洞察眼MIT系统

洞察眼MIT系统产品功能介绍

新一代终端安全、数据安全引领者

目录

CATALOGS

上网行为

生产力

文档安全

文档透明加密

设备管理

聚合报表

网络管理

敏感内容分析

运维中心

聚合搜索

AI Pro

01 上网行为

审计、管控上网行，为确保网络安全

功能简介

员工上网行为的审计与管理

问题1

从事与工作无关的上网行为，可能会严重影响工作效率！

浏览网站

炒股、看视频、浏览与工作无关的网站

即时通讯

私人社交降低工作效率以及泄密风险

电子邮件

163

邮件接收与发送过程中存在数据泄漏风险

更多

百度网盘｜腾讯视频｜腾讯游戏等上网行为

问题2

企业内部敏感文件外发途径广泛，缺少安全的管控措施！

电子邮件

通过电子邮件，私下联系客户做私单

即时通讯工具

通过微信文件传输将客户资料发送给竞争对手

网盘应用

将公司内部文件备份到网盘

解决之道

监管多种上网行为，确保互联网使用安全合规。

浏览网站

01 浏览网站监控

详细记录终端计算机浏览网页的网址和标题，并提供查询功能。

02 网站访问控制

可以对指定的网站URL进行封堵。自主研发的高性能过滤引擎，降低对计算机性能的影响，支持HTTPS/SSL加密协议的过滤。

03 网站敏感词拦截

洞察眼MIT系统支持网页关键词拦截。

04 关键词记录

统计终端搜索引擎使用情况，包括使用的搜索引擎、搜索关键词、访问时间等。

(1) 浏览网站监控

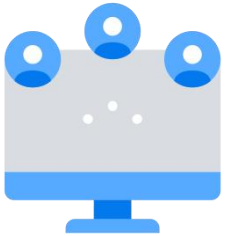
网页浏览记录

记录浏览网页的标题、网址、时间等信息。

网页浏览统计

多纬度统计网页访问的使用时长及百分比，并以图表形式进行展现，工作效率一目了然。

(2) 浏览网站控制、网站敏感词拦截



基于网址

- 与工作相关的网站 — Baidu 百度  ✓
- 与工作无关的网站 — iQIYI 爱奇艺 淘宝 Taobao ⊘

基于敏感词

- 政治敏感 ⊘
- 网络赌博 ⊘
- 色情 ⊘

即时通讯管控

01 即时通讯监控

完整记录主流即时通讯软件的对话时间、收发双方、对话内容等信息，支持聊天内容全局搜索。

02 聊天语义告警

定义即时通讯敏感词，对话内容包含了敏感词，如：帐号信息，求职信息等，管理员则会及时收到报警通知。

03 聊天帐号管控

限制终端聊天帐号的登录，可以设置终端登录指定的聊天帐号。

(1) 即时通讯监控

聊天记录审计

记录QQ、微信、企业微信、钉钉、Skype等主流技术通讯工具的聊天内容，防止信息泄密

收发文件审计

记录即时通讯工具收发文件行为，以便事后进行安全审计。并对敏感的文档进行备份、告警

(2)

聊天语义告警、账号管控

聊天账号白名单

允许白名单内聊天账号的登录使用。

实时聊天记录

对聊天内容，文件传输等进行实时记录。

敏感内容报警

对敏感内容识别告警，杜绝信息泄密风险。

邮件管控

01 电子邮件监控

记录标准协议邮箱、HTTPS/SSL加密协议邮箱的收发邮件的标题、收件人、发件人、正文、附件等内容。

02 电子邮件管控

可通过收件人、发件人设置策略来控制邮件收发，防止企业的重要信息通过邮件方式泄露。

(1) 电子邮件监控

邮件外发记录

有效记录外发邮件的收/发件人、主题、内容及附件。

支持多种电子邮件审计

Foxmail、Outlook等邮件客户端及各类常见Web邮箱。

(2)

电子邮件管控

强制抄送

邮件发送必须指定抄送人，增加邮件发送审核环节，确保邮件传输安全。

限制发送邮箱

限制员工私人邮箱的使用，只允许公司规定的邮箱发送文件，实现邮件的合规使用。

限制接收邮箱

规定员工只能将邮件发送到指定邮箱，适用于企业只允许使用邮件进行内部沟通场景。

收益

专注目标，科学评估、提升工作效率、生产力。

历时5年

通过对成功签约的部分企业，约

205,000

台终端数据，回访统计表明

77%

时间用于处理工作事务

23%

时间用于工作无关的事情

使用洞察眼
MIT系统

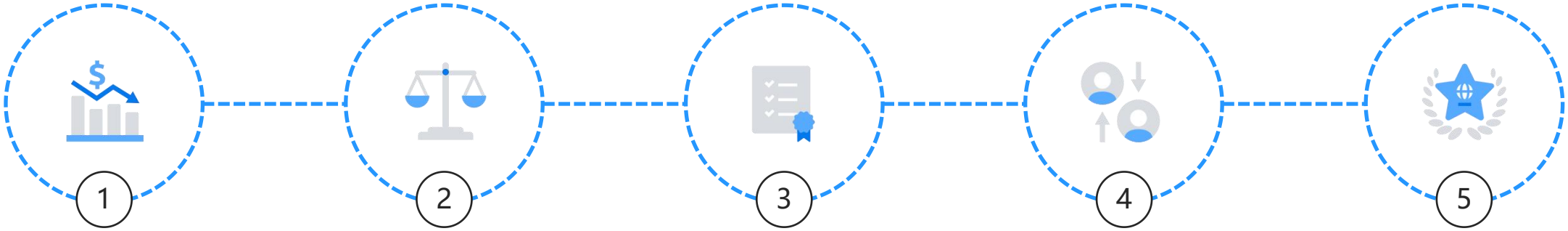
83%

时间用于处理工作事务

02 文档安全

文档安全管理 防范数据泄漏

数据泄露的危害



1

巨额财产损失

绝大多数数据泄密事件，市场人员违规，都会给企业造成直接或间接的财产损失。

2

违反法律法规

一些国家涉密领域的数据泄漏，会导致企业违反保密法、网络安全法等法律法规。

3

核心技术流失

代码、技术图纸等数字资产的外泄，会导致企业失去核心竞争力。

4

客户伙伴流失

客户、合作伙伴资料的泄密，一旦被竞争对手获取，会直接影响企业的健康发展。

5

声誉信任度受损

一些行业的数据、信息泄漏，会使企业声誉及信任度严重受损，引发舆论危机。

功能简介

员工上网行为的审计与管理

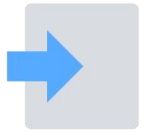
问题1

员工有意或无意的泄漏公司机密文档无从查证！

将公司内部文件备份到网盘

将敏感文件截屏发布到网络平台

离职将机密文件拷贝到U盘带走

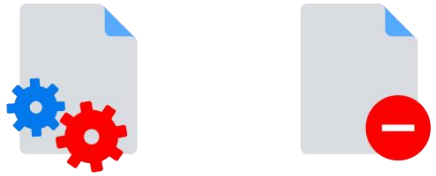


通过微信将客户资料发送给竞争对手

问题2

文档被修改、删除、感染勒索病毒等，无法复原！

员工修改、删除



来自内部

黑客、勒索病毒

来自外部

解决之道

文档安全管理，防范数据泄密。

文档安全管控、审计

01 泄密追踪

对终端通过浏览器、即时通讯、邮件外发的文件进行记录，并对外发的文件进行备份，提供泄密风险等级评定。

02 文件外发审批

开启文件外发管控后，允许通过审批的方式对指定文件进行外发。

03 文件操作监控

记录终端计算机的文件操作信息，包括本地磁盘、移动存储、网络路径、共享目录的所有文档创建、访问、修改、复制、移动、重命名、删除等操作。

04 文件操作管控

控制终端计算机指定路径下文件的读取、修改和删除操作的权限。

文档安全管控、审计

05 文件外发管控

文档外发管控可以封堵常见的文档外发行为，比如：通过电子邮件、聊天软件、网盘等途径外发文件。支持自定义文件类型、大小等。

06 剪切板监控

监控终端剪切板的文字信息，包括时间，和具体文字内容。

07 文档备份

文档备份可以将分散在客户端的文件进行集中备份管理，支持增量备份、删除备份。

08 文件删除

定时删除终端桌面、回收站或者指定路径下的指定类型的文件。

(1)

泄密追踪

泄密追踪

对通过浏览器、即时通讯、邮件、U盘外发的文件进行记录，并对外发的文件进行备份，提供泄密风险等级评定。

泄密告警

当终端用户外发文件时进行实时告警，或者触发指定规则是进行告警，如：在10s内外发20个文件。

发现泄密时截屏

当终端用户外发文件时自动记录当前屏幕内容，通过记录、图片的形式进行行为溯源。

(2)

文件外发审批

文件解密审批

具备根据不同文件类型、大小进行解密审批，
以及解密后超出指定时间自动加密的特性。

文件外发

审查外发文件的权限是否合规，直观了解文档
的外发动态，确保文件在外使用安全。

邮件解密

对邮件收件人、正文以及附件等进行合规审批，
确保邮件传输安全、合规。

(3) 文件操作监控


创建
访问
移动
重命名
复制
修改
删除
文档全生命周期操作审计
（审计详尽而细致，实现对文档的有效追溯）
文 档
离职前
转移
恶意篡改
删除
备份
文档被员工转移、篡改、删除前进行备份
（既实现有效追溯、又防止文档被破坏）

(4)

文件操作管控

区分操作权限

指定员工对重要文档可进行读取、修改、删除等操作而其他员工只能访问。

文件操作监管

监管包括存储于服务器、硬盘、移动盘、网络盘等位置的文档操作，防止用户误操作引起的文件丢失泄漏。

(5)

文件外发管控

文档外发封堵

文档外发管控可以封堵常见的文档外发行为，比如：通过电子邮件、聊天软件、网盘等途径外发文件。支持自定义文件类型、大小等。

限制外发类型

支持设置允许外发的文件类型，还可以通过软件对关联类型进行统一管理。比如：WPS文字，可关联文件类型*.wps；*.wpt；*.doc；*.txt；*.docx等。

敏感文件阻断

实时监视、分析终端外发文件的行为，对包含敏感内容的文件实施阻断传输。支持通过关键字、正则式等方式定义敏感内容。

(6) 剪切板监控

全面监控剪切板

全面监控终端剪切板的文字信息，包括时间和具体文字内容，有效防止敏感信息通过剪切板被非法获取或泄露，确保企业信息的安全性。

风险实时感知

具备实时告警机制，一旦发现剪切板中的异常文字信息，会立即触发告警，帮助管理员及时感知风险并采取相应措施，防止潜在的信息泄露事件。

历史记录回溯

记录剪切板的操作历史，包括时间、内容和操作人员等信息并进行存档，方便企业进行审计和追溯，满足合规性要求，提升信息管理水平。

(7)

文档备份

集中管理

可实现公司所有客户端文件的集中备份管理，确保文件数据的安全性和完整性，避免因文件丢失或损坏而导致的工作中断和数据泄露风险。

增量备份

支持增量备份功能，只备份自上次备份以来发生变动的文件，大大提高了备份效率，同时节省了存储空间，让用户更加便捷地管理备份数据。

灵活恢复

提供灵活的恢复功能，用户可以根据需要选择恢复特定文件或整个备份集，轻松应对文件丢失、误删除等突发情况，保障业务的连续性和稳定性。

屏幕安全

01 智能截屏

支持定时截取屏幕操作；
支持触发式截屏，当终端运行指定进程，或指定进程在仅在前台运行时进行截屏；
智能识别屏幕内容并进行分类，比如：聊天、电子邮件、求职、购物等。

02 屏幕水印

统一在终端计算机桌面显示自定义水印（文字、点阵），文字水印支持单行或多行显示方式。

03 窗口水印

指定终端在打开某个应用时添加自定义水印（文字、点阵）。

04 截屏管控

记录终端截屏内容，并且可以封堵Print Screen、聊天软件截屏、浏览器截屏插件、以及PicPick等专业的截屏工具。

屏幕安全

05 截屏水印

支持在终端通过截屏工具截取的内容中添加自动水印信息（文字、点阵）。

06 实时屏幕

实时查看终端屏幕内容，支持对多个终端屏幕进行集中监控。

07 屏幕录像

对屏幕进行不间断录像，并保存成录像文件，方便事后审计。

(1) 智能截屏、截屏管控

屏幕截图

可对监控终端界面进行截图，截图方式有智能截图和定时截图。

截屏工具封堵管控

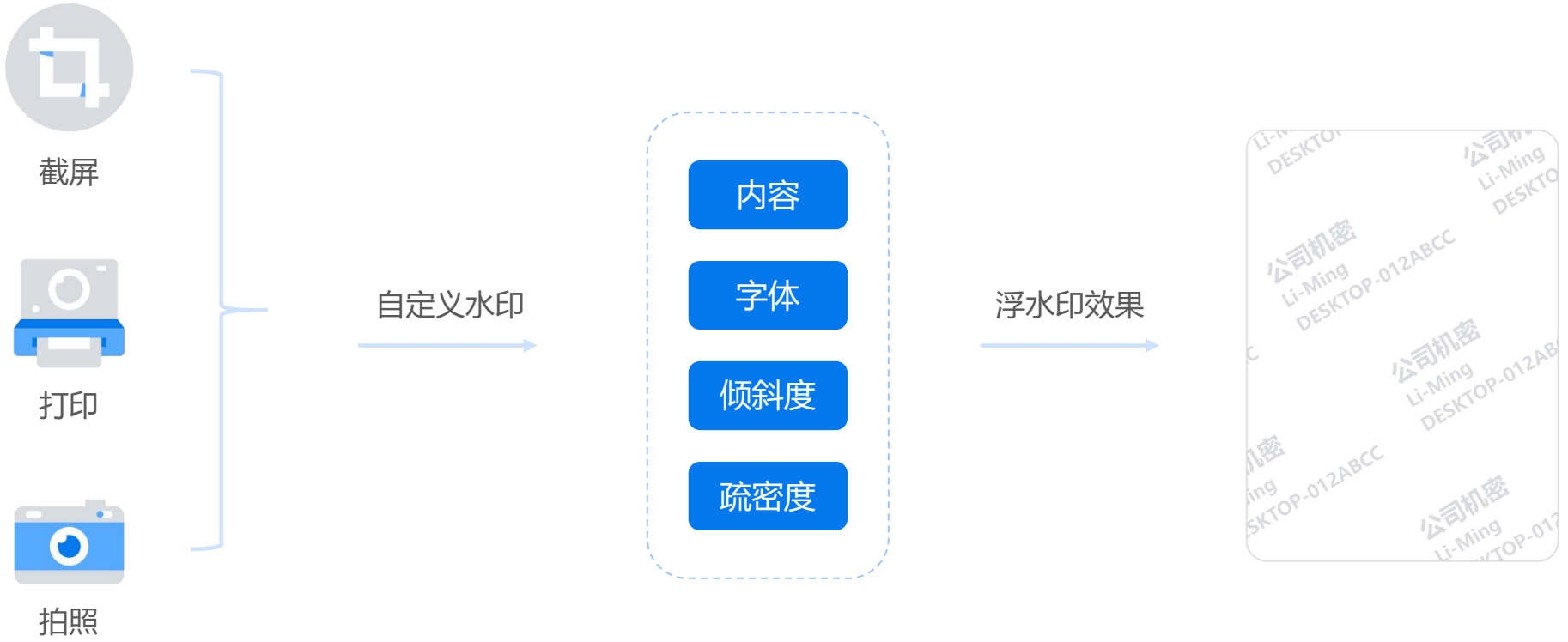
能够封堵Print Screen按键、聊天软件截屏功能、浏览器截屏插件以及PicPick等专业的截屏工具，有效防止恶意截屏行为，保护终端安全，减少信息泄露风险。

全面记录截屏内容

该功能能够实时记录终端所有截屏内容，包括Print Screen按键截屏、聊天软件截屏、浏览器截屏插件以及专业截屏工具PicPick等，确保企业或个人重要信息不被非法获取或泄露。

(2)

屏幕水印、窗口水印、截屏水印



水印设置

支持在终端计算机全屏幕或打开指定软件时在窗口上铺设水印信息。

个性化水印

支持以文字或点阵的方式显示包括终端IP/MAC地址、时间、用户名等信息，定位泄密人员。

(3)

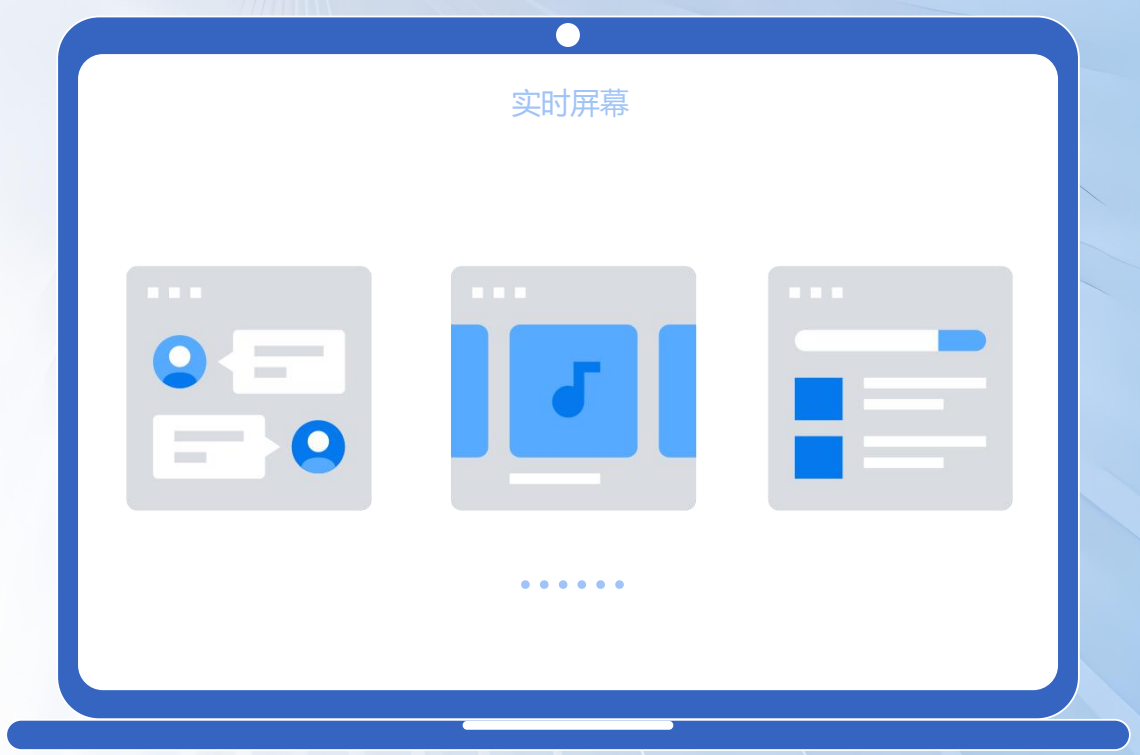
实时屏幕、屏幕录像

随时监管

通过电脑实时屏幕监控功能，你可以远程查看指定电脑的实时屏幕，直观地了解到员工正在做什么，是否从事和工作无关的事情，以及是否存在泄密等违规行为。

屏幕录像

将用户操作计算机的过程录制成视频文件。具有录像过程资源占用低、无感知，录像文件占用磁盘空间小等特点。



打印安全

01 打印监控

详细记录终端打印信息，包括打印标题、时间、页数、内容等信息。支持打印快照查看。

02 打印管控

管控终端用户使用打印权限；
禁止打印带有敏感信息的文档。

03 打印审批

开启打印管控后，允许通过审批的方式对指定文件进行打印。

04 打印水印

终端打印的文件自动置入自定义水印（文字、点阵、二维码）。支持通过取消打印水印申请对指定文件打印时不添加水印。

(1) 打印安全


数据安全
打印管控
开启后，禁止打印所有文件或包含敏感词的文件
参数设置
打印安全
数据备份
备份周期：7
备份时间：00:00:00 — 00:00:00
保留版本：7
备份路径：
备份日志：
打印水印
水印规则：打印水印-2
效果预览
允许申请移除打印水印审批
打印管控
选择文件打印时的管控类型，默认禁止所有
禁止打印包含敏感词的文件
禁止打印所有文件
禁止打印包含敏感词的文件

收益

防范商业环境中的数据泄漏，“一夫当关，万夫莫开”！

保护知识产权，提高核心竞争力

泄密跟踪溯源，避免法律商业风险

洞察眼MIT系统数据防泄漏(DLP：Data Loss Prevention)解决方案采用了主动发现、防护的策略，可全方位保护你的敏感数据。

规避舆论公关风险

提高公众的信任度

03 设备管理

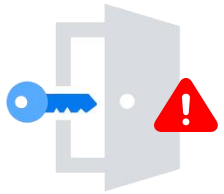
把外接设备带来的风险降到最低

细化外接设备使用权限

问题1

员工私自使用移动存储设备进行资料拷贝，企业缺少必要的管控！

员工通过U盘私自拷贝文件



U盘丢失泄密

含有U盘病毒的存储接入内网

便携性带来的内网安全风险

问题2

私自接入外接设备带来的风险！

- 员工私连手机热点、便携WIFI，导致非法外联，逃离公司监管，影响内网管理。
- 员工通过蓝牙，USB端口连接移动多媒体设备（打印机、刻录机、手机）存在泄密风险。
- 未知设备接入有病毒感染风险。


手机热点


便捷WIFI


打印机


刻录机


手机


未知设备

解决之道

针对不同外接设备做细粒度的权限划分，规范设备使用，杜绝非法设备接入。

移动存储管控

01 移动存储使用

对终端计算机的移动存储拔插事件进行记录。

02 移动存储操作

对终端计算机的移动存储的操作事件进行记录。

03 移动存储使用告警

针对终端使用U盘以及进行文件拷贝时提供实时告警。

04 移动存储管控

可以对U盘进行管控，规范U盘的使用，降低信息泄露的风险。同时，还可以对U盘进行授权，只有授权的U盘才可以使用，安全便捷两不误。

05 移动存储使用申请

当客户端移动存储被禁止使用时，允许客户端可以通过提交申请，请求读、写U盘。

06 移动存储加密

洞察眼MIT系统使用AES等高强度的加密算法对U盘 进行加密，加密后的U盘只能在企业内部使用，如果员工违规带走，在外部无法正常打开使用。

(1)

移动存储使用、操作、告警

移动存储使用记录

详细记录移动存储设备插入、拔出事件。

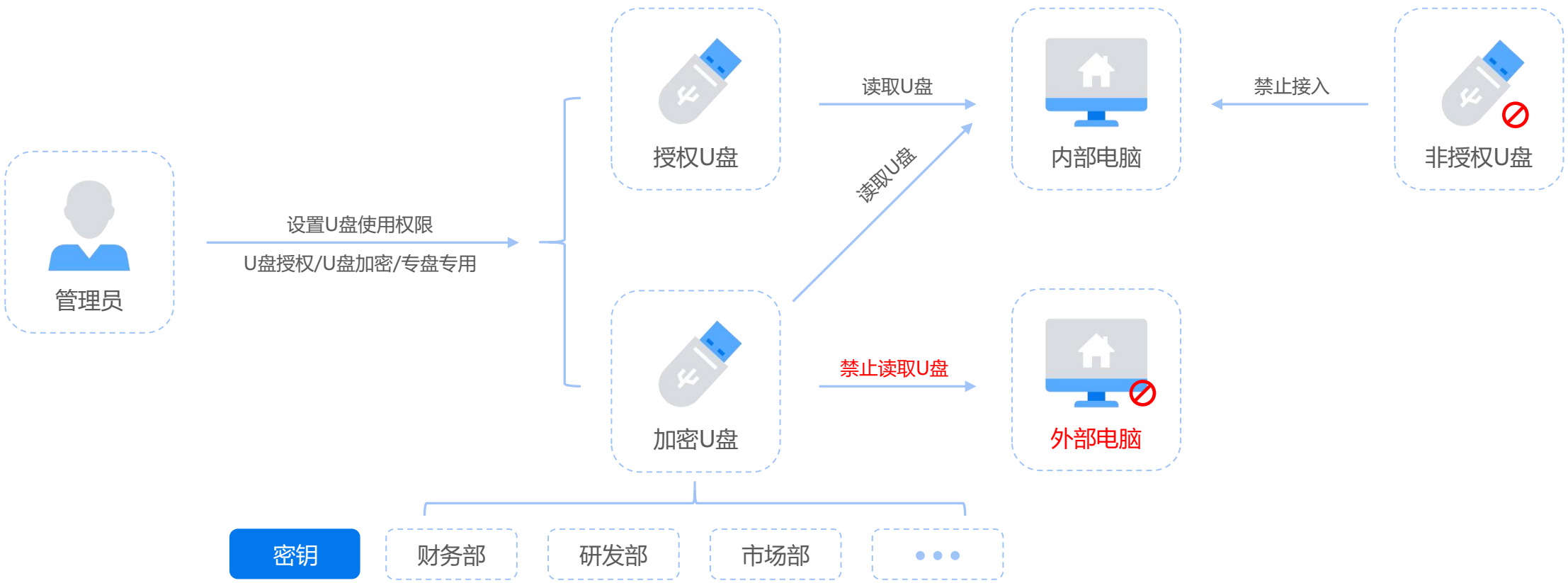
移动存储操作审计

可对终端计算机的移动存储操作进行审计，包括读写、创建、移动、修改、删除等操作。

移动存储告警

当终端插入移动存储时、使用移动存储拷贝文件，实时发出告警，提醒用户和管理员注意潜在的安全风险

(2) 移动存储管控、申请、加密



(2)

移动存储管控、申请、加密

U盘授权-外盘外用

洞察眼MIT系统识别员工个人U盘与企业内部授权U盘，禁止私人非授权U盘接入拷贝内部资料。权限：只读、读写、禁止使用。

U盘加密-内盘内用

洞察眼MIT系统通过AES-256、Blowfish等高强度加密算法，有效解决U盘丢失、外带导致的数据泄漏事件。

专盘专用

洞察眼MIT系统为企业不同职能部门分配密钥，建立部门专用U盘，实现专盘专用，防范企业内部之间数据流转泄密。

硬件&设备管理

01 硬件资产统计

终端硬件资产信息统计，全网终端硬件信息统计。

02 硬件变更报警

终端硬件资产变更记录及产生告警信息。

03 USB端口管控

禁止终端使用通过USB端口连接的设备（键盘鼠标除外），支持设置例外设备。

04 禁用设备

禁用光驱、蓝牙、串口、并口、火线、PCMCIA总线；禁用打印机、便携WIFI、无线网卡等，保证系统安全。

05 刻录审计

支持审计终端刻录行为，备份刻录文件。

(1) 硬件资产统计、变更告警

资产信息

支持分组统计资产信息，与资产使用者部门、姓名信息一一对应，方便资产丢失后快速溯源；

硬件资产自动全面盘点，方便管理员快速了解全局资产情况。

变更记录

可查看企业电脑终端硬件变更详情，变更前后对比、变更时间等信息。

预警消息

电脑终端（如：温度、CPU占用、内存占用等）达到预先设定阈值时，管理员将收到预警

(2)

USB端口管控、禁用设备

禁止USB设备使用

一键禁止终端除键盘、鼠标外的USB设备使用

授信设备使用

可查看企业电脑终端硬件变更详情，变更前后对比、变更时间等信息。

设备禁用

一键禁止局域网光驱、蓝牙、串口、并口、火线、PCMCIA总线；禁用打印机、便携WIFI、无线网卡等设备使用，保证系统安全。

收益

安全、便捷两不误！

在保证企业数据安全情况下使用U盘，提高办公效率，享受U盘带来的便利。

覆盖范围广，管控无遗漏。细化USB设备的控制，支持各种外设的控制。

04 网络管理

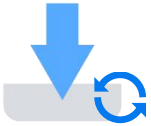
终端权限管理 保障终端安全

功能简介

管控终端系统权限，降低内网安全风险

问题1

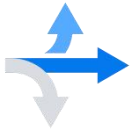
内网中常见的影响终端安全、工作效率的行为！

各类娱乐软件	软件安装	系统配置	P2P下载
			
无节制使用，严重影响工作效率	随意安装不明来源的软件	任意修改终端系统关键设置	占用公司带宽影响企业主业务运行

问题2

终端网络缺少安全管控会带来严重的内网安全隐患！

工作中常见的影响网络安全的行为



连接手机热点

随意修改IP地址

私自接入无线网络

超权限访问内网资源

问题3

盗版软件带来的安全风险！

财产损失

软件版权风险

病毒威胁

数据安全风险

解决之道

全方位保护终端安全，确保内网安全稳定

系统安全 & IT资产

01 系统安全检测

查看全网终端防火墙设置情况、杀毒软件安装情况、来宾用户开启状态、系统多用户使用状态及Internet代理使用状态。

02 系统安全策略

设置系统安全策略，如：禁止共享、禁止修改终端名等，保证系统始终处于安全状态。

03 系统密码策略

支持开启Windows强密码验证，强制验证密码复杂度、密码最小长度、密码最短使用期限、密码最长使用期限。

04 操作系统统计

终端操作系统安装情况统计。

05 杀毒软件统计

终端杀毒软件安装信息统计，全网终端杀毒软件安装信息统计。

(1)

系统安全策略

通过系统策略，可以调整系统权限，保证系统处于安全状态

- 禁用任务管理器
- 禁用控制面板
- 锁定计算机名称
- 禁用注册表
- 禁止修改网络配置
- 禁用安全模式
- 禁用CMD
- 禁止共享文件

软件管理

01 软件资产统计

终端软件资产信息统计，全网终端软件信息统计。

02 软件资产变更告警

终端软件资产变更记录及产生告警信息。

03 软件白名单

允许指定的终端计算机在指定的某段时间内使用某种程序。支持进程名、版权信息、安装目录、产品名称等多种匹配方式。

04 软件黑名单

限制指定的终端计算机在指定的某段时间内使用某种程序。支持进程名、窗口名、MD5等多种匹配方式。

05 软件安装白名单

开启禁止安装软件策略后，可通过添加软件安装白名单允许特定软件的安装，支持软件数字签名、版权、产品名称等信息。

06 软件安装审批

针对开启软件安装管控的终端，提供软件软件安装申请，允许终端在指定时间内指定安装软件。

软件管理

07 软件合规检测

监测终端是否安装指定应用软件，如果终端未按规定安装软件，则触发响应管控策略。

08 软件远程卸载

远程强制卸载终端电脑内已安装的软件。

09 软件商店

管理员可上架指定的软件到企业私有化软件商店中，员工可自行下载安装使用。

10 盗版软件检测

实时检测用户安装软件是否为盗版软件，可记录盗版软件名称、版本、开发商、软件安装路径、启动软件时间；

支持对终端运行的软件进行检测，识别为盗版时可实时禁止盗版软件运行。

(1) 应用程序管控：控制应用程序的安装卸载及使用

应用安装

通过对软件的安装、卸载进行限制，实现桌面应用程序的标准化管理。

应用使用

分时段控制软件运行黑白名单，实现人性化管理。

应用管理

统计终端软件资产，远程卸载不合规软件。

(2)

软件正版化管理：确保软件合规使用

未合规禁止联网

实时监测终端是否安装指定软件，如果未安装则禁止所有应用联网。

未合规重定向

实时监测终端是否安装指定软件，如果未安装浏览器访问网页时，重定向到指定网址。

弹窗警告

实时监测终端是否安装指定软件，如果未安装进行弹窗警告。

(3) 软件商场

软件商店 终端用户可通过软件商店安装、升级应用程序，确保软件来源安全可靠、符合企业软件标准化管理需求。

(4) 盗版软件检测

无需提前录入序列号，洞察眼MIT系统通过机器学习、智能沙箱技术分析自动识别盗版软件，将软件安装情况进行可视化展现，及时告警，执行相应管控策略。

网络管理

01 网络流量审计

统计客户端在指定时间范围内的网络通讯流量，包括按地址、协议和端口的类别进行统计。

02 网络协议

支持DNS、FTP协议的监控与审计。

03 网络访问控制

通过对程序、网络端口、IP地址、通讯方向、协议类型等参数限制计算机对内网、互联网等的访问,避免由随意的信息交互带来的风险。

04 非法外联

检测终端违规外联行为，并可同时阻断违规外联行为。

05 可信网络

用户可以自定义可信网络环境，离开可信网络支持相应策略联动、支持断网、告警、锁屏。

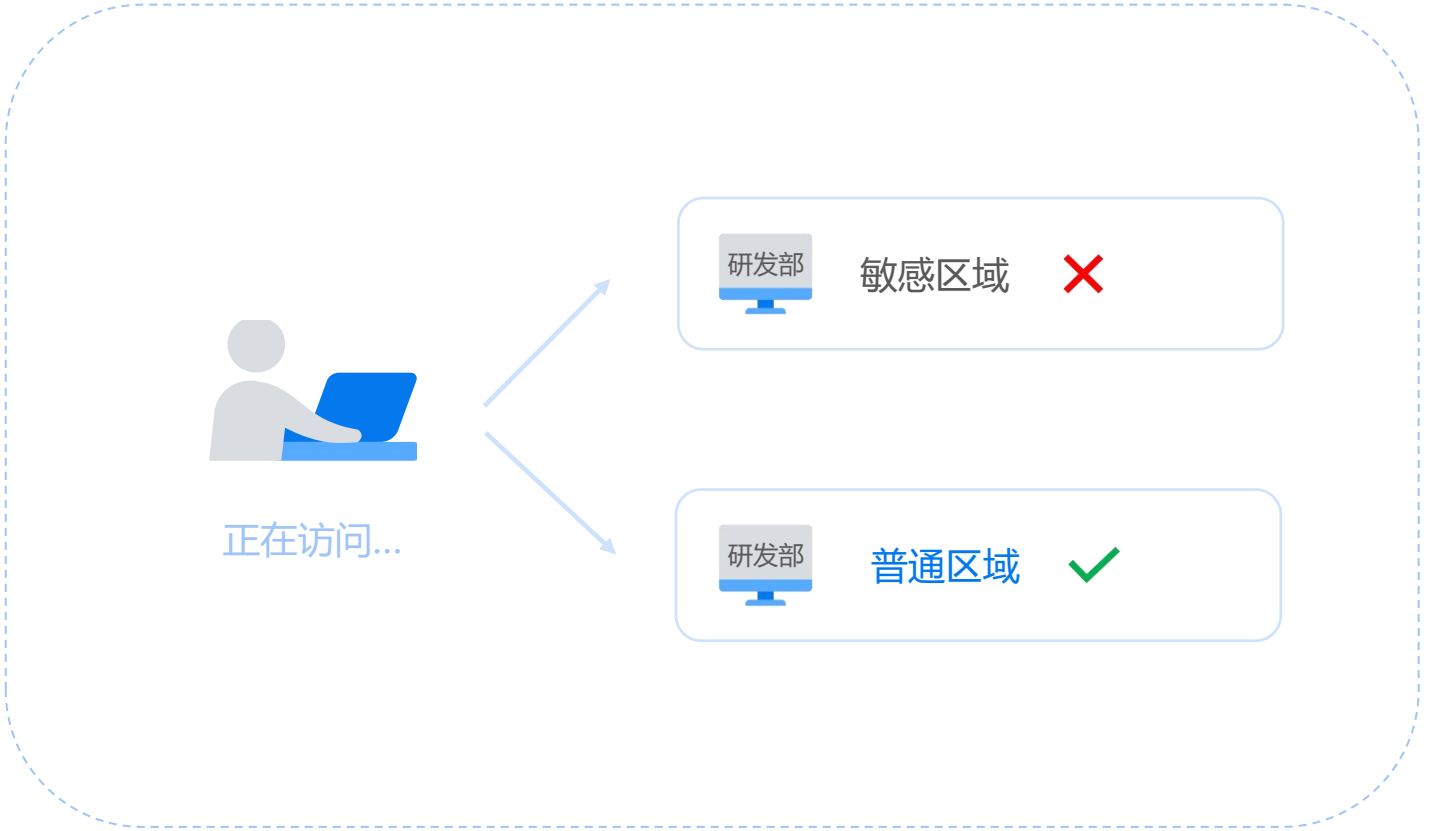
06 HTTP协议过滤

阻断终端HTTP协议的文件上传行为。

(1) 网络访问控制

驱动级的防火墙

洞察眼MIT系统使用驱动级的防火墙技术，支持进程、端口、网络地址、网络协议等对终端的网络访问权限进行控制。



（1）非法外联

非法外联

及时发现并切断员工外联行为

(1) 可信网络

划分可信网络

确保只允许终端在可信的网络中使用。

收益

范数据泄漏风险、提升工作效率、降低网络安全风险！

防范数据泄漏风险

提升工作效率

降低网络安全风险

05 运维中心

一组实用、强大的终端管理工具

功能简介

一组内网安全、桌面管理工具，助力企业IT系统高效运维，提高运维人员工作效率

远程协助

分发任务

身份认证

时间校准

桌面个性化

工单管理

节能设置

运维中心

01 分发任务

分发文件、软件、补丁到终端计算机指定路径，支持软件远程安装部署。

02 远程协助

远程连接到用户计算机的桌面，并直接对计算机进行操作或示范，快速响应系统故障。

03 节能设置

集中对终端进行定时关闭显示器、定时锁定或者定时睡眠，并可设定两次定时关机任务，有效防止能源损失。

04 工单管理

统计终端工单申请，管理员可及时有效采集终端工单信息并及时做出响应。

05 发送消息

可以对全网终端用户或指定用户发送通知消息。

06 时间校准

设置终端计算机时间与服务器时间保持同步。

运维中心

07 桌面个性化

对用户电脑自定义设置桌面背景，可禁止用户修改桌面背景，以及可以对用户电脑设置屏幕保护等。

08 终端负载

统计终端CPU、内存、硬盘占用率，提供实时负载查看，超阈值预警。

09 身份认证

自定义系统登录用户或使用Windows用户，统计登录用户操作审计信息。登录方式支持用户名、密码认证/刷卡认证。

10 Windows密码管理

管理终端计算机的用户密码（新增、修改、清除），便于管理人员统一管理终端计算机Windows用户。

分发任务：应用场景

在项目中，

项目经理如何将不同的任务分配给

对应的团队成员？

(1)

分发任务：一键下发操作，下发结果一目了然，方便定位

文件分发

支持将企业内部软件安装包或其他文件，一键分发至团队内电脑并按自定义策略运行。

脚本分发

支持将企业内部脚本上传、分发各电脑，并可自定义策略执行

远程协助：应用场景

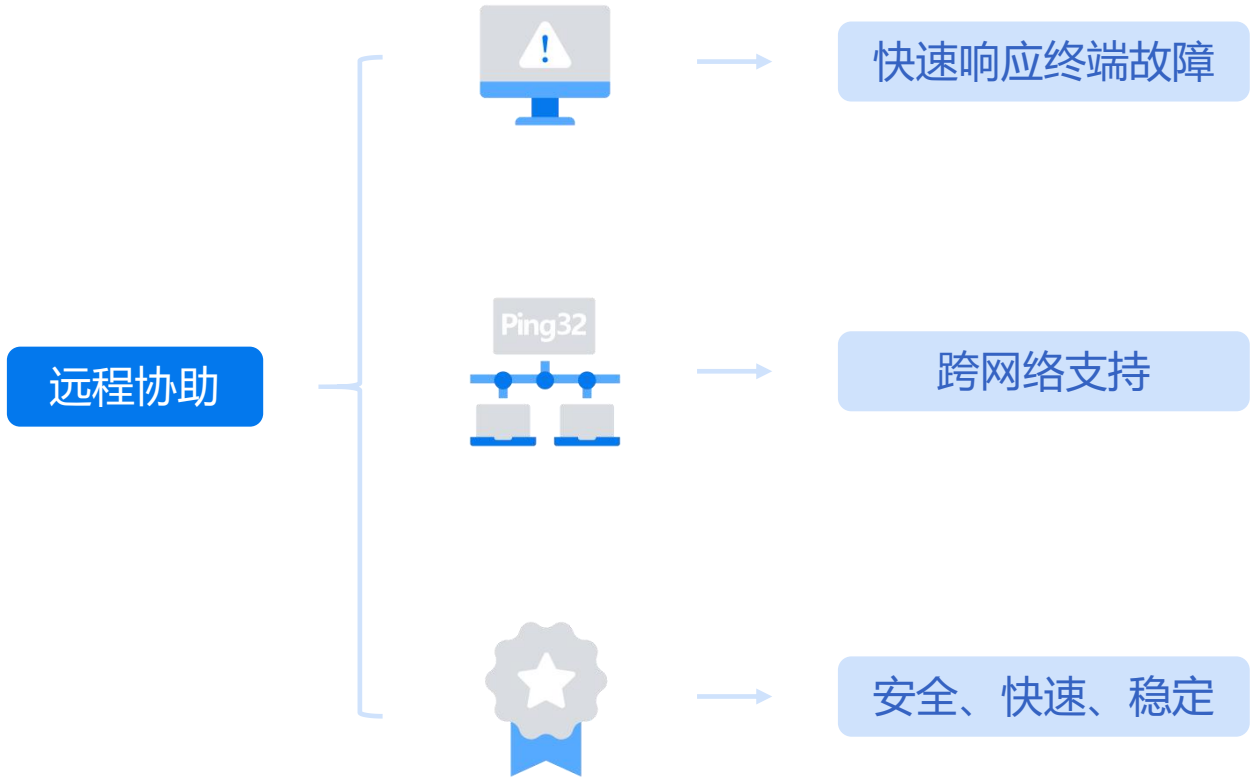
IT运维人员花费大量精力在简单的维护工作上，

效率低下，

如何提高运维效率？

(2)

远程协助：媲美商业产品的跨互联网远程协助服务



工单管理：应用场景

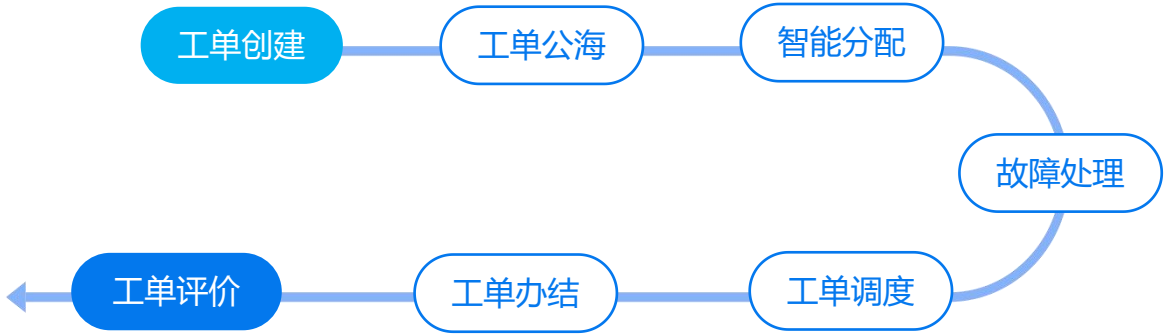
如何建立员工与IT运维人员高效的交互平台，
及时响应终端故障，
提高运维人员的工作质量？

(3) 工单管理

智能分配 通过公正的随机分配算法，分配工单处理人。

工单公海 员工提交工单至公海，空闲运维人员可主动认领。

无缝流转 可一键将工单高效流转到其他处理人，协作沟通。



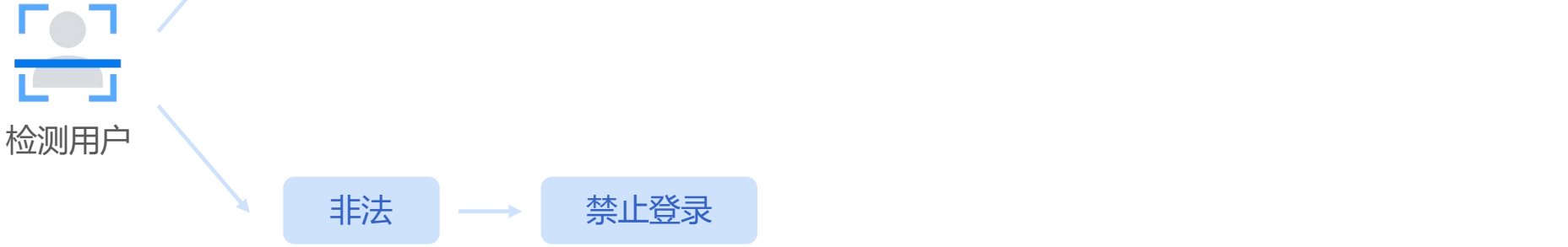
工单流转中每个步骤、每个节点状态都清晰可见，准确了解工单处理进度，确保处理质量。

身份认证：应用场景

如何审查用户登录的终端的过程，

从而确保用户拥有终端登录的权限?

(4) 身份认证：独立、多模式的身份认证服务



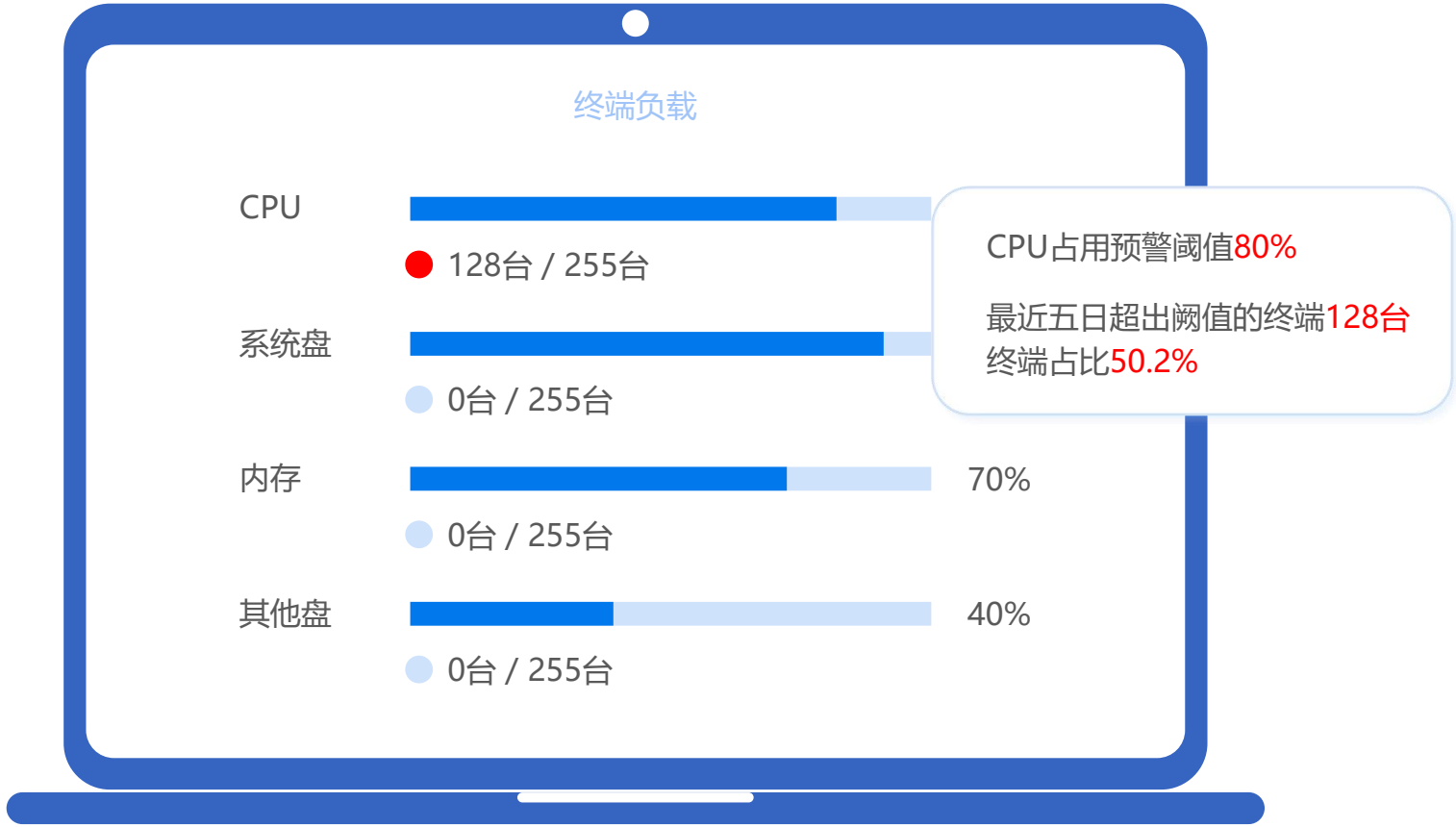
优势

终端负载：应用场景

如何快速定位终端各类资源使用状态?

(5) 终端负载

定位CPU、内存、磁盘等资源的使用状态，为计算机维护、更新迭代、故障解决提供依据



节能设置：应用场景

员工离开工位后办公电脑不锁屏不关机，

浪费能源，存在潜在的数据泄漏风险！

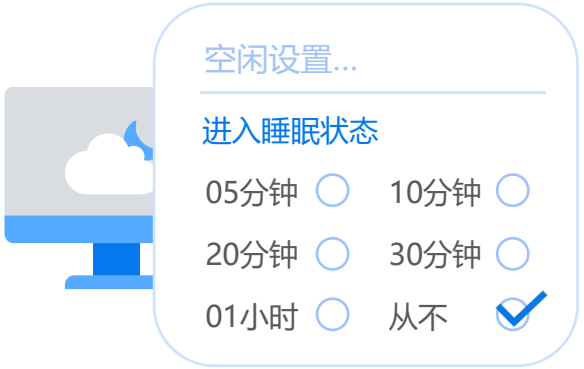
(6)

节能设置：制定合理电源计划

关闭显示器

锁定屏幕

睡眠时间



定时关机

桌面个性化：应用场景

从非官方或不可信的网站下载桌面个性化资源，
如主题、图标、插件等，可能会携带恶意软件，
存在数据安全和隐私泄露的风险！

(7)

桌面个性化：统一管理终端桌面设置

收益

助力企业IT系统高效运维，
减轻运维人员工作压力。

06 生产力

智能进行详细的梳理和分析

生产力

01 生产力评估

智能统计、分析员工使用电脑的时间，并根据员工行为自动划分高效工作时间、低效工作时间。

02 生产力排行

通过获取员工使用的软件，以及每个软件所使用的独立时间，计算员工的生产力评分，形成生产力效率排行榜。

03 活动分析

对所有终端的软件应用类型进行统计，并根据类型划分使用时长及占比，以软件类型维度分析整体的活跃度和评分。

04 时间跟踪

可以查看所有终端的软件应用及详细信息，并可对每个应用自定义个性标签，形成更智能化的统计图表。

(1)

生产力

应用软件使用

提供多种粒度的软件使用记录，包括：进程活动记录、窗口活动记录等，精确计算机指定时间内进程的启动。

(2)

生产力

网站停留时间

将网络流量过滤引擎的原始 HTTP(s) 记录与用户界面的活动记录进行关联，洞察眼MIT系统可以精准记录用户真实浏览网站的时间。

(3) 生产力

鼠标、键盘操作

捕捉用户鼠标、键盘操作识别用户活动状态，为工作效率评估增加另一维度。结合当前应用状态，判断用户是否在高效工作。

07 文档透明加密

强力守护企业核心知识产权

文档透明加密

01 透明加解密

基于驱动层过滤技术，采用高强度加密算法，对用户通过指定授权软件创建的文件实时无感知加密，访问时自动解密，文件加密后离开授信环境无法访问。

02 半透明加解密

终端通过指定授权软件访问加密文件时透明解密，加密文件进行修改、保存后仍是加密状态。终端新建的文件不加密，非加密文件操作不受管控。

03 手动加解密

终端用户可手动将文件加密处理，防止误操作、外部窃密导致的数据泄漏。

04 新建文件加密

支持对指定路径下、指定文件类型的新建文件实时监控落地加密。

05 全盘加解密

实时或定时扫描终端已存在的文件进行自动加密、解密处理。

06 智能加密

洞察眼MIT系统将敏感内容识别技术与文档透明加密技术结合，实时扫描终端新建文件，对包含敏感内容的文件进行加密（需采购敏感内容扫描模块）。

文档透明加密

07 文档权限 - 安全域

根据企业组织机构或者指定一组终端用户创建文件安全域，不同安全域内文件相互隔离，控制文档流转范围，确保文档在特定范围内使用。

08 文档权限 - 密级

根据终端用户自身属性，洞察眼MIT系统可为其赋予密级等级，使得用户只能访问小于或者等于自身密级的加密文件。

09 邮件白名单

在邮件白名单地址范围内的邮箱（支持标准协议）通过Foxmail、Outlook等邮箱客户端发送加密文件时自动解密。

10 邮件审批解密

外发邮件时提交审批流程，审批通过后邮件外发的密文被自动解密;
邮件审批流程支持指定发件人邮箱账号(依赖SMTP模板配置)。

11 文档安全外发

文档安全外发结合透明加密、权限管理等技术，设置需要外发的加密文档的使用权限，并且支持回收外发包，在不影响正常办公的同时防止二次泄密。

12 流程审批

审批流程支持文件解密审批、邮件解密审批、文档安全外发审批、离网补时审批等。

文档透明加密

13 剪切板管控

控制授权软件与非授权软件之间的剪切板使用权限，可限制禁止密文复制到明文，密文之间允许复制等权限。

14 解密网关（软件）

针对各应用服务器（如OA、ERP、PLM等）实现文件上传自动解密，下载自动加密。

15 离网办公

针对离网人员或网络故障等原因引起的客户端离线，设置用户可以可发起离网审批，确保终端密文在出差过程中保持可用状态，不影响日常办公。

16 U盘客户端

插入U盘客户端即可打开加密文件，移除U盘客户端则无法打开加密文件，同时提供透明、半透明加解密功能。

17 加密文件扫描工具

启用后终端可以扫描指定位置或指定类型的加密文档或文件夹，并且根据策略设置决定是否具备解密权限。

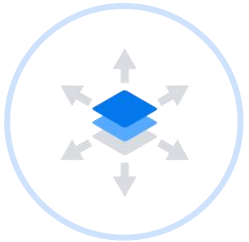
18 手机APP

支持通过洞察眼MIT系统手机APP处理终端用户提交的文件解密、外发等审批；支持加密文档预览、预览时支持显示附加水印。

问题1

企业内部文档以明文存储，文档一经发出，脱离后企业无法有效管控，该如何从根源上加以预防？

员工有意或无意泄漏，造成不可预估的损失

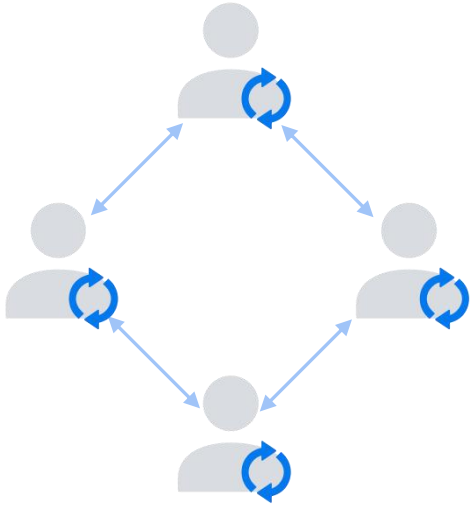


文件发给客户后，被二次泄密

出差等离网人员如何安全使用内部文档

（1） 透明加解密

合法用户正常使用



合法
出口

透明——加密过程自动完成、
不影响用户使用习惯

敏感文档 → 加密算法 → 密文

非法
出口

非法离网打开乱码

竞争对手窃密

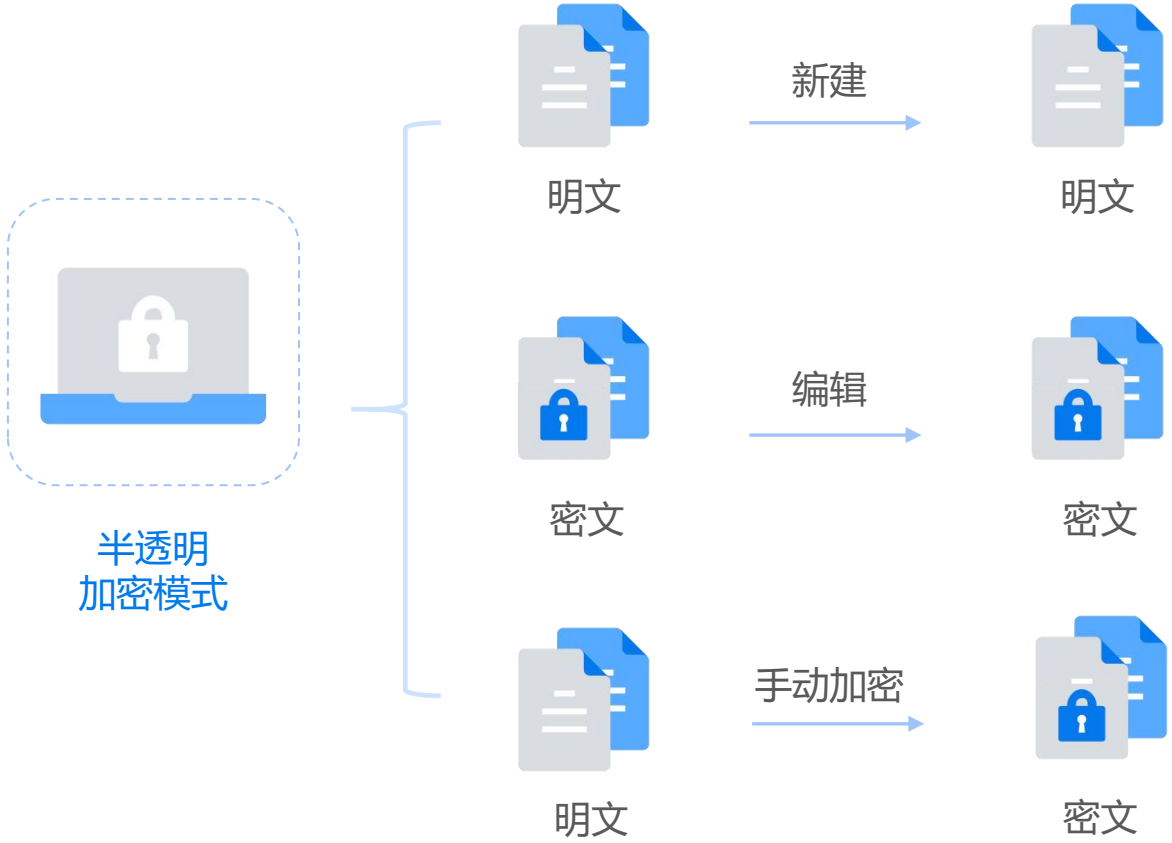
有意无意泄漏

设备丢失泄密

文档透明加密

通过AES等加密算法，对用户通过指定受控程序创建的文件实时无感知加密，访问时自动解密，离开授信环境无法打开文件。

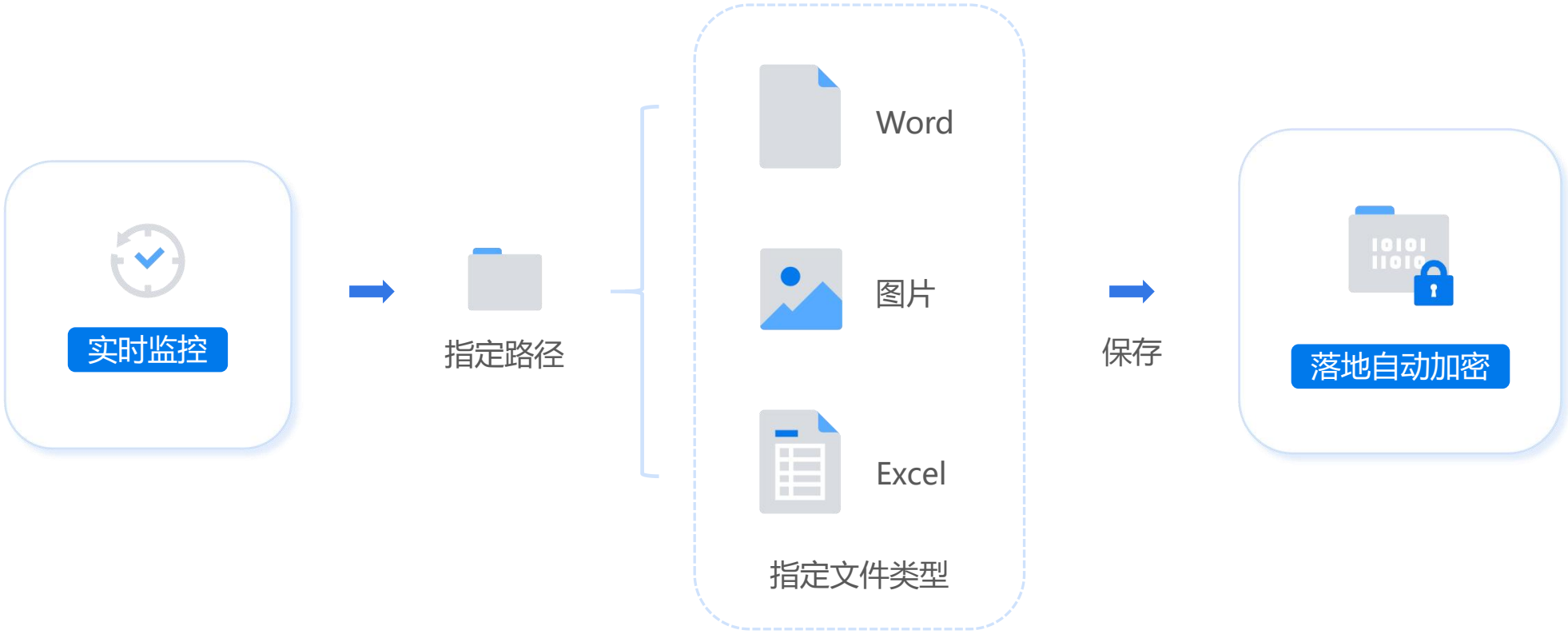
(2) 半透明加解密



- 非核心部门在需要的情况下可以正常使用核心部门加密文档。
- 非核心部门创建的文件不被加密，避免过度管控影响工作效率。

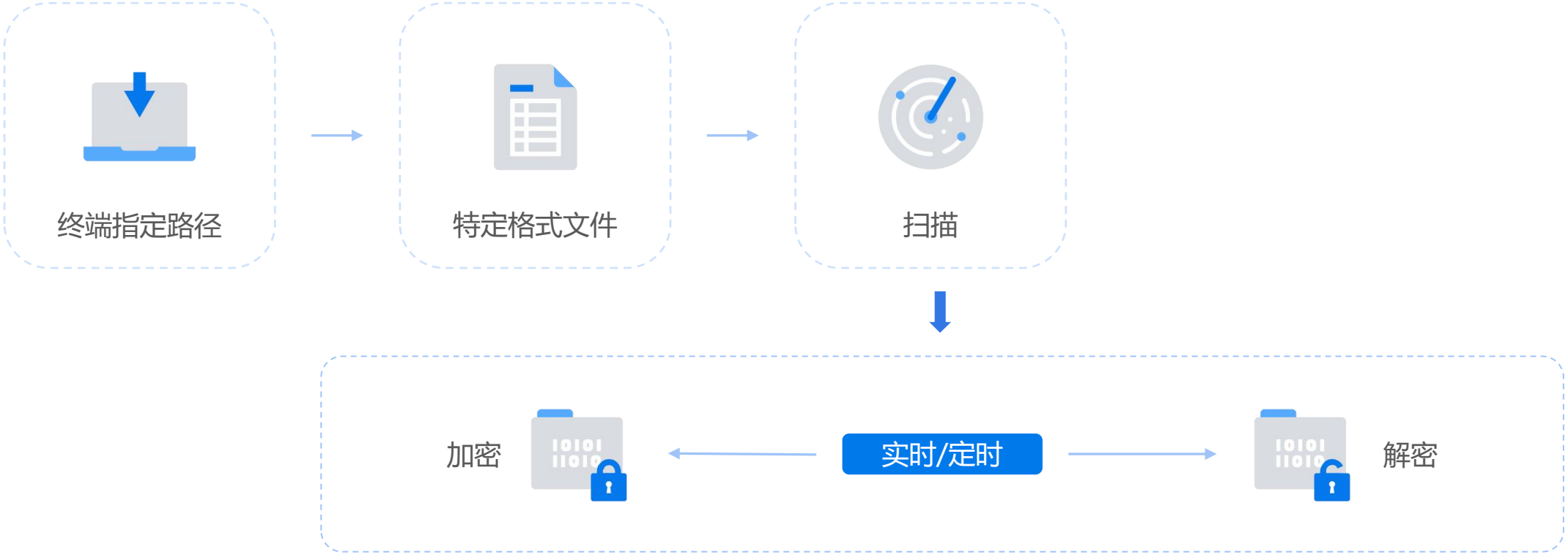
(3) 新建文件加密

实时监控终端指定路径，对存储在目录下的指定类型的文件落地自动加密。



(4) 全盘加解密：历史文件扫描加密

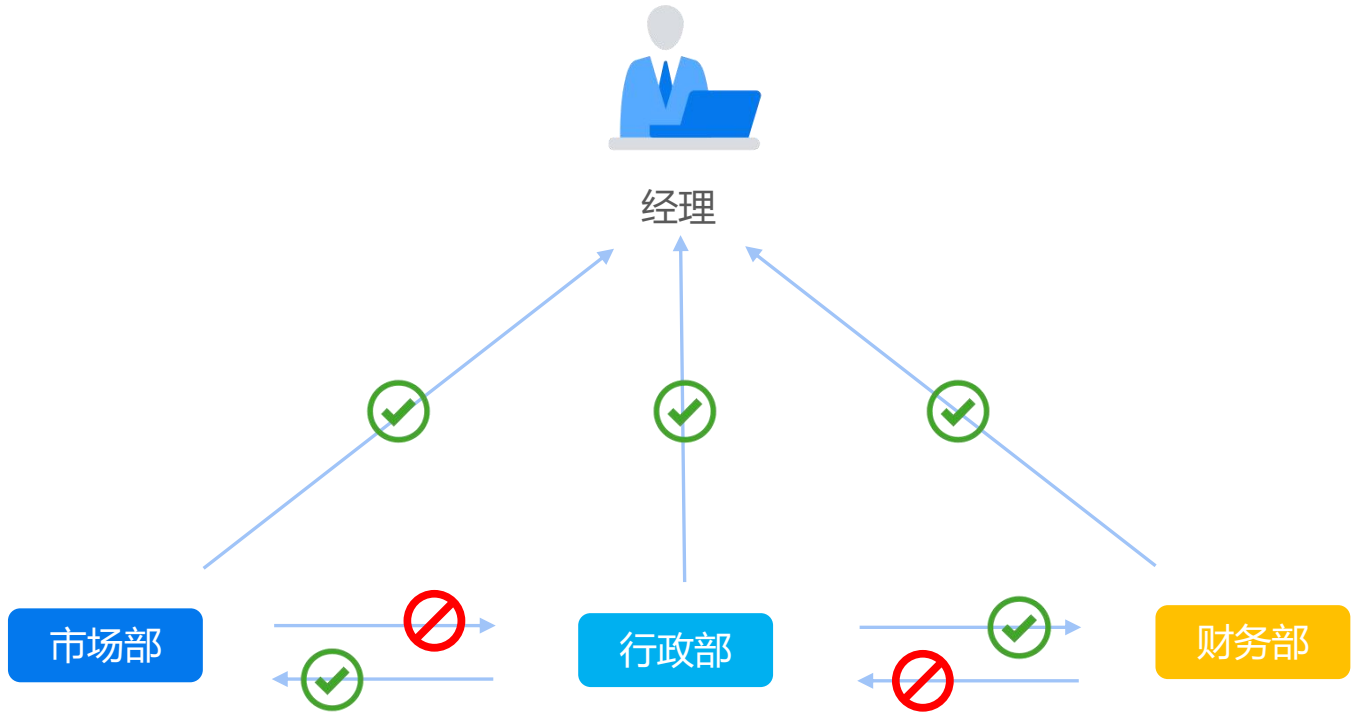
对终端指定路径下特定格式的文件扫描，并进行实时或定时的文件加密\解密操作。



(5) 智能加密

- 将敏感内容分析与文档加密技术结合，实时或定时扫描终端文件，对全网涉密信息进行针对性防护。
- 通过数据分类库可以建立属于自己的核心数据识别体系

(6) 文档权限-安全域



安全域

设置不同文件安全区域，以实现用户只能透明加解密指定的一组或者几组安全域内的加密文件，确保文档在特定范围内使用。

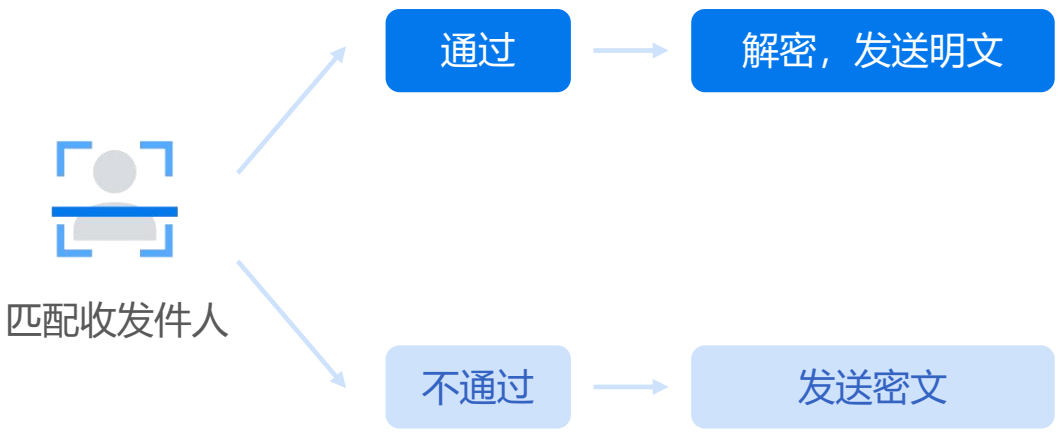
(7)

文档权限-密级

密级　对不同用户赋予不同的密级权限，密级权限低的用户无法打开高密级文档，确保文档权限安全可控。

(8)

邮件管控



邮件白名单

在可信的邮件收发地址内发送加密文件时自动解密。

发送邮件

提交邮件审批，审批通过可发送邮件，并且解密文件。

解密审批

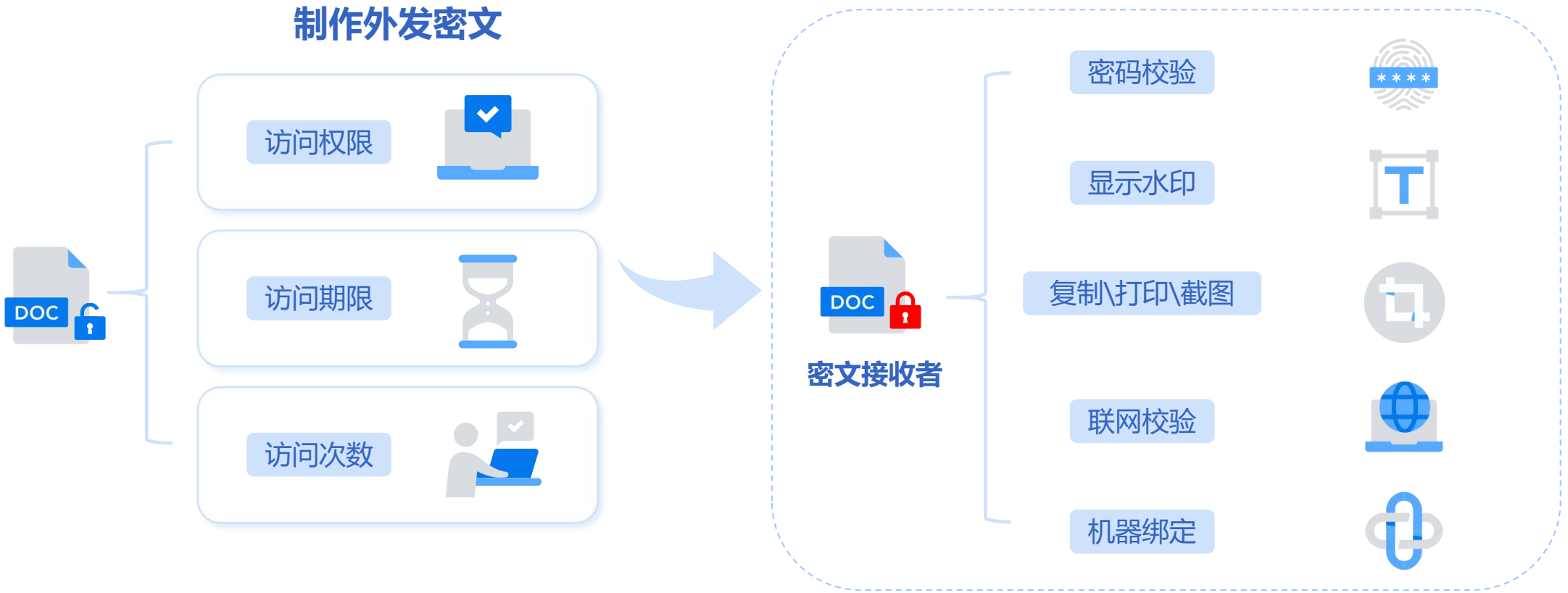
通过提交文件解密审批，在终端将文件解密后外发。

手动解密

用户可自行进行解密操作，

(9)

文档安全外发



授予外部人员的文件使用权限。

访问外发文件显示水印，震慑拍照。

无需在自己的电脑上安装任何插件即可访问。

（10） 流程审批

审批类型

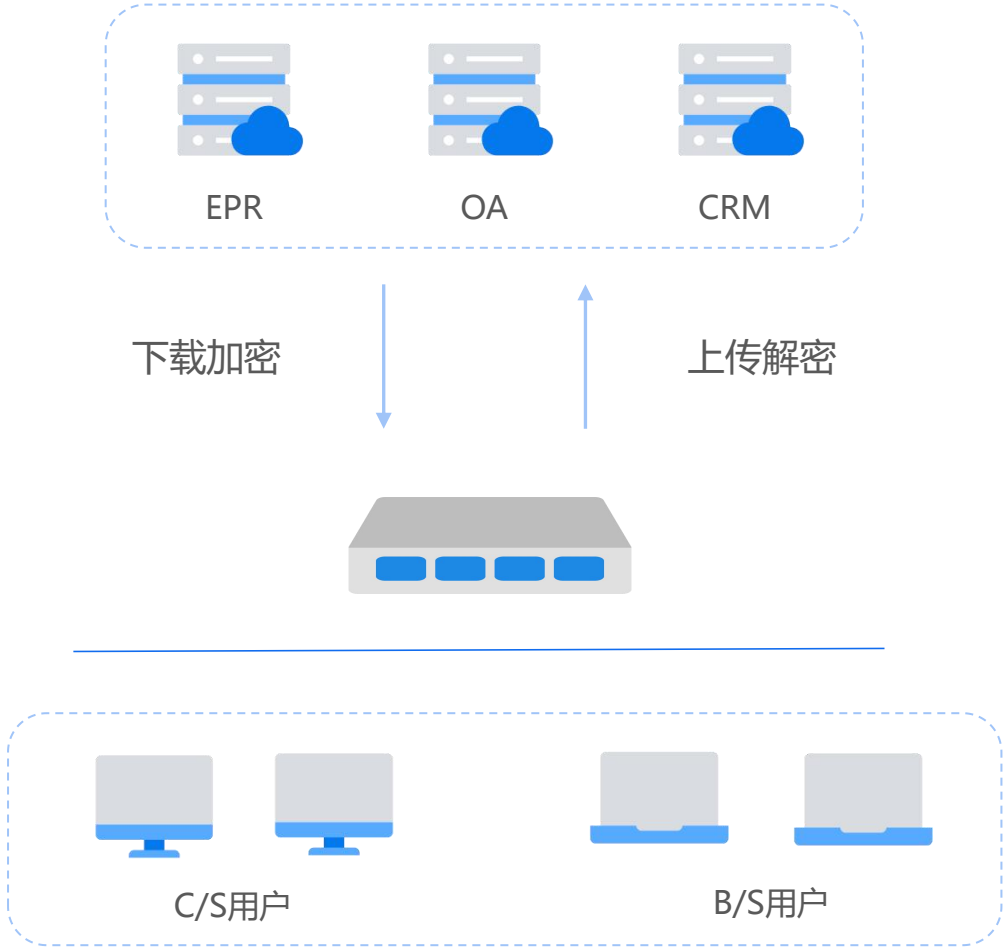
- 文件解密
- 调整安全属性
- 邮件解密
- 文件外发
- 离线补时

审批方式

- 手机APP
- 洞察眼MIT系统控制台
- 与指定业务系统集成

- 支持在Android\iOS审批端预览加密文件

（12） 解密网关



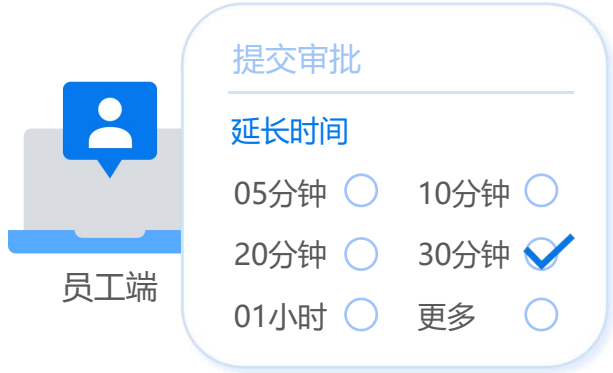
- 支持PLM、PDM等C/S架构的应用系统
- 支持OA、ERP等B/S架构的应用系统
- 实现数据上传到业务系统自动解密，下载自动加密
- 无需改变企业原有网络架构

(12) 离网办公

离线时长

预先设定离线时长，当客户端和服务器断连时，确保员工可正常使用密文，保证正常办公状态。

超时审批



员工离网办公超出预期时间时，可通过超时审批申请延长离网时间，确保业务持续运行。

(13)

U盘客户端

管理员

- 使用权限
- 解密权限
- 绑定终端

U盘

- 行为审计

管理员

- 居家办公
- 合作伙伴

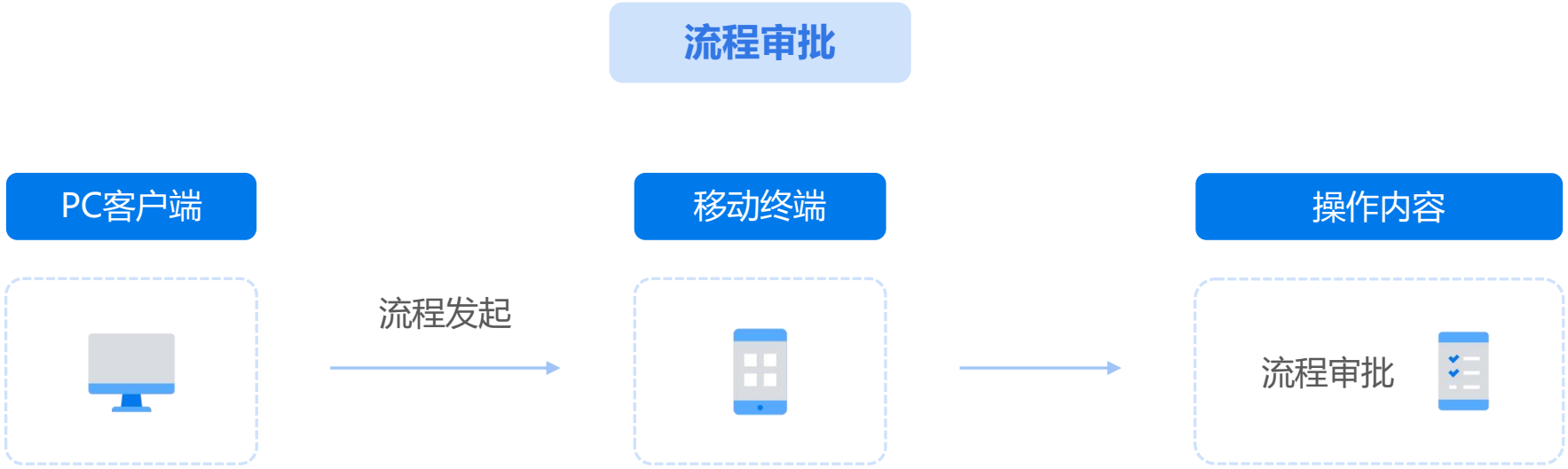
U盘加密系统

无需安装加密客户端，只需要插入洞察眼MIT系统安全U盘，即可实现外部电脑正常使用加解密功能。

使用权限控制

支持设置安全U盘使用时长、U盘绑定指定终端、防止U盘丢失导致内部信息泄密。

（14）手机APP



审批管理：

用户可通过移动设备在线处理审批工作（包括解密申请、离线申请、文件外发申请、安全属性调整申请、邮件解密申请），且审批消息实时推送，保证审批及时性。

08 智能报表

对海量数据进行智能处理、分析

智能报表

洞察眼MIT系统聚合报表支持将不同类型的统计数据导出成便于查阅的载体格式：比如打印到A4纸、导出成PDF、HTML等形式。

洞察眼MIT系统聚合报表支持根据部门对各报表进行筛选数据，轻松从海量数据中提取出特定部门的相关信息，快速生成各部门的专属报表。

洞察眼MIT系统报表系统支持聚合报表，可以将多项风险数据整合在一起，生成一个综合的、全面的报表，同时支持拖拽操作可以将报表中的元素自由排列和组合，生成各类定制化的报表。

洞察眼MIT系统聚合报表引入推送报表功能，支持灵活的推送报表模版，用户可以通过创建推送模版，为公司不同的人员定制个性化模版，根据需求自定义设置推送频率、报表内容、报表格式等。

洞察眼MIT系统聚合报表提供了在打印或导出报表时添加水印，水印支持自定义设置，如果报表被非法泄露，企业可以通过水印信息追溯到泄露的源头，从而采取相应的法律措施。

09 敏感内容分析

对海量数据进行智能处理、分析

敏感内容分析

01 数据分类库

强大灵活的数据分类规则库，将散落在终端各处以及实时产生的文本文档进行归类。

02 敏感内容扫描

通过敏感内容扫描策略，可以扫描指定终端上的文档，分析是否包含指定的敏感数据类别。

03 增强的文件外发管控和审计

对包含敏感内容的文件传输行为可以进行告警、阻断、审计。

04 增强的电子邮件管控和审计

对包含敏感内容的电子邮件发送行为可以进行告警、阻断、审计。

05 增强的剪切板审计

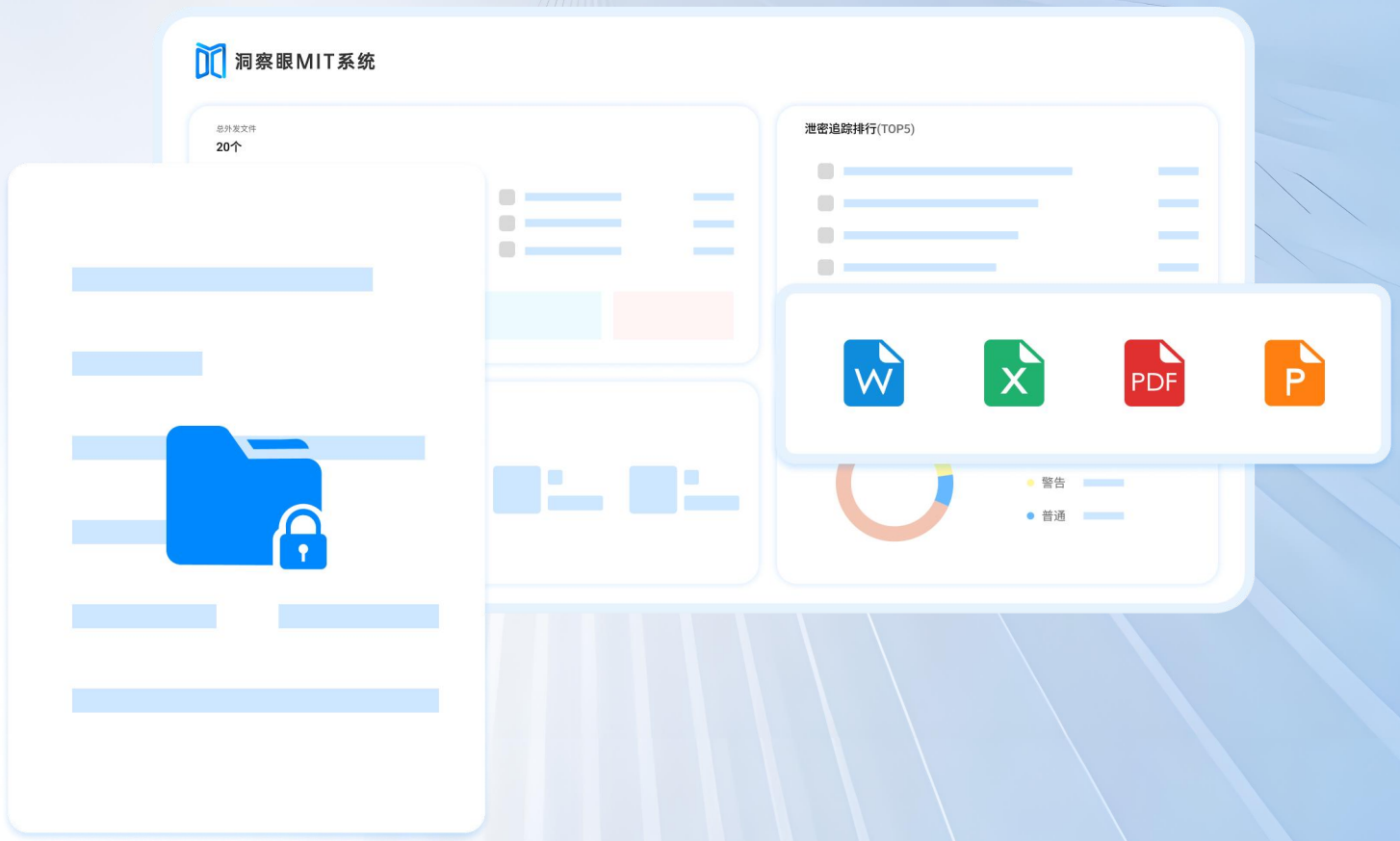
分析剪切板内容，对包含敏感内容的剪切板使用行为进行审计。

(1) 数据分类库

对动态数据、静态数据分类分级，适用于不同场景的数据加密、脱敏、审计管理需求。

(2) 敏感内容扫描

对含有敏感内容的数据流转时可进行审计或阻断，敏感数据进行统一加密处理。



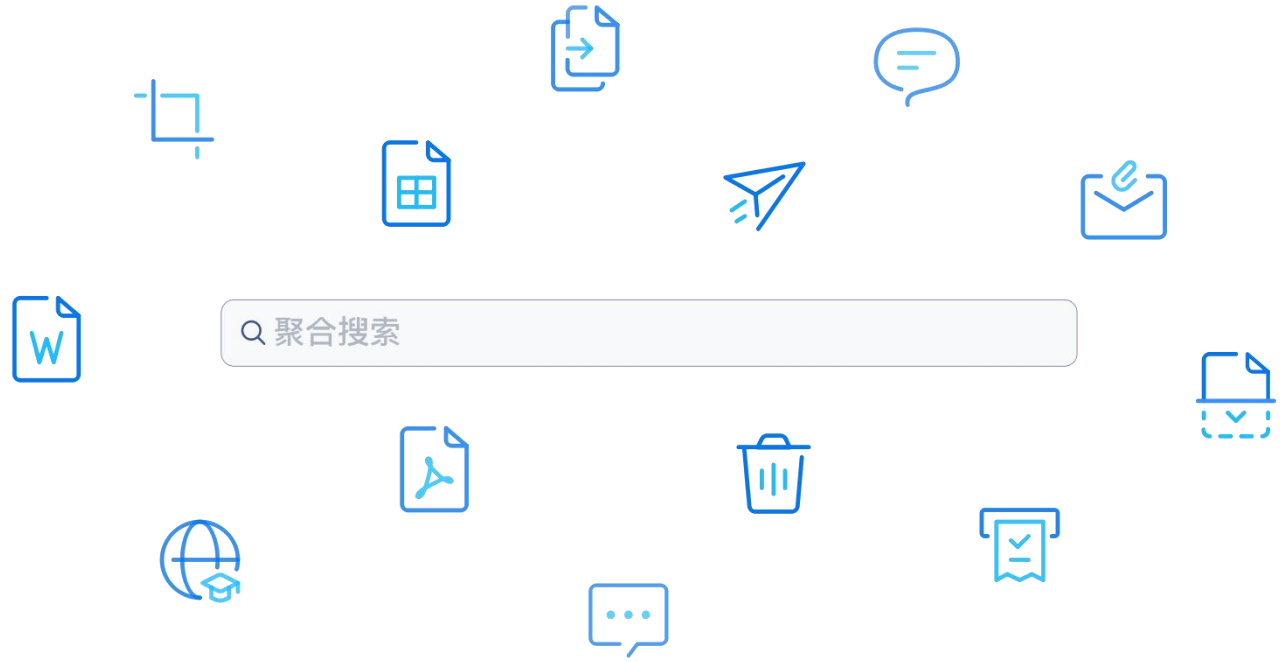
10 聚合搜索

毫秒级搜索展现，开启搜索新境界

问题1

从100条事件记录里，找到安全风险事件并非难事。

但是如何从亿级的海量记录里快速定位到安全异常事件，一直是一个巨大的挑战！



文档透明加密

01 聚合搜索

基于高性能、分布式的搜索引擎构建，集中存储、管理、分析洞察眼MIT系统各类记录事件。

02 审计记录搜索

支持将网站访问记录、即时通讯记录、邮件审计记录、屏幕截图等记录、事件进行聚合展示。

03 文档内容搜索

支持对Office文档、PDF文档、图片内容进行识别搜索展示。

04 图片内容搜索

支持OCR识别技术，识别PNG、JPG等格式的图片内容进行搜索展示。

05 压缩包穿透搜索

支持压缩包穿透技术，对压缩包中原始文件进行搜索展示，支持多层穿透。

06 组合条件搜索

支持通过关键词、正则表达式等多种条件组合进行搜索及筛选。

功能特性

整合多元信息源

支持分布式部署，轻松进行集群式部署。

支持高可用，当某一节点发生故障时，支持自动实现故障切换。

支持PB级记录的管理，毫秒级展现搜索结果。

支持搜索图片中的内容，以及扫描型PDF文档中的内容。

支持搜索Office文档，PDF文档中的内容。

支持设定多种条件组合搜索及筛选。

支持将各类审计记录、事件进行聚合展示。

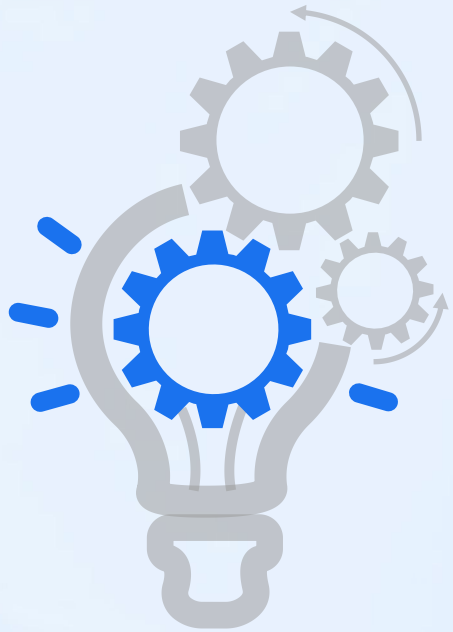
支持穿透压缩包，搜索压缩包里的文档、图片内容。

支持开放搜索接口。

11 AI Pro

AI Pro服务

洞察眼MIT系统支持与云平台深度联动，实现各类数据的实时更新，如泄密途径的增强型分析、软件分类、软件版权属性等，全面提升数据分析与安全管理能力。



感谢观看

THANK YOU