

什么是数据防泄漏

对企业而言，除了来自于外部的病毒、木马、网络攻击等网络安全威胁，还有来自于企业内部的数据泄漏威胁，也同样应该得到企业的重视，而且直接的数据泄漏比间接的数据丢失和泄漏来的威胁更大，这是一个急需企业进行重视并进行预防的重要问题。

无论企业处于何种规模，都存在数据泄密的风险，而这会让企业面临核心客户数据、知识产权、公司重大发展战略及投资决策等方面数据泄密的风险，给企业造成无法估量的损失。这部分数据的泄密，大部分都是员工无意中泄漏出去的，另外一小部分则是员工非法为之。一个没有对终端进行保护的办公电脑可能无意中通过网络或移动存储设备就将机密信息传播出去。

企业信息化的过程是为了方便进行信息的传递和共享，而数据的传递过程包括存储、使用和传输三个基本过程。数据防泄漏就是要保护企业的机密信息不被非法存储、使用和传输。

数据泄漏问题的严重性

每 400 封邮件中就有 1 封包含敏感信息

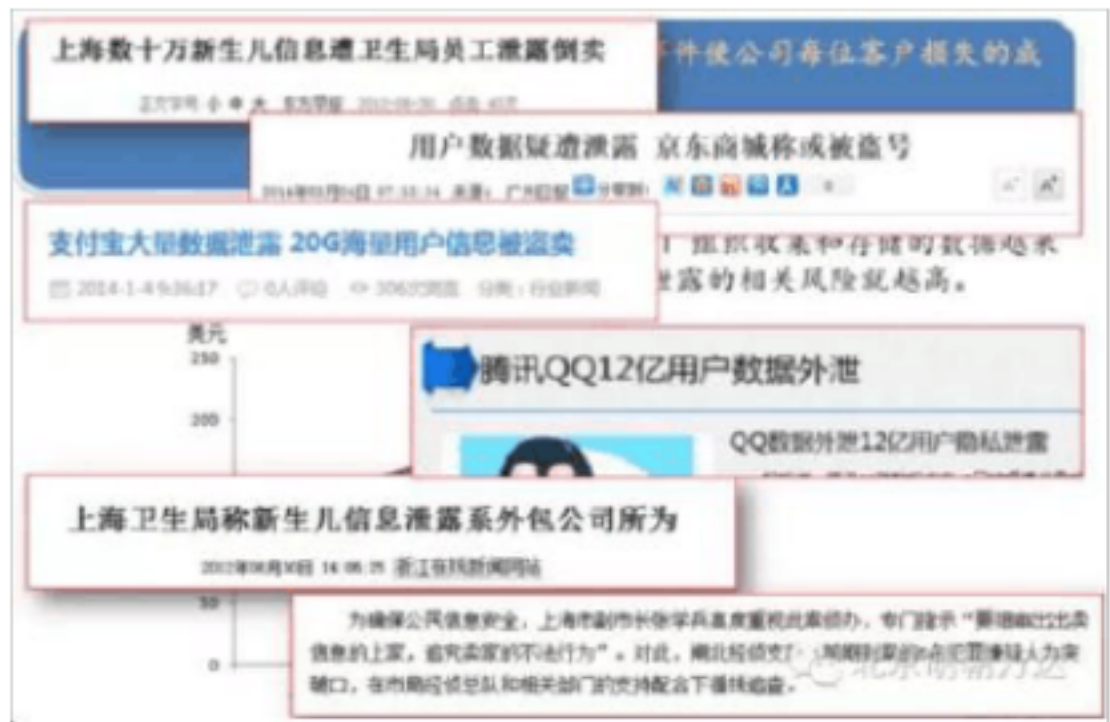
每 50 份通过网络传输的文件中就有 1 份包含敏感数据

每 2 个 USB 盘中就有一个包含敏感信息

全球 80% 的企业存在着信息泄漏的风险

在所有被调查的公司中，进行常规性安全检查的公司不到 50%，而采取措施进行控制的公司只有 30%，国内的比例会更低

在发生的数据泄密事件中，96% 是因为员工的意识和敏感数据管理制度的缺失造成的



数据泄露的信息分哪些种类

隐私数据保护	知识产权	公司机密	调查取证
<ul style="list-style-type: none"> 客户身份证号码 客户帐户 交易记录 卡号 帐单信息 联系地址 医院个人病历 	<ul style="list-style-type: none"> 产品战略规划 产品设计文档 软件产品代码 咨询报告 解决方案资料 大客户的相关资料 	<ul style="list-style-type: none"> 公司年报、季报 CEO邮件 重要会议的会议纪要 预算、采购计划 重要项目投资计划 	<ul style="list-style-type: none"> 公司发生重大数据泄露行为，公安机关或企业内部可依据NDLP相关数据进行调查取证

客户的隐私数据、公司重要的知识产权、公司的重要经营数据，这些构成了企业的核心机密信息，任何信息的泄密，都可能造成企业无法估计的损失。

对数据防泄漏产品的要求

从整个企业的 IT 架构层面来看，数据的安全架构涵盖网络和终端的安全。

对于公司的网络一般会划分安全域，在安全域之间的边界（如公司的内外网出口位置）实施监视和访问控制，做到对网络出口的数据进行抽取并分析，使数据出口可监、可管、可控。

对于终端设备，严格地管理和约束终端的用户操作行为，做到合法用户使用终端，用户的合规操作进行规范管理。通过终端安装的应用，采用技术手段有效对客户要发送的邮件、文件内容、移动存储、文件外发扫描、全盘智能扫描、打印机监等功能；并可实现对终端监控结果的统一上报及管理。

明朝万达数据防泄漏产品介绍

明朝万达，作为国内领先的数据安全厂商，自主研发并拥有自主知识产权的数据防泄漏（DLP）系统，提供针对有来自于邮件、U 盘移动设备、打印设备、

网络等渠道和设备防护，该产品具有针对网络数据防护能力的 NDLP(网络数据防泄漏系统)和针对终端数据防护能力的 HDLP(终端数据防泄漏系统)产品，整体应用架构如下：

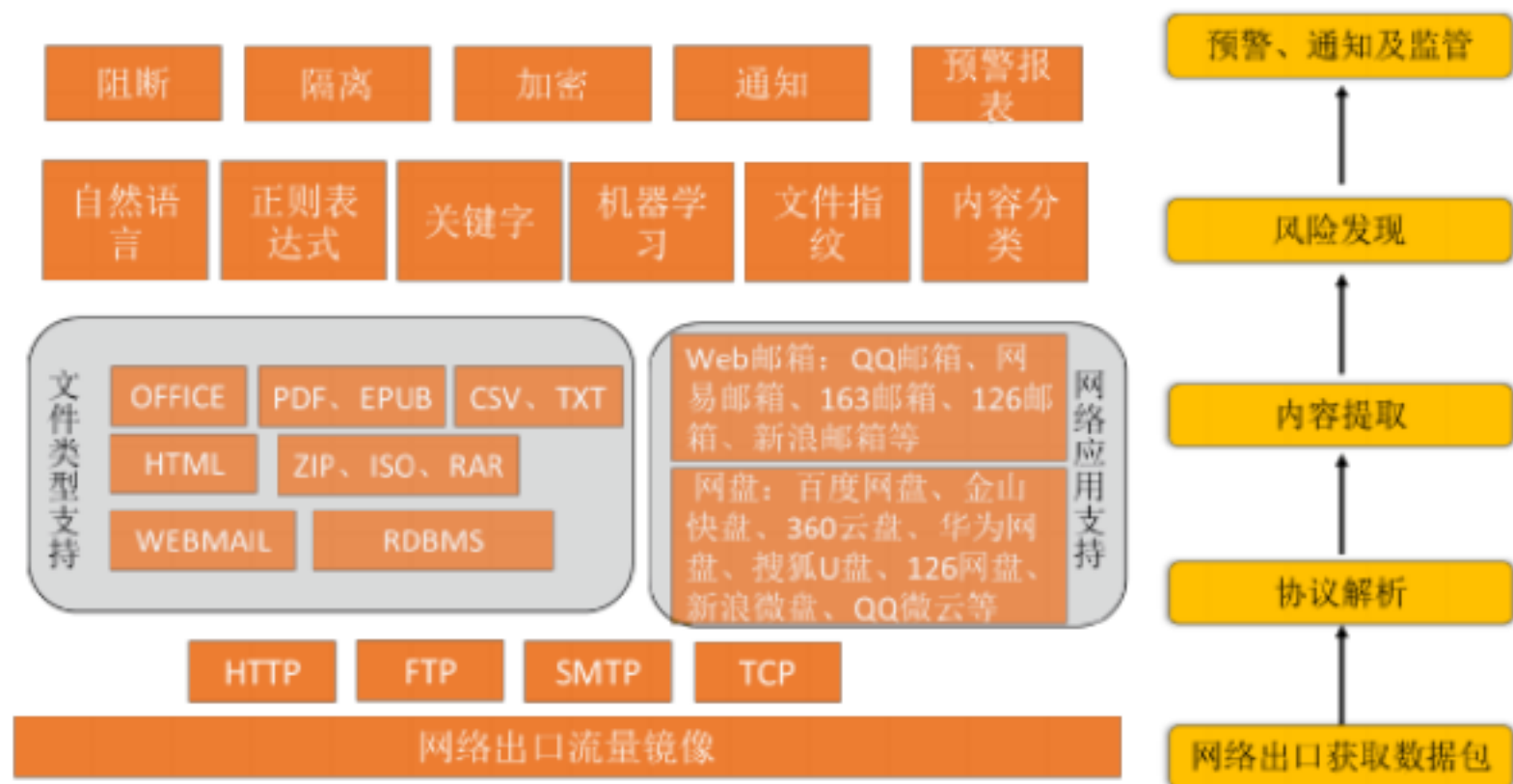


DLP管理平台：管理平台集中管理数据防泄漏产品组件；集中制定、下发数据采集、防泄漏策略；集中进行数据安全事件监控、处置、审计和分析。该组件可独立部署，也可以嵌入终端、网络产品中。

HDLP(终端数据防泄漏产品)：发现、识别、监控计算机终端的敏感数据；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。HDLP整体应用架构如下：



NDLP(网络数据防泄漏产品)：在网络出口或安全域边界识别、控制传输中的敏感数据，控制或监视通过邮件、WEB FTP 等网络协议传送敏感数据。NDLP整体应用架构如下：



明朝万达数据防泄漏产品特点

系统兼容性良好

支持多种终端系统

可以处理结构化数据及非结构化数据

智能识别与学习能力

产品客户案例介绍

目前该产品已经成功运行在中国交通银行、光大银行等近百家企业用户，且部署终端过三百万个，为这些客户提供 7*24 小时的数据防泄漏保护，满足银行业、运营商、公安等不同行业客户的终端数据防泄漏及网络数据防泄漏服务需求。