.

向日葵创新软件产品评估

上海贝锐信息科技股份有限公司

2019-8-16

目 录

[向日葵创新软件产品评估 1](#_Toc18339427)

[1. 产品创新性（1000） 2](#_Toc18339428)

[1.1. 产品新颖性 2](#_Toc18339429)

[1.2. 应用创新 3](#_Toc18339430)

[1.3. 市场创新 4](#_Toc18339431)

[2. 软件安全（1000） 4](#_Toc18339432)

[3. 软件可靠性（1000） 5](#_Toc18339433)

# 产品创新性（1000）

## 产品新颖性

软件产品具备新颖性，具有国际、国内首创的产品特点，拥有自主知识产权，已申请相关的专利和软件著作权，并通过软件产品评估及软件产品检测

国际/国内首创的产品特点：

向日葵远程控制软件，由贝锐科技独立自主研发，采用自主研发的视频压缩、解码技术以及安全的数据传输协议；具有以下：安全、高效、稳定、国内首创跨多平台远控特点；①基于RSA/AES非对称加密技术，保护用户资料，远程会话安全；②配置华东、华南、华北BGP跨线路云服务器保证高效稳定，以及H264智能视频模式，远程流畅；③支持的平台包括：Windows、Linux、iOS、Android、Mac。

软件具备多个国内首创功能：远程控制手机摄像头，远程观看手机桌面，远程管理电脑，消息群发以及文件分发等，提高了企业及个人用户工作效率。其外，向日葵还首创软硬结合远控模式，可远程开关机无人值守设备。

向日葵远程控制软件通过《ISO9001质量管理体系认证》、《计算机安全产品销售许可证》，软件具备可测试性、可用性、兼容性、可靠性、安全性等，拥有12项产品专利，及158个软件著作权

（专利和软著找黄双燕）

已申请的专利举例：

|  |  |  |
| --- | --- | --- |
| 专利号 | 专利名称 | 申请人 |
| 201821812388.5（发文序号：201906252155290） | 一种远程操控中转卡 | 上海贝锐信息科技股份有限公司 |
| ZL 2015 1 0843772.6 | 客户端批量远程控制方法及系统 | 上海贝锐信息科技股份有限公司 |

已申请的软著举例：

|  |  |
| --- | --- |
| 软件名称 | 登记号 |
| 贝锐向日葵开机棒嵌入式软件v1.0 | 2014SR12569 |
| 软件名称：向日葵远程控制客户端软件v7.0 | 2014SR125706 |
| 贝锐向日葵开机棒嵌入式软件v1.0 | 2014SR125690 |
| 向日葵远程控制Android版软件v3.1 | 2015SR100378 |
| 向日葵远程控制iOS版软件v3.3 | 2015SR100334 |
| 向日葵远程控制iOS版软件v3.3 | 2015SR100334 |
| 向日葵远程控制客户端软件v7.5 | 2015SR100617 |
| 向日葵远程控制移动客户端软件v1.0 | 2015SR130871 |
| 向日葵远程控制iOS软件v5.0 | 2016SR151031 |
| 向日葵远程控制iOS软件v5.0 | 2016SR151031 |
| 向日葵远程控制iOS软件v5.0 | 2016SR151031 |
| 贝锐向日葵远程控制Windows客户端软件v9.0 | 2017SR129579 |
| 贝锐向日葵远程控制iOS版软件v7.0 | 2017SR185995 |
| 贝锐向日葵远程控制Windows版客户端软件v10.0 | 2018SR631123 |
| 贝锐向日葵远程控制iOS版软件v11.0 | 2018SR606644 |
| 向日葵远程控制客户端软件v9.0 | 2018SR643684 |

通过的软件产品评估和产品检测举例：

|  |  |  |  |
| --- | --- | --- | --- |
| 证书 | 产品名称 | 认证机关 | 单位 |
| 《计算机安全产品销售许可证》 | 向日葵客户端7.2/主控端2.3 | 公安部计算机信息系统安全产品质量监督检验中心 | 上海贝锐信息科技股份有限公司 |

## 应用创新

软件产品开创了新的应用模式或应用领域，提出并实现了创新型的解决方案

开创新的应用模式/应用领域：

向日葵远程控制软件，致力于新兴领域发展：智慧政务、智慧医疗、智慧教育、工业4.0、IT互联网、零售行业、电竞游戏；给这些领域带来新的生产运作方式，提高发展效率

智慧政务：向日葵远协办公、远程会议等功能模为政府打造高效的远程办公环境，提高各部门高效沟通。

智慧医疗：远程医疗的实现也得到大家的重视。远程医疗通过远程技术，实现医生与医生之间、医生与患者之间、医生与医疗设备之间的远程连接，可以引用在远程病情诊断、远程学术培训、远程维护医疗设备等方向

智慧教育：老师可通过远程教学方式，给不同地区的学生同时授课，大大提高了师资资源的利用率，及知识传播的便捷性。节省了师生双方的沟通成本

工业4.0：远程控制、远程管理、远程运维，对于提升生成力与控制管理成本起到很大的帮助，是制造业转型的重要工具

IT互联网：好的IT资源管理、高效的办公环境，能大大的节省企业日常运营成本，从而提高行业竞争力。远程控制解决方案，远程管理IT设备资源、高效的远程会议模式，是提升竞争力的首要选择

零售行业：借助信息化的力量，提高远程连接提升各分区门店与总部财务数据间交互的效率与安全性，更能有效控制系统运维的成本

电竞游戏：为游戏工作室打造智能监控管理系统，保证工作室电脑正常运行，定期远程维护设备

创新型的解决方案：

基于远程控制核心解决功能，向日葵在“远程办公”、“远程运维”、“远程客服”、“远程会议”、“无人值守设备”等场景，提供更优更有效的解决方案

1、连锁门店运维解决方案：

①各连锁门店在收银系统主机上安装向日葵客户端软件，总部主机即可统一管理并随时远程查看主机桌面状态

②使用远程桌面功能，随时随地远程各门店主机，进行系统升级维护

③使用云监控功能，监控各连锁门店收银主机操作

④使用桌面录像功能，将个门店操作记录保存到云服务器

2、企业协同办公解决方案

①企业自建服务器专网部署

②协同办公系统中嵌入向日葵远程协助及远程文件

③使用此平台的双方在沟通的同时快速发起远程协助，解决所遇到的工作难题

3、户外广告机等无人值守设备解决方案

①选择向日葵独立服务器，在无人值守的联网广告机安卓向日葵客户端

②后台使用控制端，对显示终端进行一对多控制

③管理广告机文件，更换广告内容，可包括视频、文字、图片等信息

## 市场创新

软件产品具备一定的市场规模或者开拓了新的市场，且具有良好的市场前景

产品的市场规模：

1、向日葵远程控制软件现状：2019年，向日葵个人用户量3000万，装机量1.2亿，企业用户5万，每天支撑起5000万次远程连接，帮助用户远程解决问题，围绕节省人力资源，开拓了新的市场，提高了中小企业的经营效率，减少企业生产成本。

2、远程控制需求预测：由于人力成本越来越高，用最少的人力解决问题，已经成为企业在同行中的竞争力，远程控制技术的成熟，让远程资源更容易获得，解决了资源稀缺性问题，并且远程控制可拓展于大量新兴或者传统企业的日常远程办公、远程运维、远程售后中，结合向日葵已有增长数据，可预测未来向日葵远程控制软件用户量、装机量还将持续增长，市场前景良好。

# 软件安全（1000）

指：软件在受到恶意攻击的情形下，依然能够继续争取的运行及确保软件被在授权范围内合法使用的思想

<https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6%E5%AE%89%E5%85%A8>

软件产品在设备安全、网络安全、数据安全方面采用了相应的措施来保障信息安全

向日葵远程控制软件在设备安全、网络安全、数据安全方面采取多种有效技术及防范措施，主要着力于构建高效的安全防护体系

1、安全系统的主要构成一般包括证书业务服务系统、证书查询验证服务系统、密钥管理系统、密码服务系统、授权管理服务系统、可信时间戳服务系统、网络信息域系统、基本安全防护系统等

2、基本安全防护一般采用防火墙、入侵检测、漏洞扫描、安全审计、病毒防治、Web信息防篡改、物理安全等基础安全技术，以保障应用系统的安全，针对不同的安全技术；针对基本安全防护部署完成后，对每个技术点进行测试，已保证安全性。

3、向日葵软件通过安全防护策略帮助软件系统及设备对抗攻击，包括以下几方面：

    ①安全日志：记录非法用户的登录名称、操作时间及内容等信息，以便于发现问题并提出解决措施

     ②漏洞扫描就是对软件系统及网络系统进行与安全相关的检测，以找出安全隐患和可被黑客利用的漏洞，同时漏洞扫描技术也是安全性测试的一项必要手段。

     ③隔离防护是将系统中的安全部分与非安全部分进行隔离的措施

4、保证网络安全的措施：通过安全审查的网络可信接入设备和网络信任域管理系统组成网络信任域，以保证系统之间数据通信和会话访问稳定及不被非法侵犯，并进行如下测试：

①系统是否具备接入认证交换机，确保只有合法的才能接入网络；

②是否具备网络信任域管理系统，进行网络接入管理配置；

针对网络稳定性能的测试包括以下方面：

①测试认证时间是否小于1秒或用户的需求水平；

②测试接入认证并发数是否满足用户需求；

③验证接入认证交换机是否提供与客户端通信遵循IEEE 802.1X接口，传输IEEE 802.1X认证数据包；

5、保证数据安全的措施：针对数据安全，向日葵软件采用先进的数据传输加密机制，通信加密时保证数据在传输过程中数据的保密性和一致性的测试，在技术上通常使用链路加密、数据加密的方式进行，目前使用的加密技术包括VPN技术、对称加密算法、非对称加密算法、Hash算法，另外采用自主研发的密码函数，作为加密、解密、保证数据完整性、鉴别交换、口令存储与检验等的一部分，借以达到保密和鉴别的目的。密码技术能够提供或是有助于提供相关保护，以防止消息流的观察和篡改，通信业务流分析、抵赖、伪造、非授权连接、篡改消息等行为的出现，主要用于密码的保护、数据的传输过程中的安全防护、数据存储过程的安全防护；由于向日葵跨越多个平台，对于每个平台，不同加密机制或密码函数的用途、强度是不相同的，一个软件或系统的加密机制使用得是否合理，强度是否满足当前需求，强度是不相同的。所以，向日葵软件是通过模拟解密是测试来验证软件系统中的加密机制使用是否合理，强度是否满足当前需求。

针对向日葵数据库权限的测试包括以下方面：

①应用软件部署后，数据库管理用户的设置应当注意对账号的保护，超级用户的口令不得为空或默认口令。对数据库的账号和组的权限作相应设置，如锁定一些默认的数据库用户；撤销不必要的权限。

②数据库中关于应用软件用户权限和口令存储的相关表格，尽量采用加密算法进行加密。

# 软件可靠性（1000）

指：软件产品在规定的条件下和规定的时间区间完成规定功能的能力

<https://baike.baidu.com/item/%E8%BD%AF%E4%BB%B6%E5%8F%AF%E9%9D%A0%E6%80%A7>

软件产品采用了充分的手段（功能即性能测试）来保证软件的可靠，可用

向日葵远程控制软件通过大量的可靠性测试保证软件产品运行的可靠性，主要围绕黑盒测试和白盒测试展开：

一、黑盒测试：通过大量的测试用例、及自动化测试脚本对软件的功能进行可操作性、稳定性测试，保证软件在正常或非正常情况下都能安全运行

功能验证，依靠大量的测试用例，对涉及安全的软件功能，如：用户管理模块、权限管理模块、加密系统、认证系统、远控连接流程、远程管理体系等进行测试，主要是验证上述功能是否有效。

自动化漏洞扫描（自动化压力测试）：借助于特定的漏洞扫描器完成的，漏洞扫描器是一种自动检测远程或本地安全性弱点的程序，通过使用漏洞扫描器，系统管理员能够发现所维护信息系统存在的安全漏洞，及时修补漏洞。 按常规标准，可以将漏洞扫描器分为两种类型：主机漏洞扫描器和网络漏洞扫描器。主机漏洞扫描器是指在系统本地运行检测系统漏洞的程序。网络漏洞扫描器是指基于网络远程检测目标网络和主机系统漏洞的程序，

二、白盒测试：深入到代码架构，分析数据走向，保证每一步程序的正确性，主要依靠静态安全扫描测试和动态安全扫描测试。

软件安全静态扫描在代码的开发期间进行。此过程借助威胁建模和分析，对静态代码进行扫描，从而发现安全漏洞。软件安全动态扫描是对工作环境中的实际代码进行的扫描，它在代码运行期间查找漏洞。还有第三类软件安全测试，即人工渗透测试，它主要通过白帽分析进行人为干预。真正有效的应用程序安全项目利用所有的软件安全扫描测试。

三、其外，为了进一步尽早发现软件安全性问题，向日葵软件还进行模拟攻击测试：尽早发现可知故障，并做好防护措施，在故障发生时，安排软件处理异常。通过模拟攻击测试来验证软件或信息系统的安全防护能力，测试点包括以下几方面：

1、冒充：就是一个实体假装成一个不同的实体，冒充常与某些别的主动攻击形式一起使用，特别是消息的重演与篡改

2、重演：当一个消息或部分消息为了产生非授权效果而被重复时，出现重演

3、消息篡改：数据所传送的内容被改变而未被发觉，并导致非授权后果

4、服务拒绝：当一个实体不能执行它的正常功能，或它的动作妨碍了别的实体执行它们的正常功能的时候，便发生服务拒绝。这种攻击可能是一般性的，比如一个实体抑制所有的消息

5、内部攻击：当系统的合法用户以非故意或非授权方式进行动作时就成为内部攻击。多数已知的计算机犯罪都和使系统安全遭受损害的内部攻击有密切的关系。

6、外部攻击：外部攻击可以使用的方法有：搭线（主动的与被动的）、截取辐射、冒充为系统的授权用户，冒充为系统的组成部分、为鉴别或访问控制机制设置旁路。

7、陷阱门：当系统的实体收到改变，致使一个攻击者能对命令或对预定的事件或事件序列产生非授权的影响时，其结果就称为陷阱门。例如，口令的有效性可能被修改，使得除了其正常效力之外也使攻击者的口令生效。