IP-guard三维智能信息防泄露解决方案

1 企业内网安全现状

2 三维智能信息防泄漏解决方案

3 IP-guard方案优势

4 案例分享

5 溢信科技简介

近年各种泄密事件频发

招商银行
3.15曝光银行内部员工
兜售用户信息

三星电子
员工离职泄露公司
研发核心机密

东软集团
企业高管利用U盘窃取
公司商业机密

1号店
内部员工与外部勾结
泄露90万用户信息

苹果
前任资深管理人员受贿泄密
被判罚金和监禁

富士康
iPAD 2平板后壳3D数据图
遭“内鬼”泄密

HTC
副总兼首席设计师窃取
公司UI接口程序商业机密

海尔
前高管跳槽通过邮件泄露
海尔洗衣机重要生产数据

摩根士丹利
员工非法窃取35万客户信息
遭开除

数据泄露会对企业造成哪些影响？

风险巨大

企业内部泄密渠道防不胜防

邮件 打印机 QQ 网盘 智能手机 U盘 未知渠道

企业人员导致的风险

接入内网访问，引起泄密

外来人员
(客户/合作伙伴)

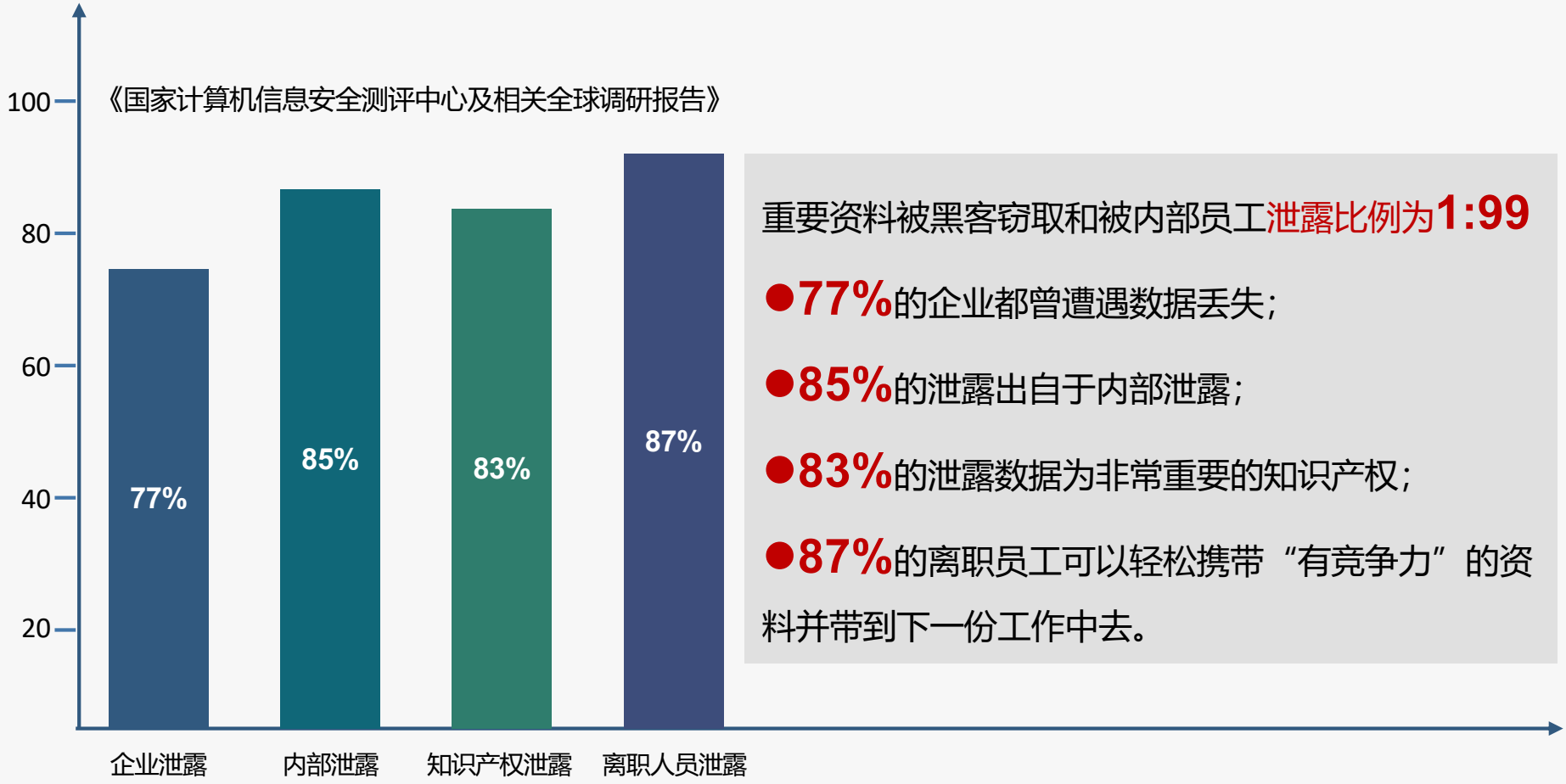
对企业机密信息缺乏有效保护

内部人员
(研发/设计/财务)

离职前拷走大量有价值机密文件

离职人员

国家信息安全测评中心调查报告



重要资料被黑客窃取和被内部员工泄露比例为**1:99**

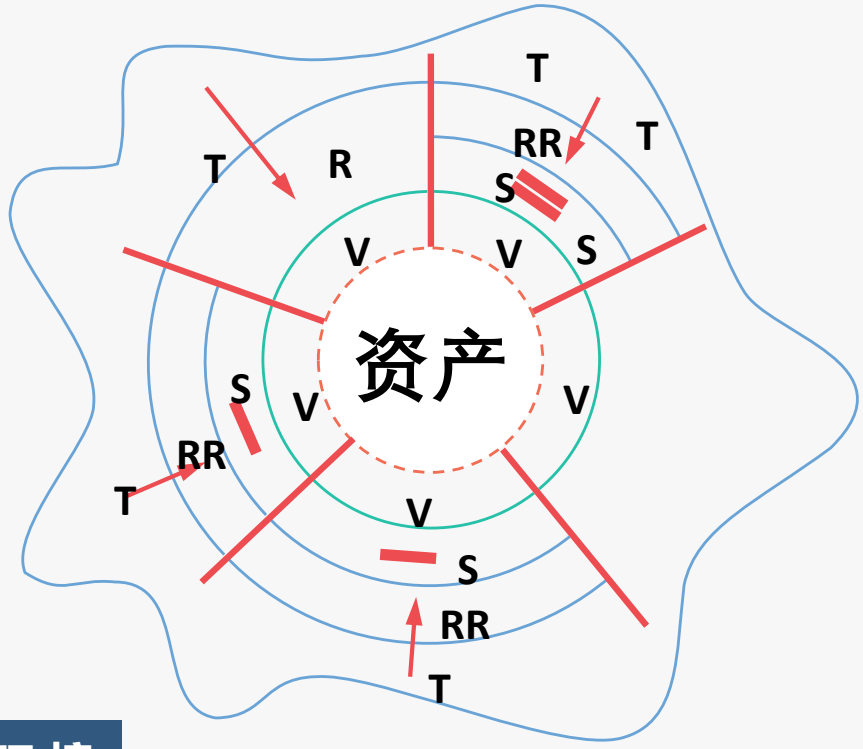
- **77%**的企业都曾遭遇数据丢失；
- **85%**的泄露出自于内部泄露；
- **83%**的泄露数据为非常重要的知识产权；
- **87%**的离职员工可以轻松携带“有竞争力”的资料并带到下一份工作中去。

目录

国标安全理论示意图

GB/T 19715.1-2005/ISO/IEC TR 13335-1:1996

安全要素关系图



图标符号：

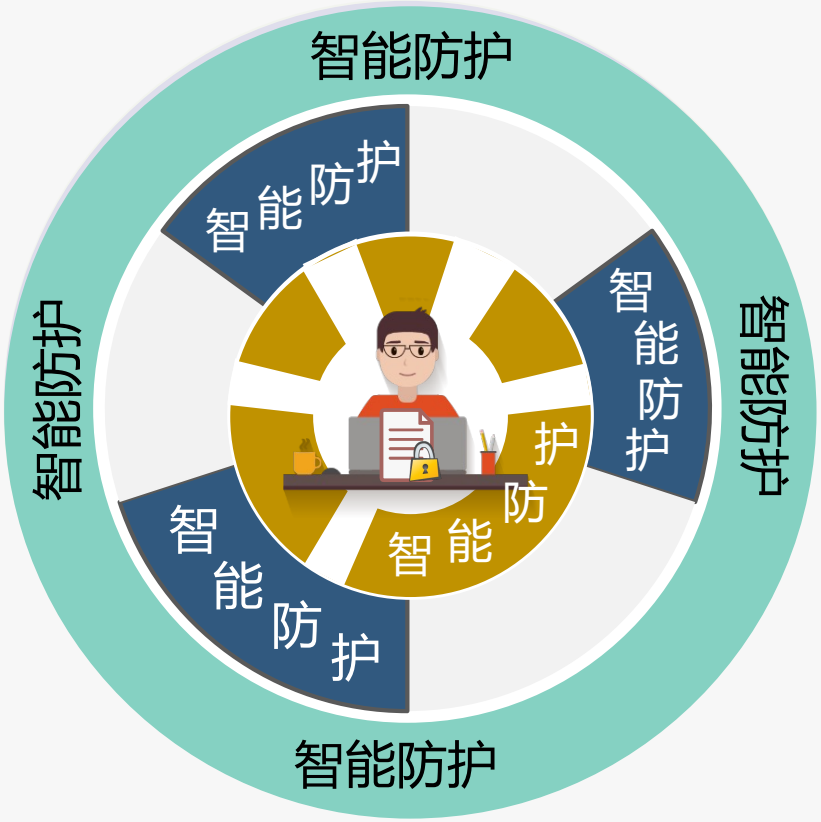
T—威胁　R—风险　RR—残留风险

S—防护措施　V—脆弱性

安全的核心是保护“资产”

- ✓ 风险是多样化的
- ✓ 单一的方法不能有效全部解决
- ✓ 需要多样化、整体性的防护

IP-guard三维智能信息防泄露体系



维度一：事前防护 文档透明加密

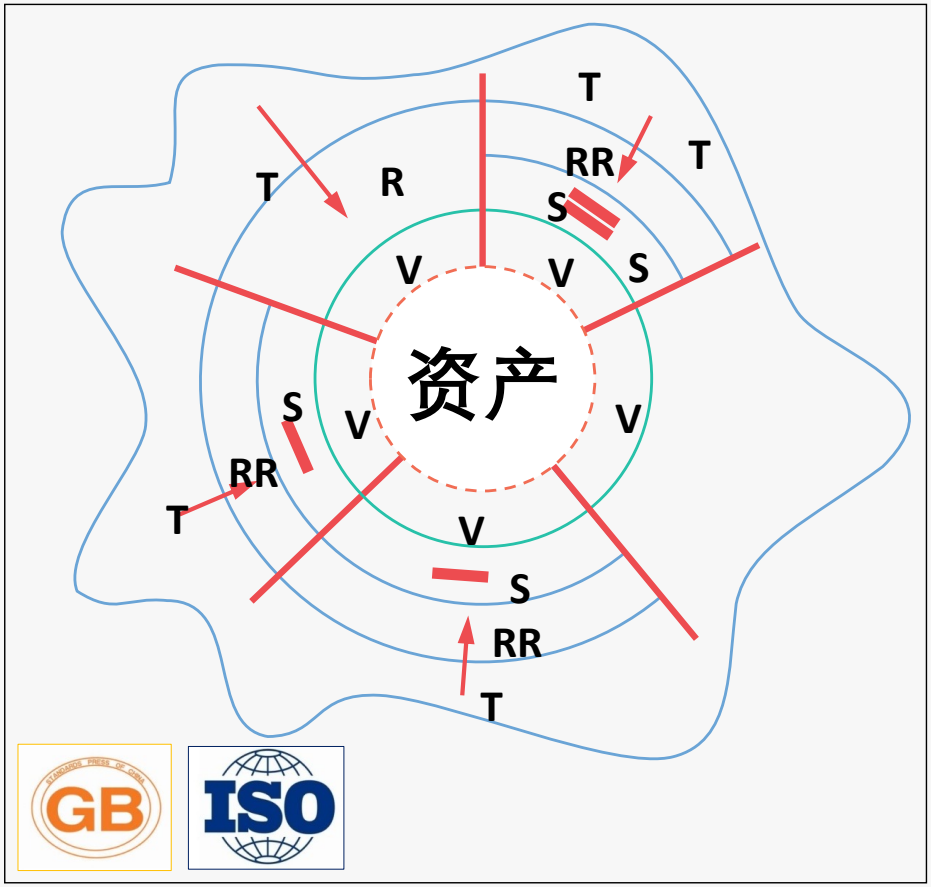
维度二：事中控制 流通渠道管控

维度三：事后审计 内容级行为审计

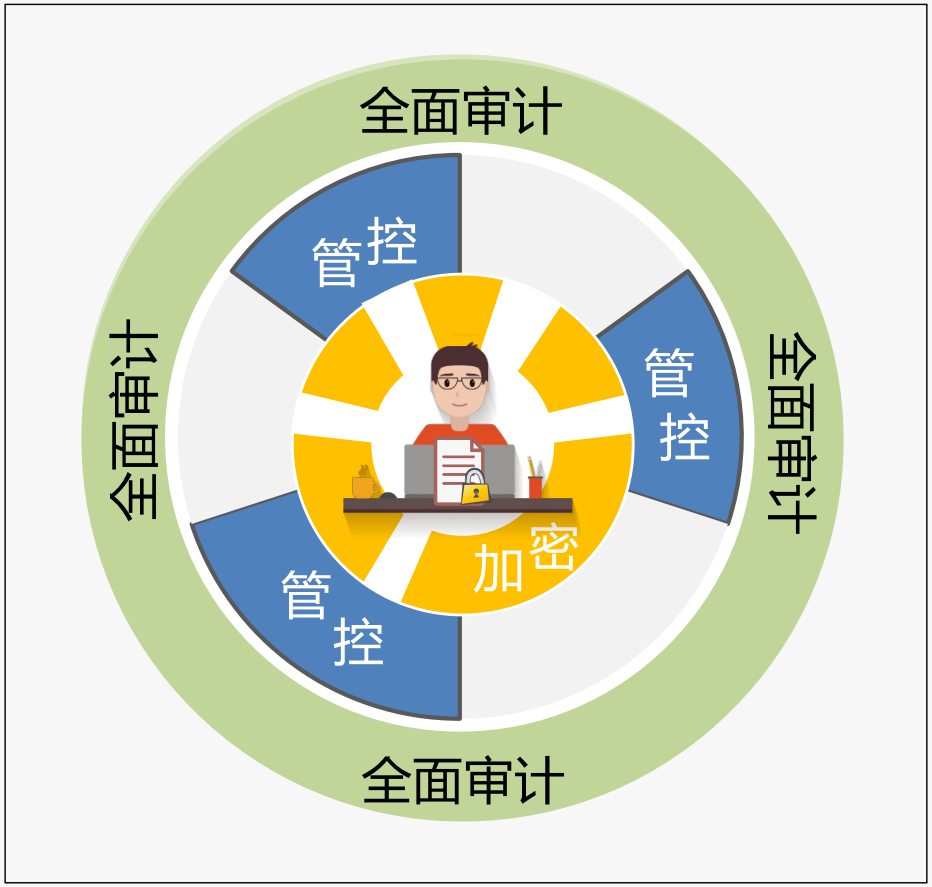
智能防护：基于敏感内容的主动防护

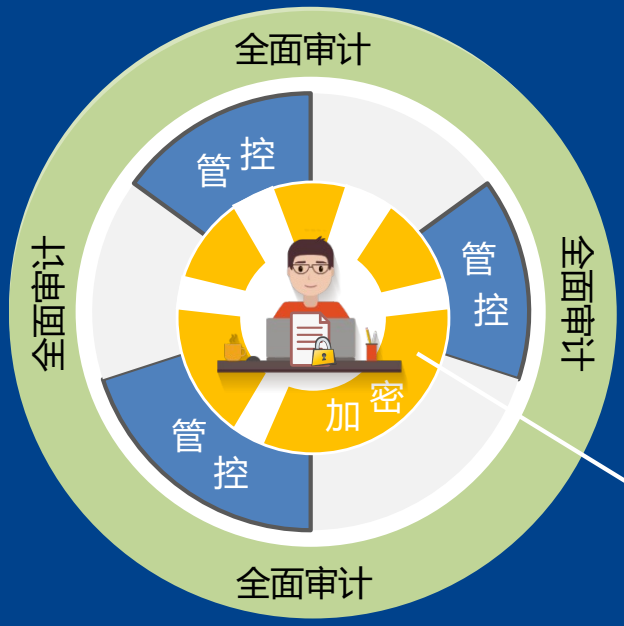
全面吻合安全理论模型

国标安全理论示意图



IP-guard三维智能信息防泄露

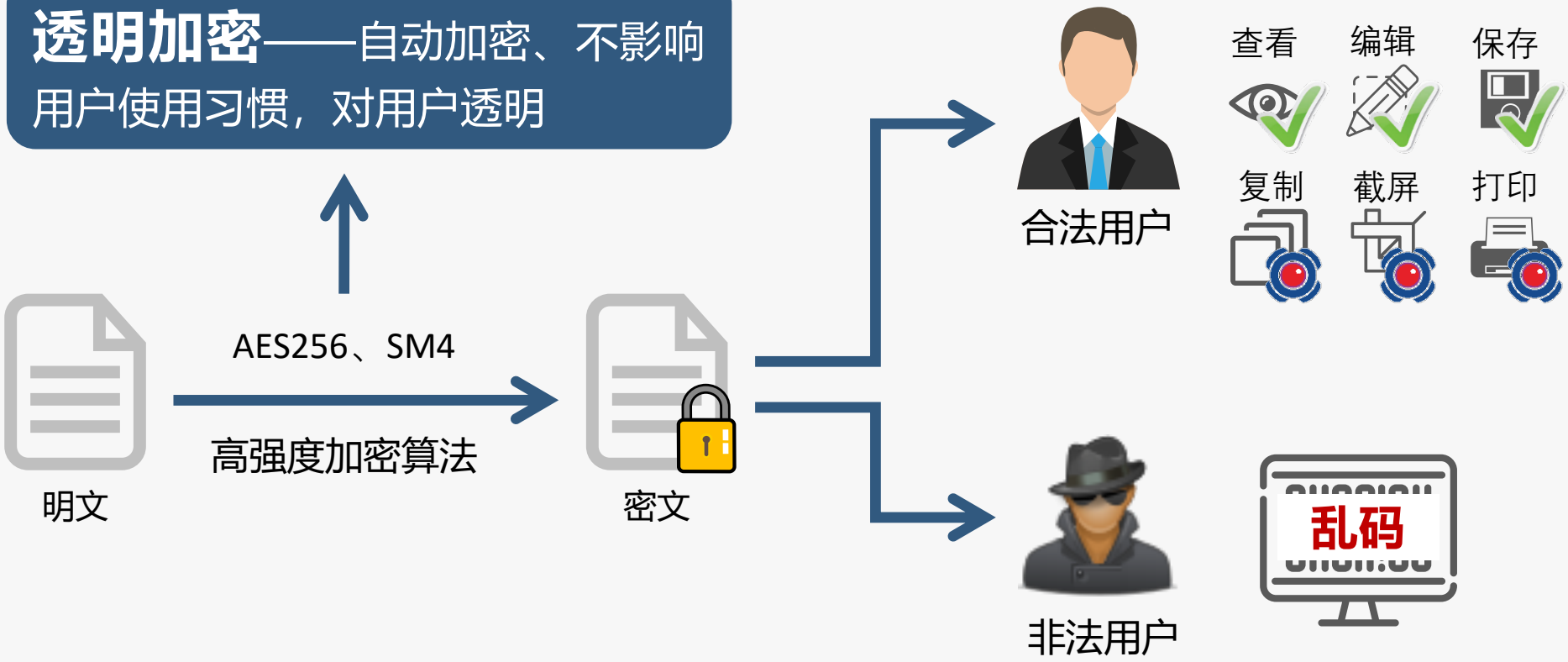




维度一：事前防护
文档透明加密

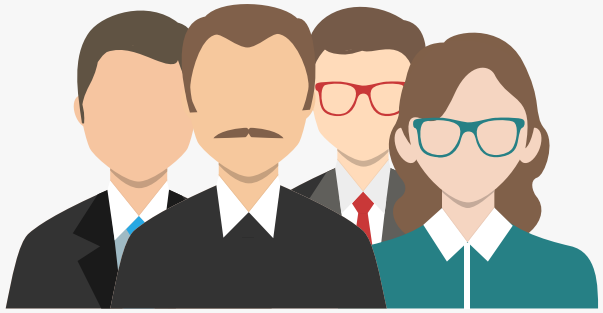
文档透明加密

透明加密——自动加密、不影响用户使用习惯，对用户透明



文档加密方案需要考虑的因素?

用户分类



不同类型的用户，采用不同的加密模式。

开发人员

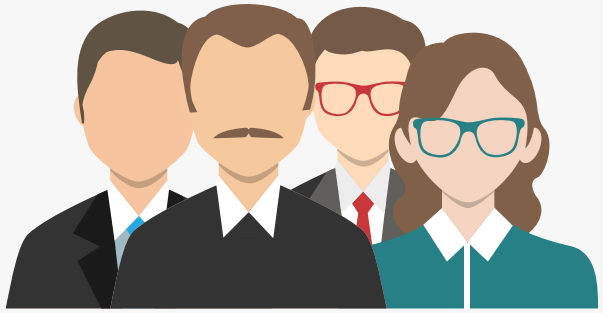
强制加密

明文

编辑、保存

密文

用户分类



不同类型的用户，采用不同的加密模式。

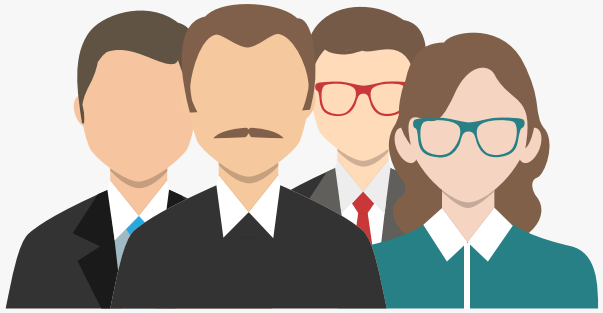
管理人员

智能加密

明文 —— 编辑、保存 ——→ 明文

密文 —— 编辑、保存 ——→ 密文

用户分类



不同类型的用户，采用不同的加密模式。

企业老板

VIP模式

密文

只解密不加密

编辑、保存

明文

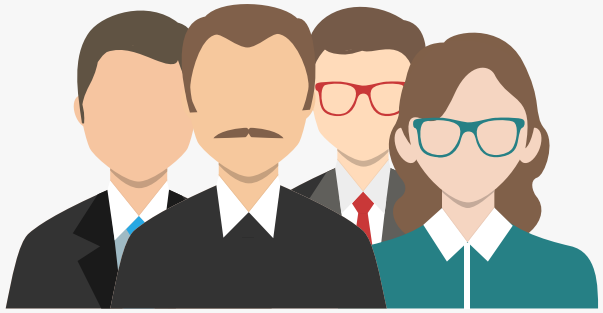
明文

自主选择加密

右键加密

密文

用户分类



不同类型的用户，采用不同的加密模式。

生产/文员

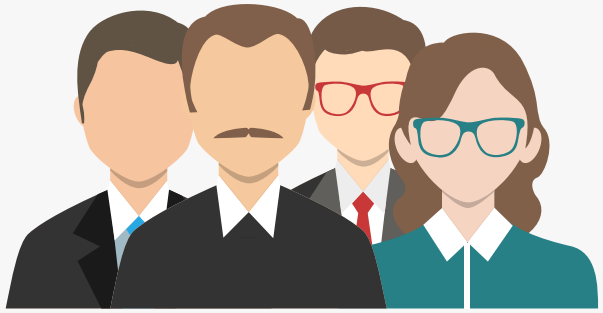
只读加密

密文

内部使用

只能读取 不可编辑

用户分类



不同类型的用户，采用不同的加密模式。

开发人员

强制加密

明文 → 编辑、保存 → 密文

管理人员

智能加密

明文 → 编辑、保存 → 明文

密文 → 编辑、保存 → 密文

企业老板

VIP模式

密文 → 只解密不加密 / 编辑、保存 → 明文

明文 → 自主选择加密 / 右键加密 → 密文

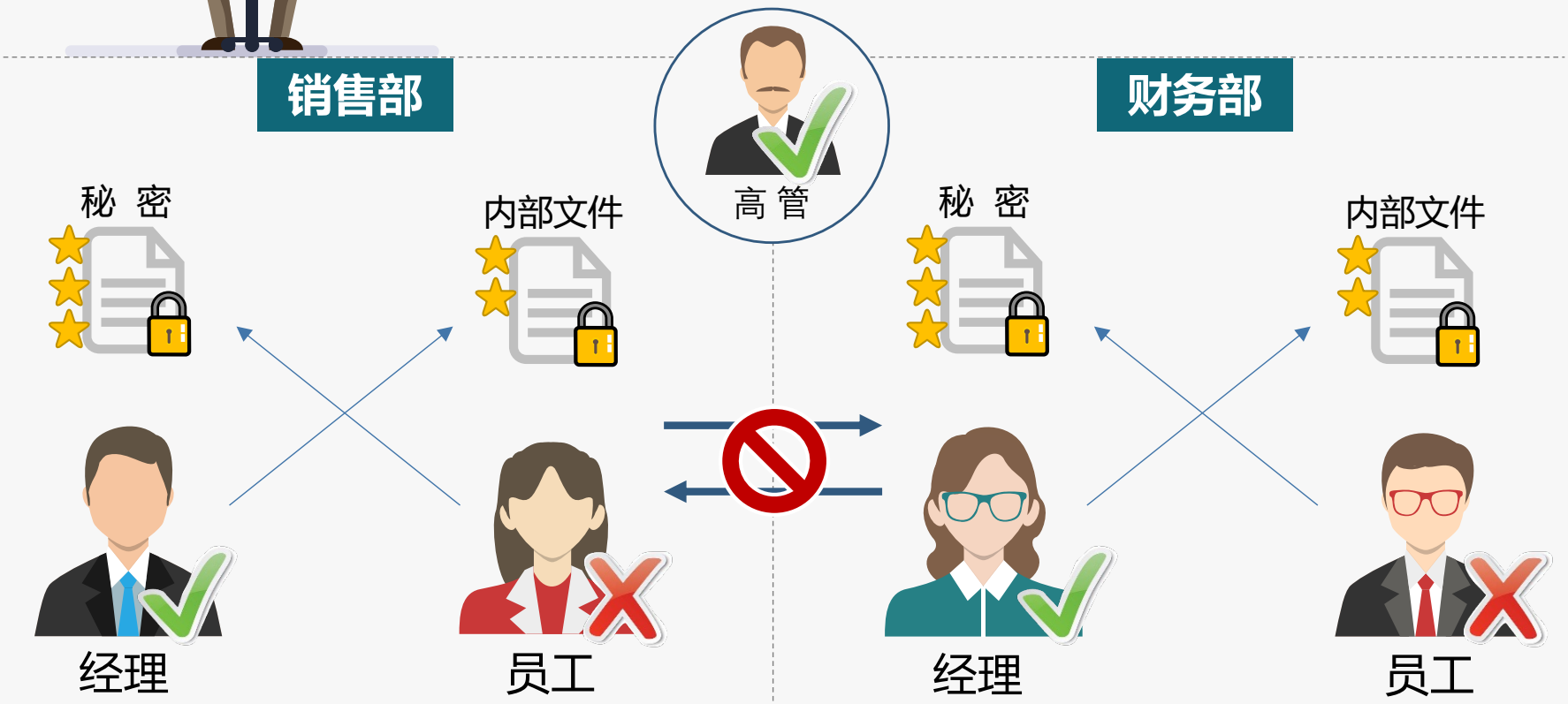
生产/文员

只读加密

密文 → 内部使用 → 只能读取 不可编辑

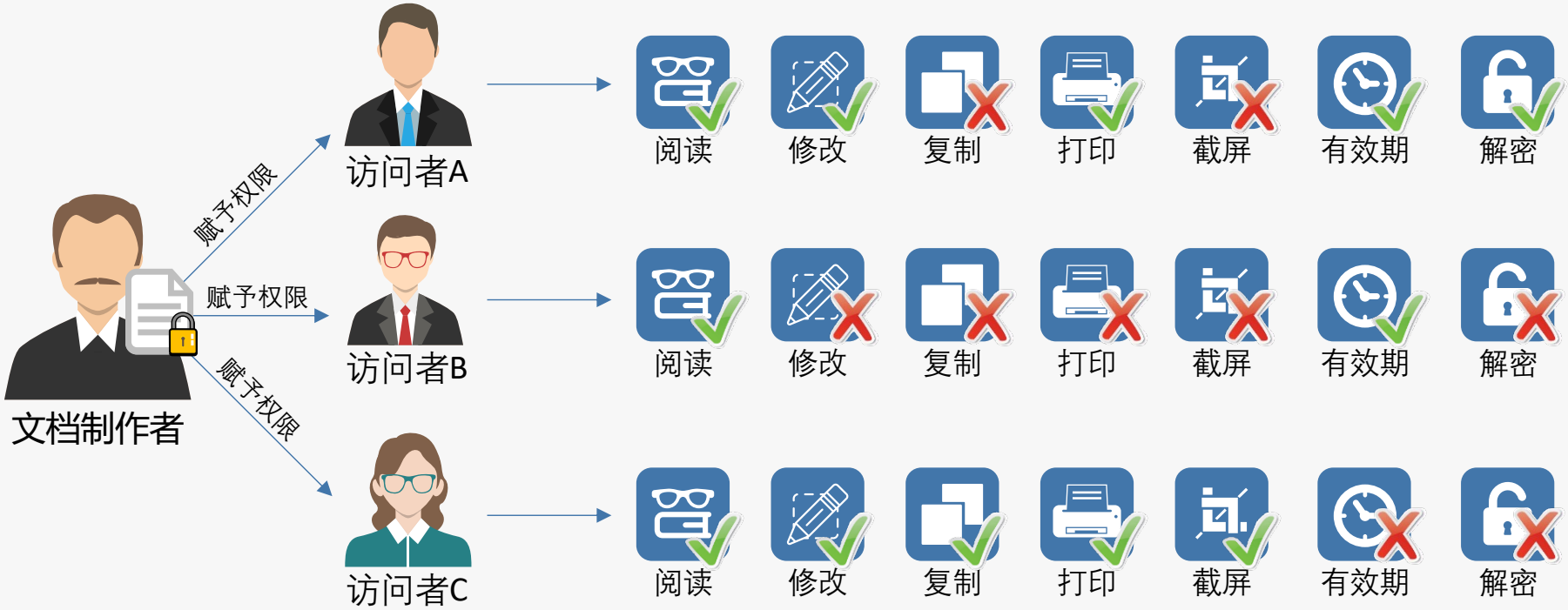
权限管理

部门/上下级/管理者的权限管理

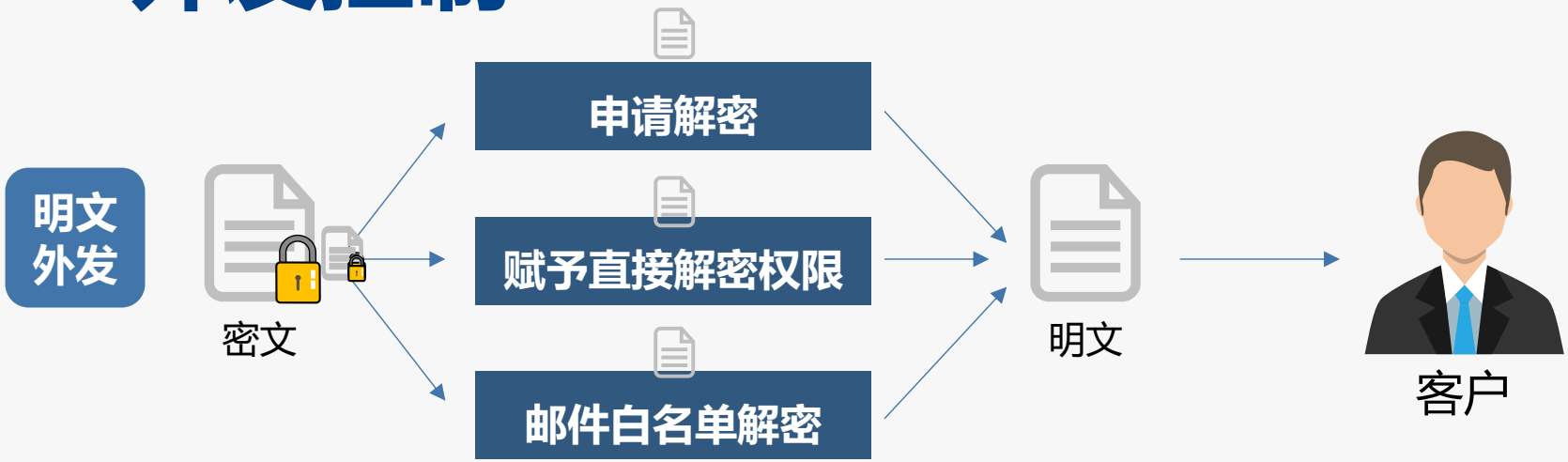


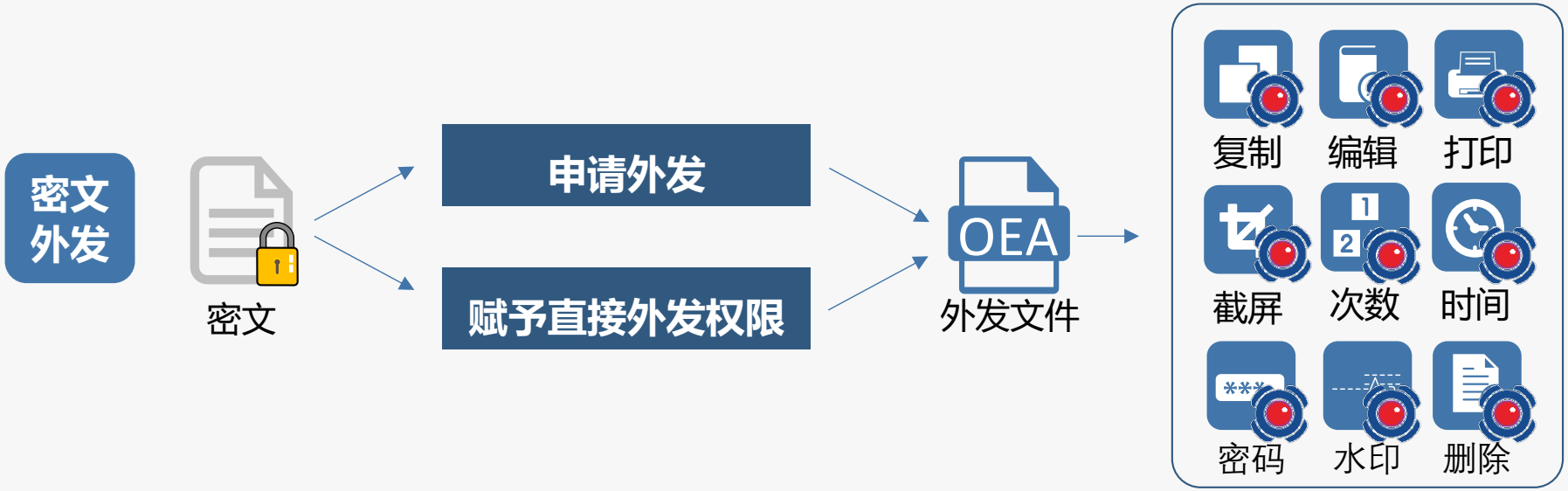
加密文档权限

自主设定文档权限
文档制作者可以自主设定查看者权限



外发控制


明文外发
密文
申请解密
赋予直接解密权限
邮件白名单解密
明文
客户


密文外发
密文
申请外发
赋予直接外发权限
OEA
外发文件
复制
编辑
打印
截屏
次数
时间
密码
水印
删除

审批灵活

申请类型丰富

- 解密申请
- 外发申请
- 安全属性变更申请
- 计算机离线申请

流程多样化

- 单级审批
- 多级审批
- 会签审批
- OA/ERP审批接口

实现方式灵活


控制台审批


代理审批


Web审批

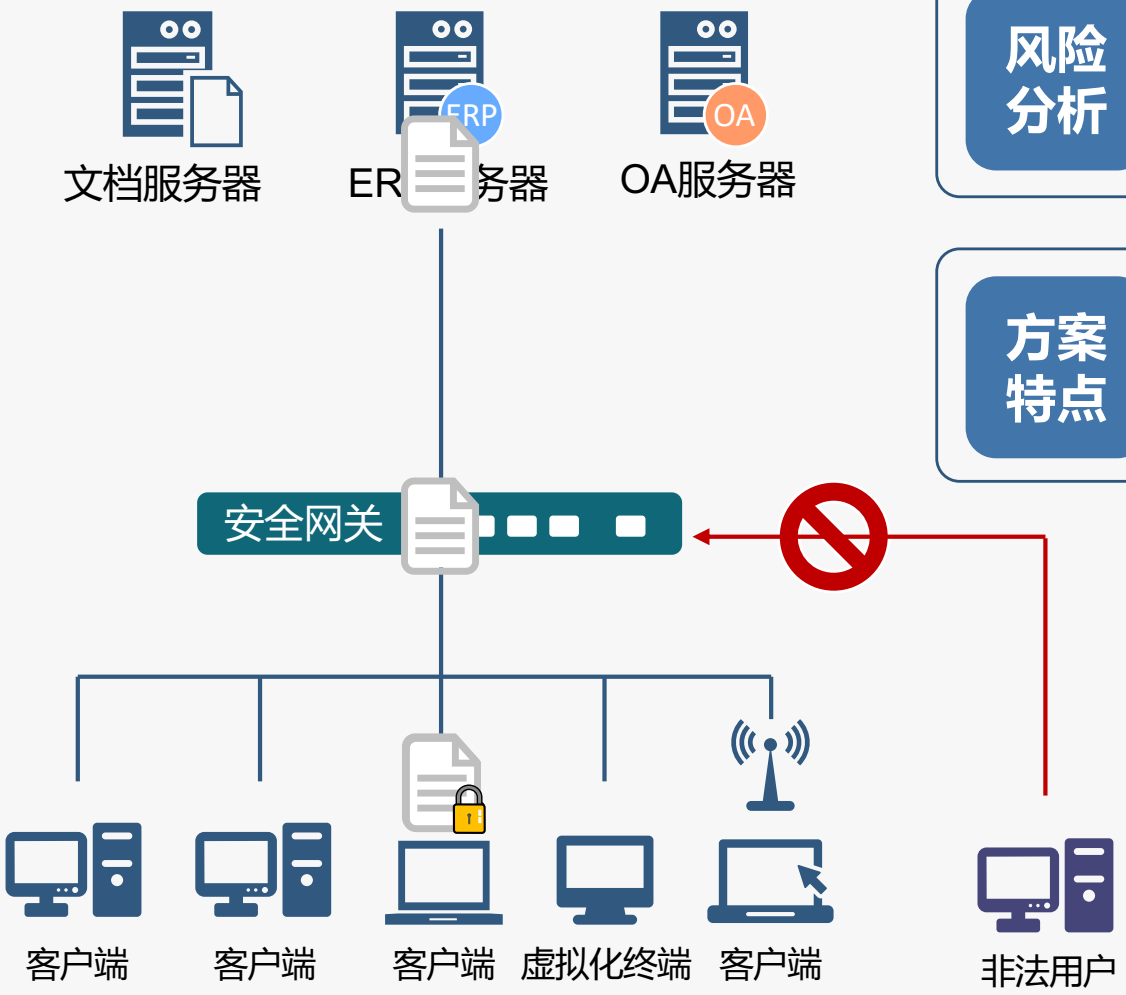

APP审批

- **Web审批：**支持文件预览、下载功能，支持手机、PAD、计算机的浏览器进行审批。
- **APP审批：**支持IOS、Android平台，支持文件预览。

出差管理

离线申请	临时离线/长期离线	正常使用/安全密码登录
紧急出差	授权申请	生成授权码使用
使用非公司电脑	授权申请	U盘客户端
离线后权限不足	授权申请	USBkey或授权码

服务器文档下载保护



风险分析

① 合法用户**下载**泄密

② 盗用账号登录下载泄密

方案特点

① 实现“**上传解密、下载加密**”

② 服务器、终端操作不变

兼容性与可靠性

跨平台支持

兼容五大常用操作系统

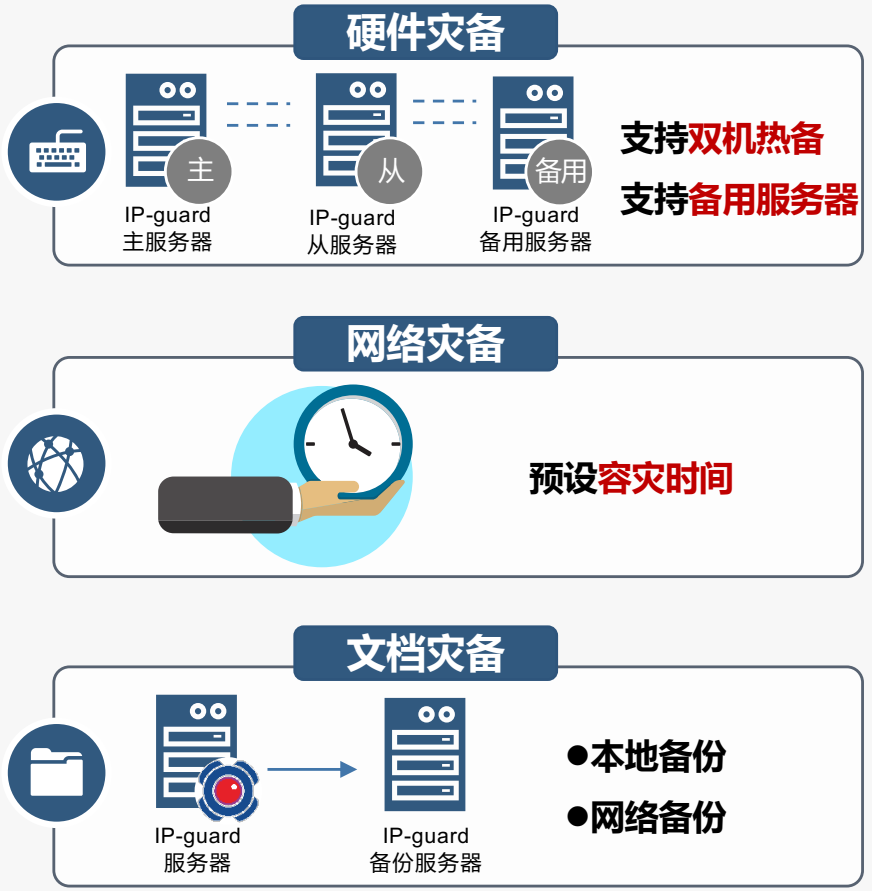
Windows　Mac　Linux

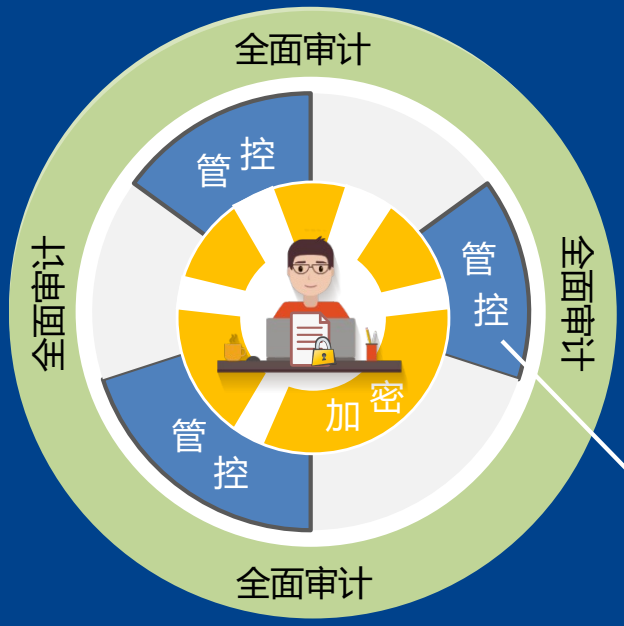
iOS ios　Android

优势

1. 支持对在Mac、Linux上产生的机密文件进行加密保护
2. 支持在五大平台之间传阅和使用加密文件，沟通更高效

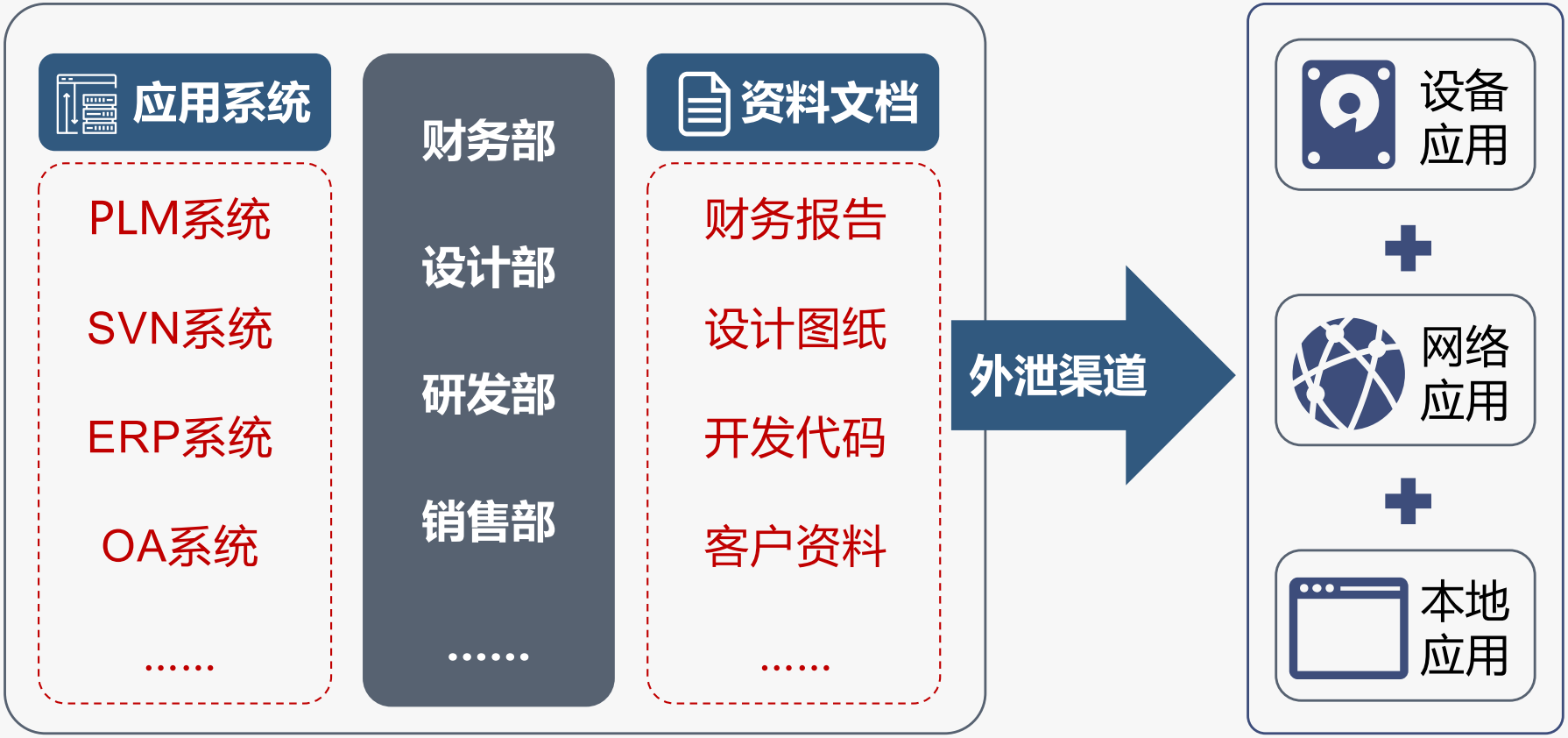
可靠灾备机制



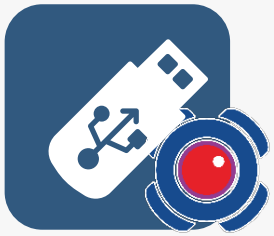


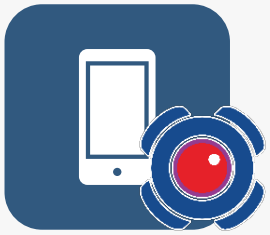
维度二：事中控制
流通渠道管控

内部信息泄密渠道分析


应用系统
PLM系统
SVN系统
ERP系统
OA系统
……
财务部
设计部
研发部
销售部
……
资料文档
财务报告
设计图纸
开发代码
客户资料
……
外泄渠道
设备应用
网络应用
本地应用

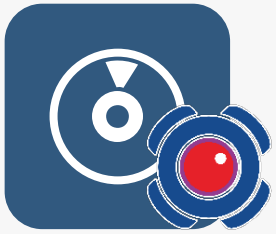
设备应用管控

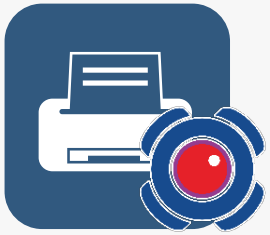

移动存储

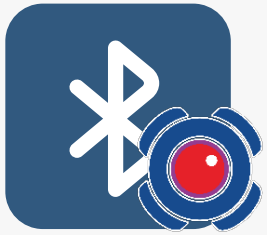

智能手机

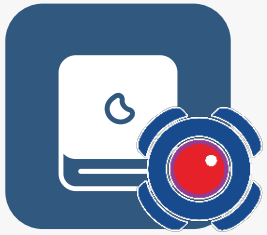

无线网卡

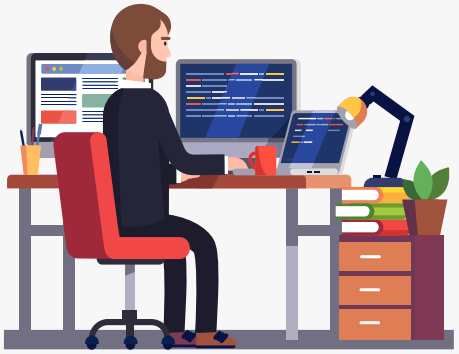

随身wifi


刻录机


打印机


蓝牙

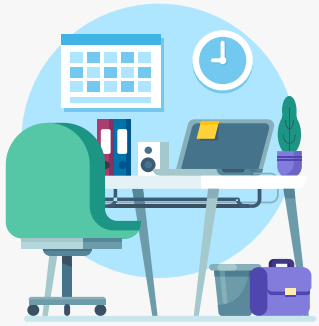

未知设备



主要优势：细颗粒的分类与控制

- ✓ 支持对38类外接设备进行细化控制
- ✓ 可允许放行网银U盾或身份验证USBKEY
- ✓ 对智能手机的多种接入方式进行管控
- ✓ 用户可自主申请开放某类设备的使用

移动存储管控



清晰分类

杜绝外来U盘随意接入
按部门分类移动存储
按人员分类移动存储

授权灵活

限制U盘的读、写权限
限制U盘的使用范围
灵活开放U盘权限

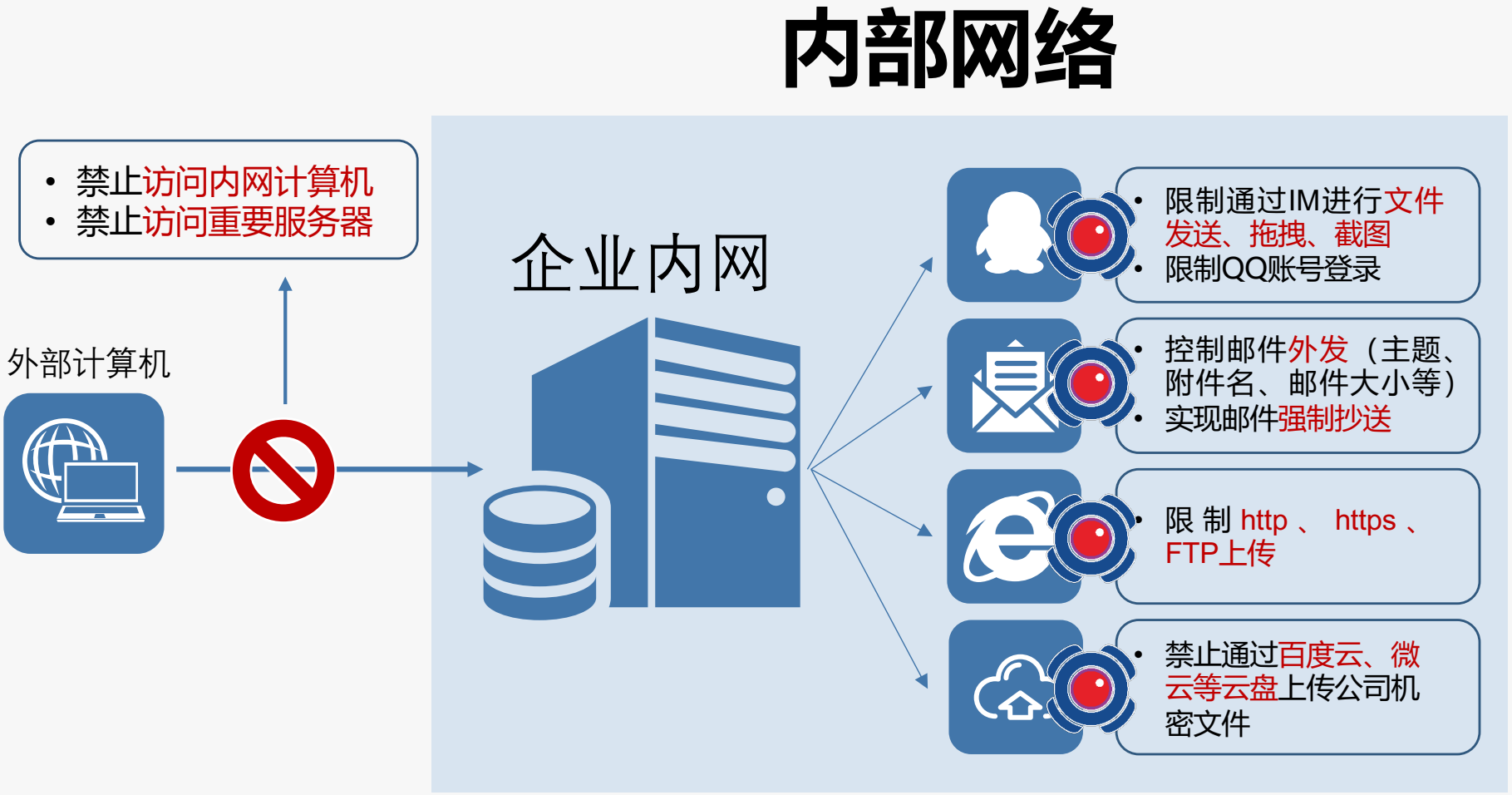
加密保护

仅限内部可使用加密盘
文档拷入U盘自动加密

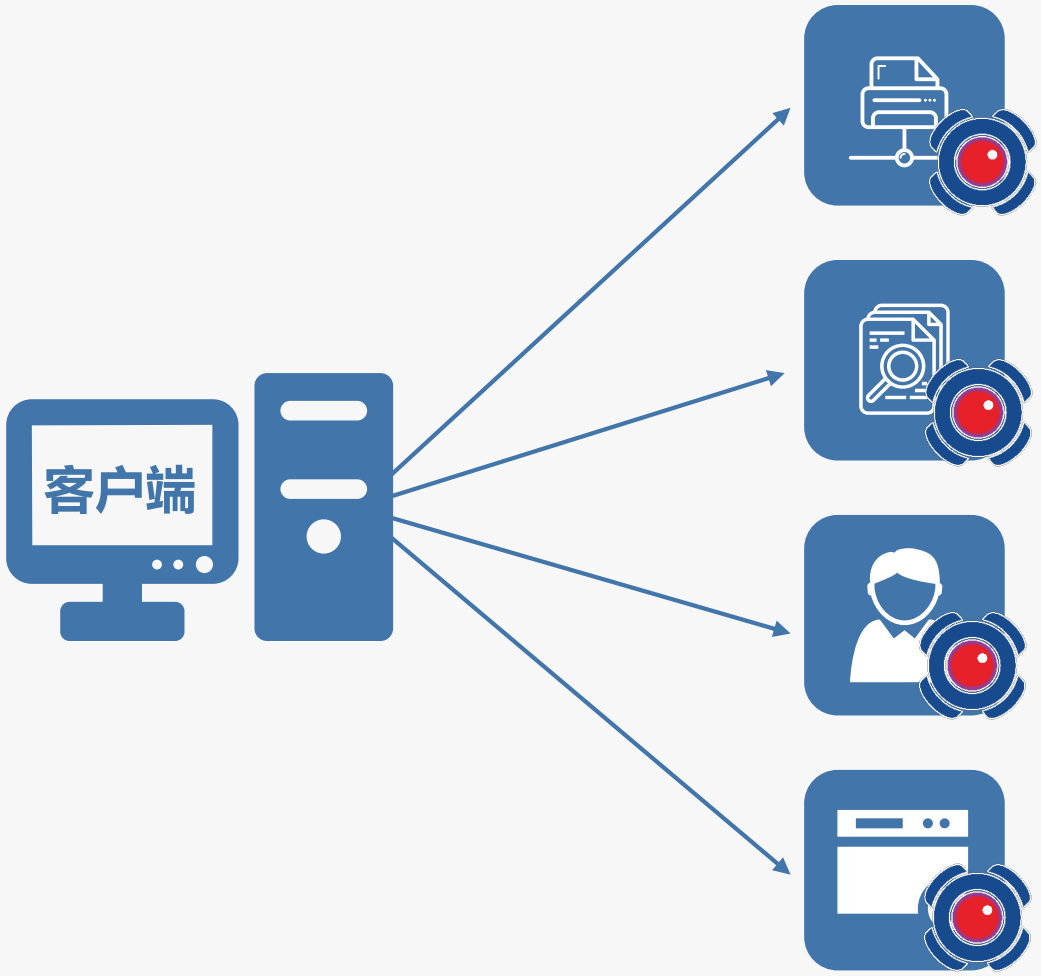
审计详细

详细记录U盘拷贝情况
备份拷贝的文件

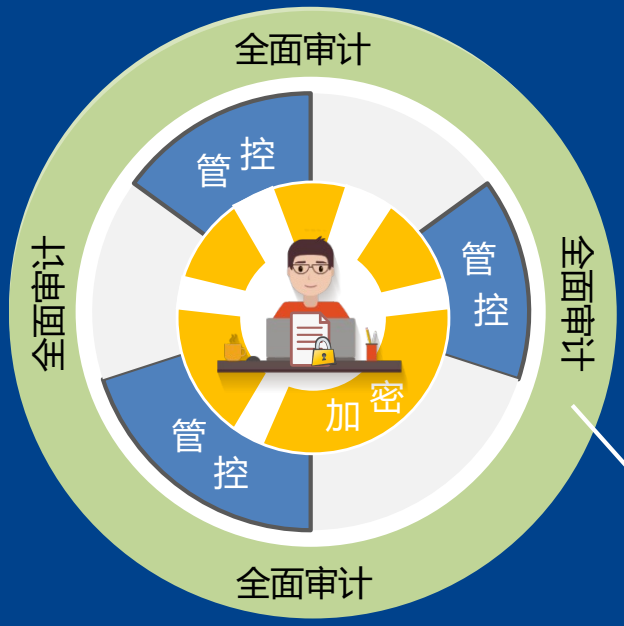
网络应用管控


内部网络
• 禁止访问内网计算机
• 禁止访问重要服务器
外部计算机
企业内网
• 限制通过IM进行文件发送、拖拽、截图
• 限制QQ账号登录
• 控制邮件外发（主题、附件名、邮件大小等）
• 实现邮件强制抄送
• 限 制 http 、 https 、 FTP上传
• 禁止通过百度云、微云等云盘上传公司机密文件

本地应用管控

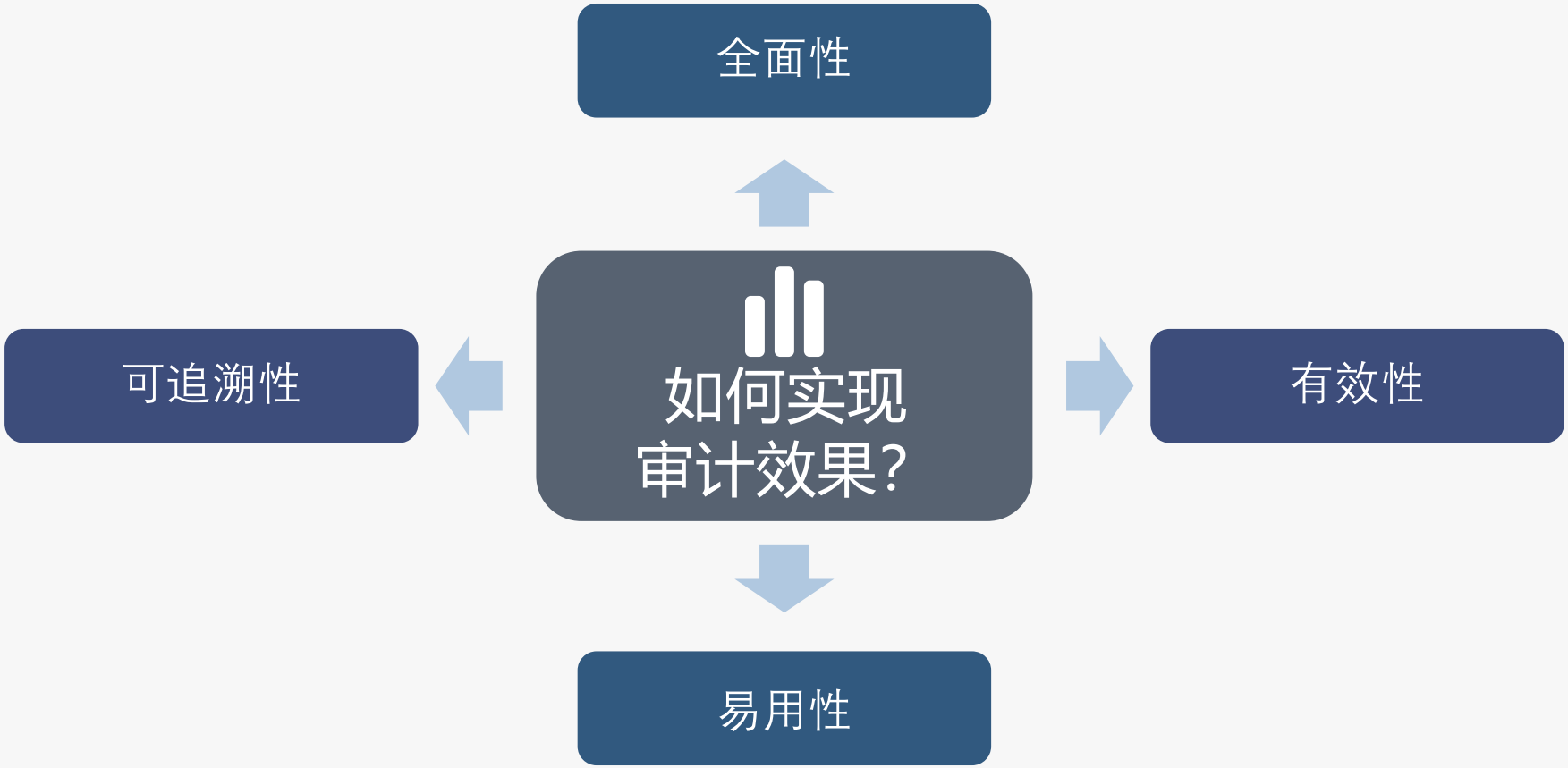


- 限制用户的虚拟打印权限，自定义添加打印浮水印
- 限制文件服务器的访问、修改和删除权限
- 员工离职前，恶意对文档进行复制、篡改或删除时，进行备份
- 限制员工随意安装和使用非法的应用程序，避免引起文件泄露的风险



维度三：事后审计
操作行为审计

详尽细致的事后审计



全面性

全生命周期的操作审计

- 创建
- 访问
- 移动
- 改名
- 复制
- 修改
- 删除
- 其他

设备途径的传播审计

- U盘拷贝
- 手机拷贝
- 移动硬盘拷贝
- 光盘刻录
- 打印

网络途径的传播审计

- QQ传输
- 邮件传输
- 网页传输
- 网盘传输

有效性

日志清晰
- 用户
- 时间
- 操作行为
- 文件
- 源位置
- 目标位置

内容完整
- 外设拷贝备份
- 网络发送备份
- 打印备份

屏幕直观
- 占用空间小
- 与应用联动
- 查看方便

细颗粒
- 私拆硬盘
- 私建虚拟机
- 添加文件到压缩包
- 其他

→ 有效

输出与分析-审计报表

如何在海量日志中，快速发现高频率的风险行为?

谁通过U盘拷贝大量文件?

打印行为是上升？还是下降?

谁在短时间内解密了大量的文件?

风险行为超越阈值时，管理员如何及时了解这个情况?

输出报表

统计表

统计某个行为在时间段内消耗的时间，进行的次数，动作发生的数量

趋势表

展现某时间段内用户行为的变化趋势，可及时捕捉到高频率的风险行为

征兆表

依据征兆条件对用户行为进行统计，用户行为超过阈值，即报警给管理员，确保及时发现和处置风险事件

示例：征兆表

标准征兆事件统计表

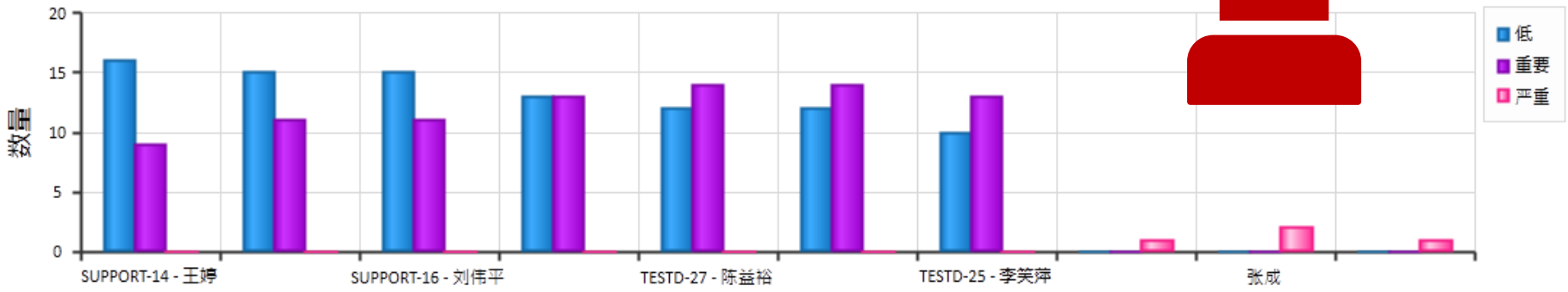
依据征兆条件对用户行为进行统计，产生征兆事件（一般、重要、严重），发现潜在安全风险

查询条件

2014-07-01 ~ 2014-07-31 | 全部 | 全部 | 高级 | 统计

统计类型

按计算机+征兆级别统 | 按组统计 | 全部

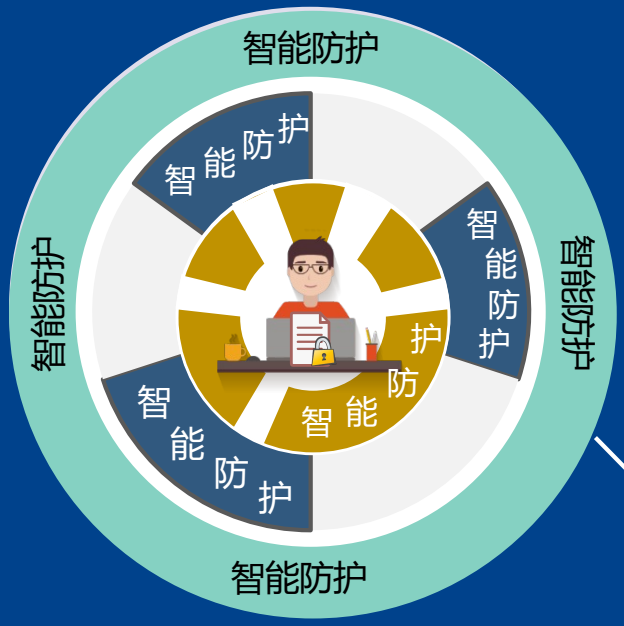


序号	所属组	计算机	低	重要	严重	合计
1	技术部	SUPPORT-14 - 王婷	16	9	0	25
2	测试部	TESTD-24 - 叶栩华	15	11	0	26
3	技术部	SUPPORT-16 - 刘伟平	15	11	0	26
4	测试部	TESTD-26 - 莫宇镇	13	13	0	26
5	测试部	TESTD-27 - 陈益裕	12	14	0	26
6	技术部	SUPPORT-15 - 王冬萍	12	14	0	26
7	测试部	TESTD-25 - 李笑萍	10	13	0	23
8	未分组	李丽	0	0	1	1
9	售前服务部	张成	0	0	2	2
10	售前服务部	刘玉	0	0	1	1
11		总计	93	85	4	182

1. 违规网站浏览时间
2. 违规应用程序使用时间
3. 打印次数、页数
4. 移动存储插入次数、拷贝数量及大小
5. 聊天语句、字符数
6. 邮件外发数量、附件大小
7. 文档拷贝到移动存储、删除文件的数量及大小

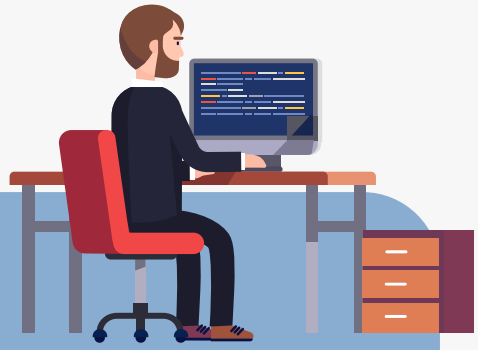
可追溯性-水印功能

- 支持多种水印样式，包括文字水印、图片水印、二维码水印、点阵水印；



智能防护：敏感信息识别与控制

敏感内容发现



本地扫描、远程扫描

- 支持并行扫描
- 对指定敏感内容进行扫描
- 对指定目录、文档类型扫描
- 加密扫描结果成指定安全区域和密级

敏感内容智能加密

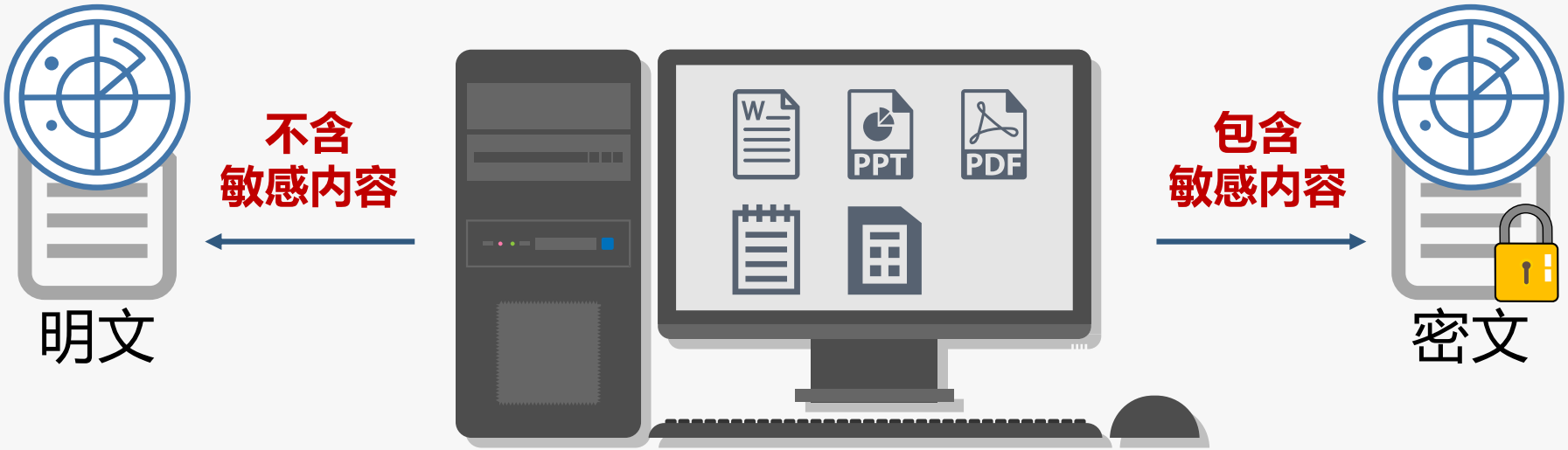
服务器下载、IM接收

邮件附件、U盘拷入

基于敏感内容识别

敏感内容智能加密

智能加密——新建、修改文档时，对含有敏感内容的文档进行加密



敏感内容外传智能控制

敏感内容智能审计

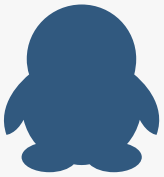
敏感内容操作监视

含敏感内容文档通过移动盘、网络盘外传时，支持审计、备份、报警和警告；

敏感内容邮件外发监视

含敏感内容文档通过邮件外发，支持进行审计、备份、报警和警告；

敏感内容IM外发监视



含敏感内容文档通过邮件外发，支持进行审计、备份、报警和警告；

敏感内容网络上传监视

含敏感内容文档通过网页上传，支持进行审计、备份、报警和警告；

目录

优势1：全面性

终 端 管 理 全 覆 盖

六大产品

十六大模块

终端安全，“全”方能“安”

优势2 有效性

闭环管理

维度一：事前防护 文档透明加密
维度二：事中控制 流通渠道管控
维度三：事后审计 操作行为审计
智能防护：敏感信息识别与控制

事前防护最重要
闭环管理才有效

细颗粒的管控、细颗粒的审计
细颗粒的权限、细颗粒的离线管理

IP-guard

优势3 一体化

统一管理

一个客户端

一个控制台

跨平台实现

Windows

Mac

Linux

“装”一个客户端，“用”一个控制台
三大操作系统 均可实现“闭环”管理

优势4 灵活性

灵活易用

- **功能模块按需集成**：量体裁衣：模块化设计，用户可根据需求自由组合
- **未来需求完美扩展**：扩展性强：集所有功能于一个客户端，既满足当下需求，也可在未来完美扩展
- **部署使用易用便捷**：部署升级方便：支持手动和自动的多种安装和升级方式
  单一管理平台：真正实现灵敏的策略联动，以及有效的闭环管理

模块化设计， 搭建灵活，无缝扩展，
易部署，易使用，易维护

优势5 稳定性


Sinopec
中国移动 China Mobile
中国电信 CHINA TELECOM 世界触手可及
三菱重工 三菱重工中央空调
三一重工 SANY
东风小康 DFSK
周大福 CHOW TAI FOOK
Mercedes-Benz
Panasonic 松下电器
Canon
中国中铁 CREC
TOYOTA
老百姓大药房 LBX PHARMACY
watsons 屈臣氏
wilmar wilmar consultancy services
中粮 COFCO
BRIDGESTONE 普利司通轮胎
长江存储
ZTE中兴
oppo
vivo
展讯通信 SPREADTRUM
MEDIATEK 聯發科技
APP 金光纸业
LENS 蓝思科技
ASE GROUP
瑞儀光電股份有限公司 Radiant Opto-Electronics Corporation
dji 大疆创新
Haier
TPK 宸鴻科技集團 Touching Tomorrow, Today
MY LIKE 美莱整形
ochirly 欧时力
神威药业 SHINEWAY
SHISEIDO 资生堂
TOTO
CATL 宁德时代
FANUC
联塑 L&S
恒大集团 EVERGRANDE GROUP
KINGFA 金发科技
唯品会 vip.com
国家电网 STATE GRID
山水比德
途牛 tuniu.com
SONY
Allianz 安联保险集团
KPMG
伊利
泰康资产 TAIKANG AMC
YKK
Nimble 敏捷地產
湖南卫视
Haid 海大集团 HAID GROUP CO.LTD
ICAC
中国农业银行 AGRICULTURAL BANK OF CHINA
华鑫证券 CHINA FORTUNE SECURITIES
GTA 国泰安
inspur 浪潮
小鹏汽车 XPENG MOTORS
汇付天下
ELEVEN
muRata 村田制作所
KYE 跨越速运 一诺定达
BITMAIN 比特大陆

目录

目录

IP-guard

专注终端安全，保护核心机密

Intellectual Property Guard

智力财产保护

溢信科技成长与发展

2001

溢信科技作为先行者进入终端安全领域并推出首款安全产品Any@Web

2002

推出IP-guard终端安全管理系统

2006

IP-guard V3模块化正式发布

2010

IP-guard V+全向文档加密功能震撼面世

2013

获得国家密码局商用密码产品定点生产单位证书

2016

国内率先推出MAC文档加密产品

2017

IP-guard V4正式发布;新三板挂牌上市，Mac终端管控推出

2018

敏感内容识别产品推出，Linux终端管控推出，杭州、济南、郑州、南京办事处成立

2019

厦门、西安办事处成立

2001 2002 2006 2010 2013 2016 2017 2018 2019

覆盖全国，优质服务

20,000

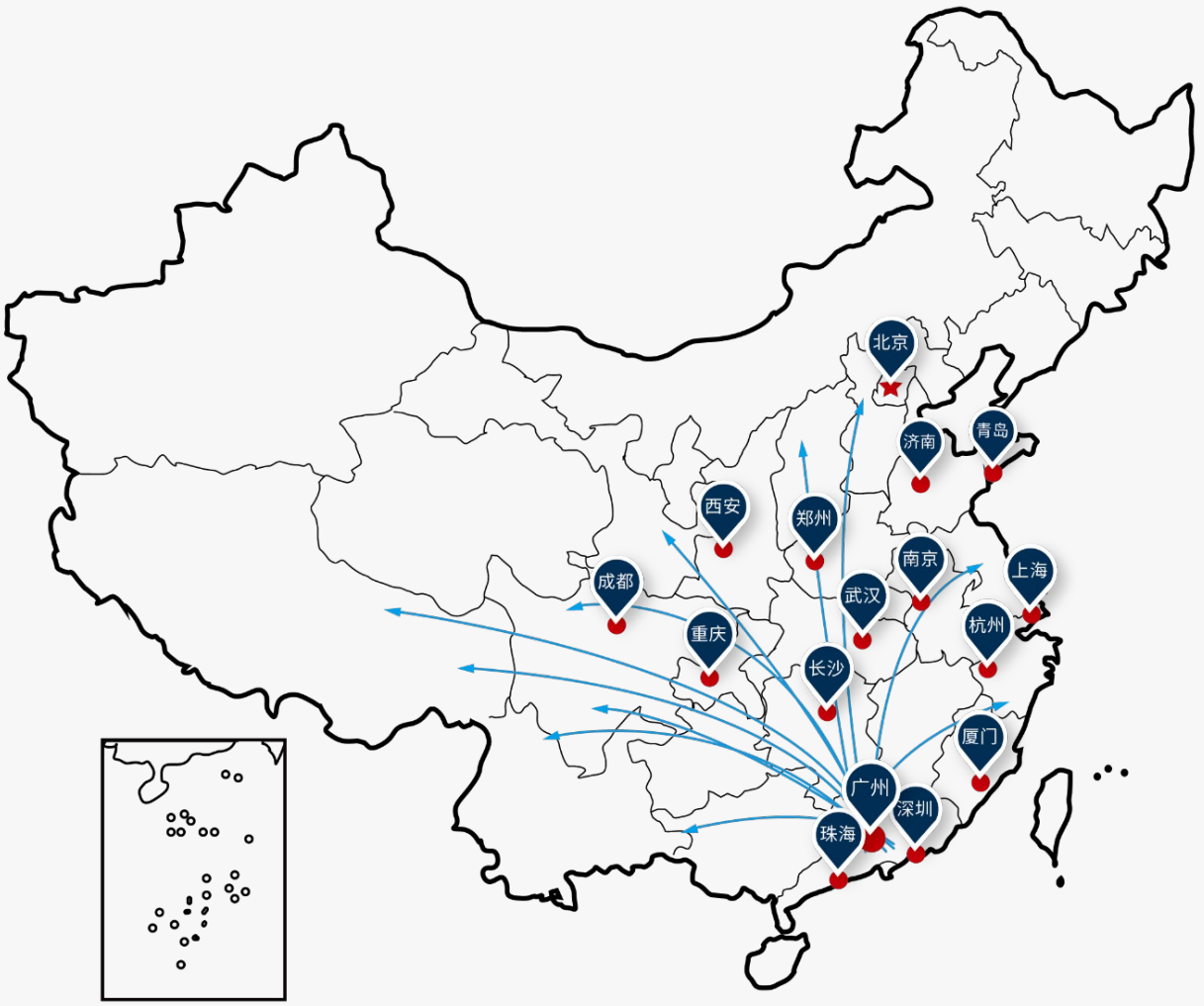
超过20,000家企业用户一致选择IP-guard

5,000,000

超过5,000,000余台计算机同时运行客户端

〉25

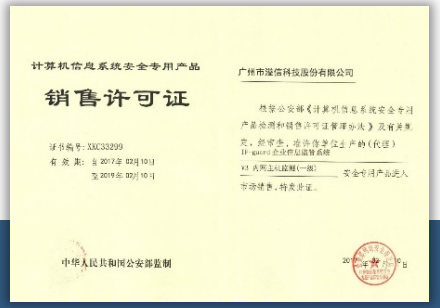
在机械、电子、纺织、金融、政府、军工等超过25个行业担任着终端安全管理的重要角色



资质齐全

信息安全产品全套资质： **“公保机丁”** 四类六种

公安部



《公安部计算机信息系统安全专用产品销售许可证》

保密局

《涉密信息系统产品检测证书》

商密局

《商用密码产品生产定点单位证书》
《商用密码产品型号证书》

解放军

《军用信息安全产品认证证书》

屡获好评








BC
AWARD
BEST CHOICE 2010

Overall Rating
Features & Design
Value for Money
Ease of Use
PC
PRO
RECOMMENDED

Brothersoft
Editor's Pick
www.brothersoft.com

cnet DOWNLOAD.COM
CNET Editor's Rating

国内外知名企业
一致信赖

专注终端安全 保护核心机密