山丽网安
SANLEN SECURITY

制造企业智力资产保护技术和发展趋势

2009-5-25

创造、提升您的安全收益 Create and Advance Your Security Income

山丽网安信息安全实验室

目录

数据防护的必要性

- 电子数据的发展；
- 数据的泄密途径；
- 数据泄漏的案例；
- 数据泄密的数据；
- 国家法律和法规；
- 解决方案的依据；

数据防护的必要性

- **人类文明进步的标志**

- 1、石头
- 2、龟壳　甲骨文　商殷 王国维
- 3、简、纸　　汉之所以兴
- 4、磁介质
- 5、光介质？磁介质

数据防护的必要性

- **电子数据的发展**

- 1、人类创造的财富的载体已经由纸类介质转化为纸类介质和磁介质并存，并有更大量和特殊的财富仅仅存在于磁介质中，如软件公司的源代码，制造飞机制造公司的设计图纸，并且，这种趋势呈现着愈演愈烈的势态；
- 2、设备制造厂商不断研制和投入使用了各种数据存储设备，容量更大、速度更快的移动存储设备不断被投入使用，一个it管理人员的公文包足够装入一个中型公司有价值的数据资产了；
- 3、更快的网络高速公路被建成，并实现最后一公里的通车，数据更容易在最短的时间被传递到网络上，从此失去数据主人更改和删除的控制，数量不菲的个人在网络上均有自己的数据仓库（免费的mail信箱、网络硬盘.....）；
- 4、无线数据传输的发展，迎来了人类数据交换的新纪元：3g，4g，wifi.....；
- 5、电磁数据捕捉技术不断发展，停在楼下的一辆长久不动的面包车，可能就是您的电脑屏幕数据的还原设备.....；

- **便捷，其实不仅仅意味自己的便捷；效率，其实不仅仅意味着自己的效率。**

数据防护的必要性

- 数据的泄密途径；

- 数据途径分类
- 1、计算机电磁波辐射泄漏。
- 2．计算机网络化造成的泄密。
- 3、计算机媒体泄密。
- 4．内部工作人员泄密

数据防护的必要性

- 数据的泄密途径；

- 操作类型分类

- **服务器泄密：**
- 网络维护人员在进行维护时使用移动硬盘将服务器上的资料自备一份。
- 维护人员知道服务器密码，远程登陆上，将服务器上的资料完全的拷到本地或者自己家里的机器上。

工作站泄密：

- 乘同事不在，开启同事电脑，浏览，复制同事电脑里的资料。
- 内部人员将资料通过软盘、U盘或移动硬盘从电脑中拷出带走。
- 将笔记本（或者台式机）带出管控范围重装系统或者安装另外一套系统从而将资料拷走。
- 将笔记本（或者台式机）带出管控范围利用GHOST程序进行资料盗窃。
- 将笔记本（或者台式机）的硬盘拆回家盗窃资料，第二天早早来泰普森恒丰安装上。
- 将办公用便携式电脑直接带回家中。
- 将笔记本（或者台式机）带出管控范围使用光盘启动的方式，使用磁盘管理工具将资料完全拷走。
- 将笔记本（或者台式机）的硬盘或整机送修，资料被好事者拷走。
- 电脑易手后，硬盘上的资料没有处理，导致泄密。
- 笔记本（或者台式机）遗失或者遭窃，里面的资料被完整的窃取。

- **网络泄密：**
- 内部人员通过互联网将资料通过电子邮件发送出去。
- 内部人员通过互联网将资料通过网页bbs发送出去。
- 随意将文件设成共享，导致非相关人员获取资料。
- 将自己的笔记本带到泰普森恒丰，连上局域网，窃取资料。
- 输出设备（移动设备）泄密：
- 移动存储设备共用，导致非相关人员获取资料。移动设备包括：u盘、移动硬盘、蓝牙、红外、并口、串口、1394等
- 将文件打印后带出。

- **客户泄密：**
- 客户将泰普森恒丰提供的招标文件自用或者给了竞争对手。
- 客户处管理不善产生的泄密。

数据防护的必要性

- 参考

- 1、计算机电磁波辐射泄漏
一类传导发射，通过电源线和信号线辐射
另一类是由于设备中的计算机处理机、显示器有较强的电磁辐射。
计算是靠高频脉冲电路工作的，由于电磁场的变化，必然要向外辐射电磁波。这些电磁波会把计算机中的信息带出去，犯罪分子只要具有相应的接收设备，就可以将电磁波接收，从中窃得秘密信息。据国外试验，在1000米以外能接收和还原计算机显示终端的信息，而且看得很清晰。微机工作时，在开阔地带距其100米外，用监听设备就能收到辐射信号。
这类电磁辐射大致又分为两类：
第一类是从计算机的运算控制和外部设备等部分辐射，频率一般在10兆赫到1000兆赫范围内，这种电磁波可以用相应频段的接收机接收，但其所截信息解读起来比较复杂。
第二类是由计算机终端显示器的阴极射线管辐射出的视频电磁波，其频率一般在6．5兆赫以下。对这种电磁波，在有效距离内，可用普通电视机或相同型号的计算机直接接收。接收或解读计算机辐射的电磁波，现在已成为国外情报部门的一项常用窃密技术，并已达到很高水平。
2．计算机网络化造成的泄密
由于计算机网络结构中的数据是共享的，主机与用户之间、用户与用户之间通过线路联络，就存在许多泄密漏洞。
（1）计算机联网后，传输线路大多由载波线路和微波线路组成，这就使计算机泄密的渠道和范围大大增加。网络越大，线路通道分支就越多，输送信息的区域也越广，截取所送信号的条件就越便利，窃密者只要在网络中任意一条分支信道上或某一个节点、终端进行截取。就可以获得整个网络输送的信息。
（2）黑客通过利用网络安全中存在的问题进行网络攻击，进入联网的信息系统进行窃密。
（3）INTERNET造成的泄密
在INTERNET上发布信息把关不严；INTERNET用户在BBS、网络新闻组上网谈论国家秘密事项等；
使用INTERNET传送国家秘密信息造成国家秘密被窃取；内部网络连接INTERNET遭受窃密者从INTERNET攻击进行窃密；处理涉密信息的计算机系统没有与INTERNET进行物理隔离，使系统受到国内外黑客的攻击；间谍组织通过INTERNET搜集、分析、统计国家秘密信息。
（4）在INTERNET上，利用特洛尹木马技术，对网络进行控制，如BO、ＢＯ２０００。
（5）网络管理者安全保密意识不强，造成网络管理的漏洞。
3、计算机媒体泄密
越来越多的秘密数据和档案资料被存贮在计算机里，大量的秘密文件和资料变为磁性介质和光学介质，存贮在无保护的介质里，媒体的泄密隐患相当大。
（1）使用过程的疏忽和不懂技术。存贮在媒体中的秘密信息在联网交换被泄露或被窃取，存贮在媒体中的秘密信息在进行人工交换时泄密。
（2）大量使同磁盘、磁带、光盘等外存贮器很容易被复制。
（3）处理废旧磁盘时，由于磁盘经消磁十余次后，仍有办法恢复原来记录的信息，存有秘密信息的磁盘很可能被利用磁盘剩磁提取原记录的信息。这很容易发生在对磁盘的报废时，或存贮过秘密信息的磁盘，用户认为已经清除了信息，而给其它人使用。
（4）计算机出故障时，存有秘密信息的硬盘不经处理或无人监督就带出修理，或修理时没有懂技术的人员在场监督，而造成泄密。
（5）媒体管理不规范。秘密信息和非秘密信息放在同一媒体上，明密不分，磁盘不标密级，不按有关规定管理秘密信息的媒体，容易造成泄密。
（6）媒体失窃。存有秘密信息的磁盘等媒体被盗，就会造成大量的国家秘密外泄其危害程度将是难以估量的。各种存贮设备存贮量大，丢失后造成后果非常严重。
（7）设备在更新换代时没有进行技术处理。
4．内部工作人员泄密
（1）无知泄密。如由于不知道计算机的电磁波辐射会泄露秘密信息，计算机工作时未采取任何措施，因而给他人提供窃密的机会。又如由于不知道计算机软盘上剩磁可以提取还原，将曾经存贮过秘密信息的软盘交流出去或废旧不作技术处理而丢掉，因而造成泄密。不知道上INTERNET网时，会造成存在本地机上的数据和文件会被黑客窃走。网络管理者没有高安全知识。
（2）违反规章制度泄密。如将一台发生故障的计算机送修前既不做消磁处理，又不安排专人监修，造成秘密数据被窃。又如由于计算机媒体存贮的内容因而思想麻痹，疏于管理，造成媒体的丢失。违反规定把用于处理秘密信息的计算机，同时作为上INTERNET的机器。使用INTERNET传递国家秘密信息等。
（3）故意泄密。外国情报机关常常采用金钱收买、色情引诱和策反别国的计算机工作人员。窃取信息系统的秘密。如程序员和系统管理员被策反，就可以得知计算机系统软件保密措施，获得使用计算机的口令或密钥，从而打入计算机网络，窃取信息系统、数据库内的重要秘密；操作员被收买，就可以把计算机保密系统的文件、资料向外提供。维修人员被威胁引诱，就可对用进入计算机或接近计算机终端的机会，更改程序，装置窃听器等

数据防护的必要性

- 数据泄漏的案例；

- 镜头？：
- 北京时间10月5日消息，据国外媒体报道，欧洲著名电信运营商德国电信周六承认，其子公司德国移动（T-Mobile）的1700万客户数据遭窃
- 镜头一：
- 2008中新网5月8日电，香港入境处多份机密文件被发现上载至点对点分享平台，当中包括列入入境监视黑名单人士名称、投诉人资料、检查护照的机密细节等。
- 镜头二：
- 2007年11月20日，英国财政大臣阿利斯泰尔·达林在国会证实，税务及海关总署邮寄丢失两张重要数据光盘，其中包括2500万人的敏感信息，属“重大失误”。英国首相布朗11月21日在议会就此事公开道歉，并宣布政府已就此事件展开深入调查。
- 镜头三：
- 20050606\快递失手 花旗集团遗失390万名客户敏感信息
- 镜头四：
- 20050622美国爆发了有史以来最严重的信用卡资料泄密事件。4000万张信用卡资料在美国被黑客窃取。
- 镜头五：
- 2005年香港神州数码财报被偷，公司宣布停牌一天。

- 这些其实是冰山的一角。

数据防护的必要性

- **巨人实例分析：**

- 巨人（征途网络）公司内部程序员将源程序带走，大肆扶持私服，这个程序员已经将源程序有意售出数百份，以躲避公安的侦查…… 。

- 纳斯达克，征途网络股票一周内下跌36%，一刹那，巨人陷入危机中

- 公司不得不启动危机公关，声明股票下跌还有其他因素的影响；公司积极和公安机关配合在一年之后将盗窃者送入囹圄中，但耗资……；

数据防护的必要性

- **某制造公司实例分析：**

- 某制造公司高管离职将设计图纸带走，在我国“同业竞争”法律规定还不太完备的情况下、以及当事人息事宁人的处事态度下，另外一家民营企业的制造公司风风火火大力发展了起来，而且效益极佳……

- 原来公司不仅仅是面临着智力资产的散失，更重要的是市场上多了一个难以想象的竞争对手！

- 公司不得不启动危机公关，但效尤者众，类似事件又发生了……

数据防护的必要性

- **英国实例分析：**

- 2007年11月，各大媒体争相报道英国数据光盘丢失事件，称该事件是历史上罕见的数据泄漏事件，震惊了英伦三岛，也震惊了全世界。事发后，直接导致税务和海关总署署长保罗.格雷的辞职。整个英国上下都在为光盘的丢失感到非常不安，因为这两张光盘记录着涉及到750个家庭的2500万人的个人信息。要知道，2500万人，对于英国来说，不是一个小数字，它将近英国人口的一半。

- 据Gartner的估计，在银行方面的直接经济损失（关闭账号、另开账号、更换信用卡等） 就可能高达5亿美元。Gartner的安全分析师Avivah Litan估计每个账号20美元应该属于保守的估计。

- 更重要的是，这起事件必须引起政府和民众对各领域公共信息安全的重视，因为目前各国政府机构和公司都大量使用网络进行信息管理，一旦出现有意或无意的信息泄密，后果将比光盘遗失事件还要严重得多。

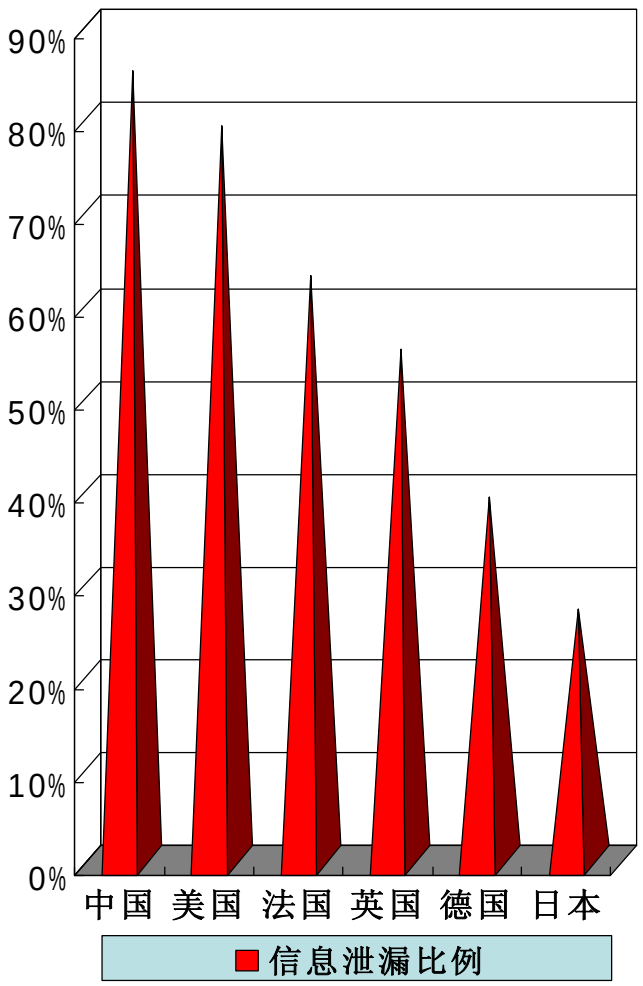
数据防护的必要性

- 数据泄密的数据

- 报告显示，在过去的一年中，美国有79%的企业发生过信息泄露事件。 法国企业发生过信息泄露事件的比例为63%，位居第二；英国第三，比例为55%。德国的比例为39%。

- 该结果源自对来自美国、英国、法国和德国的3596名IT专业人员的调查，值得注意的是，41%的信息泄露事件发生在大型主机上，而大型主机存储着全球80%的数据。

- 根据艾睿电子公司(Arrow Electronics Inc)本周公布的研究报告显示，与降低经营成本相比，大多数中型美国企业都会把信息安全看得更为重要。
- 在参与调查的200家美国公司中，近80%的公司都将信息安全看做最为关注的商业问题，有69%的公司首选降低成本，还有64%的企业则将改善客户服务作为其主要关心的问题。
受艾睿调查的公司年收入范围从不到1亿美元至超过10亿美元。



数据防护的必要性

数据泄密的数据；

- **在世界范围内，各种形式的企业、个人智力资产面临着巨大风险**
- **最新调查报告显示，75%的企业信息泄露事件都是由内部员工造成的，1%是因为外部黑客造成的。**
- **“没有谁能像一座孤岛 /在大海里独踞 /每个人都像一块小小的泥土 /连接成整个陆地 /如果有一块泥土被海水冲击 /欧洲就会失去一角 ……”**

- 所有的东西都在数字化！
- 没有什么东西不能通过数字化手段连接到网络上！
- 所有的人都更轻易使用更便捷的手段轻易获得!
- 获得数字化资料只需要更短的时间了！
- 网络犯罪已经已经有技术炫耀进入了利益驱动型，已经由零散的个人行为进入有组织的行为，受雇佣行为！

数据防护的必要性

- 国家法律和法规；

- **国际：**
- **法案：**
- 2004年，在美国上市的公司迎来了**《塞班斯法案》**，意味着在美国上市的公司不仅要保证其财务报表数据的准确，还要保证内控系统能通过相关审计。

- **国内**
- **法案：**
- 财政部、证监会、审计署、银监会、保监会联合发布了我国第一部**《企业内部控制基本规范》**，意味着中国会计审计领域的又一重大改革举措。该基本规范将于2009年7月1日起首先在上市公司范围内施行，并鼓励非上市的其他大中型企业执行。有知名专家称之为中国版的“塞班斯法案”，并认为是中国市场规则与国际融合的信号之一。**加强内控**和法规遵从已成为很多已上市或准备上市企业需要迫切解决的问题。

- 国家7部委联合发文，进行信息安全等级保护推广，国家相关的机构必须达到相应的安全等级；

数据防护的必要性

- 解决方案的依据

- 1、信息技术实施指南(ISO27001)
- 2、信息技术实施指南(企业内部控制制度基本规范)
- 3、赛班斯法案

制造企业信息安全现状

- 制造研发体系管理现状；
- 制造营销体系管理现状；
- 制造信息安全风险解构；
- 各类安全解决方案分析；
- 合作公司采纳解决方案；

制造企业信息安全现状

- 制造研发体系管理现状

- 制造设计因数据的不可想象之大，目前均使用CAD-CAM，数据形式均是以电子数据的形式存在；
- 制造设计研发机构因项目的复杂性，一般均使用系统式的设计研发管理工具，如外高桥造船使用Tribon系统对新船进行设计研发和管理：网络维护人员、一般技术管理人员和设计者均可以比较方便的拿到数据；
- 2008年国家信息技术实施指南(企业内部控制制度基本规范)颁布和实施，目前制造企业在IT管理方面尚未按照规范要求进行全局建设；“规范”是根据国家有关法律法规，财政部会同证监会、审计署、银监会、保监会制定了《企业内部控制基本规范》，现予印发，自2009年7月1日起在上市公司范围内施行，鼓励非上市的大中型企业执行；
- 制造业务发展速度往往远远大于IT管理发展速度，目前在基础网络构建上已经基本可以满足企业的需要，但在信息技术的管理方面需要进步；

制造企业信息安全现状

- 公司营销体系管理现状

- 公司营销一直冲在队伍的最前头，因业务的需要，也有大量的人员携带数据在客户现场工作，从而和客户存在着大量的数据互换行为，甚至这种互换行为是无法约束的互换；
- 在企业内部也存在着因为业务的需要，营销人员持有更多的技术数据、企业发展数据等等不宜公开传播的数据，但因为处于历史的原因，流通的管理主要靠人的自觉的约束；
- 营销人员的移动设备的使用也处于开放的现状；

制造企业信息安全现状

- 公司信息安全风险解构

- 作为10大振兴产业，企业的高速发展是制造企业的主旋律；但高速发展下面隐藏着一系列需要重视的安全风险；
- 人的风险：人是信息的载体，作人才的高地，制造企业均有相对的优势，但人才、核心人才必然会流动；
- 产业竞争的风险：制造公司所面临的竞争对手各各不一，我们面临的竞争对手毕竟一点一点对我们进行进攻，“玉树临风，风必摧之”；
- 国家管理的风险：为了防范有意和无意的安全风险，国家在上市企业内部率先实施《企业内部控制规范》，并鼓励未上市企业参照执行，不加强管理，对制造企业的未来也有影响；
- 不断发展的信息技术的风险：不断发展的有线、无线网络，数据存储设备，数据交换方式对企业的管理带来了极大的效率提升，同时也置企业于极大的安全风险之中；

- ……

制造企业信息安全现状

- 各类安全解决方案分析

- 目前国际、国内主流的结束解决方案主要有以下几种：
- 1、物理封堵
- 主要采取的措施就是电脑不上网，并且将usb等等使用硅胶封闭掉，也有采用技术手段封堵的；
- 采用这种方法的主要在部分政府部门的内网机器；此方案同时还是有些公司的补充方案，如华为公司在半军事化的管理模式下，有些部门也采用了这种解决方案；
- 这种方案主要的解决思路是以牺牲效率为代价，并且并不能真正解决问题，如硬盘被拆除外挂仍然会造成数据的泄密；
- 2、网络封堵
- 主要采用在网络上架设类似反垃圾邮件（关键字技术）防止携带了关键字的数据外漏；
- 这类技术的供应商主要是一些外资驻华办事机构，主要原因是加密技术对话出口目前发仍然处于禁止状态。目前部分外资在华机构是使用了这类产品的解决方案；
- 这种解决方案本身存在着极其容易被攻破（伪造、变化、加壳等）的缺陷，并且对公司带出的设备也处于无法管理的无奈，只能说是一种适应局部范围的解决方案；

制造企业信息安全现状

- 各类安全解决方案分析

- 目前国际、国内主流的结束解决方案主要有以下几种：
- 3、手动加密
- 主要采取的操作者本人决定是否加密，在加密的同时赋予该文档一定的权限，这样，具有权限的人收到后就可以打开使用；
- 正是其完全由作者本人决定加密与否，该产品在中国的使用面极窄，这类产品的研发者主要是美国、日本的部分二流企业；
- 目前，该类产品在国内外资企业有少量的使用；
- 4、透明加密
- 使用者本人操作方式不做任何改变（透明），策略在后台实时动态工作，不管离线还是在线，不管是在企业内部还是在企业外部。这类产品特色显然比较适用国人的使用；
- 目前提供这样产品的公司规模一般并不太大，公司接触的比较大的公司是上海山丽信息安全公司，该企业有100余人，数条产品线。目前使用其产品的主要有上海海关、造币总公司、思源电气、中兴通讯、航天科技实业公司、二纺机、丰田汽车设计中心等机构；

制造企业信息安全现状

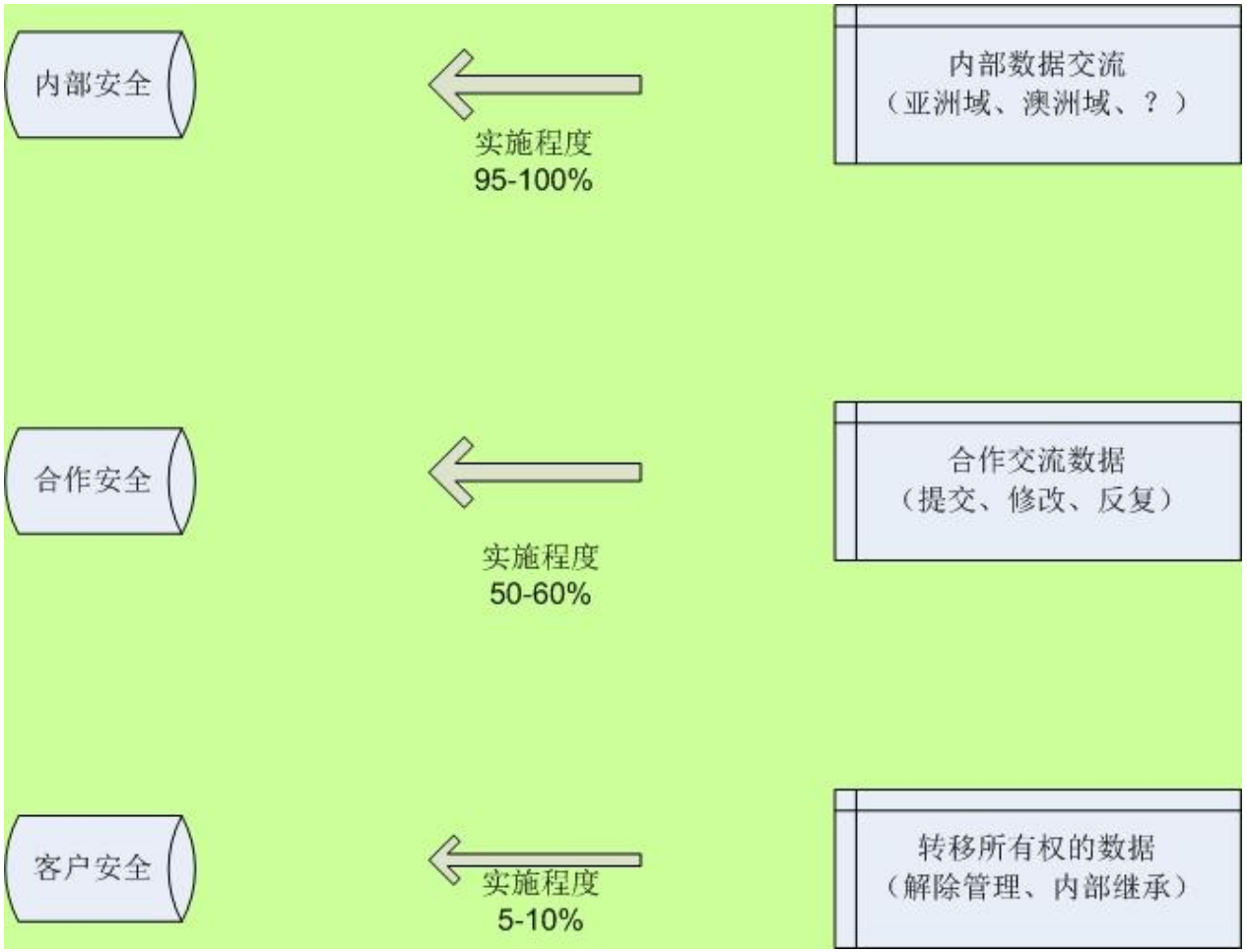
- 合作公司采纳解决方案；

- 1、物理封堵
- 政府内网机器；
- 2、网络封堵
- 部分外资在华机构，制造企业公司采用的IM管理也属于此范畴；
- 3、手动加密
- 部分外资在华机构；
- 4、透明加密
- 主流方案，目前技术条件下最安全的方案。
- 设计公司、设备制造公司、软件公司。

- 实际上，每个企业都有可能采用不同的方案来满足不同的安全需要，不同部门的需要。

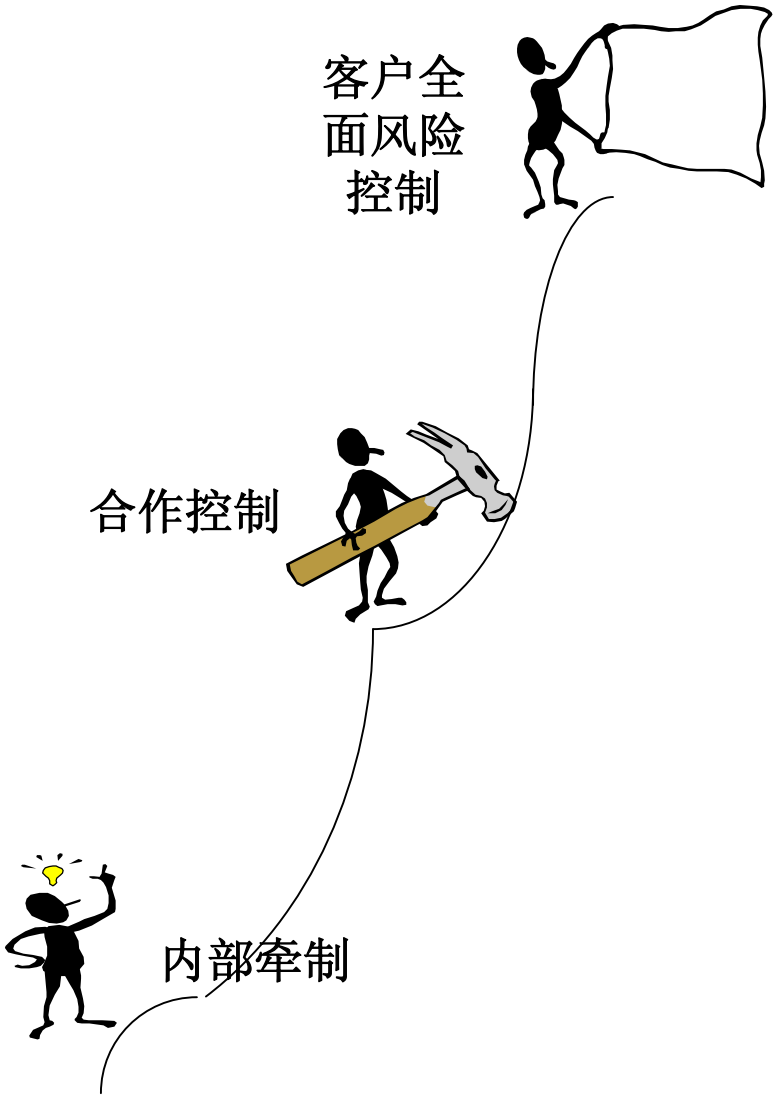
制造企业信息安全现状

- 数据生命周期的概念：DSL　DSLM
- 数据生命周期的流程：DSL



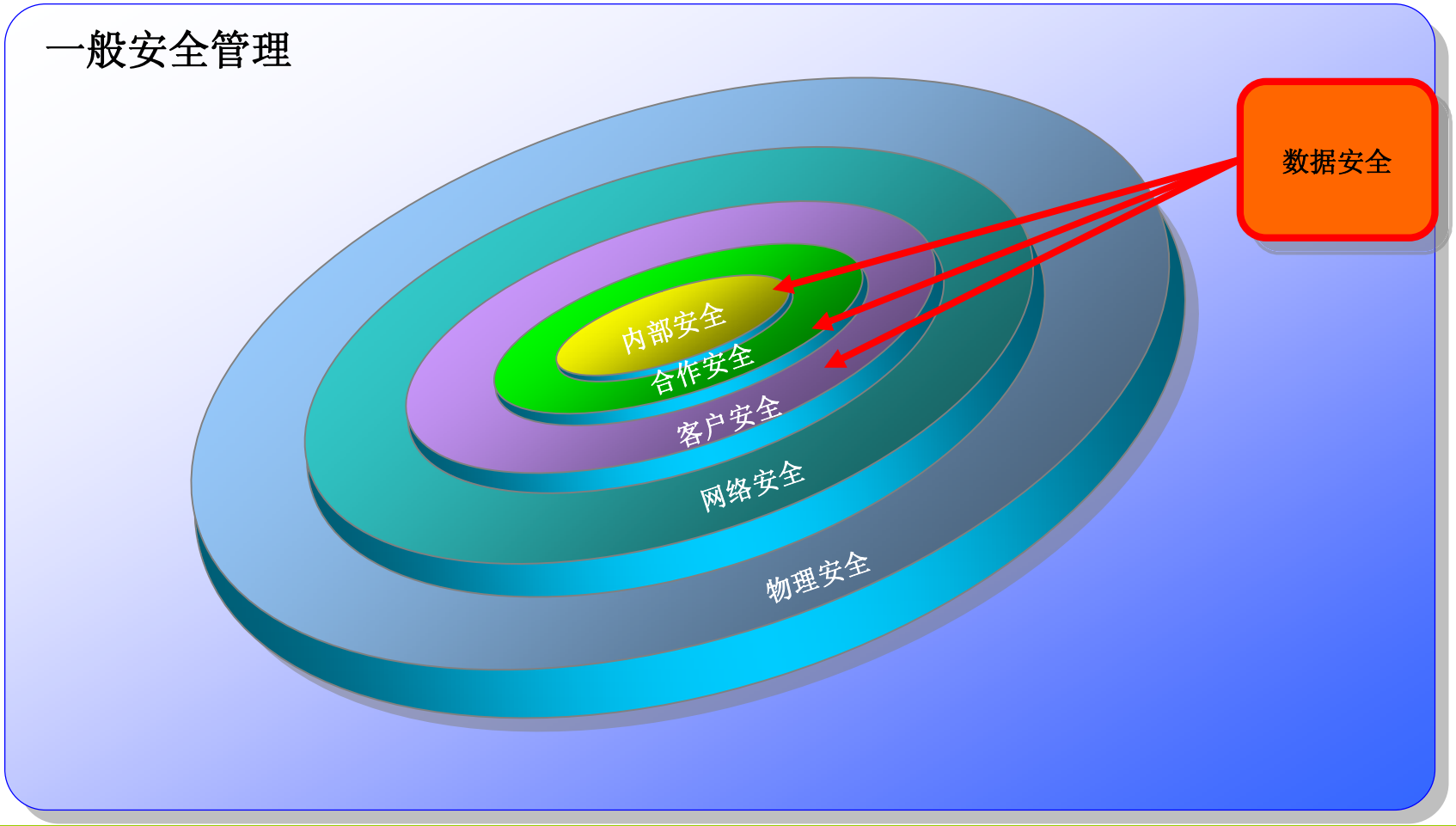
制造企业信息安全现状

- 数据生命周期的概念：DSL　DSLM
- 数据生命周期的管理：DSLM

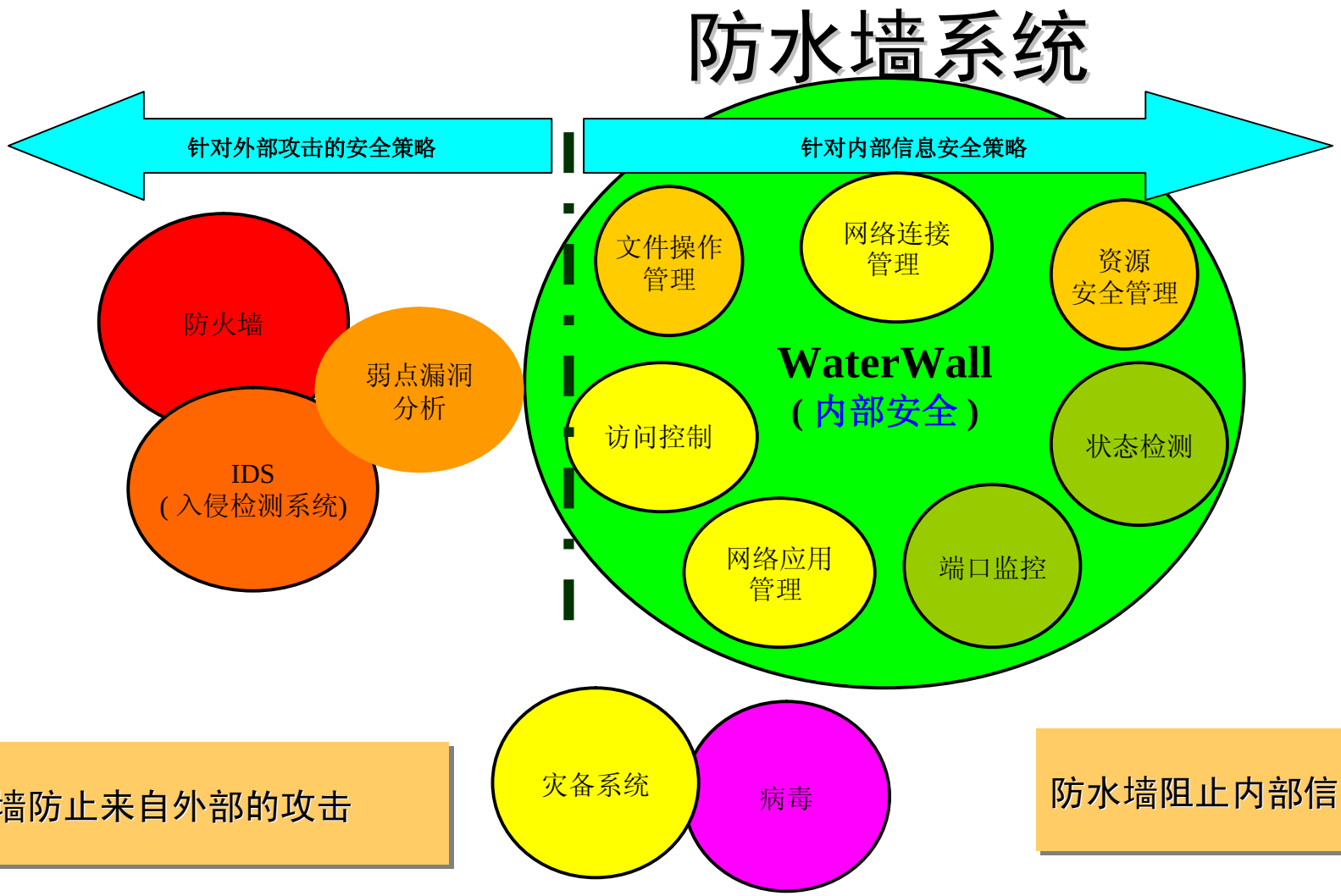


制造企业信息安全现状

- 数据生命周期的概念：DSL　DSLM
- 数据生命周期的管理：DSLM



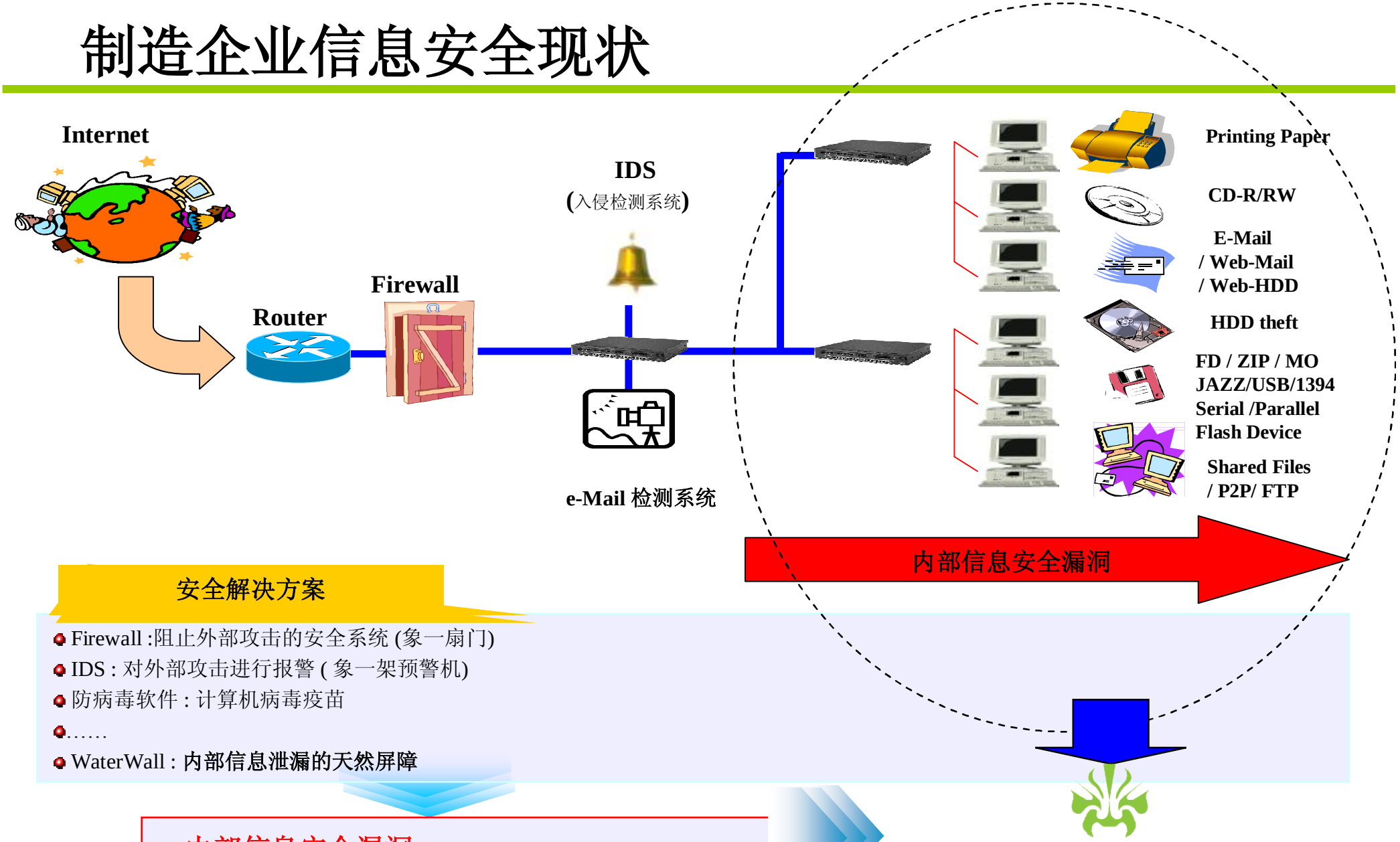
制造企业信息安全现状



防火墙防止来自外部的攻击

防水墙阻止内部信息的外泄

制造企业信息安全现状



安全解决方案

- Firewall :阻止外部攻击的安全系统 (象一扇门)
- IDS : 对外部攻击进行报警 (象一架预警机)
- 防病毒软件 : 计算机病毒疫苗
- ……
- WaterWall : 内部信息泄漏的天然屏障

内部信息安全漏洞

产品方案比较选择

- 法律限制；
- 资质限制；
- 产品报告；
- 测试结论；

产品方案比较选择

- 法律限制；

- 《商用密码管理条例》
- 第十四条　任何单位或者个人只能使用经国家密码管理机构认可的商用密码产品，不得使用自行研制的或者境外生产的密码产品。
- 第十五条　境外组织或者个人在中国境内使用密码产品或者含有密码技术的设备，必须报经国家密码管理机构批准；但是，外国驻华外交代表机构、领事机构除外。

产品方案比较选择

- 资质限制；

- 根据国家关于文档保护类软件的销售规定，生产厂家应当必须具有以下几种资质：
- 1、中华人民共和国公安部颁发的安全产品销售许可证
- 2、中华人民共和国保密局颁发的涉密信息系统检测证书（销售许可证）
- 3、中国人民解放军总参谋部颁发的军用信息安全产品检测证书（销售许可证）
- 4、中华人民共和国密码管理局颁发的商用密码产品销售许可证
- 5、中华人民共和国密码管理局颁发的商用密码产品生产许可证
-
- 代理商除持有厂家的资质外，还必须有厂家给与的代理授权。

产品介绍

问题：

- 如何保障机密文件不被盗拷出公司?
- 如何保障机密文件不被盗拷出笔记本电脑?
- 如何留下每一个人对机密文件的操作证据(拷贝,打印,修改,删除)?
- 如何保障机密文件的限时授权? 当授权过期,如何保障机密文件的自我销毁?

……

机构或组织机密信息的
二次流传困扰着管理者

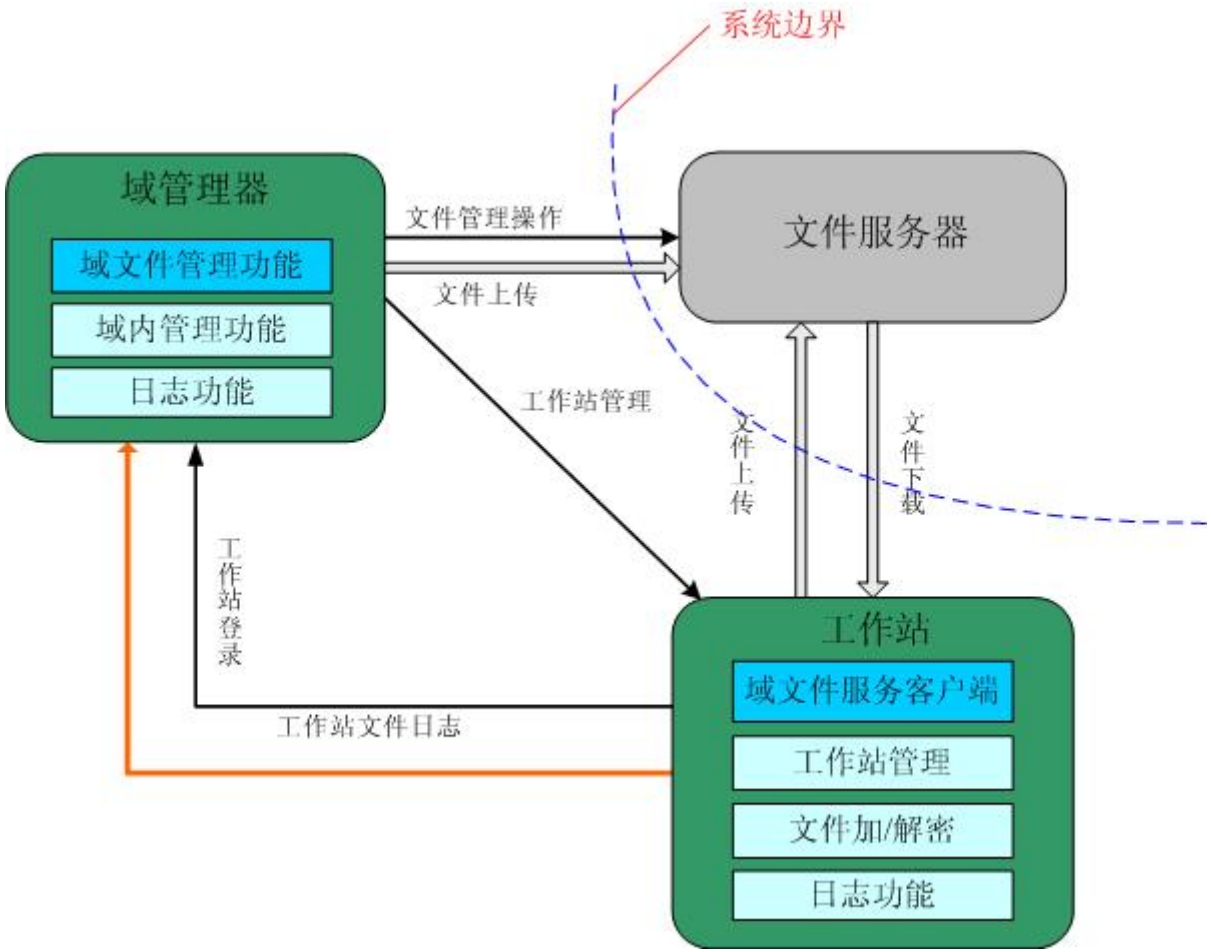
产品介绍

- 山丽防水墙数据防泄漏系统以“环境指纹”专利为基点，构建一个完备的数据防泄漏系统：

- “环境指纹”系统的各个子系统：
- 加解密子系统：透明、动态、实时
- 介质管理子系统：控制、认证、内容审计
- 客户端管理子系统：im、白名单
- 权限子系统：基于使用者身份、基于时间、基于内容等等环境
- 域管理子系统：安全域的概念
- 证书子系统：是密钥保护和身份认证的一部分
- 通讯子系统：加密传输
- 日志子系统：日志的收集、管理、分析

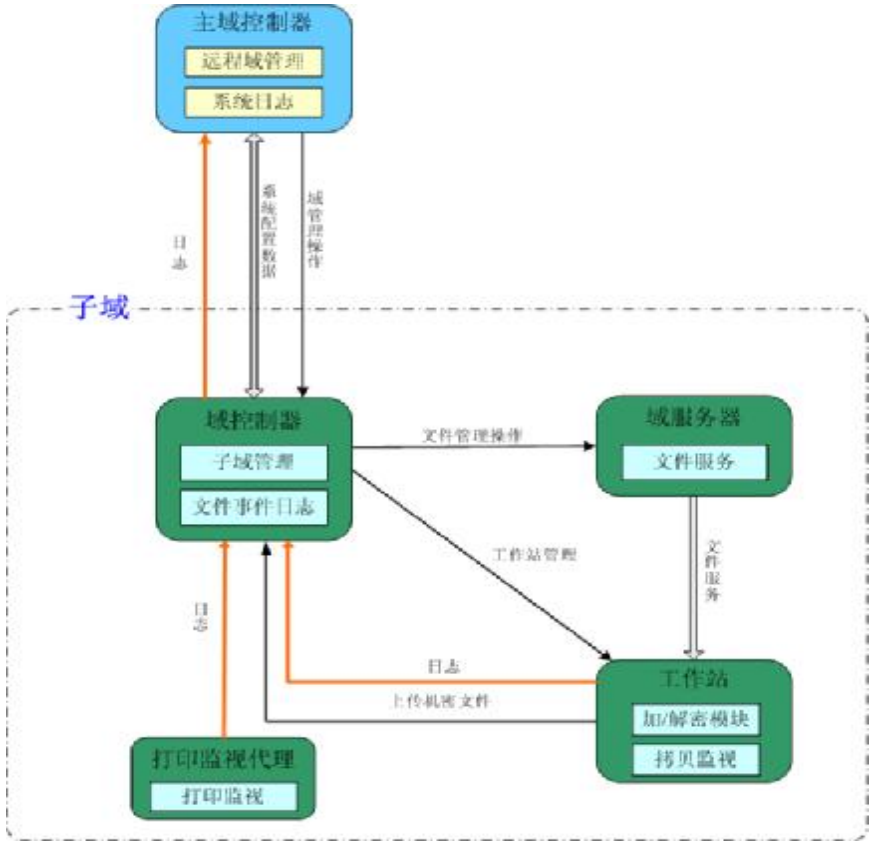
产品介绍

系统逻辑图



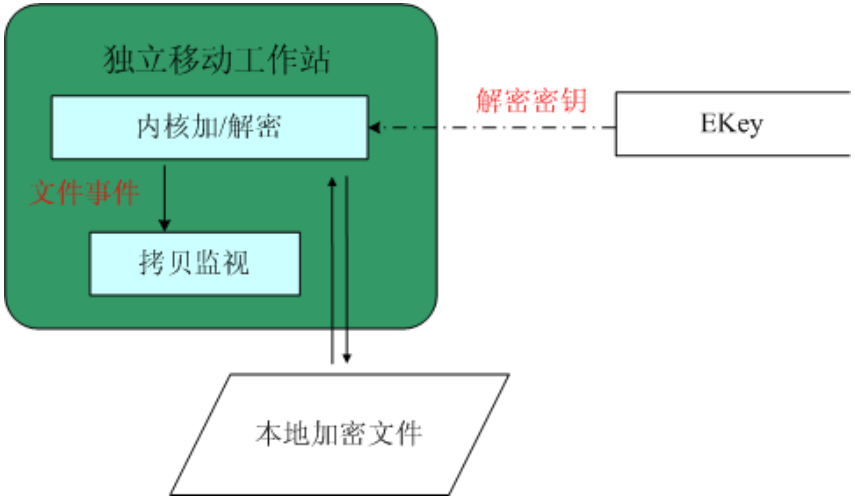
产品介绍

- 系统逻辑图



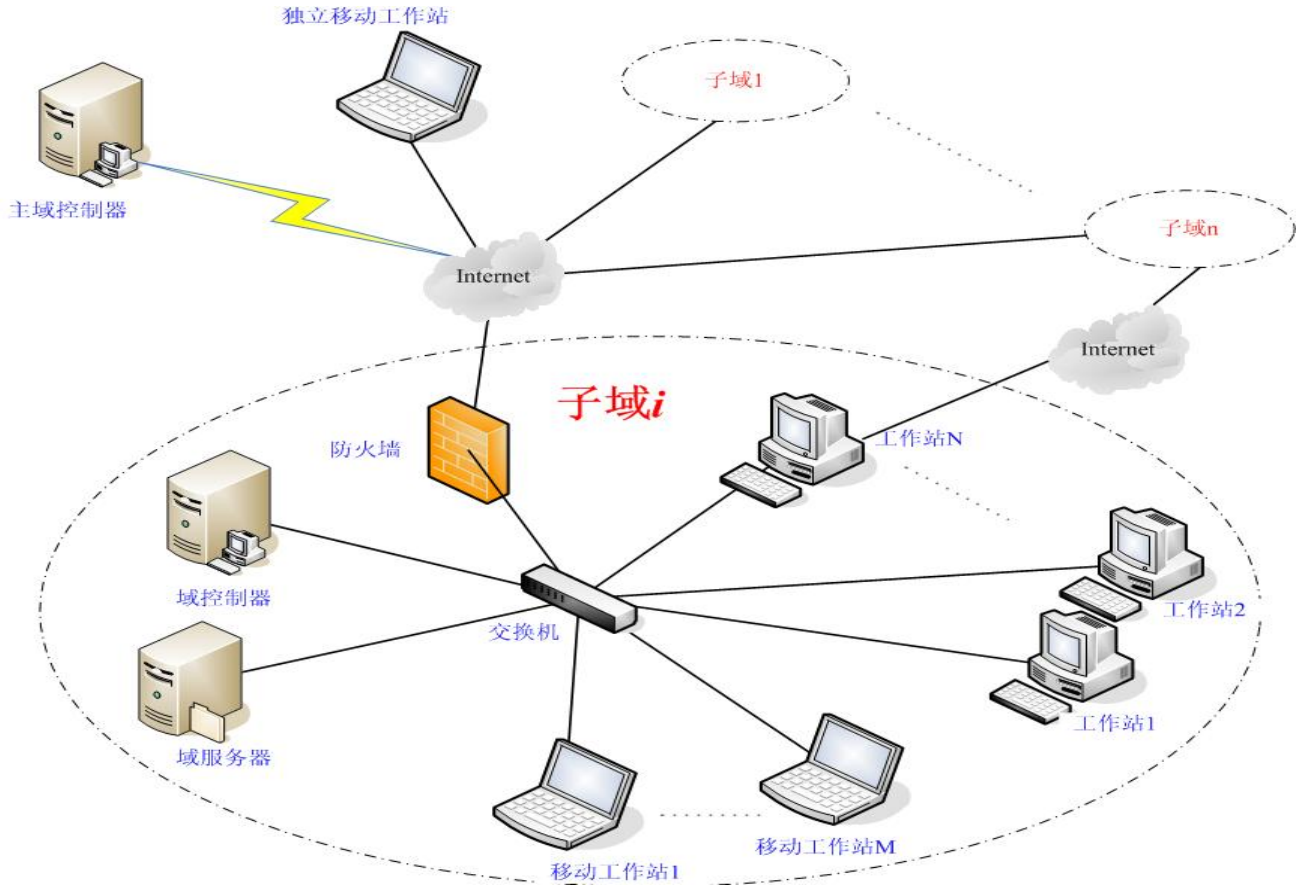
产品介绍

- 系统逻辑图



产品介绍

- 系统物理图

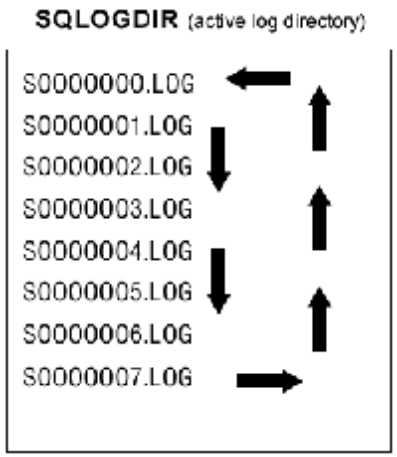


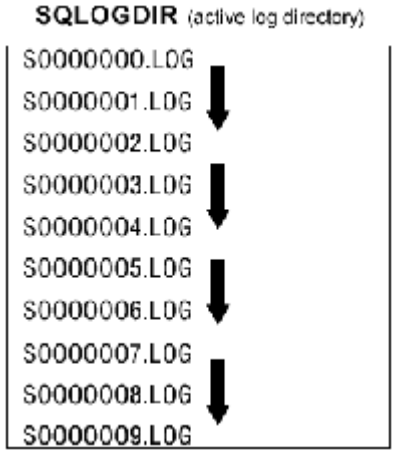
产品介绍

- **主要技术与性能指标**
-
- 最大工作站节点数：62500
  最大域服务器节点数：250
  最大并发认证数：62500
  最大并发文件连接：10000
  加密位数：128位/256位
- 加密算法：3DES-X/RSA/sm1支持网络类型：局域网/广域网/互联网
  文件访问支持协议：NetBIOS/HTTP/FTP
  支持平台：Microsoft Windows 95/98/2000/XP/Server 2003/vistra/windows7Linux/Unix
- 内核网络协议：TCP/IP
  加密算法：　3DES-X/RSA/sm1
  每秒加密字节数：　30Mb
  每秒解密字节数：　50Mb
  加密延迟：　<200ms
  解密延迟：　<100ms
  系统负荷：　<3%
-
- 最长生存期：　不受约束
- 最短生存期：　不受约束
- 时间合成算法：　不可逆
- 主要技术及性能指标：达到计算机信息系统安全保护等级划分准则 GB 17859-1999第四级：结构化保护级，第五级：访问验证保护级，执行的质量标准是：中华人民共和国国家标准 计算机信息系统安全保护等级划分准则 GB 17859-1999。

产品介绍

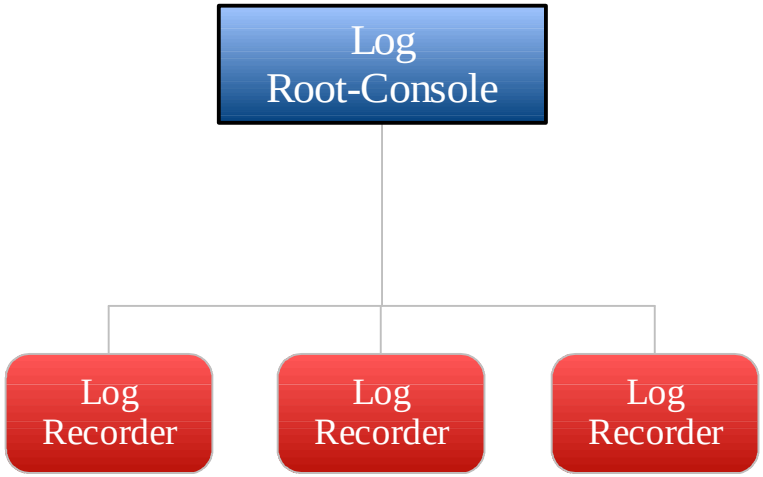
- 日志模式





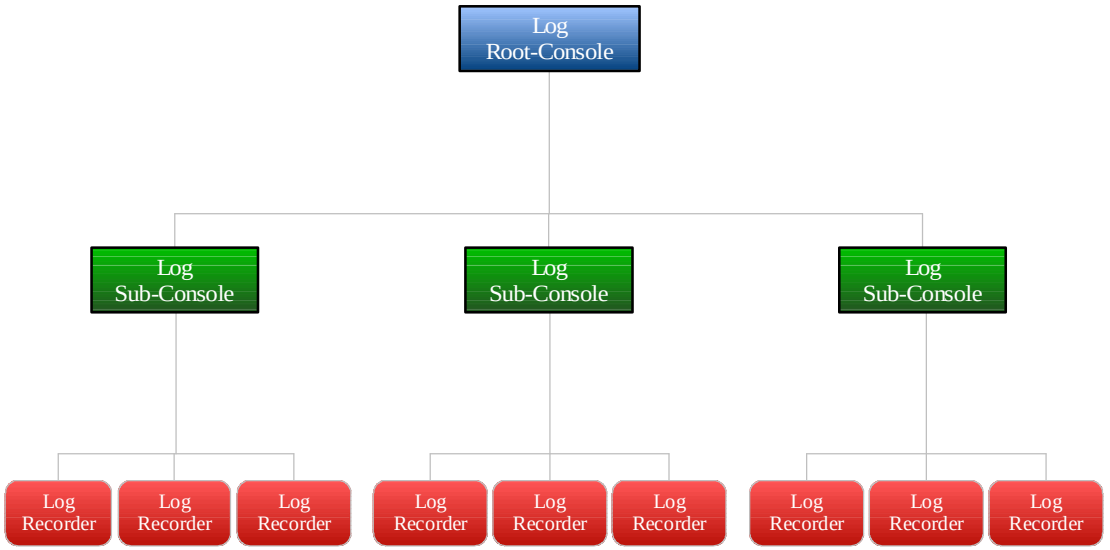
产品介绍

- 两层结构日志管理系统



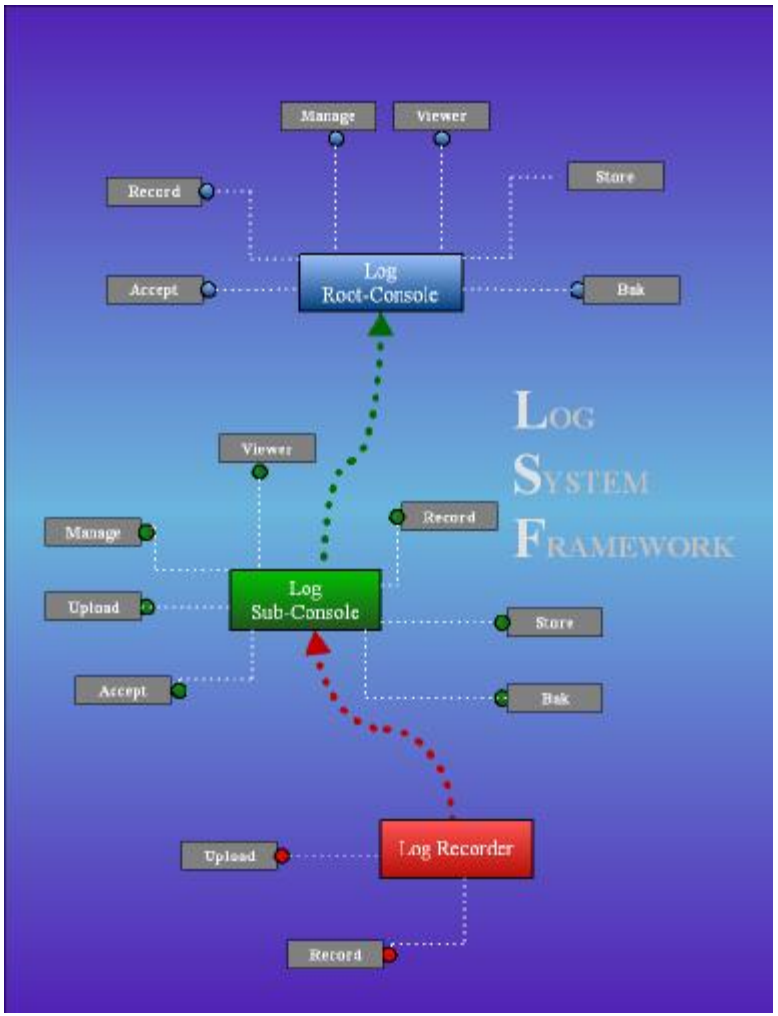
产品介绍

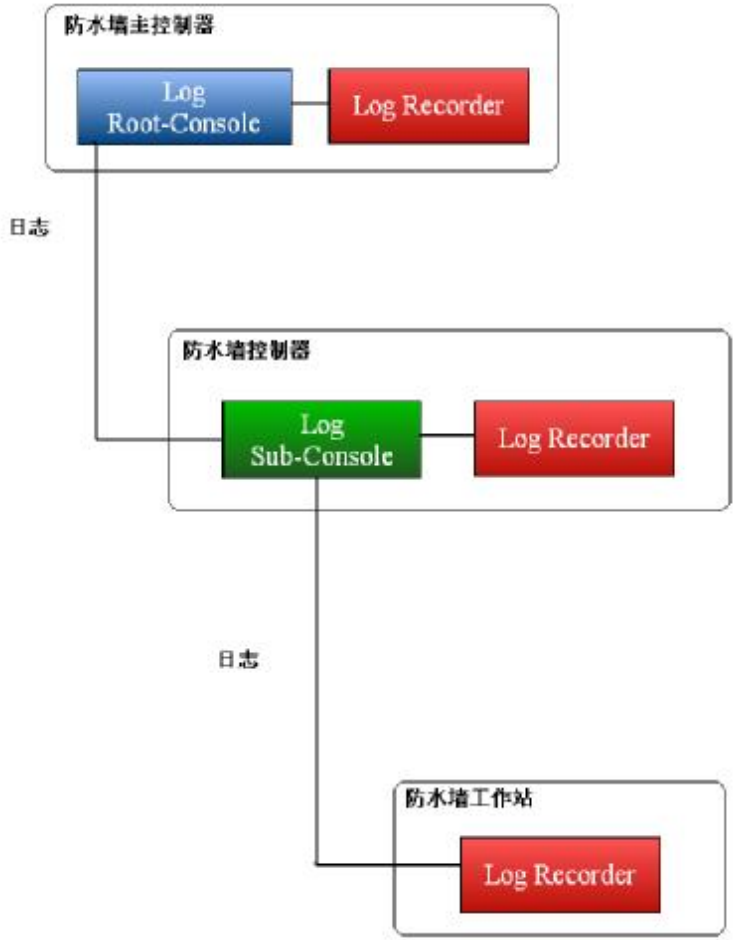
- 三层结构日志管理系统



产品介绍

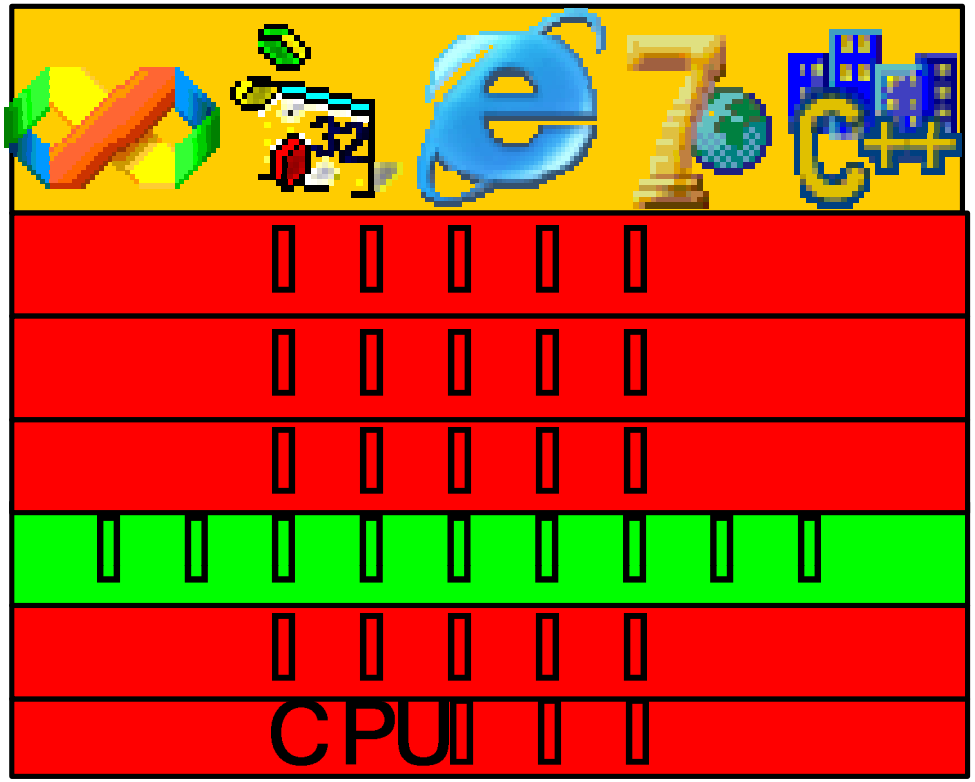
日志系统节点关系图





产品介绍

- 透明动态实时加解密子系统架构
- 计算机本身就体现了一种层的概念：系统调用层、设备驱动层、操作系统层、CPU指令集



产品介绍

- 防水墙环境指纹加密技术

  本系统创造性地引入了环境指纹设备，使得一个环境能够被独一无二地标识，且不可复制。所有应用本系统的单位都拥有自己的独特环境。即使安装的软件系统一模一样，由于环境指纹设备所产生的指纹数据并不相同，这些环境中的数据彼此不能有效交换。在一个特定的环境中，加密、授权、认证、解密等过程，都紧密依赖环境指纹。相比较起来，现有的加密、解密技术，例如文件保险箱技术等，加密和解密都只依赖于密钥，只要持有合法密钥，任何时间、任何地点都可以解密，这无法防止机密文件的在职泄漏或内部窃取。

产品介绍

- 防水墙环境指纹加密技术内核动态认证及加解密技术

- 这是本技术另一重要特点、创新点。其它的加解密系统，其加解密过程一般在应用层。其输入和输出文件（也就是加密和解密的结果）均是静态地保存于永久介质（例如硬盘、软盘、U盘等），从而存在着被拷贝并带走的漏洞。本系统将工作站的解密过程嵌入于操作系统内核中。且解密的结果只存在于动态存储器中供应用程序使用，由于并不解密到永久存储器，所以无法转移到电脑之外。如果使用者试图将解密的文本以新文件方式另外保存到磁盘。那么本系统内核仍然能在保存过程中将该新文件加密，且新文件同样受到环境限制。

  现有的加密、解密技术，都可以将解密的输出文件直接存储到磁盘，这从另一个方面增大了机密文件泄露的风险。

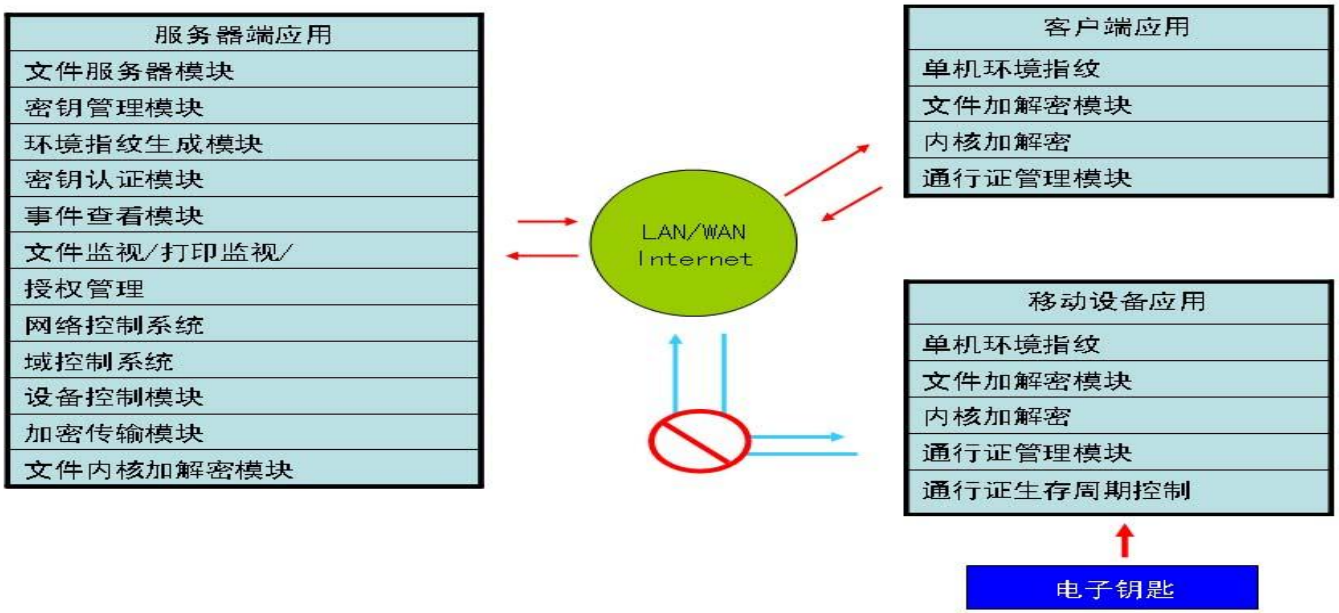
产品介绍

- 防水墙环境指纹加密技术密钥生存期技术
  密钥生存期的定义为：一段指定起止时刻的时间段，在此时间段内，密钥有效；而在这个时间段之外，密钥无效。
  给密钥加上生存期，使一种授权具有了自动失效的机制，从而锐减了密钥流失的风险。对于移动工作站的暂时性授权，特别有用。

  现有的加密、解密技术在密钥的使用上均没有时间因素。

产品介绍

WaterWall的系统架构



产品介绍

智力资产防盗

对被保护的数据，做到：

- 文件加密：盗走了，拿走了，没法用；
- 权限控管：谁能看，谁能印，防篡改；
- 时间期限：过期了，离职后，不能用；
- 使用追踪：谁看过，谁印过，有记录。

产品介绍

个人桌面系统（PC）信息泄漏保护

- **在线方式下，信息泄漏防护（网络通信）**
  - 端口： 0-65535任意制定端口；
  - 邮件应用：SMTP-Mail，Web-Mail等等；
  - 文件传输应用：FTP、Wu-ftp等等；
  - 网络联接：DDN，ISDN， PSTN(by Modem) 等等；
  - 点对点通信应用：BBS，P2P，ICQ，OICQ，QQ，Messager等等；
  - 文件共享应用：基于NETBIOS文件共享等等；
  - 个人桌面系统（PC）移动保护：脱网工作监控。
- **离线方式下，信息泄漏防护（存储媒体/介质）**
  - FD，MO，ZIP，JAZZ，Flash Device等等；
  - CD-R，CD-RW等等；
  - USB/1394 Storage Device等等；
  - 个人桌面系统（PC）移动保护：联网工作监控。
- **打印文件监控（打印机）**
  - 本地打印机/网络打印机；
  - 打印输出到其他应用系统，如：生成RTF，PDF文件等等。
- **显示器浏览文件监控（显示器）**
  - 利用主要系统应用程序对本机文件读取监控，如：MS Office，Notepad等等。

产品方案比较选择

- 结论

- 就前期的产品功能来看，山丽防水墙在满足制造企业公司的需求方面比较完善，产品性能也达到了要求，该企业的产品可以在企业内部实施。

产品方案比较选择

- 比较

- 以数据安全生命管理周期（DSLM）为主轴做一个对比
- 数据防泄漏软件实施方案的比较

山丽的调研和优势

- 企业状况；
- 产品情况；
- 服务支持；
- 比较优势；

山丽的调研和优势

- 企业状况

- **企业定位：**
- 世界范围内 信息安全行业 的领导企业
- 经营模式：网络安全、信息安全产品的研发和销售。

- **发展历程：**
- 2003年5月27日设立，注册资金100万；
- 2003年推出产品网络堡垒个人防火墙，研发安铁诺；
- 2004年推出产品安铁诺防病毒软件，研发防水墙；
- 2005年推出产品数据门卫软件，防水墙，研发动态口令、红色通道，企业通过cmm3，企业获得中国信息安全界十大创新企业；
- 2006年相关产品更新，获得创新基金，注册资金增加到1000万，实际投资超过2000余万；
- 2007年产品走向市场，产品进一步更新，企业获得中国信息安全企业十大品牌企业；
- 2008年，进行防水墙市场开拓，目前在制造业、金融业、军工业、通讯业均有案例

山丽的调研和优势

- **企业发展进度：**
- **商标：**
- 山丽、安铁诺、数据门卫、防水墙 sanlen antiunknown datagate
- **专利：**
- 具有指纹限制的机密文件访问授权系统申请号/专利号200410017241
- 剪切板信息保护装置和方法申请号/专利号： 200610029526
- 文件加密装置和方法以及文件解密装置申请号： 200610029528
- 监控键盘钩子的装置申请号/专利号： 200610029536
- 移动存储设备监控方法和装置申请号/专利号： 200610029529
- 应用程序保护装置和方法申请号/专利号： 200610029527
- 应用程序过滤方法和装置申请号/专利号： 200610029535
- 具有指纹限制的机密文件访问授权系统 ：pct
- **商业秘密：**
- 底层技术完整积累、大型软件架构的完整积累

山丽的调研和优势

- 著作权：

- 安铁诺防病毒软件
- 网络堡垒防黑软件
- 防水墙数据防泄漏系统软件
- 超级光速网络加速软件
- 防盗王银宝动态口令软件
- 数据门卫usb管控系统软件
- 红色通道文件加密传输软件
- 网络堡垒网络审计软件

山丽的调研和优势

- **山丽信息安全有限公司基本现状：**

- 山丽信息安全有限公司是一家专业的信息安全厂商，并进行自我产品的销售，目前产品销售范围主要在中国境内。公司在数据保护技术方面处于业界领先地位。
- 公司持有“防水墙”等系列商标；
- 公司持有“具有指纹限制的机密文件访问授权系统 ”专利等系列专利；
- 公司持有山丽防水墙数据防泄漏系统等产品；
- 2005年，企业被《通讯与保密杂志社》评为信息安全届十大创新企业；
- 2005年，企业通过软件能力成熟度CMM3；
- 2007年，企业被《通讯与保密杂志社》评为信息安全届十大品牌企业。

- **世界范围内，中国范围内，信息安全的焦点就在内网信息安全；**
- **山丽网安经过五年的潜心发展，正占据着中国、世界内网信息安全的一个制高点；**

山丽的调研和优势

- **山丽信息安全有限公司异地销售办事机构的布局：**

- 公司在广州、武汉、济南、北京、沈阳、西安、成都设立销售点，着重进行
- **代理商的开发；**
- **重点客户的开发；**

- 公司的目标客户群在于：
- 军工、政府、企业
- 公司客户群包括各国家部委、金融、电力、电信、军工集团、大型企业（集团），并向中小企业及个人用户拓展，销售主体为政府用户、金融和军工等大型企业集团用户。

- **山丽信息安全有限公司研发机构的布局：**

- 通过cmm的软件开发管理架构，核心技术研究和软件设计中心位于上海，利用上海的人才优势构建产品高度；

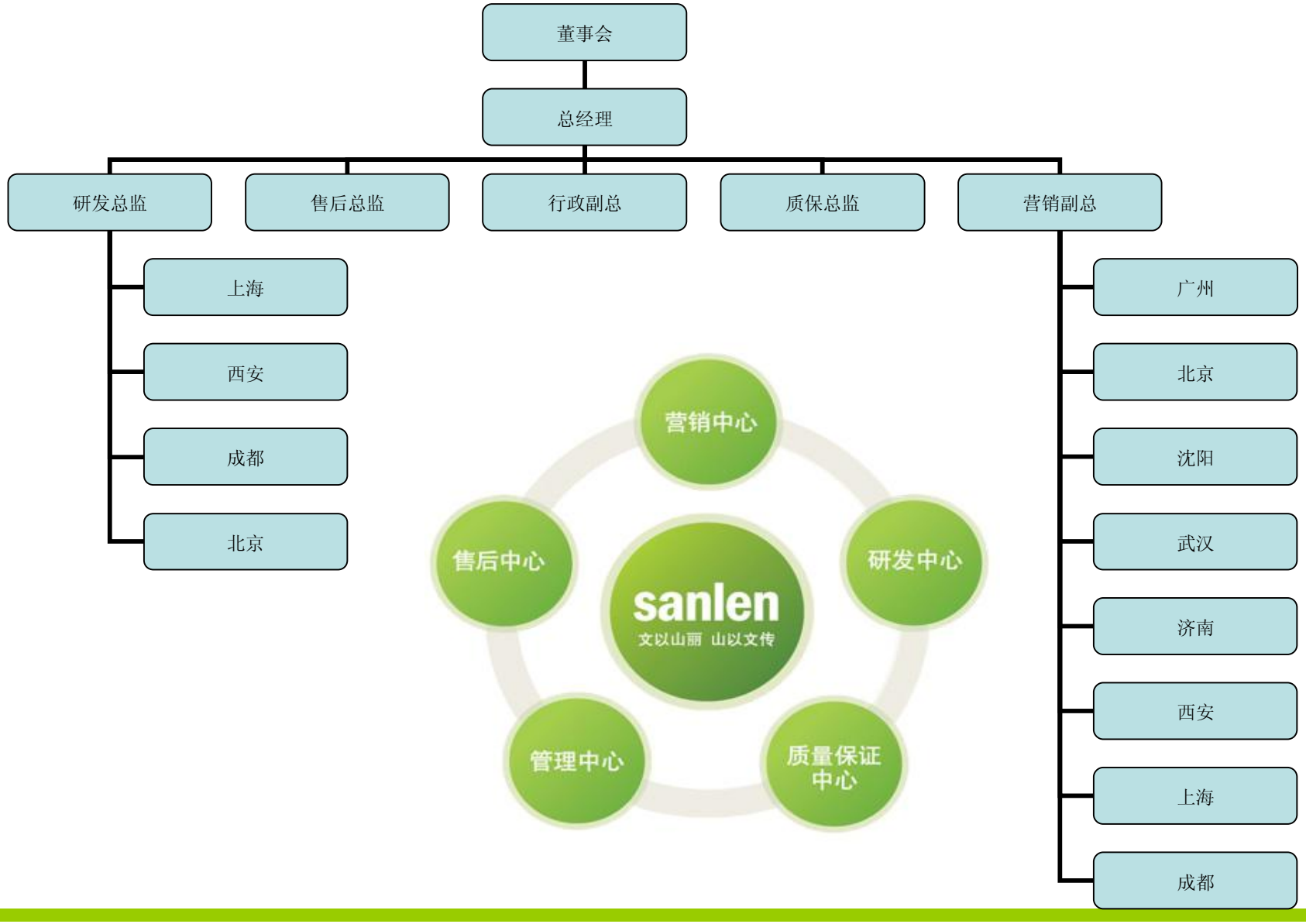
- 进一步有成都、西安开发中心分支，利用劳动力成本优势进行软件的编码和测试当地化，实现软件外围功能的商业目标；

山丽的调研和优势

- **公司已有的样板客户：**

- 中国人民银行造币总公司；
- 航天科技实业集团
- 上海海关；
- 中兴通讯
- 贵州检察院；
- 长沙交通稽查局；
- 思源电气；
- 复星药业；
- 上海水利设计院；
- 丰田汽车设计；
- 上海音乐学院；
- .....

山丽的调研和优势

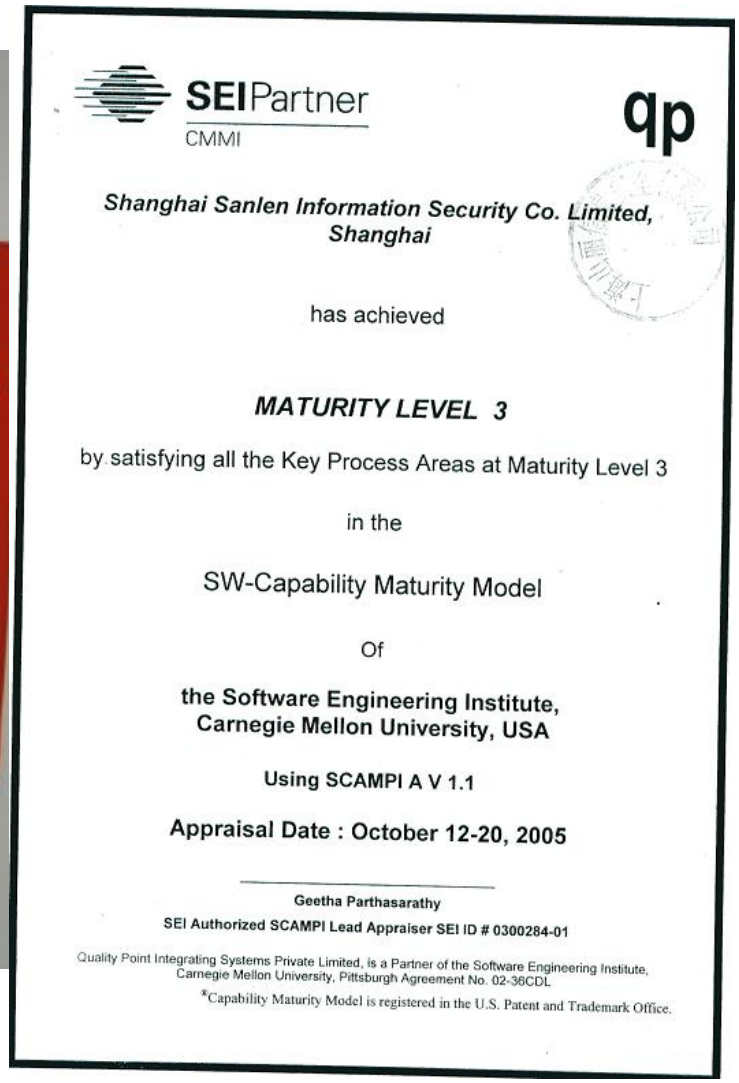


山丽的调研和优势

Ø 山丽网安通过CMM-3评估

CMM是由美国卡内基-梅隆大学的软件工程研究所(SEI)推出的评估软件能力与成熟度的一套模型。它侧重于软件过程开发的管理及软件工程能力的改进与评估，是目前国际上最流行、比较实用的一种软件生产过程标准，成为当今企业从事规模软件生产不可缺少的一项内容。CMM是全面质量管理(TQM)中的过程管理概念在软件方面的应用。它涵盖了有关计划、设计、编码、测试以及管理和支持软件开发的实践。软件组织只要遵循这些实践，就能够提高组织软件开发能力，满足降低成本、提高产品质量等目标。

山丽的调研和优势



SEIPartner
CMMI

qp

Shanghai Sanlen Information Security Co. Limited, Shanghai

has achieved

MATURITY LEVEL 3

by satisfying all the Key Process Areas at Maturity Level 3

in the

SW-Capability Maturity Model

Of

the Software Engineering Institute, Carnegie Mellon University, USA

Using SCAMPI A V 1.1

Appraisal Date : October 12-20, 2005

Geetha Parthasarathy

SEI Authorized SCAMPI Lead Appraiser SEI ID # 0300284-01

Quality Point Integrating Systems Private Limited, is a Partner of the Software Engineering Institute, Carnegie Mellon University, Pittsburgh Agreement No. 02-36CDL

*Capability Maturity Model is registered in the U.S. Patent and Trademark Office.

山丽的调研和优势

山丽的调研和优势

- 产品情况

- **销售许可：**
- 公安部颁发之销售许可证
- 保密局颁发之保密产品销售许可证
- 总参颁发之军队产品销售许可证
- 商密委员会颁发之密码产品销售许可证
- 商密委员会颁发之密码产品生产许可证

山丽的调研和优势

报告编号:公计检080156

检 验 报 告

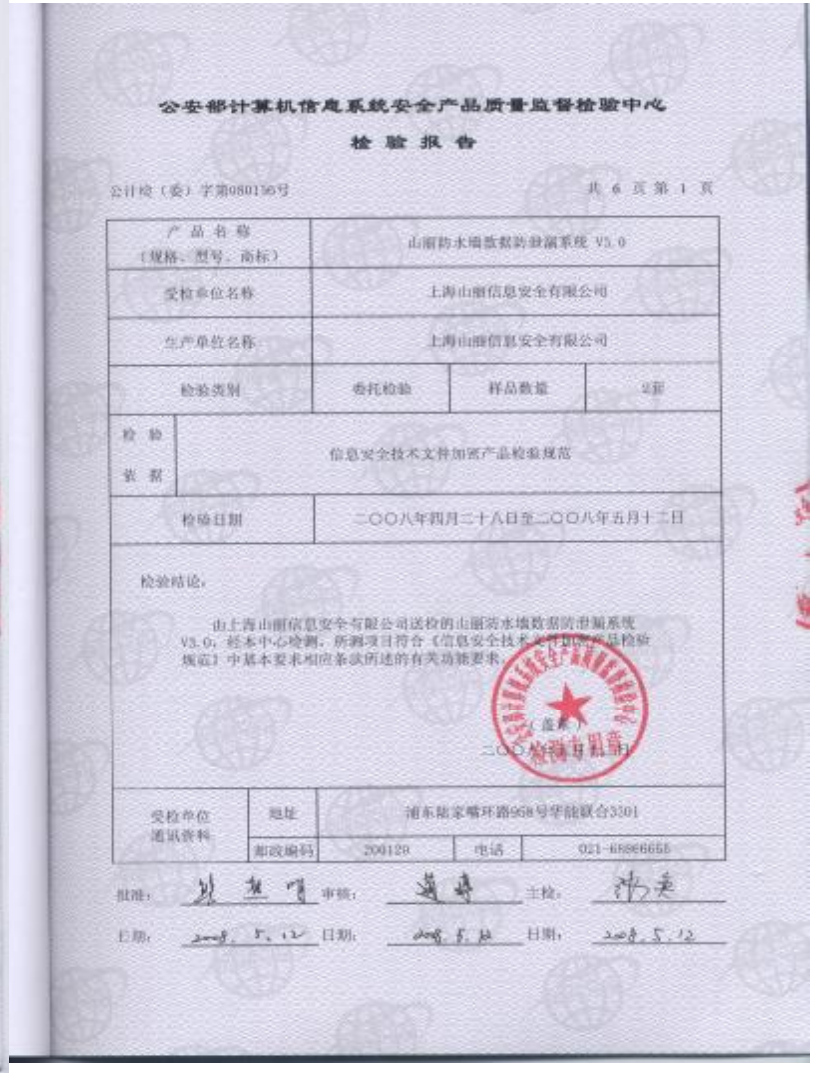
样品名称　山丽防水墙数据防泄漏系统

型号规格　V3.0

受检单位　上海山丽信息安全有限公司

检验类别　委托检验

公安部信息安全产品检测中心
公安部计算机信息系统安全产品质量监督检验中心



公安部计算机信息系统安全产品质量监督检验中心

检 验 报 告

公计检（委）字第080156号　　共 6 页 第 1 页

产品名称（规格、型号、商标）	山丽防水墙数据防泄漏系统 V3.0		
受检单位名称	上海山丽信息安全有限公司		
生产单位名称	上海山丽信息安全有限公司		
检验类别	委托检验	样品数量	2套
检验依据	信息安全技术文件加密产品检验规范		
检验日期	二〇〇八年四月二十八日至二〇〇八年五月十二日		

检验结论：

由上海山丽信息安全有限公司送检的山丽防水墙数据防泄漏系统V3.0，经本中心检测，所测项目符合《信息安全技术文件加密产品检验规范》中基本要求相应条款所述的有关功能要求。

受检单位通讯资料	地址	浦东陆家嘴环路958号华能联合3301	
	邮政编码	200120	电话：021-68866655

批准：　审核：　主检：

日期：2008.5.12　日期：2008.5.12　日期：2008.5.12

山丽的调研和优势

涉密信息系统
产品检测证书

（编号：ISSTEC2007YT0582）

兹证明：上海山丽信息安全有限公司

研制生产的 山丽电子文档安全管理系统 V3.0

经国家保密局涉密信息系统安全保密测评中心检测，符合国家保密标准《涉及国家秘密的电子文档安全保密产品技术要求》（暂行）的要求

本证书有效期自 2007 年 12 月 27 日至 2010 年 12 月 26 日

批准人：

国家保密局
涉密信息系统安全保密测评中心

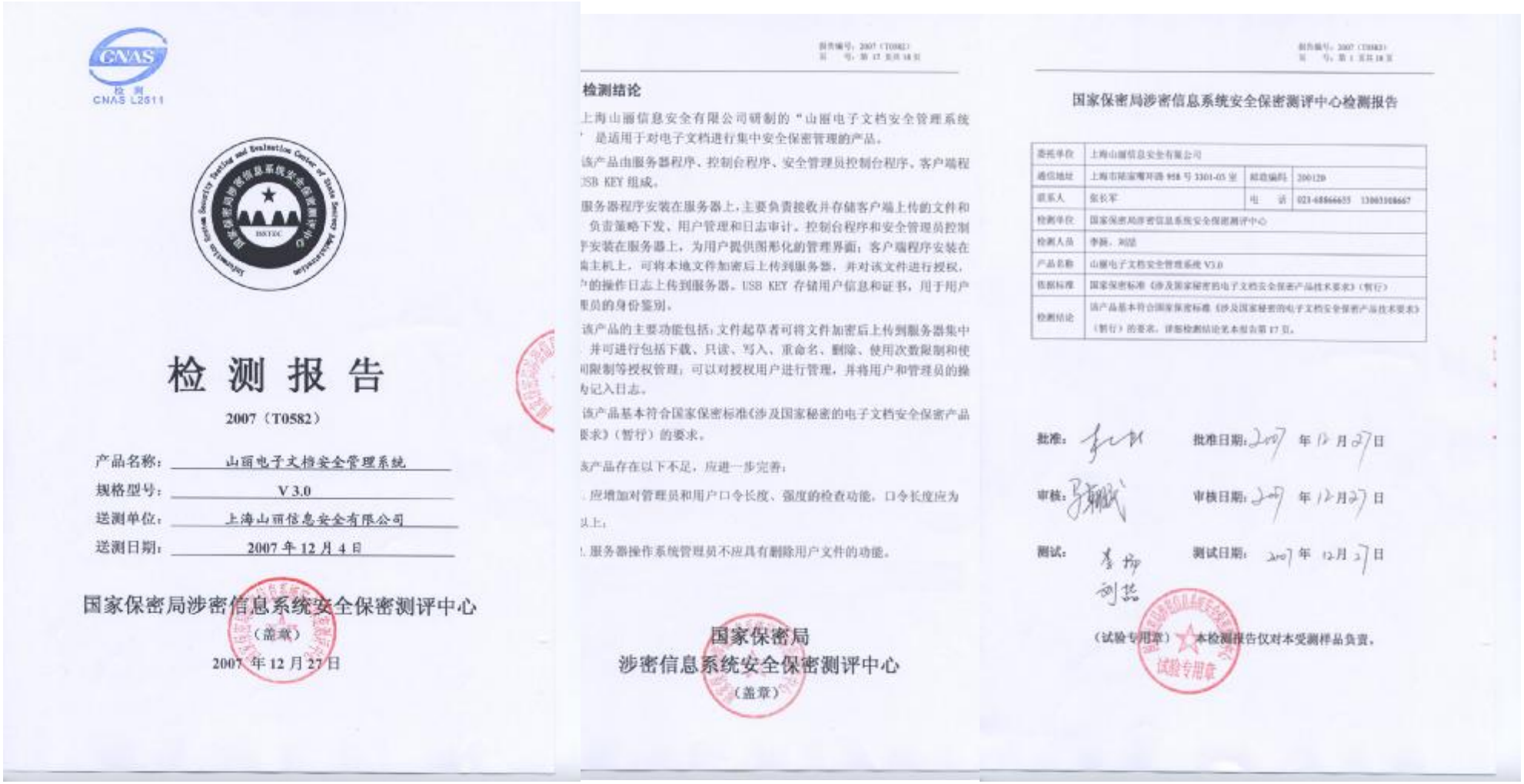
国家保密局涉密信息系统安全保密测评中心

产品检测反馈意见表

申报单位	上海山丽信息安全有限公司
产品名称	山丽防水墙数据防泄漏系统 V3.0
反馈意见	产品名称应与功能相符，建议改为："山丽电子文档安全管理系统 V3.0"

国 家 保 密 局
涉密信息系统安全保密测评中心
2007 年 12 月 7 日

山丽的调研和优势



CNAS
CNAS L2511

检 测 报 告

2007（T0582）

产品名称：山丽电子文档安全管理系统
规格型号：V3.0
送测单位：上海山丽信息安全有限公司
送测日期：2007 年 12 月 4 日

国家保密局涉密信息系统安全保密测评中心
（盖章）
2007 年 12 月 27 日

检测结论

上海山丽信息安全有限公司研制的“山丽电子文档安全管理系统”是适用于对电子文档进行集中安全保密管理的产品。

该产品由服务器程序、控制台程序、安全管理员控制台程序、客户端程序、USB KEY 组成。

服务器程序安装在服务器上，主要负责接收并存储客户端上传的文件和负责策略下发、用户管理和日志审计。控制台程序和安全管理员控制台程序安装在服务器上，为用户提供图形化的管理界面；客户端程序安装在客户端主机上，可将本地文件加密后上传到服务器，并对该文件进行授权，记录用户的操作日志上传到服务器。USB KEY 存储用户信息和证书，用于用户和管理员的身份鉴别。

该产品的主要功能包括：文件起草者可将文件加密后上传到服务器集中管理，并可进行包括下载、只读、写入、重命名、删除、使用次数限制和使用时间限制等授权管理，可以对授权用户进行管理，并将用户和管理员的操作均记入日志。

该产品基本符合国家保密标准《涉及国家秘密的电子文档安全保密产品技术要求》（暂行）的要求。

该产品存在以下不足，应进一步完善：

1. 应增加对管理员和用户口令长度、强度的检查功能，口令长度应为 8 以上；

2. 服务器操作系统管理员不应具有删除用户文件的功能。

国家保密局
涉密信息系统安全保密测评中心
（盖章）

国家保密局涉密信息系统安全保密测评中心检测报告

委托单位	上海山丽信息安全有限公司		
通信地址	上海市陆家嘴环路 958 号 3301-05 室	邮政编码	200120
联系人	张长军	电 话	021-68866655 13003108667
检测单位	国家保密局涉密信息系统安全保密测评中心		
检测人员	李振、刘洁		
产品名称	山丽电子文档安全管理系统 V3.0		
依据标准	国家保密标准《涉及国家秘密的电子文档安全保密产品技术要求》（暂行）		
检测结论	该产品基本符合国家保密标准《涉及国家秘密的电子文档安全保密产品技术要求》（暂行）的要求。详细检测结论见本报告第 17 页。		

批准：　批准日期：2007 年 12 月 27 日
审核：　审核日期：2007 年 12 月 27 日
测试：李振 刘洁　测试日期：2007 年 12 月 27 日

（试验专用章）　本检测报告仅对本受测样品负责。

山丽的调研和优势

军用信息安全产品

认证证书

军密认字第 0522 号

产品名称：山丽防水墙数据防泄漏系统 V2.0

研制单位：上海山丽信息安全有限公司

认证等级：军 C+级

有 效 期：2006 年 12 月至 2008 年 12 月

中国人民解放军
信息安全测评认证中心

2006 年 12 月 18 日

第 3875196 号

商标注册证

防水墙

核定使用商品(第 9 类)

已录制的计算机程序（程序）；计算机软件（已录制）；电脑软件（录制好的）；电子出版物（可下载）；计算机程序（可下载软件）；计算机游戏软件；计算机存储器；计算机；计算机外围设备；连接器（数据处理设备）（截止）

注 册 人 上海山丽信息安全有限公司

注册地址 上海市张江高科技园区张衡路 200 号 3 号楼 502 室

注册有效期限 自公元 2008 年 08 月 28 日 至 2018 年 08 月 27

局长签发 李建昌

中华人民共和国国家工商行政管理总局 商标局

山丽的调研和优势

中国合格评定国家认可委员会认可实验室（编号：CNAS L0286）

SSTL

上海市计算机软件评测重点实验室

Shanghai Key Laboratory of Computer Software Evaluating and Testing

测 试 报 告

Testing Report

报告类型 软件产品登记测试

报告编号 T20080127-DB01

软件名称 山丽防水墙数据防泄漏软件 V2.0

送测单位 上海山丽信息安全有限公司

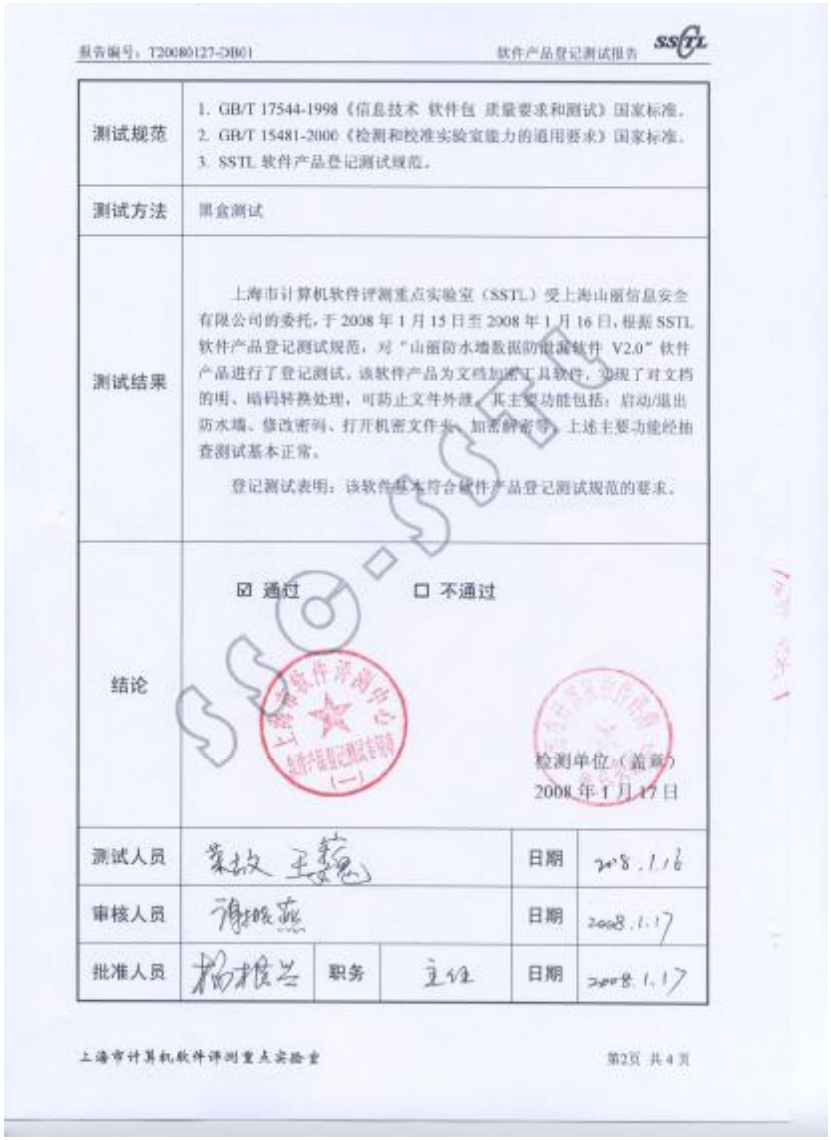
报告日期 二〇〇八年一月十七日

项目编号 T20080121

CNAS

上海市计算机软件评测重点实验室
（上海计算机软件技术开发中心）

检 测
CNAS L0286



报告编号：T20080127-DB01 软件产品登记测试报告 SSTL

测试规范	1. GB/T 17544-1998《信息技术 软件包 质量要求和测试》国家标准。 2. GB/T 15481-2000《检测和校准实验室能力的通用要求》国家标准。 3. SSTL 软件产品登记测试规范。
测试方法	黑盒测试
测试结果	上海市计算机软件评测重点实验室（SSTL）受上海山丽信息安全有限公司的委托，于 2008 年 1 月 15 日至 2008 年 1 月 16 日，根据 SSTL 软件产品登记测试规范，对“山丽防水墙数据防泄漏软件 V2.0”软件产品进行了登记测试。该软件产品为文档加密工具软件，实现了对文档的明、暗码转换处理，可防止文件外泄。其主要功能包括：启动/退出防水墙、修改密码、打开机密文件夹、加密解密等。上述主要功能经抽查测试基本正常。 登记测试表明：该软件基本符合软件产品登记测试规范的要求。
结论	☑ 通过 ☐ 不通过 检测单位（盖章） 2008 年 1 月 17 日
测试人员	日期 2008.1.16
审核人员	日期 2008.1.17
批准人员	职务 主任 日期 2008.1.17

上海市计算机软件评测重点实验室 第2页 共4页

山丽的调研和优势

商用密码产品销售许可证

（国密局销字SXS624号）

单位名称：上海山丽信息安全有限公司

经营范围：销售经国家密码管理局审批并通过指定检测机构产品质量检测的商用密码产品。

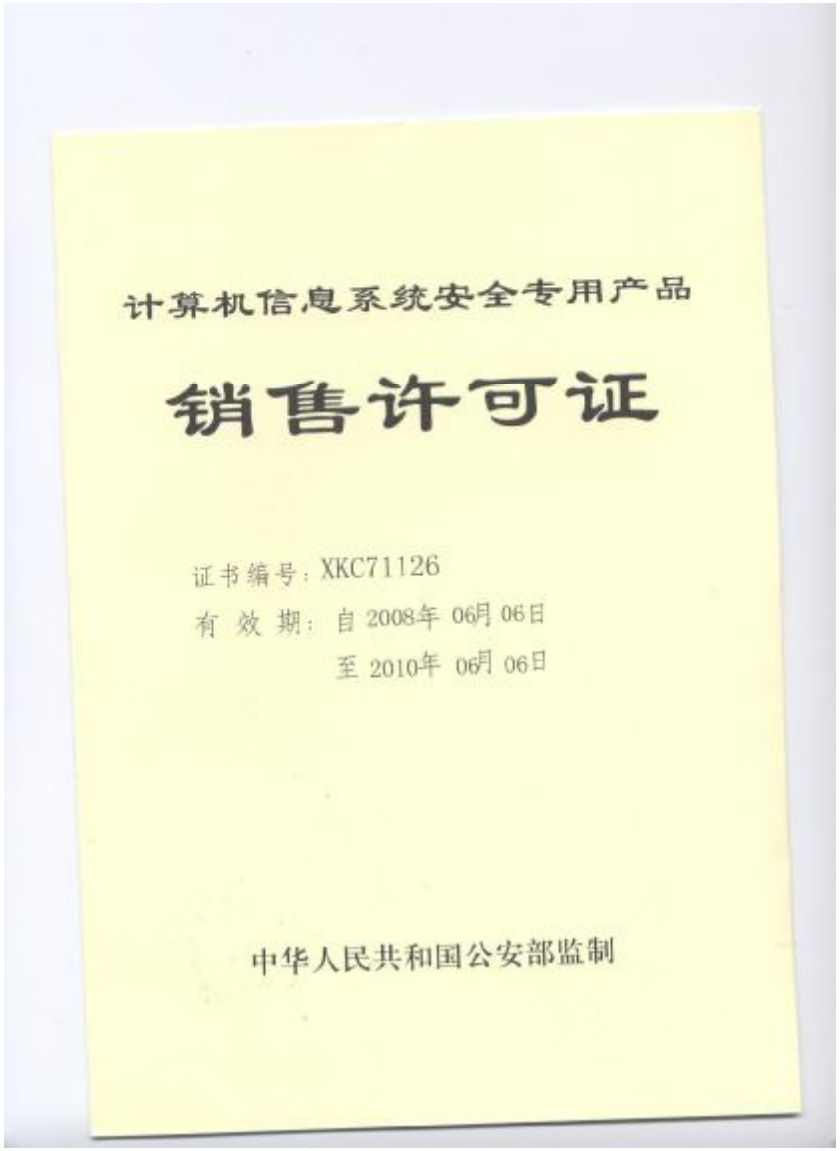
有 效 期：2006年6月22日至2009年6月22日。

国家密码管理局

2006年6月22日

2006 7 28

山丽的调研和优势



计算机信息系统安全专用产品

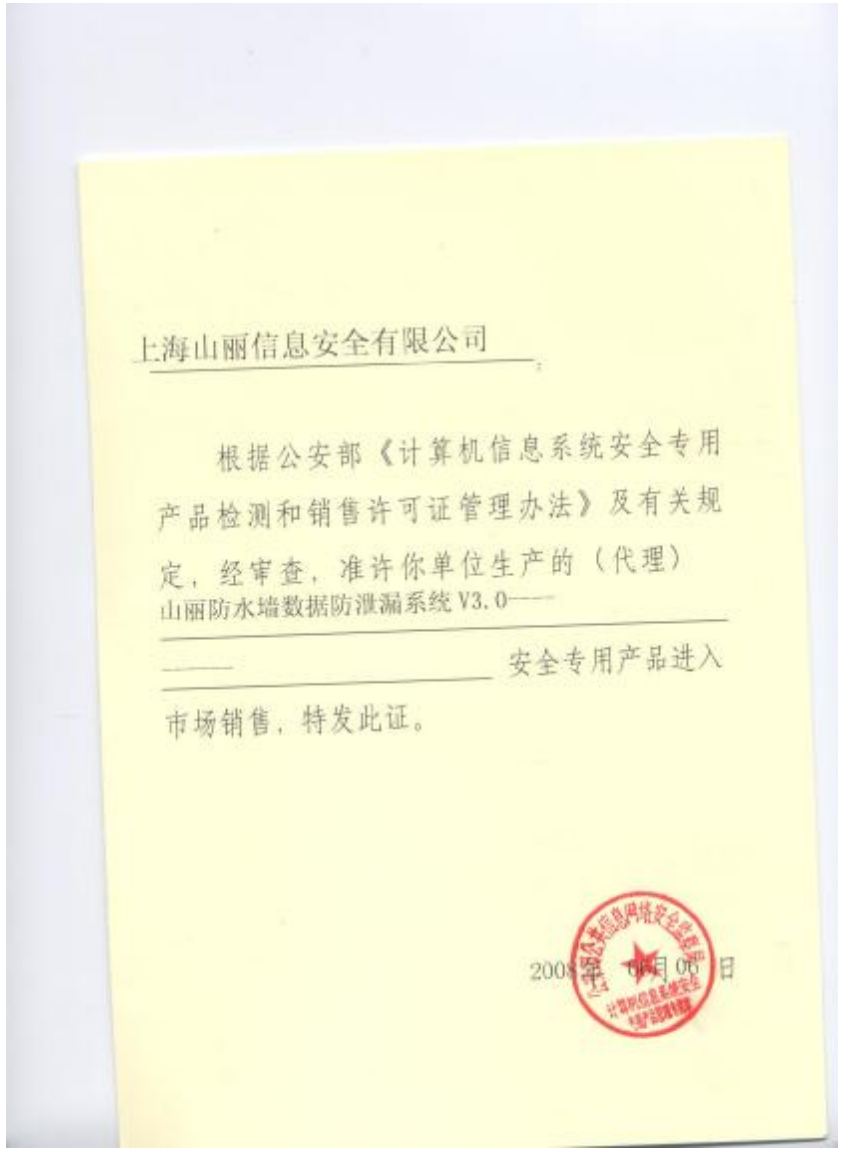
销售许可证

证书编号：XKC71126

有 效 期：自 2008年 06月 06日

至 2010年 06月 06日

中华人民共和国公安部监制



上海山丽信息安全有限公司

根据公安部《计算机信息系统安全专用产品检测和销售许可证管理办法》及有关规定，经审查，准许你单位生产的（代理）山丽防水墙数据防泄漏系统 V3.0——

——安全专用产品进入市场销售，特发此证。

2008年 06月 06日

山丽的调研和优势

中华人民共和国国家知识产权局

专利申请受理通知书

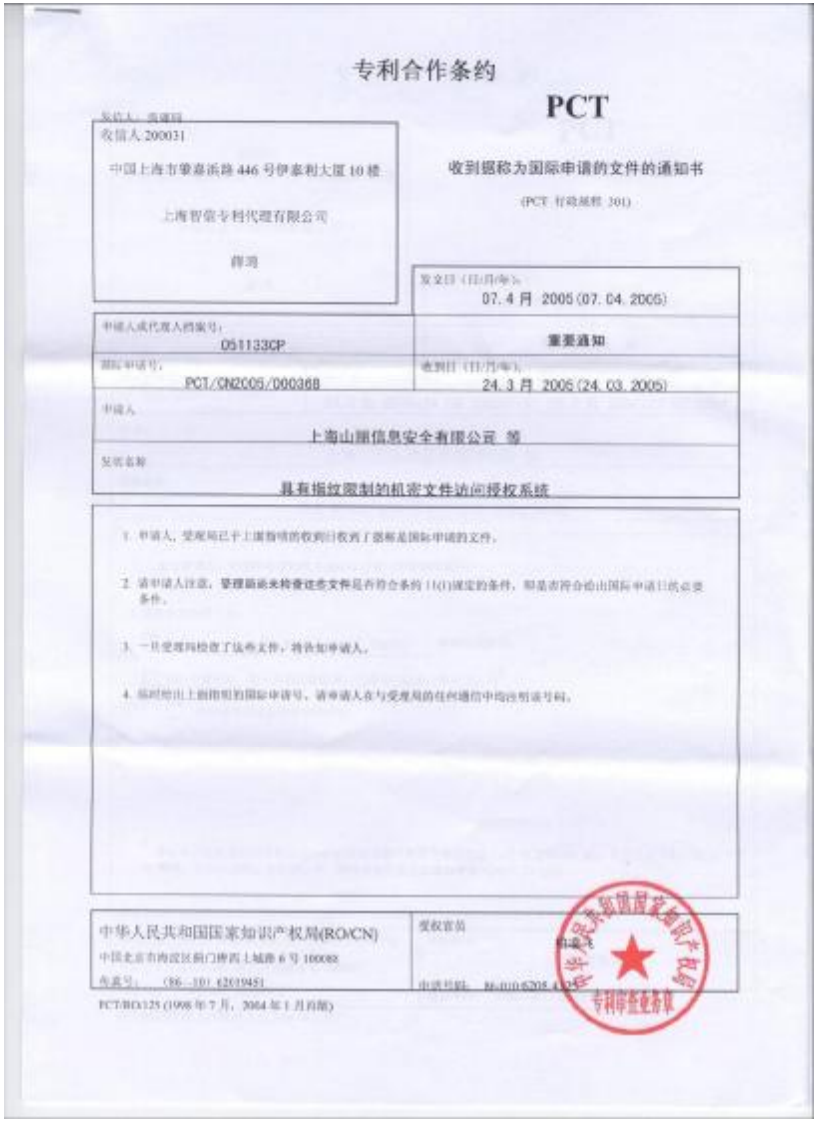
申请号：200410017241.3

申请日：2004 年 3 月 26 日

申请人：上海山丽信息安全有限公司

发明名称：具有指纹限制的机密文件访问授权系统

中华人民共和国国家知识产权局



专利合作条约

PCT

收到据称为国际申请的文件的通知书

申请人或代理人档案号：051133CP

重要通知

国际申请号：PCT/CN2005/000368

申请人：上海山丽信息安全有限公司 等

发明名称：具有指纹限制的机密文件访问授权系统

中华人民共和国国家知识产权局(RO/CN)

山丽的调研和优势

计算机软件著作权
登记证书

编号：软著登字第 035783 号

登 记 号：2005SR04282

软件名称：山丽防水墙数据防泄漏系统软件 V2.0
[简称：山丽防水墙系统]

著作权人：上海山丽信息安全有限公司

权利取得方式：原始取得

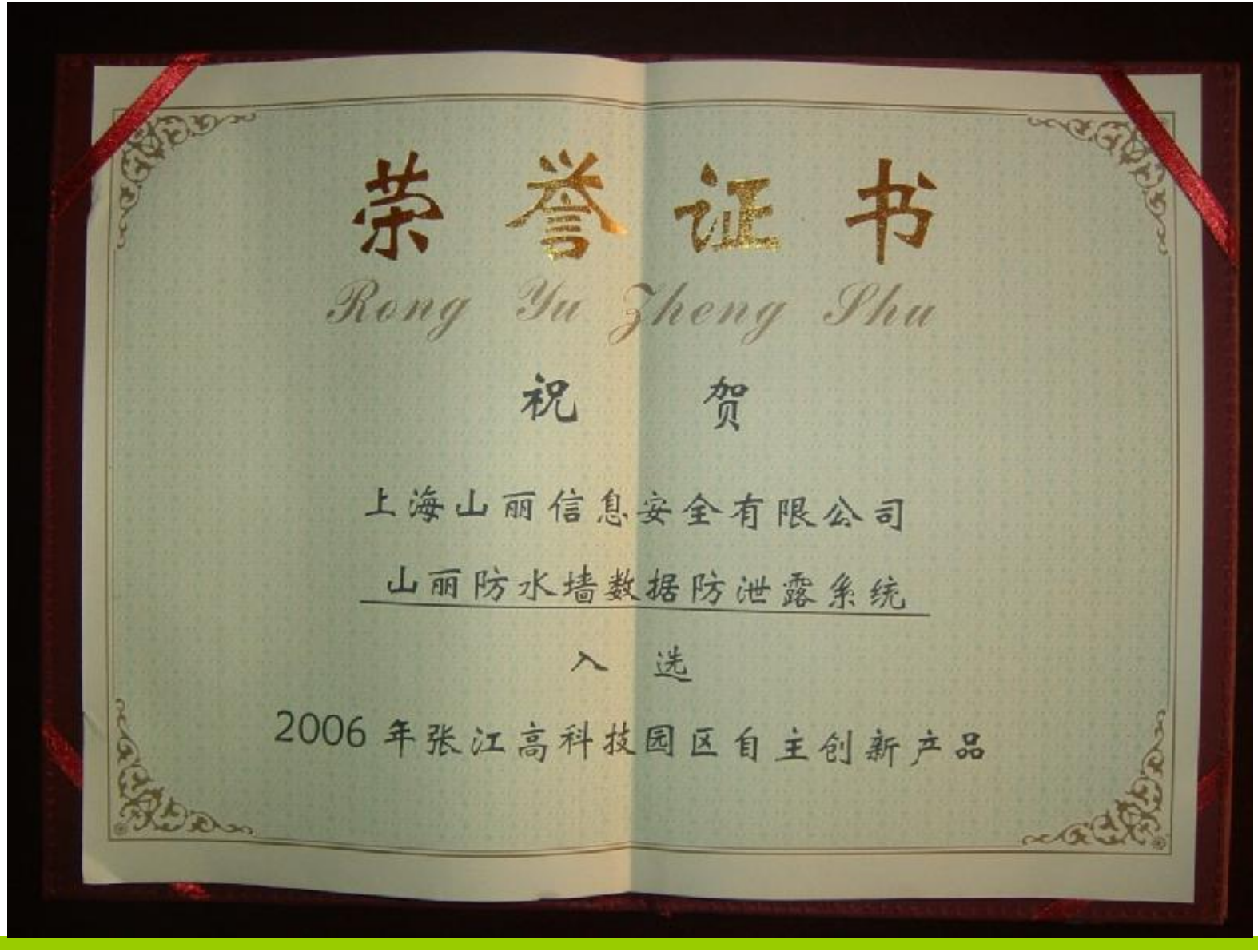
权 利 范 围：全部权利

首次发表日期：2004年03月01日

根据《计算机软件保护条例》和《计算机软件著作权登记办法》的规定，对以上事项予以登记。

2005 年 04 月 30 日

山丽的调研和优势



山丽的调研和优势

山丽的调研和优势

- 产品情况

- 关于产品功能、性能、兼容性、易用性、可靠性的情况
- 山丽防水墙产品功能比较完善，产品采用的透明加密方式和文件格式无关，即使该企业将来不从事该行业也将对本公司无影响，这好适合制造企业源代码的保护；目前大多公司使用的加密方式和文件格式有关，如果其不进行相关产品的开发，将会使得制造企业购买的软件无法支持新的文件格式，尤其不适合软件企业；
- 在产品性能方面，产品经过2轮在公司的测试，对cpu、内存的占用均比较小，没有产生明显影响，目前，其客户端对cpu的影响在3%以内，占用内存在10M左右；
- 在产品的兼容性方面，目前就支持vista，64位系统也有支持；
- 在易用性方面，其产品采用面向对象方法设计，操作简单，将来会增加一定的管理成本，但对客户端几乎没有影响，使全透明的；
- 在可靠性方面，产品客户端、服务器端在公司运行无碍，运行可靠；

山丽的调研和优势

- 服务支持

- 1、公司通过cmm3级软件能力成熟度评估（iso9001相当于软件行业的cmm1），具有国际机构认证的软件开发和完善的售后相应体系；
- 2、企业有24小时服务电话8008208681（8008209730）、13003108681/0，可以做到7*24小时的响应，并有企业客户专有的bbs、qq、邮箱，支持客户的技术响应，做到极其快捷的售后保障；
- 3、公司项目实施采取项目总监负责制，项目总监下设技术人员进行具体的基本技术设置，项目总监负责总体的技术保障和培训、实施方案的撰写，实施总监上设项目实施监督经理（QA），监督项目的正确实施，完善而周到的队伍建设是售后服务的根本保障；
- 4、项目实施结束后有售后服务梯队进行实时的跟踪，每家客户具有专人负责售后服务联系，这成为售后服务的常规联系，一旦有情况发生，则立即进入实施状态；满足需求；
- 5、公司具有的用户正说明了企业具有的项目实施经验；

山丽的调研和优势

- 比较优势

- 产品优势：
- 1、山丽防水墙对文件的加解密，不受文件格式（类型）的限制；
- 2、**和存储介质无关，在任何现有的存储介质上都以密文形式出现；**
- 3、**和应用程序无关，可以和各种PDM/PLM应用程序无缝融合；**
- 4、对文件的加解密，是完全动态的，无须人工操作；
- 5、完全防止有权限人员把加密文件的恶意外泄；
- 6、可以根据实际需要对加密文件进行自动加密或自动解密的传输；
- 7、系统管理员可以根据用户不同的安全级别，制定不同安全级别的登陆策略、加解密策略；
- 8、防水墙系统的实施，不改变用户网络结构，不影响用户原有的使用习惯；
- 9、**客户端的低反感部署；**
- 10、**大面积自动化实施的部署方案。**

山丽的调研和优势

- **产品优势**

- 以机器为单位的管理
- 以用户为单位的权限管理
- 以机器和用户为单位的权限管理
- 以用户组为单位的权限管理
- 以文档为单位的权限管理
- 以文件夹为单位的权限管理
- 以用户和用户、用户和组、组和用户、组和组为单位的权限管理
- 以时间、次数、打印、重命名、删除、读取、下载、编辑为细分权限的权限控制
- 以网上邻居上读取、下载、删除、重命名为细分权限的权限管理
- 以相同安全级别为“安全域”概念的安全域权限管理
- 以总、分公司协作单位的权限管理
- 可客户管理系统集成，留有二次开发接口的无缝融合的权限管理

- 至少支持12种以上的权限管理

山丽的调研和优势

- 企业优势

- 1、潜心研究数据防泄漏系统已经2003年至今约5年余；
- 2、2004年即申请数据防泄漏系统国内国际专利，目前已经到pct国际专利阶段，本项技术领先国际、国内同类技术，是当之无愧的技术领导者；
- 3、专业的信息安全公司，在信息安全、网络安全、数据安全有专业的团队、湛深的储备，并非一般的文档管理、数据加解密公司；
- 4、产品首创和文档格式无关，目前行内企业纷纷效仿，但我们的透明加解密又更进一步，直接和操作系统内核嵌套；
- 5、产品自2004年至今已经历经磨砺，稳定性、兼容性极佳；
- 6、产品设计极其灵活，可以满足各种各样相互矛盾之需求，一套产品可以等于同行数套产品；
- 7、加密方式灵活多样，登陆方式更是变化多端，满足客户各种苛刻需求；
- 8、权限管理从最简到最繁，如套餐式可以随意组合，权限管理可以以人、组、机器、文档、网络等为对象，并可随意组合：权限关系的演变，一切均在设置之中，可一次起效，亦可永久起效，变化多端；
- 9、产品开发管理相当完善，留有完备的二次开发接口，对有开发能力的企业而言，不是买了一套产品，而是买了一套系统，一只团队；
- 10、企业研发管理、项目管理遵循cmm3评估体系，可保证客户现场实施的有序有效性，并非一般小型企业可模仿；
- 11、强大的项目实施团队、丰富的项目实施经验、项目总监负责制的管理方式，可确保项目实施的时间、效果无忧无虞。

项目实施计划步骤

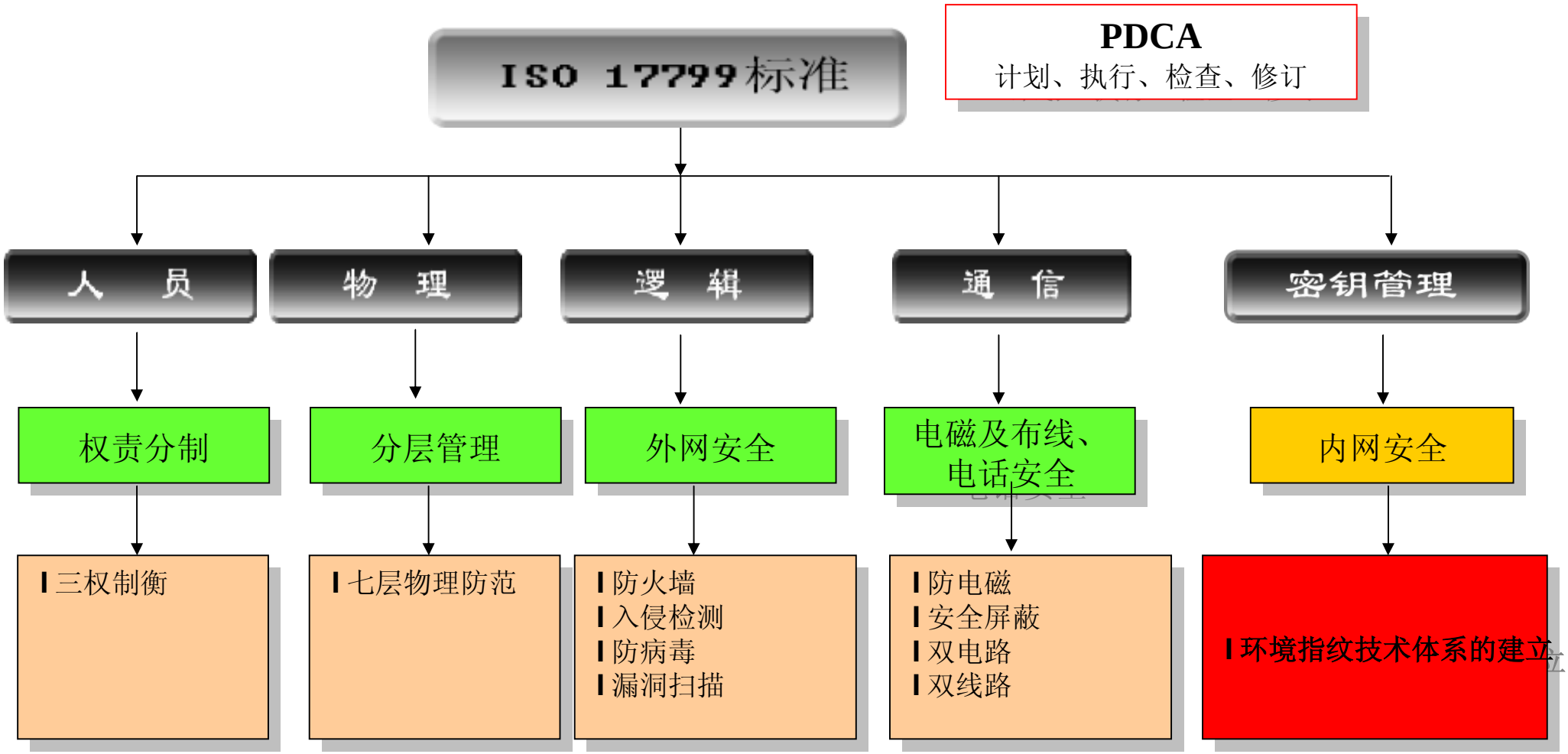
- 项目实施采用全局设计、分部实施的方案。
- 具体实施计划参见：《制造企业制造企业防水墙项目实施进度》

项目实施风险应对

- 项目实施中可能会存在的风险：
- 1、项目实施因人员原因的中止风险：
- 原因：因项目实施中，员工比较反感，而影响到公司主管领导的判断，从而中断了项目实施；
- 应对：理解国家、国际法律，明白实施信息内控势在必行，没有重大问题，不叫停项目的实施；
- 2、产品质量影响项目的实施：
- 原因：虽然经过前期的测试，但作为软件产品，在实施中仍会遇到无法预见到的质量问题；
- 应对：分步实施，减少影响范围；
- 3、产品系统重大崩溃问题：
- 原因：可能系统崩溃，造成全面无法使用；
- 应对：山丽产品本身即具有灾难恢复系统（服务器端、客户端均有），企业本身还可以增加服务器硬件备份，降低风险；
- 4、供应商永续发展的问题：
- 原因：供应商不再进行该方向得发展，影响企业对该产品的进一步使用；
- 应对：调查企业是否有比较长远的研发计划，以及研发计划的方向，从而判断该企业的永续发展计划；了解企业实力，把握企业发展的长久永续。

制造企业智力资产保护的发展趋势

建设符合ISO27001/2/bsi17799标准的运营管理体系企业信息化安全的重要道路



QA