天融信数据防泄漏系统TopDLP

www.topsec.com.cn

产品概述

天融信数据防泄漏系统（以下简称TopDLP产品）是以深度内容识别技术为核心，在数据存储、传输和使用过程中，发现并监控敏感数据，确保敏感数据的合规使用，防止敏感数据泄露的数据安全防护系统。TopDLP以智能全面保护数据安全为宗旨，在不影响现有业务，不给客户造成困扰的基础上，为客户提供完整的数据防泄露解决方案，保障企业数据资产可控、可信、可充分利用。TopDLP拥有国际领先的数据识别与数据分类技术，是国内第一家获得数据防泄露防护类销售许可证的产品，并且已经在政府、金融、电力、能源、运营商、制造、流通等行业得到广泛应用。

产品特点

深度内容识别，强大的内容感知

基于深度内容识别技术和领先的OCR引擎，支持1000多种文档那个类型的识别与检测，支持300多种文档类型的内容提取，支持30多种图片格式的识别，能识别主动泄露的异常行为，支持对加密行为识别，压缩与压缩嵌套行为识别，少量多次数据泄漏等异常行为识别。

全面掌握数据泄露全貌，及时灵活响应

全面监控敏感数据，对于违反安全策略的敏感信息泄露行为迅速响应并阻断，对敏感数据的使用行为、安全事件、策略执行记录等内容进行审计分析。掌握数据泄露事件全貌，及时预防。

与云环境，大数据环境紧密结合

应用知识挖掘、机器学习、人工智能等技术，并与精细化访问控制项结合，细粒度审计相结合，实现敏感数据在云桌面、大数据平台下的安全共享。

自主研发，安全可控

TopDLP系统完全自主开发，开发过程遵循安全开发过程，交付客户后完全由客户控制，不存在后门漏洞等隐患。丰富的管理接口，可针对客户实际使用的信息系统提供定制化的开发服务。

客户价值

实现对终端数据的安全防护

对敏感数据的违规使用、发送等进行策略控制；对敏感数据的终端使用行为进行监控，确保终端敏感数据的合规使用。

实现对存储数据的安全保护

对存储在服务器、数据库、存储库中的结构化数据和非结构化数据进行扫描，根据策略发现，记录敏感数据，并对违规存储事件报警、隔离等，实现对存储中的敏感数据的分类分级治理。

实现对网络传输数据的安全防护

在网络出口或安全域边界识别、控制传输中的敏感数据，控制或监视通过HTTP、HTTPS、SMTP、FTP、POP3、IMAP、SMB等网络协议传送敏感数据。提供数据服务接口合规审计和敏感数据泄露审计功能，可与大数据等平台对接，实现平台内的数据安全防护。

保护核心资产，为合规审计提供依据

定义企事业单位的敏感信息，制定对不同等级机密信息的监视和防护策略，多维度敏感数据检测，防止机密信息泄露，为内部合规管理和审计提供相关的依据，提供基于合规审计的资料，轻松应对审计部门的要求。

典型应用

TopDLP由一个集中管控中心和三个子系统组成，分别是：DLP集中管控平台、终端DLP、网络DLP、存储DLP。每个子系统可以作为独立的系统进行部署，也可以联合部署。

DLP建设可以为客户带来以下收益：

- 防止因数据窃取而对公司声誉带来的负面影响
- 对网络层面、终端层面泄密的途径和内容进行多维度监控和识别、管控
- 对文件服务器、数据库、存储服务器等进行敏感数据存储发现和保护，对重要敏感数据存放位置进行定位并加以保护，明确敏感数据在单位的整体分布情况
- 有效地符合不同国家对客户资料保护的法规要求，避免潜在的法律诉讼
- 提升数据流转的可视性
- 降低数据外泄的风险
- 提升员工数据安全意识