ROAR PANDA
软 件 基 因®

邮件安全净化系统
产品白皮书

戎磐网络
SOFTWARE GENE

软件基因 -开启网络安全新视角

版权声明

免责条款

1、本文档是上海戎磐网络科技有限公司相关工作人员依据现有信息制作，在编写该文档时候已尽最大努力保证其内容准确可用，公司及其员工将不对本文档中任何内容直接或间接导致第三方的损失和损害承担任何责任;

2、本文档中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，对此可能产生的差异为正常现象，相关问题请直接咨询戎磐网络科技有限公司。

信息反馈

网址：http://www.roarpanda.com

地址：上海市长宁区娄山关路 55 号新虹桥大厦 1501 室

目 录

1 概述

上海戎磐网络科技有限公司研究团队基于近十年网络安全领域的深入探索及对 APT 组织恶意代码的跟踪，提出了网络空间“软件基因”前沿理论。围绕“软件基因”理论归纳的“同源未必相似、相似未必同源”的软件特性，从软件代码的“遗传性”和“变异性”两方面进行了系统技术验证，打破了传统安全主要基于“特征检测”的技术路线，为新型网络安全技术发展与应用提出了新的研究方向。

公司在网络空间“软件基因”理论指导下，开展了利用恶意代码实现安全脆弱性分析的正向应用，也开展了基于恶意代码的动静态环境检测的相关研究，取得了一系列成功案例。特别是沿着该研究方向，自主研发了“探戎”、“猎戎”、“智戎”、“数戎”等系列十余款网络安全产品，已在军队、政府、航运、金融等用户单位进行了推广服务，并利用先进的核心技术开拓了典型的网络安全创新型应用。

1.1 产品背景

在当今的信息化社会中，电子邮件是政府机构和大型企事业单位内部与外界沟通的重要工具。随着网络技术的发展，邮件系统也成为了网络攻击者针对这些关键机构发起攻击的主要途径之一。特别是邮件攻击，它不仅频繁发生，而且手法日益狡猾，对政府和大型企事业单位构成了严重的安全威胁。邮件攻击的主要目的是诱骗收件人提供敏感信息、财务数据或点击恶意链接，从而实施盗窃、欺诈甚至是更复杂的网络攻击。对于企业邮件安全来讲，传统的邮件攻击防御手段通常包含以下三种：

1、网络入口处部署入侵检测系统（IPS），入侵检测系统可以识别入侵者及入侵行为，为对抗入侵及时提供重要信息，以阻止事件的发生和扩大，入侵检测系统检测到邮件中的病毒进行处理；

2、使用邮件网关设备，邮件接收以后保存在邮件网关，邮件网关会对邮件进行恶意代码、附件扫描，邮件网关通常辅助部署沙箱，通过沙箱可以规避已知的漏洞触发，例如office附件漏洞的触发。

3、企业定期安全意识培训，由于企业员工缺乏足够的信息安全防范意识，违反信息安全操作规范，他们通常意识不到这种行为的严重后果，导致企业信息资产处于泄露风险中，企业需通过组织员工学习专业的信息安全培训，加强和提高信息安全防范意识，以减少工作中存在的信息安全风险。

入侵检测系统和邮件网关可以对恶意代码进行扫描、规避已有漏洞，但是未知的漏洞及其攻击手法是层出不穷的，基于0day漏洞的攻击，企业安全防护系统漏洞库尚未更新，因此通常无法进行识别和处理，给企业数据安全防护带来新的挑战；同时尽管企业会定期给员工做安全意识培训，但是由于企业员工基数比较大，难免有员工缺乏安全意识，违反信息安全操作规范，导致企业数据面临泄露风险。针对以上原因和企业诉求，戎磐给出邮件安全净化解决方案，为企业邮件数据安全提供全面的防护。

1.2 产品介绍

邮件安全净化系统是上海戎磐网络科技有限公司自主研发的一套邮件安全解决方案，系统依托领先的网络安全和大数据情报系统，

能够为客户提供安全、可靠的电子邮件接收、回复及邮件内容转换和专用邮件客户端功能。在互联网侧客户通过电子邮件管理模块接收邮件和回复，内容转换模块对邮件内容、附件进行病毒检测和转换存储到本地；在隔离内网侧，客户通过系统提供的邮件管理客户端查看邮件内容并进行回复。基于以上功能，系统可避免钓鱼邮件破坏系统、窃取密码及个人数据，造成病毒在多个系统中传播，进而感染整个公司网络，造成无法估量的损失。

2 产品功能说明

2.1 邮箱管理功能

系统允许用户同时绑定多个邮箱账户，可接收主流基于 POP3 协议的邮件，对于邮件主题、邮件接收时间等数据系统保持原有数据不变。提供最长 6 个月的邮件缓存期。不仅能够满足不同用户在邮件处理上的广泛需求，还保证了邮件数据的长期安全和可访问性，实现了高效、灵活的邮件管理体验。

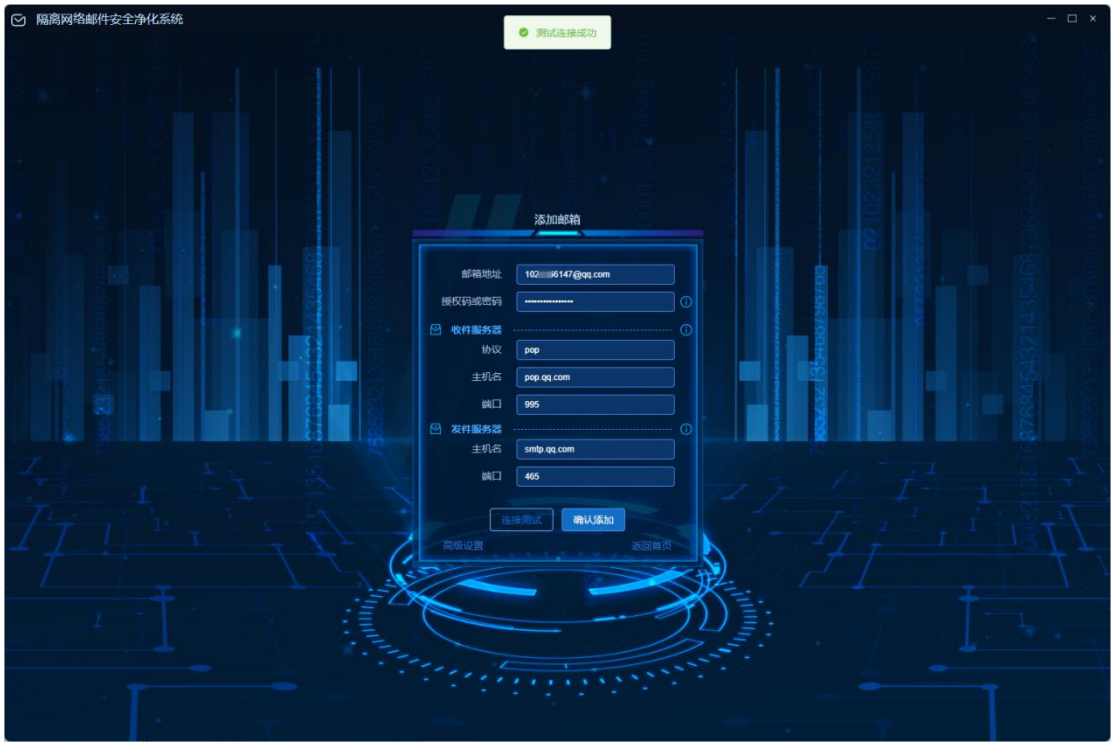


图 邮箱配置

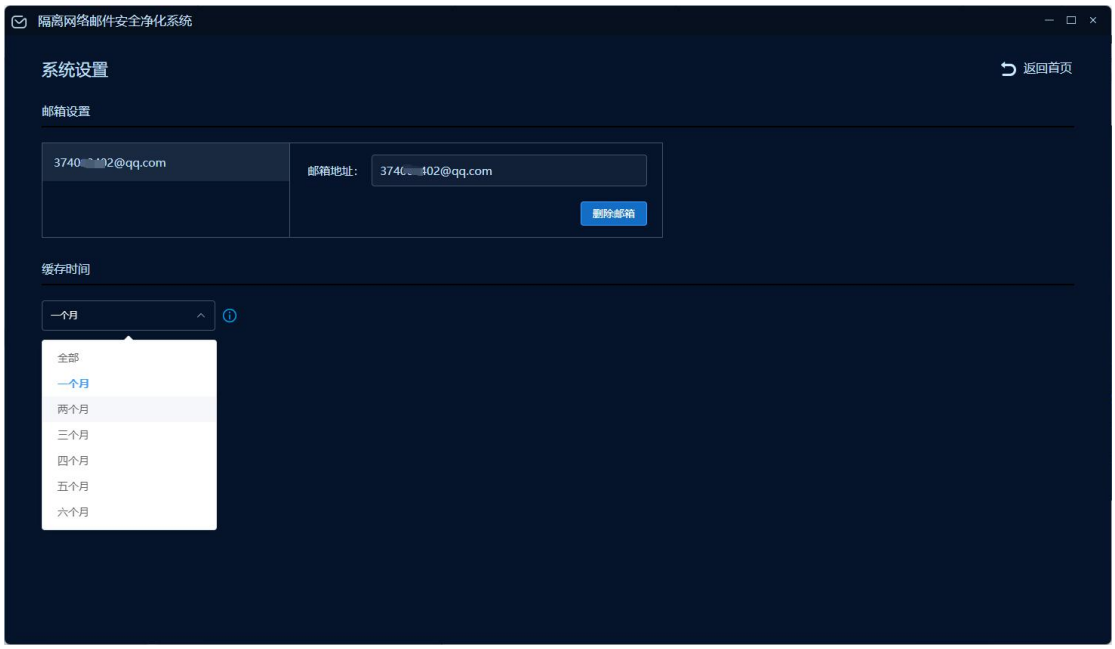


图 缓存时间设置

2.2 邮件管理功能

系统提供了一个直观易用的邮件管理功能，允许用户通过收取邮件功能，快速将邮箱中的新邮件保存至 UKey，并在首页列表中展示。用户可在本地系统中进行邮件的回复或删除操作，或者选择在隔离网环境下进行相同操作，确保邮件处理的安全性。完成隔离网中的操作后，只需将 UKey 插回联网主机即可同步操作结果，这一流程为用户提供了一个既安全又灵活的邮件管理方案。

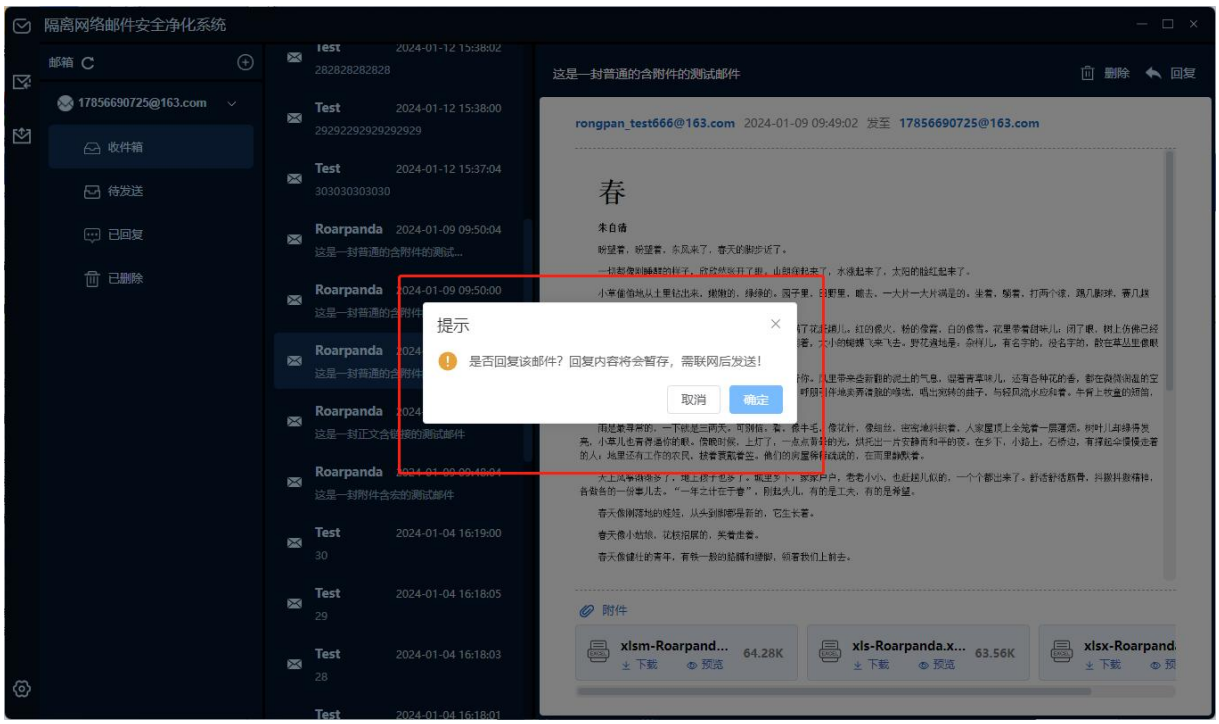


图 邮件回复页面

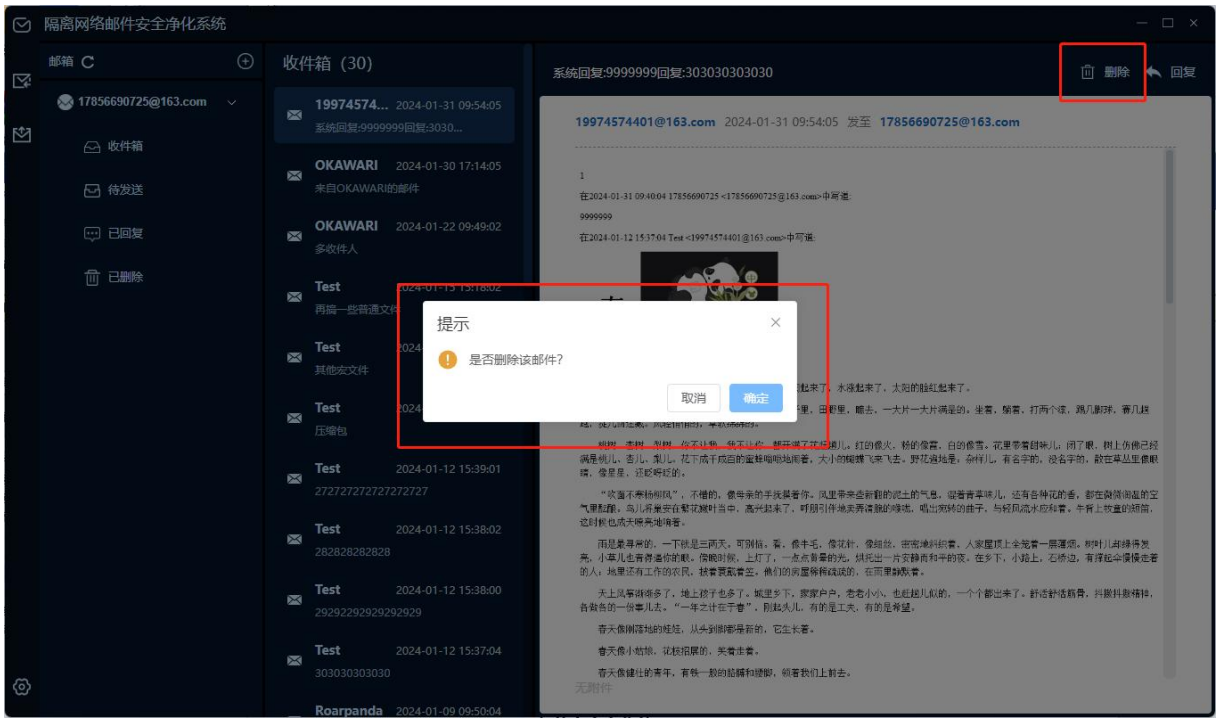


图 邮件删除页面

2.3 邮件内容静态化处理

邮件安全净化系统通过将电子邮件内容转化为静态图片的方式，

有效阻断了恶意链接的威胁。这一创新功能使得邮件接收者可以安全地查看邮件内容，而无需担心误点击可能隐藏在邮件中的恶意链接或嵌入式代码。通过将动态内容转换为静态格式，系统在保持邮件原始内容和格式的同时，消除了潜在的安全风险，从而大大降低了网络钓鱼和其他社会工程攻击的成功率。

图 邮件净化处理

2.4 附件内容安全净化

针对附件中潜在的宏病毒和其他恶意代码，邮件安全净化系统提供了一项强大的附件内容净化功能。该系统能够自动识别并处理附件文件，将其转化为安全格式，彻底剥离可能含有的宏病毒或执行代码。这一处理过程确保了附件的核心内容得以保留，同时排除了任何可能对用户设备构成威胁的恶意元素。通过这种预防性措施，用户在打开或下载邮件附件时的安全得到了显著提升。

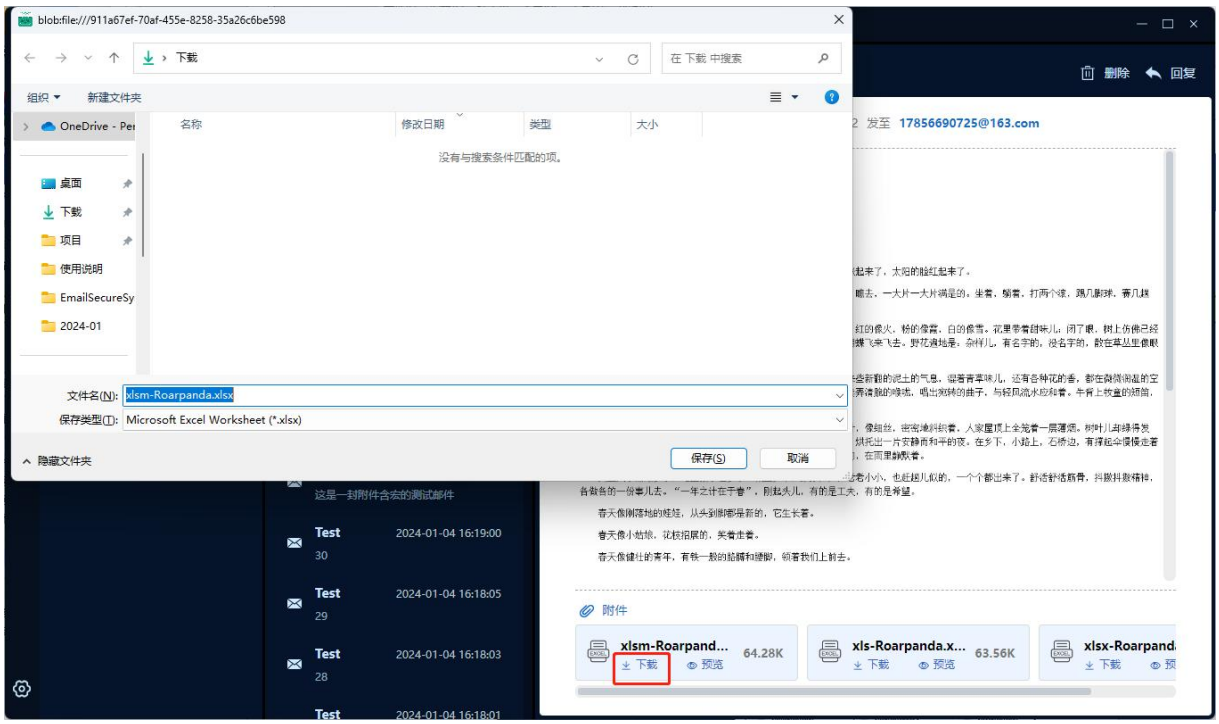


图 附件净化处理

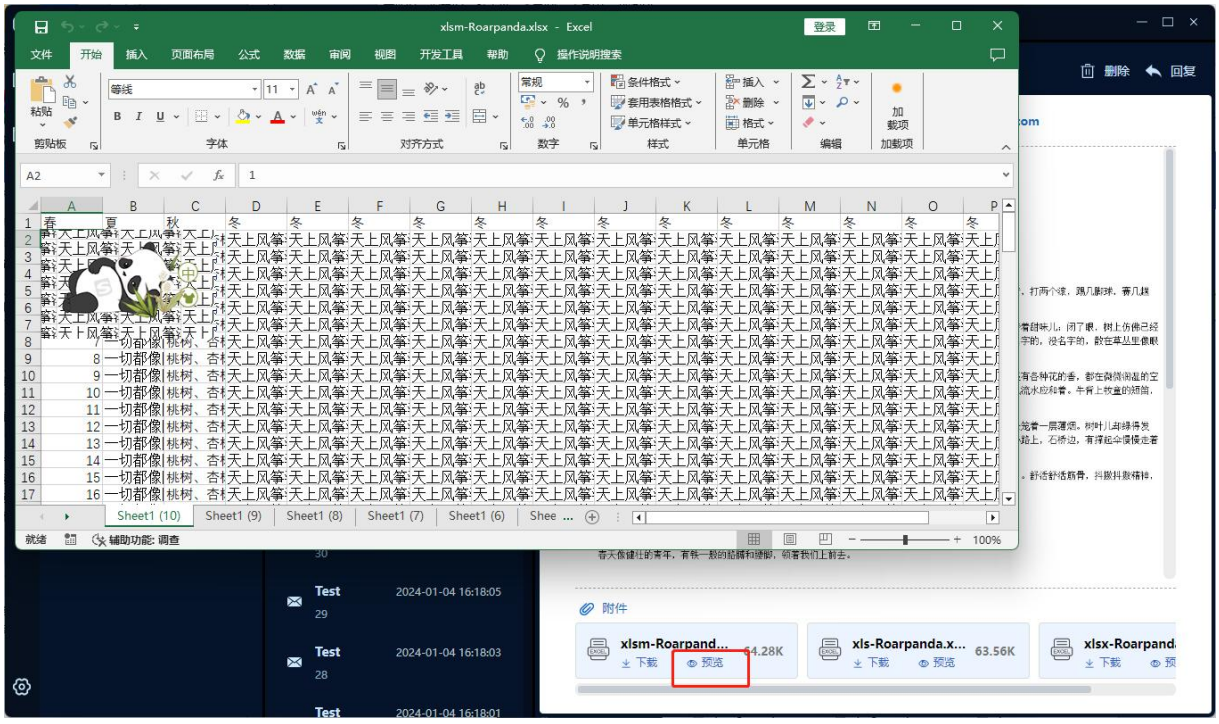


图 附件本地预览

3 产品优势

本系统通过独特的处理机制，旨在保护组织和个人用户免受恶意软件、钓鱼攻击以及其他邮件威胁的侵害。系统核心功能包括邮件内容的静态化处理以及附件内容的安全净化，确保每一封邮件和附件的安全性和完整性，从而为用户提供一个更加安全、可靠的电子邮件环境。产品主要包含以下六大优势。

1、智能识别机制：基于先进算法的智能识别系统，能够迅速准确地识别出潜在的威胁行为。

2、邮件内容静态化处理：将邮件内容转化为静态图片，有效阻断恶意链接点击，确保阅读安全。

3、宏病毒智能清除：利用高效技术识别并清除邮件附件中的宏病毒，保障附件安全性。

4、全方位安全检查：对发出和接收的邮件进行全面安全净化，提供多层次的安全保护。

5、减少员工工作量：自动化邮件处理流程，减轻员工负担，提升邮件查看和处理的效率。

6、易于集成和操作：设计简单易用，可无缝集成至现有邮件系统，确保用户快速上手。

4 产品形态

4.1 外观形态

邮件安全净化系统集成到专用 UKey 中，提供邮件接收、邮件回复、邮件正文可点击链接屏蔽及附件安全转换、专用邮件客户端等服务，系统使用方式简单。既不占用过多的计算资源，又便于用户携带和使用。UKey 采用了生物识别技术进行安全认证，确保只有授权的用户才能访问和操作系统。这种设计不仅体现了产品对安全性的高度重视，也极大地方便了用户在不同工作环境中对企业邮件进行安全防护，兼顾了便携性与安全保密性的双重需求。

4.2 工作形态

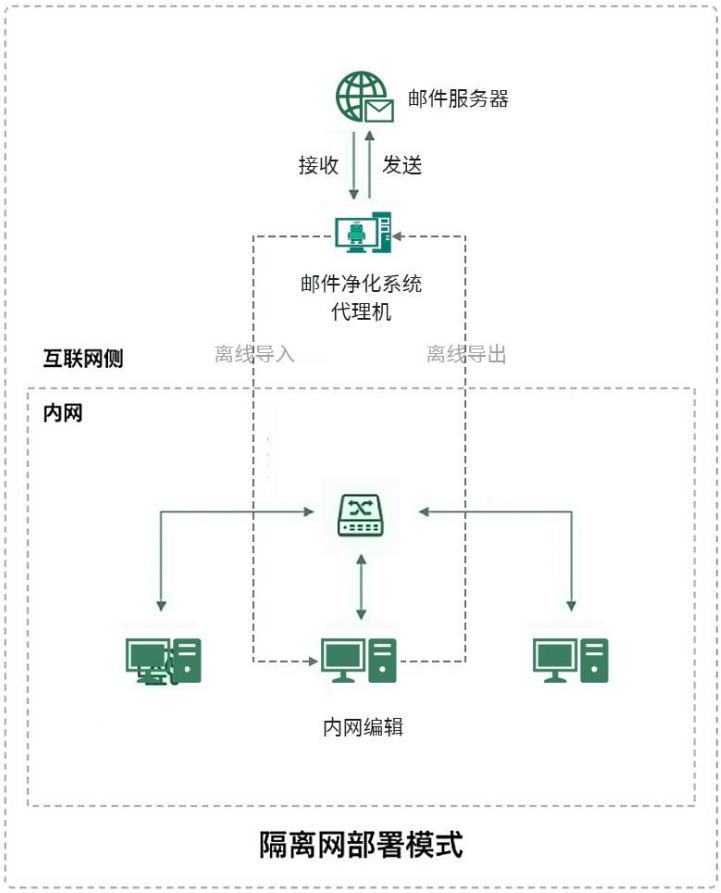
系统支持单主机操作和隔离网多主机操作两种工作形态，旨在满足不同网络环境下客户的安全需求。通过这两种模式，系统能够适应从个体用户到大型组织的多样化需求，无论是在直接联网的环境中还是在高度安全的隔离网环境下，都能提供有效的邮件安全防护和处理能力，确保邮件通信的安全与便捷。

- 单主机操作模式

在单主机操作模式下，系统允许用户在一台联网主机中接收邮件，并通过邮件净化系统对接收到的邮件进行立即的安全净化处理。用户可以直接在系统上完成邮件的阅读、回复、删除等操作，这种模式特别适合个人用户或小型组织，它简化了操作流程，确保了邮件处理的高效性和安全性，同时避免了恶意软件的潜在威胁。

- 隔离网多主机操作模式

对于处于高安全需求的环境中的用户，隔离网多主机操作模式提供了一种安全可靠的解决方案。在这种模式下，用户首先在联网主机进行邮件接收，经过邮件安全净化系统处理后，邮件被转移到隔离网内的主机上进行后续的回复或删除等操作。这种分离的操作流程特别适合需要严格数据隔离的政府或大型企事业单位，它最大限度地减少了网络攻击的风险，确保了邮件处理过程中的绝对安全。


邮件服务器
接收
发送
邮件净化系统
代理机
互联网侧
离线导入
离线导出
内网
内网编辑
隔离网部署模式

5 产品功性能参数

序号	指标名称	指标描述
1	邮件接收	支持对接市面主流协议邮箱
2		支持互联网端接收附件
3		支持同时绑定多个邮箱
4		支持多个用户同时使用
5		接收界面图形化展示
6	邮件编辑	支持隔离网访问系统
7		支持隔离网侧离线邮件回复
8		支持隔离网侧离线邮件删除操作
9	邮件安全净化	支持邮件正文安全处理
10		支持识别和清除附件中的宏病毒
11		支持邮件正文链接屏蔽
12		支持 word 格式附件净化处理
13		支持 wps 格式附件净化处理
14		支持 pdf 格式附件净化处理
15		支持 excel 格式附件净化处理
16		支持压缩包附件净化处理，压缩包内包含 word/wps/pdf/excel 文件
17	专用客户端	允许用户查看安全处理后的正文
18		允许用户离线回复电子邮件，回复数据暂存系统内部
19		允许用户查看、下载安全处理后的附件
20	主要性能指标	支持通过 UKey 离线访问系统
21		支持主流邮箱种类≥6 种，包括但不限于 163 邮箱、126 邮箱、腾讯邮箱、新浪邮箱、谷歌邮箱等
22		支持 win7 以上 windows 操作系统
23		客户端打开时间≤3s
24		专用 UKey 最大写入速度≥60M/秒
25		专用 UKey 最大读取速度≥200M/秒
26		专用 UKey 容量≥256G
27		支持附件格式≥5 种包括但不限于 word、pdf、Excel 等
28		支持附件保存时间不低于 6 个月
29		支持绑定邮箱账号≥3 个
30		支持同时操作用户数≥2 名
31		邮件正文处理准确率超过 95%
32		邮件附件宏病毒处理准确率超过 95%

PRODUCT SYSTEM
产品体系

戎磐
信息安全产品体系

安全产品类

猎戎
分布式网络诱捕威胁检测防御系统

探戎
网络威胁智能预警与防御溯源系统

智戎
恶意代码软件基因智能检测分析系统

数戎
数据库透明加密安全防护管理系统

比微云
网络威胁情报服务云平台

解决方案类

数据安全
勒索软件防护解决方案

电信安全
赌诈大数据情报解决方案

网络安全
APT组织分析溯源解决方案

软件安全
漏洞发现与补丁管理解决方案

工控安全
软件供应链威胁监测预警解决方案

国家安全
境外网络威胁态势感知与监测预警

安全服务类

安全运维、漏洞管理

渗透测试、风险评估

应急响应、攻防演练

重大活动网络安全保障

安全培训、CISP认证

安全咨询、等保2.0测评

赋能 赋能 赋能

全球软件基因库(Global Software Gene Bank)

COMPANY PROFILE
公司简介

上海戎磐网络科技有限公司成立于 2016 年 11 月，公司位于上海长宁区娄山关路 55 号（新虹桥大厦）。为布局全国技术及市场推广，在河南设有控股子公司，沈阳设有分公司，与三亚学院联合建有“ 恶意代码软件基因分析应用工程研究中心（省级）”。公司以“ 软件基因 ”为核心技术，已申请发明专利 20 余项，软件著作权 50 余项，拥有“ 软件基因 ”、“ 戎磐 ”、“ 比微云 ”等 10 余款注册商标，已经研发出猎戎、智戎、探戎等三大系列 30 余款产品，主要为客户提供信息安全、数据安全、态势感知、攻击溯源等产品研发和相关咨询与培训服务，是国家高新技术企业，也是上海市人工智能认定企业和专项支持企业。戎磐聚焦网络安全颠覆性和非对称性能力建设，能够为互联网高速发展不断创造的新业态、新场景网络安全提供全面、高效、创新的解决方案。

SOFTWARE GENE CORE TECHNOLOGY
软件基因核心技术

网络空间博弈日趋激烈，威胁无处不在，新型攻击、APT（高级持续威胁）、勒索、黑产、有国家背景的网络安全事件层出不穷。捍卫国家网络空间主权、保障国家关键基础设施安全、构建国家网络空间治理新秩序、实现国家网信事业繁荣发展等对信息安全自主核心技术提出了更高要求。戎磐网络围绕软件本身“ 同源未必相似、相似未必同源 ”的安全属性，提出了网络空间“ 软件基因 ”前沿理论，从软件代码的“ 遗传性 ”和“ 变异性 ”两方面进行了系统技术验证，打破了源自欧美传统信息安全主要基于“ 特征检测 ”一事一议、关注个体的技术路线，为新型网络安全拥有自主知识产权的核心技术发展与创新应用提出了新的方向。

基因是控制生物性状的遗传性信息。人类基因组计划（HGP）是与曼哈顿计划、阿波罗计划并肩的人类三大科学探索工程。借鉴生物基因用于研究生物群体性关系的视角，软件大量代码复用、调用和始终保持迭代发展的特性使其天然具备了“ 遗传 ”和“ 变异 ”两个基因的基本属性。

“ 软件基因 ”是以识别、分析、研究软件与软件之间群体特性为目的的具有普适性的一种认知理论和方法。戎磐团队采用大数据、AI、逆向分析等技术方法，建立了面向各类软件载体的“ 基因 ”提取算法，采用 OPCODE 中间码表示和存储“ 软件基因 ”信息，在网络空间博弈日益激烈、网络黑产威胁日益严峻趋势下，公司聚焦网络安全颠覆性和非对称性能力建设，目前具备每日 20 万级境外恶意代码搜集、全球 300+APT 组织活动动向追踪、恶意代码“ 软件基因 ”AI 分析等核心能力，形成了打击各层面网络犯罪需求的独特商业模式。

公众号

官网

021-60795361

roarpanda@roarpanda.com

上海市长宁区娄山关路55号新虹桥大厦15层