UniBDP 业务数据防泄露方案

业内首款以场景驱动的数据防泄露整体解决方案

企业信息化建设的核心目标是提高业务效率，数据的高效传输、分享和交换是实现这个目标的重要途径。而绝大多数传统的数据防泄露手段，是阻碍数据的高效传输、分享和交换的。如果不能把握好保护的“度”，简单粗暴的保护方法极可能与业务目标是相背离的。

我们认为必须根据数据的类型、使用者、交换频度来区分不同场景，采用不同技术手段予以保护，解决好“度”的问题，取得安全与效率的最佳平衡。UniBDP是业内第一款以场景驱动的数据防泄露解决方案，以数据智能识别和发现为基础，通过授权控制、智能隔离、安全流转、审计追溯等手段，保护企业业务系统和终端上的业务数据，保证数据的高效传输、分享和交换。

主要功能

定义与发现

系统支持通过数据来源定义数据类别，通过文档内容识别和智能聚类算法，实现对终端数据的自动识别，智能分类、分级，可视化展现

控制与保护

外发通道管控

在数据通过外设、网络应用外传时，根据安全策略，按数据分类、用户权限实现管控

访问权限控制

- 通过资源访问控制技术，实现只有受控终端中的合法应用才能访问受保护的各类业务系统
- 所有操作将自动进入受控状态，同时还可以精准控制到使用时间、地点、接入方式等

安全计算环境隔离

- 自动感知需要被保护的业务系统，在业务系统访问过程中进行权限管控，并将其数据进行隔离防护
- 对本地硬盘上的数据进行分析，智能识别敏感数据并将其进行隔离防护

数据安全流转

- 通过专业的数据安全摆渡和审计控制技术结合，业务数据离开安全域时依然受控，需要经过指定人员审批才能进行数据交互
- 对于需要外发的数据，可按级别、类型进行管控，可只允许通过打包、转 PDF 或原格式外发

行为审计与追溯

- 自动识别用户访问业务系统、敏感数据的行为，对要保护的数据进行标签化管控，通过标签记录数据在内部的流转途径，一旦发生泄露可快速追溯完整泄露轨迹
- 全量采集用户行为信息，通过深度学习和异常检测模型，自动发现业务数据泄露风险
- 对企业文档进行统计汇总，可查询某文档全部或部分内容在企业终端上的分布情况
- 通过水印技术，防止用户通过打印、截屏、拍照等方式泄密

协同

- 与安全数据摆渡系统协同，实现跨网或网内不同用户间的数据安全流转
- 通过与 UniNAC 准入控制系统协同，实现资源访问控制

主要优势

以场景驱动，最大限度保障业务效率

针对不同类型用户、数据类型、使用环境，提供多种技术手段和方案供选择，实现安全保护的“度”与业务效率的最佳平衡

内置大数据引擎，保障审计追溯效果

大数据引擎支持并行计算与横向线性扩展，实现海量审计数据的高速存储、计算和分析

部署简单，运维成本低

可对 B/S、C/S 业务系统中的数据进行保护，无须改造网络、系统和终端环境，文件不染色、外设不封堵

创新技术更优保护

- 透明（矢量）水印、图片水印、文字水印、二维码水印等多种专业水印技术，针对拍照、打印、截屏等泄密行为快速定位责任人
- 提供文档水印发布系统，在方便文档发布的同时防止数据的下载、拍照、截屏泄密

- 针对高权限帐号进行透明审计，防止高权限帐号被恶意使用（仅限专用版）
- 针对敏感业务系统的数据字段在显示前进行脱敏处理（仅限专用版）

方案成熟、应用范围广

在多个行业有大量可验证的大规模部署案例

主要价值

在解决敏感数据防泄露的同时，让员工工作更高效

在数据泄密后提供快速、有效的追溯手段

性价比高、风险可控

典型应用场景

客户信息保护、业务数据保护、OA 系统公文保护、Office 与 PDF 类文档保护