C3安全峰会
CYBER | CLOUD | COMMUNICATION

An emerging technology to enhance the ability to control financial risks

一种提升金融风险管控能力的新兴技术：第三方安全评价服务（SRS）

赵毅

谷安天下高级经理

安全值产品总监

一种提升金融风险管控能力的新兴技术

C3安全峰会
CYBER | CLOUD | COMMUNICATION

一、第三方安全评价服务（SRS）的兴起

二、从外部视角看金融行业网络安全现状

三、SRS在金融领域的应用场景

四、国内首个第三方安全评价服务 - 安全值

C3安全峰会
CYBER | CLOUD | COMMUNICATION

The rise of the third party Security Rating Service (SRS)

第三方安全评价服务（SRS）的兴起

Gartner’s new security rating service (SRS)

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Gartner’s new security rating service (SRS)

provide continuous, independent quantitative security analysis and scoring for organizational entities. The services gather data from a variety of public and private sources via passive and active (but nonintrusive) means, analyze the data using proprietary analysis and rate the entities using their own standard scoring methodologies. These tools can be used for internal security reporting and management and for third-party risk management.

Gartner

安全领域新概念：安全评级服务的兴起

作者：王小瑞 星期二, 十月 18, 2016 0

分享:

Gartner最近的报告中出现了一种安全领域的新概念——安全评级服务(SRS, Security Rating Services)，Gartner将其定义为，“为组织实体提供持续的、独立的、量化的安全分析和评级服务”。

到底什么是SRS?

说的直白一点，SRS就是一种以大数据分析和威胁情报为基础，对企业的信息资产，进行量化的快速的安全风险评估。这种评估通过主动和被动（均无需打扰被评价方）两种形式，从各种公开和私有资源收集数据，使用特定的分析方法分析数据并使用实体自身的标准评级方法论来打分。可用来做企业内部的安全报告，以及对第三方合作伙伴的风险管理。

对于企业来说，核心业务之外的服务需要越来越多的第三方供应商，在网络虚拟化的大潮下，对云服务提供商的需求尤为凸显。为此，除了对本身安全状况的掌握，“如何了解大量业务伙伴和第三方服务安全状况”的需求也逐渐增长起来。

传统的第三方安全评估有着各种限制，尤其是当涉及到成百甚至上千的外部服务和合作伙伴时。而且，

20个行业180多个领域6万家企业/机构

C3安全峰会
CYBER | CLOUD | COMMUNICATION

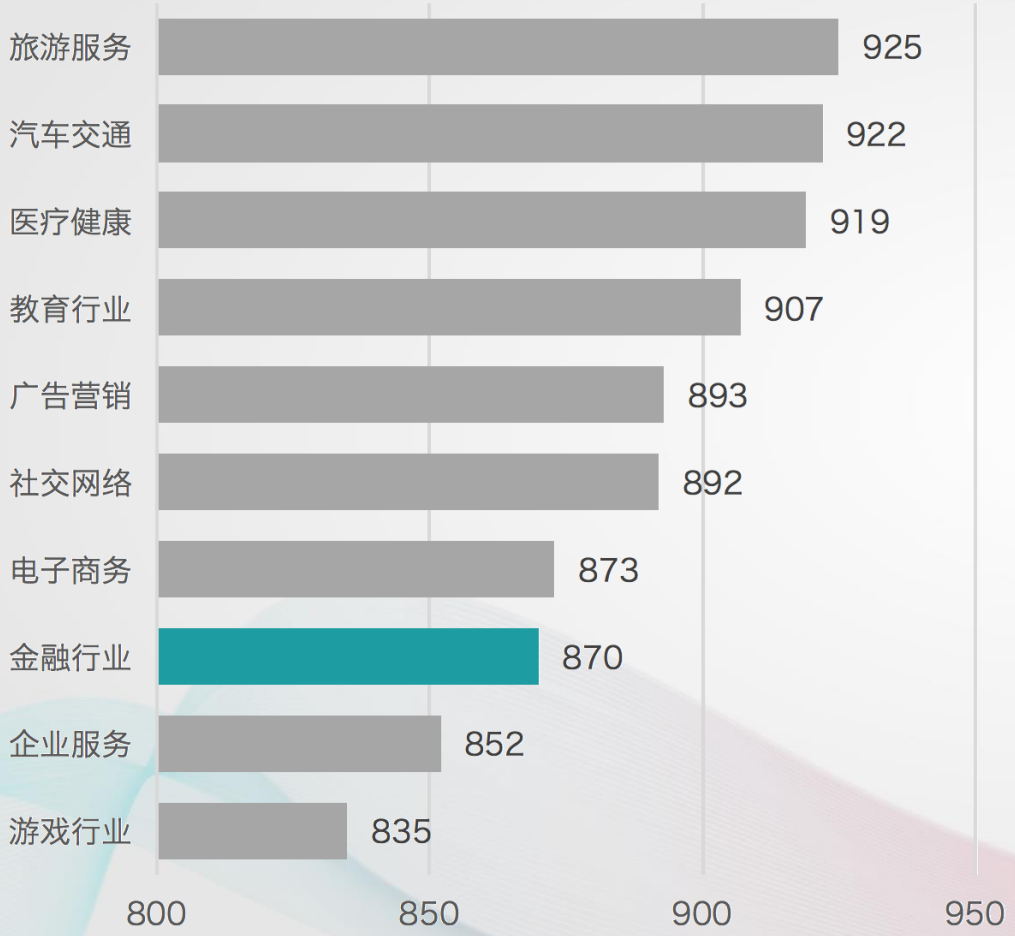
金融	银行 企业征信	证券 互联网理财	基金 彩票	保险 虚拟货币	信托 金融信息化	股票交易 金融综合服务	第三方支付 外汇期货贵金属	小贷P2P 其它金融服务	消费金融	投资众筹
教育	重点高校 教育企业	教育信息化 人力资源	职业培训 教育综合服务	媒体及阅读 出国留学	教辅设备 儿童早教	语言学习 其他教育	兴趣教育	校园服务	行业解决方案	综合文娱
医疗健康	三甲综合医院 医疗综合服务	医疗信息化 其他医疗服务	医生服务	健康保健	寻医诊疗	PUMC	专科服务	生物技术	医疗服务	医疗健康硬件
电子商务	大宗商品 其他电商服务	医药电商 母婴玩具	化妆品 跨境电商	家居家纺 商户服务及信息化	数字虚拟商品	图书影音	珠宝首饰	生鲜食品	服装服饰	奢侈品
企业服务	ISV独立软件开发 IT基础设施	客服 知识产权	数据服务 综合企业服务	电商解决方案 SaaS服务	B2D开发者服务 IaaS服务	企业安全 PaaS服务	商务社交	办公OA	法律服务	财务税务
物流	品牌快递	综合物流	货运物流	跨境物流	同城配送	仓储服务	天津跨境物流	浙江同城配送	北京品牌快递	其他物流
汽车交通	汽车金融	交通出行	车主工具及服务	汽车电商	汽车后服务	二手车	车联网及硬件	汽车综合服务	其他汽车服务	交通运输辅助
房产服务	商业房产	租房	房产金融	房产电商	房产信息化	装修装潢	房产综合服务	其他房产服务		
旅游	旅游综合服务	旅游工具及社区	交通食宿	主题特色游	景点门票	旅游信息化	跨境游	国内游	其他旅游服务	
游戏	游戏直播及玩家	游戏发行及渠道	游戏开发商	游戏媒体及社区	游戏硬件	游戏道具衍生品	消费电子	游戏综合服务	其他游戏服务	
社交网络	婚恋交友	女性社群	同性社交	陌生人交友	综合社交	校园社交	家庭熟人社交	其他社交		
广告营销	移动及网络广告	整合营销传播	销售营销	广告平台	广告技术	设计及创意	传统广告	其他广告		
软件服务	优化清理 其他工具	浏览器	搜索引擎	无线通讯	应用商店	文件文档	操作系统及ROM	事项及效率	位置定位	图像视频
智能硬件	传感器及中间件	智能家居	3D打印	飞行器	车载及出行	芯片半导体	综合硬件	其他硬件服务		
本地生活	婚礼婚庆 休闲娱乐	3C电子 兴趣社区	美食餐饮 内容类移动应用	小区服务 本地综合生活	宠物服务 其他生活服务	美业服务	维修服务	家政服务	本地生活类应用	实用生活服务

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Analysis of the financial industry cyber security from the outside

从外部视角分析金融行业网络安全现状

从外部视角评价各行业安全状况



分析对象选择：

基于20个行业6万家机构数据中选择网络安全关注度较高、较流行的10个行业10000家企业/机构。

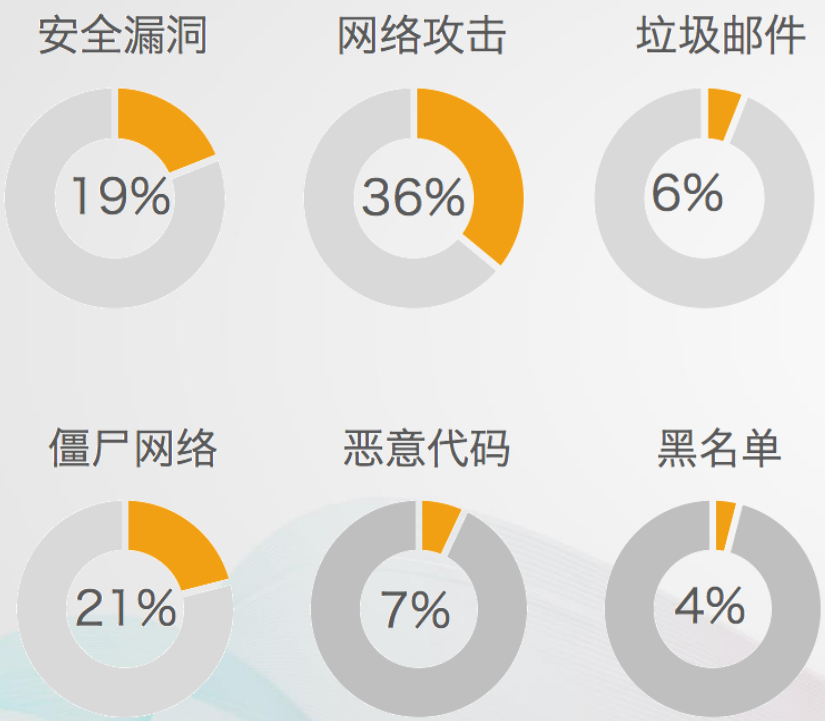
分析数据：

来自外部100多个安全数据资源，自2017年1月至6月的安全事件数据。

报告数据来源：

安全值《10大金融领域2017年6月网络安全报告》

10大金融细分领域外部安全威胁分析

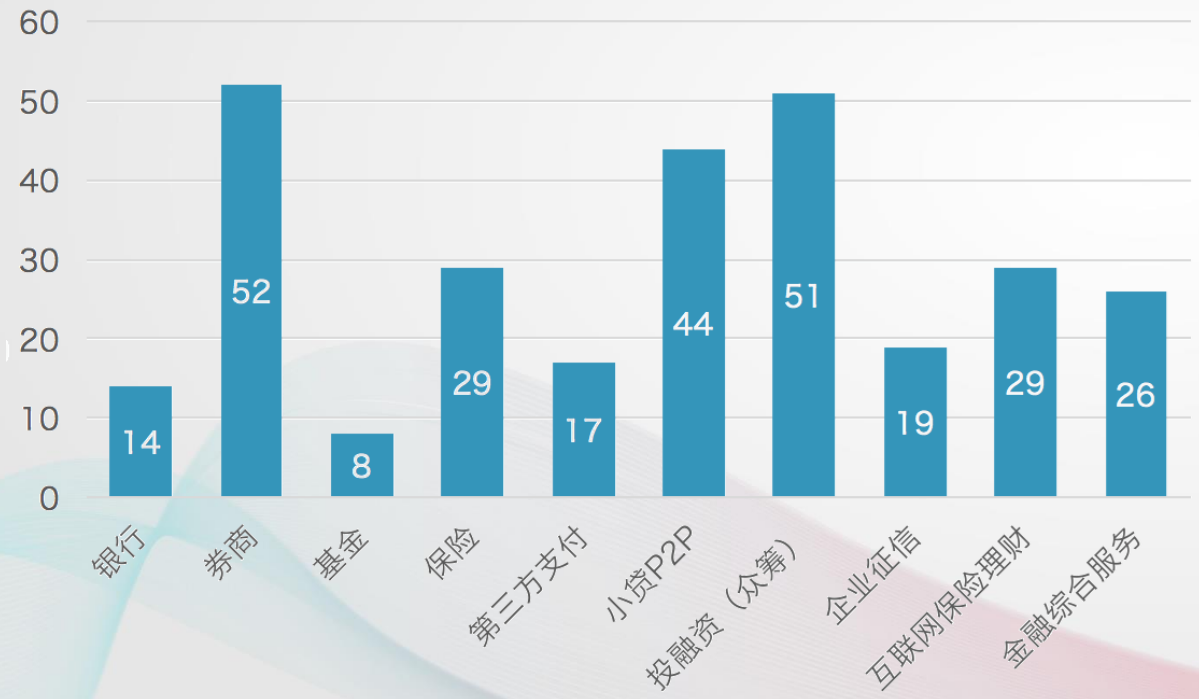


	机构数	安全漏洞	络攻击	圾邮件	尸网络	意代码	黑名单
银行	100	26%	35%	22%	32%	27%	4%
券商	100	31%	30%	14%	14%	22%	3%
基金	100	18%	13%	5%	10%	4%	3%
保险	100	28%	24%	11%	12%	5%	5%
第三方支付	100	24%	67%	6%	37%	2%	2%
小贷P2P	100	12%	55%	1%	27%	5%	3%
投融资（众筹）	100	4%	28%	1%	20%	0%	7%
企业征信	100	11%	27%	0%	14%	0%	3%
互联网保险理财	100	16%	45%	1%	19%	1%	4%
金融综合服务	100	15%	39%	1%	25%	2%	2%

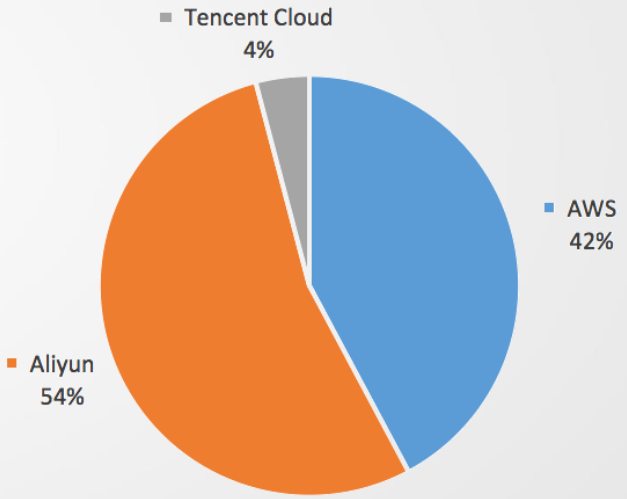
金融行业公有云应用现状

- 分析范围内有29%企业使用公有云服务

10大金融领域云迁移比例

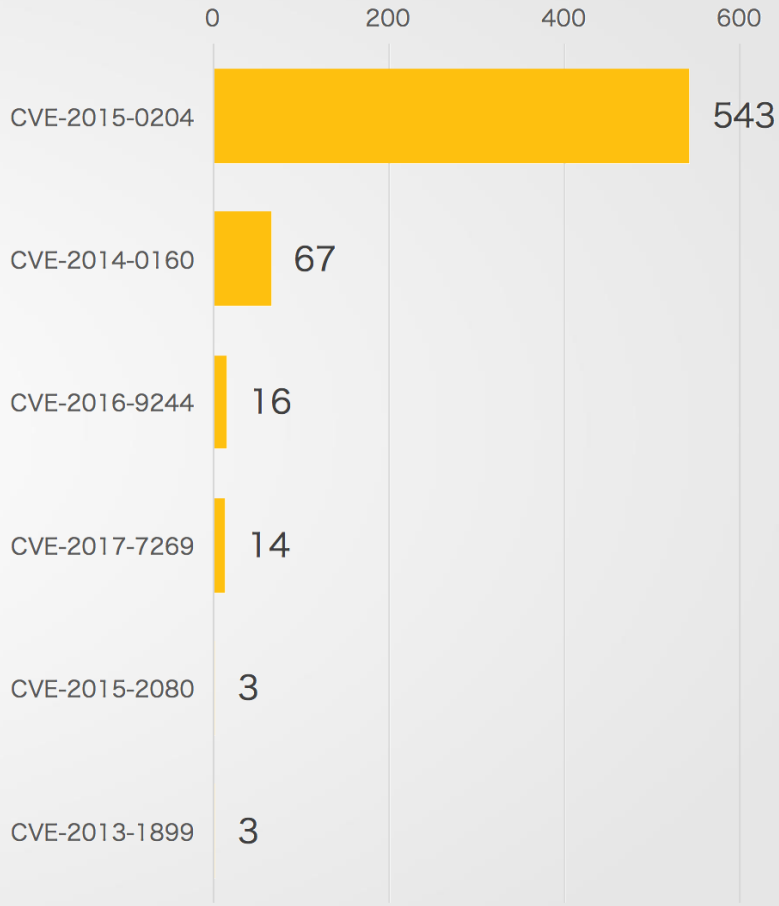


共有云供应商分布



关键问题分析：安全漏洞

- **CVE-2015-0204** 该漏洞是由于OpenSSL库里的s3_clnt.c文件中，ssl3_get_key_exchange函数，允许客户端使用一个弱RSA秘钥，向SSL服务端发起RSA-to-EXPORT_RSA的降级攻击，以此进行暴力破解，得到服务端秘钥。此问题存在于OpenSSL版本0.9.8zd之前, 或1.0.0p之前的1.0.0，或1.0.1k之前的1.0.1
- **CVE-2014-0160**（OpenSSL Heartbleed 心脏滴血）在OpenSSL1.0.1版本的心跳包模块存在严重漏洞（CVE-2014-0160）。攻击者可以通过构造特殊的数据包，直接远程读取存在漏洞的OpenSSL服务器内存中多达64KB的数据，极有可能导致网站用户帐号密码等敏感数据被非法获取。漏洞发现者甚至声称可以直接获取到证书私钥和重要的商业文档。
- **CVE-2016-9244**（Ticketbleed）是F5 BIG-IP设备的TLS / SSL堆栈中的软件漏洞，允许远程攻击者一次提取高达31字节的未初始化内存。
- **CVE-2017-7269** 开启WebDAV服务的IIS 6.0被爆存在缓存区溢出漏洞导致远程代码执行，目前针对 Windows Server 2003 R2 可以稳定利用，该漏洞最早在2016年7,8月份开始在野外被利用。



关键问题分析：网络攻击

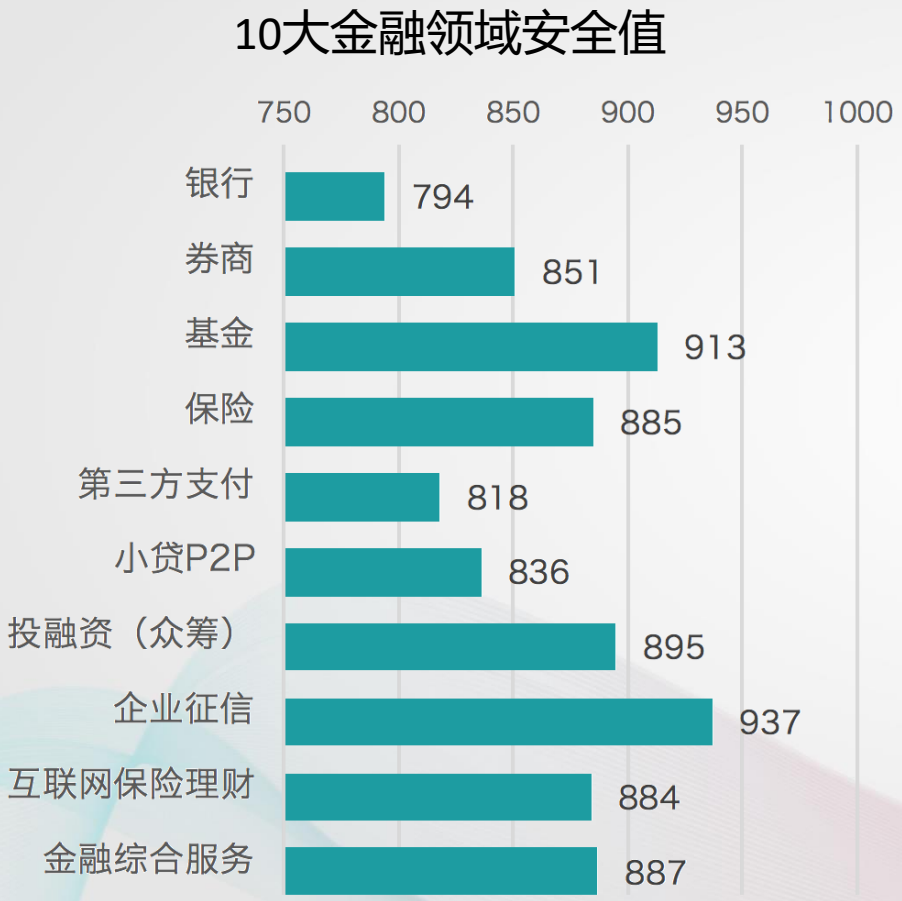
- 受到拒绝服务攻击的端口：

  80、4444、443、53

Top 10 威胁金融行业的IP地址

威胁地址	事件数	说明
221.238.7.97	6048	天津市天津市 电信
180.213.7.20	4717	天津市天津市 电信
117.25.222.122	3943	福建省厦门市 电信
124.200.96.218	1948	北京市北京市 鹏博士宽带
221.238.191.122	1677	天津市宝坻区 电信
27.191.225.23	1326	河北省唐山市 电信
219.141.149.59	969	北京市北京市 电信
65.48.174.139	922	巴巴多斯
62.212.236.10	876	阿塞拜疆
1.193.145.232	762	河南省洛阳市 电信

10大金融细分领域安全评价



子行业	安全值	机构数	A	B	C	云
银行	794	100	37%	51%	12%	14
券商	851	100	38%	32%	7%	29
基金	913	100	73%	26%	1%	8
保险	885	100	58%	38%	4%	29
第三方支付	818	100	27%	70%	3%	17
小贷P2P	836	100	37%	57%	6%	44
投融资（众筹）	895	100	66%	28%	6%	51
企业征信	937	100	72%	27%	1%	19
互联网保险理财	884	100	47%	51%	0%	27
金融综合服务	887	100	50%	48%	2%	26

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Application Scenarios In The Financial

SRS在金融领域的应用场景

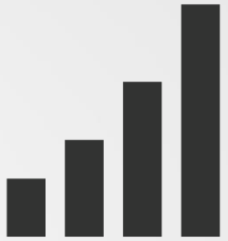
SRS在金融领域的应用场景

行业安全态势分析

为行业主管部门和研究分析机构提供行业网络安全态势分析报告，随时完成行业网络安全风险评估。

第三方风险管理

为风险管理部门提供合作伙伴或供应商的安全评价报告，实现对第三方风险进行持续监测。



企业安全评级

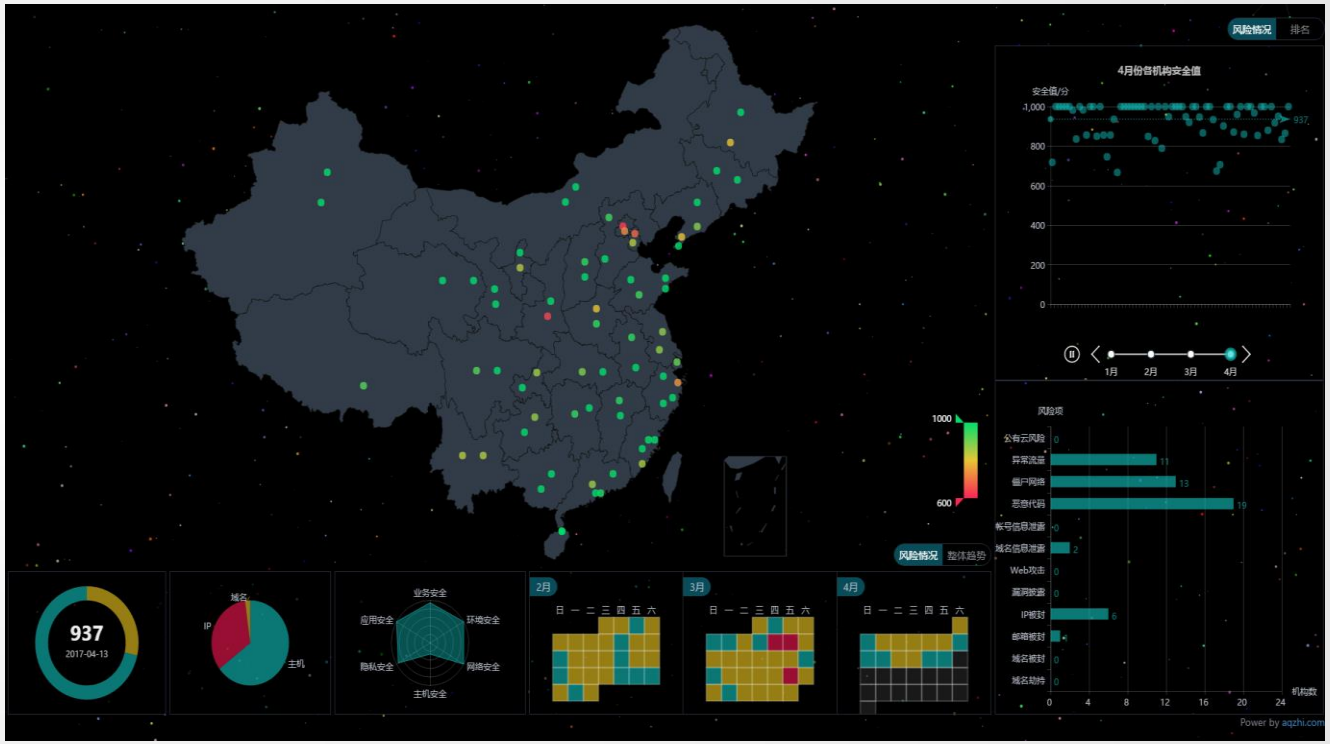
为征信机构和保险公司提供企业安全评级报告，帮助挖掘潜在客户并提高业务竞争力。

行业态势分析

为行业主管部门和集团型企业提供行业网络安全态势分析和绩效评估，形成由上至下安全管理的有力抓手。

金融业务与互联网结合的应用越来越广泛，由此带来的网络安全趋向于复杂化和、多面化、难管控；越来越多的单位希望将安全工作纳入绩效考核的内容之一，从而督促安全责任的落实。

传统的评估方法存在很大局限性，一方面通过现场调查形式只能发现某个时间点的风险状态，无法提供持续性的安全状态评估，而且结果的准确性还要取决于被调查者回答的客观性。另一方面通过渗透、扫描等技术检查需要依赖部署各种检查设备获取信息，实施成本高、周期长。



第三方风险管理

为风险管理部门提供合作伙伴或供应商的持续监测和安全性评估，加强数字供应链风险控制能力。

数字供应链是数字经济时代的主要特征，数字化供应商或者合作伙伴对企业带来的网络威胁不容忽视。为了提高效率大量的与合作伙伴或者供应商的信息系统进行对接，在数字供应链中有大量的信息交互，为避免敏感信息泄漏企业首先需要发现合作伙伴或者供应商的网络安全风险，并采取不同程度的风险控制，降低带来的第三方风险。

风险管理部门需要能够及时获取对其客观的安全评价报告，完成风险评估，采用人工检测和调查的方法势必会带来巨大工作量，并且无法做到及时性和持续性。“安全值”可以保护业务和品牌的完整性，同时对合作伙伴、供应商网络安全状况进行持续监测。

Gartner预测：

到2020，超过70%的公司（当前是25%）将完全把IT风险管理集成到企业风险管理中去。

企业安全评级

为保险公司提供对投保人网络安全、风险等因素进行综合分析，帮助保险公司快速决断业务办理以及挖掘潜在优良客户。

- 普华永道最近一份报告《Insurance 2020 & beyond: Reaping the dividends of cyber resilience》预测，到2018年，全球网络安全保险市场将增至50亿美元，到2020年将增至75亿美元。在美国约有50家保险公司提供专门的网络攻击保险，包括AIG、Chubb和ACE等保险行业巨头。
- 据报道中国人保财险、众安保险、苏黎世保险、阳关财险、安联财险、美亚财险等一些国内和外资保险公司网络安全保险正进行一些探索。
- 随着刚刚实施的《网络安全法》加强对网络安全法律责任和约束。

http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf

企业安全评级报告

C3安全峰会
CYBER | CLOUD | COMMUNICATION

The first 3rd party Security Rating Service in China - aqzhi.com

国内首个第三方安全评价服务 - 安全值

国内首个第三方安全评价服务

安全值产品凭借中立的行业定位，整合全球100多个数据资源，融合多年安全风险管理经验和大数据技术提供多样化服务。

（https://www.aqzhi.com/）

- 安全监管平台
- 企业SaaS服务
- 供应商风险管理平台
- API接口

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank You