数据安全的保护对象是公司机密数据。

理论上任何公司都需要数据安全。

数据可分为 客户数据，员工数据，业务数据，财务数据，权限数据，代码数据。

数据分为结构化数据，如SQL中的数据。以及非结构化数据，如各种电子文件及纸质文件。

围绕数据的生命周期展开，从各阶段提升数据安全能力，数据安全能力建设会涉及大量的系统改造、工作流程建设、安全产品采购。

持续运营及优化，

数据生命周期保护，DLP产品，只是宣称自己做到了生命周期保护。

## 人选要求

要理解完整建设。

只有办公终端DLP产品运营经验，是瘸腿的。

## 落地

一般是先进行纯技术体系的落地，然后是运营体系，然后是管理体系。

### 技术体系

数据安全治理，首先要能够发现数据流转行为。

内部系统的调用，外部系统的调用，数据库的读取等都属于数据流转。

数据流转的发现，依赖于完善的日志及日志解析。如果某系统日志未记录数据流转日志，那么就存在着黑洞，无法发现就无法预防风险，无法审计。

将所有系统的数据流转行为统一入库，不同系统使用不同标识符。不同系统按不同的行为规则进行安全审计。

数据加密，防黑客。数据必须经过自研系统才能正常使用解读。

时间-系统-接口-调用人-调用结果-IP

### 审计

数据源：源数据库。操作审计。

<https://help.aliyun.com/product/52432.html?spm=5176.139959.J_5253785160.5.1abe2c63yIDQE6>

mysql-audit等

数据系统：业务系统，内部系统，消息队列，日志系统。完善的日志及解析及审计规则。

数据终端：员工PC电脑。DLP软件。

对所有信息流转行为构建出完善的日志审计等体系之后，能够有其他的价值。如能够发现是否有爬虫。

有用户在极短时间内，大批量调用某接口，可能存在爬虫或黑客攻击。

系统间的信息流转，可以改造系统，留下日志。

数据源的信息流转，可以记录数据库/数据中心操作，记录日志。

数据终端的信息流转变化，可以依赖以上信息，持续监控对应文件的处理，如复制删除恢复，加密，传输等行为。

以上这些东西可以升级成为一个乙方的数据安全产品对外售卖。

产品提供统一的规定，业务系统按规定改造后，接入产品，产品就能提供整体的前后端数据库，内置有分析规则，实现数据安全运营报警，实现大数据安全分析等等。

数据水印技术，用于审计。

### 数据保护

数据加密技术，用于防泄漏。

数据加密体系建设，依赖系统对所有数据进行使用流转。有些地方没法进行数据加密。

## 运营体系

## 管理体系