**行业分析**

随着制造业信息化的迅速发展，企业信息，尤其是文档信息如何能更有效、更安全的流转和使用成为生产商所关心的问题，文档信息的安全传输也随之成为一项重要的业务需求。 制造业是我国国民经济的重要支柱产业。大部分企业，尤其是制造型企业，随着信息化建设的推进，在网络方面增加了硬件设备，在软件方面，增加了ERP、PDM、CRM和SCM等专业系统，企业内部的数据流越来越丰富。伴随着愈来愈激烈的行业竞争，数据安全问题就显得尤为重要。

据权威机构调查，80%以上的安全威胁来自泄密和内部人员犯罪，而非病毒和外来黑客引起。防火墙、入侵检测、隔离装置等网络安全保护对于防止外部入侵有着不可替代的作用，而对于内部泄密显得无可奈何，真正有目的盗取或破坏信息的黑客也许正在隐藏在内部。企业内部的信息安全需要一个整体的策略方案，以巩固信息化成果，降低企业信息安全风险。

**二、客户需求**

随着近年来的市场规模的扩大和竞争的加剧，尤其是占据市场佼佼者地位的公司，对核心技术、图纸和文档类保护越来越重视。该公司也陆续制定了相关的信息安全管理制度对员工的行为和不良习惯进行约束。但在泄密事件频发的当下，紧紧依靠管理制度来保护数据安全是行不通的，必须采用适当的、先进的技术手段配合管理制度来防护数据信息的泄露，保证公司的核心文档安全。

该公司的安全管理制度健全，但只有制度没有防护技术是无法杜绝泄密事件发生的，数据的泄露的途径：

1）企业研发部门的汽车相关设计图纸、设计文档等具有高度保密性、高度敏感性数据，数据泄露会造成重大危险；

2）企业的认证体系、业务信息系统和办公OA系统等应用平台数据交互频繁，与合作单位有大量的对外接口；

3）企业内部网络有多种业务平台，移动设备如笔记本电脑、U盘使用广泛；

4）与外部单位的合作，对外发出文件数量较多。

在制造、设计高度信息化、网络化的趋势带动下，企业引入了大量与生产制造相关的应用系统，而这些应用系统在存储、使用、传输、交互的过程中都会造成数据泄密。具体表现如下：

1.系统内产生的数据和文档有高度保密性、高度敏感性，数据泄露会造成重大危险；

2.企业的认证体系、业务信息系统和办公OA系统等应用平台数据交互频繁，与合作单位有大量的对外接口；

3.企业内部网络有多种业务平台，移动设备如笔记本电脑、U盘使用广泛；

4.与外部单位的合作，对外发出文件数量较多；

5.办公网上的信息都未被加密，采用明文传输；

6.办公网的用户权限控制不严密。

**三、解决方案**

亿赛通数据泄露防护（DLP）是专为企业级用户设计的数据防泄密解决方案，从数据的存储、传输、交换过程中的安全环节，采用了多种加密手段结合的方式保护。从终端、网络和存储三个层次入手，对核心数据的形成、存储、使用、传输、归档及销毁等全生命周期进行安全控制，结合企业特有的业务需求、业务模式和管理文化，为企业制定完整的数据泄漏防护解决方案，实现企业核心信息资产防泄漏的安全目标。

1. 加密系统：采用亿赛通数据泄露防护系统（DLP），运用透明加密、主动加密和智能加密的梯度式加密方式，对设计图纸、文档、财务报表、业务合同等核心数据进行保护。从数据的产生，到数据使用传输，数据都处于加密状态，从源头保证数据的安全；

2. 采用亿赛通安全准入网关，通过DLP系统加准入网关的方式对OA、MES、SVN业务系统的安全保护及终端电脑文件的自动加密保护，达到数据安全从源头做起，凡事从业务系统下载下来的数据都已经做过加密处理，员工拿到的数据就已经是加密文件，但服务器中保存的文件仍保持明文状态；

3. 采用亿赛通数据泄露防护系统（DLP），对内网使用的多种系统进行统一平台管控。对终端、网络、邮件、移动终端、端口等进行多层次防护，保护文档安全；

4. 采用亿赛通数据泄露防护系统的外发管理，可以将外发文档进行统一管理，通过设置外发信息的秘钥、权限、机器码绑定等设置，文档是无法打开的，保证了与外部单位合作的外发文档的安全。

**四、方案价值**

亿赛通数据泄露防护系统（DLP）解决方案与企业的安全理念、安全需求高度融合，从根本上解决了企业存在的信息泄密隐患；通过高效先进的数据安全技术手段，解决了企业数据的存储、使用和传输中可能存在的泄密问题；提供丰富的的审计记录，帮助员工提高安全意识。