bicdroid 佰倬

金融行业数据安全解决方案

佰倬信息科技有限公司

目录

1.概述

1.1 背景

依据《中华人民共和国网络安全法》第三十一条，阐明了保护范围是国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施。保护方法为在网络安全等级保护制度的基础上，实施重点保护。重点保护的对象及关键信息基础设施，包括设施保护、数据保护、产品和服务保护，其中数据保护的对象为“个人信息”与“重要数据”。

近年来，以《中华人民共和国网络安全法》为核心，我国就数据安全相继出台多项新政策，包括已提请审议草案的《数据安全法》《中华人民共和国个人信息保护法》，已发布的《信息安全技术个人信息安全规范》《网络安全等级保护制度》 2.0、《数据安全能力成熟度模型》等。

金融行业作为关乎国计民生的重要行业，一直是国家的强监管领域，近两年多项数据安全相关规范相继发布，包括《个人金融信息保护技术规范》《金融数据安全数据安全分级指南》《金融数据安全数据生命周期安全规范》等。所有新政的数据保护核心对象依然都是“个人信息”和“重要数据”。

1.2 数据安全现状

过去的几年间，大型数据泄露事件层出不穷，这其中不免存在媒体聚焦度提升带来的舆论转移，但究其根本是社会各界对于数据资产安全的关注度与日俱增。Facebook 数据泄露事件，AWS、德勤、网易、Equifax、京东、优酷、58 同城等商业巨头纷纷中招，政府机构和组织也不能幸免，考生信息、公民医疗信息等民生数据泄露事件正在倒逼政府主管机构和企业对数据安全建设重视与落实。其中既有黑客的攻击，更有内部员工的信息贩卖、离职员工的信息泄露、第

三方外包人员的交易行为、数据共享第三方的数据泄露、开发测试人员的违规操作等；究其原因，既有安全意识的薄弱，也有由于安全体系的老旧或安全策略的过时而导致的数据泄露。

这些复杂的泄露途径无一不在证明：传统网络安全中以抵御攻击为中心、以黑客为防御对象的策略和安全体系构建存在重大的安全缺陷，传统网络安全为中心需要向以数据为中心的安全策略转变。

1.3 参考标准及文献

- GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求
- GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型
- GB/T 25069—2010 信息安全技术术语
- GB/T 35273-2020 信息安全技术个人信息安全规范
- JR/T 0092—2019 移动金融客户端应用软件安全管理规范
- JR/T 0158—2018 证券期货业数据分类分级指引
- JR/T 0068—2020 网上银行系统信息安全通用规范
- JR/T 0171—2020 个人金融信息保护技术规范
- JR/T 0197—2020 金融数据安全数据安全分级指南
- JR/T 0223—2021 金融数据安全数据生命周期安全规范
- JR/T 0068—2020 网上银行系统信息安全通用规范
- ……

2.数据安全需求

2.1数据安全风险分析

2.1.1. 数据泄漏

数据窃密事件频发、泄密数据量大成为当今数据泄密事件的典型特征。主要存在以下三大风险。

1） 数据基础设施频受攻击，数据泄露风险加大

近年来各种恶意应用、木马、后门等日益增多，攻击手法从破坏数据转型为获取数据。如 2014 年底发生的 12306 网站 13 万用户信息泄露；2016 年雅虎全

部 30 亿帐户都被泄露。最终雅虎被收购。2018 年 Facebook 遭遇大规模泄密，市值蒸发 1230 亿美元以上，同时还面临 2 万亿美元罚金。英国航空 2018 年大规模泄露了旅客信息，被欧盟处以 1.83 亿英镑罚款……以上泄密事件都给其公司造成了极大的负面影响，并且部分泄密事件还涉及到用户的个人隐私敏感信息。

2） 新型安全威胁层出不穷，数据保护技术有待革新

新型网络安全威胁的技术复杂性和隐蔽性越来越高，危害范围不断扩大。2014 年发现的“心脏出血”漏洞，威胁全球约 2/3 的网络服务器内存储的用户名、密码以及服务器证书、私钥等敏感数据安全；同年索尼公司遭遇 ATP 攻击，大量员工信息及影视拷贝遭泄露。新型网络威胁层出不穷要求传统数据保护技术进行创新突破。

3） 数据交易地下产业链活动猖獗，数据窃取贩卖加剧风险

在利益驱动下，针对用户信息的非法收集、窃取、贩卖和利用行为日渐猖獗，据统计，国内倒卖用户信息的地下产业链总规模已超百亿。监管部门也面临攻击技术手段多样、涉及环节多、隐蔽性强等执法挑战，长期治理任重道远，企业还需从内部加强自身数据安全防护能力。

2.1.2. 数据篡改

如果数据管理人员对数据的使用权限不进行严格控制，对哪些人有数据访问权限、哪些人有数据修改更新权限，缺乏严格的检查控制措施，对用户在计算机上的活动没有进行监督检查，就会导致非授权用户非法存取，合法用户对数据进行篡改。导致数据被破坏，无法使用，防止数据被非法篡改凸显重要。

数据安全问题多数是从 Web 端开始，各行各业根据自身需要大都进行了网站建设，用于信息发布、网上电子商务、网上办公、信息查询等等，网站在实际应用中发挥着重要作用。尤其是我国电子政务、电子商务的大力开展，网站建设得到了空前发展，与此同时随着网民数量的快速增长，通过网站来了解新闻、在线处理业务、查询关键信息等对网站的发展也起到了关键性的促进作用，网站的社会舆论效益逐步显现，已经引起了社会的广泛关注。

然而不幸的是，黑客强烈的表现欲望，国内外各种非法组织的不法企图，商业竞争对手的恶意攻击，不满情绪离职员工的泄愤等等各种原因都将导致网页被

“变脸”。网页篡改攻击事件具有以下特点：篡改网站页面传播速度快、阅读人群多，复制容易，事后消除影响难，预先检查和实时防范较难，网络环境复杂难以追查责任。

2.1.3. 勒索病毒

计算机病毒具有繁殖性、破坏性、传染性、潜伏性、隐蔽性、可触发性，在科技发展的今天，病毒多样性，尤其是最近流行的勒索病毒，对数据安全的造成巨大的威胁，可能会直接威胁到数据库。

企业内部人员在上网时候不小心中了病毒或木马，电脑上存储的重要资料被流恶意失的情况也非常多。由于病毒和木马泛滥，使得企业泄密的风险越来越大。这种有针对性的泄密行为，导致的危害也相当严重。尤其是对于近期频繁爆发的勒索病毒，病毒文件一旦进入本地，就会自动运行，同时删除勒索软件样本，以躲避查杀和分析。勒索病毒利用本地的互联网访问权限连接至黑客的 C&C 服务器，进而上传本机信息并下载加密私钥与公钥，利用私钥和公钥对文件进行加密。除了病毒开发者本人，其他人是几乎不可能解密。由于勒索病毒攻击拥有低成本、高产出等特性，网络犯罪集团可以通过不断推出新的变种版本，来躲避杀毒软件的查杀。而一旦中招，受害者往往为了减少损失，会选择支付赎金，无疑助长了勒索病毒的泛滥态势。

2.1.4. 内鬼作案

金融机构是掌握大量隐私信息、商业机密、财产安全等数据的重要部门，经济驱使的“内鬼”作案，管理松散的资料拷贝，是造成数据被窃的重要原因。这些活动常常是通过电子手段的人为犯罪，可能改变数据，也可能不改变数据。

除此之外，企业的内部员工对公司不满，也会通过恶意破坏数据等行为来发泄不满情绪。

2.1.5. 黑客攻击

黑客以攻击、入侵他人电脑系统、盗窃系统敏感数据信息、破坏目标系统的数据为目的，通过获取的非法数据信息牟取利益。如今黑客的攻击手段也是日新月异不断发生改变，Web 应用漏洞提权、SQL 注入、社会工程学、0day 漏洞利用、Rootkit、无线入侵、邮件攻击、拒绝服务攻击等都可作为黑客的入侵手段。

2.2 合规需求

2.2.1. 网络安全等级保护基本要求

等保 2.0 安全通用要求中的安全计算环境对重要数据的安全防护要求如下：

安全控制域	安全控制点	要求项	适用等级
安全计算环境	访问控制	d)应授予管理用户所需的最小权限，实现管理用户的权限分离；	2，3
		e)应由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则	3
		f)访问控制的粒度应达到主体为用户级或进程级，客体为文件、数据库表级	3
		g)应对重要主体和客体设置安全标记，并控制主体对有安全标记信息资源的访问。	3
	安全审计	a)应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要的安全事件进行审计；	2，3
		b)审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息	2，3

	入侵防范	f)应能够检测到对重要节点进行入侵的行为,并在发生严重入侵事件时提供报警。	3
	恶意代码防范	应采用免受恶意代码攻击的技术措施或主动免疫可信验证机制及时识别入侵和病毒行为,并将其有效阻断。	3
	可信验证	可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证,**并在应用程序的关键执行环节进行动态可信验证,**在检测到其可信性受到破坏后进行报警,并将验证结果形成审计记录送至安全管理中心	3
	数据完整性	应采用校验技术保证重要数据在传输过程中的完整性。	2

		b)应采用校验技术或密码技术保证重要数据在存储过程中的完整性,包括但不限于鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等	3
	数据保密性	b)应采用密码技术保证重要数据在存储过程中的保密性,包括但不限于鉴别数据、重要业务数据和重要个人信息等。	3

2.2.2. 网上银行系统信息安全通用规范

2020 年中国人民银行对《网上银行系统信息安全通用规范》进行了修订，此标准既可作为各单位网上银行系统建设、改造升级以及开展安全检查、内部审计的安全性依据，也可作为行业主管部门、专业检测机构进行检查、检测及认证的依据。

其中服务器安全的安全计算环境规范提到了以下要求：

访问控制要求：

1）应实现操作系统和数据库系统特权用户的权限分离，系统管理员只具备操作系统的运维管理权限，数据库管理员只具备数据库的运维管理权限。

2）应根据业务必需和最小权限原则，对主机系统的访问控制规则进行精细化配置

入侵防范要求：

应采取技术手段对攻击活动进行检测和报警，例如，文件完整性监控、主机型入侵检测、 进程白名单、父子进程关联检测、攻击脚本检测等。

Web 应用安全要求：

1）应对网上银行系统 Web 服务器设置严格的目录访问权限，防止未授权访问。

2)应采取网站页面防篡改措施,应具备对 Web 后门进行检测和报警的能力。

数据库服务安全要求：

应采用技术手段对异常连接和请求进行控制和审计。

2.2.3. 个人金融信息保护技术规范

个人金融信息是个人信息在金融领域围绕账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息等方面的扩展与细化，是金融业机构在提供金融产品和服务的过程中积累的重要基础数据，也是个人隐私的重要内容。个人金融信息一旦泄露，不但会直接侵害个人金融信息主体的合法权益、影响金融业机构的正常运营，甚至可能会带来系统性金融风险。

个人金融信息保护技术规范规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求。

个人金融信息生命周期指对个人金融信息进行收集、传输、存储、使用、删除、销毁等处理的整个过程，其中涉及到可信计算环境的要求如下：

传输阶段： 通过公共网络传输时，C2、C3 类别信息应使用加密通道或数据加密的方式进行传输，保障个人金融信息传输过程的安全；

存储阶段： C3 类别个人金融信息应采用加密措施确保数据存储的保密性。

使用阶段： 应部署信息防泄露监控工具，监控及报告个人金融信息的违规外发行为。

2.2.4. 金融数据安全数据生命周期安全规范

中国人民银行 2020 年发布的 JR/T 0223—2021《金融数据安全数据生命周期安全规范》对金融数据生命周期安全做了更详细的技术要求说明：

数据传输安全要求：

1）2 级及以上数据的对外传输，应事先经过审批授权并采取数据加密、安全传输通道或安全传输协议进行数据传输。

2）3 级及以上的数据内部传输，应采取数据加密、安全传输通道或安全传输协议进行数据传输。

存储安全要求：

1）应采取一定措施确保数据存储的完整性，存储 3 级及以上数据时，应采用密码技术、权限控制等技术措施保证数据完整性。

2）3 级数据的存储应采取加密等技术措施保证数据存储的保密性。

3）文件系统中存放含有 3 级及以上数据的文件，宜采用整个文件加密存储方式进行保护。

数据使用安全要求：

1）3 级及以上的数据导出应使用加密、脱敏等技术手段防止数据泄露，国家及行业主管部门另有规定的除外。

2）3 级及以上数据加工之前应进行数据安全评估，并采用加密、脱敏等技术措施，保证数据加工过程的数据安全性。

3）应通过安全运维管理平台或数据提取专用终端获取数据，专用终端应事先经过审批授权后方可开通，原则上不应涉及 4 级数据。

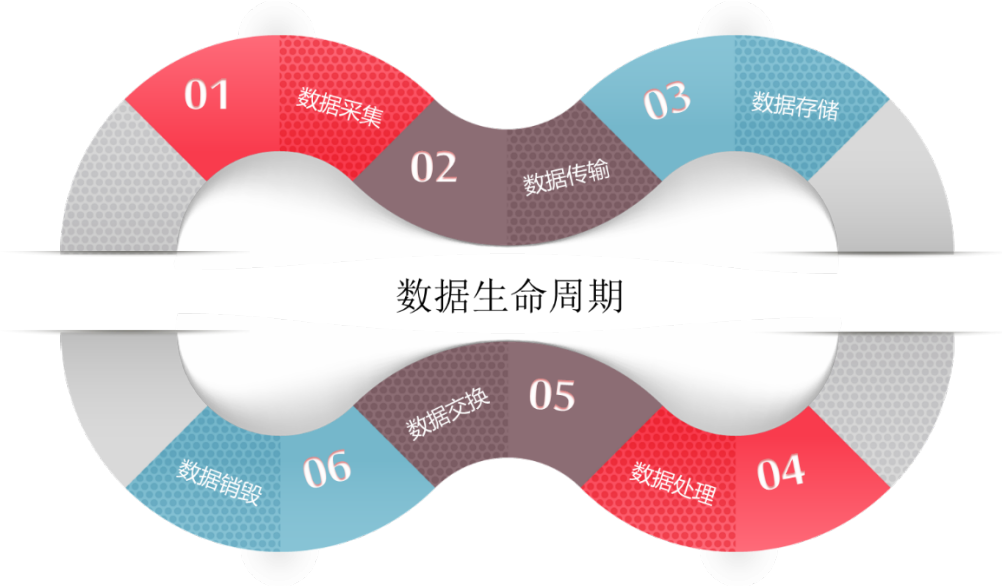
4）公开披露：通过金融业机构官方网站披露数据时，采取包括网页防篡改等技术措施，防范披露数据 篡改风险。

5）委托处理和数据共享：涉及 2 级、3 级数据的，应对数据进行加密处理，并采收数据标记、数据水印等技术，降低数据被泄露、误用、滥用的风险。

3.数据安全防护思路

依据数据的生命周期，参考 DSMM 数据安全能力成熟度模型，佰倬提出以内生安全、数据自保为核心，结合组织建设、制度流程、技术工具和人员能力四个领域的建设，帮助用户构建可信的数据安全计算环境。

3.1 数据生命周期



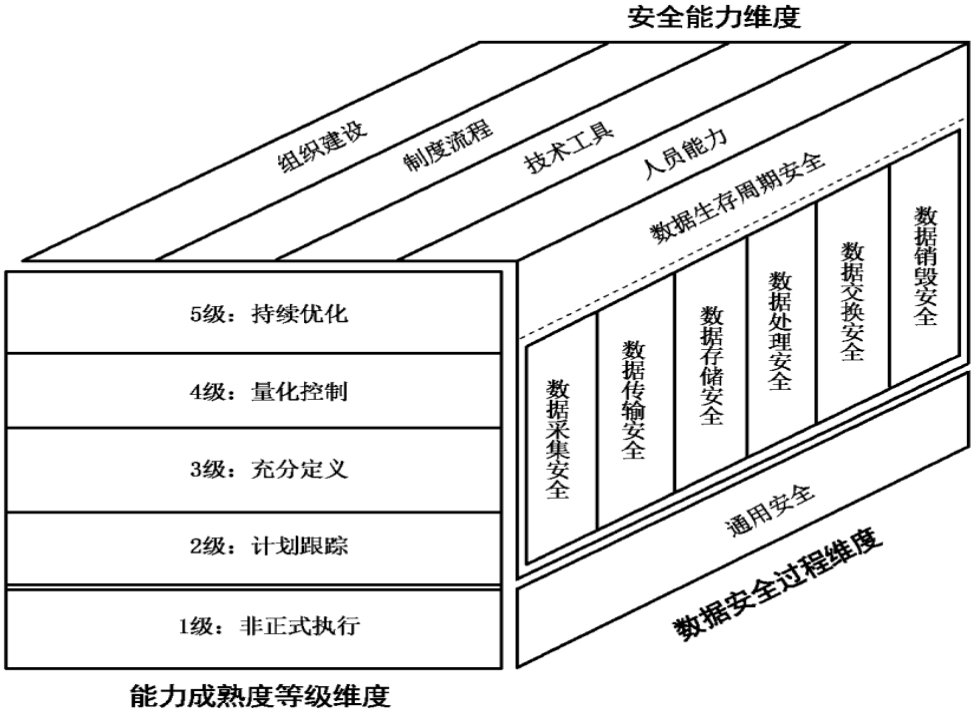
- 数据采集：指在组织机构内部系统中新生成数据，以及从外部收集数据的阶段。
- 数据传输：指数据在组织机构内部从一个实体通过网络流动到另一个实体的阶段。
- 数据存储：指数据以任何数字格式进行物理存储或云存储的阶段。
- 数据处理：指组织机构在内部针对数据进行计算、分析、可视化等操作的阶段。
- 数据交换：指数据由组织机构与外部组织机构及个人交互的阶段。
- 数据销毁：指通过对数据及数据的存储介质通过相应的操作手段，使数据彻底消除且无法通过任何手段恢复的过程。

特定的数据所经历的生命周期由实际的业务场景所决定，并非所有的数据都会完整的

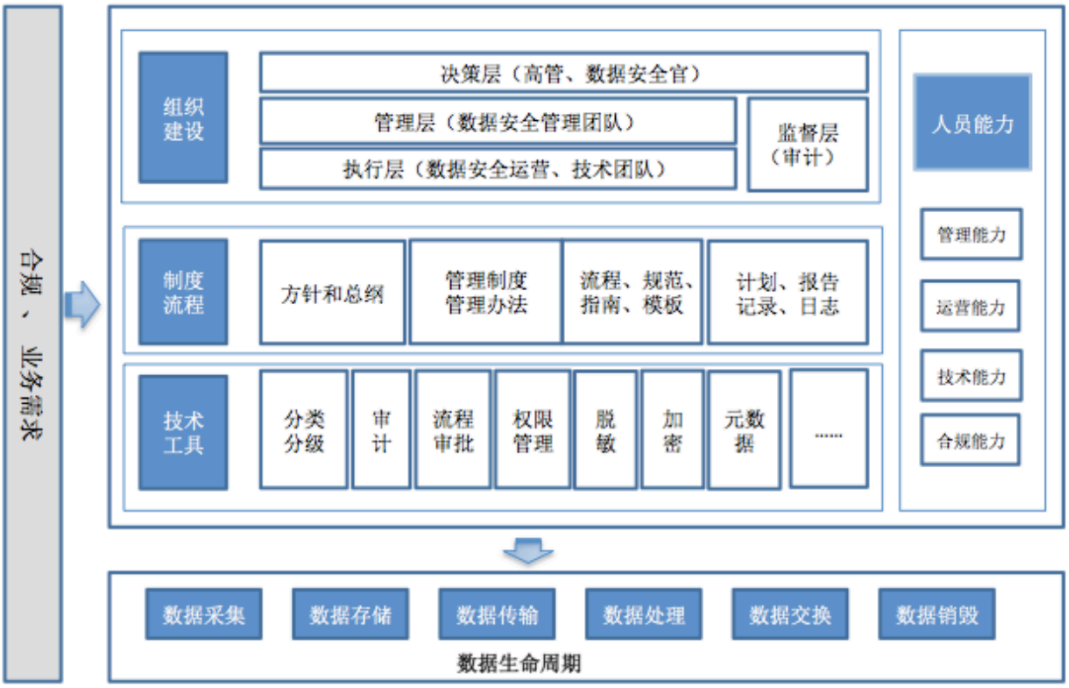
经历六个阶段。

3.2 数据安全成熟度模型（DSMM）

模型架构如下：



参考实施框架如下：



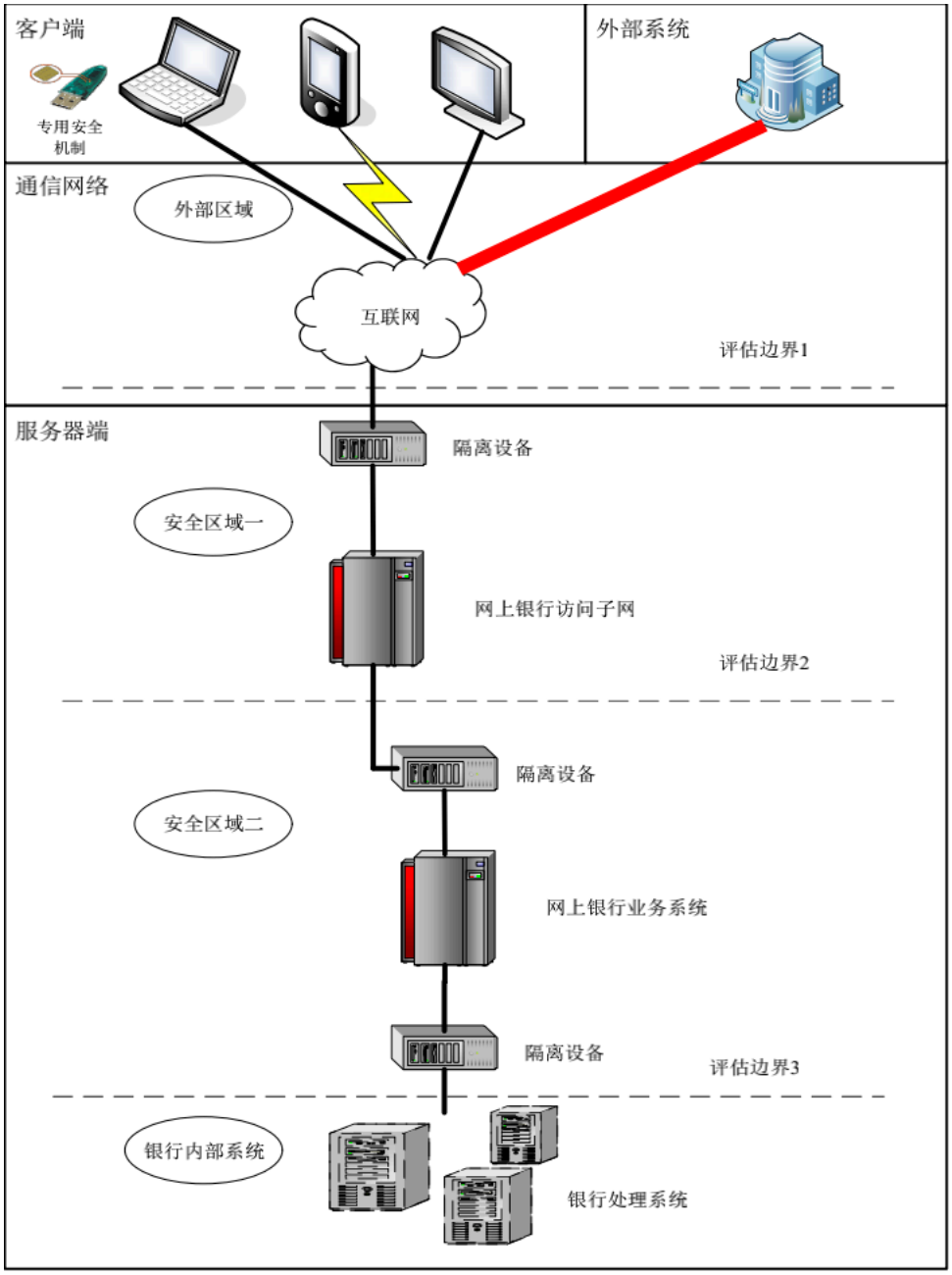
4.佰倬数据安全解决方案

随着互联网的快速发展，传统的银行业务大部分均可以通过银行的网上银行系统来办理，由于互联网环境的复杂性，网上银行系统同样面临着相对较大的数据安全风险

4.1 网上银行系统架构及数据分析

网上银行系统将传统的银行业务同互联网等资源和技术进行融合，将传统的柜台通过互联网、移动通信网络、其他开放性公众网络或专用网络向客户进行延伸，是商业银行等银行业金融机构在网络经济的环境下，开拓新业务、方便客户操作、改善服务质量、推动生产关系等变革的重要举措，提高了商业银行等银行业金融机构的社会效益和经济效益。网上银行系统主要包括通过 PC、手机、平板电脑、智能电视、可穿戴设备等终端访问的网上银行系统，例如，手机银行、微信银行、直销银行、银企直联、小微企业银行等系统。网上银行系统涵盖个人网银系统和企业网银系统。

网上银行系统主要由客户端、通信网络和服务器端组成，并可通过不同类型的通信网络连接到外部系统，开展各类合作业务，其中服务器端包括网上银行访问子网、网上银行业务系统、中间隔离设备和银行处理系统等，如下图所示：



注 1：外部区域：网上银行的用户或外部机构，利用网上银行客户端，通过互联网、移动通信网络、其他开放性公众或专用网络访问网上银行业务系统；

注 2：安全区域一：网上银行访问子网，提供基于 WEB、客户端的访问或跳转服务；

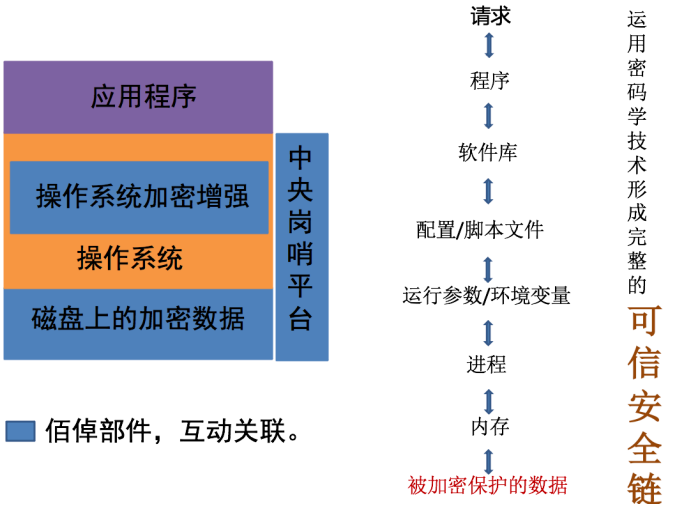
注 3：安全区域二：网上银行业务系统，主要进行网上银行的业务处理；

注 4：银行内部系统：银行处理系统，主要进行银行内部的数据处理；

注 5：隔离设备：不限于硬件或软件等具体形态，主要起到隔离不同安全区域的作用。

4.2 数据安全技术解决方案

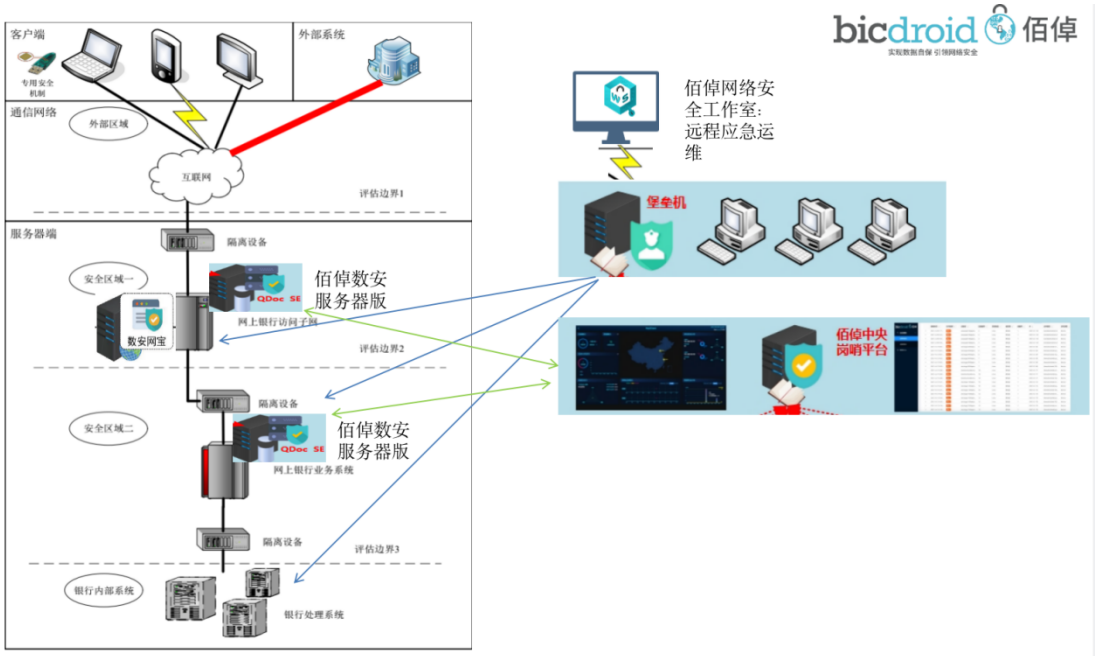
佰倬信息数安解决方案提供“以数据为中心，以数据流动为线索”的数据自保，通过“后量子密钥管理”和“强制访问控制”的智能集成，实现数据自保，使服务器和终端数据能够抵御勒索软件、恶意软件、内鬼等已知未知威胁而带来的数据安全问题。



实现原理图如上图所示，通过独特的技术有效的运用密码学形成从程序、程序软件库、相关的程序配置、程序运行脚本、程序运行环境变量和参数到进程，进程到被保护数据的可信安全链，做到授权的进程才可以访问被保护的数据。

对于任何一个企业的应用环境中，不管是前端应用服务器或是中间件服务器还是数据库服务器都可以被佰倬的数据安全产品进行保护。无需要应用层对佰倬的产品进行适配，实现对应用层的透明加解密，实现数据文件的存储级加密。佰倬的数据安全产品默认使用国密算法（SM4），并已经获得国家密码管理局颁发的《商用密码产品认证》，同时佰倬的数据安全产品目前除了支持通用的操作系统(Linux 系列、Windows 系列)之外，还可以支持麒麟、统信、深度、普华等国产主流操作系统，完全符合国家要求。

整体部署架构如下：



1）在 DMZ 区域（上图的安全区域一）的应用服务器、中间件服务器部署佰倬数安网宝，对网上银行系统的前端展示页面做网页防篡改保护，基于文件系统内核层的强访问控制技术，对 Web 站点目录提供全方位的安全防护，防止网页内容被黑客、系统漏洞、木马以及后门等已知或未知的攻击非法篡改和破坏。

2）在 DMZ 区域（上图的安全区域一）的应用服务器、中间件服务器，以及在业务区（上图的安全区域二）部署佰倬数安服务器版，对服务器上的数据文件和数据库进行保护，可以做到防数据被窃取、防数据被勒索软件加密、防恶意内部人员泄露、防根用户攻击。

3）在运维管理区部署佰倬数安的中央岗哨平台，可以对各个服务器的岗哨进行远程安装、配置、和管理。同时，中央岗哨平台可以大屏展示被保护服务器的数据访问记录，包括目标数据，来访进程的路径信息，来访的时间，访问的结果（允许或拒接）等在内的岗哨记录，以及包括 CPU 占比，内存占比，磁盘占比等在内的系统运行状态信息实时汇总到中央岗哨平台，进行归一化处理加工，实现实时监察和全面审计。

4）另外，在做远程应急维护或者系统开发时，银行通常会使用到 SSLVPN 和 VDI

系统，但是对使用 VPN 的终端的自身安全情况无法进行管控，同时行方要分别采购 VPN 和 VDI 系统，并配备相应的运维管理人员，增加了设备和人员成本；使用佰倬数安的网络安全工作室（QWS），可以轻松解决以上问题。佰倬网络安全工作室在个人电脑或者单位提供的受控终端上，创建完全隔离的虚拟安全工作环境，虚拟环境中集成了 VPN 连接器，通过 VPN 可以访问单位内部允许访问的应用系统、运维管理系统等，从而解决远程办公的数据安全的问题，同时实现的员工能够用个人电脑随身、随地、线上、线下为企业安全办公，保障企业对企业数据的全程掌控。

方案具备以下特点：

- **低资源消耗**

被保护数据为数据库时，数据自保软件的内核模块对数据库吞吐量的影响要低于 5%。

- **强制访问控制和加密（可选项）智能相结合**

对需要保护的数据进行自动加密保护，基于进程指纹信息和加密数据的保护标识，建立岗哨白名单，在系统驱动层设置安全岗哨，只授权合法进程访问被加密保护的数据，拒绝非法进程访问被加密保护的数据。即使非法或恶意内部人员将强制访问控制强行关掉，数据仍一直保持被加密状态，无明文泄漏。

- **操作系统内核层的文件系统数据透明加密与数据访问控制紧密结合**

在操作系统内核层的文件系统中实现数据加密，此加密机制对合法进程透明，即加密机制不改变合法进程对数据的访问方式。同时，文件系统使用强制访问的授权判定信息决定是否对数据进行加解密，从而保证在系统漏洞/系统后门被利用时数据仍不会泄露。

- **零知识数据保护**

作为数据保护服务的提供者，不收集关于用户的网络、系统和数据的任何信息。在提供服务的同时对用户的网络、系统和数据一直保有零知识。

- **数据防泄漏、防破坏**

能够保证在非易失性存储介质(如服务器硬盘)由于种种可能而脱离数据保护系统控制后，所存储的数据内容仍然安全而不会被窃取或泄露。

- **抵御已知未知的外来恶意软件攻击(防勒索软件对数据的窃取、破坏等)**

能够做到服务器系统对恶意软件的性质种类毫不知情的情况下，保护数据不被窃取、破坏、劫持及勒索。被保护数据免疫已知和未知威胁，可抵御已知和未知的外来恶意攻击，不惧怕系统漏洞和后门，防勒索、破坏、和泄漏。

- **抵御内部人员对数据的蓄意窃取(防内鬼)**

支持禁止操作系统用户及系统管理员使用未授权程序对被保护数据文件进行复制、移动、删除、或修改，防内部攻击。

- **用户对加解密过程无感知**

运行在操作系统的内核层，用户无需关注加解密的过程。

- **对系统计算性能进行实时监测**

安全岗哨对系统的关键计算性能指标实时做出完整的记录，并上传至中央岗哨平台。

- **对软件自身的运行情况的监察**

对软件自身的运行情况和工作状态做出完整的记录，从而保证整体系统的安全性。

- **边缘安全自保与中央管控监察的完美结合**

各个服务器上的安全岗哨自动与数安岗哨平台连接，将岗哨记录和系统性能实时汇总到数安岗哨平台。

- **满足合规要求**

通过强访问控制和加密智能结合技术，可以帮助行方满足安全合规要求：

满足等保 2.0 可信计算环境的访问控制、数据保密性、数据完整、恶意代码防范和可信验证方面的要求；

满足《网上银行系统信息安全通用规范》中对服务器数据访问的最小权限原则和放数据篡改的安全的要求；

满足《个人金融信息保护技术规范》和《金融数据安全数据生命周期安全规范》对数据生命周期的传输、存储和处理阶段的防泄漏、防篡改、数据完整性和机密性的安全技术要求。

4.3 数据安全管理

安全三分靠技术，七分靠管理，只靠防护技术无法完全保证数据的安全，还要配合相应的数据安全管理制度和数据安全组织的建设。

4.3.1. 数据安全管理制度与规范

安全制度和规范是对过往经验的高度总结，同时也是对未来潜在隐患的前瞻性思考。企业需在数据安全管理规范上以国家相关法律法规为指导，结合企业的实际安全管理情况，制定相应的数据管理规范和细则，严格按照规章制度和工作规范办事，从而构建起完善的数据安全管理体系框架。

通过制度和规范建设，实现对员工在日常数据生产行为上的指导性和约束

性，在思想态度上的鞭策性和激励性；在流程上的规范性和程序性；在岗位责任上的法制化，以及管理上的科学化。要根据数据安全面临的新情况、新问题，紧密联系企业数据安全工作的实际，本着“堵漏、补缺、管理”的原则，完善数据安全工作的各项规章制度及操作规程，切实增强制度的可操作性，为企业的工作和活动提供可供遵循的依据。同时，应采取适当的监督检查手段来贯彻落实各项数据安全规章制度。

4.3.1.1. 数据安全管理制度制定

- 制定数据安全工作的总体方针、政策性文件和安全策略等，说明机构安全工作的总体目标、范围、方针、原则、责任等；
- 对数据安全相关的管理内容建立数据安全管理制度，以规范数据安全管理活动，约束人员的行为方式；
- 对要求管理人员或操作人员执行的日常管理操作，建立操作规程，以规范操作行为，防止操作失误；
- 形成由安全政策、安全策略、管理制度、操作规程等构成的全面的数据安全管理制度体系；
- 由数据安全组织定期如召集相关部门和相关人员对数据安全管理制度体系的合理性和适用性进行审定。在数据安全领导小组的负责下，组织相关人员制定；
- 保证数据安全管理制度具有统一的格式风格，并进行版本控制；
- 组织相关人员对制定的数据安全管理制度进行论证和审定；
- 数据安全管理制度应经过管理层签发后按照一定的程序以文件形式发布；
- 数据安全管理制度应注明发布范围，并对收发文进行登记；
- 定期对数据安全管理制度进行评审和修订，对存在不足或需要改进的制度进行修订；
- 当发生重大数据安全事件时，应对数据安全管理制度进行检查、审定和修订；
- 每个制度文档应有相应负责人或负责部门，负责对明确需要修订的制度文档的维护；

4.3.2. 数据安全组织及人员管理

数据安全组织管理是信息安全体系建设的一个前提条件，对数据安全工作的保障至关重要。

通过建立专门的数据安全组织机构，健全信息安全组织体系，以便能够切实落实数据安全管理责任制，明确数据安全治理的政策、落实和监督由谁来长期负责，以确保数据安全相关工作能够长期持续的得以执行，为数据安全提供有力的组织支撑。

数据安全人员管理应作为安全管理的重中之重。数据安全组织的成员应由数据的利益相关者和专家构成，要覆盖到安全、业务、运维等多个部门。这里之所以称之为利益相关者，是因为这些人不仅仅是数据的使用者，可能是数据本身的代表者（比如用户），数据的所有者，数据的责任人。

数据安全组织中另一个关键角色就是数据安全的受众，这些受众是数据安全策略、规范和流程的执行者和被管理者；包括了数据的使用者、管理者、维护者、分发者；大多数数据利益相关者都属于数据安全治理的受众；将这些人员纳入到这个组织中，才能够使数据安全治理过程中制订的安全原则、安全措施和安全规范在具体执行中被有效地贯彻落地。

只有有效地构建一个涵盖业务、管理、安全、执行等部门的数据安全组织机构，才能做到业务和安全的有效平衡。

另外，企业可以通过与接触重要或敏感数据的人员签订相应的安全保密协议，确保员工保护好公司数据安全义务，以便在数据泄密事件发生后，能够通过法律手段对数据泄露事件追责。

应对企业员工进行安全培训，让员工增强安全意识，否则在某些情况下将会无意泄露公司数据。