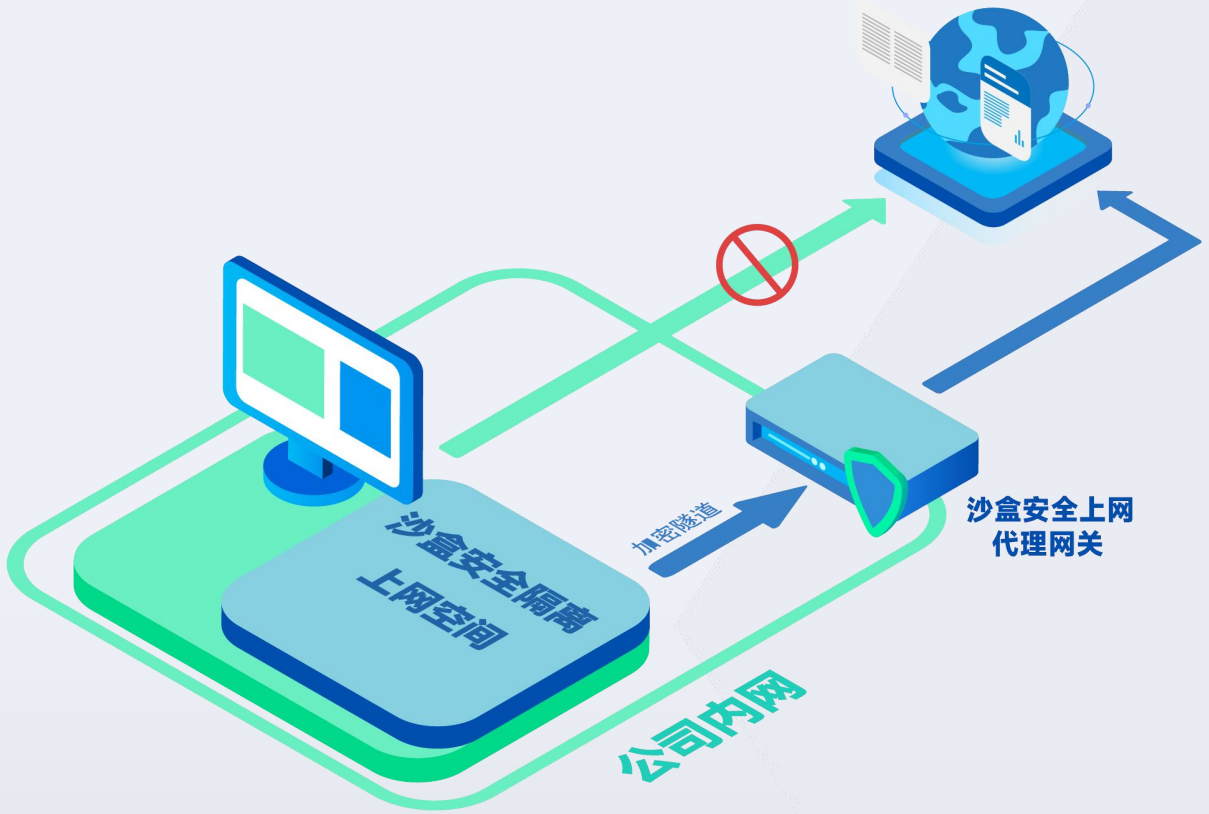
本地数据信息不被偷走

外面病毒木马进不来

SPN沙盒-安全上网解决方案

CNSINDA深信达

深信达SPN（Sandbox Proxy Network）安全上网解决方案，是直接把终端传统外网物理断开，然后在内网中部署一个沙盒安全上网网关主机，在需要访问外网的终端上安装一个沙盒，当需要访问互联网的时候，在这个隔离沙盒内访问互联网。主机本机和互联网物理隔离，只有沙盒能访问互联网，沙盒和本机是隔离的。



SPN安全上网系统构成

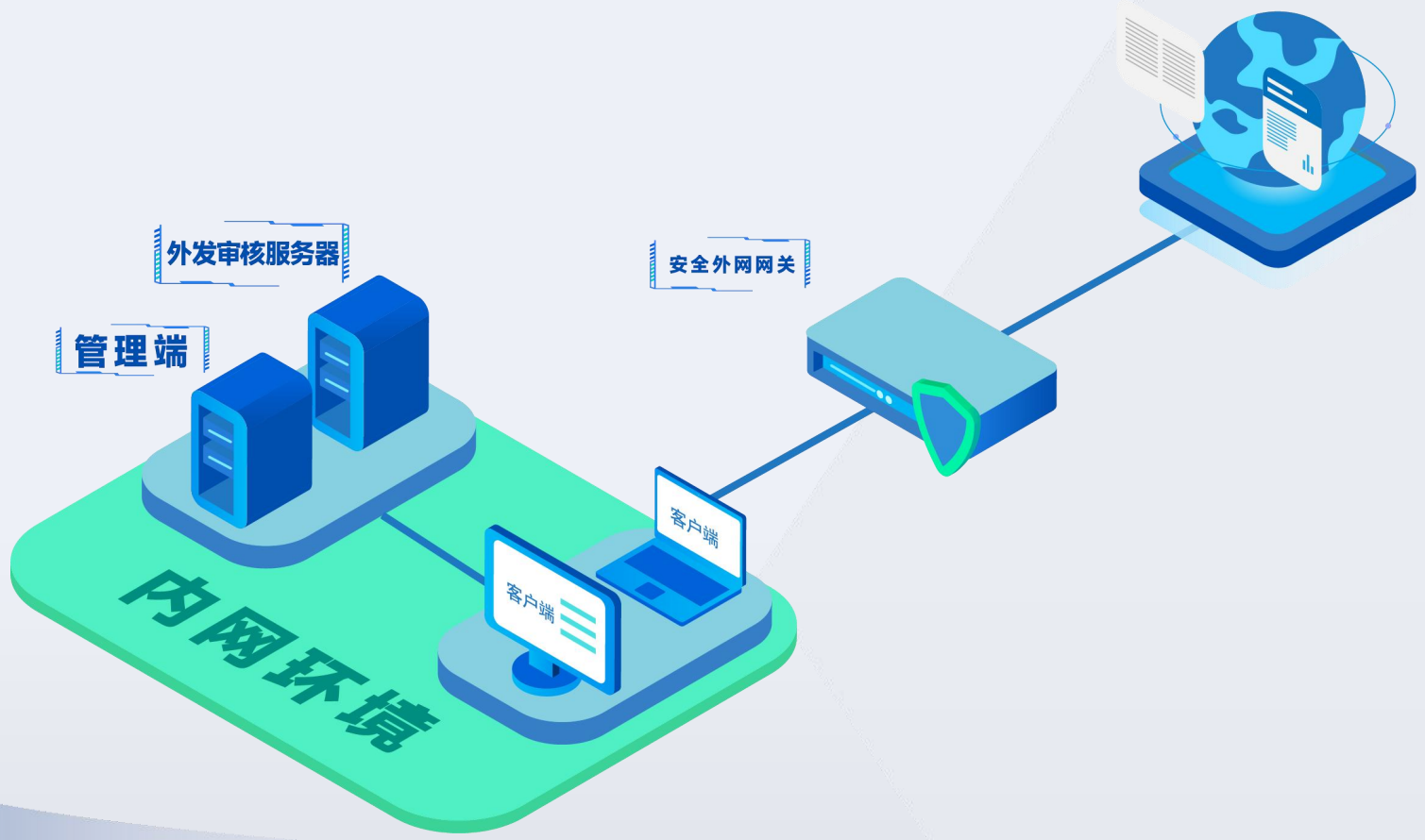
CNSINDA深信达

1.管理端：系统控制中心，对整个沙盒系统进行管理控制。

2.外网设备网关：安全上外网网关，有外网访问权限。

3.外发审核服务器(可选):外发涉密文件。

4.沙盒客户端：对外隔离的安全上网空间，数据进出审计。



02 功能介绍

SPN沙盒-安全上网功能介绍

CNSINDA深信达

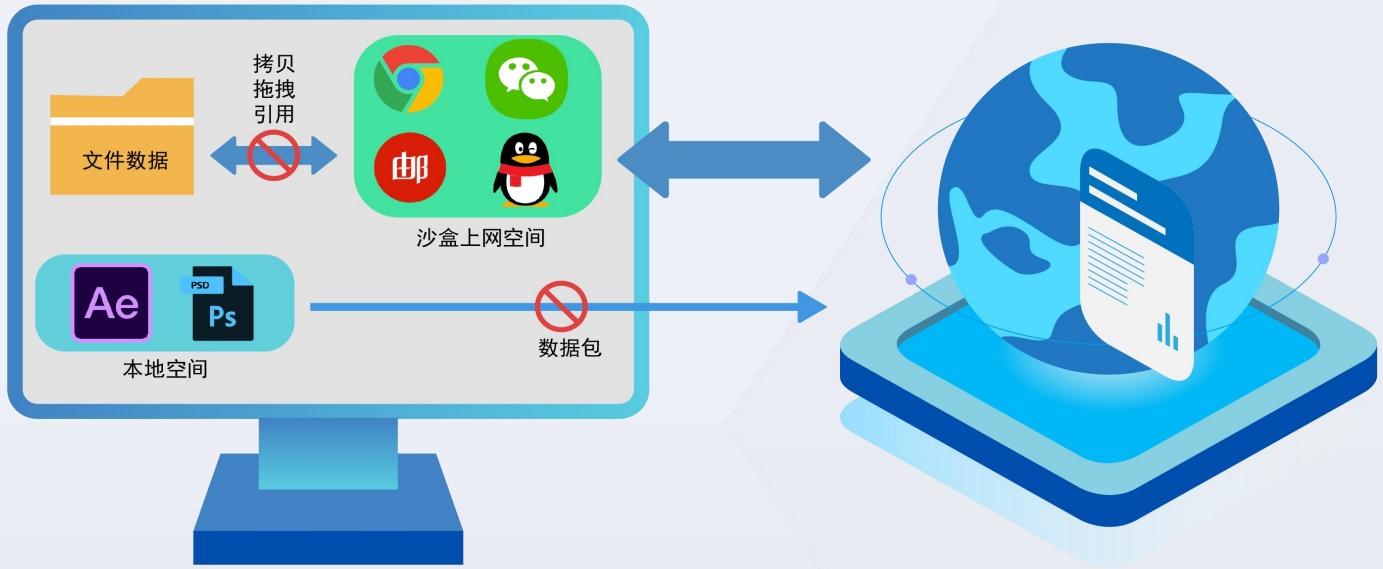
安全上网数据不泄漏，病毒进不来，一机多用

在终端上部署沙盒，只有沙盒内白名单程序(如：浏览器、IM工具）才能访问外网

-本机沙盒外程序无法访问外网（**可以杜绝间谍软件发消息**）

-本机数据不能向沙盒内上网程序复制拷贝、拖拽、引用；

-上网空间浏览的**文本**内容，可以通过拷贝粘贴到主机环境；



SPN沙盒-安全上网功能介绍

CNSINDA深信达

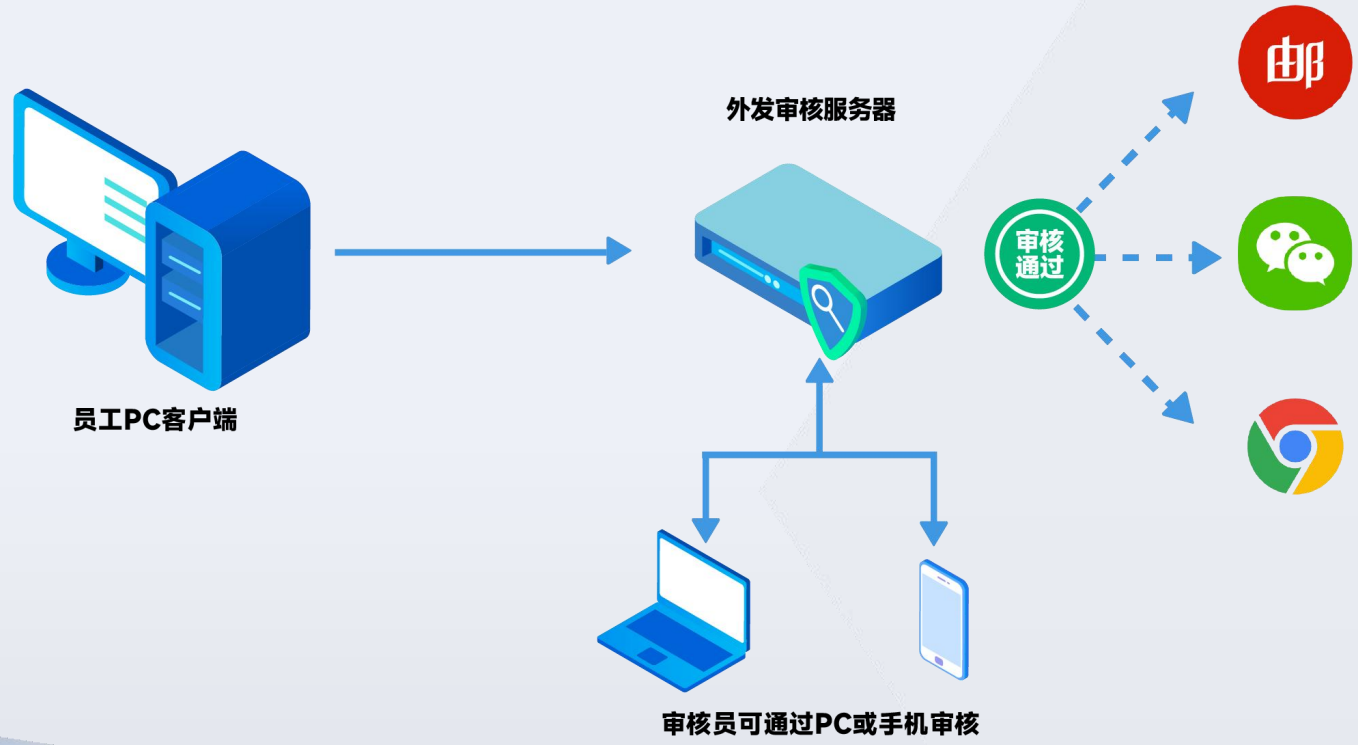
数据外发要审批

-终端本机上的文件发到外部上网空间，需要走审批：

-审批流程自定义，支持多级审批；

-支持鼠标选中文件鼠标右键菜单审批；

-审批过的文件服务器上有完整记录；



SPN沙盒-安全上网功能介绍

CNSINDA深信达

外网陌生程序文件进不来

在上网空间内，浏览器下载的文件、以及QQ/微信/钉钉获得的文件，无法直接拷贝进内网，需要管理员授权。管理员可针对程序设置访问类型：只读访问/禁止访问。

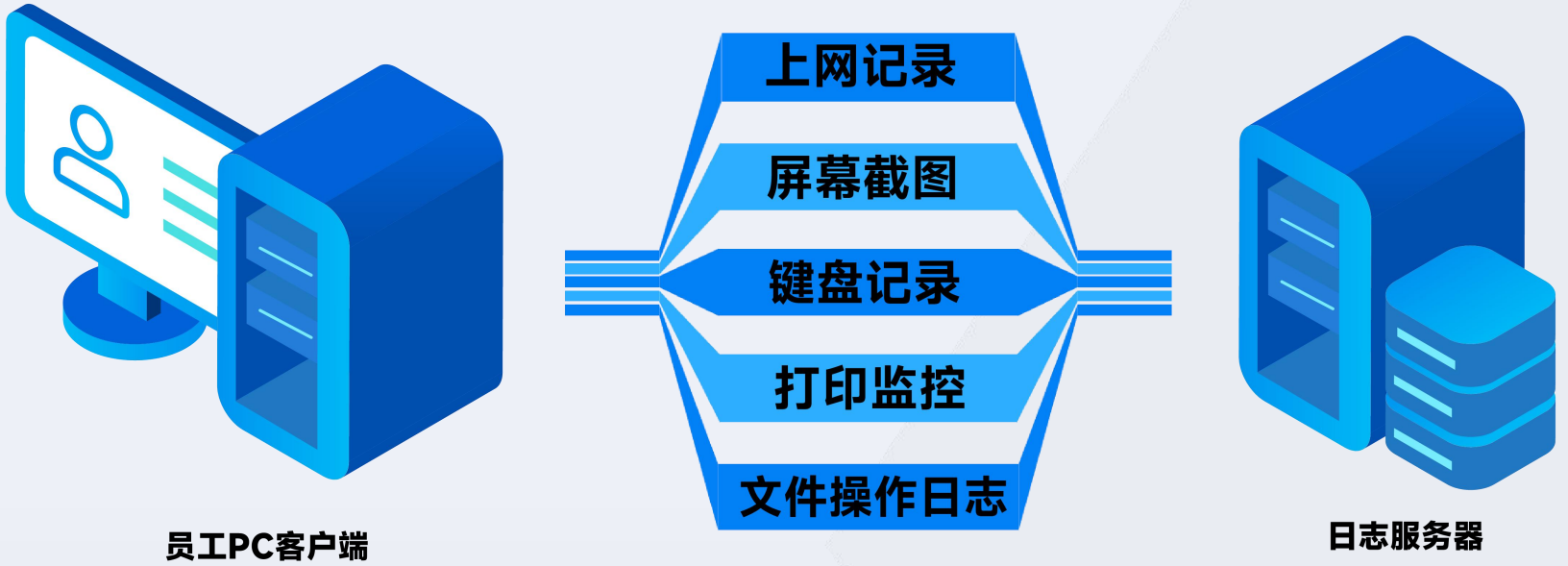
员工PC客户端

SPN沙盒-安全上网功能介绍

CNSINDA深信达

客户端行为日志

客户端可针对员工的操控行为（包含上网）做审计，如屏幕截图、上网记录、键盘录入内容、文件操作日志等。



03 产品特点

SPN沙盒-安全上网防泄露级别可调

CNSINDA深信达

标准级

- **感知到沙盒上网空间存在，在隔离空间内上网（标准级）**

本机不做任何管控，在沙盒内安全上外网，沙盒和本地隔离界限清晰，数据交换方便，安全可控。

基本级

- **无感知模式，隐藏沙盒上网空间，白名单代理上网（基本级）**

白名单进程透明走隧道代理访问互联网

不改变原有使用方式和工作习惯，用户感觉不到沙盒存在

SPN沙盒-安全上网模块特点

CNSINDA深信达

不和现有安全措施抢资源

本机的安全措施不改变，只是对网络出口进行强化管控。

不改变原有网络架构

在原有网络中，部署一个能访问外网的SPN专用网关即可， 该网关仅允许上网空间访问通过。

部署轻盈，对主机原环境影响小

安装包小，占用资源低，在原有主机中开辟一个上网空间即可。

实现成本低，性价比高。

支持平台全

支持windows/linux/苹果/统信/麒麟/鲲鹏等国产操作系统。

产品对比

CNSINDA深信达

产品 / 对比项目	SPN沙盒-安全上网	VDI云桌面访问互联网
设计理念	主机上开辟一个空间上网。	通过另一个和本机无关的主机上网
实现方式	一个主机多用，数据隔离	物理隔离
负载	使用终端硬件算力，负载低，高效	使用服务器硬件算力，随着用户增多，压力大
离线使用	可正常使用	无法正常使用
支持平台	Windows平台/linux平台/苹果/国产操作系统	Windows平台/linux平台/苹果
成本低廉、安全性高		**笨重，性价比差**

产品对比

CNSINDA深信达

产品 / 对比项目	SPN沙盒-安全上网	零信任
设计理念	主机上创建一个微隔离的沙盒空间，主机是高安全用于工作、沙盒内是低安全，用于访问外网	主机上创建一个微隔离的沙盒空间，主机是低安全用于上网、沙盒内是高安全，用于工作
解决问题	安全访问网络，避免程序后门	业务数据防泄露
实现方式	一个机多用，微隔离、底层虚拟化	一机多用，微隔离、应用虚拟化
数据流转	主机到沙盒空间需要审批； 沙盒空间到主机策略控制；	数据从主机到安全空间自由进入 安全空间内数据无法拷贝到主机
离线使用	可正常使用	可以正常使用
支持平台	Windows平台/linux平台/苹果	Windows平台/linux平台/苹果
成本低廉、安全性高		**成本低廉、安全性高**

产品对比

CNSINDA深信达

产品 / 对比项目	SPN沙盒-安全上网	上网行为管理
设计理念	主机上创建一个微隔离的沙盒空间，主机是高安全用于工作、沙盒内是低安全，用于访问外网	网关设备，对路过的上网数据流进行解析，并作相应控制
实现方式	一个机多用，微隔离、白名单程序上外网	协议流量拦截分析
控制颗粒度	以进程为单位进行控制，只允许白名单程序能上外网	无法进行进程级别拦截，特别是http访问只能根据网站url或IP地址拦截
内容控制	微信、浏览器、钉钉、QQ，企业微信等，和本地涉密数据隔离	只能禁止或允许，无法区分内容进行控制，如微信，可以设置禁止使用，但无法限制其传输内容
防陌生程序发包	可防间谍软件和盗版软件网络发包	无法禁止
成本低廉、安全性高		**成本低，安全性低**

沙盒支持OS

CNSINDA深信达

沙盒管理端

支持window server2008/2012/2016/2019

支持linux和国产操作系统

沙盒上网网关

支持windows/linux/国产操作系统

沙盒客户端

支持windows 7/8/10 32/64位

支持linux常用版本

支持UOS、麒麟等国产操作系统

支持Mac

04 客户案例

深信达的客户

CNSINDA深信达

深信达成立10多年来，已成功为众多知名客户提供数据安全服务，涵盖通信、无人机、机器人、医疗仪器、汽车、研究院、金融所等众多领域。

感谢您的观看

CNSINDA

深信达