**数据泄露防护系统**

随着信息技术的飞速发展，计算机和网络已成为日常办公、通讯交流和协作互动的必备工具和途径。但是，信息系统在提高人们工作效率的同时，也对信息的存储、访问控制及信息系统中的计算机终端及服务器的访问控制提出了安全需求。目前对内外安全的解决方案，还停留在防火墙、入侵检测、网络防病毒等被动防护手段上。在过去的一年中，全球98.2%的计算机用户使用杀毒软件，90.7%设有防火墙，75.1%使用反间谍程序软件，但却有83.7%的用户遭遇过至少一次病毒、蠕虫或者木马的攻击，79.5%遭遇过至少一次间谍程序攻击事件。

捷普数据泄露防护系统基于内容识别技术，能够协助用户快速而准确地感知和阻止潜在的敏感数据泄露威胁，实现遵从行业标准、法规以及降低数据安全风险的目标，确保企业核心数据资产处于任意状态（存储、传输、使用），均能受到保护。

捷普数据泄露防护系统能为客户的数据资产提供“梳理、识别、发现、感知、监控、防护、审计”等多维角度全方位的泄漏监控与保护，识别并大幅降低数据泄漏风险。

**产品特点**

**精准防护**

采用中文语义识别、深度内容检测、OCR、机器学习等核心技术实现对数据库、文档敏感内容的精准识别，大幅降低敏感信息识别的漏报率和误报率。

**安全融合**

系统可以集成活动目录系统的用户信息，指定基于不同用户的敏感数据防护策略（主机组、域用户、用户邮件地址等）。

**智能引擎**

通过对敏感数据的持续监测，利用智能算法形成数据安全行为基线，并将违规事件反馈终端用户和管理员，提高组织的数据安全能力。

**全面可视化**

丰富的数据安全可视化展示方式，多层面的将数据安全状态展现出来，使管理者能够清晰、准确的认知数据运行状况与安全态势。

**快速发现扫描敏感数据**

发现扫描敏感数据依托于各类数据资源的逻辑关系组合构成，是数据发现扫描的核心条件，每个规则都具有各自不同的敏感度。发现数据的敏感度等于匹配该数据的发现扫描规则的敏感度。

**高效敏感数据检测**

违规检测规则由各类数据资源的逻辑关系组合以及响应规则构成，是数据违规检测的核心条件，同时每个规则都具有各自的严重性。违规数据的严重性等于匹配该数据的违规检测规则的严重性。



**产品部署**

捷普数据泄露防护系统能够提供对网络、终端、存储区的敏感信息深度内容识别、精准定位，对敏感信息的违规操作行为进行实时阻断、警告、审计。捷普数据泄露防护系统部署后可以有效保护用户最核心、最具价值的数据资产，实现业务高效与数据安全平衡。

