安全的困扰与思考

叶根平

三花控股集团 信息总监

困扰1：病毒侵入

2016年5月，cryptolocker的新变种侵入 ……

2013年10月，勒索病毒在我司第一次爆发。技术部、生产计划处、采购部等多部门多台电脑接到……

要求在三天内支付300美金或等额比特币，才给文件解密！

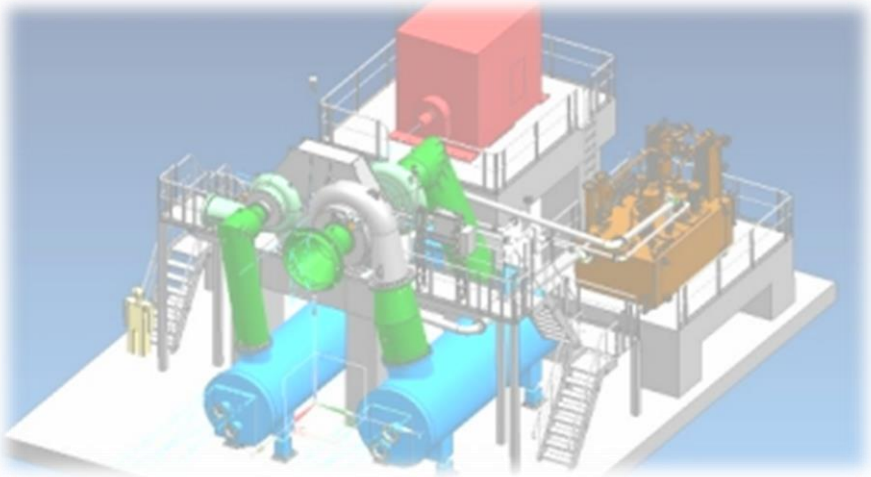
只有报警？

困扰2：网络侦听

2017年5月底，某知名软件公司对我司曾试用过的某款软件提出……

怎么“侦听”到试用后没被卸载干净的……

有效阻断？



困扰3：远程一致

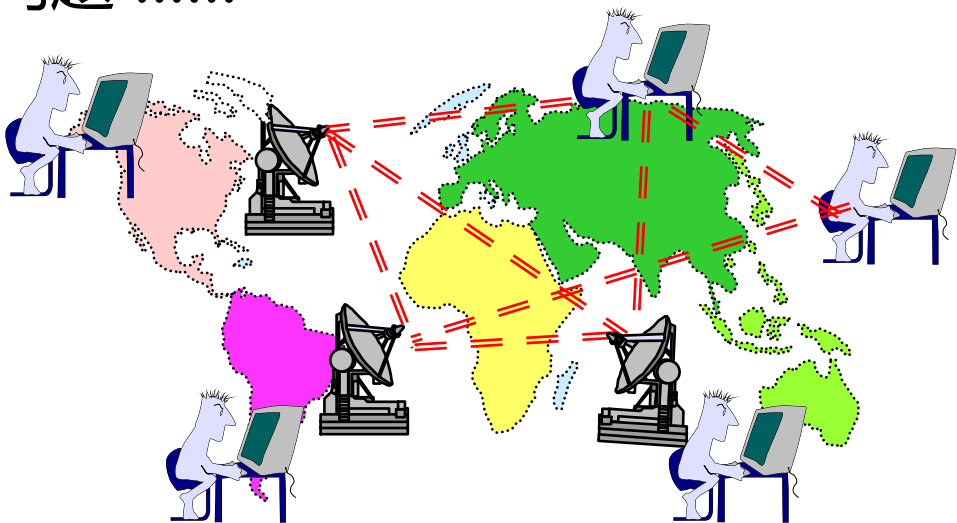
散布在全球各地的研发团队（成员），带着系列产品的某版本做测试、调试、验证 ……

严格的项目管理，可以解决一部分问题 ……

桌面虚拟化，可以解决一部分问题 ……

加密、解密，可以解决一部分问题 ……

上云？



困扰4：信息外泄

高层级人员带着核心信息资产，较长时间在出差 ……

竞争对手在很短的时间，就开发出来相似性很高的产品 ……

加密？水印？

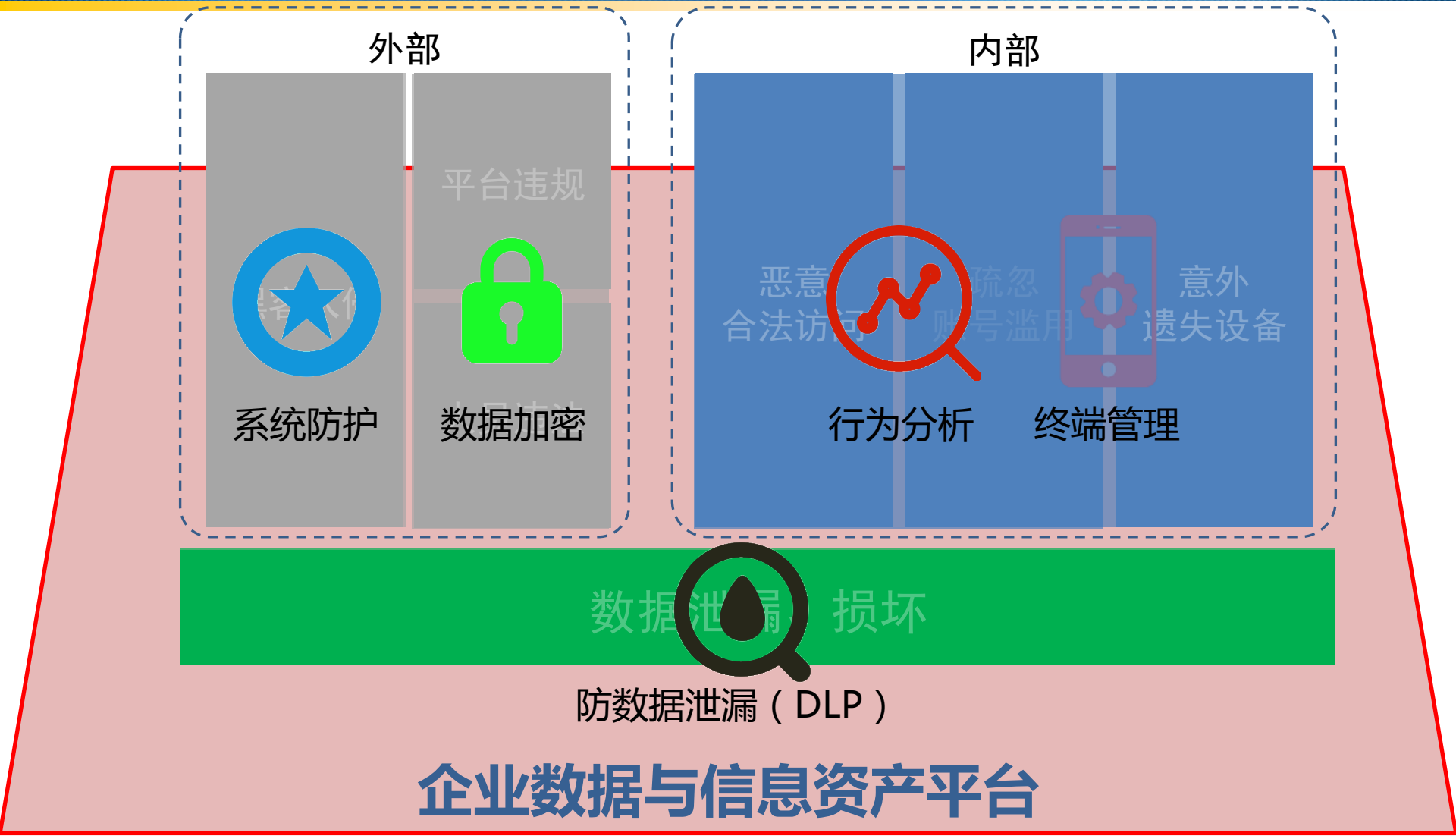
困扰5：数据丢失

- 服务器宕机，部分业务数据丢失，……
- 新开发软件逻辑错误或BUG，真实业务数据丢失 ……
- 内/外部 IT人员误操作，导致一些数据丢失，……

双机热备等功能在云上实现

也有性价比优势？

思考：传统模式下的策略


外部
内部
平台违规
恶意
合法访问
疏忽
账号滥用
意外
遗失设备
系统防护
数据加密
行为分析
终端管理
数据泄漏
损坏
防数据泄漏（DLP）
企业数据与信息资产平台

传统的模式太累

云：是可以信任的新模式吗？

困扰6：“云”故障

- 美国东部2017年2月28日下午，亚马逊位于美国北弗吉尼亚的S3云存储服务器出现故障，导致使用该服务器的数千个网页完全无法访问，大量app功能失效，十多万个网页内部分链接失效且图片无法显示。
- 事故持续了3.5小时……

类似的情况会不会重复发生？

云的安全性让企业担忧

Security is the No. 1 reason preventing firms from moving to SaaS.

企业未采用SaaS的首要原因是安全。

--Forrester 分析师 Liz Herbert

49% of respondents had slowed their cloud adoption due to a lack of cybersecurity skills。

49%的回复者因缺少安全技能而延缓了云部署。

--McAfee 2016年底的调查

87.2%的用户看重产品的安全性、可靠性。

--易观，2015年9月客户调查

“云”事故列举

- 2012年08月 盛大云部分服务器出现宕机，由于无锡机房的一台服务器硬盘突然发生硬件故障，导致旅游服务网站“背包兔”等个别“盛大云”客户数据丢失，以至用户网站访问异常。
- 2012年10月30日，由于电力故障，导致阿里云部分服务器于10月30日下午出现短暂无法访问情况。
- 2014年11月2日下午，腾讯云服务器出现了6分钟的访问故障。腾讯云网站响应速度慢，图片打不开，并出现无法登录管理中心控制台等问题。
- 2015年3月11日，AppleiCloud内部DNS错误导致其iTunes和AppStore的服务宕机，一些iCloud的电子邮件帐户也受到短暂影响。
- 2015年，５月２７日晚6点时左右，杭州、北京、上海、武汉等地用户反映，支付宝无法正常使用。支付宝公司对故障的回应称，杭州萧山某地光纤被挖断，导致故障。

“云”事故列举

- 2015年6月21日，阿里云香港节点出现全线宕机，业务中断超过12小时，甚至有部分用户数据出现损毁，在业界引发轰然大波。6月21日晚，阿里云发布公告称，本次故障因香港运营商IDC电力问题所致，阿里云已责成香港运营商尽快完成机房整改措施，规避此类问题的再次发生。
- 2015年，8月22日，位于美国硅谷的富士通数据中心供电异常，导致公有云服务暂时下线，5天后才恢复正常。
- 2015年9月1日，阿里云云盾的安骑士产品升级触发bug导致了用户ECS里的部分正常文件被误隔离。故障是由于工程师粗心大意写错了一行代码，从而将所有新启动的可执行文件都当成了恶意文件进行隔离。由于我们之前在设计上的缺失，对这一特殊的异常情况缺乏快速恢复的机制，只能临时写程序进行紧急恢复，因此整个故障持续了较长的时间。

“云”事故列举

- 2015年9月20日，亚马逊AWS宕机，首先是亚马逊DynamoDB服务出现问题，此后亚马逊的其他服务也受到影响，同时波及了很多著名网站。
- 2016年4月11日晚，Google Cloud Platform出现18分钟的中段，影响到Compute Engine实例和所有地区的VPN服务。
- 2016年6月2日Apple云发生广泛的服务中断，让Apple一些受欢迎的零售和备份服务服务都出现中断。这次故障从太平洋时间下午12:30开始，让一些客户无法访问多个iCloud和App Store服务。
- 2016年6月4日澳大利亚悉尼早上暴风雨，导致该地区的一个AWS域断电，一些托管了关键工作负载的EC2实例和EBS卷随后出现故障。同时在那个周末，澳大利亚AWS可用区域内的网站和在线服务出现大约10个小时的中断，从银行服务到披萨送货都受到了影响。受影响的企业客户敦促这个全球最大的云提供商尽快恢复服务。

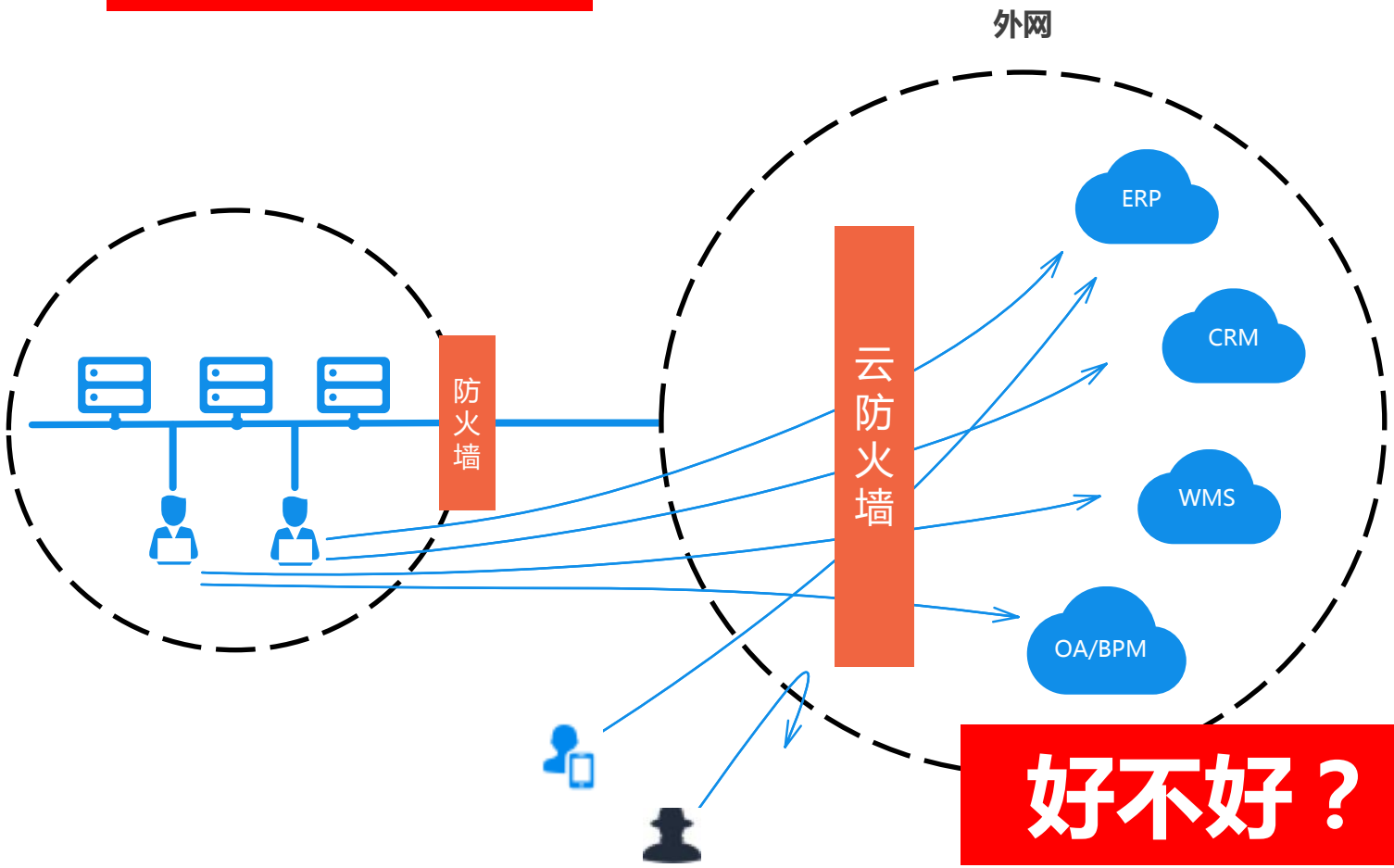
思考：云环境下的数据安全

- 数据访问的权限控制
- 数据在云存储中的私密性
- 数据在运行时的私密性
- 数据在网络传输时的安全可靠
- 数据在云存储中的完整性
- 数据在云存储中的持久可用性
- 数据在云存储中的访问速度
- 数据使用和存储的安全审计

责任主体

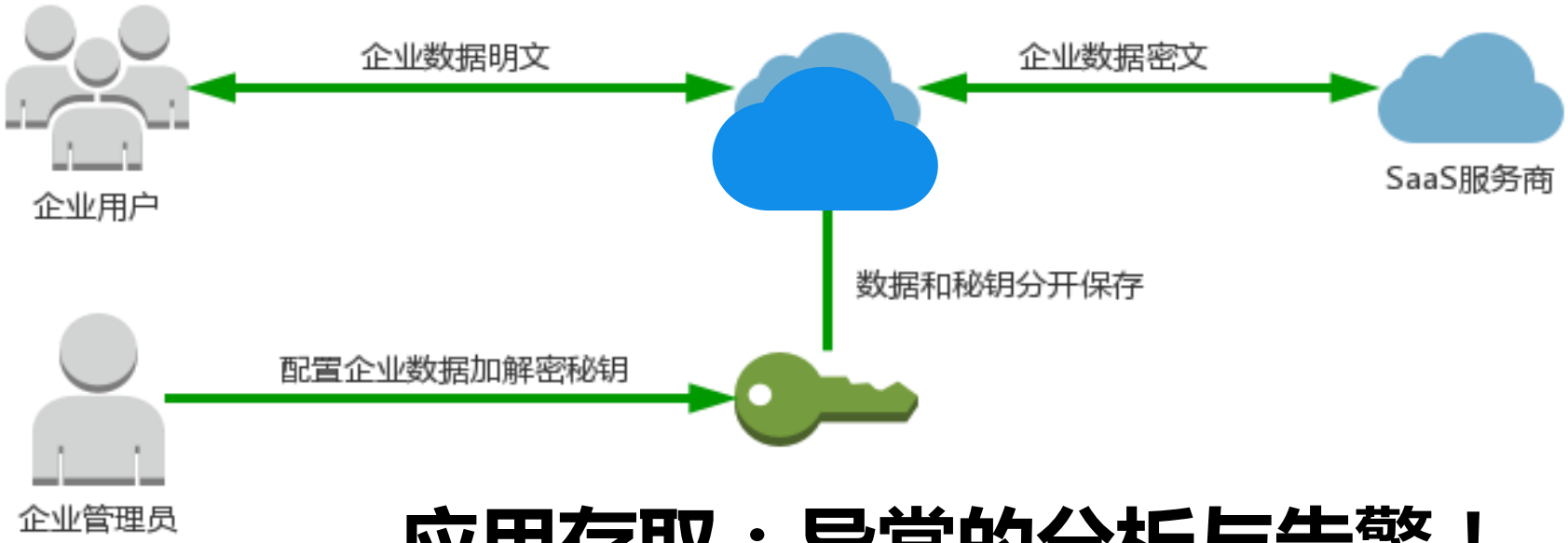
思考：云环境中的“防火墙”

有没有？



好不好？

思考：比加密更有效



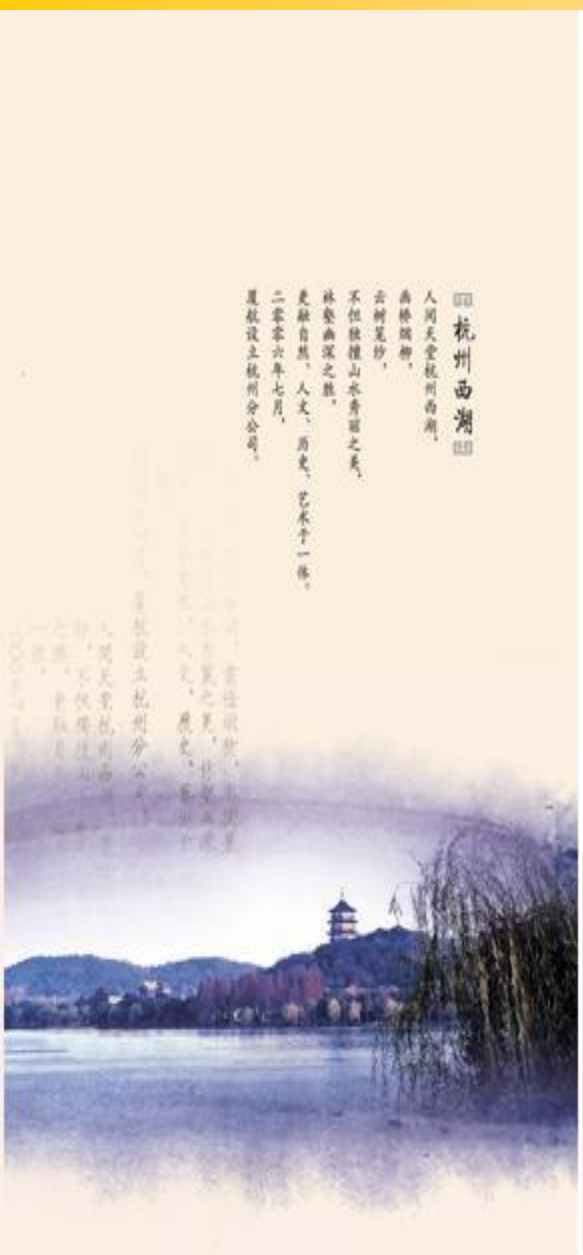
应用存取：异常的分析与告警！

非授权异动：告警！加锁……

思考：可以相信吗？

可以相信云吗？

可以相信云服务提供商吗？



谢谢！

联系方式：

邮箱：ygp@zjshc.com

sam_ye2003@hotmail.com