

风险管控 以人为本
面向管理 深入业务



驾驭企业信息化风险
引领信息安全管理方向



GooAnn
gooann.com 谷安天下

安全值-量化安全风险

赵毅
2016.7

数据驱动安全

引起重大变革，驱动相互连接协作、产品升级和服务创新。

- 从2015年RSA大会上演的“砸盒子”到2016年RSA的“connection to protect”
- 产业链各环节趋向成熟，需中立第三方资源整合和交换
- APT产品、WAF产品、防病毒产品已利用数据服务升级
- 安全咨询和安全服务也必然通过数据服务转型升级



产品基本介绍

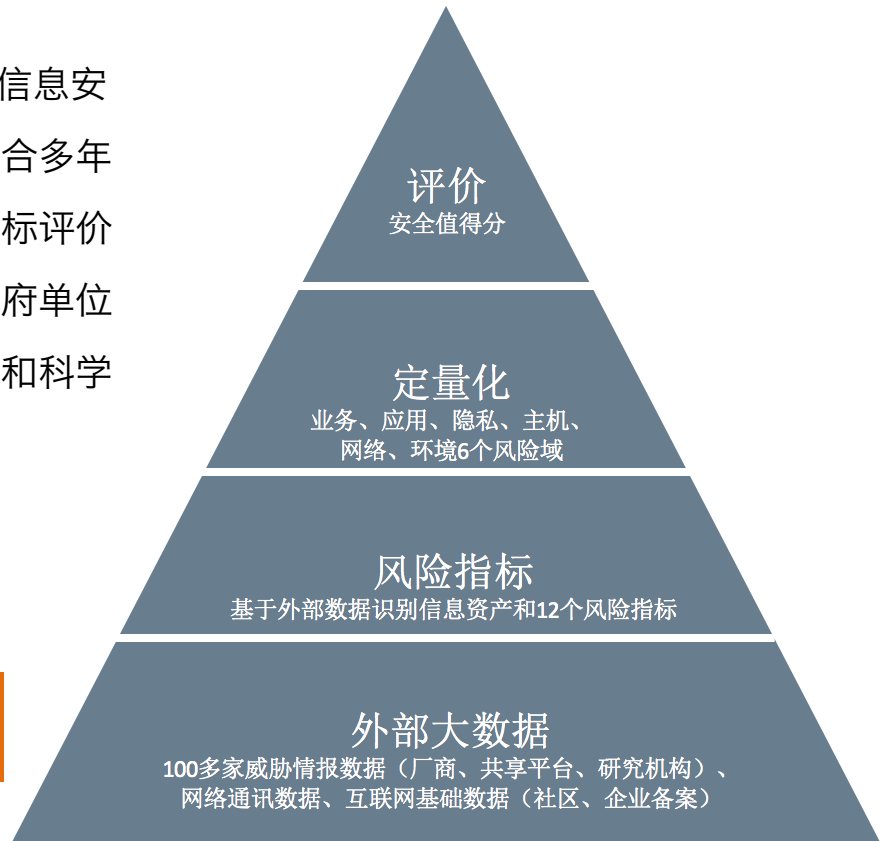
谷安天下凭借多年的信息安全咨询服务经验积累，整合了100多家威胁情报数据资源，构建了一套自动化的大数据风险评估数据服务产品“安全值（www.aqzhi.com）”。实现了从全新视角对外部大数据和威胁情报进行数据挖掘，当前建立了域名劫持、邮箱/IP/域名被封、漏洞披露、Web攻击、恶意代码、僵尸网络、异常流量等12项安全风险指标（持续更新），并完成定量化风险计算和整体评价，提供同行业横向差距对比分析。产品适用于第三方安全评估、安全绩效测量、供应商风险管理和IT审计4大解决方案。



基于威胁情报大数据的风险评估和量化评价方法

参考ISO27001标准实践、等级保护要求、《信息安全保障指标体系及评价方法》等标准规范，结合多年风险领域最佳实践经验，建立信息安全风险指标评价体系，经过银行、证券、保险、大型央企、政府单位客户的实际使用，充分验证了可行性、实用性和科学性。

当前300家客户正在使用，完成对4000家企业资产和风险指标的识别与安全量化评价。



整合顶尖威胁情报资源

安全厂商+交换平台+研究机构+共享平台+开源社区

国内外 100+ 威胁情报数据资源，每天10亿+数据更新，基于自动化平台对实时数据进行大数据挖掘分析，完成量化指标计算，实现外部安全评价，提升综合风险管理能力。



方案核心价值

1

第三方安全评估

- 1.帮助主管部门定期对行业进行第三方安全评估工作，从外部视角的**完成全局、可量化的安全评估**
- 2.弥补传统手段应对**互联网威胁下新风险**时的缺陷
- 3.与同行业进行**行业差距对比**分析，提供管理层决策支持

2

安全绩效指标测量

协助行业主管部门或集团信息安全管理部**门安全绩效考核**工作，在统一评价体系下进行评价，提高下级单位对**互联网风险的和工作积极性**，丰富绩效指标测量手段。

3

供应商风险管理

针对大量的合作伙伴和供应商带来的第三方安全风险。**能够实时提供安全评价报告**，通过在线SaaS模式，自助完成评估需求。保护业务和品牌的完整性，同时对合作伙伴、供应商网络安全风险状况进行**持续监测**。

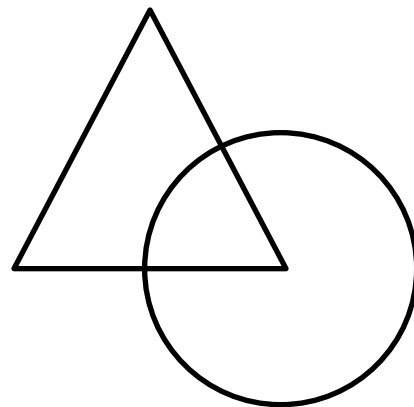
4

IT审计外部评估

依托外部数据实施**独立、客观的检查**，丰富IT审计手段，发现现有控制措施和管理流程的不足。

创新亮点

1. 应对互联网威胁带来的新型风险技术创新
2. 无需部署，提供全局性、多维度的风险评估能力
3. 基于威胁情报国际标准的大数据风险评估方法
4. 基于数据分析技术的风险评估指标计算模型
5. 整合100多家威胁情报数据资源，共建良性发展的数据服务市场生态
6. 利用在线SaaS服务模式的便捷性和低成本特点，实现对全行业用户自动化风险评估
7. 产品同时提供4大领先解决方案，市场空间巨大



团队介绍

依托谷安天下强大的风险管理顾问团队基础成立项目组，从产品销售、售前、运营、市场、研发、数据多层面建立项目组，以下是产品项目组主要成员：

序号	姓名	项目组角色	从业经验
1	赵毅	产品负责人	10年
2	李华	总监/质量管理	15年
3	陈伟	专家顾问	22年
4	范亚玲	主管研发	15年
5	张妤	主管售前	15年
6	冯俊	行业顾问	6年
7	李少鹏	主管市场	15年
8	金炫臻	运营/售后	10年
9	李博	数据分析	6年
10	于彦哲	主管销售	10年

1 人员构成

- 公司注册资金500万
- 公司员工120人，其中专业技术人员逾80人
- 信息安全相关专业硕士、博士、MBA
- 架构设计、风险管理、IT治理、IT审计、IT内控、合规咨询、体系认证、软件安全等方面专家

2 专业资质

- 国际认证信息系统审计师 (CISA)
- 认证信息系统安全专家 (CISSP)
- ISO27001 / 20000 Lead Auditor
- 信息安全专家 (CISP)
- 国际认证信息安全经理 (CISM)
- IT服务ITIL Foundation/Manager.....

3 服务经验

- 曾服务于著名的跨国IT、咨询和安全公司
- 为央企、政府、金融、运营商等行业提供安全咨询、技术、培训等服务的丰富经验

4 安全研究

- 多数顾问在主流安全媒体发表专业文章，是多家媒体特约撰稿人
- 顾问著有黑客攻防、网络安全、信息安全管理等知名著作
- 资深顾问为清华、北京大学CIO班特聘讲师

商业模式及市场情况



央企与政府

交通部 农业部 海关总署 审计署 上海高法 国家认监委 中期协 陕西省网络与测评中心 中国国家博物馆 青岛审计局 中国金融认证中心 广东核电集团 中海油 中石油 中亚管道公司 中国五矿集团 厦门建发集团 首都国际机场 南方航空 神华集团 中国电力投资集团 北京燃气 大唐电信 贵州电网通信公司 深圳供电局... ..



金融行业

中国农业银行 中国银联 上海银联 国家开发银行 民生银行 北京银行 招商银行 江南农村商业银行 晋商银行 重庆银行 上海浦东发展银行 广东发展银行 东亚银行 广州农村商业银行 江阴商行 石嘴山银行 辽宁朝阳商行 深交所 国信证券 安信证券 世纪证券 长城证券 上海证券 天风证券 中国人寿 太平保险 中美大都会 大都会 鹏华基金 科信期货 美尔雅期货... ..



运营商行业

中国电信集团 中国电信北京研究院 天津电信 北京移动 天津移动 湖北移动 河南移动 江西移动 新疆移动 广东移动 山东移动 福建移动 甘肃移动 安徽移动 中国移动 无线音乐运营中心 中国联通 系统集成公司... ..



其他行业

华胜天成 国富安 易宝支付 京北方 北京NTT DATA 同方鼎欣 天融信 西门子 中华英才网 西安未来国际 信城通 南京可鲁 昆山频道 苏州华冠 松下电器 青岛啤酒 拉手网 辉山乳业 佳通轮胎 易宝支付 千红药业 深圳巴士集团 昆山频道 厦门吉联 万欣和... ..

谷安天下10年积累的企业客户基础

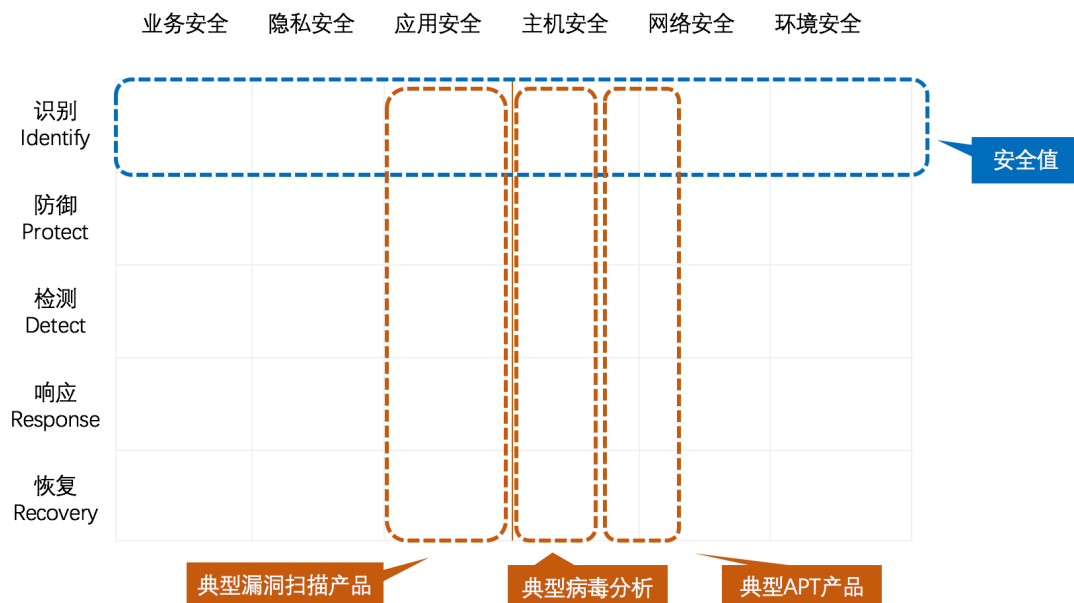
公司现有业务：咨询客户、审计客户、培训客户、意识客户、安全牛、在线教育

市场分析

解决方案	目标客户	市场分析
第三方安全评估	行业信息安全主管部门 安全服务/集成商 企业信息安全管理部	国内的银行、证券、保险、教育、卫生、医疗、制造、能源、交通、零售、互联网等行业机构的信息安全管理部门（例如招商银行、国信证券、中信建投、人寿保险等）。各行业单位数量不一致，保守估计每年投入10万元以上进行风险评估的企业大于 3000家
安全绩效指标测量	行业信息安全主管部门 集团信息安全管理部	我国税务、海关等政府单位以及地方政府部门 100多家 ，神华、五矿、中粮等央企 100多家 ，均对下级进行垂直管理，有迫切的市场需求。
供应商风险管理	科技风险管理部	面向全行业中的供应商、合作伙伴，风险管理部有责任对供应商风险进行控制，《银行业金融机构信息科技外包风险监管指引》要求对外包服务商开展独立性、客观性及公正性的第三方评估报告。
IT审计外部评估	IT审计部	银行、证券等金融机构已经全面开展IT审计工作，迫切需要对互联网业务进行IT审计。

国内市场和竞争分析

属于信息安全服务新业态，市场空间巨大，但还没有直接竞争对手。



对比行业内的其它数据类产品来说，安全值更注重全面、量化，提供安全风险管理解决方案。其它产品均为在特定领域或单维度上发现、分析和解决问题，是横向和纵向的能力管理，避免恶性竞争，形成能力互补，促进行业良性发展。

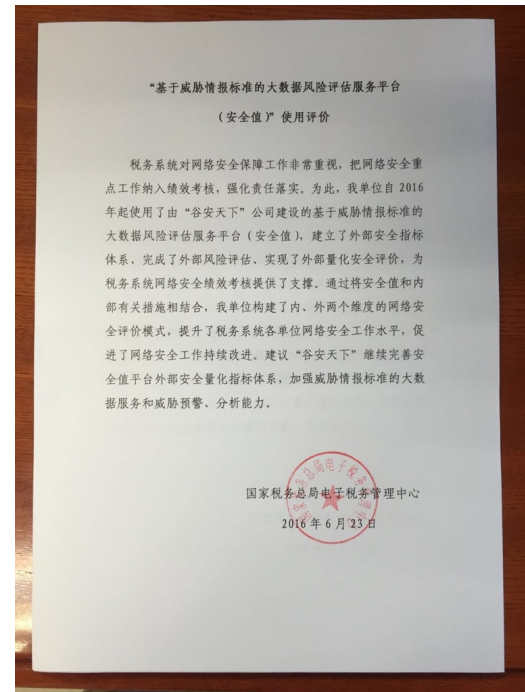
客户评价

已在税务、电力、证券等行业中应用，并得到显著成效。

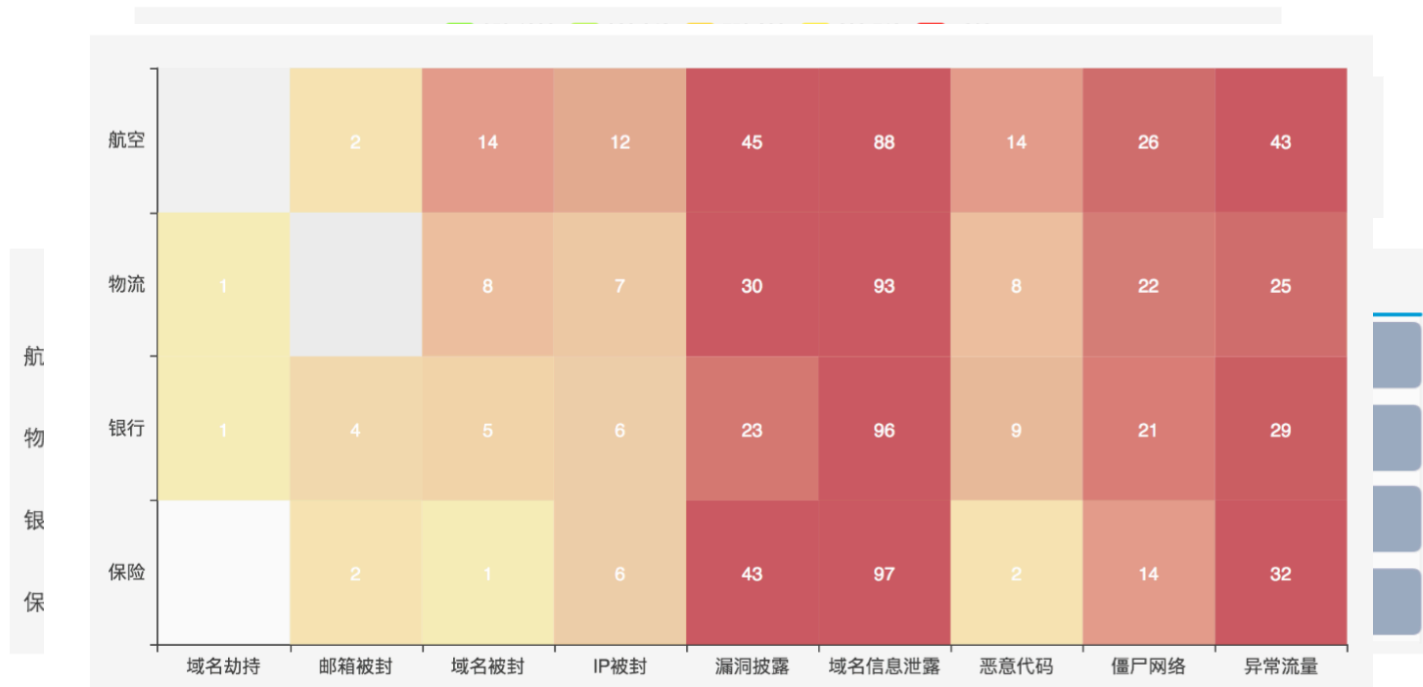
网络安全指数—安全值

考评省税务局门户网站、邮件服务及网上办税系统等综合安全值占网络安全指数一部分，利用在互联网运行的“安全值”平台对省税务局互联网安全状况进行评估打分，考评期内月度得分平均值参与打分。“安全值”网址和省税务局用户帐号已经通过税务网络安全保障网进行发布，各地可自行查看本单位安全值数据及报告。

注：安全值目前是采取每日打分制。



行业报告



根据统计信息来看，2016年上半年航空业漏洞被披露过的单位有19个，占45%，也为上述各行业中**最高**。航空业共发现138个公开发布的漏洞，平均每个航空公司7.26个。

攻击
加
要



行业报告下载 <https://www.aqzhi.com/>

产品演示

面向行业可汇报的绩效指标管理视图



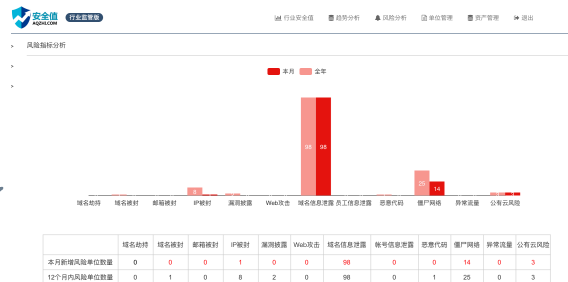
行业安全值



安全值分布



趋势分析



风险分布

更多...

产品演示

面向企业单位的在线SaaS服务平台



安全值报告

互联网资产

风险详情

共137条数据 1 / 100

输入要查看的内容

类型	资产信息	解析设置	名称	状态	识别方式	识别日期	审核状态	操作
域名	aqzhi.com	N/A	安全值	在线	手动	2016-3-1	通过	🔍
域名	aqzhi.com	1.2.3.4	安全值	在线	手动	2016-3-1	未通过	🔍
		1.2.3.4						
主机	edu.gooann.com	1.2.3.4		网络	在线	自动	2016-3-1	审核中
		1.2.3.4						
主机	www.gooann.com	1.2.3.4		门户	下线	自动	2016-3-1	通过
		1.2.3.4						
IP地址	1.2.3.4	www.aqzhi.com		在线	自动	2016-3-1	通过	🔍
		edu.gooann.com						
IP地址	1.2.3.4	CON		在线	自动	2016-3-1	通过	🔍
IP地址	1.2.3.4		办公网出口	在线	手动	2016-3-1	通过	🔍
IP地址	1.2.3.4		办公网出口	在线	手动	2016-3-1	通过	🔍
IP地址	1.2.3.4		办公网出口	历史	手动	2016-3-1	通过	🔍
IP地址	1.2.3.4		办公网出口	历史	手动	2016-3-1	通过	🔍
IP地址	1.2.3.4		办公网出口	历史	手动	2016-3-1	通过	🔍

帐号信息泄露风险详情 企业的员工帐号在第三方数据源中被泄露, 可能包括密码等敏感信息

处置建议:

- 1.加强员工的安全意识宣传和管理制度, 避免使用企业邮箱注册个人的信息帐号;
- 2.加强安全意识宣传办公使用的帐号密码避免和个人帐户的相同, 避免信息泄露之后引来撞库攻击影响企业安全;
- 3.通知泄露信息的员工尽快修改邮箱及其它帐号的密码

请升级为 **专业版用户** 查看全部数据。

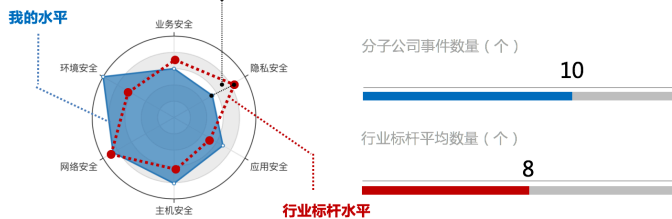
每页显示: 5条 5 条记录

分析时间	员工帐号	泄露信息	泄露时间	泄露源
2016-03-31	fd@aqzhi.com	1*3*5*	2012-05-25	4008000000_COM
2016-03-31	ky@aqzhi.com	k*y*8*0	2012-05-25	4008000000_COM
2016-03-31	ad@aqzhi.com	1*1*3*0*	2012-04-02	YY_COM
2016-03-31	jd*****	*****	*****	*****
2016-03-31	da*****	*****	*****	*****

当前显示 1 到 5 条, 共 44 条记录

上一页 下一页

与数量,频率,时间,影响等多维度量化指标进行差距分析



Q&A
谢谢!

www.gooann.com