|  |
| --- |
| 福建康众畅想信息科技有限公司  www.canpay.com.cn |
| **康众智防** |
| **金融机构信息数据安全解决方案** |
|  |
| **产品项目部** |
| **2016/3/30** |

|  |
| --- |
| 康众智防系统致力于为金融行业提供全面的信息数据安全解决方案，康众畅想公司拥有业界一流的安全研究团队以及安全知识库，针对各种金融平台安全威胁和攻击有着深入的分析和理解，研制了相应的金融信息数据安全防护、监控产品，以及各种专业的安全服务，为金融信息数据安全提供全面的解决方案。 |

**目录**

[一、政策背景 - 2 -](#_Toc447179857)

[二、金融行业安全威胁 - 3 -](#_Toc447179858)

[三、康众智防金融信息数据安全解决方案 - 5 -](#_Toc447179859)

[3.1安全解决方案概述 - 6 -](#_Toc447179860)

[3.1.1攻击行为威胁 - 6 -](#_Toc447179861)

[3.1.2安全防御建设目标 - 8 -](#_Toc447179862)

[3.2安全解决方案组成 - 8 -](#_Toc447179863)

[3.2.1金融行业Web安全解决方案 - 8 -](#_Toc447179864)

[3.2.2入侵检测与防御安全解决方案 - 12 -](#_Toc447179865)

[3.2.3安全基线管理解决方案 - 13 -](#_Toc447179866)

[3.3可量身定制的专业安全服务 - 13 -](#_Toc447179867)

[3.4应用优化加速 - 13 -](#_Toc447179868)

[3.5金融信息数据安全解决方案部署形式 - 13 -](#_Toc447179869)

[四、方案价值 - 14 -](#_Toc447179870)

[五、方案优势 - 14 -](#_Toc447179871)

[六、公司介绍 - 15 -](#_Toc447179872)

[七、联系我们 - 15 -](#_Toc447179873)

**金融机构信息数据安全解决方案**

**适用对象：**

金融机构信息数据中心、互联网金融平台等

# 一、政策背景

随着信息技术的广泛应用和电子商务的快速发展，金融业务与互联网的进一步融合，我国金融业信息化正经历向信息化金融的转变，信息化金融已逐渐成为我国金融业的发展方向。但与此同时，由于这种新型服务方式虚拟化、业务边界模糊化、经营环境开放化等特点，使得互联网上的金融业务面临网络攻击、病毒侵扰、非法窃取账户信息、客户信息泄漏等新的信息安全挑战。

党和国家领导人多次就金融行业信息安全做出重要指示，要求金融业研究和把握又好又快的发展规律，努力提高信息安全保障水平，坚决打击危害金融信息安全的犯罪活动。

2014年2月，中央网络安全和信息化领导小组成立。习近平任组长，李克强、刘云山任副组长。习近平在小组会议上强调，没有网络安全就没有国家安全，没有信息化就没有现代化。建设网络强国的战略部署要与“两个一百年”奋斗目标同步推进，向着网络基础设施基本普及、自主创新能力显著增强、信息经济全面发展、网络安全保障有力的目标不断前进，网络安全问题上升到国家战略高度。

2015年6月，全国人大委员会颁布了《中华人民共和国网络安全法（草案）》，明确指出建设、运营网络或者通过网络提供服务，应当依照法律、法规的规定和国家标准、行业标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行；国务院和各级政府扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发、应用和推广，保护网络技术知识产权，支持科研机构、高等院校和企业参与国家网络安全技术创新项目。

2015年7月，全国人大委员会颁布了《国家安全法》，要求国家建设网络与信息安全保障体系，提升网络与信息安全保护能力；加强网络和信息技术的创新研究和开发应用，实现网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全可控；加强网络管理，防范、制止和依法惩治网络攻击、网络入侵、网络窃密、散布违法有害信息等网络违法犯罪行为，维护国家网络空间主权、安全和发展利益。

2015年8月，经李克强总理签批，国务院日前印发了《促进大数据发展行动纲要》。《纲要》中要求在涉及国家安全稳定的领域采用安全可靠的产品和服务，到2020年，实现关键部门的关键设备安全可靠，完善网络安全保密防护体系；建设完善金融、能源、交通、电信、统计、广电、公共安全、公共事业等重要数据资源和信息系统的安全保密防护体系。

# 二、金融行业安全威胁

**迅速发展的信息化金融体系未匹配可靠的安全系统**

数据中心作为金融机构承载业务的重要IT基础设施，承载着金融机构业务发展和创新提供基本保障的重任。近年来，国内各类金融机构业务发展和相应的机构扩张非常迅速，建设新的数据中心和灾备中心的情况非常普遍。

在新的业务规模要求下，数据中心需要更高效地支持业务和信息共享需求，提供不间断的服务，这对数据中心的资源整合、全面安全、高效管理和业务连续性提出更高的要求。

2014年1月，韩国发生金融行业最大规模信用卡个人信息泄密事件，涉及约2000万用户，共1亿多条客户信息被泄露，最多的用户有19项个人信息被泄露。

2014年3月23日凌晨，携程被爆安全支付日志可遍历下载，因此导致大量用户银行卡信息泄露，其中包括持卡人姓名、身份证号、银行卡号、卡CVV码、6位卡Bin。

2014年10月2日，摩根大通银行承认7600万家庭和700万小企业的相关信息被泄露。身在南欧的黑客取得摩根大通数十个服务器的登入权限，偷走银行客户的姓名、住址、电话号码和电邮地址等个人信息，与这些用户相关的内部银行信息也遭到泄露。受影响者人数占美国人口的四分之一。

2015年5月，中国某大型保险公司公司也经历了泄露危机。公司系统存在高危漏洞，10万份保单或遭泄露。保单信息、微信支付信息、客户姓名、电话、身份证、住址、收入多少、职业等敏感信息一览无余。

2015年6月，信融财富、宝点网和立业贷等多家P2P平台同时遭受黑客流量攻击，造成网站无法打开或访问速度缓慢。根据世界反黑客组织的通报，中国P2P平台已成为全世界黑客“宰割的羔羊”。

2015年11月，补天漏洞响应平台爆出重庆网贷平台易九金融的系统存在漏洞，上万用户数据泄露再次拷问国内P2P金融数据系统安全。

2016年3月7日，孟加拉国央行称，他们在美联储的账户遭遇黑客攻击，部分资金被盗走，被盗资金约为1亿美元。

**不安全的网络正在遭受更不安全的使用**

各金融机构缺乏严格的政策管理和代码审计，业务发展的速度又远超安全可提供的支撑能力，前台代码质量较低，导致出现大量设计逻辑错误、SQL注入、跨站脚本攻击；从业人员安全意识低，管理不到位，导致出现大量弱口令、框架漏洞、配置错误、敏感信息泄露；软件更新缓慢，导致框架错误等。

“乌云”等知名漏洞响应平台曾曝光了多家银行、券商、保险、基金公司网站存在漏洞。2015年上半年我国金融机构的互联网安全漏洞数量快速增长，投资者的个人信息、账号密码、交易记录均存在被泄露的风险。银行、证券、保险、基金等均有知名机构“中招”，“乌云”平台漏洞数据显示，仅2015年上半年，已被金融机构确认、修复的自身网站安全漏洞的数量已超过去年同期，其中金融机构网站高危和中危漏洞数量的总和，已占总体探知漏洞总数的97.2％。

2015年9月至11月三个月的时间里，安华金和在乌云漏洞平台上汇总金融行业已被客户确认的安全漏洞共206个。其中高危漏洞195个，中危漏洞9个，低危漏洞2个。而这206个漏洞中，直接与数据泄露相关的漏洞110个，占漏洞总量的的53%。

**更深度的安全威胁日渐繁多**

金融机构所面临的安全形势也越来越严峻，安全威胁越来越突出，病毒、木马、蠕虫、黑客攻击等，都可能使数据中心网络和核心业务造成严重的破坏。数据中心与灾备中心是金融机构绝大部分重要信息系统所在的位置，通常包括核心生产系统、网上银行系统、支撑系统、交易系统、管理系统及其他运行关键业务或涉及客户身份、资产、交易记录等敏感信息的重要信息系统。一旦出现问题，后果将不堪设想。

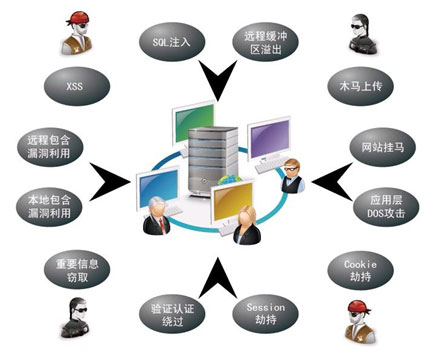
金融行业重要的信息系统关系到国计民生，是国家信息安全重点保护对象，国家信息安全监管职能部门需要对其重要信息和信息系统的信息安全保护工作进行指导监督。因此金融监管部门要求金融机构的信息科技风险和信息安全管理水平必须符合一定的要求，以免某个机构自身的问题影响金融业整体安全与稳定。

# 三、康众智防金融信息数据安全解决方案

康众智防系统致力于为金融行业提供全面的信息数据安全解决方案，康众畅想公司拥有业界一流的安全研究团队以及安全知识库，针对各种金融平台安全威胁和攻击有着深入的分析和理解，研制了相应的金融信息数据安全防护、监控产品，以及各种专业的安全服务，为金融信息数据安全提供全面的解决方案。

## 3.1安全解决方案概述

### 3.1.1攻击行为威胁

金融信息数据的风险和安全问题，主要来自有组织有目的黑客频繁侵袭、拒绝服务攻击（DDOS）、恶意代码（如病毒蠕虫）、越权访问、网络传输泄密、内部人员越权和滥用、数据篡改和抵赖行为等。

**1、黑客攻击：**攻击者利用黑客技术非法入侵机构的数据库等系统，窃取、篡改、拷贝系统数据，私自添加或删除账号、注入木马、盗取用户账户、修改用户设置、盗取敏感信息等从而进行有目的的金融犯罪行为；常见的攻击场景如下：

（1）黑客利用对网站影响较大的漏洞，如，Stuts2命令执行漏洞，轻易攻陷网站服务器，获取网站注册用户的帐号密码和个人资料；

（2）机构平台受到大规模钓鱼攻击，大量客户诱骗录入用户名、账号、转账密码等敏感信息造成资金损失。

（3）黑客行为所带来的影响也难以预知，如果黑客试图操纵股票价格，或虚假交易，或篡改账户信息，或者获得一些内幕消息，也会不可避免的使投资者的资产化为泡沫。

**2、拒绝服务攻击（DDOS攻击）：**金融机构由于外部访问门户网站及互联网交易平台IP数剧增，攻击者的网络地址针对注册页面发起探测攻击，尝试上百万个身份证信息进行用户注册，从而导致服务平台无法正常提供服务，导致门户网站及交易平台反应迟缓，互联网出口堵塞，网络使用带宽超过日常使用值，且占满总体带宽。这种攻击使金融行业的门户网站、交易网站无法为客户提供正常服务，造成经济损失，同时也使行业形象受到损害。

**3、蠕虫、病毒攻击：**蠕虫、病毒泛滥可能导致机构重要信息遭到损坏，或者导致机构网络和信息系统瘫痪。以移动智能终端病毒为例，典型的攻击场景如下：

(1)手机支付病毒植入机构手机客户端再通过二次打包的方式把恶意代码嵌入机构的APP程序，一旦被该病毒感染，会不经用户允许私自下载软件并安装，危及用户的帐号安全。

(2)攻击者欺骗买家或卖家在手机上扫描二维码查看订单详情或者打折优惠，被植入“验证码”大盗病毒，攻击者会通过“验证码”大盗病毒截获某些电商官方发送的相关验证码信息，通过重置电商支付帐号密码，盗取资金。

**4、安全系统疏于维护：**因为金融行业一般都较早的进行了信息化建设和维护，很多时候做过周密的预案和灾备演练后就放松了对系统的整体安全维护，让怀有不轨想法的内、外部泄密人员钻了空子，而这点往往是泄密事件高发的诱因。

### 3.1.2安全防御建设目标

根据金融信息数据的风险和安全问题，金融行业数据信息的安全方案应根据不同系统承载的功能进行对应的设计，**重点保障与核心业务、实时业务有关的系统，以保证业务持续运行和数据安全为主要目标。**

金融行业信息数据网络可以根据业务连续和数据安全的原则进行保护措施的设计，可能包括访问控制、异常流量检测与清洗、Web应用防护、入侵检测、安全漏洞管理、安全配置管理、病毒检测与清除、安全运维管理、认证和加密等。康众智防结合行业观察以及相关实践，为金融行业提供整体安全解决方案，以长期保证金融系统的信息安全。

## 3.2安全解决方案组成

**康众智防针对金融行业的主要威胁，提供以下安全解决方案：**

* 金融行业Web应用安全解决方案
* 入侵检测与防御安全解决方案
* 安全基线管理解决方案
* 可量身定制的专业安全服务

### 3.2.1金融行业Web安全解决方案

康众智防系统属于国内领先，世界先进的大型网络防御系统。在国内尚无同类产品可形成同等技术高度和性能的对比。

针对金融行业Web应用威胁的特点，从开发（代码层）和运行等环节，从事前、事中、事后等风险管理角度出发，采用内、外的结合的防护手段，建立了主动、纵深、多层面的安全保障体系，可以有效保护金融行业web应用的安全性，降低系统面临的风险。

加强对金融信息数据平台Web服务器、数据库服务器等的安全配置；加强自主可控密码算法在应用系统中的使用，切实保护敏感数据的传输和存储安全性；合理部署防病毒系统、入侵检测系统等安全防护系统，确保其策略合理配置、特征库定时升级；针对常见攻击点，调整优化网络结构。

提供七层的DDOS攻击防护，包括CC攻击、SYN、flood等所有DDOS攻击方式通过分布式高性能防火墙、精准流量清洗、CC防御、web攻击拦截，组合过滤精准识别，完美防御各种类型攻击。

#### 1）针对金融行业web应用事前检测优化

* **面临威胁：扫描，探测等攻击开始前进行站点信息采集**

金融机构各系统网络站点的信息收集是不法份子为非法访问、攻击或诈骗作准备。Web服务器漏洞中，跨站脚本漏洞与SQL注入漏洞所占比例很高，黑客可以利用网络爬虫技术对Web漏洞直接进行探测、扫描。由于缺乏足够的安全知识，相当多的程序员在编写金融机构Web应用程序时对网页的请求内容缺乏足够的检查，使得不少金融机构Web应用程序存在安全隐患。黑客通过提交一段包含SQL语句或脚本的URL请求，根据程序的返回结果获得有关的敏感信息甚至可以直接修改金融机构web应用网站的后台数据。因此，在防爬虫探测及事前及时发现系统漏洞并进行修复变得极其重要。

* **防护措施：**
* 爬虫防护，保护金融平台敏感数据信息内容，过滤恶意扫描、探测；
* 安全评估测试，对金融信息数据平台进行全面安全评估，并进行渗透测试，及时针对平台系统进行安全加固；
* Web漏洞扫描，对金融信息数据平台进行系统漏洞扫描，提前发现漏洞并进行修复，提高金融信息数据平台防御能力；
* 代码审计，对金融信息数据平台进行代码静态/动态安全检测，消除系统代码层的安全漏洞，并提高开发人员的安全开发水平。
* 黑冰加密系统，对系统代码层（PHP代码）进行高强度加密。

#### 2）针对金融行业web应用事中安全防护

* **面临威胁：黑客侵袭、DDOS攻击、病毒木马攻击、用户数据窃取、数据篡改等金融信息数据的风险和安全问题**

《IT时报》消息：汇丰银行网上银行遭遇DDoS攻击被迫下线。2016年1月4日，汇丰银行遭受不明流量攻击，系统崩溃，服务中断两天;1月29日，汇丰银行再次遭受DDoS攻击，服务再次陷入瘫痪，这次袭击意味着用户无法在线访问他们的账户，业务损失惨重。由此可以窥见，2016年DDoS攻击将再度猖獗。

* **防护措施：**
* 访问控制（如防火墙）用于应对外部攻击；
* 协同防护，共同防御黑名单，阻止已知疑是用户访问平台，管理员可在后台设置防御等级；
* 篡改监控，添加伪装虚拟服务器进行系统防护，监控攻击手段，检测入侵目的；
* 高级CC防御，自动检测流量变化，防止应用层DDOS攻击；
* 高级DDOS防御，海量的宽带储备和自有抗DDOS防御系统集群，流量监测和清洗设备用于应对大流量拒绝服务（DDOS）攻击；
* 金融平台安全检测，实时监测平台运行状态，钓鱼网站及挂马情况等，并及时清理；
* 高级WAF防护，支持多种防御规则集，有效控制和缓解HTTP及HTTPS应用下各类安全威胁，防御诸如参数篡改、路劲穿越、SQL注入、跨站脚本攻击、Cookie窃取等攻击手段，实时保护防止黑客攻击；
* 安全监控，对金融信息数据系统进行远程安全漏洞扫描、挂马检测、敏感内容监控、网站流量监控检测、网页篡改检测、钓鱼网站监测等，实时评估和发现系统的安全隐患和攻击，并与WAF防御系统联动，提供多层面的安全防护能力。

#### 3）针对金融行业web应用事后处理

* **面临威胁：网页篡改、网页挂马等**

国家计算机网络应急技术处理中心数据公布，2016年1月，我国被篡改网站的数量为6364个其中，被篡改政府网站(GOV类)占比约为1.8%。福建省被篡改网站数量为574个，江苏省被篡改网站数量428个，其中金融类网站被篡改数量181个。金融机构网站作为金融机构对外业务的重要窗钩，一旦被篡改将造成多种严重的后果，主要表现在以下一些方面：

1、机构形象受损：金融机构网站的网页被篡改后，访问者将看到被涂鸦的页面，会导致广大民众对金融机构信息安全防护能力的怀疑，更会担心金融机构在资金及信息数据安全等诸多问题，给金融机构的可信形象打上问号。

2、影响信息传达：网页被篡改后，访问者将无法获取自己需要的内容，金融机构发布的各种信息将得不到传达，影响了信息的发布和传播，假如黑客非法破坏了金融网站的数据库，更长的系统恢复时间将带来深远的影响。

3、恶意发布信息：有些黑客会篡改网页的内容，以金融机构的名义发布恶意和不良信息及言论，从而导致社会金融恐慌。

4、 木马病毒传播：黑客入侵金融机构网站后，或会在网页中插入木马和病毒程序，来访者将会被感染，从而导致计算机病毒的传播，引发系统崩溃、数据损坏和银行账号被盗等严重后果。

* **防护措施：**
* 网页防篡改，在web应用上检测、阻止非法网页篡改或及时进行网页恢复；
* 篡改日志查询，对后端数据库及代码层操作行为进行记录，发现各种潜在的非法操作和攻击行为，并进行法律取证及数据修复；

### 3.2.2入侵检测与防御安全解决方案

* 入侵检测（IDS）用于应对外部入侵和蠕虫病毒；
* 敏感数据保护，识别并阻断特定格式的文件的外发，同时能够检测出文件中包含的敏感数据，进行告警和阻断，保护企业敏感数据，防止敏感数据泄露造成的损失。
* 客户端防护，增加了针对主流客户端应用程序的攻击签名规则，如Word、Excel、PDF、Firefox等，增强了客户终端应用程序的安全防护能力。
* 服务器非法外联防护，通过服务器的自学习功能或手动设置服务器正常外联行为，建立合法连接，能够检测服务器异于该合法连接的非法外联行为，及时产生告警信息通知网络管理人员，从而检测是否存在跳转等攻击行为。
* 僵尸网络防护基于实时的信誉机制，结合企业级和全球信誉库，可有效检测恶意URL、僵尸网络，保护用户在访问被植入木马等恶意代码的网站地址时不受侵害，第一时间有效拦截Web威胁，并能及时发现网络中可能出现的僵尸网络主机和C&C连接。
* 安全应急响应，对未知的攻击手段进行自学习或抵制防御，探索攻击的途径和方式，找出问题原因，从根本上解决安全问题。

### 3.2.3安全基线管理解决方案

* 远程接入管理（如VPN）用于应对非授权接入；
* 轻卫士高强度密匙，通过专用软件系统实现身份认证、权限管理、数据加密等功能。

## 3.3可量身定制的专业安全服务

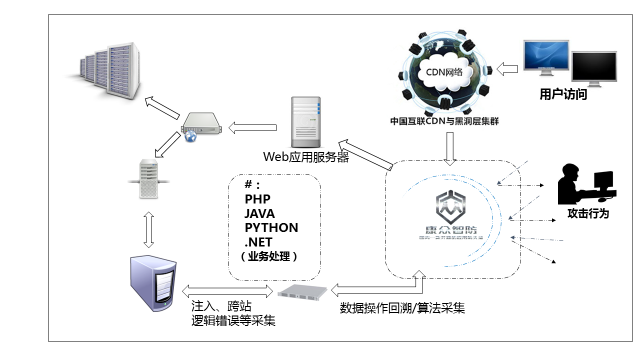
采用大数据分析技术，实时分析互联网上各种攻击数据，进行针对性防护方案定制。

## 3.4应用优化加速

* 全球CDN加速支持，拥有全球节点，提升任何地区访问金融web应用网站速度；
* 资源缓存，自动缓存金融机构业务平台静态/动态资源，提升网速并节省宽带和流量；
* 全球DNS,全球泛播到最近最快速的节点，加快金融服务平台系统响应速度。

## 3.5金融信息数据安全解决方案部署形式

通常部署于骨干网节点公共服务器群（即云端），或部署于企业自有服务器群时可选择纯软件方式或硬件服务器方式实施部署。（如下图）



# 四、方案价值

* 保障信息化金融服务平台的安全、可靠、稳定运行，提高客户满意度；
* 设计金融机构整体安全体系的基本架构，从根本上建立扎实的基础；
* 切实防御已知攻击手段，并对未知攻击手段有一定检测与防御能力，并快速完善到现有防御体系中；
* 建立安全体系的宏观视角，避免各部分安全工作零散、不成系统；
* 严格遵从监管部门相关要求，有效控制合规风险；
* 能够适应金融机构业务发展迅速的特点，在有需要时可灵活扩展安全设备或服务；
* 同时可用于指导灾备中心安全建设。

# 五、方案优势

* 对安全漏洞进行管理，降至安全成本；
* 立体的安全防护体系，高针对性的防护措施；
* 有效地监控、备份与恢复措施，彻底保障金融信息平台的完整性；
* 7\*24小时金融信息系统安全监控；
* 可靠的安全审计措施，可供事件追溯和法律取证；
* 统一安全管理；
* 可随时接入安全设备或扩展其他专业安全服务

# 六、公司介绍

福建康众畅想信息科技有限公司主要从事互联网安全、软件开发、运营管理，提供互联网应用整体解决方案。

福建康众畅想是中国互联网应用环境安全建设的先行者和技术开拓者，企业前身是原“中国计算机病毒防御中心”（[www.54vb.com](http://www.54vb.com)），创建了专业领域久负盛名的BlackIce中国区防御规则团队。这个发展了10余年，安全技术积累深厚的网络安全专家团队，专业面向网络大环境的安全问题研发技术和工具，并转化相关技术成果。迄今已获关键性安全技术著作权18项，攻击防御领域的软件成果和平台性系统型成果数十项。是国内少有具备完善安全生态环境和商业发展模式的企业。企业凭借强大的技术实力和独特的运营模式，以及世界先进水平的WEB应用安全防火墙，填补了国内的行业短板。在结合优秀商业模式后，打造出国内互联网整体安全环境的技术核心。

# 七、联系我们

公司名称：福建康众畅想信息科技有限公司

联 系 人：

联系方式：

公司地址：厦门市思明区龙山南路84号（厦门工业设计中心207室）