SDC沙盒数据防泄密解决方案

数据安全解决方案专家

CNSINDA

关于我们

成立于2008年，专注于数据安全，在数据加密、反偷窥、反扩散、反盗版领域，推出了SDC、MCK、CBS、SPN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。

本部位于苏州市高新区。

精通windows/Linux/MacOS等操作系统底层技术，在数据安全领域深耕10年，积累了丰富的产品经验和项目经验。

产品资质

CONTENT

PART 01

需 求 背 景

前言

随着各行各业业务数据信息化发展，各类产品研发及设计等行业，都有关乎自身发展的核心数据，包括业务数据、代码数据、机密文档、用户数据等敏感信息，这些信息数据有以下共性：

— 属于核心机密资料，万一泄密会对企业造成恶劣影响，包括市场占有率下降、丧失核心竞争力、损失客户信心等各种显性与隐性影响；

— 核心数据类型多，还有业务系统数据，非实体文件，管控难；

— 员工计算机水平高，有多种泄密途径；

企业对数据的保护最先考虑的是外部攻击者，容易忽略内部员工。内部人员比外部攻击者更有优势。如果不对其进行管控，设计者和使用者很容易通过各种途径把核心数据复制出去，造成泄密。

常见泄密途径

由于研发人员比普通办公人员要精通电脑，除了常见的网络，邮件，U盘，QQ等数据扩散方法外，还有很多对于研发人员来说非常容易的方法（未列全）：

物理方法：

— 网线直连，即把网线从墙上插头拔下来，然后和一个非受控电脑直连； — winPE启动，通过光盘或U盘的winPE启动，甚至直接用ISO镜像启动；
— 虚拟机，通过安装VMWare虚拟机，在虚拟机内使用外设U盘，网络； — 其他非受控电脑中转，即把数据拷贝给网络内其他非受控电脑上，中转；
— 网络上传，通过在公网上自建一个上传服务器，绕过上网行为管理；

数据变形：

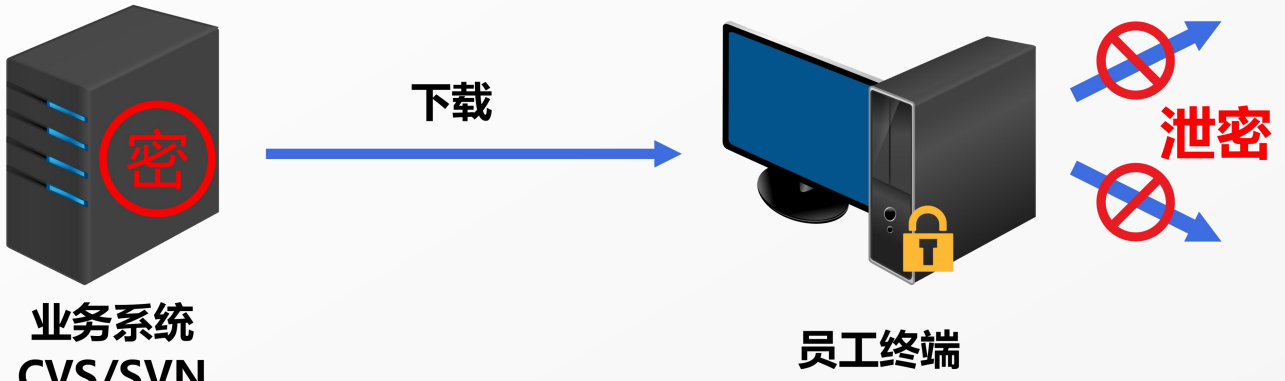
— 编写控制台程序，把代码打印到DOS控制台上然后屏幕信息另存；
— 把代码写到Log日志文件中，或把代码写到共享内存，然后另一个程序读走；
— 编写进程间通信程序，把代码通过socket，消息，LPC，COM，mutex，剪切板，管道等进程间通信方式，中转把数据发走；
— 通过IIS/Tomcat等web解析器中转，把代码数据当网页发布出去，然后浏览器浏览后另存，或干脆写个txt框，初始化时把代码都拷贝进来；

外设中转：

— 对于嵌入式开发场景，可以通过串口，U口，网口把代码烧录到设备中转泄密。

SDC沙盒系统

深信达**SDC沙盒**数据防泄密系统，是专门针对敏感数据防泄密的保护系统，尤其是对研发型企业数据防泄密保护。实现对数据的代码级保护，且不影响工作效率，不影响正常使用。所有敏感数据都自动加密并配合多种管控机制，从而得到有效的范围控制，防止泄密。

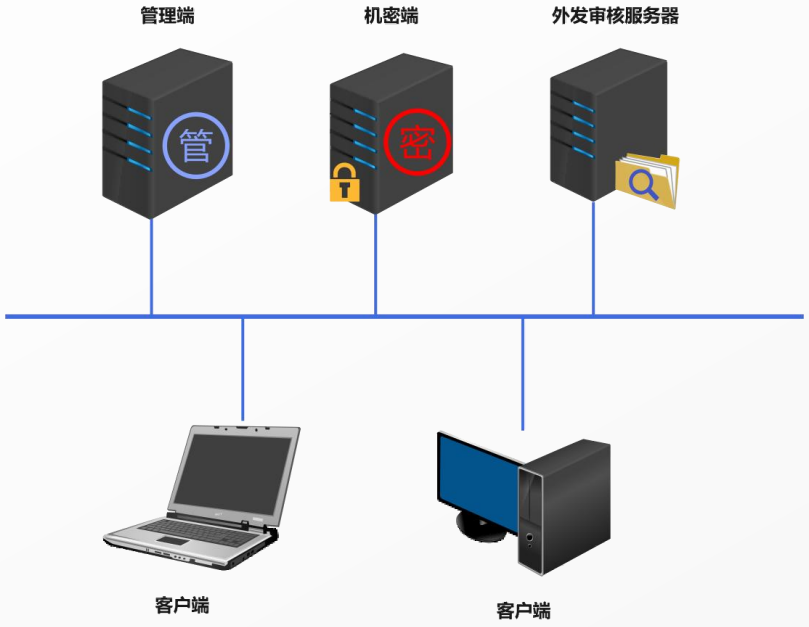


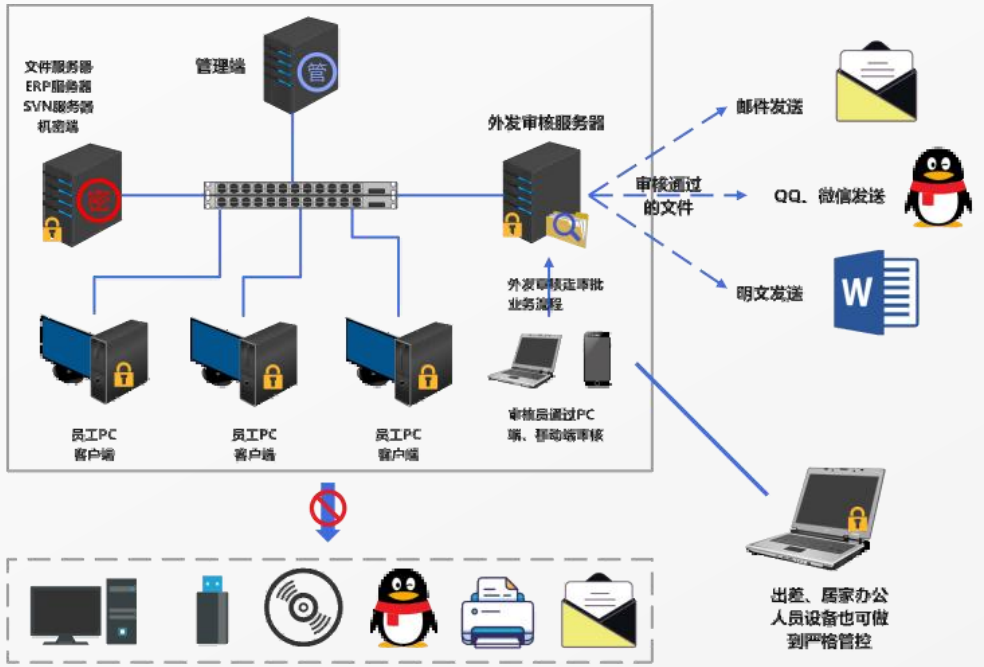
- 不影响正常使用；
- 支持所有文件格式；
- 数据只进不出，外发需审批；

说明：SDC：Secret Data Cage 企业核心机密数据防泄密保护之意

SDC沙盒系统的构成与概念

- **管理端：**系统控制中心，对整个沙盒系统进行管理控制
- **机密端：**源代码及设计文档版本管理服务器，可以有复数台
- **外发审核服务器(可选):**外发涉密文件
- **客户端：**防泄密终端，可以有复数台，所有终端源代码，文档全盘透明加密



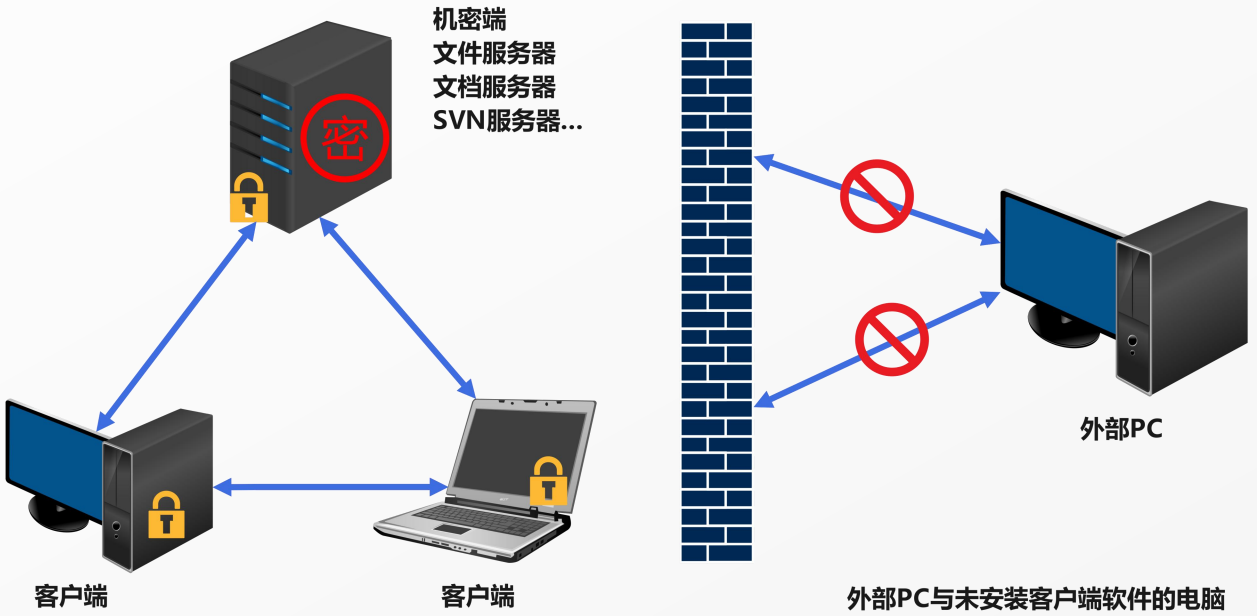


PART 02
功 能 介 绍

涉密可信网络（在不可信的环境下建立可信网络）

-客户端和机密服务器通过相互主动认证，建立加密隧道，组成可信网络；-可信网络内，客户端和机密端之间，客户端和客户端之间，自由通信。

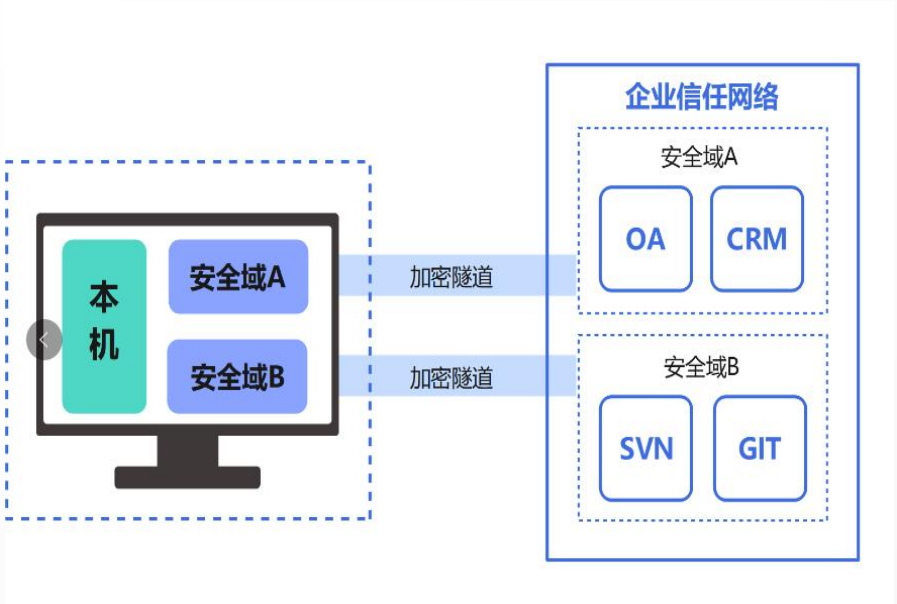
-非客户端或外来PC进入该网络，被主动隔离，无法访问到机密服务器和客户端。

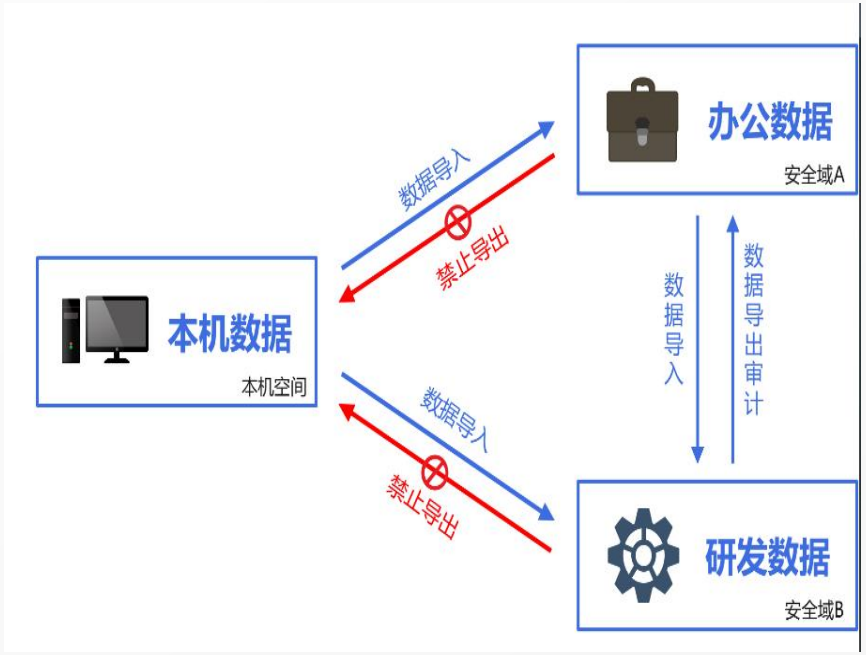


多安全域支持

SDC沙盒支持单个终端启用多个沙盒接入多个不同安全域，安全域之间、安全域与本机之间，有严格的数据隔离机制以及权限划分

SDC沙盒支持多安全域之间的文件流转，支持不同业务部门间的文件传输等业务场景。



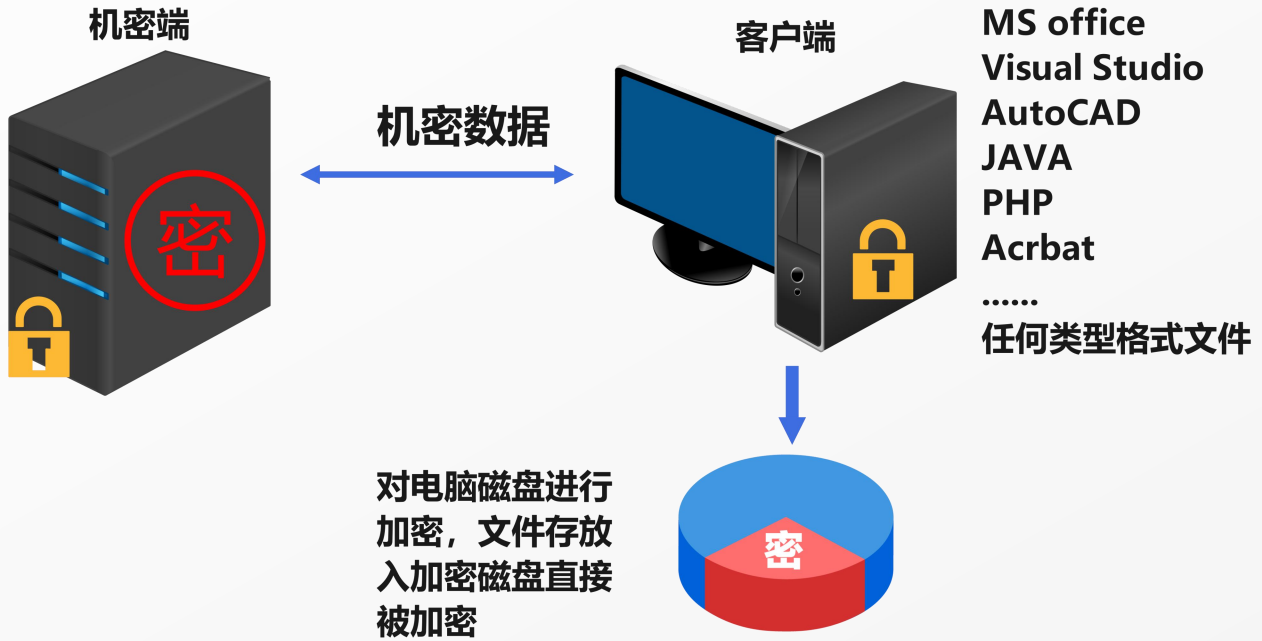


客户端所有涉密数据自动加密

客户端从SVN等服务器下载代码、文档等数据都只能存放在加密磁盘内，沙盒内所有文件格式、所有软件读写的数据都自动加密，不区分文件格式，不影响正常开发调试。

终端的涉密数据无法通过U盘，邮件，网络通信，聊天工具，光盘刻录，硬盘拔取等所有泄密途径泄密。

数据可以是源代码、文档、图纸、数据库等。



涉密文件加密导入导出

客户端可以把某文件加密导出，然后发给另一个客户端，再解密导入，整个过程不泄密。

应用场景例：

沙盒客户端之间进行文件交互，过程不泄密。

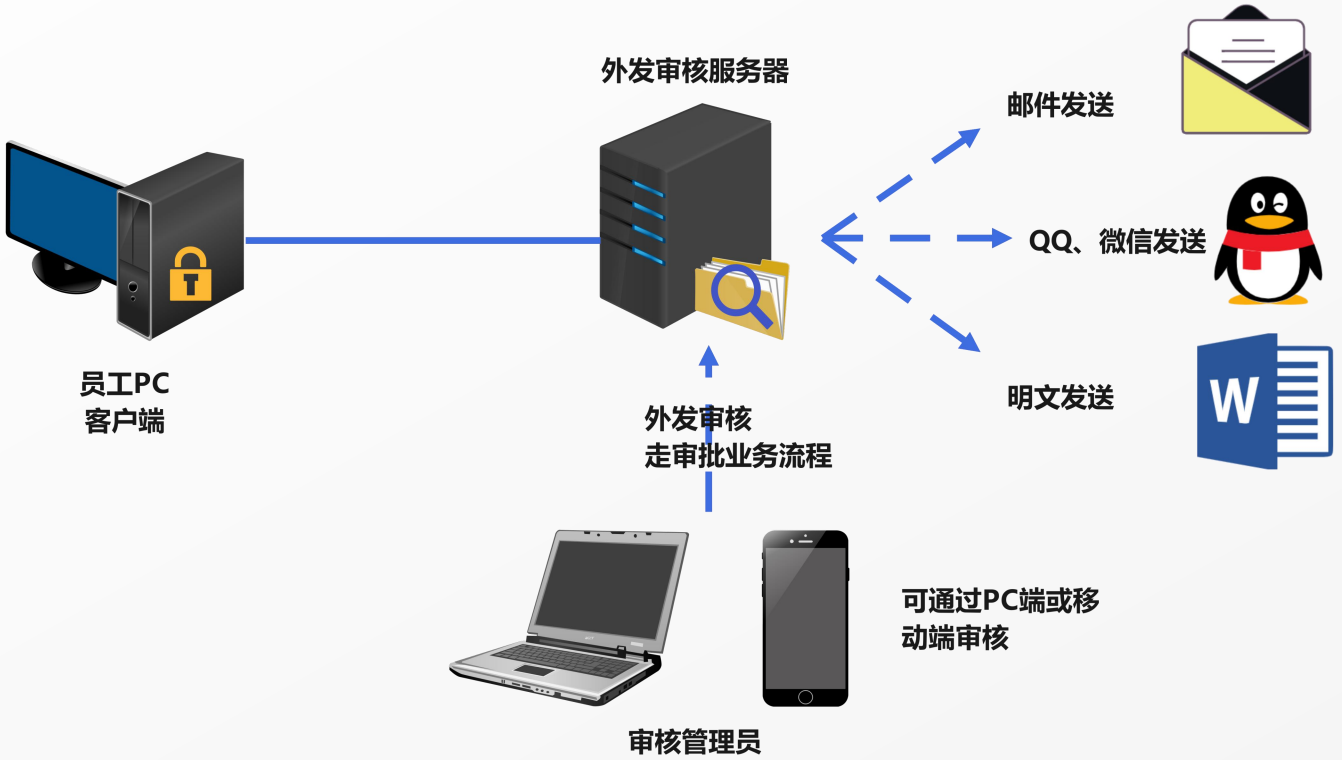
员工出差外地，现场根据客户需求开发调试，调试好了的东西，需要提交给客户，如果直接让解密，无法控制该人把其他涉密文件拷贝出去。所以这个时候，出差人员把要给客户的文件加密导出，然后发回公司，公司审核后，解密，走审核流程，然后把明文发给客户，形成有效控制。

文档外发审核

对于需要把包含源代码等涉密资料以明文的形式从涉密环境内导出，系统提供了文件外发审核功能

-文档明文外发：涉密文档明文发出必须经过审批，具有支持多流程、多级审批、事后审计等特点。

-移动端审核：管理员在审核文件时，可通过PC端、手机端（企业微信、钉钉）等形式进行审核。



安全隔离上网

对于在涉密状态下需要上外网查找资料的客户提供此功能模块。

在涉密状态下，通过该模块，可以正常上网查找资料，QQ、微信等聊天工具可用，Web邮件可用。由于与机密数据完全隔离且数据只进不出，安全隔离上网具有以下特点：

-无法把机密文件与文件内容复制粘贴出去；

-无法把涉密文件通过微信、邮件或网站上传出去；

-无法通过微信截图等把涉密截屏发送出去。

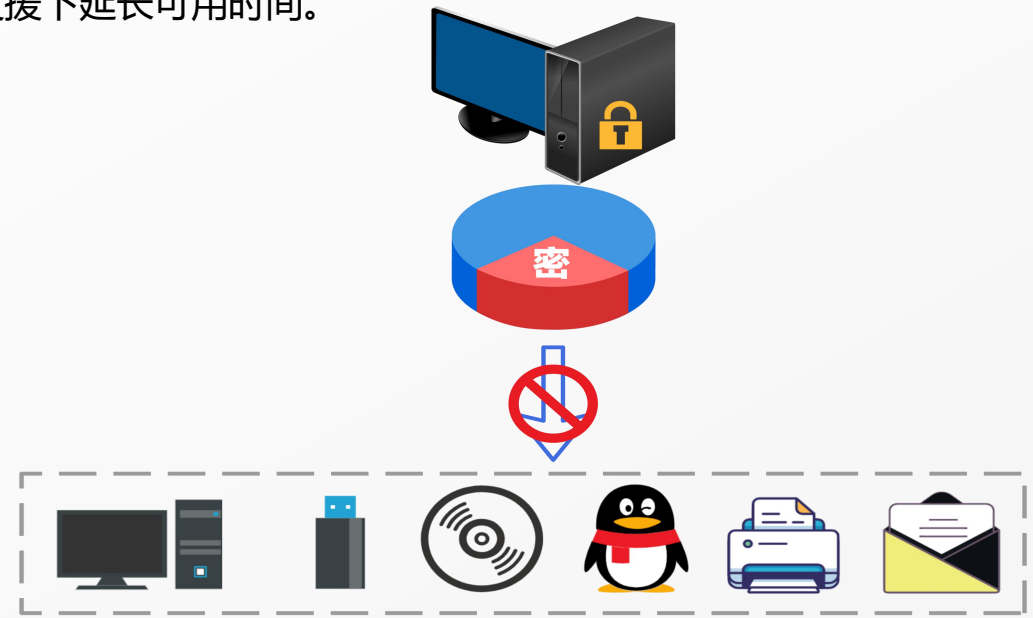
离线策略

为满足出差或家里加班情况，通过策略设定，可以让携带涉密数据的终端离线使用：

-离线使用时，所有涉密文件都还处于加密状态，可以在防泄密状态下正常继续工作。但如果超过期限，所有涉秘密数据都自动关闭，整个系统将处与保护状态，直到返回公司接入网络连接服务器后，才能正常工作。

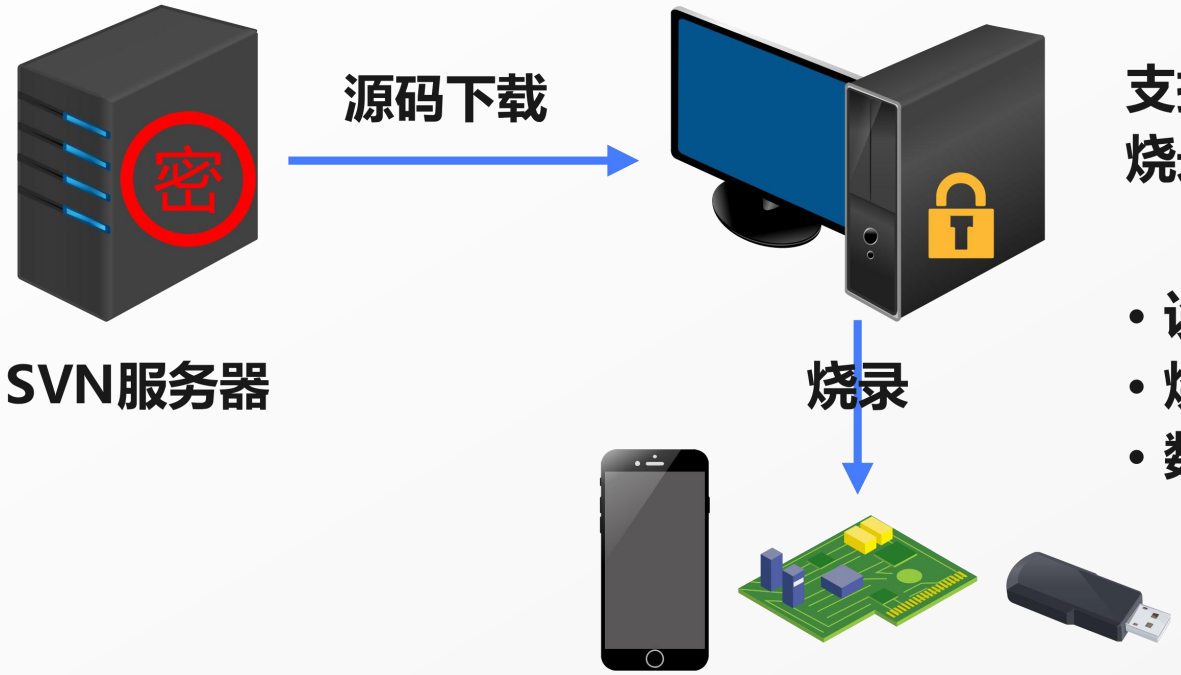
-如果万一笔记本电脑丢失或被盗，由于对方没有解密口令，所有涉密数据都处于保护状态，重新安装系统，硬盘插拔等，都无法获取电脑中的机密数据。

-离线策略过期可以在管理员支援下延长可用时间。



智能端口功能

智能端口过滤功能是SDC沙盒防泄密系统的外设控制模块。是通过软件方式，控制外设准入，过滤传出的数据文件，并对通过的数据进行服务器记录追溯。

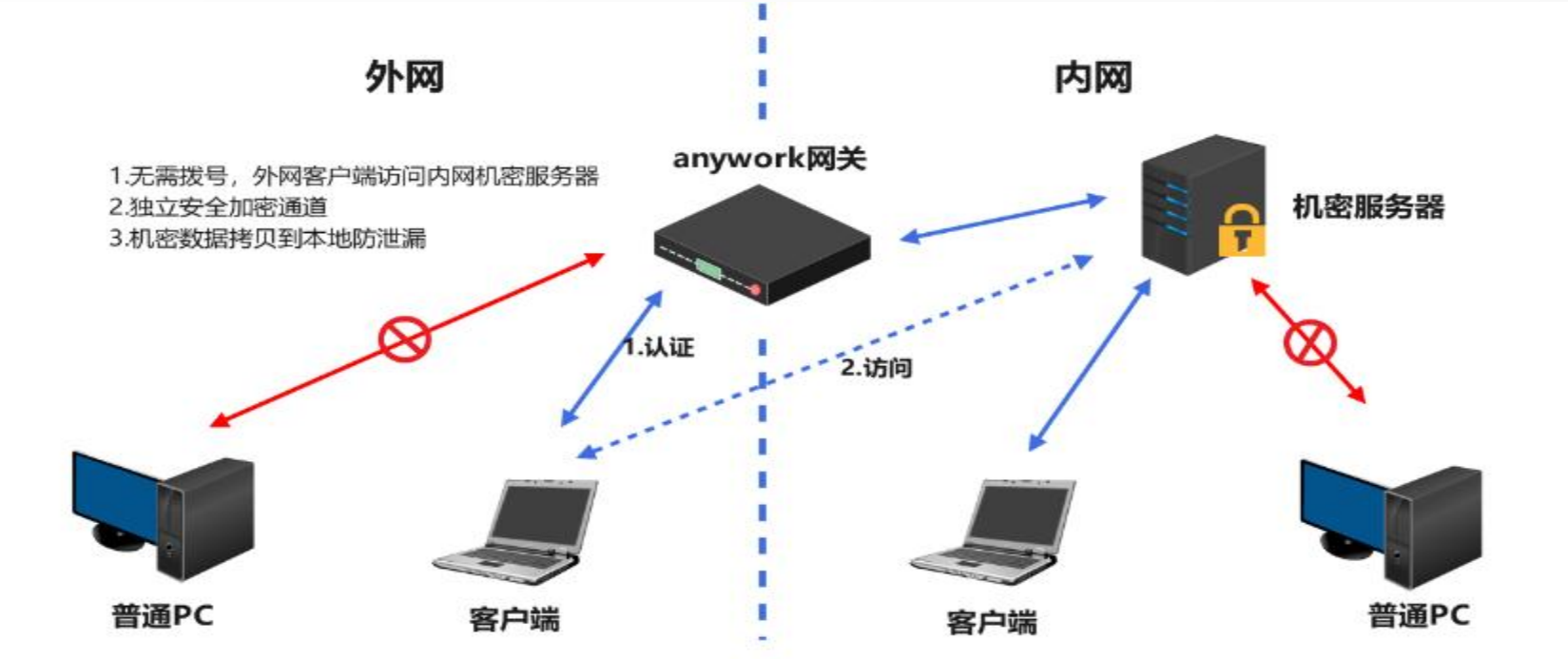


支持各种U口/网口/串口烧录工具

- **设备准入**
- **烧录数据过滤**
- **数据审计**

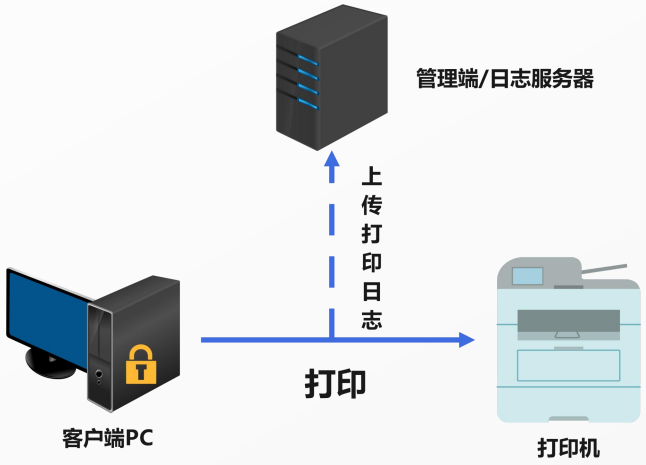
AnyWork网关

SDC沙盒客户端在公司外部，通过AnyWork网关访问内网，无需借助VPN，解决居家办公或出差在外的接入内网办公需求，在沙盒内访问内网数据，整个过程在沙盒内完成，沙盒内数据无法拷走，在做到灵活条件办公的同时，保障数据安全。



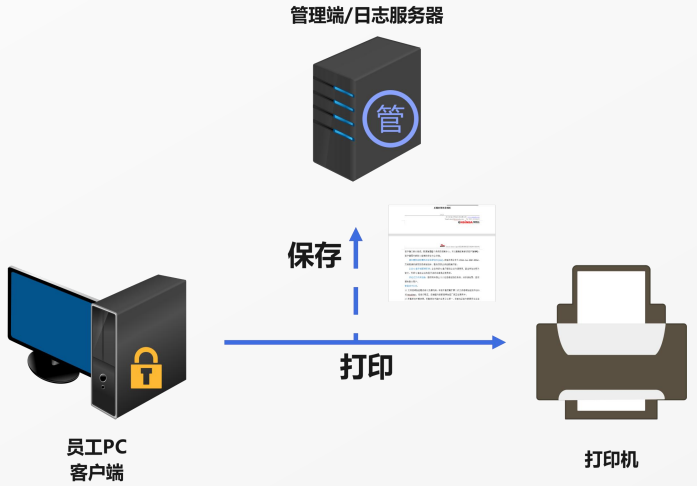
打印控制功能

通过策略设定可以允许某人在指定打印机上打印，
但文档打印内容将被转成图片日志收集到管理端，
做为事后审核凭证(谁什么时间打印了什么)。
可自定义设置打印水印。



日志监控功能

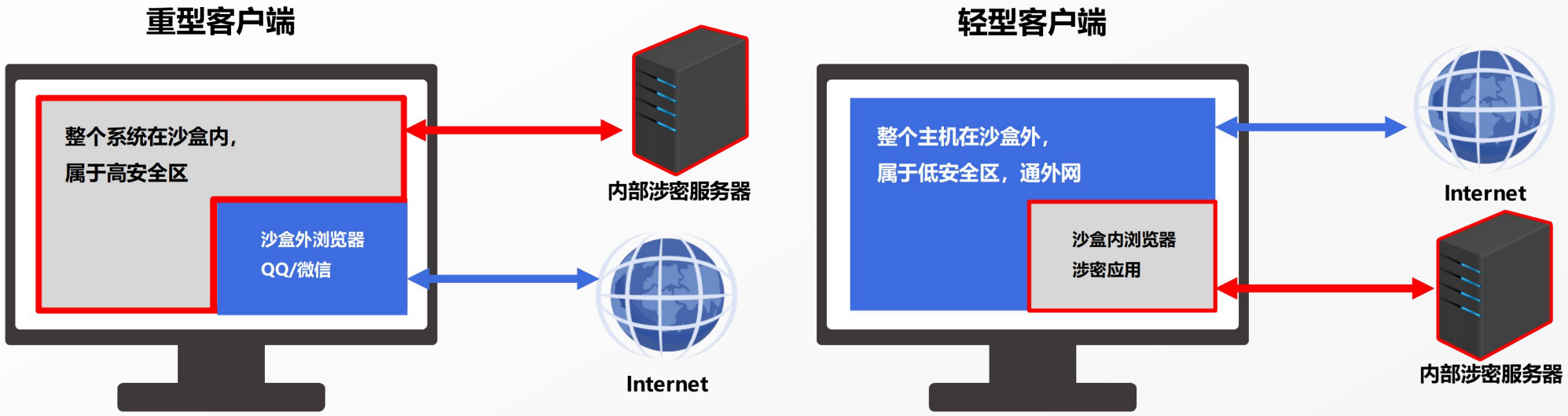
对管理端与客户端上用户操作进行记录，
包含管理端的管理员登录记录、修改策略记录等日志；客户端的登录日志、屏幕截屏监控、打印记录、剪贴板记录、智能端口日志记录等日志监控功能。



根据不同场景安装不同客户端

-研发人员的电脑，因为要进行调试编译，直接安装沙盒重型客户端。

-非研发人员（无需编译调试）的电脑安装沙盒轻型客户端。



由于整个主机都在沙盒内，沙盒内可以运行各种应用，不受限制。
但沙盒网络只能访问涉密服务器，沙盒外访问互联网。

在主机内挖出一块空间用来运行沙盒，沙盒内可以运行简单应用，访问涉密资源。
沙盒外主机可以自由访问互联网。

PART 03

产 品 特 点

产品特点 / 3-1

适合有业务系统和文档源代码等需要防泄密的企业，特别是研发型企业

SDC沙盒采用内核级加密技术，拥有代码级安全防护，可以防止各种变形泄密途径（如日志输出，web平台中转发布，通信小程序，外设烧录中转等），对精通开发的程序员也能有效管控。研发环境内所有涉密文件都只进不出，要出必须走审批。

支持所有文件格式，是环境加密。

-能对研发人员进行有效管理；

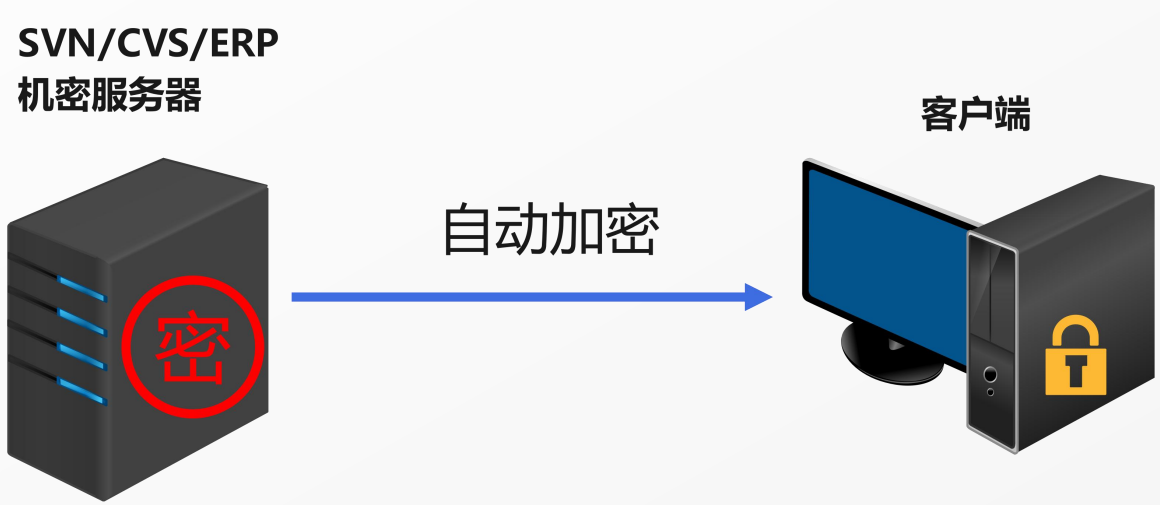
-允许使用非涉密资源（如上网），不影响工作效率；

-对外设烧录内容过滤和审计；

与应用服务器无缝结合，服务器端无需加密

能和现有的B/S架构系统，C/S架构系统无缝集成；如业务系统，文件共享服务器，文档服务器，ERP服务器，PDM服务器，OA等，VSS,CVS,SVN版本服务器等无缝结合。

服务器上的数据都是原数据，不需要对其进行加密，当数据离开服务器到达客户端时，才自动加密。原有的服务器备份等都继续使用，从根本上保证了业务的连续性，可用性，稳定性。



产品对比

产品 / 对比项目	SDC沙盒(代码级)	文档加密产品
设计理念	代码级安全，不区分进程和文件类型，是一个容器。	文档级安全，绑定进程和文件类型，对保存的文件进行透明加密解密
管控人员	精通电脑的，会编程的研发人员	主要针对不太懂电脑的办公人员。
管控内容	涉密空间内的文档文件和非文件数据(业务系统表单，数据库)	指定进程保存的文档文件
抗破解度	可以抵御会编程的人，可支持各种数据变形	可以抵御办公人员，会编程人员可以秒破，比如数据变形
复杂大型图纸加密	可以，且无速度损耗,速度快	可以，但速度损耗大
文件破损	无文件破损	小文件不会破损，大文件容易破损
支持平台	Windows平台/linux平台	Windows平台/linux平台
总结	**代码级安全，适合安全要求高的公司**	**基本安全，适合安全要求不高的公司**

产品对比-2

产品 / 对比项目	SDC沙盒(代码级)	某零信任沙盒产品
技术原理	依托终端微隔离管控，软件定义网络边界 **依托终端纵深防御管控，增加容器对应用兼容**	依托终端微隔离管控，软件定义网络边界
设计理念	基于零信任，软件定义边界，实现不同安全桌面，**可实现源码级防护。**	基于零信任打造的，定义软件边界，实现不同的安全桌面，**对数据做基本防护**
管控内容	办公文档、简单**和复杂**图纸、会话表单，**以及源代码**	办公文档、简单图纸、会话表单
内网交互	内网终端智能准入，终端和服务器之间用加密隧道**直接数据交互**，**不走网关**	内网终端依靠SDP网关准入，终端和服务器之间数据交互经由网关（**网关压力大**）
外网准入	外网终端通过AnyWork网关接入内网，和内部服务器进行交互	外网终端依靠SDP网关准入，终端和服务器之间数据交互经由网关
沙盒类型	应用级沙盒+系统级沙盒组合，大文件性能损耗很低，复杂软件支持好，**支持编译调试及烧录场景。**	只有应用级沙盒，大文件性能损耗大，不支持复杂软件，**不支持编译调试及烧录场景**
虚拟机支持	虚拟机**可以**运行在沙盒内	虚拟机**无法运行**在沙盒内
总结	**高级安全，不仅涵盖普通办公场景，还支持研发场景**	**基本安全，适合非研发普通办公场景，无法涵盖研发**

SDC沙盒支持OS

SDC沙盒管理端

- 支持window server 2008/2012/2016/2019

SDC机密端（SVN/GIT/PLM）

- 支持windows server2008/2012/2016/2019
- 支持linux常用服务器版本

SDC客户端

- 支持windows 7/8/10/11 32/64位
- 支持linux常用版本
- 支持真机Windows+虚拟机（任何操作系统）模式

PART 04

客 户 案 例

深信达的客户

深信达成立10多年来，一直深耕信息安全领域，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、研究院所等众多领域。

案例分享

高科技行业，担心核心代码和设计文档在研发过程中泄漏。

研发人员学历高，精通电脑操作，很容易通过编程泄密。

阻断互联网，不方便查询资料，影响效率；允许访问互联网，又会造成核心代码及数据泄漏。

通过移动存储设备拷贝，或者U口、串口、网口等端口连接外部设备进行调试，无法使用透明加密等产品。

通过安全工作环境隔离，形成研发安全域，保护核心代码安全。

一机两用，即可安全工作，又可方便上网。

多种安全机制，不能绕过系统防护泄密。

不影响软件调试，兼容性好，产品安全可靠。

深圳市速腾聚创科技有限公司

速腾聚创是激光雷达及感知解决方案市场的全球领导者。通过芯片、激光雷达平台与感知算法三大核心技术闭环，为市场提供具有信息理解能力的智能激光雷达系统，颠覆传统激光雷达硬件纯信息收集的定义，赋予汽车与机器人超越人类眼睛的感知能力。

研发环境一体化数据安全

保证企业研发环境安全，防止核心代码泄露

部署客户端数量：980

案例分享

高科技行业，担心核心代码和设计文档在研发过程中泄漏。

研发人员学历高，精通电脑操作，很容易通过编程泄密。

阻断互联网，不方便查询资料，影响效率；允许访问互联网，又会造成核心代码及数据泄漏。

通过移动存储设备拷贝，或者U口、串口、网口等端口连接外部设备进行调试，无法使用透明加密等产品。

通过安全工作环境隔离，形成研发安全域，保护核心代码安全。

一机两用，即可安全工作，又可方便上网。

多种安全机制，不能绕过系统防护泄密。

不影响软件调试，兼容性好，产品安全可靠。

大疆创新

大疆创新致力于持续推动人类进步，自 2006 年成立以来，在无人机、手持影像、机器人教育及更多前沿创新领域不断革新技术产品与解决方案，重塑人们的生产和生活方式。

研发环境一体化数据安全

保证企业研发环境安全，防止核心代码泄露

部署客户端数量：10000+

荣誉证书 / 4-3


苏州市信息技术应用创新联合会
政务工作组成员单位
单位名称：苏州深信达网络科技有限公司
证书编号：No.SZXCZWZ027


信息安全管理体系认证证书
苏州深信达网络科技有限公司
ISO/IEC 27001:2022


涉密信息系统
产品检测证书


图谱收录通知
苏州深信达网络科技有限公司：


麒麟软件NeoCertify认证


麒麟软件有限公司
杰出伙伴
苏州深信达网络科技有限公司


软件产品证书
深信达沙盒防泄密系统软件 V5.0
（T/SIA003-2019），评估为软件产品，特发此证。


信息技术应用创新工作委员会
技术活动单位
苏州深信达网络科技有限公司
有效期限：2024年8月至2025年7月
中国电子工业标准化技术协会
信息技术应用创新工作委员会
二〇二四年八月


统信软件产品互认证明


高新技术企业
证书
企业名称：苏州深信达网络科技有限公司
证书编号：GR202332006787
发证时间：2023 年 11 月 6 日
有 效 期 ： 三 年
批准机关：

感谢您的观看

CNSINDA

深信达