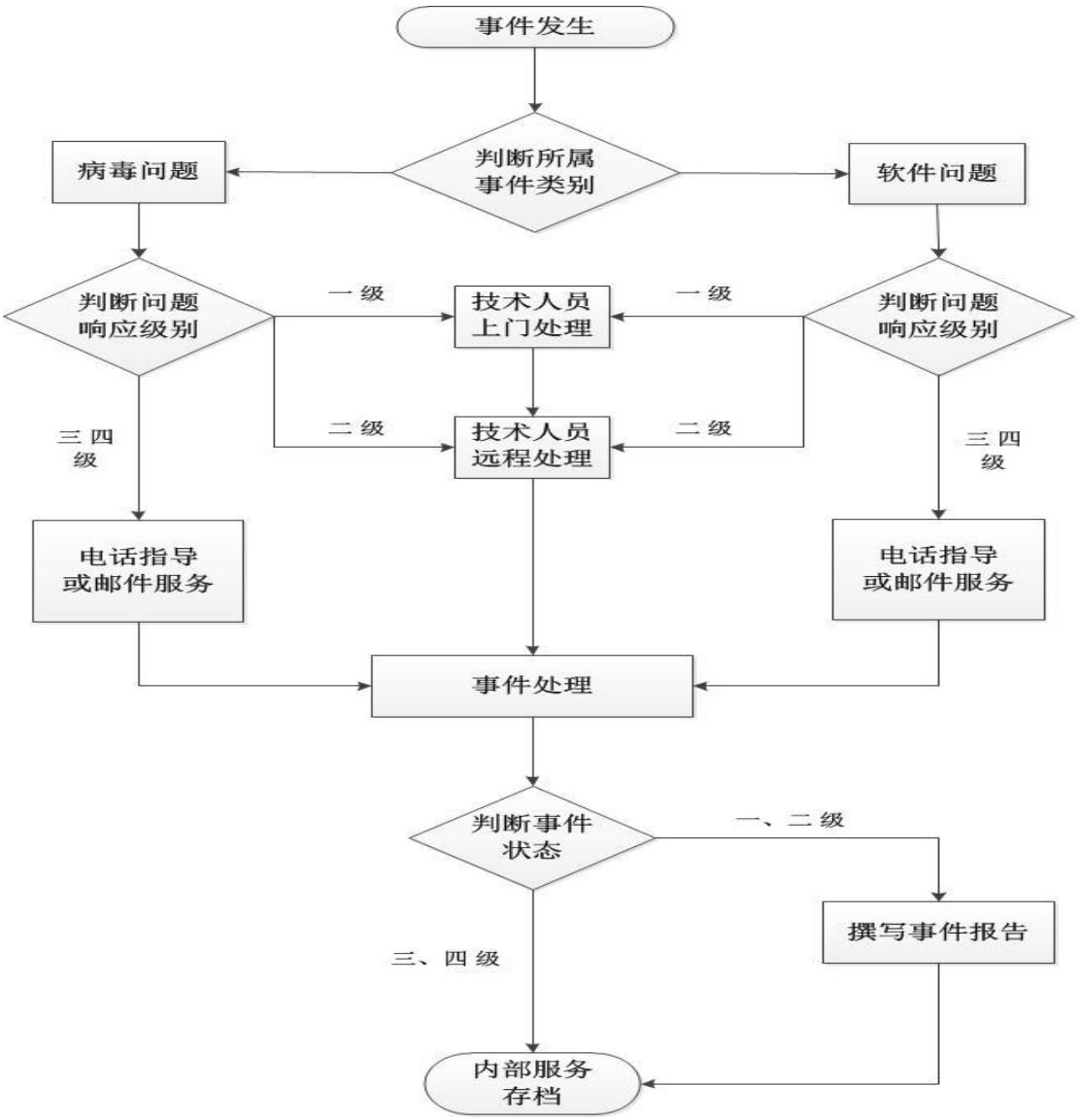
企业级产品应急服务

一、 服务概述

在产品使用过程中遇到任何与瑞星产品或计算机病毒相关等问题时，可迅速根据具体事件级别启动响应的应急响应预案，并由应急响应实施小组人员根据事件级别通过相应方式进行解决。如遇无法解决问题时或无法预知问题时，由应急响应实施小组组长收集相关问题并上报至瑞星公司，由瑞星公司组成的专家应急小组对相关问题进行及时处理，并提供一套适合的解决方案。

1) 应急响应流程图



2) 应急响应级别判定标准

应急响应级别	应急响应级别判定标准	应急响应时间
一级响应	由计算机病毒或瑞星网络版产品问题引起，严重影响计算机系统或网络无法正常使用等相关问题。	北京地区：1-3 小时抵达现场 其他地区：需根据情况协调

二级响应	由计算机病毒或瑞星网络版产品问题引起，但并不影响计算机系统或网络正常运行等相关问题。	全国各地区：即时响应 内网环境，可根据事件具体情况，协调上门
三级响应	对于计算机病毒无法处理或瑞星网络版产品功能无法正常使用等相关问题。	全国各地区：即时响应 （通过电话或邮件服务） 特殊问题可通过远程解决
四级响应	对于瑞星网络版产品使用上存在问题，导致的病毒无法处理，瑞星网络版产品无法升级的相关问题。	全国各地区：即时响应 （通过电话或邮件服务） 特殊问题可通过远程解决
其他	对于数据恢复、企业网站挂马处理或特殊项目需要瑞星提供信息安全支持等相关问题。	全国各地区：即时响应 针对事件具体情况判断，启动相应级别应急响应流程。

对于在应急响应过程中，如果发现是由于第三方厂商软件导致瑞星杀毒软件无法正常工作（如：瑞星系统中心无法正常升级、服务器死机、系统崩溃、病毒无法查杀或网络异常等情况），瑞星公司会提出相应修改方案或解决此问题的相关建议，由企业内部自行联系第三方软件公司解决，瑞星公司可配合第三方软件公司针对具体问题进行沟通处理。

如是由于第三方软件公司所属软件引起造成的瑞星软件工作异常所导致的问题，瑞星公司对于在此期间产生的任何损失不承担任何责任。

3) 应急响应具体服务内容

应急响应服务具体分为现场紧急救援、远程紧急救援、数据灾难恢复和网站挂马应急处理四部分，具体服务内容如下：

1. 现场紧急救援服务

1) 服务概述

现场紧急救援服务为应急响应最高级别服务，主要针对在发生突发性问题（如：病毒、网络和瑞星产品等问题）时提供及时现场技术支持，为用户提供解决方案并协助解决问题。

2) 服务响应时间

a) 应急响应区域时间

北京地区：根据路程 1-3 小时内抵达现场。

其他地区：根据具体情况确定时间或更换远程紧急救援服务。

b) 特殊问题响应时间

- **病毒误报：**

  自瑞星公司获取到误报样本时间起，根据具体误报情况最快 2 小时，最慢不超过 12 小时内解决。

- **病毒无法彻底清除：**

  优先由现场瑞星应急工程师手动清除病毒，并自瑞星公司获取到可疑样本时间起，根据病毒具体情况 24-48 小时内通过升级彻底解决。

  对特殊病毒如需要涉及较长时间更改瑞星软件功能或架构等问题，由瑞星应急工程师在 24 小时内通过电话回访或邮件服务方式告知用户，并提供临时解决方案，并负责定期告知用户相关问题处理进度直至彻底解决。

注意：无法清除病毒仅包含瑞星无法查杀病毒或清除失败类型病毒，不包含已知病毒或具备局域网传染特性病毒（如：蠕虫类型病毒、传染型木马病毒）。

- **软件冲突**

  自瑞星公司获取相关软件冲突有效信息起，由瑞星应急工程师在 24-72 小时内（包含测试时间）通过电话回访或邮件服务方式告知用户，并提供临时解决方案，并负责定期告知用户相关问题处理进度直至彻底解决。

3) 服务流程

针对突发性病毒事件或由病毒引起的相关问题，应急响应小组工程师服务流程如下：

a) 通过瑞星应急小组工程师现场具体分析瑞星系统中心日志定位报毒严重计算机 IP 或用户指定病毒影响严重计算机，初步了解具体病毒现象与病毒类型；

b) 对于出现可能由病毒引起的网络异常情况（如 ARP 病毒），优先使用抓包工具或用户内部网络审计软件定位发包源，并通过切断发包源计算机网络连接单独处理；

c) 针对具体病毒尝试优先升级使用瑞星最新版版杀毒软件是否可以正常查杀；

d) 如可以正常查杀，通过分析瑞星系统中心日志查看报毒严重计算机是否存在重复报毒情况，并通过分析病毒日志中的病毒感染路径确定是否为特殊路径报毒（如系统还原文件夹、移动存储介质或临时文件等）；

e) 如发现病毒查杀不干净或病毒总是重复出现等问题，由瑞星应急小组工程师现场通过使用相关病毒专杀工具或反病毒处理工具进行快速处理，并收集相关病毒关联样本，提供具体相关暂时规避方法，后期通过瑞星升级包统一升级解决；

f) 如发现瑞星无法清除病毒或可以破坏瑞星杀毒软件正常功能的病毒，由瑞星应急小组工程师现场通过反病毒处理工具优先处理，并收集相关可疑病毒样本，带回瑞星公司分析后，通过瑞星升级包解决；

g) 如大规模感染未知病毒并严重影响计算机系统正常使用情况下，通过分析瑞星应急小组工程师带回相关未知病毒样本，优先提供专杀工具解决，后期通过瑞星升级包统一升级解决；

h) 病毒清理完毕后，继续通过分析病毒日志查找可能存在的病毒感染安全隐患，并提供相应的整体预防病毒感染的解决方案；

i) 针对处理的病毒具体情况，协助用户调整瑞星系统中心整体客户端防病毒策略，预防病毒再此大规模爆发。

针对突发性瑞星软件问题导致的企业内部软件无法使用、瑞星系统中心客户端无法正常升级等问题，应急响应小组工程师服务流程如下：

a) 对于安装瑞星软件或升级瑞星软件后导致企业内部软件无法使用问题，通过现场定位导致问题的瑞星升级模块，提供相应临时解决方案，后期通过瑞星升级包统一升级解决；

b) 对于突然出现的瑞星系统中心和客户端无法正常升级问题，通过瑞星应急小组工程师现

场分析瑞星软件运行日志，分析判断可能造成的原因，并现场恢复处理瑞星软件相关异常问题；

c) 如遇软件冲突造成的蓝屏重启等问题，由瑞星应急小组工程师现场提取相关计算机系统或第三方软件可供分析判断定位问题的文件，需带回瑞星公司在特殊系统环境详细测试分析，以便于快速解决问题；

d) 瑞星软件恢复正常使用后，通过现场调整锁定瑞星系统中心、客户端升级或软件策略，预防此类事件再此发生；

e) 针对瑞星软件由于设置不当引起的其他类型特殊问题，可由瑞星应急小组工程师现场及时处理，并提供相应正确设置使用解决方案供用户参考。

4) 服务意义

通过瑞星应急小组工程师现场操作、现场分析、现场解决的技术支持方式，快速解决用户各种突发性网络安全事件，避免由于提供问题描述不准确、病毒处理方式不正确、无法提供有效分析日志、物理隔离内网环境等因素导致的问题解决时间较长的情况。并通过在此基础上构建的工程师专属电话通道，为企业在后期瑞星产品使用与病毒处理上提供快速响应与沟通机制，大幅提高了企业内部应对网络安全事件的及时应变处理能力。