天锐绿盾终端安全管理系统

技术白皮书

厦门天锐科技股份有限公司

版权声明

本文件由厦门天锐科技股份有限公司免费提供，其内容专供用于评估厦门天锐科技股份有限公司为其提供产品及服务的能力，仅供参考。

1. 概述

企业大量技术和业务机密数据以电子文档的形式存储在计算机和网络中，其传播的方式多样，通过网络传播、U 盘拷贝、人员离职把电脑上的资料直接带走或全盘删除、黑客入侵窃取机密数据等，造成客户档案、财务报表、技术图纸、战略计划书等重要文档被非法传播或丢失，给企业带来严重的损失。需要有效地制定安全策略以保护机密数据信息。事实上，随着企业信息化进程的加速，内部泄密正在成为企业内部数据安全的最大威胁之一。

据IDC 报告，70%的安全损失是由企业内部原因造成的，也就是说企业中不当的资源利用及员工上网行为往往是“罪魁”，间谍软件、恶意程序、计算机病毒、端对端文档分享等不当的上网行为，导致了企业机密资料被窃，网络资源的浪费，企业运作的不畅等损失。FBI 和CSI 调查显示，超过 85%的安全威胁来自企业内部，威胁源头包括内部未授权的存取、专利信息被窃取、内部人员的财务欺骗等。在国内，诸如设计方案被窃取、关键客户名单和销售数据丢失等事件屡见不鲜，给企业造成了非常大的经济损失。

作为数据安全的老牌提供商，厦门天锐科技股份有限公司从全局的视角出发，整合数据防泄密系统、桌面管理系统和行为审计系统，对数据安全问题进行统筹规划、统一管理。从文档透明加解密、桌面行为管控、内外网行为审计等方面来减少内部泄密的可能，在内部构建起立体化的整体数据防泄露体系，使得成本、效率和安全三者达到最优平衡，实现真正意义上的数据安全。

2. 设计理念

2.1. 设计理念

天锐绿盾终端安全管理系统的设计理念是从源头保护数据安全，防止企业机密信息被破坏、丢失、泄密。通过对电子文档的实时动态保护、操作全过程的跟踪和操作行为的统一审计功能，实现了电子文档全生命周期的安全管理；对各种可能造成泄密的途径进行控制，达到保护企业数据安全的目的。追查数据泄露的渠道，使得“事前防泄露、事中可控制、事后易追查”落到实处，防止内部泄密行为的发生。

2.2. 工作流程

- 系统管理员通过控制台为每个终端操作员定制安全策略；
- 终端从服务器获取对应的安全策略后，自动加密安全策略保护范围内的文档，加密文档不影响安全进程的读写操作；
- 在机密文件使用过程中，终端将对操作员的所有操作行为进行全程监控；
- 系统具有强大的自我防护功能，任何恶意终止、退出或卸载客户端程序的行为都将是徒劳；也可以对客户端程序进行全面的隐藏，隐藏后终端电脑看不到客户端程序运行。
- 企业密钥可根据企业需要进行更改（需要 USBKEY 支持）。

2.3.文档保护方案概述

通过天锐绿盾对机密文件进行保护时，系统在不改变用户原有工作流程和文件使用习惯的前提下，对需要保护的进程生成的所有文件（无论该文件原来是明文还是密文）进行强制加密保护，并对机密文件的使用过程进行全程监控，有效防止了被动和主动泄密，消除内部安全隐患于无形之中。

解决问题：

- 防止单位内部机密电子数据泄露；
- 防止单位内部不同部门越权使用文档；
- 可追查数据泄露的渠道；

- 普遍适用于各种格式的电子文档；
- 从根本上解决了文档的二次传播，有力保障企业数据安全；
- 有效管理、监控局域网内电脑，提升办公效率。

系统方案：

只有安装了天锐绿盾终端的电脑在登入账号并授权后，才可以使用或查看加密文档，否则如果要查看加密文档，需要授权或提前对文档解密。终端电脑上的文件在创建、存储、应用、传输等环节中均以加密形式存在，可以杜绝黑客工具的窃取和监听，防止磁盘介质丢失导致的资料外泄等。

文件外发方案：

如有加密文件或机密文件需要外发出去，并希望对该文件做一些权限限制或者希望追踪文件的阅读记录，可以使用外发功能。外发功能对文档的限制方式包括：限制打开次数、限制只在规定时间段内可以打开、限制只能在某一台电脑上打开，限制打印、截屏，以及设置文件打开密码、超时自动销毁等。这样可以轻松、灵活地控制外发文件，在实现数据共享的同时，能够防止资料越权读取， 防止外发文档二次扩散，确保数据安全。

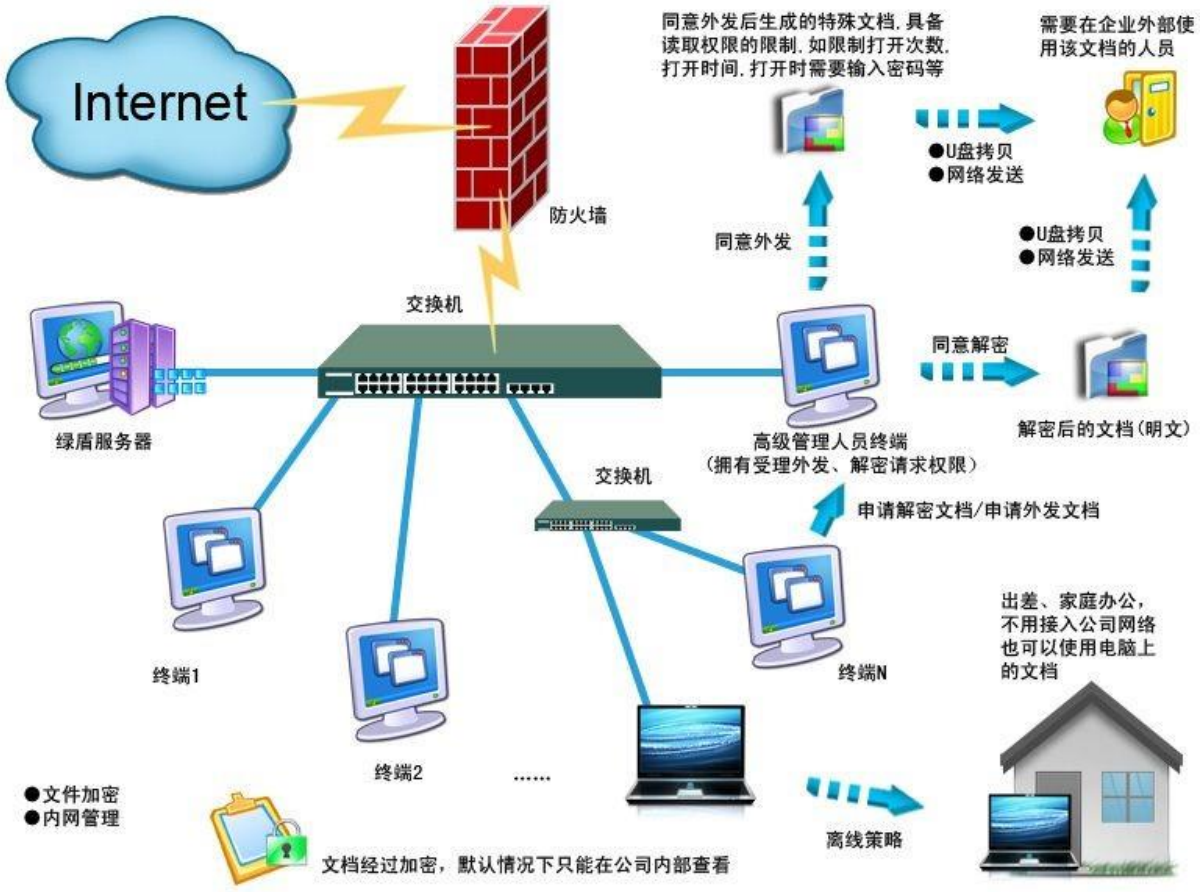
外发也可以通过云平台追踪阅读记录，对已授权权限进行修改等。

离线方案：

- 短期离线方案：直接在服务器上设置允许脱机时间，离线后仍可以阅读文档。比如高级管理人员的笔记本电脑下班后需要阅读加密文档；
- 中长期离线方案（如出差）：可以使用天锐绿盾的离线策略。离线策略需要向管理员申请，获得批准后导入即可。且离线策略可以灵活设定离线使用天数，这样在方便员工外部办公的同时也有效地保证了文档的安全。

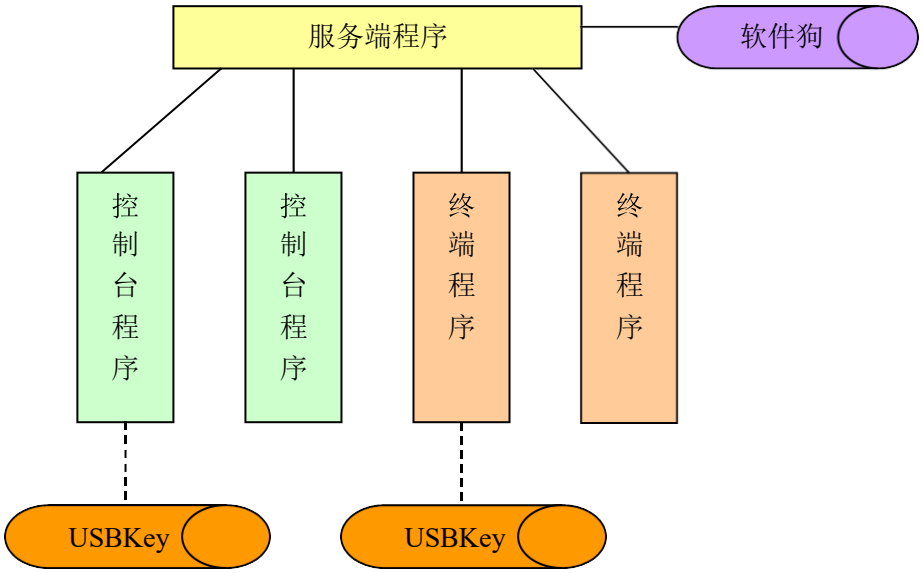
3. 产品架构

3.1. 产品架构



3.2. 产品组成

天锐绿盾终端安全管理系统（以下简称：“天锐绿盾”）是数据防泄密系统、桌面管理系统和行为审计系统共同的工作平台。天锐绿盾由硬件和软件组成。软件包括服务端程序、控制台程序和终端程序；硬件上由服务端使用的软件狗，以及控制台和终端使用的 USBKey 组成。



服务端程序

服务端程序需要运行在不关机的服务器电脑上。用于管理密钥及各种策略；用于存储终端的屏幕录像数据、实时程序窗口切换记录、文件操作记录、聊天内容等；用于处理来自于客户端的各项验证，避免客户端可以随意安装和使用。服务端程序支持扩容，支持海量数据存储。

主要作用包括：

- 管理加密密钥
- 进行软件注册
- 终端操作员身份验证
- 存储系统配置信息
- 海量存储系统运营数据
- 提供控制台接入

控制台程序

控制台程序运行在管理员电脑上，是系统的管理配置界面。控制台通过网络与系统管理中心联接，对系统管理中心进行在线配置和管理。只有持有管理员密钥的用户才能登录控制台。

主要功能包括：

- 实时监视终端操作行为
- 配置终端策略
- 查看历史记录
- 查询统计信息

终端程序

终端程序安装在需要保护机密文件或者是需要阅读加密文件的主机上。

天锐绿盾终端类型分为两种类型：全功能版本和特殊版本，其中特殊版本又包括两种类型：只启用文件加解密功能终端和离线终端。特殊版本只适用于天锐绿盾数据防泄密系统中。

全功能版本：包含全部功能的终端，可在服务端调整系统功能模块；

只启用文件加解密功能：只包含文件加解密功能；

离线终端：长期不与服务器通信（比如在公司外部），但又要查看公司的加密文件、以及需要加密自己电脑上文件的电脑，可以安装离线终端。

安装成功以后，在线终端会随操作系统的启动而自动启动，每次启动时，终端会从服务器获取最新的安全策略及系统密钥，所有策略范围内的文件都会被自动加密，并且在使用过程中被全程监控，并生成操作日志，留待日志审计员事后追踪责任人。终端主机只有在与管理中心联机的状态下或者在离线策略（包括短期离线策略和长期离线策略两种）允许下，才能正常启动终端。终端根据 IP 地址来识别服务端，支持更改终端连接的服务端地址，方便服务器迁移。

主要功能包括：

- 操作员登录验证
- 自动加解密文件
- 实时记录操作行为，并上传记录

- 执行终端策略

4. 产品功能

4.1. 文件透明加解密

天锐绿盾能在不影响使用者操作习惯的情况下，在操作系统内核里面采用文件过滤驱动程序实现透明加密存储，加密后的文件可以在公司内部正常流通使用，一旦脱离公司网络，文件将无法打开。即在操作编辑文档或图纸同时后台自动加密文件，操作人员毫无察觉。

加密文件只能在公司内部安装有天锐绿盾终端的电脑上正常使用，离开企业电脑环境无法使用。在脱离企业电脑环境下，文件只有经过公司管理人员解密后， 才能正常使用。防止用户之间非法复制、外部发行，防止单位内部机密电子数据泄露及电子文档的二次传播，有效的保证了核心数据的安全。

4.2. 半透明加密

对于企业的管理部门，他们往往不是数据的生产者，但由于业务需要，会是数据的使用者。管理部门本地自己生成的文件都不加密，同时又要能打开公司内部的加密文件，并确保这些加密文件编辑保存还是处于加密状态，有效保证数据的安全。

4.3. 敏感内容识别

为了确保企业涉密文档的安全性，通过事先设置的敏感数据特征（关键字/对、正则表达式、文件名），对于正在编辑、保存的文件进行内容检测，当检测到文档中包含敏感内容时则会自动加密上，整个过程对于操作员毫无感知。

4.4. 落地加密

在日常工作中，员工常常要通过企邮箱、企业通讯工具等方式接收外部文件，

为防止这些渠道接收的文件泄密，员工从邮箱、通讯工具等途径下载的文件，下载即加密，在企业内部可正常查看、编辑、保存和交互，在不影响员工日常办公的前提下保证从网络平台接收、下载数据的安全。

4.5. 全盘扫描加解密

在系统部署上线时，企业可根据管理需要对企业内部终端电脑的历史文件进行全盘或指定目录、文件类型以及包含敏感信息数据等扫描加密。卸载系统时，对终端电脑的加密文件进行解密。

4.6. 密级管理

为了确保企业内部核心文件的安全，可对每个终端用户设置用户密级：公开文件、内部资料文件、秘密文件、机密文件、绝密文件。设置密级后，用户创建、编辑的文档上会被自动标识指定的密级（公开文件密级只显示加密锁，内部资料文件、秘密文件、机密文件、绝密文件还会在加密锁上显示数字标识，分别对应为1、2、3、4，）用户只能查看不高于自己密级的文档，从而有效防止内部重要文档被越权查看。

4.7. 离线管理

多种终端离线类型：短期离线、长期离线和永久离线（离线终端），可适应不同的网络环境和使用需要。出差或工作需要外带笔记本电脑暂时离开单位环境，可通过离线授权，设定资料正常使用时间。在授权的离线时间内，终端可以正常工作，超过离线时间，将无法打开加密文档，从而使重要数据一直处于加密状态，避免外出时有意或无意的传播。

离线期间用户的操作记录也会保存下来，回到单位后，终端连接上服务器，这些记录会自动上传至服务器，供管理员审计查看。

4.8. 水印技术

支持打印水印和屏幕浮水印功能，可以自定义水印信息内容和水印显示方式，防止通过打印机打印、屏幕截屏、手机拍照等方式把机密文档信息内容泄漏出去。屏幕浮水印可以设置只对指定的应用程序生效，即需要保护的程序使用时才显示水印，其他应用程序不受影响；或者设置只有截屏时才显示水印，其他时候使用不受影响。

4.9. 文件外发控制

文件加密后，在本机上打开和在公司内流通都可以正常，如果要发送给协作单位，且要控制文件的操作权限，可以将文件制作成天锐绿盾外发文件。外发文件可以控制文件的操作权限，其中包括：打开次数、生存周期、密码验证、修改限制、截屏限制、打印限制、过期自毁等，超出限制将无法打开文件并自动删除文件，防止外发文档二次扩散，确保数据安全。除此之外，还支持屏幕水印、打印水印，对于打印和拍照可以起警示作用。

4.10. 审批流程

当终端用户需要外发加密文件或带笔记本电脑出差时，需向指定的审批人员发送解密/离线申请。可以根据企业的业务流程自定义审批流程。

- 流程支持多级审批、同级多人审批、委托审批等模式，审批方式支持手动审批、审批人离线时自动审批等。
- 支持 Web、移动终端审批，审批人员可以通过网页、手机 APP、移动办公设备来处理申请，提高流程审批便捷性。
- 申请解密支持根据文件密级、文件后缀类型智能选择审批流程。
- 审批消息即时提醒，提高审批效率。
- 审批人员审批时可以设置需要输入合法口令，提高审批安全性。

- 所有审批日志均保存在服务器上，方便日后统一审计及查看。申请人和审批人也可以查询自己的申请记录、待审批、已审批信息。

4.11. 工作模式切换

可根据需要，允许某些用户可以在规定的时间段内自由地切换工作模式：开启加密或关闭加密功能。在工作模式下（开启加密），修改和创建的文件自动加密，防止机密资料外泄；非工作模式下（关闭加密），新创建的文件不加密，但也不能打开加密文件，在机密资料不外泄的前提下，可以处理个人事务。

4.12. 文件自动备份

可以设置需要自动备份到服务器的文件类型，防范重要文件遭破坏或恶意删除等情况。文件自动备份包括：新建、编辑加密文件时备份，拷贝文件到 U 盘时备份，新建、编辑、删除、复制、打开、重命名文件时备份（可以是非加密文件）。可以自定义需要自动备份的文件类型，设置超过指定大小的文件不备份， 减少对服务器和网络的负载。

对加密文件，可以同时备份到本地和备份到服务器。提供本地备份文件的自动管理，设置只保留最近多少天的备份文件，超过指定天数的备份文件自动删除， 减少长期备份文件对终端硬盘的负载。

4.13. 与应用服务器无缝兼容

天锐绿盾提供成熟的企业业务系统（OA、ERP 等应用服务器）数据安全解决方案，满足与各类业务系统的无缝安全集成，在不改变用户现有工作习惯时，实现对核心业务数据的安全防护。

可以与天锐绿盾应用服务器安全接入系统结合，在终端访问应用服务器时进行终端身份的强制合法性验证，合法的终端才可以正常接入应用服务器，非法终端禁止访问。同时，配合终端的透明加解密和服务器白名单模块，实现文件上传自动解密、下载自动加密。通过对应用服务器的绑定，有效控制仿冒应用服务器， 防止终端非法外联泄密。

4.14. 桌面行为管控

- 远程管理。可以对终端进行远程协助、远程注销/重启/关机、远程发送消息、远程锁/解屏、远程进程管理、远程服务管理、远程资源管理、远程共享管理等。可以远程查看终端电脑的 CPU、内存、硬盘、网卡等使用情况。
- 应用程序黑、白名单管理。提供应用程序白名单和黑名单功能，管理控制终端可以使用哪些应用程序，不能使用哪些应用程序。当终端用户运行的程序窗口标题包含一些敏感关键字时，可以阻止其运行。
- 聊天工具白名单。控制终端用户在指定时间（如上班时间）只能使用白名单中的聊天工具账号，禁止登录使用私人聊天工具账号。
- 上网行为管理。可以对终端电脑的上网行为进行管控，包括禁止或只允许浏览指定网站或端口，限制上传/下载流量，对网络进行有效隔离，违规访问时进行报警提醒或断开网络。可以对发帖内容和邮件内容进行控制，当发送内容包含指定关键字时，阻断此次发送行为。
- 软硬件资产管理。记录并统计终端的软、硬件资产情况，方便资产盘查。当资产发生变更时，可提醒管理人员。

4.15. 硬件设备管理

可以对各种硬件设备进行管理控制，包括打印机、光盘、软盘、USB 存储设备（包括 U 盘、移动硬盘、数码相机等）、WiFi 连接限制、串口、并口、红外线、蓝牙、MODEN、1394 主控制器、USB 鼠标、USB 网卡、无线网卡、虚拟网卡、声音设备、拨号连接等进行有效管控。

打印机限制可以禁止使用所有打印机、禁止使用所有网络打印机、只允许使用指定打印机、只允许指定程序使用打印机等；对 USB 存储设备可以设置允许使用、禁止使用、只读及插入 U 盘时断开网络。此外，USB 存储设备还可以进行认证管理，在限制 USB 存储设备使用的情况下，认证的 U 盘、移动硬盘可以正常使用，没经过认证的外来 USB 存储设备将不能被识别。

4.16. 远程任务推送

可以远程下发各类应用程序安装包和补丁（可以指定目录），安装程序可根据执行参数和安装包类型（MSI 包）自动完成安装，提高系统维护效率。可设定任务的执行时间，指定时间段生效或永久有效，并记录所有任务情况供后续审计查看。

4.17. 全面操作行为审计

- 文件操作记录。全程记录文件的各种操作，包括新建、编辑、删除、复制文件等，记录通过 U 盘、移动磁盘、网上邻居的文件操作，监视文件打印操作行为及其打印内容。
- 聊天内容监控。可以监控主流聊天工具的聊天内容，记录QQ、微信、钉钉、企业微信、企业QQ、千牛、Skype、飞秋、飞书等聊天工具发送的文字、图片和文件内容。
- 网页浏览记录。记录网页浏览信息，支持HTTPS，可点击记录直接访问该网页，并可审计网页浏览时长；记录员工在主流论坛上的发帖记录，审计外发言论的合法性。
- 邮件内容监控。可以监控邮件收发记录，记录信息包括邮件的标题、大小、发件人地址、收件人地址、邮件正文内容以及附件内容。
- 屏幕追踪、录像。远程实时监视终端电脑的屏幕画面，追踪员工桌面操作情况，并可以定时进行屏幕录像，供事后查看。
- 报警规则。提前设置监控各种操作的监控阈值，对于触发报警规则的操作进行报警并记录。
- 统计报表。可以按分组统计终端的使用程序、浏览网页、聊天内容及网络流量使用情况，并生成饼图或柱状图。

5. 产品特点

5.1. 平台化管理

天锐绿盾整合了多个系统，可以根据实际运用需要，选择一个或多个系统。部署多个系统只需一个安装包一次性安装，后续增加其他系统不用另外再安装部署，只需后台进行管理控制，大大减少实施维护成本。多个系统统一一个管理入口，方便管理员的日常维护，减少学习成本。

5.2. 安全性

- 三重密钥管理。文档加密采用独有的三重密钥管理，用户可自定义密钥，在安全上更有保障，大大增强破解难度。
- 服务器策略备份。服务器端具有安全备份及恢复机制，一旦出现硬件故障， 可以及时将配置导出恢复，降低用户使用风险。
- 文件容灾备份。可以根据需要，设置需要自动备份的文件类型，备份文件会自动上传到服务器进行保存，防止误操作或恶意删除带来的文件丢失。

5.3. 兼容性

- 操作系统：支持 Windows 各版本；支持简体中文、繁体中文、英文版；支持Linux 各主流版本；支持Mac10.12及以上系统；支持 iPad、iPhone 和 Android 各主流版本。
- 杀毒软件：兼容了国内外近 20 种杀毒软件，包括诺顿、卡巴斯基（Kaspersky）、McAfee、瑞星、江民、金山毒霸、360 安全卫士、Nod32、趋势等。
- 应用程序软件：兼容支持各种应用软件，包括文档类、工程类、设计类、编程类、图像类等工具软件。
- 网络环境：支持多网段、跨 VLAN 和VPN 环境。

5.4. 灵活性

- 不改变用户的操作习惯，不需要用任何第三方的查看工具。
- 提供多种用户认证方式，满足不同应用需求。包括：用户名和密码登录；绑定电脑自动登录；USBKEY 绑定登录；域结合登录；钉钉、微信、企业微信扫码登录等。
- 支持带笔记本电脑回家、出差办公，在保障安全的同时给予灵活管控。
- 支持自定义添加受控程序，可以满足所有的应用程序加密。
- 策略配置灵活，可以对不同的用户分配不同的控制策略。
- 自定义审批流程，满足不同的业务流程。支持多级流程审批、同级多人审批、委托审批等模式，支持审批人离线时自动审批。可查询所有审批信息。
- 可以直接使用 Outlook、Foxmail 邮件工具（不局限于自带邮件工具）发送邮件到邮件白名单地址，不改变用户的操作习惯。
- 支持 iPad、iPhone 和Android 移动终端设备，实现通过手机端直接阅读加密文件、审批处理解密申请等，解决移动办公问题，提高工作便捷。

5.5. 易用性

- 可以与域结合进行远程推送安装，也可以选择静默安装，简化管理员的操 作。
- 支持从服务器端对用户终端强制批量升级。
- 系统内置一些常用的应用程序文件加密策略、角色、网页库，只需简单的勾选操作，无需复杂的设置，即可满足大部分用户的使用需要。
- 管理操作界面简单，容易上手，管理员查看记录一目了然。
- 支持AD域组织架构、钉钉组织架构、企业微信组织架构同步。

5.6. 实时性

- 终端策略规则实时下发，一旦更改，即时生效。
- 终端操作行为实时上传，管理员即时查看。

5.7. 可扩展性

- 实施多个系统只需一次性安装部署，后续增加平台中其他系统不用再另外安装，只需后台进行管理控制，降低部署和维护成本。
- 多采集服务器部署方式，可以添加多个采集服务器，缓解主服务器压力。适用于用户数较多、分公司部署的情况，理论上可以支持无限终端用户。

6. 关键技术

6.1. 文件过滤驱动加密技术

目前市面上的文件透明加密技术，主要分为两大类：应用层透明加密技术和驱动层透明加密技术。大部分的加密软件是采用应用层透明加密技术。

应用层透明加密技术：通过 Windows 的钩子技术，监控应用程序对文件的打开和保存，与应用程序密切相关。由于不同应用程序在读写文件时所用的方式方法不尽相同，同一个软件不同的版本在处理数据时也有变化，必须针对每种应用程序、甚至每个版本进行开发。且很容易通过反钩子来避开绕过。

驱动层透明加密技术：基于 Windows 的文件系统（过滤）驱动（IFS）技术，工作在 Windows 的内核层，与应用程序无关。由于工作在受 Windows 保护的内核层，运行速度更快，加解密操作更稳定。但因为要充分考虑到与 Windows 及其它应用在驱动层软件（如杀毒软件）的兼容，驱动层开发难度相对应用层要高。

天锐绿盾采用 Windows 内核的文件过滤驱动实现透明加解密，对用户完全

透明，用户打开文件、编辑文件和平常一样，甚至毫无感觉，不影响用户操作习惯。同时由于在文件读写的时候动态加解密，不产生临时文件，因此基本不影响速度。

6.2. 三重密钥体系

天锐绿盾采用独有的三重密钥管理，包括主密钥、企业密钥和文件密钥，在安全上更有保障。

- **主密钥：**全球唯一，保证不能搭建出两套一样的加密环境，即保证任何两家使用天锐绿盾的客户文件无法相互打开。
- **企业密钥：**企业自行设置，保证厂家获取到密文，也无法解密。
- **文件密钥：**每个文件加密时会随机生成一个文件密钥，以提高加密的安全性和破解难度。

6.3. 自主研发数据库

采用自主研发的专用数据库，为天锐绿盾量身定做，存取数据速度快，兼容性好， 性能安全稳定。无需另外安装部署数据库，系统一键式安装、升级，系统维护和数据库迁移简单快捷，降低企业投资成本。

6.4. 严密的途径控制

严格控制可能导致泄密的各种途径，包括：

- 控制打印机、光驱、软驱、USB存储设备、WiFi
- 禁止屏幕截取（如QQ 截屏、红蜻蜓截屏、屏幕录像工具等）
- 控制复制粘贴
- 禁止 OLE 插入
- 禁止 WPS 等网盘
- 控制虚拟打印机

6.5. 支持 Linux 系统加密

Linux 操作系统是非常流行的开发、编译平台，对程序开发公司来说，Linux

平台上的源代码保护至关重要。天锐绿盾支持对 Linux 平台中的源代码、文档进行加密保护，且与 Windows 加密客户端完美兼容，方便用户在 Windows 和Linux 平台上对加密文档进行查看、编译等交互操作。

- 采用基于 Linux 内核的文档透明加解密技术，不改变用户操作习惯，不改变文件格式和大小，编译加密后的源代码时长增加很少，为5%以内。
- 应用防护，支持防拷贝、粘贴、截屏等操作控制。
- 支持 Ubuntu、CentOS、Debian、Redhat、Fedora、中标麒麟、银河麒麟等各种 Linux 操作系统。
- 支持系统工具类、文本编辑类、编译运行类、交叉编译类等，支持自定义添加受控程序。

6.6. 支持 Mac 系统加密

Mac操作系统是苹果电脑的专用系统，Mac平台上的保护也至关重要。天锐绿盾支持对 Mac平台中的源代码、图形、办公文档进行加密保护，且与 Windows、Linux 加密客户端完美兼容，方便用户在 Windows 和 Linux 以及 Mac 平台上对加密文档进行查看、编译等交互操作。

- 采用基于 Mac内核的文档透明加解密技术，不改变用户操作习惯，不改变文件格式和大小，编译加密后的源代码时长增加很少，为 5%以内。
- 支持XCode等各种开发工具、Photoshop等平面设计软件以及Pages、Numbers、Keynote办公软件、微软Office办公软件所生成文件的加密，支持自定义添加受控程序。
- 应用防护，支持U盘限制，端口限制，支持防拷贝、粘贴、截屏等操作控制。
- 支持的系统版本 10.12-12.3。

7. 建议运行环境

服务端程序

- CPU：Intel Core i5 / Intel Xeon E3 4核 3.0GHz
- 操作系统：Windows 7/10/11;Windows Server 2008/2012/2016/2019
- 内存：8G
- 硬盘：500G

（根据用户数量的差异，中大型企业建议选购专业的服务器作为天锐绿盾服务器、安装WindowsServer系列服务器操作系统，小微企业也可用普通PC作为绿盾服务器）

控制台程序

- CPU：Intel Core i5
- 操作系统：Windows XP/7/10/11;Windows Server 2008/2012/2016/2019
- 内存：4G或以上
- 硬盘：SATA500G

终端程序

- CPU：Intel Core i5
- 操作系统：Windows/Linux/macOS/iOS/Android
- 内存：4G或以上
- 硬盘：SATA500G

移动终端

- iPhone，iPad 7.0 及以上
- Android 4.0 及以上