IP-guard九大产品19大模块功能

IP-guard 文档加密系统

IP-guard 敏感内容识别系统

IP-guard 终端安全管理系统

文档操作管控	文档打印管控	设备管控	移动存储管控
即时通讯管控	邮件管控	网页浏览管控	网络控制
网络流量管控	应用程序管控	软件中心	文档标签
水印及追溯	屏幕监视	资产管理	远程维护
风险审计报表	文档云备份	基本功能（必选）	

IP-guard 视觉感知

IP-guard 文档安全交换系统

IP-guard 安全桌面

IP-guard 安全网关

IP-guard 准入网关

IP-guard 安全U盘

各行业标杆企业一致信赖IP-guard

闻泰科技 · 中航锂电 · 美的Midea · 国轩高科 · 浪潮inspur

科大讯飞 · 小米 · 华星光电 · 天马微电子 · 北斗星通

追觅 · 米哈游 · 海天 · 唯品会 · 屈臣氏

oppo · vivo · 华为终端 · 深信服科技 · 中兴

海辰储能 · 比亚迪 · 蔚来 · 小鹏汽车 · 广汽集团

中国移动 · 发那科 · 三一重工 · 中南市政院 · 深圳发改委

万科 · 海正药业 · 美莱整形 · 老百姓大药房 · 石药集团

微众银行 · 长沙银行 · 容诚 · 飞鹤 · 海大集团

TEC Solutions Limited 溢信科技

广州 | 深圳 | 北京 | 上海 | 长沙 | 珠海 | 中山 | 东莞 | 重庆 | 成都 | 武汉 | 西安
郑州 | 济南 | 沈阳 | 青岛 | 南京 | 合肥 | 杭州 | 苏州 | 宁波 | 厦门 | 南昌

广东广州科学城科学大道182号创新大厦C3区401、501室

400-666-1438　　sales@ip-guard.net

www.ip-guard.net　　印刷日期：2024年11月

大讲堂

IP-guard 一体化终端安全管理系统

- 您是否担心企业内部机密被随意泄露出去？
- 您是否面临U盘、移动硬盘等外设使用混乱的终端安全管理问题？
- 您是否有提高企业工作效率、加强运维管理的需求？

终端安全专家IP-guard为您分忧！

IP-guard

专注终端安全 保护核心机密

IP-guard三维智能信息防泄露整体解决方案

保护商业机密，提高企业竞争力

企业信息泄露常见途径：

- ▶Email导致重要信息在网络上肆意流传
- ▶U盘、移动硬盘、打印机等外部设备泛滥，信息被随意传播
- ▶U盘、笔记本电脑丢失，其中机密随之泄露
- ▶重要文档被随意浏览，并恶意篡改、删除
- ▶外发重要文档遭遇接收方泄密
- ▶ERP等服务器被非法访问，机密亦被顺手牵羊
- ▶公司内部信息被非法上传到网盘

防止机密文档泄露

对重要文档采用高强度透明加密，通过控制复制、打印、截屏等权限，随时随地保证机密安全；采取敏感内容识别技术，精准识别高价值文档，实施更准确保护。

防止重要信息被非法操作

控制用户对重要文档复制、修改与删除的权限，在修改或删除时可以自动备份，并通过审计详尽记录文档全生命周期的操作，杜绝非法操作造成企业损失。

防止文档上传网盘泄密

封锁网络上传的行为，防止非法上传重要文件到网页邮箱、网盘等网络服务器。

防止打印泄密

限制用户使用打印机以及打印程序，并可在打印文件上添加水印，同时详尽记录每一次打印操作。

防止邮件泄密

通过限定收发件人、主题、附件内容及大小等，限制电子邮件发送，并详尽记录邮件来往的信息，杜绝不合规的邮件发送行为。

防止即时通讯泄密

禁止通过IM发送文件、图片及截图，降低泄密风险。

防止U盘丢失泄密

支持对U盘加密或对拷入U盘的文件自动加密，消除由于U盘被盗或者丢失导致的泄密风险。

可记录所有U盘的插拔和拷贝文件的详细情况，对U盘使用情况了然于心。

防止外设泄密

对企业内部U盘、移动硬盘、智能手机、上网卡、随身wifi等外设进行统一管控，禁止随意接入企业计算机，防止非法拷贝和非法外联。

防止未经允许访问服务器

防止内部计算机擅自脱离监管，对试图接入公司内网并访问受保护服务器的行为进行阻断，保证只有安装了客户端并进行人工授权的计算机才能正常访问服务器。

震慑拍照泄密行为

支持在计算机屏幕或应用程序上显示水印，有效震慑通过拍照、截屏、录屏泄密的行为。

文档流转追踪

支持在文档中加入显性、隐性水印，或在文档中加入流转标记，从而掌握文档流转的情况，并进行精准追溯。

文档标签管理

用户可自主根据文档的重要程序加上合适的标签和密级，系统根据标签和密级对文档进行加密保护或外传控制。

IP-guard一体化终端安全整体解决方案

提高工作效率 加速企业前进

企业行为管理常见问题：

- ▶上班时间炒股、玩游戏、网络闲聊、浏览无关网页，降低工作效率
- ▶随意安装软件，导致恶意软件横行及版权纠纷
- ▶访问黄色、反政府等网站，导致病毒、木马泛滥
- ▶滥用公司打印机，造成资源浪费

禁止访问与工作无关的网页

限制用户访问与工作无关的网页，可通过网站分类库，分时段管控用户的网页浏览行为，并通过审计详细了解用户访问网站情况。

管控IM软件

禁止非工作相关的IM帐号登录，防止闲聊。

禁止游戏、股票等与工作无关的程序运行

禁止在工作时间使用游戏、股票等应用程序，并阻止一切有安全风险的程序运行。

流量管控，保证网络通畅

对企业中网络流量使用情况进行分析，及时发现流量滥用问题并进行有效限制，合理分配带宽，保证关键业务的正常运行。

限制软件安装和卸载

禁止员工安装与工作无关的应用程序，禁止卸载与工作相关的应用程序，确保终端应用程序的标准化避免软件版权纠纷。

提供软件中心服务

管理员可将软件上架到软件中心，员工可从软件中心下载安装软件，避免用户随意从互联网下载软件导致感染病毒的风险。

防止浪费打印资源

灵活控制打印权限，防止无需打印的人员滥用打印资源，并详细审计每次打印操作，统计资源使用情况。

IP-guard资产管理解决方案

让管理化繁为简，省时省力又省心

企业运维管理常见困扰：

- ▶软硬件资产无法确实掌握，人工盘点耗时耗力
- ▶硬件设备被私下挪用、窃取，造成财产损失
- ▶无法及时更新高危补丁，终端安全基线失守
- ▶终端频频发生故障，维护工作应接不暇
- ▶管理员与用户交互困难，运维难度大

杜绝漏洞修复延迟

自动检测计算机的补丁安装情况，根据需要及时更新。

实时了解IT资产情况

自动统计计算机的软硬件资产，及时更新软硬件变动情况。

远程协助

管理员申请远程连接到终端计算机的桌面，用户端同意后管理员可直接操作客户端电脑，进行远程协助或操作示范。

及时发现版权软件风险

统计终端版权软件的安装数量，与公司购买的授权数进行比对，及时发现侵犯软件版权的风险。

快速实现软件部署

支持通过控制台统一分发程序、分发文件和可执行文件，使软件派发和文件推送可以快速完成。

IP-guard敏感内容识别解决方案

高效识别敏感内容，精准化防泄密

企业防泄密常见难点：

- ▶无法准确发现和定位企业内部敏感文档的存放位置并加以保护
- ▶员工在工作中既需要对外交互信息，又要防止敏感内容泄露
- ▶员工不清楚文件是否为机密信息，导致无意间泄密
- ▶通过存储设备、网络盘、IM、邮件外传敏感内容，亟需进行更精准的管控

及时发现敏感内容

支持全盘扫描含敏感内容的文档，对发现的敏感文档进行加密保护或进行其他防泄密处理措施。

重要文档加密保护

支持对含敏感内容、标签、密级的文档进行加密保护，从源头保护重要机密数据的安全。

重要文档外传限制

通过存储设备、网络盘、网页、IM、邮件、打印传输文档时，可阻断含有敏感内容、标签、密级的文档传输，普通文档可以正常传输。

重要文档外传审计

记录通过存储设备、网络盘、网页、IM、邮件、打印外传含敏感内容、标签、密级文档的行为，并可报警、警告、备份和记录屏幕画面。

IP-guard远程办公解决方案

远程办公也安全，无惧任何场景

远程办公常见安全风险：

- ▶远程终端的安全基线偏低，容易给内网带来安全隐患
- ▶服务器的机密文档下载到远程终端的泄露风险
- ▶终端接入内网时权限过大，容易引发安全问题
- ▶用户随意外传机密文档而无法追溯
- ▶截屏、录屏、拍照导致文档内容泄露的风险

远程终端安全基线加固

当远程终端使用VPN接入企业内网时，VPN客户端检测终端是否安装了IP-guard客户端和杀毒软件，如不符合要求可拒绝其登录VPN，以此来强化远程终端的安全性。

文档加密保护

对从服务器下载到终端的文档自动加密保护，用户不能通过剪贴板、截屏、打印窃取文档内容，未经过授权外发加密文档，其他人员无法打开，确保加密文档安全。

限制用户权限

对通过VPN接入内网的终端进行权限管控，包括外接设备、移动存储的使用权限、打印权限、文档外传权限等，严格规范用户的计算机行为；还可以通过屏幕水印有效震慑拍照、截屏泄密的行为。

全面审计终端行为

审计远程终端接入内网后的操作行为，包括对文档操作、网页访问、邮件收发、应用程序运行、外设接入、打印文档、屏幕画面等进行审计，帮助企业及时发现风险以及对泄密行为进行有效追溯。

拍照行为检测

对通过VPN接入内网的终端进行手机拍照检测，当用户使用手机拍摄屏幕画面时，将采取遮蔽屏幕、锁定计算机或报警给管理员等保护措施。

IP-guard水印追溯解决方案

文档流转可追溯，泄密者无所遁形

文件追溯常见问题

- ▶机密文档被截图、拍照、打印出去，却无法追溯泄密者
- ▶文档在哪些终端流转过？最终文档是通过谁的电脑发送出去的

防止打印泄密

防止用户随意使用打印机，并可在打印文件上添加文字、图片、标记点或二维码，可通过纸质文件追溯泄密者。

震慑拍照泄密行为

支持在计算机屏幕或应用程序上显示水印，有效震慑通过拍照、截屏、录屏泄密的行为。

文档流转追踪

支持在文档中加入显式、隐式水印，或在文档中自动加入流转信息，以追踪文档在计算机上的流通情况。

文档标签

支持用户根据文档的重要程度打上标签和密级，再通过文档的标签密级进行外发管控或加密保护。

产品功能模块详细介绍

产品	模块	功能介绍
文档加密系统		**【透明加密 】** √ 重要文档从生成即强制加密，强力守护信息资产 √ 在授权环境中，文档能自动解密，不影响用户原有使用习惯 √ 在非授权环境中，加密文档无法正常打开和使用，严防文档泄露 √ 在使用加密文档时，可防止用户通过剪贴板、截屏、打印等方式窃取文档内容 √ 可自定义安全密钥，并能自由选择加密算法，安全性尽由用户掌握
		【智能加密】 √ 对于加密文档，编辑、保存后依然为加密文档，不改变文档的加密状态 √ 对于非加密文档，编辑、保存后仍然为非加密文档 √ 用户新产生的文档不会强制加密
		【只读加密】 √ 用户产生的文档不加密，只能以只读方式查看加密文档，无法对文档进行编辑和保存等操作 √ 在只读授权环境下，依然可以防止用户通过剪贴板、截屏、打印（包括虚拟打印）等方式窃取加密文档内容的行为
		【权限控制】 √ 文档制作者可设置加密文档的权限，如设定文档的访问者，及阅读、修改、复制、打印、截屏、有效期和解密等权限 √ 以公司组织架构为依托，可将加密文档划分不同的安全区域和级别，建立“分部门分级别”的保密机制，防止加密文档在企业内部扩散泄密 √ 用户可以调整加密文档的安全区域和密级，对重要文档可采取提高密级的方法防止普通用户访问 √ 部门间需要进行文档交互时，可通过修改加密文档的安全区域与级别实现
		【对外交互】 √ 可对需要外发的文档进行权限控制，防止二次泄密 √ 可指定特定的计算机才能打开并查看外发文档 √ 能够限制外发文档的查看期限、打开次数、打开密码、复制、编辑、打印、截屏、过期自动删除等权限 √ 支持外发USBkey功能，插入USBkey才能打开外发文档，不需要绑定计算机 √ 支持自定义外发模板，方便用户快速配置外发权限

产品	模块	功能介绍
文档加密系统		**【出差办公】** √ 针对人员出差，可对其授予离线权限，确保出差期间依然可正常使用加密文档，不影响日常办公 √ 可对出差人员设置个性化的离线权限，包括离线时长、加密软件类别、文档解密、外发等权限 √ 出差时可插入出差USBkey，可保证正常使用加密功能，也可以提升当前的加密权限 √ 出差时，在外部计算机上插入U盘加密客户端，可正常使用加密文件，拔出U盘加密客户端则不能打开加密文件
		【移动终端查看器】 √ 支持在手机、平板等终端安装查看器APP，可通过APP查看办公类加密文档，满足企业移动办公场景 √ 管理员可授权移动终端加密或解密权限，被授权的移动终端可以通过查看器APP加密或解密文档 √ 用户通过查看器APP查看文件时显示水印，有效震慑通过截屏或拍照泄密的行为 √ 可以设定查看器与服务器的认证间隔时间，规定查看器的使用期限，避免脱离管控
		【审批机制】 √ 支持单级、逐级、会签审批，满足多样化审批流程需求 √ 支持通过安全平台APP、web、控制台、即时通讯工具或OA等工具进行审批 √ 支持对解密申请、外发申请、安全属性变更申请和临时离线申请进行审批
		【灾备机制】 √ **双机热备** 通过主从服务器实现双机热备，在主服务器出现故障时，从服务器可完全接替主服务器的工作，确保审批流程正常，日志的收集及查看正常 √ **备用服务器** 部署一个或多个备用服务器，当主从服务器出现硬件故障时，备用服务器将自动接管加密客户端，确保客户端可以正常使用加密文件 √ **网络灾备** 预设容灾时间，当出现网络故障时，在容灾时间范围内，用户仍然能正常使用加密文件 √ **文档灾备** 可将终端加密文档备份到服务器，当出现文档损坏或丢失时，可从服务器中找回文档，避免文档损失
		【系统支持】 √ 支持Windows、Mac和Linux操作系统，实现跨平台管理 √ 加密文档可在Windows、Mac及Linux三个系统平台上正常使用，也支持通过智能手机（iOS/Android）预览加密文档，兼容性强
敏感内容识别系统		√ 支持通过关键字、正则表达式、文件名称、文件类型定义敏感内容 √ 支持对客户端进行全盘扫描，发现含有敏感内容的文档时，可进行加密保护、或导出扫描结果通知用户 √ 当含有敏感内容、标签或密级的文档通过移动存储、网络盘、Email、IM、网页外传时，可阻断其外传行为 √ 当含敏感内容、标签或密级的文档外传时，可进行报警、警告、审计、备份和记录屏幕等审计措施

产品	模块	功能介绍
终端安全管理系统	文档操作管控	√ 文档操作审计，可记录核心资料流通情况 √ 文档操作控制，管理用户使用文档的权限 √ 对通过U盘、智能手机等设备传送文件，进行操作记录 √ 支持记录刻录操作日志，可备份刻录的文件副本 √ 在重要文档被复制、篡改或删除前备份，防止文档损坏和丢失
	文档打印管控	√ 打印行为审计，实现泄密追溯 √ 打印内容备份，支持以图片或文本格式备份打印内容 √ 打印权限控制，节省打印成本防止泄密 √ 打印浮水印，可显示标记点、文字水印、图片水印、二维码水印或点阵水印 √ 用户可申请临时放开打印权限，或申请临时取消打印水印，也可以通过自我备案开放权限
	设备管控	√ 存储设备管理，防止内部信息外泄 √ 通讯设备管理，避免非法外联带来风险 √ 音视设备管理，避免工作时间分散注意力 √ 新设备管理，规范企业的外设使用 √ 支持控制智能手机、5G上网卡、随身wifi以及刻录机等几乎所有外设 √ 用户可申请审批流程临时放开指定设备的使用权限，也可以通过自我备案开放设备的使用权限
	移动存储管控	√ 移动存储审计，记录设备插拔及拷贝的详细信息 √ 移动存储注册，确保外来U盘无法随意接入企业内网 √ 移动存储授权，指定U盘使用范围 √ 移动存储加密，加密盘只能在企业内部使用 √ 用户可以通过申请读、写U盘，也可以通过自我备案开放权限
	即时通讯管控	√ 支持管控主流即时通讯工具，防止有意无意泄密 √ 备份外发文档和图片，审计更全面 √ 文档外发控制，控制机密文件传输 √ 截图外发控制，防止截图泄密
	邮件管控	√ 邮件记录，便于企业对邮件的安全使用情况进行审计 √ 邮件发送控制，防止企业的重要信息通过邮件泄露 √ 支持对Lotus、Exchange、标准协议、网页邮件进行审计 √ 发送邮件时，可要求必须抄送给相应的管理者才能正常发送 √ 支持自动备份邮件附件
	网页浏览管控	√ 网页浏览统计，详细掌握用户浏览网页的时长 √ 网页浏览审计，详细记录网页浏览信息 √ 网页浏览控制，禁止访问非法网站带来的安全风险和工作效率损失 √ 用图表的方式展现统计结果，各种数据一目了然 √ 支持包含IE、Edge、Firefox、Chrome等主流浏览器 √ 可禁止通过http(s)、FTP、TCP协议的上传文件的行为

产品	模块	功能介绍
终端安全管理系统	网络控制	√ 通过网络通讯控制，避免随意的信息交流带来的风险 √ 可以控制企业内部每台计算机之间的网络通信 √ 支持禁止Office、WPS同步文档到云盘的泄密风险 √ 终端安全检测不通过时，可断开终端网络，防止安全基线过低的终端接入内网 √ 可检测到外来接入内网的计算机，可禁止其访问企业的计算机
	网络流量管控	√ 流量统计，随时了解流量的使用情况 √ 流量控制，保证关键业务流量充足 √ 以图表形式输出流量统计结果，清晰明了 √ 支持根据端口、地址范围分时段限制计算机的网络流量 √ 可以有效控制企业任何一台计算机的网络流量
	应用程序管控	√ 应用程序控制，防止非法程序运行 √ 自动收集应用程序的特征信息，进程改名依然无法逃避管控 √ 允许管理者对不同种类的程序进行分时段管理，让管理更加人性化 √ 支持限制软件安装权限，可禁止黑名单软件安装 √ 支持限制软件卸载权限，可禁止必备软件卸载 √ 软件安装卸载管理，使应用程序趋于标准化，避免版权纠纷 √ 应用程序统计，全面掌握应用程序使用时长 √ 用图表的方式展现统计结果，应用程序使用情况一目了然
	软件中心	√ 管理员可通过软件中心上架软件，确保软件安装包的来源权威可信 √ 可限制用户的软件下载权限，防止版权软件被随意安装，避免版权纠纷 √ 用户可通过软件中心下载、安装、升级、卸载软件，提高用户满意度 √ 支持http、P2P两种软件分发模式，提高分发效率 √ 审计管理员的操作行为，包括：登录软件中心、上架软件、发布软件、下架软件、注销、退出等行为
	文档标签	√ 支持对文档（Office、PDF、图片）定义标签，可按内容分为技术文档、销售合同，也可以按部门分为研发文档、财务文档 √ 支持按照密级定义文档，如从低到高分为公开、内部、秘密、机密、绝密 √ 支持通过文档的敏感内容实现自动打标签和定义密级 √ 支持用户通过右键手动设置文档密级 √ 支持依据文档标签和密级，限制文档通过移动盘、网络盘、IM、Email、网页、打印等方式传输出去 √ 支持依据文档标签和密级对文档进行加密保护 √ 记录添加标签和密级的日志，可通过文档编号、标签、密级实现泄密追溯
	水印及追溯	√ 支持在计算机的屏幕上显示图片水印、文字水印、二维码水印和点阵水印，可有效震慑拍照和截屏泄密行为 √ 支持在打印的纸张上呈现文字水印、图片水印、标记点、二维码水印和点阵水印，以申明文档的出处或版权信息 √ 支持在文档中加入显式水印或隐式水印，水印将跟随文档一直存在，显式水印震慑效果更佳，隐式水印追溯效果更好 √ 支持在用户外传文档时加入流转信息，以记录文档在各个计算机节点上的流通情况，方便日后审计和追溯 √ 支持手动对Office、WPS、PDF、图像文件添加水印，也支持手动去除水印 √ 支持记录文档添加水印、流转信息的日志

产品	模块	功能介绍
终端安全管理系统	屏幕监视	√ 屏幕查看，了解用户的工作状态 √ 屏幕记录，便于随时查看屏幕历史 √ 高危行为记录，当用户通过邮件、IM、网页、打印、拷贝等进行文件传送时，支持记录行为发生时的屏幕画面 √ 采用增量、变频等技术，屏幕记录数据量业内最小 √ 对特定的程序进行记录，并且支持自定义记录频率 √ 可将屏幕历史转换为视频格式，更方便查阅
	资产管理	√ 资产管理，收集计算机软硬件信息及变更情况 √ 版权管理，了解计算机安装版权软件的数量 √ 可以自定义生成软硬件资产统计报表 √ 自动收集网内计算机的补丁安装情况，并可集中管理和安装补丁 √ 支持通过P2P分发软件或补丁，部署效率更高 √ 软件管理，可查看终端软件安装列表，支持批量卸载软件 √ 支持对打印机、路由器等非IT资产进行自定义管理
	远程维护	√ 管理员申请远程终端计算机，经用户同意后管理员可操作客户端电脑，进行远程协助或操作示范 √ 支持远程文件传送 √ 可查看客户端计算机安装的所有软件信息，可远程卸载软件 √ 支持查看客户端计算机的运行状态信息
	风险审计报表	√ 通过统计表、趋势表、征兆表发现用户行为变化趋势及泄密风险 √ 重点监控版权软件的安装数量和使用数量，可设置版权软件授权数，快速发现安装数超过授权数的风险 √ 通过饼状图呈现外传文件类型的百分比或外传文件途径的百分比 √ 支持通过样本数和标准差等统计学方法，发现外传文件较多的用户 √ 统计时段内风险人员的数量及风险事件的数量，支持以趋势图的方式呈现风险事件
	文档云备份	√ 自动对终端文档进行备份，支持即时备份和定时备份 √ 可设置备份文档类型、排除文件、备份文件大小、备份间隔、备份流量、备份日期和时段等条件 √ 支持设置保留多个历史副本 √ 支持按公司组织架构列表查看备份库，备份文档以终端实际盘符目录的形式呈现 √ 支持用户检索备份文档，可设置不同用户对备份文档的查看、下载和删除权限
	基本功能（必选）	√ 统计计算机的基本信息和策略总览 √ 支持限制计算机的系统设置功能，比如：控制面板、网络属性、注册表等 √ 支持对终端计算机进行锁定、注销、重启、关闭等操作 √ 支持对计算机的安全基线进行检查，包括杀毒软件检查、软件安装检查、程序运行检查、系统服务检查、补丁检查、域用户身份检查等 √ 支持角色管理、支持用户系统、支持与AD域、LDAP用户系统实现同步 √ 支持按用户或计算机两种方式进行管理 √ 支持多国语言
视觉感知		√ 支持实时检测手机拍摄计算机屏幕的行为，识别速度及精度均高于业内领先的AI模型 √ 用户违规拍摄计算机屏幕时，可自动遮蔽屏幕、锁定计算机或报警给管理员 √ 支持从松到紧三种解锁屏幕方式，无拍照自动解锁、手动点击解锁、人脸解锁 √ 支持记录拍摄计算机屏幕的日志，可通过日志查看拍照人和屏幕画面

产品	模块	功能介绍
文档安全交换系统		√ 搭建隔离网络间的文档共享及内外网文档外发的管控平台 √ 用户提交文档交换申请，可通过安全平台APP、即时通讯工具、业务系统进行审批 √ 集成加解密接口，确保上传下载时自动加解密，实现明文区与密文区的无障碍交互 √ 通过系统交换文档时，含敏感内容需由领导审批，不含敏感信息则自动审批通过 √ 系统将完整记录文档交换行为、审批操作及系统操作日志，以便于泄密事件的溯源
安全桌面		√ 通过沙盒技术将普通桌面和安全桌面进行隔离，保护安全桌面中的敏感数据 √ 无需重启计算机即可在两个桌面之间自由切换，兼顾安全性与办公的便捷性 √ 支持安全桌面窗口模式，可在普通桌面直接访问安全桌面中的文件和应用系统 √ 涉密程序限制在安全桌面中运行，防止核心数据外泄 √ 为安全桌面开设专属的网络共享目录，满足文件传输需求 √ 安全桌面默认禁止访问任何网络，可根据需要开通访问重要应用系统 √ 安全桌面默认禁止连接外设和打印机，可根据需要放开外设和打印机的使用权限 √ 安全桌面支持导入、导出文件管控，保证核心数据安全 √ 支持记录安全桌面登入、登出，文件导入、导出的日志
安全网关	硬件网关	√ 服务器文档下载加密：服务器数据下载到终端自动加密，防止服务器数据下载泄密 √ 加密文档上传解密：终端的文档上传到服务器时自动解密，服务器以明文存储，确保良好的兼容性 √ 杜绝非法计算机和非法程序对服务器进行访问，有效保障服务器的明文文件的安全 √ 支持串联、旁路两种部署方式 √ 支持企业常用信息管理系统OA、PLM、SVN、ERP等 √ 支持B/S、C/S两种服务器访问方式 √ 采用高强度的通讯加密技术
	软件网关	√ 适用于云服务器的保护，对不方便架设硬件网关的传统物理服务器，也可通过软件网关进行保护 √ 杜绝非法计算机和未授权程序访问服务器，保障服务器的访问安全 √ 服务器文档下载到终端自动加密，防止服务器文档下载泄密 √ 终端文档上传到服务器自动解密，服务器以明文存储，确保良好的兼容性 √ 支持企业常用的各类应用系统OA、PLM、SVN、ERP等 √ 支持B/S、C/S两种服务器访问方式 √ 采用高强度的通讯加密技术 √ 可用于保护Linux服务器，也可以通过反向代理保护其他操作系统的服务器
准入网关		√ 计算机访问服务器或互联网时，需要经过准入网关的严格审核，只有合法的计算机才能访问受保护的资源，非法计算机将被引导至隔离区进行修复，或完全阻断其访问 √ 支持对终端计算机进行安全状态检查，满足条件则允许接入网络，否则拒绝访问并发出警告提示，并强制跳转至隔离区进行修复 √ 对于临时来访的外来计算机，可以建立访客账号，通过Web浏览器输入账号密码进行身份认证，验证通过后，可访问受保护的资源 √ 防止计算机通过重装系统、安装多系统、虚拟机等方式脱离管控 √ 支持串联、旁路和镜像三种部署方式 √ 支持Bypass容灾机制
安全U盘		√ 密码保护，U盘读写，需要密码认证才能使用安全U盘 √ 详细记录，U盘的使用和U盘文档操作的记录 √ 使用专属的资源管理器，可有效防范木马病毒 √ 区分保密区和交互区，通过内外分区，确保U盘使用安全 √ 采用芯片级保护，有效防止非授权的U盘格式化