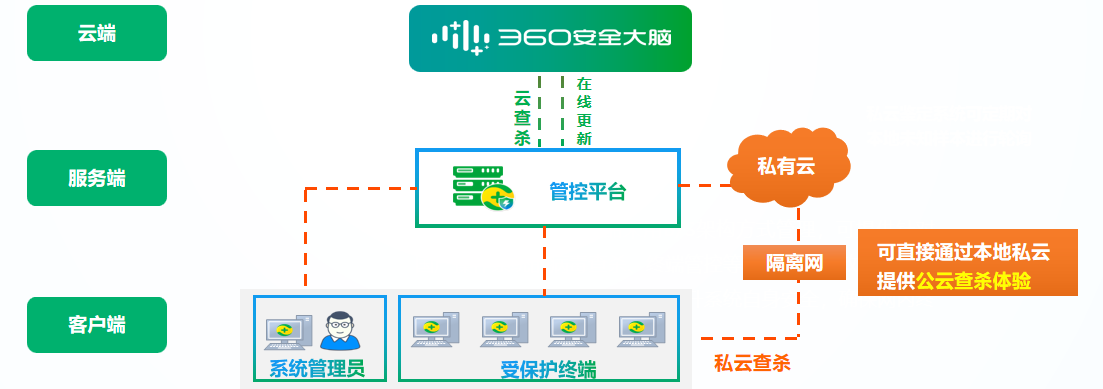
**功能结构说明**

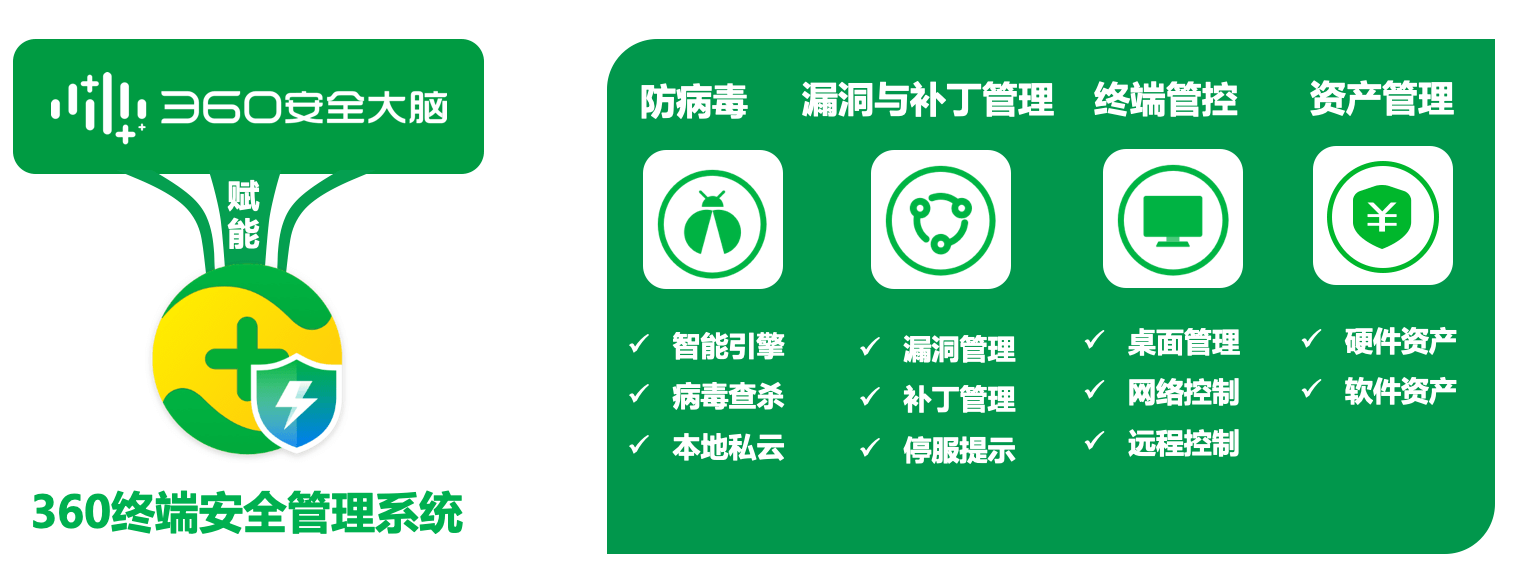
**功能概述**

360 终端安全管理系统是在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，帮助政企用户快速掌控全网终端安全状态，有效保障全网终端安全。

**系统框架**

****

**功能介绍**



**1、防病毒**

通过公有云查杀引擎、私有云查杀引擎全面识别各类恶意威胁，结合基于大数据技术的鲲鹏引擎、QEX脚本查杀引擎以及使用360自主研发的机器学习引擎QVM，内置多种算法模型并且通过海量样本进行训练实现自动演进，对各类木马病毒、新型威胁实现精准查杀。

提供主动防御能力，从系统防护、浏览器防护、入口防护、上网防护等方面，对文件访问、进程创建、注册表读写、设备加载等场景实现主动防御拦截。

**2、漏洞与补丁管理**

对操作系统漏洞、Office漏洞以及特定第三方软件漏洞进行检测修复。

**3、终端管控**

桌面加固：通过对终端的账号密码强度、屏保和桌面壁纸的策略控制，实现用户桌面的统一管理。

违规外联管控：侦测内部终端是否存在非法连接外网或指定网络的行为，并可对违规终端执行断网处置。

网络控制：从IP、域名和端口等维度进行终端网络控制，阻止访问攻击。管理员还可以对终端的DNS地址进行统一配置，阻止通过指定的DNS进行攻击。

远程控制：运维人员可以通过远程连接的方式，获得对远程终端的操作权限，提高终端故障处置效率。

**资产管理**

统计终端软硬件资产，及时发现终端资产风险

**技术优势**

**1、多引擎技术**

基于360安全大脑的持续赋能，通过云查杀引擎、鲲鹏引擎、 QVM人工智能引擎、QEX脚本检测引擎打造云端一体的多引擎检测架构，全面、及时、精准处置各类威胁。

**2、漏洞修复能力**

依托360安全大脑的漏洞情报大数据，提供业界领先的漏洞发现和修复能力。

**3、智能管控平台**

提供统一管控平台，通过灵活的配置策略集对全网终端实现智能化安全管控。

**部署方案**

