360数字安全

数 字 安 全 的 领 导 者

构筑纵深防御体系
实现大规模企业内外部安全

——360数字安全医疗行业终端安全解决方案

目录 | CONTENTS

PART 01

医疗行业终端安全背景

勒索病毒保持高位攻击态势

2021-3
台湾宏碁电脑遭遇Revil勒索攻击

2021-4
美国华盛顿警察局遭受Babuk勒索软件攻击

2021-5
美国最大输油管道公司Colonial Pipeline遭受勒索软件攻击

2021-7
西班牙电信运营商MasMovil Ibercom遭受Revil勒索攻击

2021-9
美国太平洋城市银行遭受AvosLocker勒索软件攻击

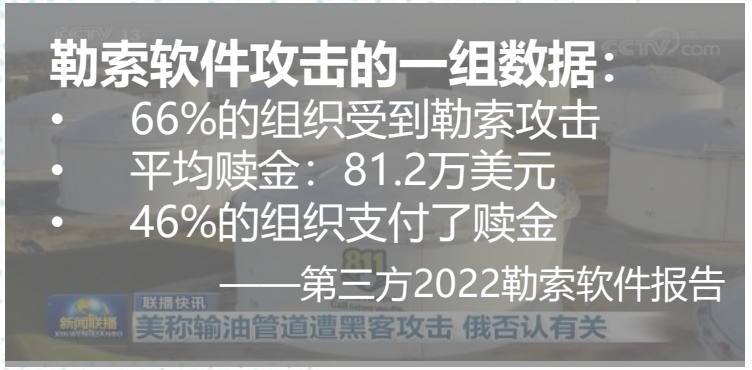
2022-8
我国知名财务软件公司遭受TellYouThePass勒索软件攻击

2022-12
我国知名制造业车企蔚来汽车遭受勒索软件攻击

勒索软件攻击的一组数据：

- 66%的组织受到勒索攻击
- 平均赎金：81.2万美元
- 46%的组织支付了赎金

——第三方2022勒索软件报告



勒索病毒对行业客户提出巨大挑战

医疗行业成为勒索病毒主要攻击目标

2017	2018	2019	2020	2021至今
WannaCry爆发	**数百家医疗机构检出勒索病毒**	**精准化、高质量狩猎**	**长期演变、趋于成熟**	**门槛降低，成功率高**
2017年爆发的WannaCry勒索使勒索病毒正式被大众熟知，据美国电信巨头Verizon统计，2017年勒索病毒在医疗行业所有的恶意软件攻击中的占比达到惊人的85%。	根据《医疗行业勒索病毒专题报告》显示，我国三甲医院中，有247家医院检出了勒索病毒。攻击者往往通过漏洞利用方式发起攻击。	GlobeImposter、Crysis为主的老牌勒索家族进行精准化、高质量的狩猎行动。出现赎金定制化，针对不同目标定制赎金数额。医疗行业受勒索病毒影响占全行业的7%。	总体感染情况较上年度略有下降，数据价值较高的传统企业、教育、医疗、政府机构遭受攻击最为严重。攻击更精准，不交赎金立即公开敏感数据。	出现RaaS（勒索软件即服务）模式，勒索攻击门槛降低，成功率提高，解密还原难度大。目前，每年全网遭受勒索攻击高达几千万次，医疗行业成为勒索病毒重灾区。

医疗行业终端安全管理现状

终端种类多

- PC、服务器、云桌面、医疗设备等终端种类繁杂，需要不同的管控策略，人工维护难度大，如何统一纳管。

终端故障多

- 老旧终端多，故障多，需要投入大量人力进行维护和故障排查，如何简化运维。

终端威胁多

- 病毒、ATP、钓鱼邮件，终端面临的威胁层出不穷，难以发现、难以防护、难以溯源。

数据易泄露

- 终端保存大量敏感数据，没有监测和拦截机制。

PART 02

终端安全管理系统介绍

同平台、多品类

同平台多品类的管理中心

360数字安全大脑

面向服务器

CDR

- 暴力破解
- 系统后门
- 文件删除
- 恶意扫描

与主机加固产品共存

对业务系统零干扰

面向终端

EDR

- 进程行为
- 文件行为
- 注册表行为
- 网络行为
- 系统行为

发现未知威胁攻击线索

面向服务器

CWPP

- 资产管理
- 安全检查
- 入侵防御
- 入侵检查

实战化防护

面向终端

EPP

- 资产管理
- 终端发现
- 漏洞补丁
- 桌面优化
- 终端审计
- 准入控制
- 防病毒
- 安全U盘
- 环境感知
- 轻量DLP
- 终端管控
- Win7盾甲
- EDR
- 软件管家
- 可视化大屏

多场景下的立体防护

360终端安全统一管理平台

产品功能架构图

360数字安全
数 字 安 全 的 领 导 者

热点场景

勒索防护 | APT防护 | 挖矿防护 | 攻防演练 | 重大事件保障 | 等保合规 | 数据安全

运营管理

终端安全统一管理平台 | 终端安全管理大屏展示 | 第三方对接 | API/SYSLOG数据对接 | 本脑、云盘、零信任联动

安全功能

资产管理

- 资产盘点
- 实名认证
- 终端发现
- 资产登记

威胁对抗

病毒查杀	漏洞修复	主动防御
勒索专防	宏病毒专杀	挖矿专杀
停服补丁	文档备份	文档恢复
主机加固	主机CDR	终端EDR

合规管控

外设管控	网络防护
违规外联	移动存储
桌面加固	进程管理
软件管家	终端审计

安全自助管理

弹窗防护	垃圾清理
开机加速	文件粉碎
能耗管理	隔离沙箱
流量管理	桌面助手

安全接入

- NAC准入
- 802.1X准入
- Portal准入
- DHCP准入
- 安全检查

数据安全

- 敏感信息审计
- 文件外发防护
- 文件智能备份
- 数字水印
- **安全U盘**

数据支撑

威胁情报 | 云端样本库 | 知识库 | 设备库 | 威胁图谱 | 终端行为数据

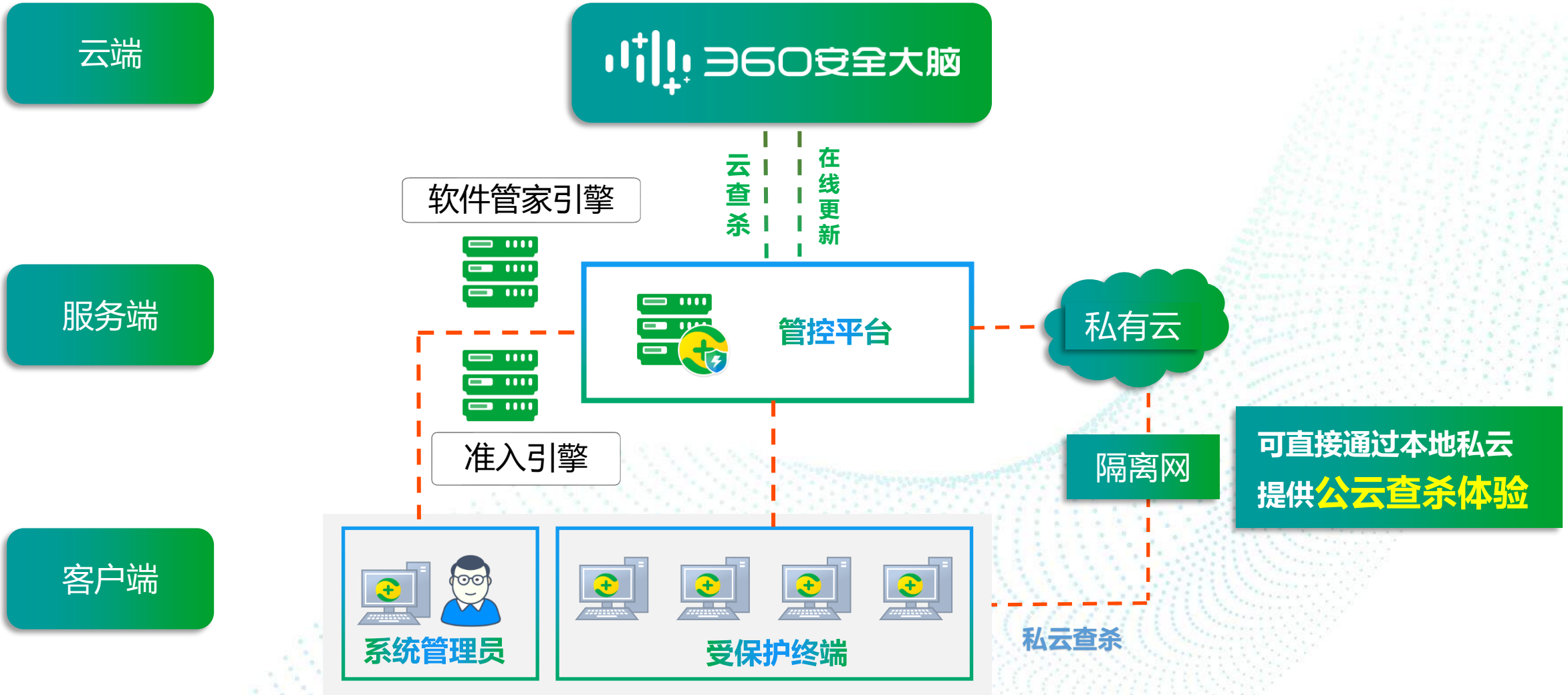
核心技术

云查杀引擎 | **微补丁修复** | **冰刃安全虚拟机** | **信创专杀引擎** | **WIN7专项加固**

端点类型

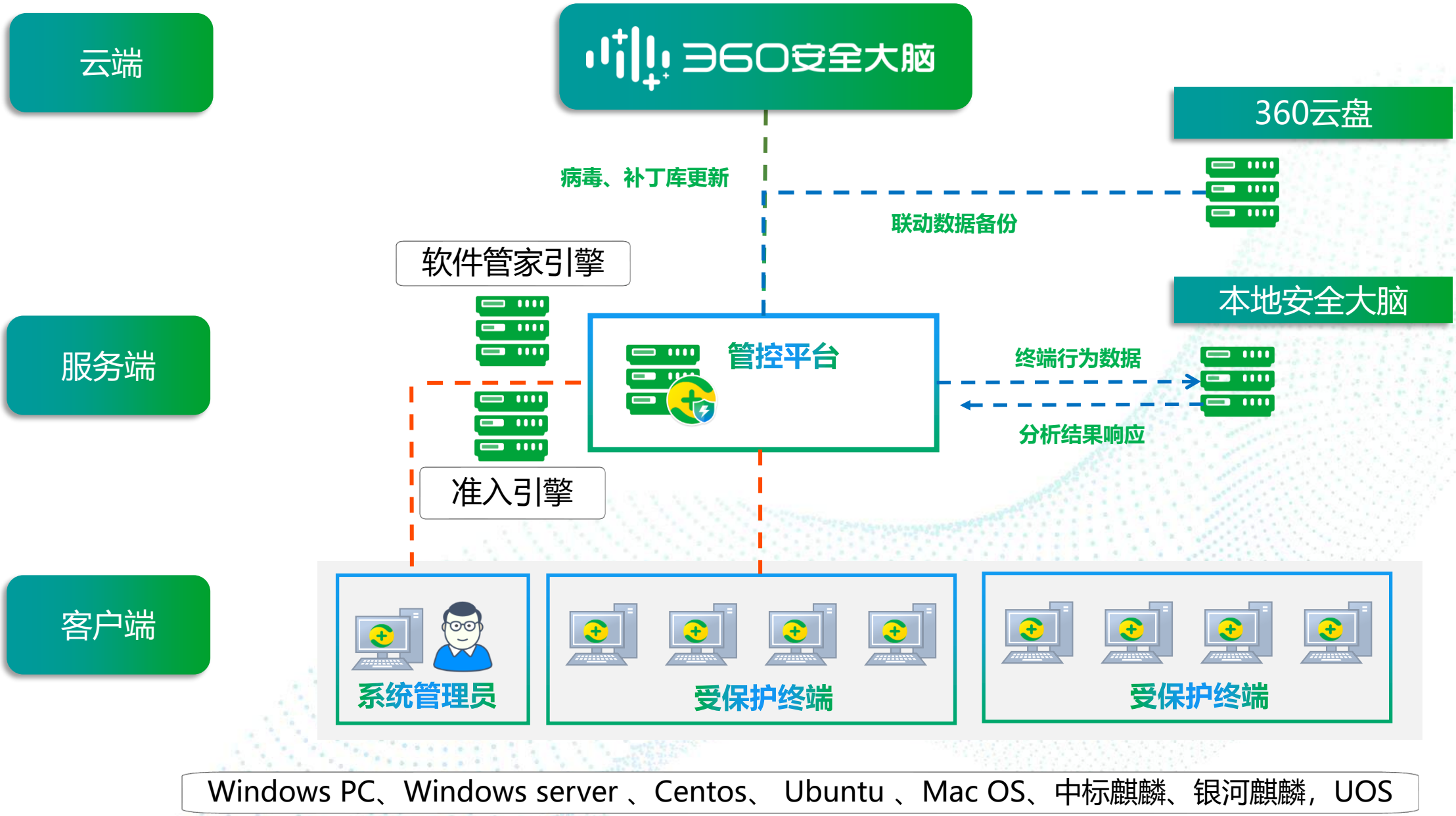
Winpc/WinServer | Linux | MacOS | 信创终端

产品系统架构



Windows PC、Windows server 、Centos、 Ubuntu 、Mac OS、中标麒麟、银河麒麟，UOS

产品系统架构-EDR



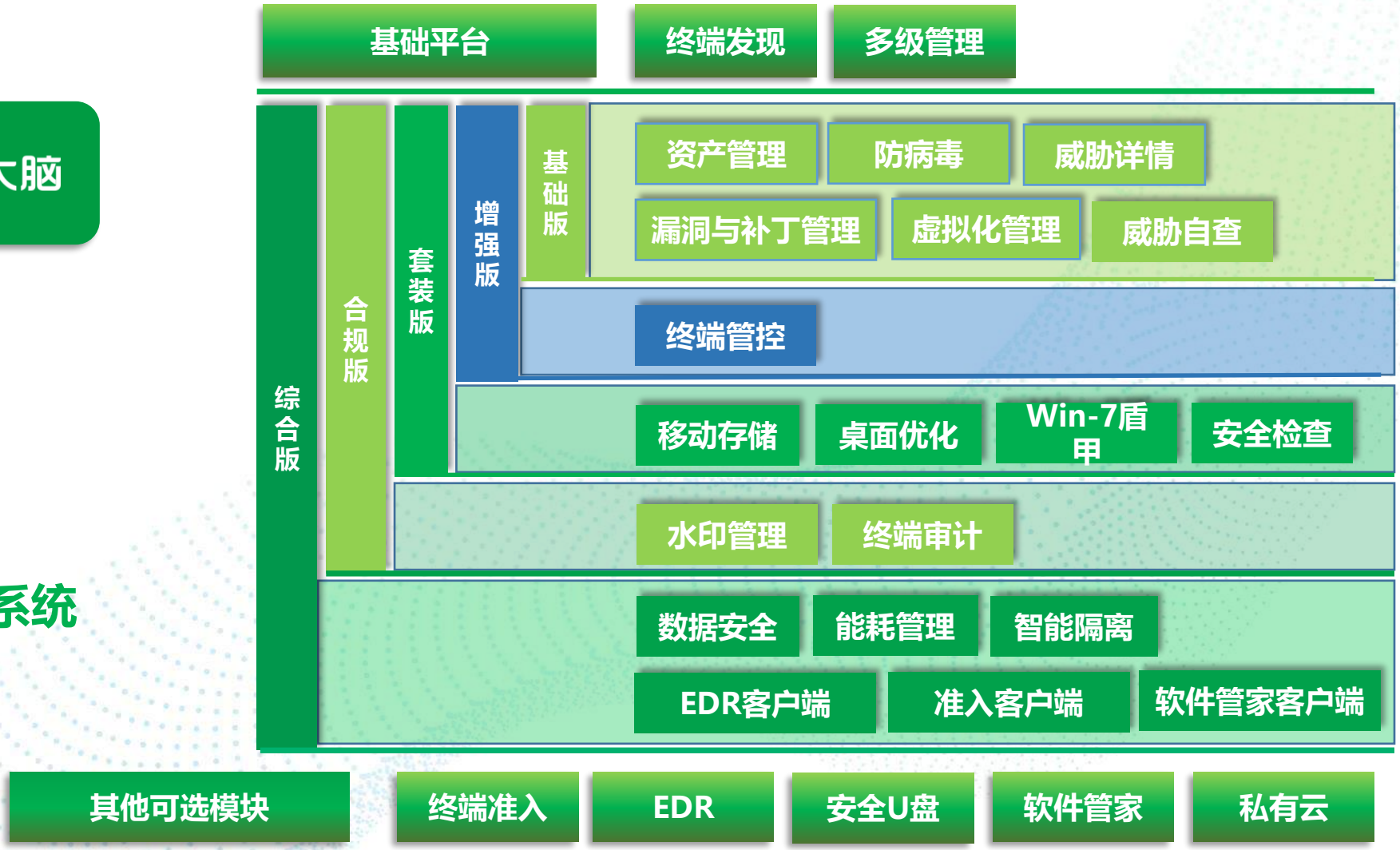
Windows PC、Windows server 、Centos、 Ubuntu 、Mac OS、中标麒麟、银河麒麟，UOS

360终端安全管理系统-产品模块表

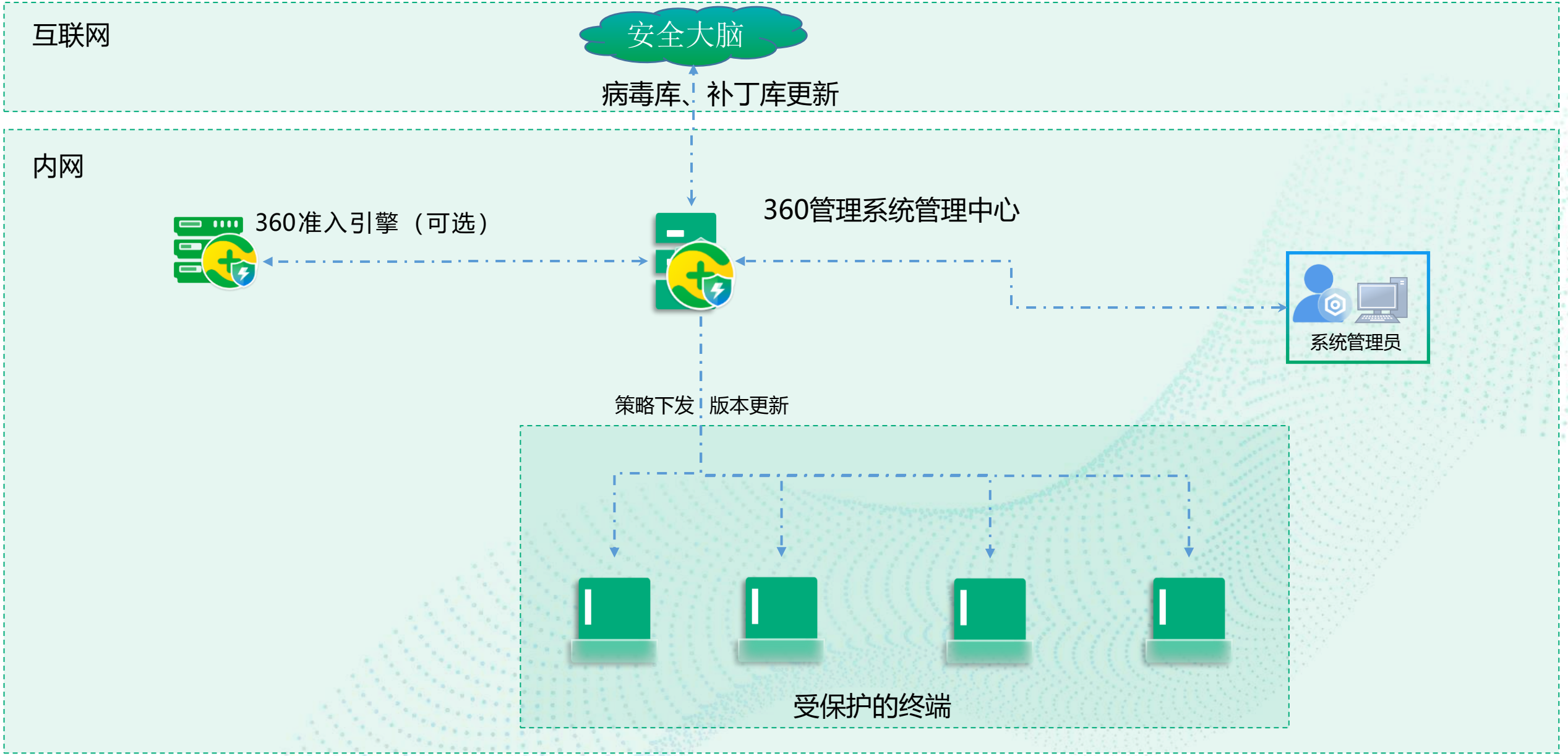
360数字安全 数字安全的领导者

360终端安全管理系统软件是在360安全大脑极智赋能下，以大数据、云计算、人工智能等新技术为支撑，以可靠服务为保障，集防病毒与终端安全管控于一体的企业级安全产品，帮助用户快速掌控全网终端安全状态，有效保障全网终端安全。

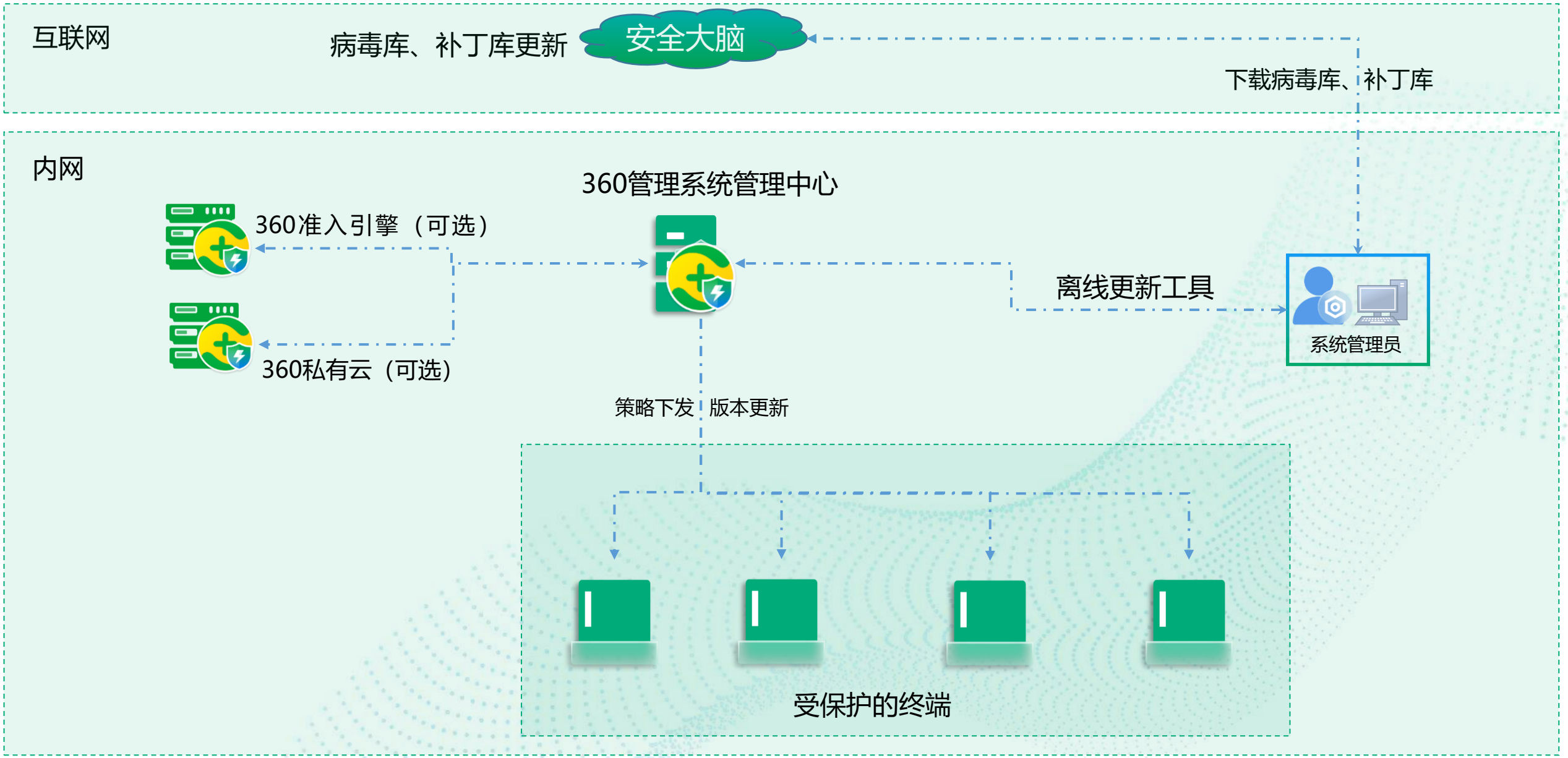
360终端安全管理系统



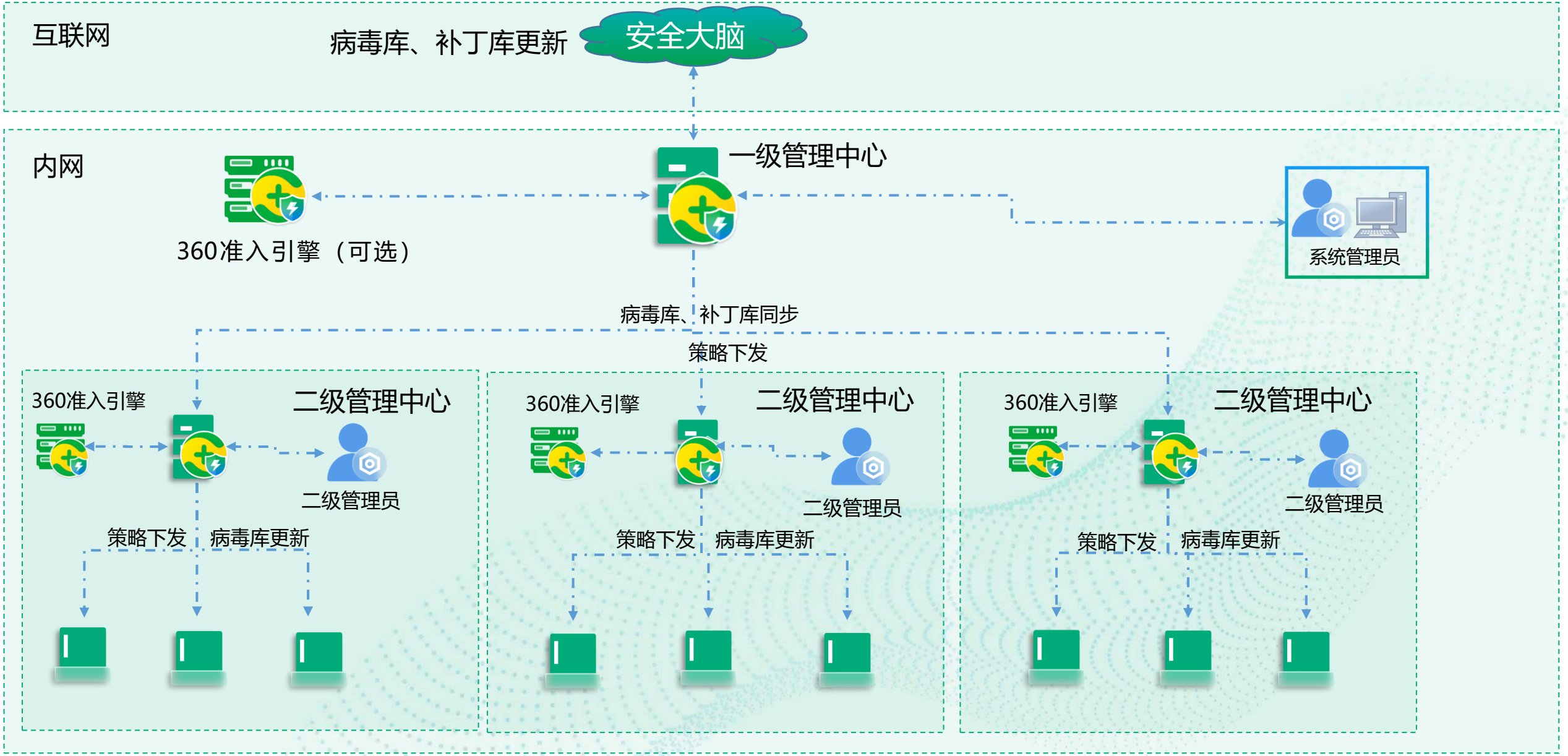
互联网部署模式


互联网
安全大脑
病毒库、补丁库更新
内网
360准入引擎（可选）
360管理系统管理中心
系统管理员
策略下发
版本更新
受保护的终端

隔离网部署模式


互联网
病毒库、补丁库更新
安全大脑
下载病毒库、补丁库
内网
360管理系统管理中心
360准入引擎（可选）
360私有云（可选）
离线更新工具
系统管理员
策略下发
版本更新
受保护的终端

多级署模式


互联网
病毒库、补丁库更新
安全大脑
内网
一级管理中心
360准入引擎（可选）
系统管理员
病毒库、补丁库同步
策略下发
360准入引擎
二级管理中心
二级管理员
策略下发
病毒库更新
360准入引擎
二级管理中心
二级管理员
策略下发
病毒库更新
360准入引擎
二级管理中心
二级管理员
策略下发
病毒库更新

PART 03

360EPP在医疗行业的应用

产品主要适用场景

勒索攻击防护

防免杀、防绞杀
诱饵文档
文档备份
文档还原
勒索解密
系统登陆双因子
。。。

终端统一纳管

Win、XC、Linux
统一纳管
防病毒
桌面管理
准入
统一管控
。。。

数据安全防护

敏感信息定义
敏感信息审计
移动存储拷贝阻断
网络共享拷贝阻断
文件打印阻断
。。。

360终端安全管理系统适用的场景

PART 3-1

勒索病毒专项防御场景

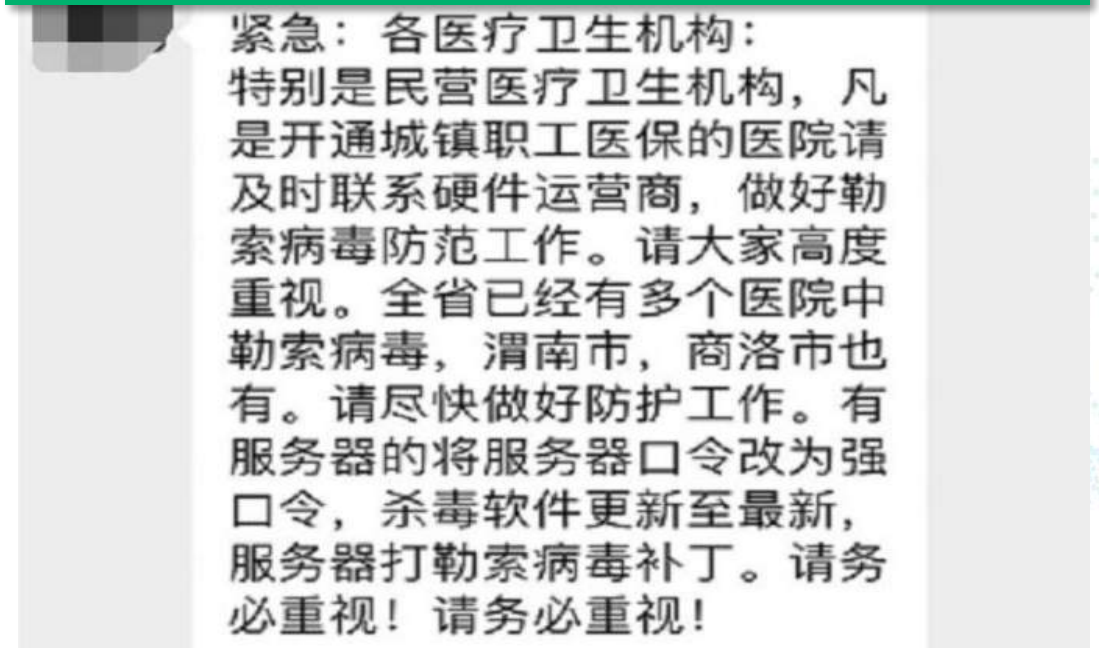
勒索病毒专项防御场景-医疗行业已成为攻击者实施勒索的最主要目标

360数字安全
数 字 安 全 的 领 导 者

场景需求

- 勒索查杀：出现勒索病毒攻击时，能够检测并处置内网终端的勒索病毒，阻断勒索病毒入侵和扩散，阻断勒索加密行为，避免内网终端失陷，避免感染扩散
- 文档挽救：被勒索病毒恶意加密的文件，能够提供恢复或找回机制，减少文档被破坏所造成的损失

某医疗机构通报：当地多家医疗机构出现勒索软件感染



紧急：各医疗卫生机构：
特别是民营医疗卫生机构，凡是开通城镇职工医保的医院请及时联系硬件运营商，做好勒索病毒防范工作。请大家高度重视。全省已经有多个医院中勒索病毒，渭南市，商洛市也有。请尽快做好防护工作。有服务器的将服务器口令改为强口令，杀毒软件更新至最新，服务器打勒索病毒补丁。请务必重视！请务必重视！

解决方案

- 从攻击前、攻击中到攻击后，在勒索病毒每一个主要的攻击节点定向查杀，让勒索病毒**进不来**（互联网入口检测阻断）、**散不开**（横向渗透阻断）、**加不了密**（主动防御实时感知勒索行为、勒索诱饵逆向感知查杀）、**加密也能恢复**（文档备份恢复、特定勒索家族解密），从而提供基于勒索病毒攻击链的完整解决方案

客户收益

- 勒索阻断：提供对勒索病毒专防专杀的全攻击链防御能力，能发现勒索病毒，阻断勒索加密行为，防止核心文件被勒索加密
- 事后恢复：具备文档恢复能力，文档被加密可以第一时间恢复，同时具备对部分重点勒索病毒家族的勒索解密能力，尽最大可能减少经济损失

勒索病毒专项防御场景-勒索攻击过程详解

攻击流程

勒索病毒 → 突破边界 → 病毒投放 → 加密勒索 ⇄ 横向传播

攻击技术手段

1

外网到内网的传播

- 钓鱼邮件
- 水坑站点
- Web漏洞利用/RDP

2

恶意程序安装和通信

- 下发提权程序
- 下发勒索加密钥匙
- 宿主信息提交

3

漏洞利用提权/加密勒索

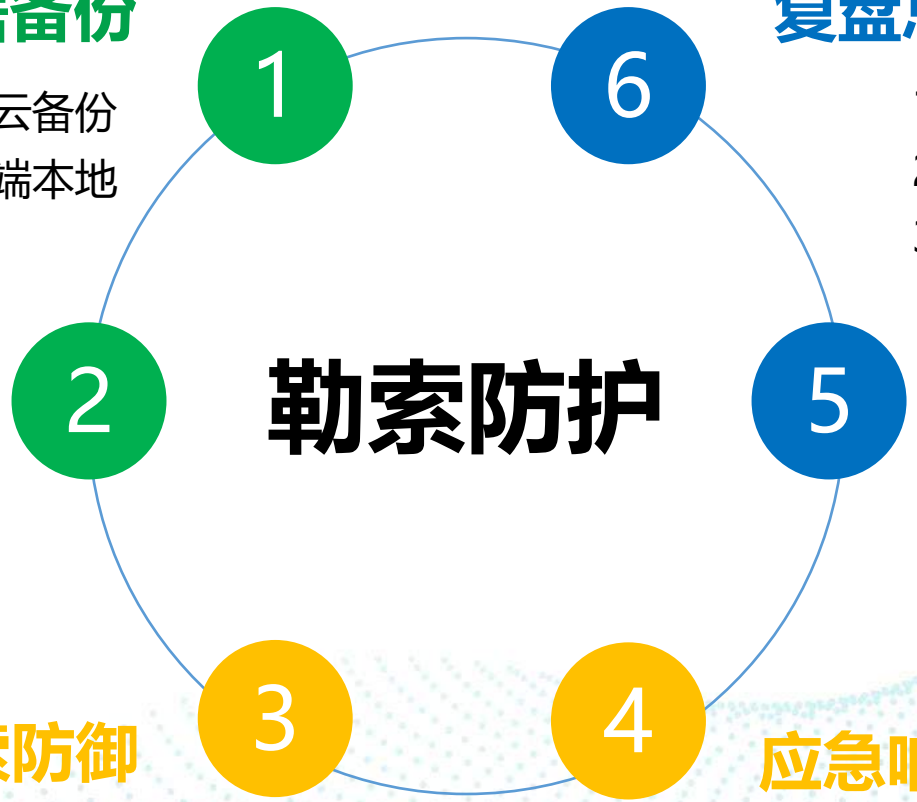
- 执行提权/加密程序
- 数据窃取
- 勒索弹窗或直接破坏

4

横向持续扩散

- RDP/SSH爆破
- 蠕虫式传播
- 系统利用传播

勒索病毒专项防御场景-勒索病毒攻击链防护



数据备份

1、云盘联动，办公文档自动云备份
2、本地备份，备份至办公终端本地

检测预防

1、勒索风险评估
2、勒索漏洞修复
3、终端安全加固

勒索防御

1、登录攻击防护
2、勒索防御引擎（诱饵文件等）
3、文档图片防护
4、高风险远程登录防御

应急响应

1、终端扫描上报
2、勒索病毒查杀
3、终端远程服务紧急关闭
4、终端紧急隔离（解除隔离）

备份恢复

1、云盘数据还原
2、本地备份文件还原
3、勒索文件解密（勒索解密）

复盘总结

1、文件备份建议
2、安全加固建议
3、勒索风险评估

勒索病毒专项防御场景-多引擎查杀，实现已知各类病毒的快速根除

多引擎查杀功能，充分发挥360在恶意代码对抗领域的深厚积累，提供查杀任务管理、本地多引擎查杀、云查杀等功能，构造立体协同检测机制，可以对木马蠕虫/恶意软件/挖矿木马/勒索病毒高危漏洞利用攻击等实现持续有效对抗，提升终端整体防病毒能力。

查杀任务管理

- **本地优先策略**：优先选用本地扫描方式进行恶意代码查杀，若遇到未知病毒，发送到云端查杀；
- **云查杀优先策略**：优先选用云端查杀，提升检出率与检出事件；
- **查杀引擎调度**：依据本地/云端优先策略，编排引擎调度次序。

本地多引擎查杀

- **鲲鹏引擎**：提供自动化病毒特征提取分析能力。
- **QVM II引擎**：对360已经积累的海量样本进行多次切片学习，抽取出病毒与恶意代码共性特征，建立恶意代码不同族系模型，对加壳和变种病毒具有出色的免疫能力。
- **QEX脚本引擎**：该引擎既能结合精确特征和启发特征，来检出已知和高级恶意威胁，又能对针对非PE类宏病毒、VBS 和 BAT脚本模拟执行，根据输出结果做二次检查，确保结果的准确性。

云查杀

- **云查杀引擎**：360云查引擎建立在云端庞大的黑白名单数据库基础上，病毒检出率高，系统资源占用低。
- **云等级判定**：依据不同的鉴定过程，给出“安全”“未知”“低风险”“高风险”等级判定结果
- **云QVM引擎**：以360全量云端大数据、弹性算力为支撑，提升未知病毒的检出率。

提升病毒检出率，有效应对变种
基于人工智能技术的查杀引擎，精准掌握病毒家族基因，有效应对病毒变种、加壳等，提升病毒检出率。

提升查杀效率，降低业务影响
云查快速比对技术，极大提升查杀效率，缩短由于病毒查杀、病毒隔离造成业务等待的时间。

独创的多病毒查杀引擎，有效应对未知病毒木马

基于360独有的QVM-II/QEX/鲲鹏等本地化查杀引擎及云查引擎，构建多层次协同的病毒查杀机制，提升病毒检出率。

全球第一的云端大数据，提供充足的云查数据支撑

从业内首创的云查技术开始，积累了全球第一的安全大数据，为病毒木马云查的检出率、检出效率技术支撑

勒索病毒专项防御场景-通过Win主动防御，实时阻断终端恶意行为

Win主动防御，依托360云端行为规则库，以终端浏览器、操作系统、应用入口等层面的行为数据为切入点，提供终端行为实时采集、云端行为库比对、实时阻断等功能，提升终端异常行为的实时阻断能力，在危害产生影响前，将其遏制。

行为实时采集

- **浏览器行为采集**：网址访问行为，互联网下载行为，浏览器配置修改行为等；
- **系统行为采集**：摄像头使用行为、系统安全配置行为、文件系统行为、驱动修改行为、进程修改行为以及注册表修改行为等；
- **威胁入口行为采集**：聊天安全行为、下载安全行为、U盘使用行为、黑客入侵行为等；

云端行为库实时比对

- **目标网址比对**：高置信度的网址的黑白名单库进行比对，；
- **操作行为比对**：横向渗透行为库比对、提权行为库比对、软件劫持行为库比对、无文件攻击行为库比对；

实时阻断

- **实时阻断**：对命中黑白名单行为库的行为流量进行阻断/放行，提升实时防护效率。对于灰色流量进行深度动态分析。

浏览器防护，守住终端互联网入口

依赖信誉库检测，规避恶意网站或黑链接

系统防护，抵御高级威胁

驱动级监控，监控入侵攻击、持久化痕迹，能有效遏制无文件攻击

入口防护，阻断威胁植入

阻断外部入侵，检测文件安全性

360独创主动防御技术，基于独有云端规则库，大幅领先同级别对手

基于360独有的云端主动防御规则库，不断积累互联网海量终端行为特征，用于本地行为实时监测阻断。在开启主动防御后，在众多测试中大幅领先同级别对手。

勒索病毒专项防御场景-停服加固，通过Win7盾甲内核防护，实现系统级安全防护

360数字安全 数字安全的领导者

Win7盾甲采用未知漏洞防御技术和缓存技术，通过缓和引擎、加固引擎、补丁引擎和虚拟化引擎，提供系统核心加固、高危漏洞管理和防护状态设置等功能，从威胁洞察、漏洞修复、核心加固、关键程序防护等多维度出发，切断漏洞利用通路，消除Win7停服而带来高危安全漏洞安全隐患。

系统核心加固

内存保护检查、导入导出表检查、系统调用者检查，提供栈置换防护、阻止远程映射、零地址防护、堆喷射防护、内核攻击防护、子系统隔离保护、镜像攻击防护、内核隔离防护等高级防护。

高危漏洞管理

以高危漏洞维度展示存在的高危漏洞情况，包括漏洞编号、终端总数、开启免疫终端、关闭免疫终端、无需免疫终端；以终端维度展示存在的高危漏洞免疫情况，可查看已开启免疫、不需要免疫的漏洞。

防护状态设置

低级、中级、高级三种防护状态设置。

提升微软停服系统漏洞防护效率

360Win7 盾甲主机安全加固系统的安全管理中心能够提供针对所有用户端的统一漏洞修复、统一加固、统一防护的能力，方便用户进行统一管理，为用户建立统一的安全基线。

整合安全防护引擎，提升停服系统安全防护能力

360将遗留补丁 / Patch Diff、漏洞缓和、操作系统/应用程序加固、威胁情报+微补丁、隔离和虚拟化等四大引擎融入Win7盾甲，全面提升安全防护能力。

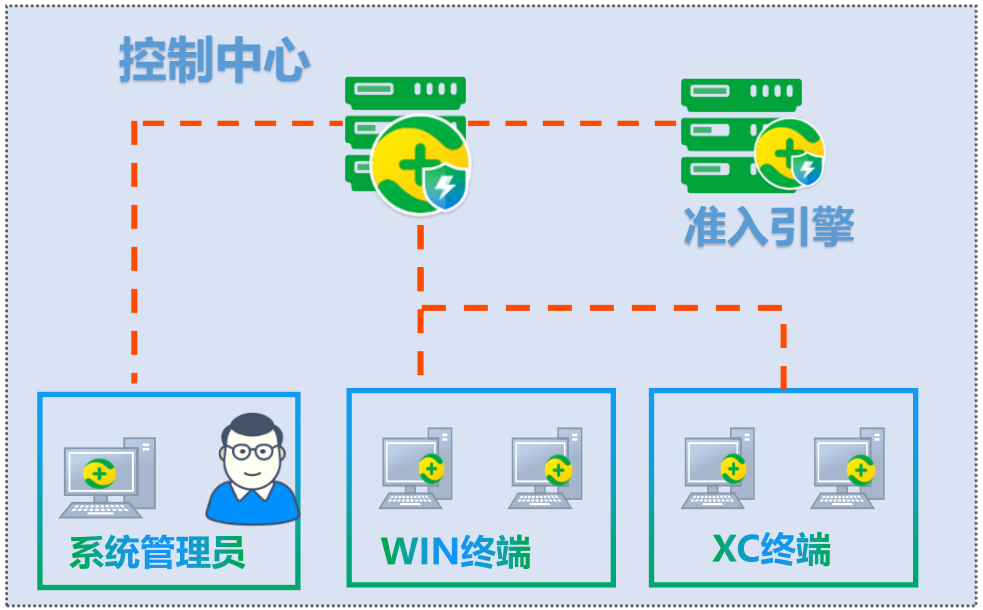
紧跟停服系统漏洞情报，提升漏洞阻断效率

360紧跟win7和IE浏览器漏洞威胁情报，建立漏洞分析与优化平台，结合微补丁漏洞免疫技术，拦截各类恶意攻击，全维度护航Win7系统安全。

PART 3-2

终端统一纳管场景

终端统一纳管场景



场景需求

- 医院终端设备数量多、类型多，需要一个统一的平台纳管所有终端设备。
- 国产化政策执行过程中，势必存在**win和XC终端共存**的情况，且大部分客户是混用的情况，无法利用IP段等技术手段做区分管理。
- **win和XC终端共存**的情况下希望有一款准入产品可同时对两种类型的终端做**准入控制**

客户收益

- 所有类型终端设备统一纳管，一套平台解决终端运维需求。
- 响应国家政策，建立**逐步替换的平稳策略**，避免了替代过程中管理混乱的问题，**节省管理成本**
- 产品已经入围四期ML，从政策上符合客户的**合规要求**。

解决方案

- 360终端安全管理系统支持WIN-XC **杀毒桌管等功能统管**，可实现一套管控中心即可对全部类型终端统一管理
- 360终端安全管理系统支持以不同的**产品授权切换产品名称**，可根据授权切换为360终端安全防护系统。360终端安全防护系统已经**入围四期ML**，解决客户合规需求
- 360终端安全管理系统支持准入功能，可有效对win及XC终端做**统一的入网管控**，并支持普遍存在的**NAT环境**。
- 360终端安全管理系统支持安装在**X86、ARM**等不同CPU上的linux、国产化等操作系统，**部署方式灵活**。

资产信息总览

01 软件资产

02 硬件资产

03 进程资产

04 漏洞资产

05 账户资产

06 开放端口

07 启动项

08 计划任务

09 运行服务

10 环境变量

客户端总数：内网终端安装数
风险资产：自动统计内网中存在风险的资产信息
资产统一查询平台：多维度的资产查询

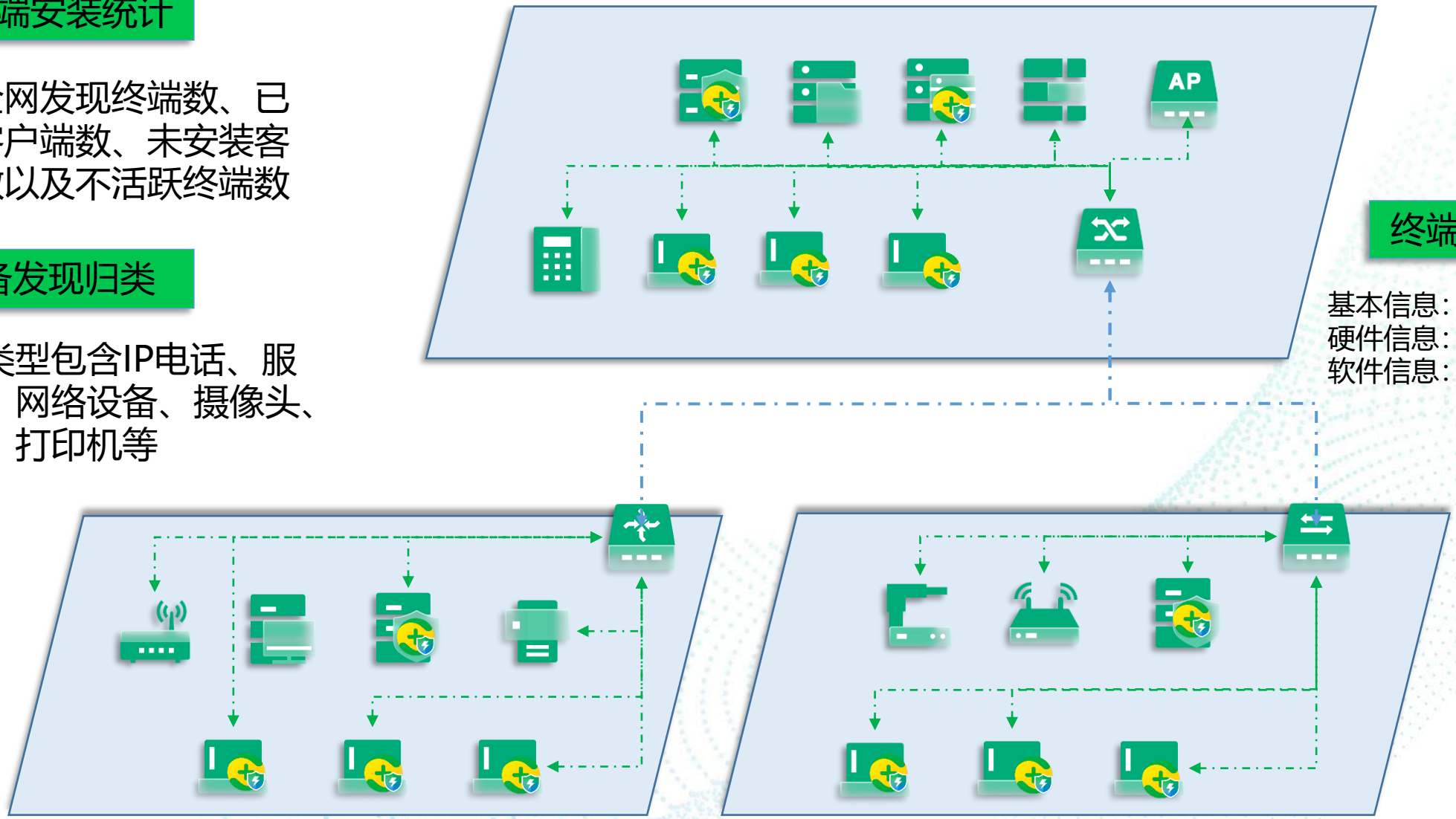
终端统一纳管场景-看见真正的资产

客户端安装统计

查看全网发现终端数、已安装客户端数、未安装客户端数以及不活跃终端数

设备发现归类

终端类型包含IP电话、服务器、网络设备、摄像头、手机、打印机等



终端软硬件搜集

基本信息：计算机名，ip、mac
硬件信息：CPU、硬盘、内存等
软件信息：已安装软件、版本

利用终端代理探测机制，确保探测不留死角

终端统一纳管场景-资产实名管理

- **资产登记**

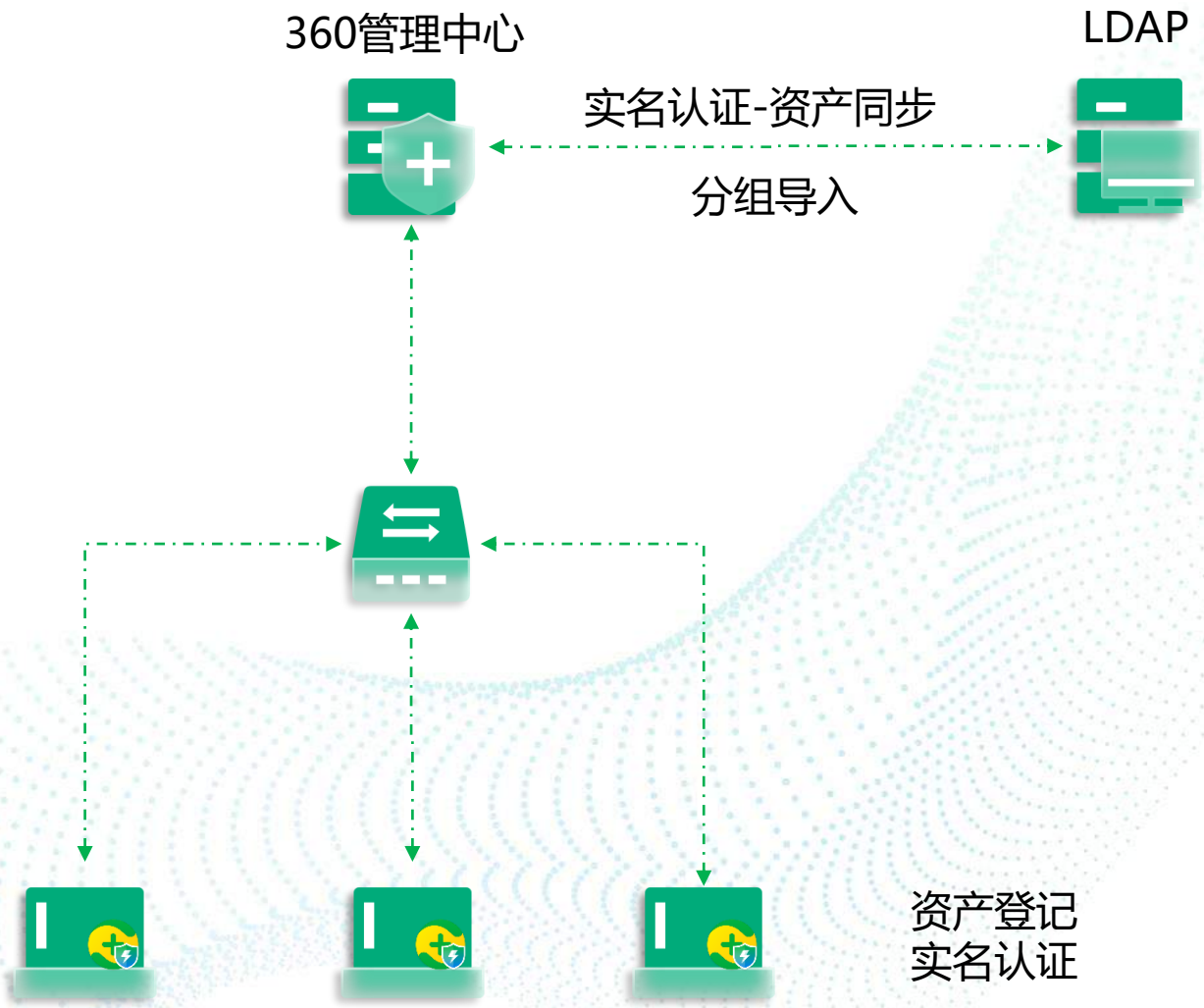
  配合自动登记策略，将终端使用人，手机等联系人信息与终端绑定，确定终端的责任人

- **LDAP联动**

  支持LDAP联动导入组织信息，无需二次创建分组

- **实名认证**

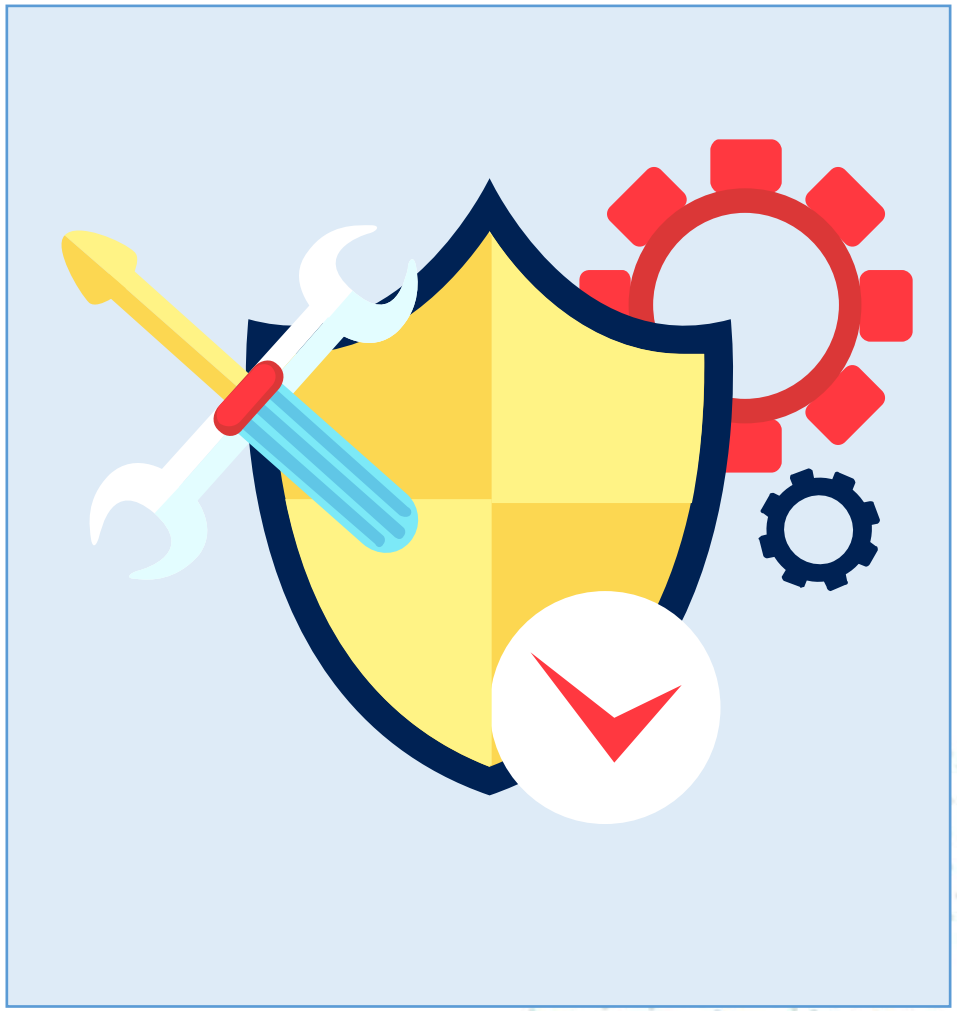
  支持LDAP联动实名认证，可自动同步LDAP资产信息至终端，无需终端手工填写



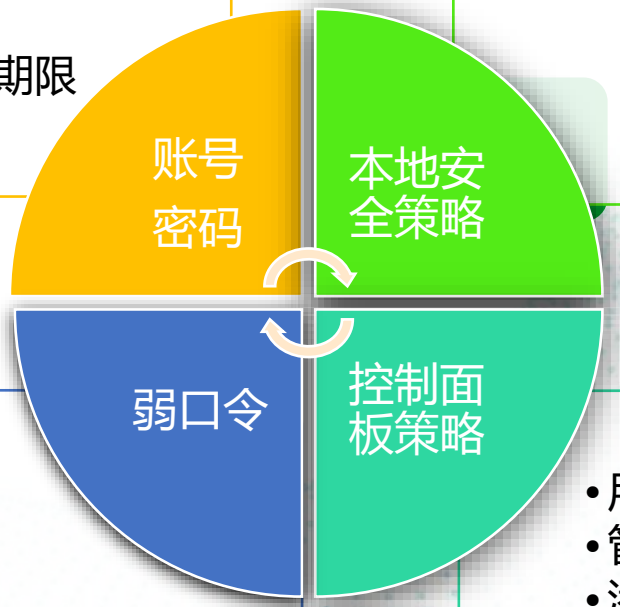
终端统一纳管场景-终端合规管控

多维度管理能力，符合三级等保安全管控部分要求

终端统一纳管场景-系统加固，减少风险暴露面



- 密码复杂度
- 账号增删提权
- Guest账号管理
- 账户锁定阈值
- 添加删除账号
- 密码长度、使用期限
- 强制密码历史



- 组策略/注册表
- 系统共享/用户共享
- 远程桌面
- 系统防火墙
- 用户自动登录
- U盘自动播放
- 远程修改注册表

- 万级弱密码库
- 自定义弱密码库
- 密码不合规提示

- 用户账号
- 管理工具
- 添加/删除程序
- 共享中心
- 安全模式

终端统一纳管场景-终端漏洞修复与停服加固

灵活 自动修复 / 手动修复 / 补丁排除

精细 按操作系统 / Office版本 / 漏洞级别

实用 无人值守重启 / 蓝屏修复 / 灰度发布

全面 针对微软停服系统加固、高危漏洞免疫

漏洞利用攻击是重要的勒索投毒方式

终端统一纳管场景-软件管家

软件管家依托云端海量的软件，提供软件统计、软件商店、软件卸载、软件分发等功能，实现企业网内软件下载、使用需求全面覆盖，帮助企业快速搭建起一个安全、软件资源丰富、富含企业特色的软件商店。

软件统计

软件统计：通过系统API获取软件安装列表，上报管控中心
软件活跃度统计：下载安装、卸载、升级

软件商店

软件获取：客户端通过软件管家客户端，从管控中心获取内网软件分类以及每个分类下软件列表
软件安装和升级：当选择安装\升级软件时，客户端从管控中心下载选择软件的安装包并启动，完成软件的安装和升级

云端海量的软件

软件分发

软件分发：客户端根据管控中心下发的分发命令，从管控中心下载响应的文件，并根据策略将软件防止在指定的目录，以及是否启动

软件卸载

客户端接收管控中心下发的软件卸载命令，启动相关软件的卸载程序完成卸载

减轻终端软件的运维工作
对终端软件的全生命周期管控，极大简化内网终端软件的管理和控制

利用云端海量软件，满足普遍需求

360软件管家在个人用户使用过程中经过大量用户的验证，精选收录了**8000多款**安全软件，覆盖了PC端软件使用的普遍需求

依托云端海量病毒样本，保证软件资源的高安全性

360经过多年的投入与沉淀，积累了海量的病毒样本，为软件管家保障软件资源安全性方便打下了坚实的基础

终端统一纳管场景-自助化运维

傻瓜式自助运维工具，降低运维投入

办公优化

- 广告弹窗拦截
- 右键菜单项清理
- 桌面助手（文档归类）

终端办公优化方案

性能优化

- 优化开机速度
- 系统盘空间减负
- 系统垃圾清理
- 应用流量控制

创建无干扰的轻爽办公桌面

100%
您的系统优化指数

无干扰办公

- 桌面助手
- 弹窗防护
- 断网急救箱
- LSP修复
- 右键管理
- 默认软件设置
- 自定义工具

系统减负

- 垃圾清理
- 优化加速
- 文件粉碎机
- 查找大文件
- 流量管理
- 系统盘瘦身

其他工具

- 隔离沙箱

PART 3-3

数据防泄漏场景

数据防泄漏场景

医疗行业数据安全现状

- 医疗信息化发展迅猛，向数字医院、智慧医院转型，带来便利也带来海量医疗数据。
- 医院终端多、医生诊疗需频繁进入多个系统，医院人员流动量大、各类人员日夜进出医院，易发生数据泄露事件。
- 医疗数据价值高、敏感度高、泄露成本高，成为攻击者的首选目标之一。

解决方案

- 办公数据安全：多种数字水印，警醒员工保障办公数据安全；文档卫士智能备份文档数据，防止贵重资料被勒索绑架；详细的终端审计功能，记录重要操作行为，及时发现异常操作。
- 敏感信息安全：敏感信息扫描，提前应对、看清自己；敏感数据检测，阻拦敏感数据外发；安全U盘，助力文件外出安全流转。

网信办通报：当地某医院出现信息泄露事件

近日，衡南县网信办在省、市网信办的指导下，对违反《中华人民共和国数据安全法》的相关单位及责任人作出行政处罚。经查，衡南县某医院未履行数据安全保护义务，造成部分数据泄露，违反《中华人民共和国数据安全法》第二十九条规定。衡南县网信办依据《中华人民共和国数据安全法》第四十五条规定，对该医院作出责令整改，给予警告，并处罚款5万元的行政处罚。同时，对第三方技术公司及相关责任人处以1.2万元罚款。据悉，这是衡阳市县级网信部门开出的首张“罚单”，也是衡阳网信部门在数据安全领域开出的首张“罚单”。

互联网不是法外之地，衡南县网信办将依法治网，加强对属地网站监管，依法查处违法违规行为，切实筑牢县域网络安全屏障，维护网络安全、数据安全和社会公共利益，全力保障广大人民群众合法权益。

数据防泄漏场景-水印管理

数字水印包括屏幕水印、打印水印、进程水印、应用水印等，在日常工作中对员工起到提醒和警示的作用，从而保障办公数据安全。

屏幕水印

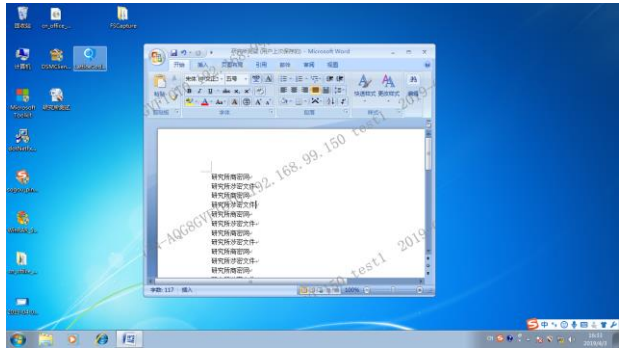
01

打印水印

02

进程水印

03



应用水印

04

依托十几年C端业务和经验积累，降低终端敏感数据泄漏风险

- “免费安全”实现了用户的快速覆盖，安全卫士全球15亿终端，覆盖225个国家和地区。

保障办公数据安全

通过设置数字水印，可加强企业内部信息管理，防止截屏、拍照泄密

数据防泄漏场景-数据智能备份

文档卫士利用强大的预警监测机制 + 自动备份引擎，提供文档备份、文件解密等功能，有效防御勒索软件及其他威胁，坚决保护文档安全。

文档备份

- 支持360云盘备份及本地备份两种模式
- 备份原始文档（开机后首次写操作触发备份）
- 自定义备份文档格式与本地备份路径
- 以加密形式保存于本地磁盘
- 自选择已备份的指定文件进行恢复

文件粉碎机

- 恶意文件强行删除，避免恢复
- 关键资料安全擦除（多种擦除机制，自由选择）

一级（擦除1次，全部写入0，急速）
二级（擦除1次，全部写入随机数，快速）
三级（擦除7次，美国国防部U.S. DOD 5220.22-M 标准，缓慢）
四级（擦除35次，Gutmann 算法，非常缓慢）

保护文档安全

文档防护一键开启，病毒篡改、恶意操作、系统崩溃统统搞定，为企业文档安全保驾护航

数据防泄漏场景-终端审计

终端审计依托EPP终端安全管理权限，提供文件操作审计、终端打印审计、网络连接访问审计、终端开关机审计、系统账户审计、外设使用审计等功能，帮助终端使用者和管理者记录重要操作行为，及时发现异常操作，提升终端安全管理水平。

文件操作审计

- 审计位置：本地磁盘、移动存储设备、光盘、网络共享。
- 审计操作覆盖读取、修改、删除、重命名、创建、复制、移动、恢复。

终端开关机审计

- 审计覆盖终端的开机、关机、睡眠、登录、注销、切换用户以及锁定行为。

终端打印审计

- 审计打印行为，可阻止打印操作。
- 审计内容覆盖打印时间、打印文件名、打印页数、份数、打印结果。

系统账户审计

- 操作系统账号的新增、删除、登录、注销。
- 账号属性信息变更。
- 用户组的新增、删除、用户组成员变更。

网络连接访问审计

- 审计终端网络连接访问行为，可对终端发起的特定进程名、host地址进行审计。
- 目标IP、目标端口、进程名都一致时，可过滤数据，优化审计记录。

外设使用审计

- 支持审计指定设备名称、VID/PID的外设插拔操作。
- 可过滤鼠标、键盘类型设备。

提升终端安全管理科学性

对终端操作行为的记录，分析，科学制定管理策略，逐步提升管理水平

全面行为审计，有效记录各类终端操作

支持文件操作、终端开关机、打印行为、系统账户管理审计、网络连接审计、外设使用审计等。

终端行为细颗粒度审计，支撑各类审计应用场景

支持审计白名单，对于敏感文件、内容、打印操作不执行审计操作
支持对于用户权限及配置修改相关功能

数据防泄漏场景-敏感信息扫描

终端敏感文件检测，提前应对

扫描能力

- 扫描范围：全盘扫描、指定路径扫描，提供便捷扫描路径（我的桌面/文档/下载、当前用户缓存）。
- 文件格式：office、WPS、PDF、TXT等。

扫描效率

- 提供增量扫描形式，无需重复扫描。
- 支持单次、周期性执行扫描频率。
- 提供扫描文件的大小、压缩包层数、单个文件扫描时长、文件日期过滤等优化手段，提升扫描效率。

资源优化

- 监控终端的CPU使用率、磁盘IO使用率，超过阈值时，不进行扫描，灵活优化终端资源占用。

敏感信息库

- 预置敏感信息库，可自定义敏感识别规则，支持正则表达式、关键字，可多规则组合利用。
- 提供敏感信息模板，支持复用，便于管理。

数据防泄漏场景-敏感数据外发拦截

数据外发管控依托全面细致的终端数据安全防控机制，提供敏感信息扫描、文件外发防护、文件外发审批、文件外发审计等功能，对文件外发行为进行严格的监控，从而保护外发文件的安全。

敏感信息扫描

- 支持全部扫描、增量扫描
- 可设置扫描频率，按照单词执行、或按照每天/周/月的周期执行扫描任务

文件外发防护

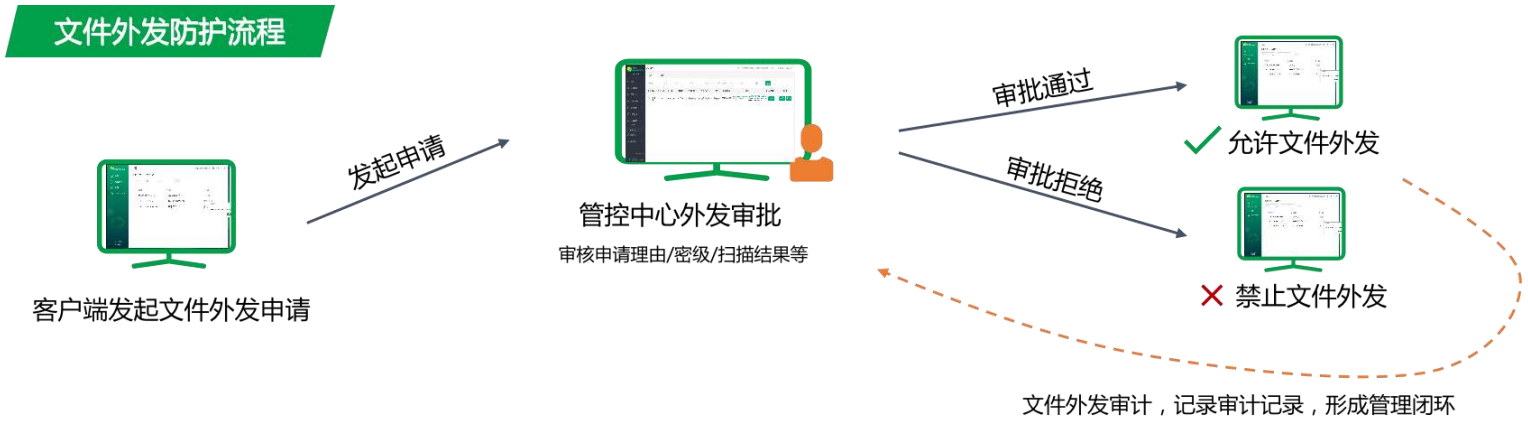
- 识别风险行为包括：移动存储拷贝、网络共享、进行文件打印、红外/蓝牙外发、内容拖拽、剪切板
- 管控方式：阻断、审计、用户确认

文件外发审批

- 客户端外发申请：通过客户端文件外发申请界面，提交需要外发的文件。系统将对外发文件进行扫描，并将结果提交给管控中心发起申请。
- 管控中心审批：可查看客户端的外发申请信息，可对申请信息执行同意或拒绝。

文件外发审计

审计内容包括出时间、平台类型、终端名称、IP、分组、风险行为、文件名、命中规则、密级、处理方式、详情。支持多条件复合查询



基于内容识别技术，准确判断目标数据敏感情况，降低终端敏感数据泄漏风险

- 内容过滤技术依托强大的解析库，支持绝大多数的常用办公文件内容的识别和判断，例如Office、PDF、WPS等。除文件正文外，还能有效检测文档页眉、页脚等，同时还可识别多层嵌套、压缩文件。

保护外发文件的安全

文件外发防护，对敏感文件外发渠道有针对性的控制，阻断风险操作，避免敏感信息泄漏

数据防泄漏场景-文件外出安全流转

防丢失，防破坏，防越权

- 设备授权
- 标签授权

- 普通U盘操作记录
- 安全U盘操作记录

外出权限

操作审计

安全指纹

信创兼容

- 跨平台（Windows+信创桌面机）
- 灵活注册方式
  U盘管理工具注册
  用户申请注册（Windows）

- 停用/挂失/注销
- 用户申请注销（Windows）

存储区划分

安全存储区+普通存储区

安全性	密码保护 指纹登录
规格容量	32G/64G标称容量

PART 04

优势及价值

全球顶级网络安全赋能

360数字安全
数 字 安 全 的 领 导 者

安全大数据

10万+台服务器/2EB安全大数据（相当于大约4亿部高清电影的总存储量）

程序样本库：300亿+
每天新增900万样本

程序行为库：总日志数22万亿条
每天新增380亿条

网址安全查询库：每天800亿条

全球域名信息库：90亿域名信息
每天新增100万

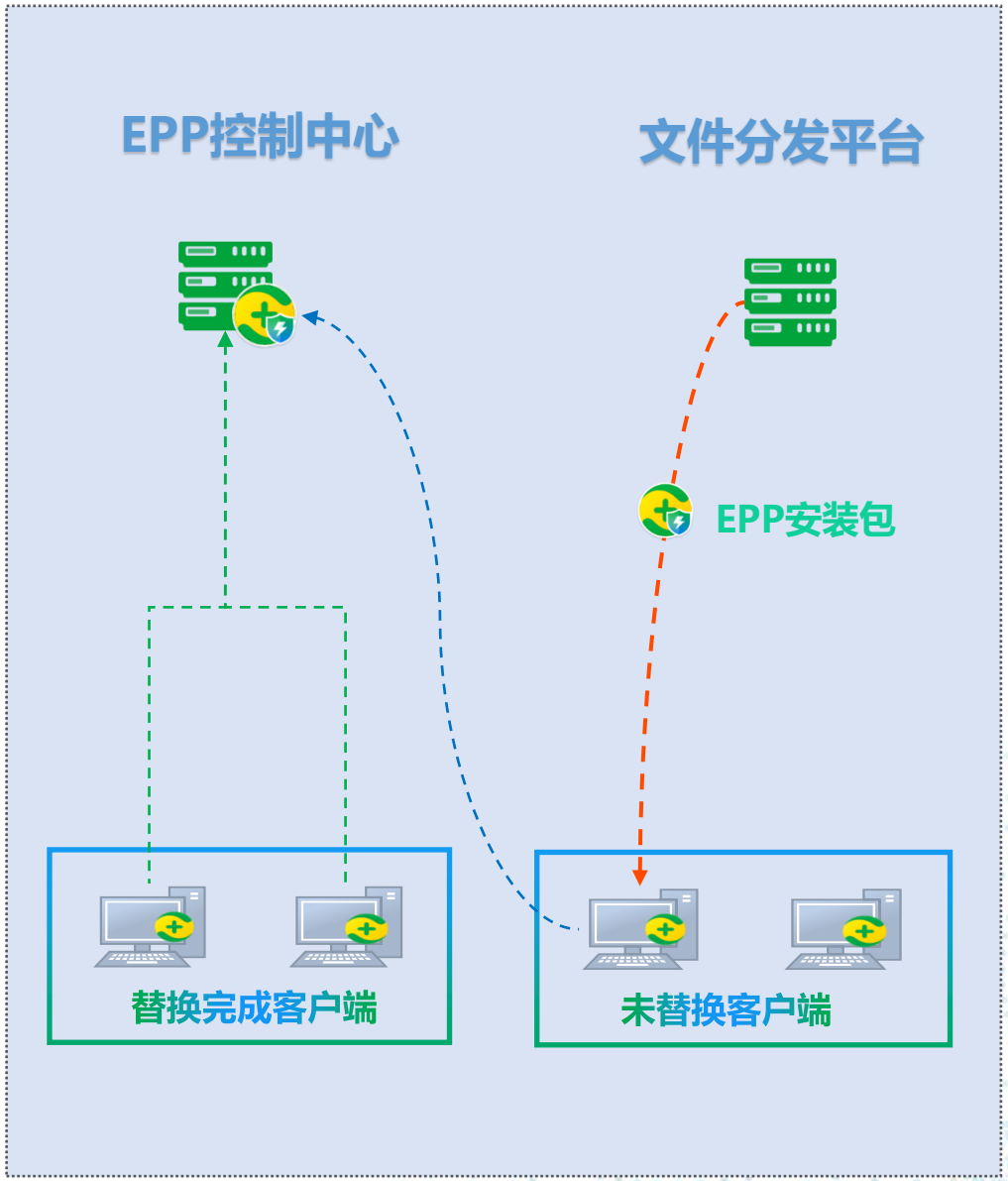
发现跟踪APT组织 50个

安全专家

东半球最强白帽子军团，安全团队2000+

- 2021谷歌Chrome Top20精英榜6人入选
- 2019 The Pwnie Awards大奖
- 2018 & 2019 二度蝉联“天府杯”冠军
- 微软 Bluehat 2019“最佳守护用户”奖
- 2017年起连续三年问鼎MSRC安全精英榜

平滑替换



静默安装

- EPP支持静默安装，可通过第三方分发工具将EPP安装包**静默的分发**至客户端且进行**静默安装**，产品替换不影响办公人员。

静默卸载

- EPP客户端在终端安装时，可静默卸载部分杀毒产品(360卫士、360杀毒、TQ等)，且无需终端人员参数与。

产品优势

360数字安全
数 字 安 全 的 领 导 者

NO.1 兼容能力

1、最大规模的互联网终端部署量，系统兼容能力充分验证。

2、 数亿终端体量。全球任何角落新发木马病毒或攻击事件，360可**第一时间感知**并由安全专家分析产出免疫查杀方案。

NO.2 自助运维能力

1、C端受欢迎的**桌面优化**工具：垃圾清理、开机加速、系统盘瘦身、文件粉碎机等系统优化的工具，**延续**终端用户对C端产品的**使用惯性**

2、傻瓜式自助工具，解决大量终端运维问题，**缓解运维压力**

NO.3 防护能力

1.独一家的**CPU虚拟化机制**，拥有64位系统上最强的安全防护能力

2.文档卫士：内核写时备份，对用户无感知无干扰；且**备份文件对勒索病毒免疫**；

3.业界独有的，对内核层或应用层的二进制**0day**攻击行为的**捕获能力**

NO.4 停服防护

1.内核级专项**系统加固**、全方位拦截恶意攻击

2.先行覆盖**免疫紧急漏洞**、业务零干扰防护不断线

3、**80+高危漏洞免疫**热补丁，业界领先

4、**数亿用户**十几年补丁经验，全面解决已知漏洞的问题

NO.5 信创生态适配

1.多款信创产品**入围**XC目录，满足客户合规需求

2.WIN终端和信创终端**同台管理**机制，可有效解决信创替代**过渡期**，不同系统的共存问题。

NO.6 模块化、一体化

1、单个产品集成杀毒、管控、准入、审计、数据防护**多个模块**功能，支持根据不同客户诉求，**灵活适配**

2、通过多合一技术，实现终端安全管控一体化，后台管理一体化，**降低**终端**资源占用**，**降低**各个管理后台**运维人员投入**

PART 05

典型案例

江苏某中医医院

项目简介

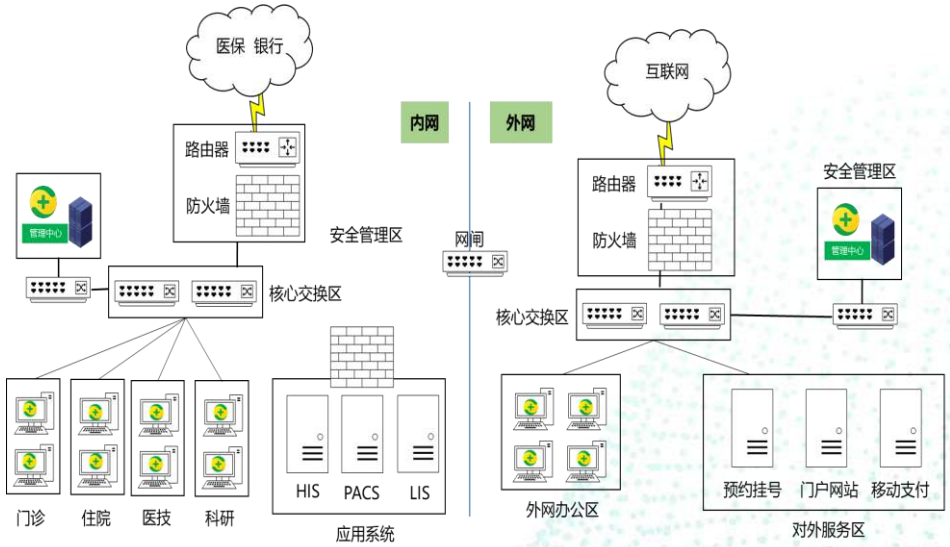
该医院是一家集医疗、教学、科研、 预防保健及康复为一体的现代化综合性三级甲等中医医院。为建设符合等级保护2.0要求的信息安全网络，需要对医院现有的信息化系统进行升级改造。

建设目标

覆盖2000Windows PC+20Windows Server，搭建内网和外网两套防病毒系统，保障正常诊疗秩序，实现恶意代码防护需求，满足等级保护测评要求。

解决方案

系统架构：2套系统独立部署，互联网区和医院内网各部署一套360终端安全管理系统，实现内外网分区分级管控
安装部署：使用URL链接、客户端下载安装等方式部署
查杀能力：基于360 鲲鹏大数据引擎、QVM Ⅱ人工智能引擎、QEX脚本引擎簇提供全面的恶意代码检测查杀能力



价值收益

终端防病毒：基于360在终端领域15年的积累，防病毒能力全面下沉到产品，有效检测处置已知未知威胁。
协同纵深防御：360终端安全管理系统负责端侧的威胁检测处置，网络和边界安全由网络安全设备进行防御，通过在网络边界和终端部署双层防线，构筑纵深防御体系，防护内部和外部木马病毒攻击。
满足等保合规：提供恶意代码检测、外部入侵防御和终端加固能力，满足等级保护测评需要。

北京某医院

项目简介

该医院原有杀毒产品客户端1000点，本次项目为扩增1000点。单位内多数人使用过360个人版产品，有使用360安全卫士小工具的需求，因此希望将原有产品切换为360产品，且不想重复实施。

解决方案

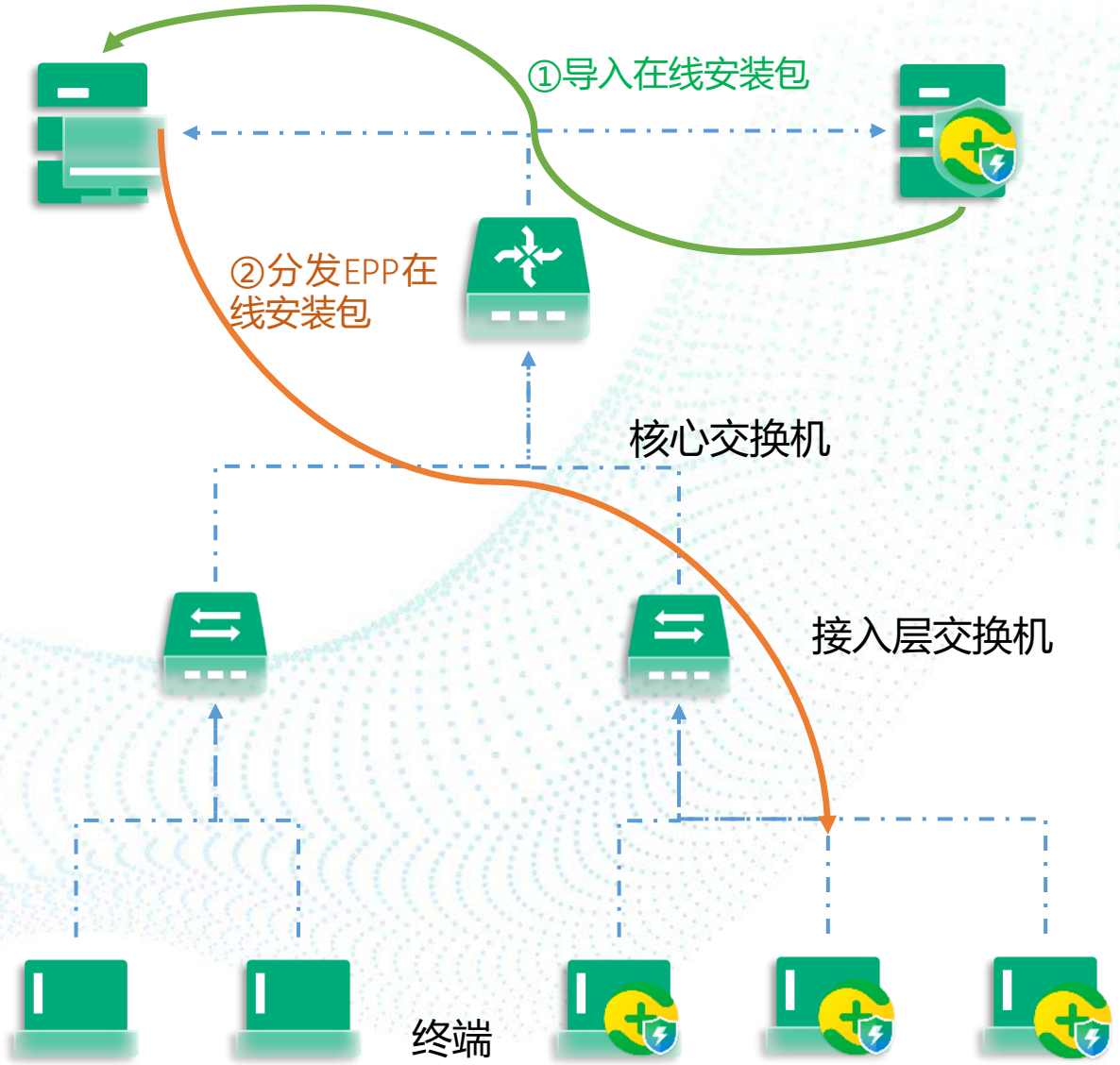
利用分发工具分发EPP在线安装包，平滑替换客户原有杀毒产品。

项目亮点

平滑替换：360产品静默分发后无需终端人员介入，可快速完成产品替换。

软件管家：绿色软件过滤，防止终端安装大量捆绑软件，导致弹框过多问题。

安全卫士小工具：360可提供给用户使用安全卫士小工具，如桌面优化模块：垃圾清理、优化加速、文件粉碎机等，节省客户运维压力。



医疗客户案例集

360数字安全
数 字 安 全 的 领 导 者

长海医院 CHANGHAI HOSPITAL

首都医科大学 附属北京潞河医院 潞河临床医学院
BEIJING LUHE HOSPITAL,CAPITAL MEDICAL UNIVERSITY

HBCH 河北省儿童医院 CHILDREN'S HOSPITAL OF HEBEI PROVINCE

大连市中心医院 Dalian Municipal Central Hospital

无锡市中医医院
南京中医药大学无锡附属医院
厚德 精业 传承 创新

青海省妇女儿童医院
Qinghai Province Women and Children's Hospital
省级三级甲等专科医院

湖南省直中医医院

甘肃省中医院
GANSU PROVINCIAL HOSPITAL OF TCM
甘肃中医药大学第一附属医院

河南中医药大学人民医院
PEOPLE'S HOSPITAL OF HENAN UNIVERSITY OF CHINESE MEDICINE
郑州人民医院
PEOPLE'S HOSPITAL OF ZHENGZHOU

EENT 复旦大学附属眼耳鼻喉科医院
EYE & ENT HOSPITAL OF FUDAN UNIVERSITY
上海市五官科医院

桂林市中西医结合医院
GUILIN HOSPITAL OF CHINESE TRADITIONAL AND WESTERN MEDICINE

复旦大学附属中山医院青浦分院
上海市青浦区中心医院
复旦大学附属青浦区中心医院（筹）

淮北矿工总医院集团

沛水县人民医院
湖北科技学院附属浠水医院

呼和浩特市蒙医中医医院

北京大学 Peking University 滨海医院（天津市第五中心医院） BinHai Hospital

Ankang Hospital of Traditional Chinese Medicine
安康市中医医院
安康市中医药研究所
广州中医药大学附属医院
陕西中医药大学附属医院

无锡市儿童医院
WUXI CHILDREN'S HOSPITAL
南京医科大学附属无锡儿童医院

四川大学华西口腔医学院 华西口腔医院
WEST CHINA SCHOOL / HOSPITAL OF STOMATOLOGY SICHUAN UNIVERSITY

THANKS!

360数字安全

数 字 安 全 的 领 导 者

联系人：曹有军
Tel：13011160389
Email：cyj@schj.net.cn