魔盾 ESG 管理员手册

版本：1.03

魔盾邮件安全网关 | MalDun Email Security Gateway | ESG/ESGv

内容索引

第一章： ESG/ESGv 简介 4
1. 连接管控、发件人信誉过滤 (Sender Reputation) 4
2. 用户自定义策略 (Custom Policy) 5
3. 病毒分析 (Anti-Virus) 5
4. 钓鱼分析 (Anti-Phishing) 5
5. 垃圾邮件分析 (Anti-Spam) 6
6. 广告邮件分析 (Anti-Ads.) 6
7. 高级威胁分析 (Anti-APT/Advanced Threat) 7
8. ESG 分析流程 7
9. ESG 部署形式 8
10. 配置 ESG 8
11. 使用 ESG 8

第二章：配置 ESG 9
1. 配置 ESG 邮件安全网关之前的准备工作 9
2. ESG 网络环境配置 9
2.1 网络配置说明 9
2.2 网络配置步骤 10
3. 激活 ESG 邮件安全网关 11
4. 配置 ESG 邮件安全网关系统 12
4.1 版本 12
4.2 系统参数设置 13
4.3 管理员账号 13
4.4 系统更新 14
4.5 远程技术支持 15
4.6 系统状态 16

第三章：登录 ESG 系统 17

第四章： 用户设置 19
1. 用户信息 19
2. 修改密码 19
3. 操作记录 20

第五章：使用 ESG 21
1. 信息概览 21
2. 隔离邮件 26
2.1. 隔离邮件查询 27
2.2. 隔离邮件信息 28
2.3. 隔离邮件操作 29
3. 高级威胁 43
4. 统计报表 49
4.1. 综合统计 51
4.2. 病毒邮件 53
4.3. 垃圾邮件 54
4.4. 高级威胁 55
4.5. 邮件溯源 56
5. 邮件追踪 58

5.1. 邮件追踪查询 58
5.2. 邮件状态信息 60
5.3. 邮件追踪操作 61
6. 策略设置 63
6.1. 基本策略 64
6.2. 自定义策略 72
6.3. 高级威胁报告订阅 73
附录 A：名词解释 76
附录 B：报告误判(False Positive) / 漏判(False Negative) 77
附录 C：联系我们 79

第一章： ESG/ESGv 简介

魔盾邮件安全网关，Email Security Gateway，或 Email Security Gateway virtual （包含魔盾邮件安全虚拟网关，以下统称 ESG）系统是上海魔盾信息科技有限公司推出的企业电子邮件安全网关产品。

魔盾邮件安全网关可以以实体网关机器形式部署，也可以以 VMware ESXi 虚拟机形式部署。结合魔盾邮件安全云服务，用户还可以选择混合形式部署。

有别于传统的防垃圾邮件系统，魔盾 ESG 是基于下一代安全架构的邮件安全解决方案，高效的结合了实时信誉过滤与内容识别，恶意软件行为动态分析，以及机器学习与威胁情报。ESG 可以帮助企业发现，阻止基于邮件的威胁， 实现全方位的邮件安全防护，并在此基础上提供警报触发，威胁分析与追踪的工具。ESG 的主要邮件分析功能如下：（图 1：ESG 邮件安全）

1. 连接管控、发件人信誉过滤 (Sender Reputation)

由魔盾安全综合自有网络安全数据平台/全球威胁情报源，与本地邮件流数据打造的发件人信誉系统，是一套强大的基于域名、IP、发件地址、收件地址、和发收件人关系等关键因子的自适应信誉数据库。通过域名/IP 大数据和网络数据关联模型分析，侦测域名、IP 和发件人在威胁活动中的行为（垃圾邮件、恶意软件和网络攻击等）、收件人活跃状态、发收件人邮件行为学习，ESG 动态计算和生成发件人综合信誉分数，并通过信誉分数控制和过滤向客户发送邮件的发件人和邮件服务器。（图 2：发件人信誉系统）

2. 用户自定义策略 (Custom Policy)

魔盾 ESG 支持灵活的自定义策略功能，以适应客户的不同需求。用户可以根据邮件量、邮件类型、邮件趋势等因素，启动或关闭 ESG 特定功能或模块，调整威胁阻截/隔离/传递行为。用户可以针对发件地址、收件地址及邮件标题设定黑白名单，以控制魔盾 ESG 扫描阻止，投递，或标记特定邮件。

关于用户自定义策略的设定，请参考“策略设置”章节。

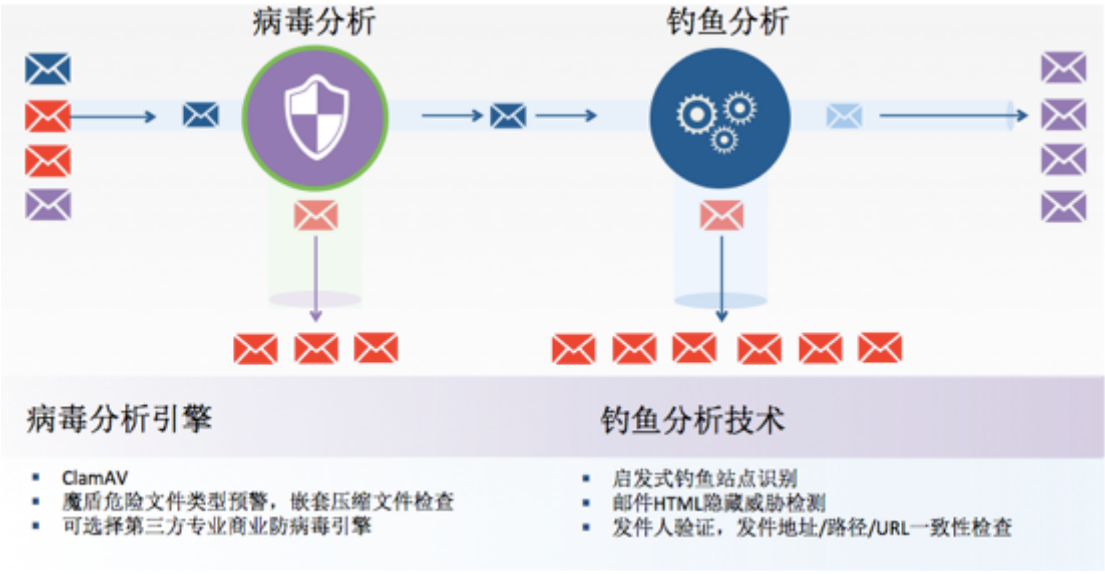
3. 病毒分析 (Anti-Virus)

魔盾 ESG 配置了灵活的威胁附件监控与过滤规则，可以高效拦截可能对用户造成威胁的附件文件。魔盾 ESG 还内嵌了 ClamAV 防病毒引擎，支持对病毒附件的扫描和查杀。

针对客户的不同需求，魔盾 ESG 也支持嵌入第三方商业版本防病毒引擎，作为魔盾 ESG 病毒分析的模块之一。

4. 钓鱼分析 (Anti-Phishing)

针对客户高度重视的钓鱼邮件防范，魔盾 ESG 专门开发了钓鱼分析引擎，对邮件中的钓鱼威胁进行检测和分析。通过启发式的钓鱼站点识别与钓鱼发件人/HTML/邮件内容检测，魔盾 ESG 可以高效识别可疑欺诈并对邮件进行隔离/标记操作。（图 3: 病毒分析与钓鱼分析）



5. 垃圾邮件分析 (Anti-Spam)

魔盾 ESG 打造的业界顶尖的深度垃圾邮件分析引擎，通过发件人信誉与黑名单，邮件内容分析规则，机器学习规则，全球垃圾邮件投诉样本库等因素的综合分析，动态生成垃圾邮件概率，并支持用户通过垃圾邮件概率（垃圾邮件防护等级）设定邮件处理策略。

6. 广告邮件分析 (Anti-Ads.)

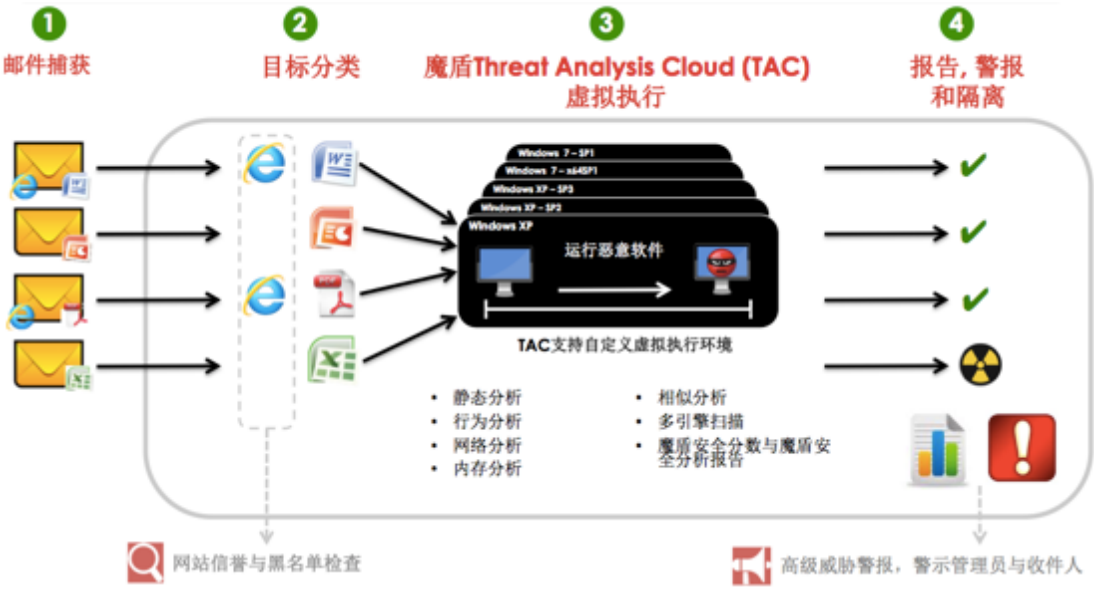
广告类邮件往往处于垃圾邮件的灰色地带，客户对广告类邮件的判别主观性较强。针对客户对广告订阅类邮件或商务推广类邮件的不同需求，魔盾 ESG 特别加入了广告邮件分析模块，帮助用户甄别与控制是否接受广告邮件。 （图 4: 垃圾邮件分析与广告邮件分析）

7. 高级威胁分析 (Anti-APT/Advanced Threat)

高级威胁分析是魔盾 ESG 特有的针对常规防垃圾邮件引擎和防病毒引擎难以识别的未知威胁和高级针对性威胁（如 0-day，APT，勒索软件等）的检测模块。

需要注意的是，只有当用户选择并开启高级威胁分析模块时，该功能才会生效（需要管理员用户在配置 ESG 时加入 ESG 高级威胁分析 API Key）。高级威胁分析会将可疑邮件中的附件与链接通过加密的 HTTPS 连接传递到魔盾 TAC 环境中分析。分析样本与分析结果报告的读取权限将经过魔盾 TAC 严谨的隐私与安全保护。

魔盾 ESG 依托强大的魔盾 Threat Analysis Cloud (TAC)，将邮件附件和链接传递到 TAC 分析环境中进行实时动态威胁分析。魔盾 TAC 在可控虚拟环境执行附件/链接，并进行一系列静态分析和深度行为分析，生成威胁等级和威胁分析报告等。用户可以针对高级威胁的威胁等级设定阻截/隔离策略，对高级威胁进行过滤，最大程度的保护终端用户安全。魔盾 ESG 还独创的提供了互动视图威胁分析工具，帮助用户对威胁进行更深层的分析。（图 5: 高级威胁分析）



8. ESG 分析流程

魔盾 ESG 系统将按照以下模块顺序对邮件进行分析（当该模块/功能开启时，请参考“基本策略”章节了解更多关于各功能策略设置的信息）：

- 连接控制/发件人信誉过滤
- 自定义策略
- 病毒分析（包含危险附件类型）/ 钓鱼分析（同时并发进行）
- 垃圾邮件分析

- 广告邮件分析
- 高级威胁分析

当邮件在一个模块分析中被判定为威胁并进行阻挡或隔离后，将直接进入隔离区，不会进行之后的分析流程。

9. ESG 部署形式

针对企业实际需求和企业网络架构，魔盾 ESG 邮件安全网关通过串联形式接入邮件（SMTP）数据流，直接对企业邮件进行过滤。魔盾 ESG 系统会检查、分析经由 ESG 的邮件，并根据 ESG 系统的分析结果以及用户的策略设置对邮件进行相应的操作，例如隔离，投递，标记等。过滤后的正常邮件将被投递到用户内部邮件服务器。魔盾 ESG 邮件安全网关起到邮件中继，过滤，控制，分析的作用。除此之外并不影响用户已有邮件处理流程。

10. 配置 ESG

ESG 提供独立的 WebUI 配置系统，供有管理权限的企业管理员用户进行系统初始验证，企业用户与域名设置，系统与规则更新等操作。ESG 系统的正确配置对于管理和使用 ESG 系统至关重要。如果需要支持与协助，请联系魔盾技术支持。关于配置 ESG 的详细信息，请参考管理员手册第二章：配置 ESG。

11. 使用 ESG

ESG 提供友好易用的 WebUI 邮件管理界面和隔离邮件管理系统。企业邮箱管理员，企业安全团队和有权限的用户可以根据企业邮件情况调整策略，设置自定义规则，生成邮件分析报告，对威胁进行深度分析等；以及对 ESG 隔离邮件进行管理，分析，预览，释放，删除等操作。关于管理 ESG 的详细信息，请参考管理员手册第五章：使用 ESG。

第二章：配置 ESG

1. 配置 ESG 邮件安全网关之前的准备工作

1) 在配置魔盾 ESG 邮件安全网关之前，请确认您已经收到魔盾 ESG 的产品许可编号（License Key）；如果您同时选择了魔盾 ESG 高级威胁分析功能，请确认您已经收到魔盾高级威胁分析模块的接口秘钥（API Key）。

2) 对于 ESGv 虚拟版本的 ESG 邮件安全网关，请确认您已经将 ESGv 虚拟邮件安全网关正确安装部署在企业邮件网络环境中的服务器上（魔盾 ESGv 目前支持 VMware ESX/ESXi 部署）。

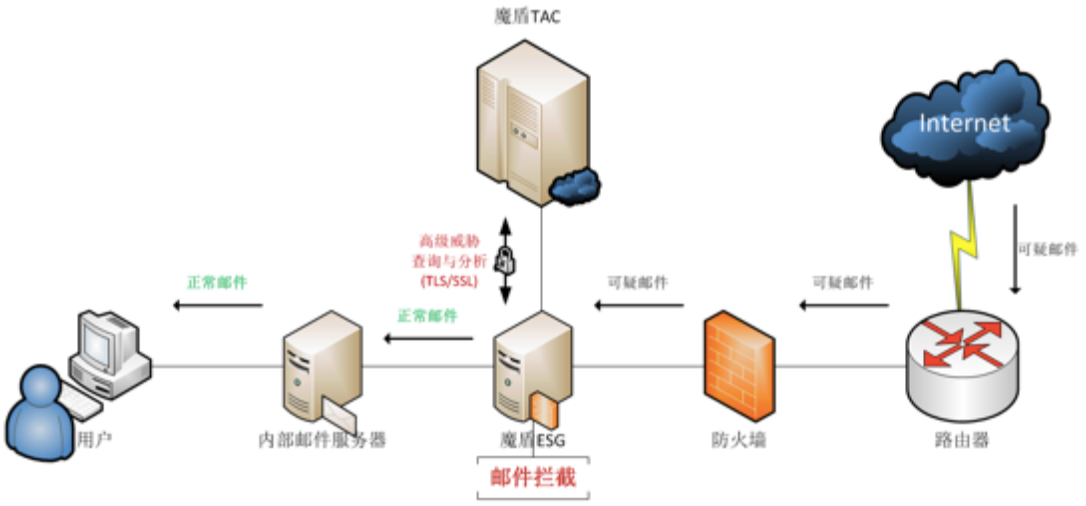
3) 针对企业网络架构和使用意图，正确配置中继控制和邮件路由。

此外，我们建议使用本文档的邮件/系统管理员了解以下知识：

- SMTP（包括 POP3）协议基本原理
- DNS 原理及 A 纪录，MX 纪录，TXT(SPF, DKIM)记录及 PTR 记录等概念
- 常见邮件系统（如 Exchange, MDaemon, Domino 等）与邮件网关等的相关配置
- 垃圾邮件的概念（包括广告邮件，病毒邮件，钓鱼邮件等）与防垃圾邮件的基本原理
- 高级威胁的概念与高级威胁分析的基本原理

2. ESG 网络环境配置

魔盾 ESG 邮件安全网关在用户网络环境中的拓扑结构为：



2.1 网络配置说明

魔盾 ESG 邮件安全网关可以在用户网络中被设置为负责接受外域邮件的邮件网关。从外域发往用户邮箱域名的邮件，根据域名 MX 记录的指向，先经过魔盾 ESG 邮件安全网关，通过 ESG 的邮件分析与过滤后，再投递到用户内部邮件服务器。

（注： 由于魔盾 ESG 下一代邮件安全解决方案包含防垃圾邮件，防病毒，高级威胁分析等功能模块，并集成了强大的邮件威胁信息与分析能力。我们建议您将魔盾 ESG 作为邮件过滤分析的入口，或邮件安全分析的第一步。如果您的企业已经部署了邮件防病毒（AV）/防垃圾邮件（AS） 等邮件过滤系统，您可以将魔盾 ESG 部署在其它邮件过滤系统之前以获得最优的过滤分析效果。根据用户需求，魔盾 ESG 邮件安全网关也可以部署在用户网络中其它邮件过滤产品之后。）

如果邮件被魔盾 ESG 判定为垃圾邮件，或高级威胁等，并且用户策略设定为隔离的。邮件将被 ESG 存入邮件隔离区，而不会继续投递。用户可以通过 ESG 管理系统或隔离邮件报告对 ESG 隔离区中的邮件进行释放。释放后的邮件将从 ESG 系统投递到用户内部邮件服务器。

用户通过客户端收发邮件的方式保持不变：

- 通过邮件客户端（如 Outlook, Foxmail 等）收发邮件的用户，其 SMTP 服务器和 POP3 服务器的 IP 地址仍指向内部邮件服务器。
- 通过 Web 方式收发邮件的用户，仍然通过 HTTP/HTTPS 方式访问邮件服务器。

2.2 网络配置步骤

根据魔盾 ESG 邮件安全网关的网络拓扑，ESG 系统的网络配置步骤如下：

1) 了解用户内部邮件服务器的域名和 IP 地址：
   如：邮件系统域名：mail.domain.com
   IP: 192.168.101.100

2) 给 ESG 邮件安全网关提供内网 IP 地址（及内网域名），以及缺省网关地址，DNS 服务器地址：
   如：IP: 192.168.101.50
   网关：192.168.101.1
   DNS：192.168.114.100 / 114.80.207.44

3) 修改防火墙上公网地址与内网地址的映射，将域名 mail.domain.com 的 MX 记录指向 ESG 邮件安全网关的 IP 地址，如： 192.168.101.50。

4) 在防火墙上开放 TCP/UDP 端口：

端口	协议	In/Out	说明
25	TCP	In/Out	用于收发邮件
53	TCP/UDP	Out	DNS 解析与 RBL 查询
2703/7	TCP	Out	ESG 邮件样本库指纹查询
24441/6277	UDP	Out	ESG 邮件样本库指纹查询
80/443	TCP	Out	ESG 高级威胁分析提交与查询，ESG 系统,规则与病毒库更新
8443	TCP	Out	ESG 远程技术支持

5) 在魔盾 ESG 管理页面中，针对不同的邮箱域名，设置该邮箱域名所需要投递的下一跳用户内部邮件服务器地址。

如：下一跳服务器地址： 192.168.101.100

（若下一跳服务器为其他邮件网关，则将下一跳服务器指向该邮件网关地址，同时请在下一跳邮件网关上将魔盾 ESG 的 IP 地址加入 IP 连接白名单）

具体信息请参考“使用 ESG”章节中的策略设置部分。

（注 1：当用户使用多个内部邮件服务器管理多个邮箱域名时，可以先将邮件统一投递到魔盾 ESG 邮件安全网关进行分析过滤，之后再根据不同的邮箱域名所需设置，投递到不同的内部邮件服务器。）

（注 2：魔盾 ESG 使用端口 8000 和 8001 进行内网 UI 系统访问，配置，与管理。）

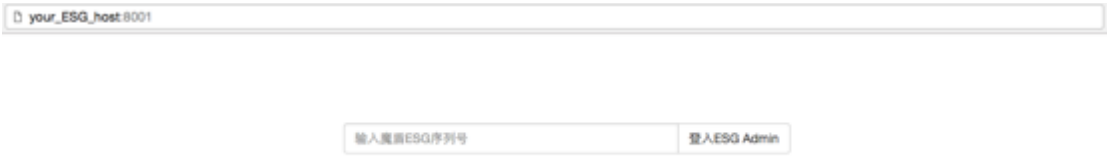
3. 激活 ESG 邮件安全网关

当 ESG 邮件安全网关系统部署成功后，用户可以在 Web 浏览器并输入：

http://<ESG 邮件安全网关 hostname 或 IP 地址>:8001

（注：8001 为端口号）

进入 ESG 邮件安全网关的配置界面。



在页面中输入魔盾 ESG 产品许可号，点击“登入 ESG Admin”按钮后，即可激活魔盾 ESG 邮件安全网关系统

4. 配置 ESG 邮件安全网关系统

当用户输入 ESG 产品许可号并激活 ESG 邮件安全网关后，即可进入魔盾 ESG 邮件安全网关配置系统。

魔盾 ESG 邮件安全网关配置系统包含以下部分：

- 版本
- 系统参数设置
- 管理员账号
- 系统更新

4.1 版本

ESG 系统版本信息页面显示了 ESG 系统各部分的版本信息，包括：

其中，邮件过滤引擎版本为魔盾 ESG 内置垃圾邮件分析模块的版本，魔盾 ESG 内置垃圾邮件引擎包含了发件人信誉，钓鱼分析，病毒分析，垃圾邮件分析，广告邮件分析及其它邮件分析相关功能，以及对于魔盾 ESG 邮件分析与过滤的流程优化。魔盾 ESG 邮件过滤引擎的更新，保证了魔盾 ESG 邮件安全网关的邮件处理性能和效率。

垃圾邮件规则版本为魔盾 ESG 垃圾邮件分析内容过滤规则版本。魔盾 ESG 垃圾邮件分析内容过滤规则包含内容过滤，机器学习规则，基于垃圾邮件样本指纹的规则及其它规则等。为了应对不断变化的垃圾邮件内容和形态，魔盾 ESG 垃圾邮件分析内容过滤规则将保持频繁更新。魔盾 ESG 垃圾邮件规则的更新，确保了魔盾 ESG 邮件安全网关对垃圾邮件的高效阻截，以及对已有规则的更新优化。

管理页面版本为魔盾 ESG 系统的 Web 管理和使用系统。包含了对 ESG 所处理的邮件流的监控和管理，以及邮件与威胁分析功能。魔盾 ESG 管理页面的更新，保证了魔盾 ESG 最新的页面功能的呈现和正常使用。

系统更新程序版本为魔盾 ESG 系统各项更新模块的控制程序。魔盾 ESG 系统更新程序的更新，确保了魔盾 ESG 系统各项更新模块能够正常运行，也因此保证了魔盾 ESG 系统整体的正常使用。

需要注意的时，当用户每次点击进入版本页面时，ESG 系统将会自动启动版本更新检查，确认当前系统版本是否为最新版本。如果检测到有可更新的版本，ESG 版本页面会提示有更新。

4.2 系统参数设置

ESG 系统参数页面包含了 ESG 系统参数设置的功能。

其中，魔盾 ESG 高级威胁分析 API KEY 为启动魔盾 ESG 高级威胁分析所必须。当魔盾 ESG 系统对邮件处理中的可疑附件/URL 提交到魔盾 Threat Analysis Cloud （TAC）平台进行分析时，需要通过 API Key 将邮件附件/URL 以安全加密形式提交到魔盾 TAC。

ESG 系统主机名提供设置 ESG 系统的主机名称的功能，ESG 系统在用户邮件网络环境中将以该主机名称出现。

4.3 管理员账号

魔盾 ESG 管理员账号设置页面提供了 ESG 系统管理员账号，与所关联的邮件域名的设置。

ESG 管理员用户可以在该页面对管理员账号和邮件域名进行管理和设置。魔盾 ESG 支持多域名管理，管理员用户可以在该页面进行邮箱域名及其管理员账户的分配，尤其是当大型企业需要多个邮件管理员对不同邮件域名进行管理时。

用户可以通过“管理员账号”页面添加管理员账号，和所管理的邮箱域名。需要注意的是，一个管理员用户名可以同时管理多个邮箱域名；而一个邮箱域名也可以由多个管理员用户管理。

此外，当管理员用户被添加时，管理员用户名所对应的密码缺省为：“用户名”+“#maldun”。例如，当管理员用户名为“test”时，该用户的缺省密码为：“test#maldun”。该用户可以在登陆 ESG 管理系统后对密码进行修改。具体信息请参考“登陆 ESG 系统”的修改密码章节。

4.4 系统更新

魔盾 ESG 系统更新页面提供了对魔盾 ESG 系统更新功能的管理。

魔盾 ESG 系统支持自动定时更新与手动更新方式。管理员用户可以开启定时更新（每天更新一次），并设置希望每日定时更新的时间。

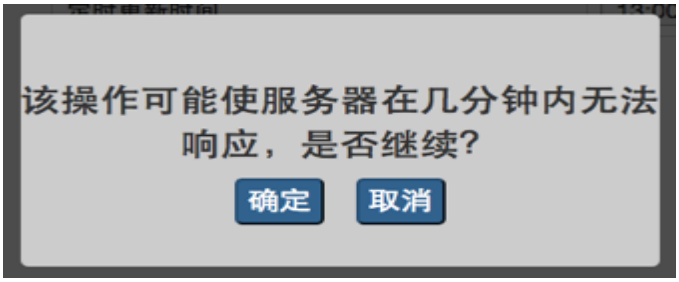
蓝色的开关圆圈在右代表该功能开启，在左（变为灰色圆圈）代表该功能关闭。

当用户选择关闭定时更新时，系统将提示：

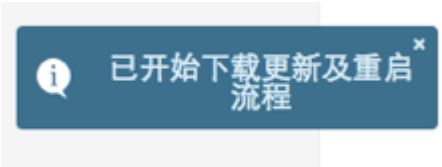
当用户选择开启定时更新时，系统将提示：

当用户设定定时更新时间后，系统将提示：

管理员用户也可以进行手动系统更新。当用户点击“下载更新并重启服务”按钮时，系统会做出提示并要求用户确认。



当用户确定下载更新并重启服务后，ESG 系统会提示开始更新与重启流程：



并尝试连接魔盾更新服务器，下载系统更新，并重启服务。

当管理员用户对 ESG 系统环境做出重要改动时，管理员用户也可以点击“立即重启服务”，强制重启 ESG 系统和服务。同样，ESG 系统会需要用户确认该次操作，并在用户确认后提示开始重启流程：

4.5 远程技术支持

魔盾 ESG 远程技术支持页面提供了 ESG 远程技术支持连接开启的功能，方便魔盾 ESG 技术支持人员对用户 ESG 系统提供技术支持。

远程技术支持功能缺省为关闭，当管理员需要魔盾 ESG 技术支持人员协助时，可以选择开启远程技术支持。此时魔盾 ESG 系统会尝试对魔盾 ESG 技术支持服

务器进行远程连接（通过 8443 端口），魔盾 ESG 技术支持人员即可连接到魔盾 ESG 系统进行问题排查和解决。

远程技术支持功能完全由管理员控制，在远程技术支持功能关闭时，魔盾技术支持或外部人员无法连接到魔盾 ESG 系统。当远程技术支持功能开启时，ESG 系统将只建立到魔盾 ESG 技术支持服务器的连接。

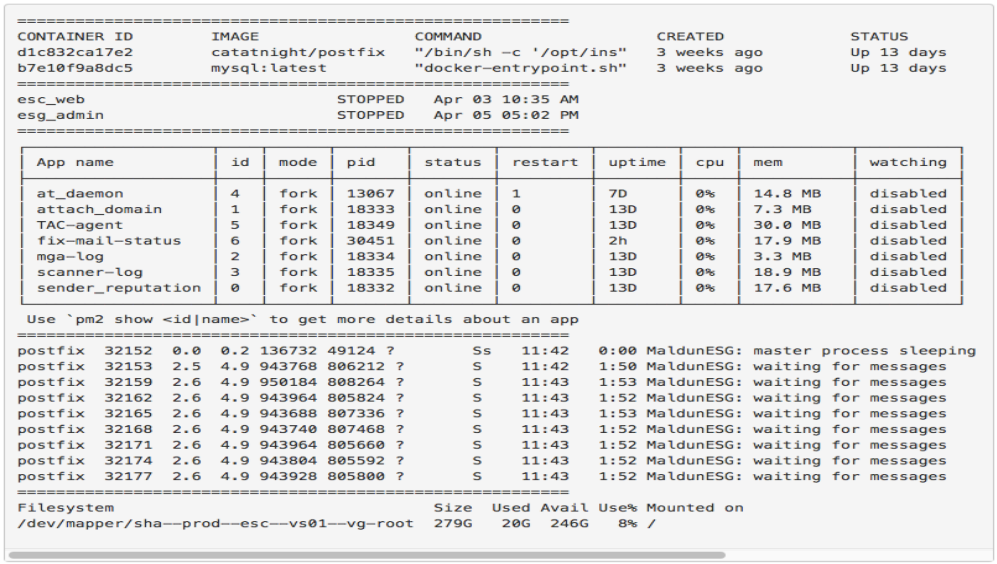
我们建议 ESG 管理员在不需要远程技术支持时保持关闭远程技术支持功能，只有在需要远程技术支持协助，并与魔盾 ESG 技术支持人员取得联系后，再选择开启远程技术支持。在结束远程技术支持连接之后，及时关闭远程技术支持功能。

4.6 系统状态

魔盾 ESG 系统状态页面提供魔盾 ESG 系统运行状态查询的功能，使 ESG 管理员可以了解魔盾 ESG 系统的工作情况。

在用户点击查询系统状态后，ESG 系统会自动实时查询并综合系统信息，并将各项系统状态数据呈现在页面上。

ESG 系统状态包含了系统各模块及子进程的运行情况，CPU 使用率，内存使用率，启动时间，运行时间，状态等信息；以及系统磁盘空间使用情况等。



```
============================================================
CONTAINER ID        IMAGE                COMMAND                  CREATED             STATUS
d1c832ca17e2        catatnight/postfix   "/bin/sh -c '/opt/ins"   3 weeks ago         Up 13 days
b7e10f9a8dc5        mysql:latest         "docker-entrypoint.sh"   3 weeks ago         Up 13 days
============================================================
esc_web                          STOPPED   Apr 03 10:35 AM
esg_admin                        STOPPED   Apr 05 05:02 PM
============================================================
┌──────────────────┬────┬──────┬───────┬────────┬─────────┬────────┬─────┬──────────┬──────────┐
│ App name         │ id │ mode │ pid   │ status │ restart │ uptime │ cpu │ mem      │ watching │
├──────────────────┼────┼──────┼───────┼────────┼─────────┼────────┼─────┼──────────┼──────────┤
│ at_daemon        │ 4  │ fork │ 13067 │ online │ 1       │ 7D     │ 0%  │ 14.8 MB  │ disabled │
│ attach_domain    │ 1  │ fork │ 18333 │ online │ 0       │ 13D    │ 0%  │ 7.3 MB   │ disabled │
│ TAC-agent        │ 5  │ fork │ 18349 │ online │ 0       │ 13D    │ 0%  │ 30.0 MB  │ disabled │
│ fix-mail-status  │ 6  │ fork │ 30451 │ online │ 0       │ 2h     │ 0%  │ 17.9 MB  │ disabled │
│ mga-log          │ 2  │ fork │ 18334 │ online │ 0       │ 13D    │ 0%  │ 3.3 MB   │ disabled │
│ scanner-log      │ 3  │ fork │ 18335 │ online │ 0       │ 13D    │ 0%  │ 18.9 MB  │ disabled │
│ sender_reputation│ 0  │ fork │ 18332 │ online │ 0       │ 13D    │ 0%  │ 17.6 MB  │ disabled │
└──────────────────┴────┴──────┴───────┴────────┴─────────┴────────┴─────┴──────────┴──────────┘
 Use `pm2 show <id|name>` to get more details about an app
============================================================
postfix   32152  0.0  0.2 136732 49124 ?        Ss   11:42   0:00 MaldunESG: master process sleeping
postfix   32153  2.5  4.9 943768 806212 ?       S    11:42   1:50 MaldunESG: waiting for messages
postfix   32159  2.6  4.9 950184 808264 ?       S    11:43   1:53 MaldunESG: waiting for messages
postfix   32162  2.6  4.9 943964 805824 ?       S    11:43   1:52 MaldunESG: waiting for messages
postfix   32165  2.6  4.9 943688 807336 ?       S    11:43   1:53 MaldunESG: waiting for messages
postfix   32168  2.6  4.9 943740 807468 ?       S    11:43   1:52 MaldunESG: waiting for messages
postfix   32171  2.6  4.9 943964 805660 ?       S    11:43   1:52 MaldunESG: waiting for messages
postfix   32174  2.6  4.9 943804 805592 ?       S    11:43   1:52 MaldunESG: waiting for messages
postfix   32177  2.6  4.9 943928 805800 ?       S    11:43   1:52 MaldunESG: waiting for messages
============================================================
Filesystem                                Size  Used Avail Use% Mounted on
/dev/mapper/sha--prod--esc--vs01--vg-root  279G   20G  246G   8% /
```

第三章：登录 ESG 系统

在正确配置了 ESG 系统，并在 ESG 配置界面中添加管理员用户后，用户即可在 Web 浏览器中输入：

http://<ESG 邮件安全网关 hostname 或 IP 地址>:8000

（注：8000 为端口号）

进入 ESG 管理系统。

在魔盾 ESG 页面上点击登录按钮后，用户/管理员将进入 ESG 系统的登录界面。

魔盾 ESG 管理系统用户名为管理员在配置 ESG 时添加的管理员用户名，密码缺省为“用户名”+“#maldun”。

登录框的下方列出了“技术支持”的邮件链接，当您有任何关于魔盾 ESG 系统的技术问题时，可以点击技术支持，发送邮件给我们。

我们建议您在第一次登录 ESG 系统后立即更改您的用户密码，并在之后定期更换密码，以保障您的用户信息安全。

如果您需要更改密码，请在登录 ESG 系统后点击您的用户名，之后在左侧菜单中选择“修改密码”。

之后您可以在修改密码的页面中更改您的登录密码。请保存好您的密码，并定期更新。

出于安全考虑，魔盾 ESG 系统对密码长度和密码字符组成做出了限制。如果用户输入的新密码不符合要求，系统会提示修改不成功，以及密码修改要求。我们建议管理员用户使用强健的不容易被猜到的密码。

当您成功更改后，系统会提示“密码修改成功”。

第四章： 用户设置

成功登录 ESG 系统后，您可以点击系统页面右上方您的 ESG 登录用户名，进入用户设置页面。用户设置页面包含以下标签页：

- 用户信息
- 修改密码
- 操作记录

1. 用户信息

用户信息包含了管理员用户的基本信息以及用户 ESG 产品的状态与使用情况等。

用户名	test1
激活日期	2017-04-02

域名	ESG状态	ESG有效期至
test.com	启用	2017-10-02
test1.com	启用	2017-10-02

用户名： 该用户/管理员的用户账号
激活日期：该用户/管理员所使用的 ESG 系统的激活时间，即该邮箱域名开始使用 ESG 邮件安全产品的时间

此外，用户信息页面列出了该用户/管理员所管理的属于该企业的邮件域名。包含域名、ESG 状态以及 ESG 有效期至。

域名：即 ESG 系统防护的（邮件）域名
ESG 状态：ESG 系统当前的状态，状态包括：启用，测试，失效，未启用等
ESG 有效期至：该邮件域名所使用 ESG 系统的有效期限。请确定 ESG 使用有效期与您和上海魔盾信息科技有限公司约定的日期一致。当 ESG 有效期即将结束时，请尽快与魔盾销售人员或售后工程师联系续期，以确保您可以正常接收邮件。

需要注意的是，一个用户/管理员可以管理多个邮件域名，当多个域名与该用户/管理员关联时，该页面将分别显示每个域名的相关信息。

2. 修改密码

修改密码页面支持管理员用户对 ESG 系统登录密码进行更改，关于修改密码的详细信息，请参考“第二章：登录 ESG 系统”

3. 操作记录

操作记录页面纪录了该用户/管理员在 ESG 系统中的所有操作纪录。

时间	源IP	操作
2016-12-13 20:37:09	114.92.191.226	delete mail: A669E840AF.A1025
2016-12-13 20:35:58	114.92.191.226	更改基本策略: 安全等级 -> 高
2016-12-13 20:35:56	114.92.191.226	更改基本策略: 安全等级 -> 中
2016-12-13 19:15:08	114.92.191.226	登入
2016-12-13 19:08:08	114.92.191.226	登出

主要操作记录类型包括：

登入/登出：即登录或退出 ESG 系统
策略操作：即添加，更改，删除基本策略，或自定义策略等。
邮件操作：即释放，删除邮件等

操作纪录页面显示如下信息：

时间：该操作的发生时间
源 IP：连接 ESG 系统进行该操作的 IP 地址
操作：具体的操作内容

第五章：使用 ESG

您可以在登录 ESG 系统后点击页面右上角的“管理 ESG”进入 ESG 管理界面。

ESG 管理界面包含以下功能：

- **信息概览**：用户邮件流处理信息概览
- **隔离邮件**：ESG 隔离邮件信息
- **高级威胁**：ESG 邮件高级威胁信息
- **统计报表**：ESG 邮件流量统计与分析
- **邮件追踪**：追踪查询 ESG 接收与处理的邮件
- **策略设置**：ESG 策略与自定义规则设置

在导航栏的右侧显示了当前用户/管理员所管理的邮件域名。

如果当前用户/管理员管理多个邮件域名，用户可以点击下拉菜单选择需要管理的域名。

1. 信息概览

魔盾 ESG 信息概览页面以组合仪表盘形式一目了然的呈现了一系列企业邮件相关的重要信息。要访问信息概览，请单击顶部导航栏中的“信息概览”。信息概览提供了对用户企业邮件的主要信息总结，包括邮件概括（所有邮件，拒收邮件，隔离邮件，投递邮件数据），以及邮件流量，隔离邮件原因和附件类型，高级威胁警报数量和最近的高级威胁信息等。您可以选择显示一天，一个星期，或过去的 30 天的邮件概览信息。

信息概览页面包含以下部分：

时间范围

信息概览页面缺省显示的数据时间范围是一星期，用户可以点击下拉菜单选择：一天，一星期，或一个月。信息概览页面将会切换显示相应时间范围内的邮件数据。

邮件概况

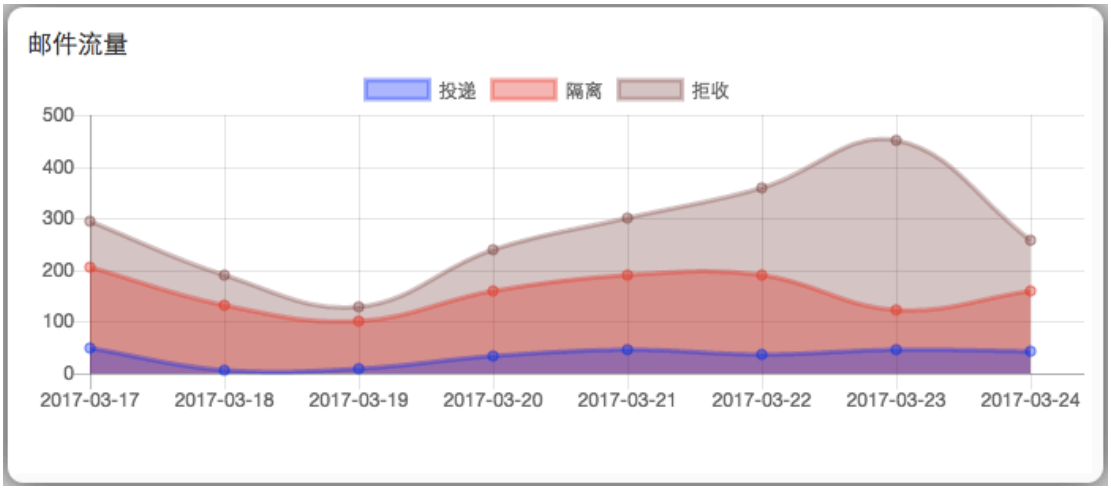
邮件概况包含用户该邮件域名在一定（“时间范围”中所选择的）时间范围内的邮件流量数据。其中包含（投递到该用户域名的）：

- **所有邮件**：该时间范围内 ESG 所接收到的邮件数量
- **拒收邮件**：该时间范围内 ESG 由于 SMTP 连接控制（RBL 黑名单，不符合标准 SMTP 协议规范的邮件连接等）所拒绝接收的邮件数量，以及百分比
- **隔离邮件**：该时间范围内 ESG 所接收并判定为威胁而隔离的邮件数量，以及百分比
- **成功投递**：该时间范围内 ESG 所接收，经过分析与过滤判定为正常邮件，并成功传递给用户的正常邮件数量，以及百分比

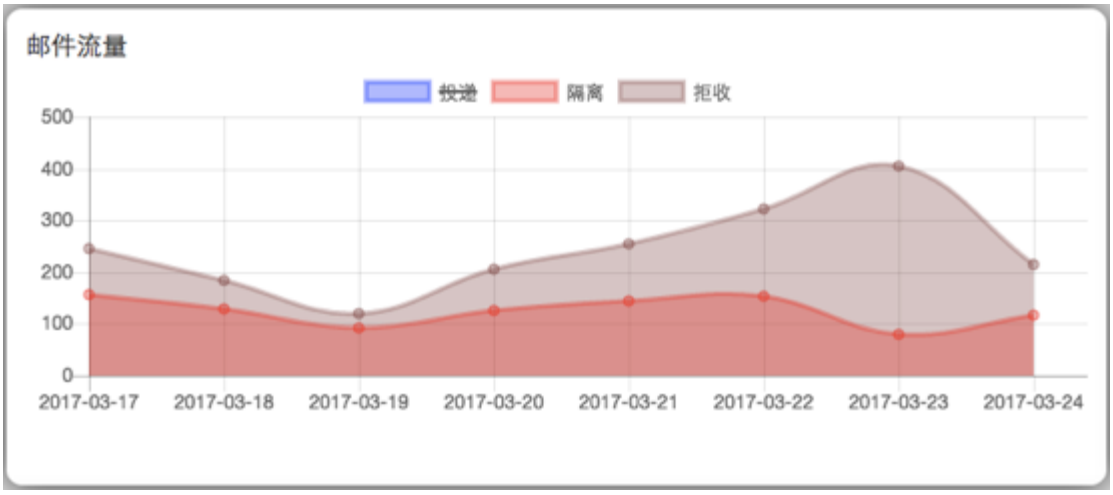
邮件流量

邮件流量以曲线堆栈图的形式呈现了在一定（“时间范围”中所选择的）时间范围内的邮件流量变化趋势。

曲线图的横轴代表时间，纵轴代表邮件量。曲线图以蓝色堆栈显示所有 ESG 投递的邮件流量，以亮红色堆栈显示 ESG 系统所隔离的邮件流量，以暗红色显示 ESG 系统所拒收的邮件流量。而所有颜色堆栈的总和显示了 ESG 系统所总计处理的邮件流量。用户可以将鼠标挪着流量图上的某一个数据点以查看该时间点各种邮件状态的具体邮件流量。



用户可以通过点击图表上方的一种邮件状态类型，（如“投递”及蓝色图标）选择隐藏该邮件状态类型堆栈，此时邮件流量图将只显示剩余两种邮件状态类型的流量趋势：



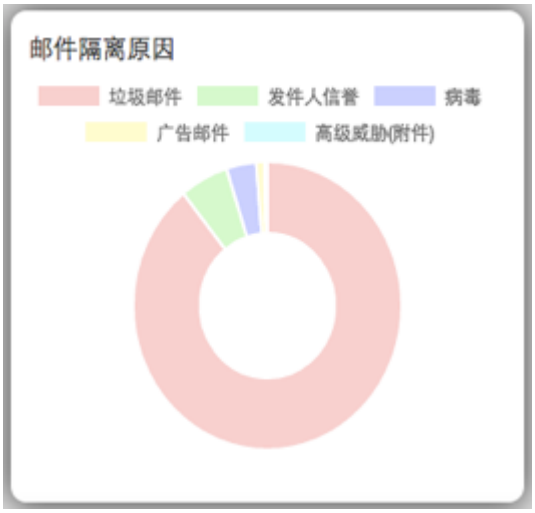
用户也可以通过点击图表上方的两种邮件状态类型，（如“投递”及蓝色图标，和“隔离”及亮红色图标）选择隐藏该两种邮件状态类型堆栈，此时邮件流量图将只显示剩余一种邮件状态类型的流量趋势：

隔离邮件类型

隔离邮件类型以环形图的形式按数量比例呈现了在一定（“时间范围”中所选择的）时间范围内的 ESG 所隔离的邮件中各类型邮件的分布。隔离邮件类型包括了：发件人信誉、垃圾邮件、病毒、高级威胁（附件）、高级威胁（URL）、广告邮件以及用户策略。

不同的隔离原因将通过不同色块进行区分，用户可以将鼠标挪至某一色块查看该类型隔离邮件在一定（“时间范围”中所选择的）时间范围内的具体数量。

用户可以点击图示中的一种或多种隔离原因，在图中隐藏由于该原因隔离的邮件，以帮助用户更灵活地对比特定隔离邮件原因类别。

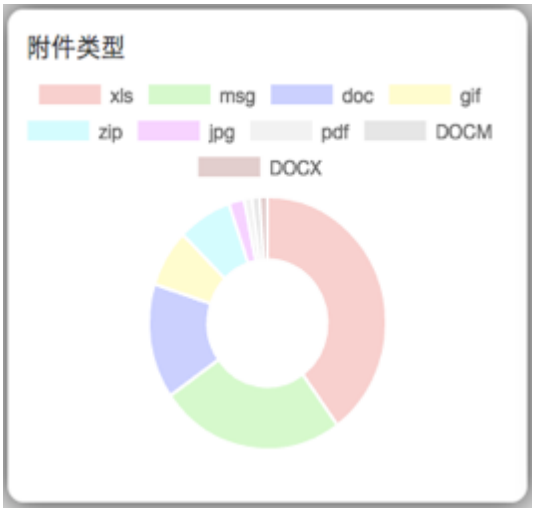


附件类型

附件类型以环形图的形式按数量比例呈现了在一定（“时间范围”中所选择的）时间范围内的 ESG 所处理的邮件所携带的附件中不同的附件类型（即附件文件扩展名或后缀），例如 zip、xls、doc、pdf 等。

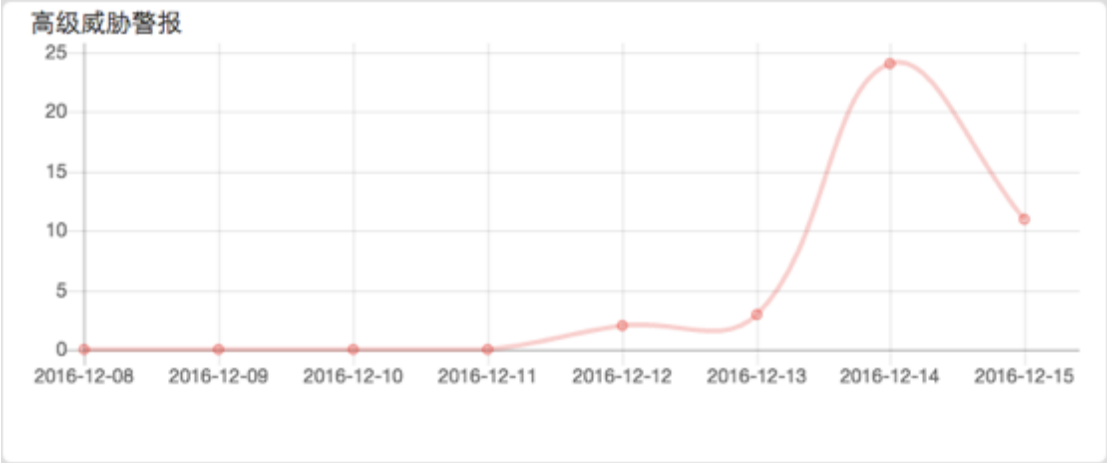
不同的附件类型将通过不同色块进行区分，用户可以将鼠标挪至某一色块查看该附件类型在一定（“时间范围”中所选择的）时间范围内的具体数量。

用户可以点击图示中的一种或多种附件类型，在图中隐藏包含该类型附件的邮件，以帮助用户更灵活的对比特定邮件附件类型数量区别。



高级威胁警报

高级威胁警报以曲线图的形式呈现了在一定（“时间范围”中所选择的）时间范围内的高级威胁事件数量，即通过 ESG 高级威胁分析，判定为高级威胁的邮件附件文件，或邮件中的 URL 链接。



高级威胁通常是经过 ESG 反病毒扫描以及反垃圾邮件扫描，而未被判定为病毒邮件和垃圾邮件的用户邮件中所包含的未知威胁。魔盾 ESG 通过动态高级威胁分析，查询魔盾高级威胁数据库和通过魔盾 TAC 实时虚拟执行附件文件和 URL 链接，以判断邮件是否隐藏可能危害客户网络和系统的高级威胁。

需要注意的是，当一封邮件中包含多个附件和 / 或链接时，可能触发超过一个高级威胁警报，即高级威胁警报与邮件中包含的附件文件或 URL 链接相关。

最近的高级威胁

最近的高级威胁显示了该用户域名所收到的邮件中检测出的最近 5 个高级威胁，包括威胁传递形式，即通过邮件附件或 URL 传递；以及威胁内容，即附件文件名或 URL 链接。

2. 隔离邮件

隔离邮件页面显示了所有 ESG 系统所隔离的邮件的相关信息。要访问隔离邮件，请单击顶部导航栏中的“隔离邮件”。隔离邮件中包括发件人信誉，垃圾邮件，病毒邮件，广告邮件，高级威胁邮件，或根据用户自定义策略所隔离的邮件。隔离邮件页面包含了隔离邮件的基本信息、隔离原因、隔离邮件分析、预览以及释放和删除操作的功能。

2.1. 隔离邮件查询

隔离邮件页面的上方提供了针对特定时间范围、特定隔离原因以及特定关键字的隔离邮件查询，可以帮助用户快速定位符合查询条件的隔离邮件。

时间

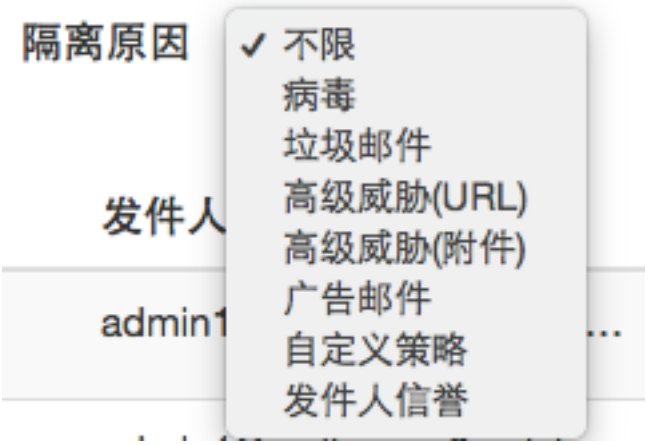
ESG 提供了三个时间范围的隔离邮件查询：一天，一星期（缺省选择），一个月。

需要注意的时，除非特别协定，超过一个月的用户隔离邮件将被删除，隔离邮件页面也将无法提供超过一个月前的隔离邮件查询。

隔离原因

ESG 系统支持通过以下原因隔离用户邮件：

- 垃圾邮件：邮件被 ESG 判定为垃圾邮件（即通过 ESG 垃圾邮件分析，该邮件是垃圾邮件的概率超过用户设定垃圾邮件防御等级所关联的阈值）
- 病毒：邮件被 ESG 判定为包含病毒
- 高级威胁（URL）：邮件被 ESG 判定为包含高级威胁 URL/链接，通常为恶意网站，钓鱼网站，和其他危险网页链接等
- 高级威胁（附件）：邮件被 ESG 判定为包含高级威胁附件文件，通常为恶意软件（勒索软件，APT 等），包含恶意代码的文档等
- 广告邮件：邮件被 ESG 判定为广告邮件
- 自定义策略：由于用户设置的自定义策略而被隔离的邮件，由于用户自定义策略在 ESG 其他分析模块之前处理邮件，所以该邮件通常未经过 ESG 其他分析模块扫描
- 发件人信誉：邮件被 ESG 发件人信誉系统判定为来自低信誉发件人。



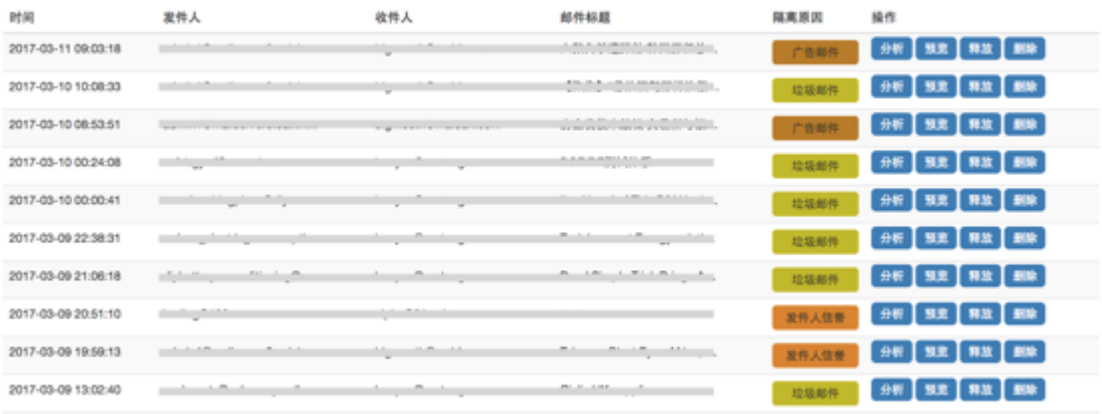
用户可以通过点击隔离原因下拉菜单选择查询因为特定原因隔离的邮件。在查询结果中，ESG 系统也将以不同颜色的标签显示不同的隔离原因，以帮助用户快速区分由于不同原因而隔离的邮件。

关键字

隔离邮件页面支持用户根据邮件标题，发件人/发件地址，收件人/收件地址中包含的关键字对 ESG 系统隔离的邮件进行查询，用户可以输入所需要查询的关键字，点击“搜索”。

2.2. 隔离邮件信息

隔离邮件信息部分显示了当前查询条件下所有的 ESG 隔离邮件。



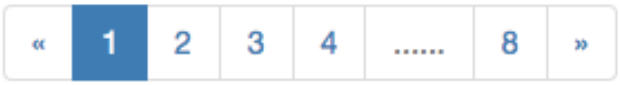
隔离邮件页面显示的信息包括：

- **时间**：该邮件被 ESG 系统所分析与处理的时间，时区为 GMT。

- **发件人**：该邮件的发件人邮件地址（信封地址，即 Envelope From）
- **收件人**：该邮件的收件人邮件地址（信封地址，即 Envelope To）
- **邮件标题**：该邮件的主题或标题（Subject）
- **隔离原因**：该邮件被隔离的原因，包括垃圾邮件、病毒、高级威胁（URL）、高级威胁（附件）、广告邮件 d、发件人信誉、以及自定义策略
- **操作**：ESG 系统支持管理员/用户对该隔离邮件的操作

隔离邮件页面缺省按时间倒序每页显示最多 50 封隔离邮件的信息，如果当前时间范围内的隔离邮件超过 50 封，隔离邮件信息将会分页显示。

用户可以点击页面顶部右侧，或底部右侧的页码选择翻页显示，或 直接点击页码跳转到某一页。



2.3. 隔离邮件操作

ESG 系统支持用户对一封隔离邮件进行如下操作：

操作 — 分析

用户可以通过“分析”操作了解 ESG 系统对该邮件处理过程中的各项分析信息。当用户点击“分析”按钮时，用户浏览器将在一个新的标签页中打开该邮件的分析信息。信息包括：

- 发件人信誉系统
- 垃圾邮件分析
- 病毒分析
- 钓鱼分析
- 高级威胁分析

＊发件人信誉系统 (Sender Reputation)

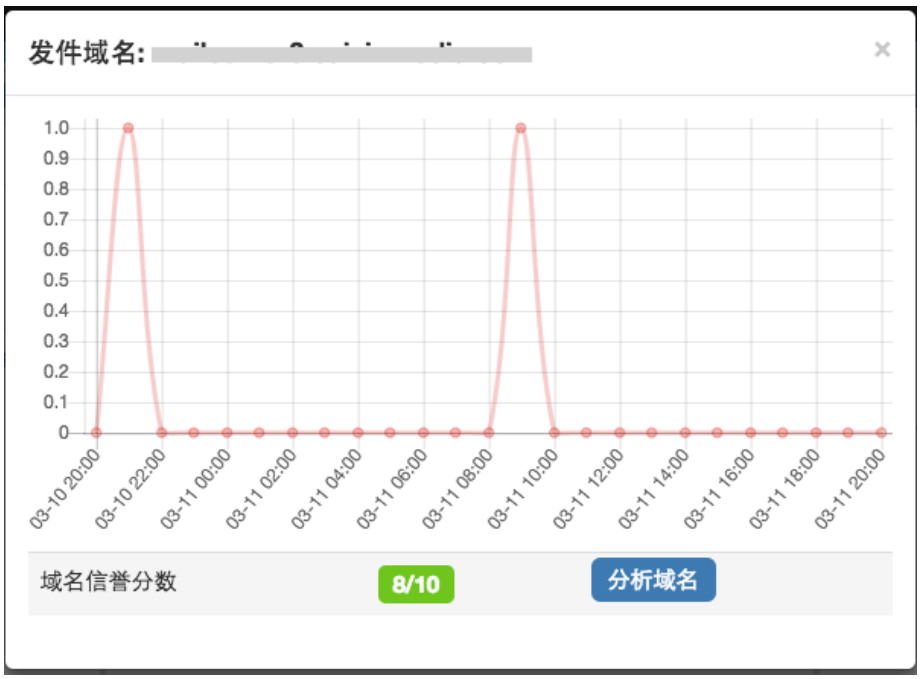
当用户打开邮件分析页面时，该邮件的发件人信誉信息以及综合信誉评级将会实时生成，发件人信誉系统信息包括：

- 发件域名：该邮件发件人邮件地址的域名，该域名的信誉评级
- 连接 IP：该邮件连接到魔盾 ESG 系统的 IP 地址，该 IP 的信誉评级
- 发件地址：该邮件的发件人邮件地址（Envelope From），该发件地址的信誉状态
- 收件地址：该邮件的收件人邮件地址（Envelope To），该收件地址的状态
- 发收件人关系：ESG 系统通过机器学习判定的发件人与收件人之间的邮件关系
- 发件人综合信誉：ESG 系统通过该邮件的发件域名、连接 IP、发件地址、收件地址、以及发收件人关系所综合判定的相对于该邮件收件用户的发件人综合信誉评级

其中发件域名，连接 IP，以及发件人综合信誉，以蓝色状态进度条的形式呈现，蓝色进度条越接近右侧，代表信誉越高，蓝色进度条越接近左侧，代表信誉越低。用户可以将鼠标挪至进度条上方，查看具体的信誉数值。ESG 发件人信誉系统是一套 0-10 分制的信誉系统，信誉数值越接近 10，信誉越高；信誉数值越接近 0，信誉越低。

此外，用户可以点击信誉状态右侧的放大镜图标，对该信誉因素进行分析。

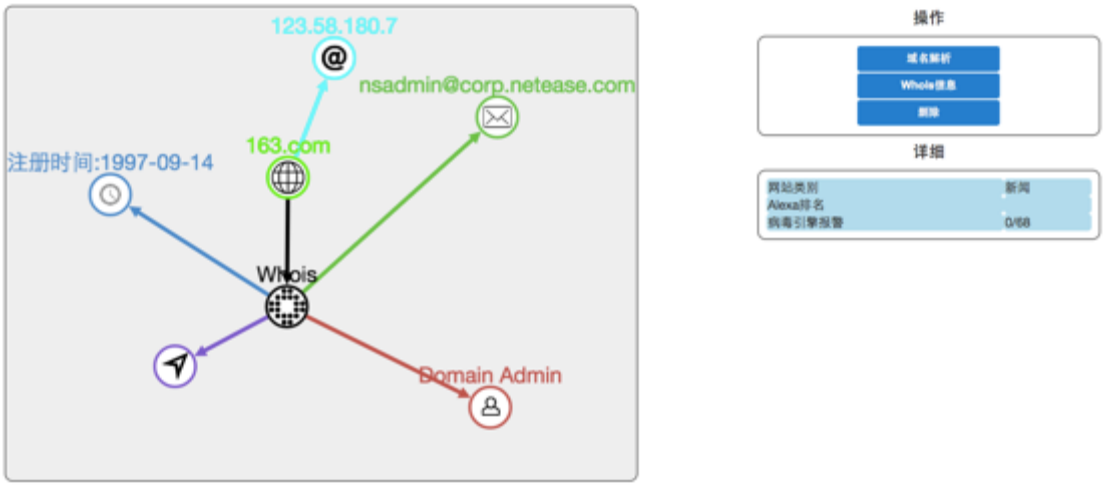
当用户点击发件域名信誉图标右侧的放大镜图标时，ESG 系统会弹出窗口显示来自该发件域名最近 24 小时内的邮件流量信息，实时域名信誉分数，以及“分析域名”按钮。



邮件流量图的横轴表示时间（最近的 24 小时，每个小时为一个节点），纵轴表示邮件数量。

域名信誉分数以数字的形式呈现当前查看域名的实时信誉数据。（最高为 10，信誉数值越接近 10，信誉越高；信誉数值越接近 0，信誉越低。）

用户可以点击“分析域名”按钮对该域名进行互动视图分析。互动视图分析页面的左侧是视图部分，显示了分析元素节点；页面右侧上方是操作部分，显示了针对视图中某一个节点可以执行的操作；页面右侧下方是详细部分，显示了视图中选中节点的详细信息。



魔盾 ESG 的域名互动视图分析功能提供了对该域名信息的动态查询和关联功能。

对于视图中的任一域名，互动视图分析系统提供三种操作：

- 域名解析：解析该域名所对应的 IP 地址
- Whois 信息：查询该域名的注册信息
- 删除：在视图中删除该域名节点

域名在视图中以地球图标表示，当用户在视图中选中一个域名时，页面右下方的“详细”区域将提供以下详细信息：

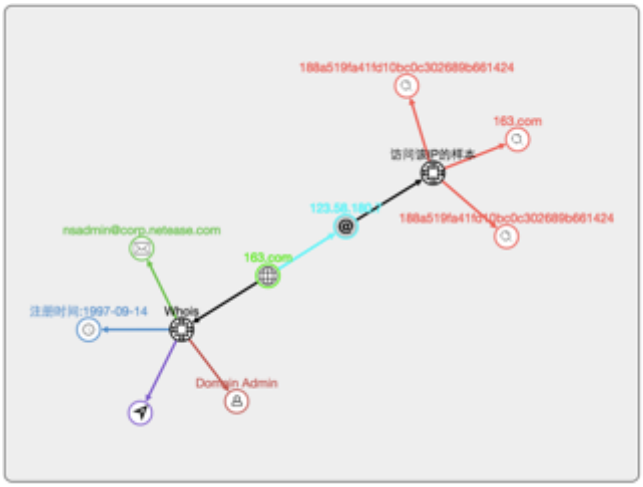
- 网站类别：该域名相关网站的类别
- Alexa 排名：该域名的 Alexa 全球域名排名
- 病毒引擎报警：该域名是否被列入全球各网络安全机构的域名黑名单中

当用户在视图中选中一个域名，在页面右上方的操作区域点击“域名解析”后，互动视图分析系统将会尝试解析该域名所对应的 IP 地址，并将 IP 地址显示在视图中。

当用户在视图中选中一个域名，在页面右上方的操作区域点击“Whois 信息”后，互动视图分析系统将会尝试查询该域名的 Whois 信息，即该域名的注册信息，并将信息显示在视图中。Whois 信息包括：

- 注册时间：该域名申请注册的时间（在视图中以钟表图标表示）
- 注册人：该域名的拥有者（在视图中以人型图标表示）
- 注册邮箱：该域名注册时的联系邮箱（在视图中以邮件图标表示）
- 注册地点：该域名所处的地理位置（在视图中以定位箭头图标表示）

当用户对视图中的域名进行了域名解析后，可以进一步对域名解析得到的 IP 做分析。



对于视图中的任一 IP， 互动视图分析系统提供四种操作：

- IP 信息：查询该 IP 的相关信息
- 反向域名解析：通过 IP 反向查询有哪些域名关联在该 IP 上
- 访问该 IP 的样本：查询魔盾系统所分析过的样本行为中访问过该 IP 的样本
- 删除：在视图中删除该 IP 节点

当用户在视图中选中一个 IP 时，页面右下方的“详细”区域将提供以下详细信息：

- ASN：该 IP 所属的自治网络编号
- ASN 拥有者：该 IP 所属的自治网络拥有者
- 经纬度：该 IP 所处的位置坐标

当用户在视图中选中一个 IP，在页面右上方的操作区域点击“IP 信息”后，互动视图分析系统将会尝试查询关于改 IP 的信息。

当用户在视图中选中一个 IP，在页面右上方的操作区域点击“反向域名解析”后，互动视图分析系统将会尝试查询解析到该 IP 的所有域名，并将域名显示在视图中。用户可以在视图中点击“反向域名解析”查询出的域名，并对该域名做进一步的分析。

当用户在视图中选中一个 IP，在页面右方的操作区域点击“访问该 IP 的样本”后，互动视图分析系统将会尝试查询魔盾威胁分析云系统（Threat Analysis Cloud, 简称 TAC），找出所有在 TAC 威胁行为分析中尝试访问该 IP 的文件或 URL 样本，并将样本显示在视图中。

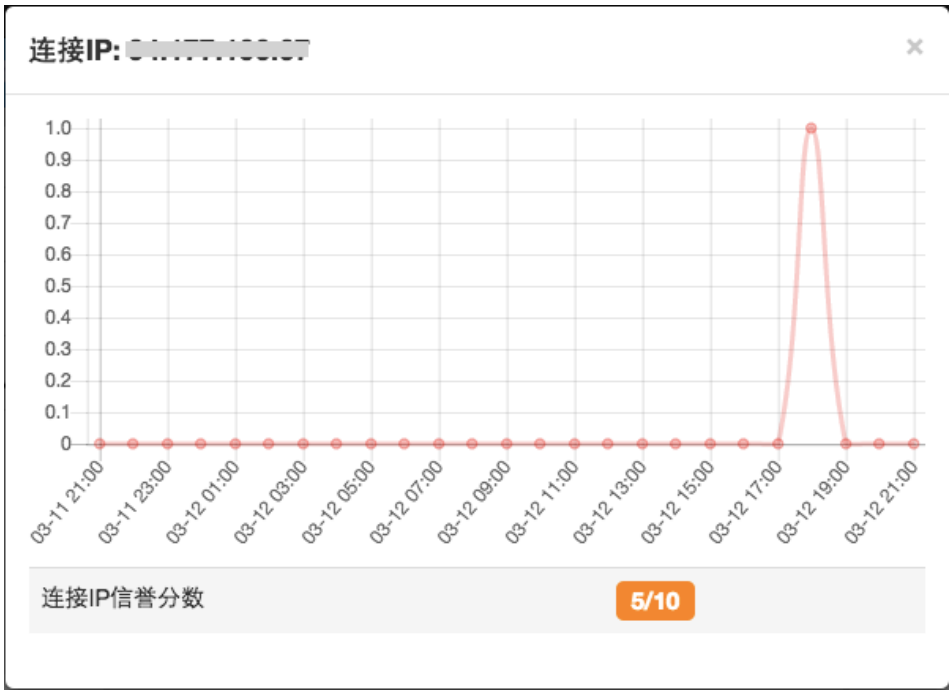
样本将在视图中以放大镜图标表示，文件样本在视图中显示为该文件的 MD5 哈希值，URL 样本在视图中显示为 URL 链接。用户可以点击一个样本，并对

这个样本的信息与特征做进一步分析。对样本的互动视图分析，请参考“高级威胁”章节的“视图分析”功能。

当互动视图分析中有超过 10 个查询结果返回时，视图将只显示 10 个元素节点。

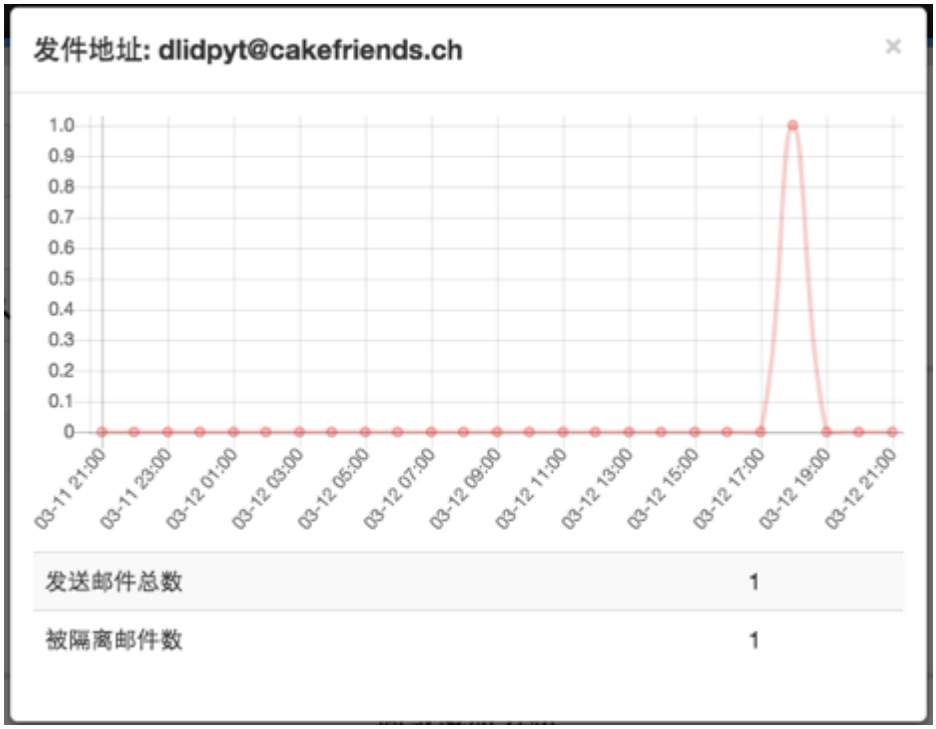
对于视图中的每一个元素节点，用户都可以点击页面右侧操作区域的“删除”按钮，将该元素节点从视图中删除。该元素节点所衍生出的后续视图分析节点也将被删除。

当用户点击连接 IP 信誉图标右侧的放大镜图标时，ESG 系统会弹出来自该发件域名最近 24 小时内的邮件流量信息，以及实时 IP 信誉分数。

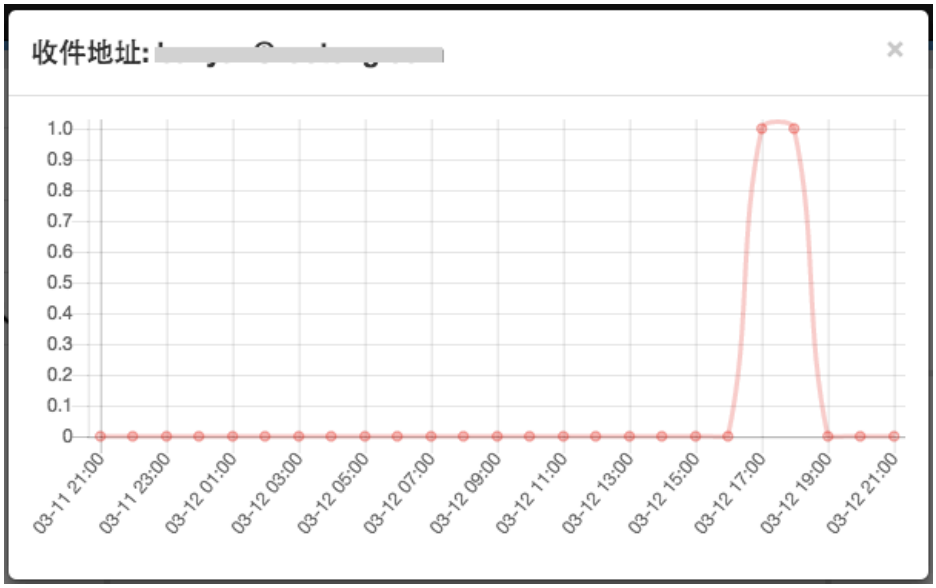


对于发件人信誉系统中的发件地址，收件地址，以及发收件人关系，魔盾 ESG 发件人信誉系统通过历史邮件数据自动识别与学习，对发件频率，发件状态，收件状态等信息进行分析，生成评级。评级状态包括：正常，未知，可疑等。

此外，当用户点击发件地址信誉状态右侧的放大镜图标时，ESG 系统会弹出窗口显示来自该发件地址最近 24 小时内的邮件流量信息，该发件地址 24 小时内发送的邮件总数，以及该发件地址 24 小时内发送的邮件中被隔离的邮件总数。



当用户点击收件地址信誉状态右侧的放大镜图标时，ESG 系统会弹出发送到该收件地址最近 24 小时内的邮件流量信息 。



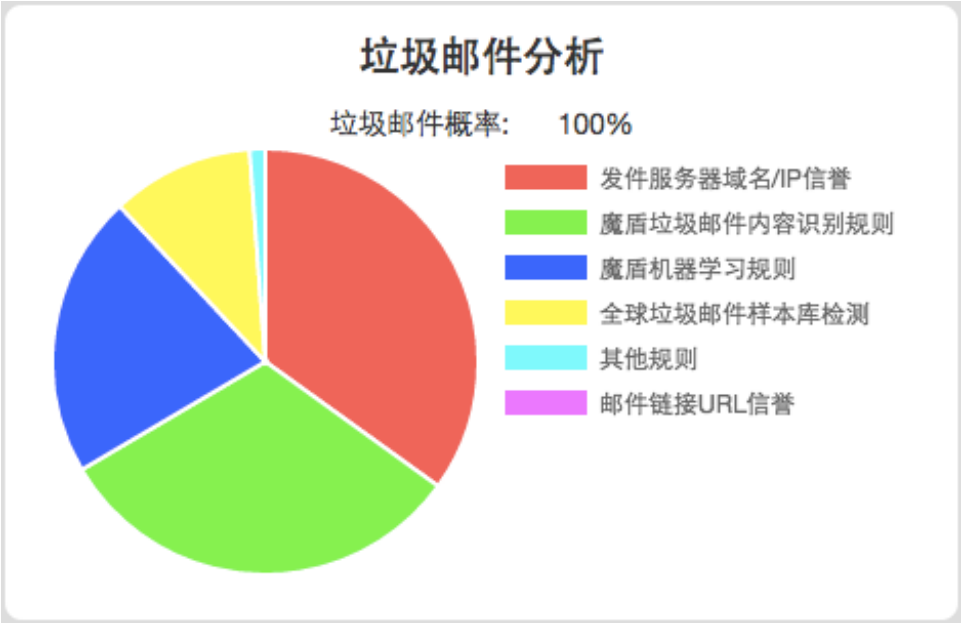
最后， ESG 发件人系统通过该邮件的发件域名、连接 IP、发件地址、收件地址、以及发收件人关系所综合判定和生成相对于该邮件收件用户的发件人综合信誉评级。

需要注意的时，即使用户并未在策略设置中开启发件人信誉拦截，发件人信誉信息也将在隔离邮件分析页面中显示，并且发件人综合信誉评级为页面生成时动态实时计算，最终评级可能会因时间发生变化。

＊垃圾邮件分析 (Anti-Spam)

如果该邮件经过了 ESG 垃圾邮件分析（策略设置中开启了垃圾邮件分析），垃圾邮件分析部分计算并显示了 ESG 判定该邮件为垃圾邮件的概率。

ESG 垃圾邮件概率是由 ESG 系统通过深度和全面的垃圾邮件扫描，计算各项垃圾邮件因素综合计算而成的概率分数。概率越大，该邮件是垃圾邮件的可能性越大；概率越小，该邮件为垃圾邮件的可能性越小。ESG 缺省情况下将隔离垃圾邮件概率超过 50%的邮件（即垃圾邮件防护等级：中），用户可以在策略设置中进行更改。



垃圾邮件分析部分还以饼图的形式呈现了 ESG 垃圾邮件分析各模块在判定垃圾邮件概率时所起到的作用和分值所占比例，并以颜色区分，以此帮助用户更准确的理解该邮件被 ESG 系统判定为垃圾邮件的原因。ESG 垃圾邮件分析模块包括了：

魔盾垃圾邮件内容识别规则：由魔盾自行开发和维护的垃圾邮件内容识别规则。魔盾通过分析垃圾邮件特征和模式，针对垃圾邮件的不同组成部分开发了超过 5 万条的垃圾邮件内容规则，并保持每日更新。

魔盾机器学习规则：由魔盾自行开发的机器学习算法，通过机器自动学习垃圾邮件和正常邮件样本区别而生成机器学习规则。魔盾机器学习算法将不断自我调整和更新学习内容，以阻挡新的垃圾邮件和改善误判/漏判情况。

发件服务器域名/IP 信誉：由魔盾 ESG 综合自有信誉系统以及第三方黑名单，RBL 等生成的发件人信誉系统。通过发件人信誉系统对垃圾邮件发件服务器和/或发件域名/IP 进行识别，而生成的针对垃圾邮件概率的分数。

全球垃圾邮件样本库检测：由魔盾 ESG 通过不同的指纹算法，计算垃圾邮件指纹，并通过比对全球垃圾邮件样本库指纹，而生成的针对垃圾邮件概率的分数。

邮件链接 URL 信誉：由魔盾 ESG 通过查询邮件中包含的 URL 在全球 URL 信誉库及黑名单中的信息，而生成的针对垃圾邮件概率的分数。

其它规则：其它第三方垃圾邮件规则。

魔盾 ESG 垃圾邮件分析通过以上模块对用户邮件进行实时扫描和分析，最终生成 ESG 垃圾邮件概率，并通过垃圾邮件概率判定是否隔离该邮件。用户可以直观的通过饼图了解各模块在垃圾邮件判定中所占比例。用户可以点击屏蔽其中一个或几个模块，显示其余模块在 ESG 垃圾邮件判定中所占的比例大小。

如果该邮件没有经过 ESG 垃圾邮件扫描（策略设置中关闭了垃圾邮件分析，或用户选择直接投递/白名单特定邮件），垃圾邮件分析部分将显示：未经过垃圾邮件分析。

＊病毒分析 (Anti-Virus)

如果该邮件经过了 ESG 病毒分析（策略设置中开启了病毒分析，邮件经过垃圾邮件分析且未被判定为垃圾邮件），并被 ESG 判定为病毒，病毒分析部分将显示魔盾 ESG 系统对该邮件附件部分的病毒分析。

ESG 病毒分析包括了 ESG 通过 ClamAV 引擎附件文件扫描所得到的扫描结果。如果 ClamAV 防病毒引擎判定邮件附件文件包含病毒，病毒分析部分将显示 ClamAV 扫描结果。

ESG 病毒分析还包括了魔盾威胁附件类型和威胁附件文件检查。如果 ESG 检测到邮件中包含可能危害用户的威胁附件类型和威胁附件文件，该邮件将被判定为病毒，病毒分析部分将显示 ESG 检测内容和病毒原因。

如果该邮件经过了 ESG 病毒分析且未被判定为病毒邮件，或该邮件没有经过 ESG 病毒分析（策略设置中关闭了病毒分析，用户选择直接投递/白名单特定邮件，或该邮件在垃圾邮件分析中已被判定为垃圾邮件），病毒分析部分将显示：未发现病毒特征。

＊钓鱼分析 (Anti-Phishing)

如果该邮件经过了 ESG 钓鱼分析（策略设置中开启了钓鱼分析），并被 ESG 判定包含钓鱼威胁，钓鱼分析部分将显示 ESG 系统对该邮件的钓鱼信息分析。

魔盾 ESG 钓鱼分析包含了启发式钓鱼站点检测，发件人一致性检查，URL 分析，HTML 分析等。钓鱼分析部分会向用户显示 ESG 钓鱼分析的检测到钓鱼的具体原因。

如果该邮件经过了 ESG 钓鱼分析且未被判定为钓鱼邮件，或该邮件没有经过 ESG 钓鱼分析（策略设置中关闭了钓鱼分析，用户选择直接投递/白名单特定邮件），病毒分析部分将显示：未发现钓鱼特征

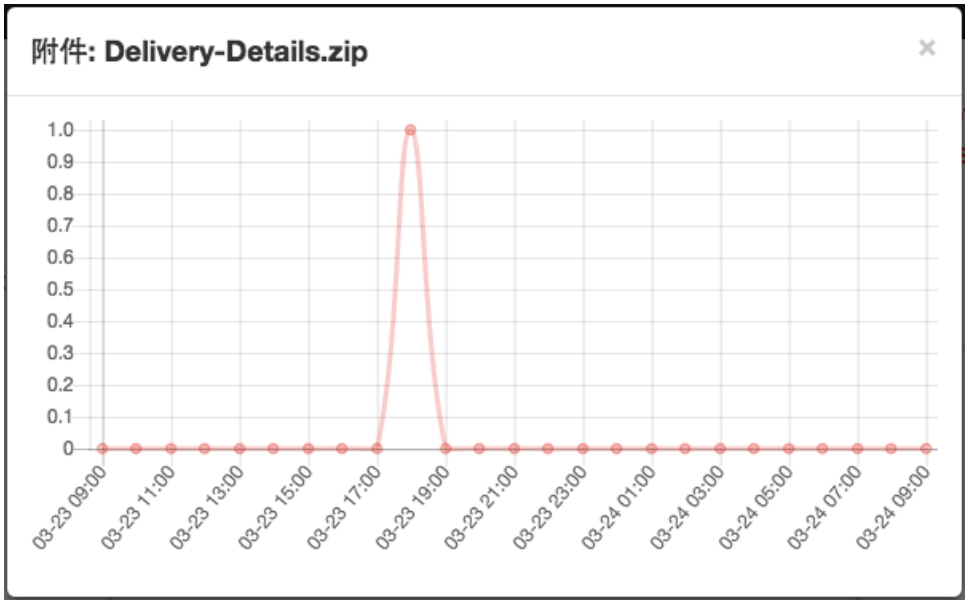
＊高级威胁分析 (Advanced Threat Anslysis)/Anti-APT

高级威胁分析是魔盾 ESG 通过对邮件附件和 URL 在魔盾 Threat Analysis Cloud (TAC) 系统中的实时动态分析而生成的。高级威胁分析信息包括：附件分析和链接分析

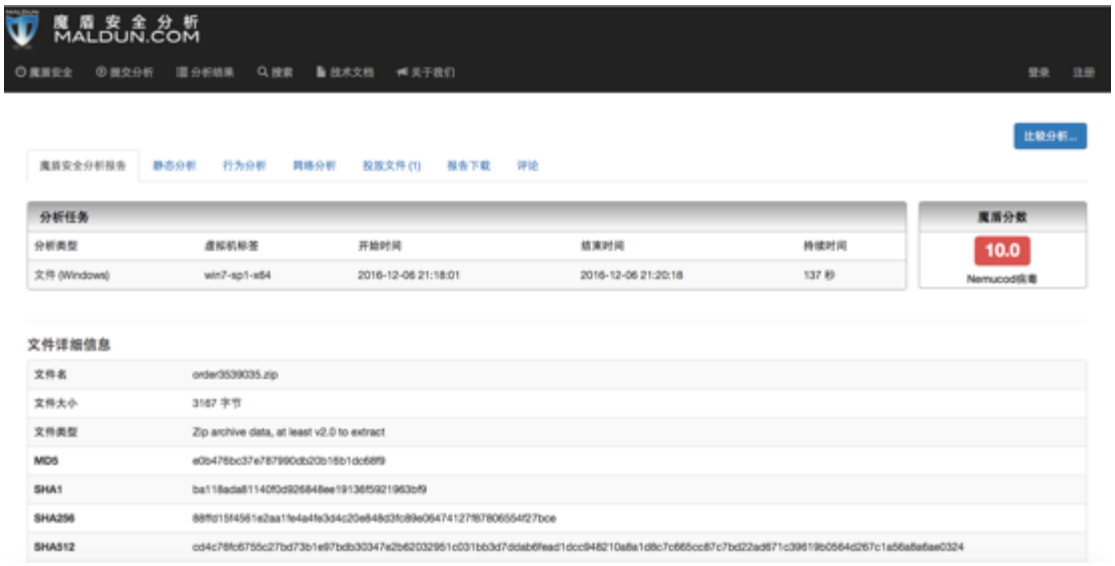
附件

附件部分列出了该邮件所包含的全部附件的信息，包括附件文件名、附件文件大小以及附件文件的 MD5 值。

用户可以点击附件的文件名，查看该附件最近 24 小时内在 ESG 系统中的流量状况。该流量分析可以帮助用户了解附件的传播状况（如大范围转播，或高针对性传播等）。



如果该附件附件经过了 ESG 高级威胁分析，页面信息中还将包括威胁等级，即魔盾安全分析分数；该威胁所属的病毒家族，即威胁类型；以及查看魔盾安全分析报告的按钮。点击“查看魔盾安全分析报告”按钮，用户浏览器将在一个新的标签页中打开该文件经过魔盾安全分析生成的详细分析报告。



了解更多魔盾安全分析报告的相关信息，请访问：
https://maldun.com/submit/help/#maldun-report

如果 ESG 没有在邮件中发现任何附件，则附件部分显示“该邮件不包含附件”。

链接

链接部分列出了该邮件所包含的全部 URL 链接的信息，包括链接本身，如果 ESG 判定链接为高级威胁，ESG 高级威胁信息（如恶意网站等）将会显示在链接之后。

为了帮助用户了解该链接所指向的网站的信誉及其他信息，ESG 链接部分还增加了一个“查询网站信誉”功能。点击“查询网站信誉”按钮，用户浏览器将在一个新的标签页中打开该 URL 在 WPING.ORG 网络信誉评级系统上的信誉及网站分析信息。

WPING.ORG 网络信誉评级系统 (https://www.wping.org) 是魔盾打造的基于域名和 IP 的信誉，及网站安全查询平台。了解更多 WPING.ORG 的使用方法，请访问：
https://www.wping.org/help/

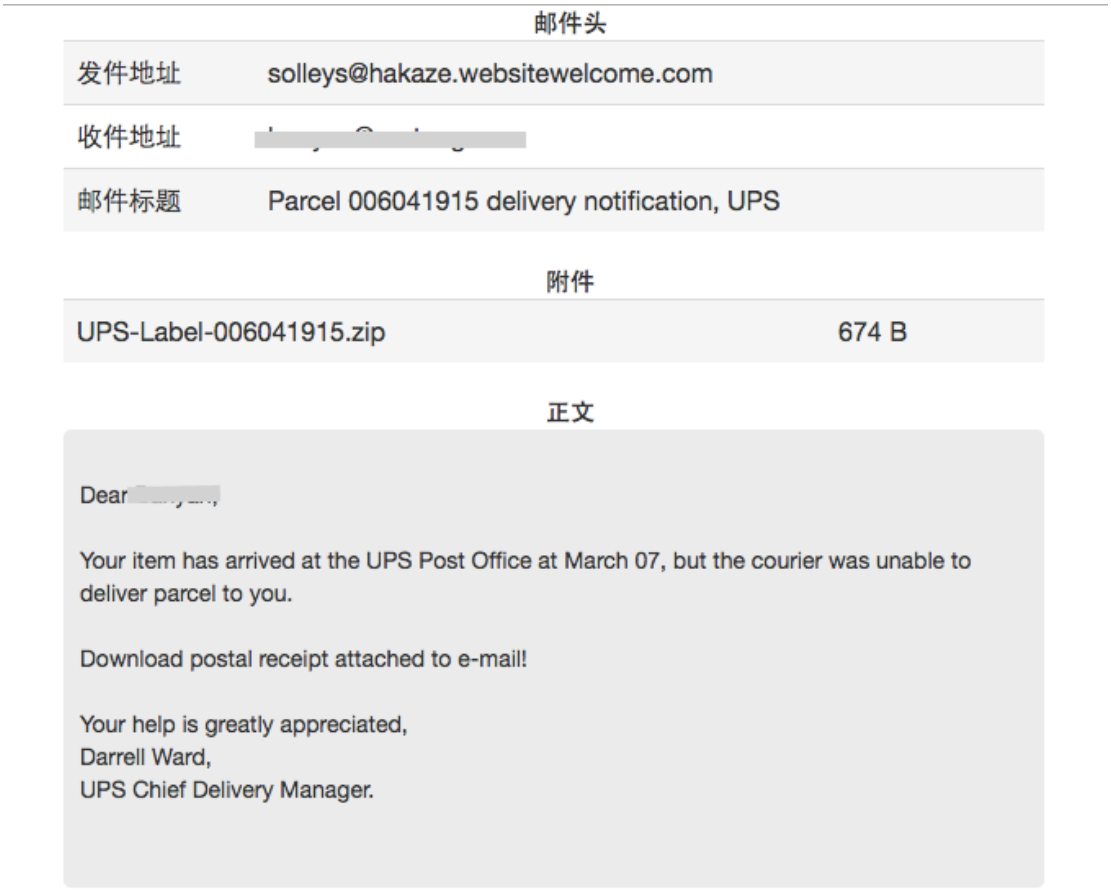
如果 ESG 没有在邮件中发现任何链接，则链接部分显示“该邮件不包含链接”。

操作 — 预览

ESG 给用户提供了邮件内容预览功能，方便用户查看具体的邮件内容，以确定该邮件是否为误判正常邮件或是否需要释放。

当用户点击隔离邮件信息中操作栏的“预览”按钮时，ESG 将会在浏览器中打开一个新的标签页，以显示该邮件的预览信息。

需要注意的是，为了保障用户安全，预览页面为纯文本显示。Html 格式的邮件也将被转换为文本格式。



预览信息包括了

邮件头： 其中包含：

发件地址：该邮件的发件人邮件地址（Envelope From）
收件地址：该邮件的收件人邮件地址（Envelope To）
邮件标题：该邮件的标题或主题

附件：

该邮件中所包含的所有附件文件名，以及附件文件大小。

正文：

该邮件中所包含的正文内容。

操作 — 释放

ESG 系统支持用户/管理员释放隔离区中的邮件。当用户/管理员确定需要收到隔离区中的邮件时，可以点击隔离邮件信息中操作栏的“释放”按钮，ESG 系统会提示用户/管理员是否确定释放该邮件，当用户/管理员选择“确定”时，该邮件将被 ESG 从隔离区中释放，并发送到该邮件的收件地址；当用户/管理员在提示页面选择“取消”时，该邮件将不会被释放。

当邮件被用户/管理员从隔离区中释放后，该邮件将不会再出现在隔离区中。

操作 — 删除

ESG 系统支持用户/管理员删除隔离区中的邮件。当用户/管理员确定不再需要隔离区中的邮件，希望删除隔离区中的邮件时，可以点击隔离邮件信息中操作栏中的“删除”按钮，ESG 系统会提示用户/管理员是否确定删除该邮件，当用户选择“确定”时，该邮件将被 ESG 系统从隔离区中删除；当用户在提示页面选择“取消”时，该邮件将不会被删除。

当邮件被用户/管理员从隔离区中删除后，该邮件将不会再出现在隔离区中。

3. 高级威胁

高级威胁页面显示了所有 ESG 系统所检测到的高级威胁的相关信息。要访问高级威胁页面，请单击顶部导航栏中的“高级威胁”。

高级威胁页面纪录了 ESG 所处理的用户邮件中包含的高级威胁。高级威胁是魔盾 ESG 将邮件中的附件文件 / 网页链接通过魔盾 Threat Analysis Cloud 实时分析，根据威胁等级与威胁报告将可能对用户产生威胁的事件返回警示的功能模块。

高级威胁是对 ESG 用户更深层的安全保障。高级威胁通常在垃圾邮件分析和病毒/钓鱼分析之后，即该邮件并未被判定为垃圾邮件或病毒。由于一些未知威胁利用零日漏洞，高级持续性攻击，针对性攻击，社会工程学攻击等方式通过附件或链接传递，很难被常规的垃圾邮件与病毒引擎检测到，因此 ESG 高级威胁分析以实时沙盒行为分析加威胁情报的方式对邮件中的附件和链接进行动态分析，以确保附件或 URL 中不包含威胁。 高级威胁中包括附件文件威胁，和链接威胁。

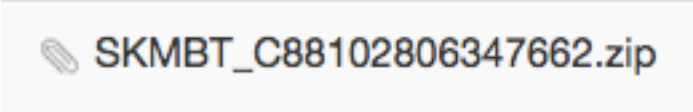
同样的，高级威胁页面缺省按时间倒序每页显示最多 50 条高级威胁信息，如果当前时间范围的高级威胁信息超过 50 条，高级威胁页面将会分页显示。

用户可以点击顶部右侧，或底部右侧的页码选择翻页显示。向左的双箭头表示第一页，向右的双箭头表示最后一页。用户也可以直接点击跳转到某一页。

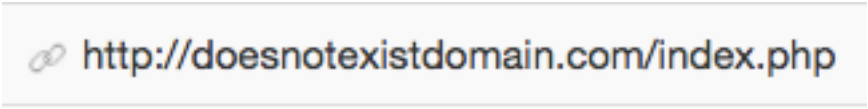
高级威胁信息中显示以下信息：

时间：ESG 系统检测到高级威胁的时间，时区为 GMT。

威胁文件/URL：ESG 系统检测到的威胁所使用的附件文件名称，或 URL 链接。当高级威胁以附件文件形式传递时，“威胁文件/URL”如下图所示：



当高级威胁以 URL 链接形式传递时，“威胁文件/URL”如下图所示：

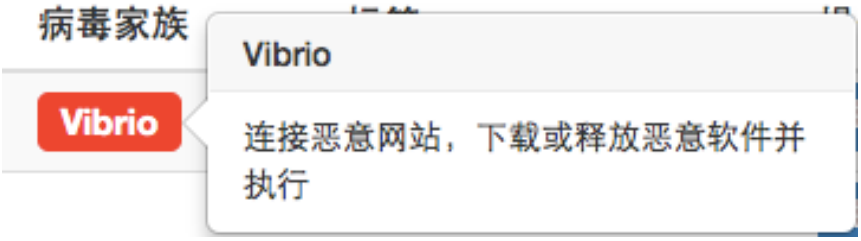


威胁等级：ESG 系统所评估的高级威胁对用户的危害等级。

魔盾 ESG 高级威胁页面以红色状态进度条的形式呈现威胁等级，红色进度条越接近右侧，威胁等级越高，红色进度条越接近左侧，威胁等级越低。

用户可以将鼠标挪至威胁等级进度条上方，查看具体的魔盾威胁分数。ESG 魔盾威胁分数通常代表了样本可能的危害程度或样本为恶意软件/恶意链接的概率。魔盾威胁分数在 0 到 10 分范围内，分数越低通常危害越低，而分数越高通常危害越高。当魔盾威胁分数在 6 分到 10 分范围时，我们通常认为该样本是危险的或恶意的(携带病毒，具有攻击性，或被用来传播恶意软件)，建议用户加强防范。

病毒家族：如果 ESG 系统检测到该威胁符合某一种特定的威胁类型特征时，将会显示该病毒家族名称（通常为描述该病毒种类或变种的名称 ），以方便用户了解威胁特性。用户可以将鼠标挪至病毒家族名称上方，查看该病毒家族的具体威胁特征。



ESG 用户/管理员可以点击高级威胁页面上的病毒家族名称，进入该病毒家族的详细信息页面。病毒家族页面显示以下信息：

- 标签：该病毒家族的特征标签，即通常被定义的威胁类型，如木马，蠕虫，广告软件，勒索软件等
- 平台：该病毒家族通常传播和感染的操作系统平台
- 常见威胁形式：该病毒家族的常见威胁行为特征
- 详细说明：该病毒家族的详细介绍，命名原因等

此外，病毒家族页面还以流量图的形式展现了 30 天内 ESG 所检测出的属于该病毒家族的高级威胁流量。

最后，病毒家族页面列出了最近的 10 个属于该病毒家族的高级威胁样本，用户可以点击“查看报告”，或“视图分析”对指定样本进行更深入的分析。

操作

ESG 系统支持用户对一个高级威胁事件进行如下操作：

操作 — 邮件信息

邮件信息可以帮助用户了解包含该高级威胁的邮件的信息。 当用户点击“邮件信息“按钮时，用户浏览器将在一个新的标签页中打开该邮件的分析信息。该信息页面与隔离邮件操作中的“操作 — 分析” 功能所生成的页面相同，即包含：

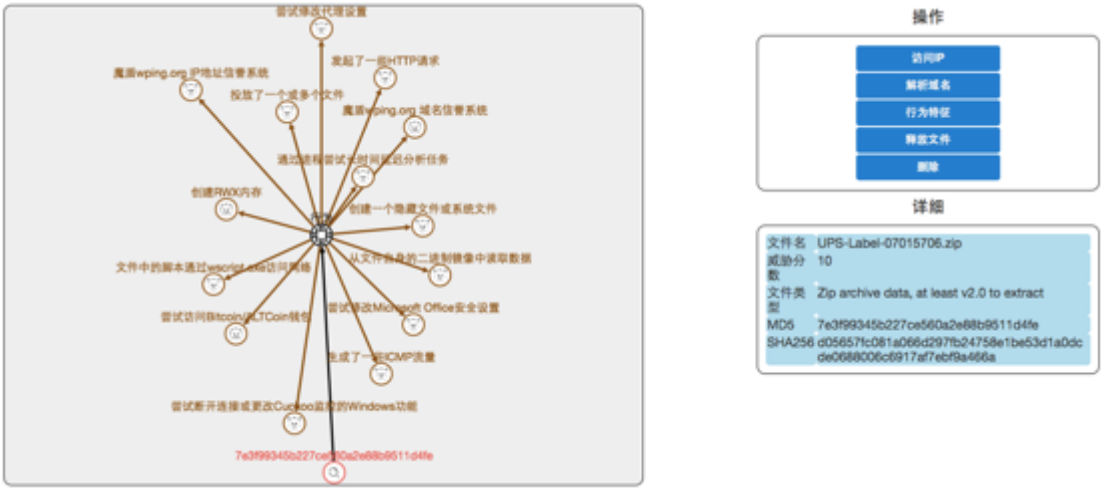
- 发件人信誉系统
- 垃圾邮件分析
- 病毒分析
- 钓鱼分析
- 高级威胁分析

操作 — 威胁报告

威胁报告可以帮助用户了解该威胁的具体威胁信息。当用户点击“威胁报告”按钮时，用户浏览器将在一个新的标签页中打开该文件经过魔盾安全分析生成的详细分析报告。关于“威胁报告”的详细内容，请参考隔离邮件分析章节的高级威胁分析中的附件部分。

操作 — 视图分析

和域名视图分析一样，高级威胁互动视图分析页面的左侧是视图部分，显示了分析元素节点；页面右侧上方是操作部分，显示了针对视图中某一个节点可以执行的操作；页面右侧下方是详细部分，显示了视图中选中节点的详细信息。



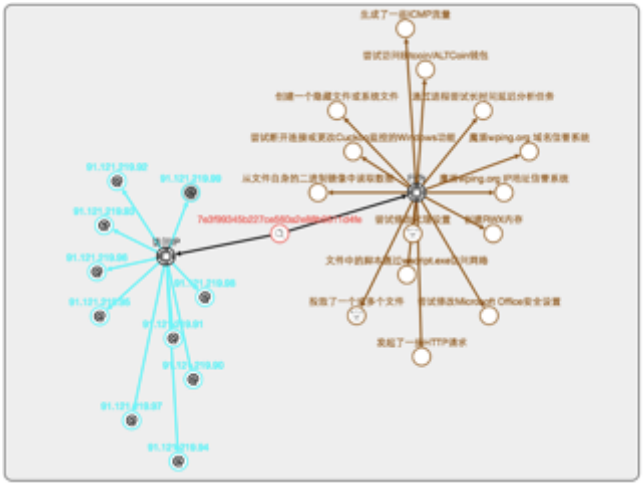
高级威胁分析中视图分析页面缺省显示了该高级威胁的行为特征，即该样本的静态和动态特征，及在魔盾 Threat Analysis Cloud 系统分析中触发的可疑行为。页面右下方的详细部分缺省显示了该样本的详细信息，包括：

- 文件名：该样本（通常为邮件附件）的文件名称
- 威胁分数：该样本的魔盾 TAC 分析结果分数，即该样本的威胁等级
- 文件类型：该样本所属的文件类型
- MD5：该样本的 MD5 哈希值
- SHA256：该样本的 SHA-256 哈希值

针对每一个分析样本，高级威胁视图分析支持的操作包括：

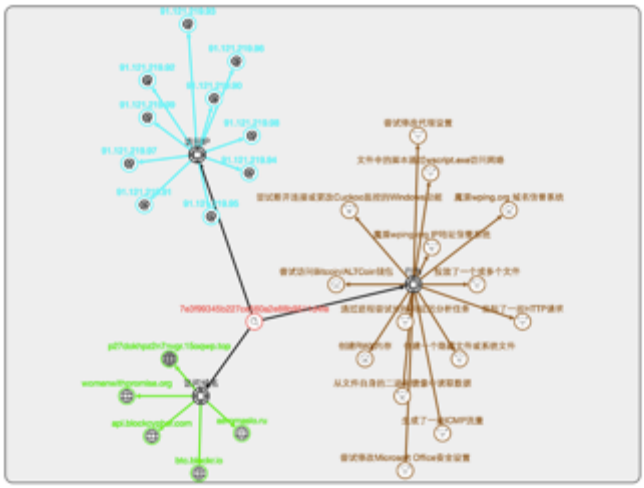
- 访问 IP：查询该样本在 TAC 分析中触发的远程主机访问行为
- 解析域名：查询该样本在 TAC 分析中触发的域名解析行为
- 行为特征：查询该样本在 TAC 分析中触发行为特征
- 释放文件：查询该样本在 TAC 分析中在虚拟环境中释放的文件
- 删除：在视图中删除该样本节点

针对一个视图中的分析样本，当用户点击右面右上方操作部分的“访问 IP”时，视图中将会呈现该样本在 TAC 虚拟环境分析中访问的 IP。（当有超过十个 IP 访问时，视图页面中将只显示十个。）用户可以点击视图中的一个 IP，继续对该 IP 进行分析。



关于视图分析中的 IP 地址分析，请参考“隔离邮件操作”章节中发件人信誉系统部分的连接 IP 视图分析。

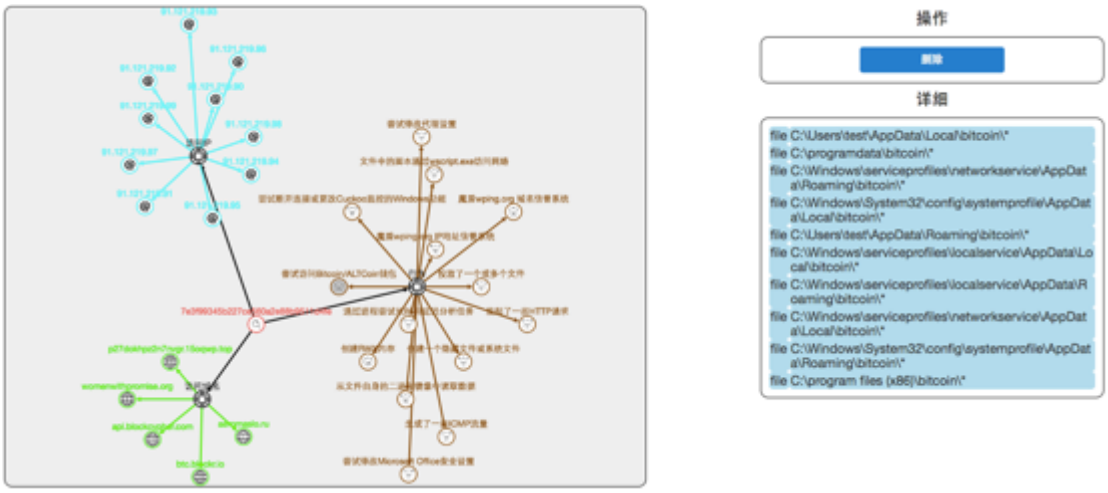
针对一个视图中的分析样本，当用户点击页面右上方操作部分的“解析域名”时，视图中将会呈现该样本在 TAC 虚拟环境分析中解析的域名。（当有超过十个域名解析时，视图页面中将只显示十个。）用户可以点击视图中的一个域名，继续对该域名进行分析。



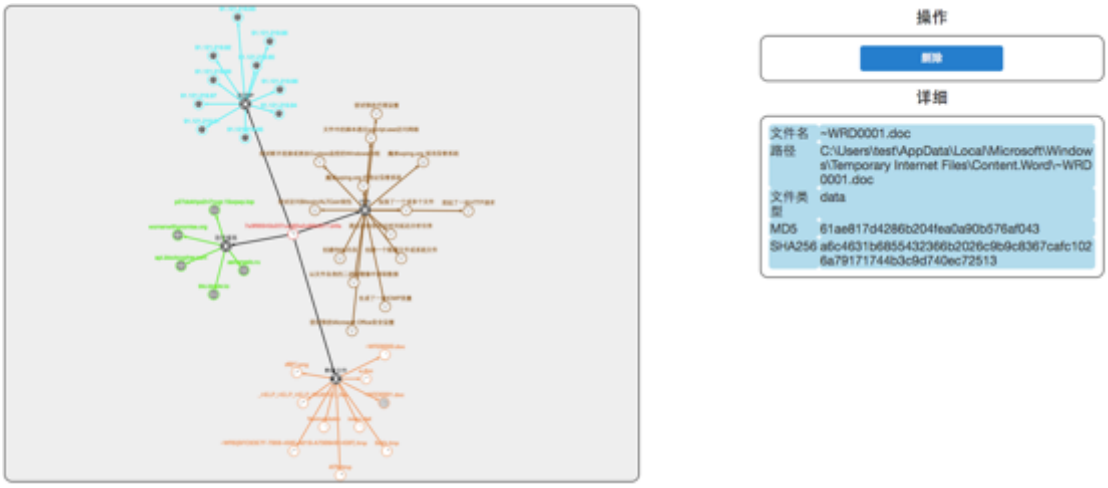
关于视图分析中的域名分析，请参考“隔离邮件操作” 章节中发件人信誉系统部分的发件域名视图分析。

针对一个视图中的分析样本，当用户点击页面右上方操作部分的“行为特征”时，视图中将会呈现该样本在 TAC 虚拟环境分析中所呈现出的静态和动态行为特征。（当有超过十条行为特征时，视图页面中将只显示十个。）用户可以点

击视图中的一条行为特征，页面右下方的详细部分将会显示该行为特征的具体含义与具体信息等。



针对一个视图中的分析样本，当用户点击页面右上方操作部分的“释放文件”时，视图中将会呈现该样本在 TAC 虚拟环境运行中所衍生出的文件。（当有超过十个衍生文件被释放时，视图页面中将只显示十个。）用户可以点击视图中的一个释放文件，页面右下方的详细部分将会显示该文件具体信息等。



针对视图中的任意元素节点，用户都可以点击页面右上方操作部分的“删除”按钮，在视图中删除该元素节点。由此节点在视图中衍生出的其余元素节点也将被删除。

4. 统计报表

统计报表页面以图表的形式直观的呈现了 ESG 系统所处理邮件的相关信息。要访问统计报表页面，请单击顶部导航栏中的“统计报表”。

统计报表页面帮助企业用户与管理员通过清晰易读的图标曲线，了解企业邮件流量，威胁趋势与相关数据汇总，并以此为基础，生成邮件相关报表。

统计分析页面包含以下类型的统计分析报告：

- 综合统计
- 病毒邮件
- 垃圾邮件
- 高级威胁
- 邮件溯源

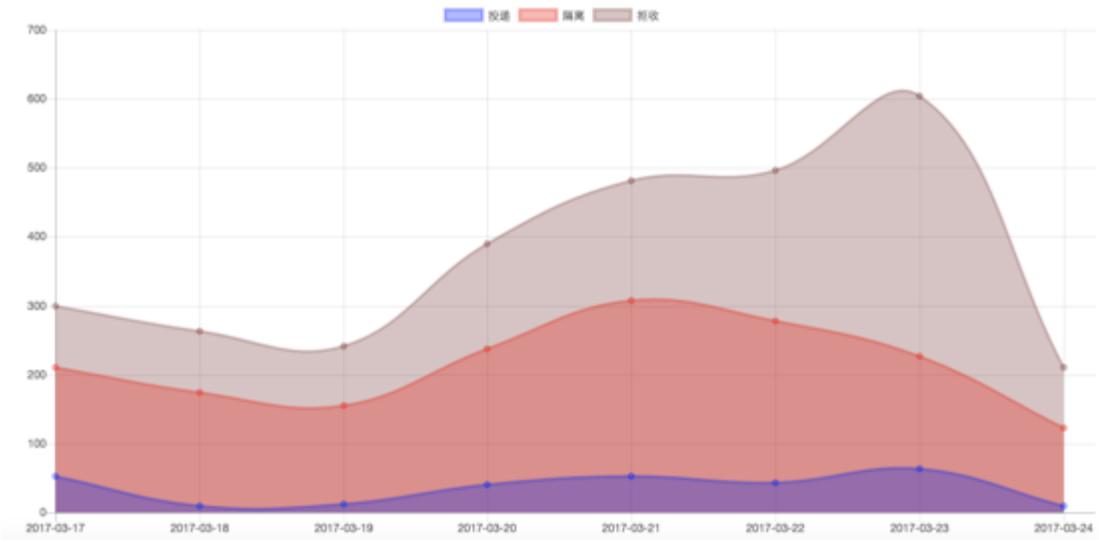
用户/管理员可以选择需要生成图表的时间范围。时间范围包括：一天，一星期（缺省选择），一个月。

4.1. 综合统计

综合统计报告显示该用户域名的全部邮件流量趋势图；该用户域名收到的邮件中被隔离邮件的类别统计；被投递邮件的类别统计；邮件附件的大小统计；邮件附件的类型统计；以及发件地址 / 收件地址 / 连接 IP / 发件域名排行等信息。要访问“综合统计”报告，在“统计报表”页面中点击“综合统计”。

综合统计页面以曲线堆栈图的形式呈现了在一定（“时间范围”中所选择的）时间范围内的邮件流量变化趋势。包含投递邮件，隔离邮件，以及拒收邮件的数据统计与趋势。

曲线图的横轴代表时间，纵轴代表邮件量。曲线图以蓝色堆栈显示所有 ESG 投递的邮件流量，以亮红色堆栈显示 ESG 系统所隔离的邮件流量，以暗红色显示 ESG 系统所拒收的邮件流量。而所有颜色堆栈的总和显示了 ESG 系统所总计处理的邮件流量。用户可以将鼠标挪着流量图上的某一个数据点以查看该时间点各种邮件类型的具体邮件流量。

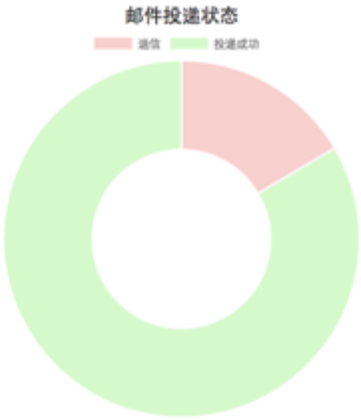


与信息概览中的邮件流量图一样，用户可以通过点击图表上方的一种邮件状态类型，选择隐藏该邮件状态堆栈，此时邮件流量图将只显示剩余两种邮件状态的流量趋势；用户也可以通过点击图表上方的两种邮件状态类型，选择隐藏该两种邮件状态堆栈，此时邮件流量图将只显示剩余一种邮件状态的流量趋势。

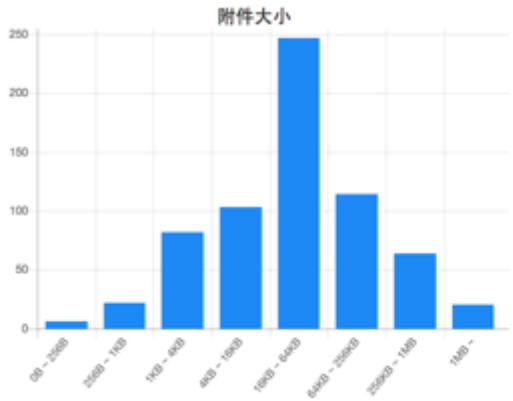
在邮件流量趋势图下方，分别以环形图的形式显示了在一定（“时间”中所选择的）时间范围内该用户域名所收到的邮件中，被隔离邮件的隔离原因分类以及数量分布，和被投递邮件的投递状态以及数量分布。

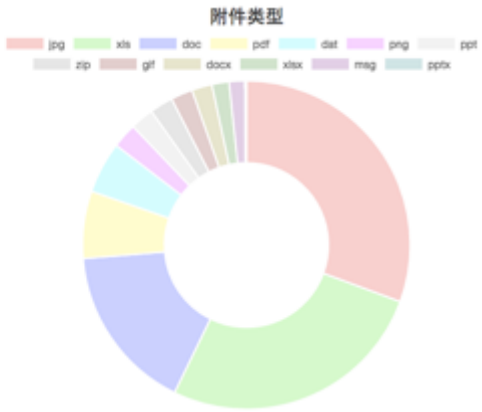
不同类型的隔离邮件和邮件投递状态将以在图中以不同的颜色按比例呈现，用户可以将鼠标挪至图中一个颜色区域查看该隔离邮件类型，或投递状态所包含的具体邮件数量。

用户可以点击图示中的一种或多种隔离原因或邮件投递状态，在图中隐藏与该因素相关的邮件，以帮助用户更灵活的对比和分析。



在隔离邮件分类和邮件投递状态图标下方，以柱状图的形式显示了在一定（“时间”中所选择的）时间范围内该用户域名所收到的邮件中，附件大小的分布情况；以及以环形图的形式显示了在一定（“时间”中所选择的）时间范围内该用户域名所收到的邮件中，附件类型的分布情况。





在附件大小柱状图中，横轴代表附件大小范围的分布，纵轴代表附件数量统计。用户可以将鼠标挪至图中一个附件大小范围柱状图块中，查看该附件大小范围的具体附件数量。

在附件类型环形图中，不同类型的附件将以在图中以不同的颜色按比例呈现，用户可以将鼠标挪至图中一个颜色区域查看该附件类型的具体数量。用户可以点击图示中的一种或多种附件类型，在图中隐藏与该附件类型相关的统计，以帮助用户更灵活的对比和分析。

在附件大小与附件类型图表下方，分别显示了在一定（“时间”中所选择的）时间范围内该用户域名所收到的邮件中，按发件数量排名的前十个发件地址，及发件量；和按收件数量排名的前十个收件地址，及收件量。

发件地址排行

发件地址	邮件数
	32
	21
	18
	15
	14
	14
	12
	12
	11
	11

收件地址排行

收件地址	邮件数
	351
	215
	154
	151
	121
	90
	73
	71
	58
	48

在发件地址与收件地址排行图表下方，分别显示了在一定（“时间”中所选择的）时间范围内该用户域名所收到的邮件中，按连接 IP 数量排名的前十个连接邮件服务器 IP 地址，及发件量；和按发件域名数量排名的前十个发件域名，及收件量。

连接IP排行

连接IP	邮件数
	38
	21
	21
	18
	18
	15
	14
	14
	14
	13

发件域名排行

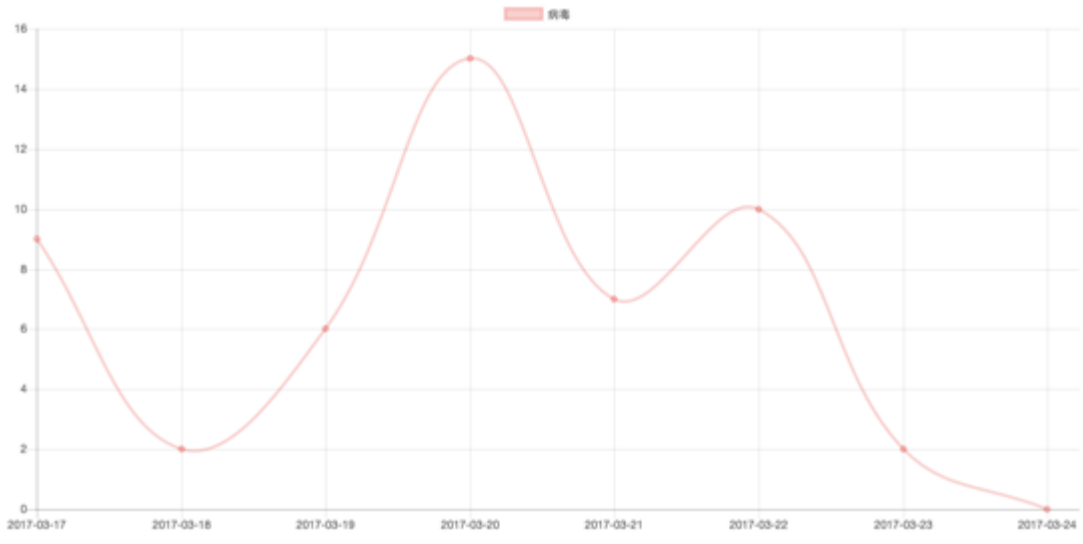
发件域名	邮件数
	33
	27
	26
	24
	22
	21
	21
	18
	17
	17

4.2. 病毒邮件

病毒邮件报告显示该用户域名的病毒邮件流量趋势图，以及该用户域名收到的病毒邮件中发件人地址 / 收件人地址 / 连接 IP / 发件域名的排行。要访问“病毒邮件”报告，在“统计报表”页面中点击“病毒邮件”。

病毒邮件页面以曲线图的形式呈现了在一定（“时间”中所选择的）时间范围内该用户域名的病毒邮件流量变化趋势。病毒邮件指在 ESG 系统分析中被判定为包含病毒的邮件。

曲线图的横轴代表时间，纵轴代表邮件量。曲线图以红色曲线显示 ESG 系统所处理的病毒邮件流量。



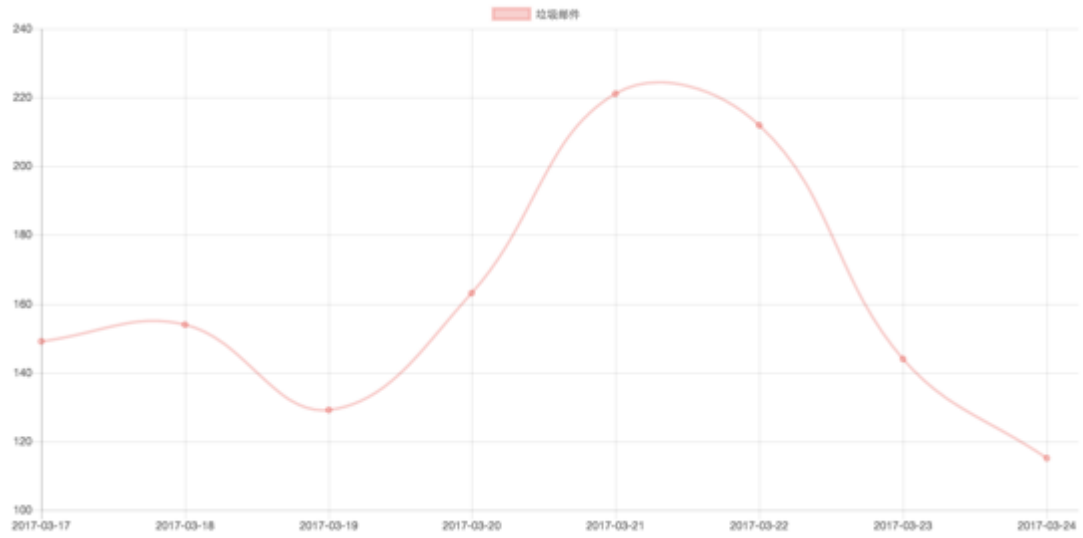
在病毒邮件流量趋势图下方，分别显示了在一定（“时间”中所选择的）时间范围内该用户域名所收到的病毒邮件中，按发件数量排名的前十个发件地址，及发件量；按收件数量排名的前十个收件地址，及收件量；按连接 IP 数量排名的前十个连接邮件服务器 IP 地址，及发件量；和按发件域名数量排名的前十个发件域名，及收件量。

4.3. 垃圾邮件

垃圾邮件报告显示该用户域名的垃圾邮件流量趋势图，以及该用户域名收到的垃圾邮件中发件人地址 / 收件人地址 / 连接 IP / 发件域名的排行。要访问“垃圾邮件”报告，在“统计报表”页面中点击“垃圾邮件”。

垃圾邮件页面以曲线图的形式呈现了在一定（“时间”中所选择的）时间范围内该用户域名的垃圾邮件流量变化趋势。垃圾邮件指在 ESG 系统分析中被判定为垃圾邮件的邮件。

曲线图的横轴代表时间，纵轴代表邮件量。曲线图以红色曲线显示 ESG 系统所处理的垃圾邮件流量。



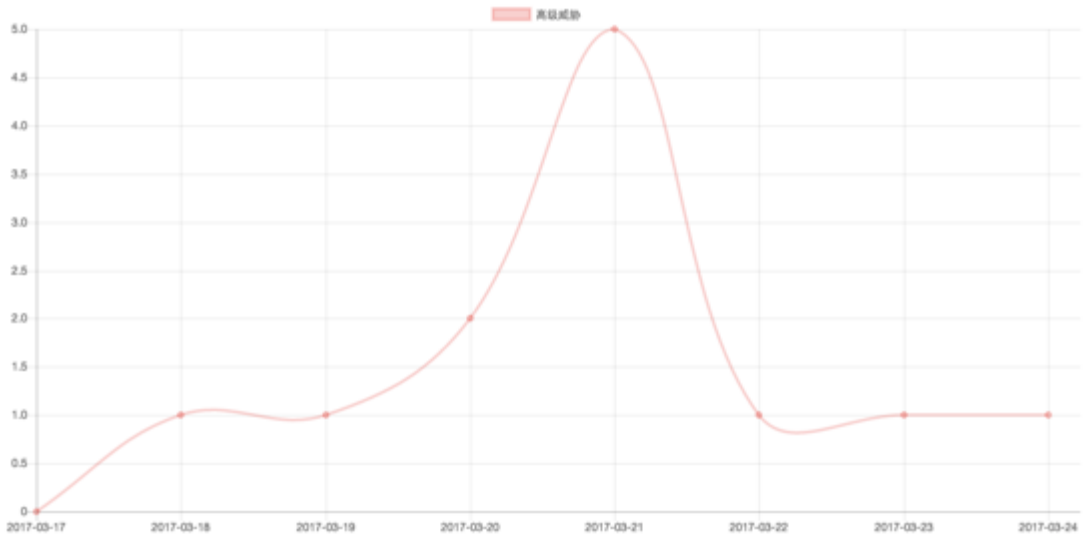
同样的，在垃圾邮件流量趋势图下方，分别显示了在一定（“时间”中所选择的）时间范围内该用户域名所收到的垃圾邮件中，按发件数量排名的前十个发件地址，及发件量；按收件数量排名的前十个收件地址，及收件量；按连接 IP 数量排名的前十个连接邮件服务器 IP 地址，及发件量；和按发件域名数量排名的前十个发件域名，及收件量。

4.4. 高级威胁

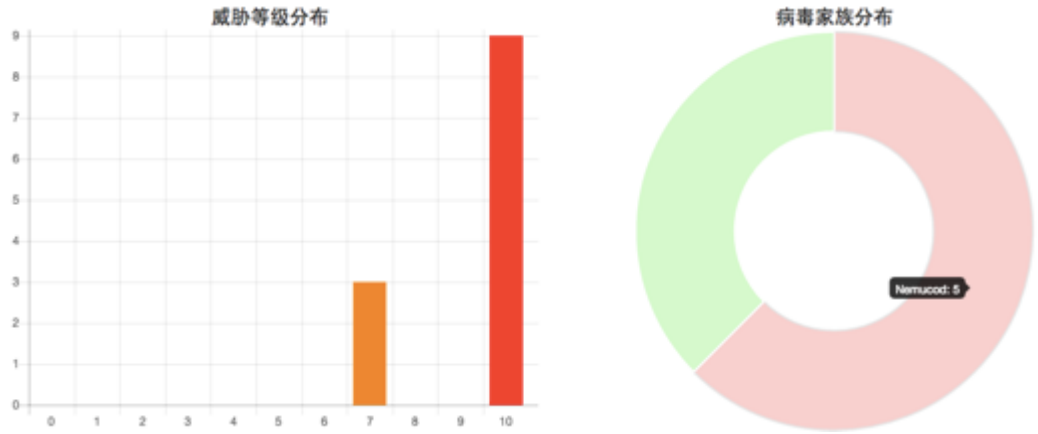
高级威胁报告显示该用户域名的高级威胁警报流量趋势图，以及该用户域名收到的高级威胁警报中的威胁等级与威胁类型（病毒家族）信息。要访问“高级威胁”报告，在“统计报表”页面中点击“高级威胁”。

高级威胁页面以曲线图的形式呈现了在一定（“时间”中所选择的）时间范围内该用户域名的高级威胁警报流量变化趋势。高级威胁警报指在 ESG 系统分析中被判定为高级威胁的邮件中包含的附件或 URL。

曲线图的横轴代表时间，纵轴代表高级威胁警报数量。曲线图以红色曲线显示 ESG 系统所处理的高级威胁警报流量。



在高级威胁趋势图表的下方分别以柱状图的形式显示了在一定（“时间”中所选择的）时间范围内该用户域名所收到的高级威胁警报中，威胁等级的分布情况；以及以环形图的形式显示了在一定（“时间”中所选择的）时间范围内该用户域名所收到的高级威胁警报中，威胁类型（病毒家族）的分布情况。



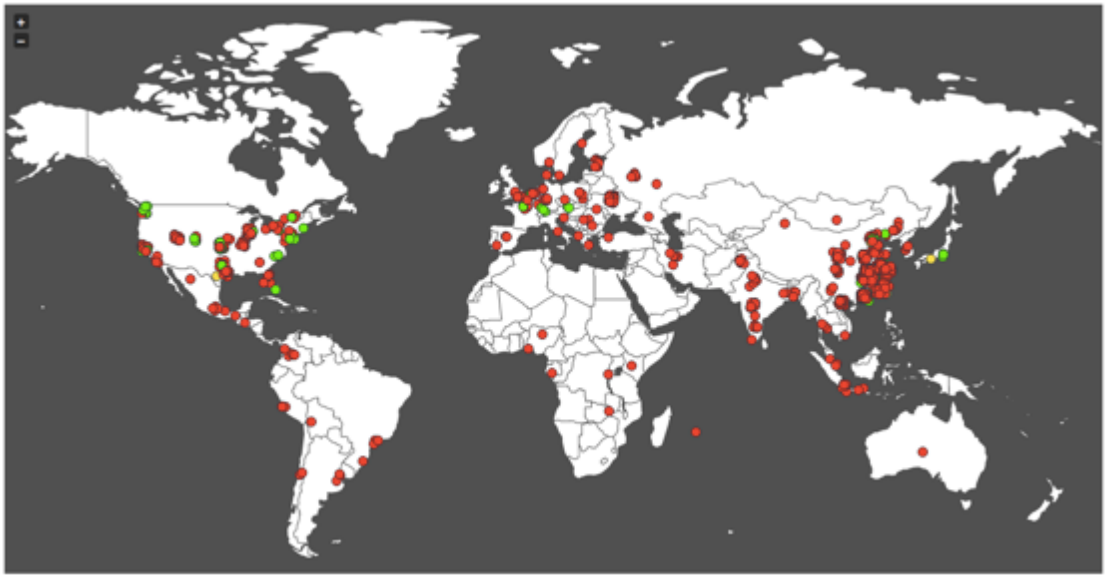
在威胁等级分布柱状图中，横轴代表威胁等级的分布（威胁等级为 0-10 的分数，分数越接近 10，威胁等级越高，分数越接近 0，威胁等级越低），纵轴代表高级威胁警报的数量统计。用户可以将鼠标挪至图中一个威胁等级范围柱状图块中，查看该威胁等级范围的具体高级威胁警报数量。

在附件类型环形图中，不同类型的附件将以在图中按比例以不同的颜色呈现，用户可以将鼠标挪至图中一个颜色区域查看该附件类型的具体数量。关于病毒家族的详细信息，请参考“高级威胁”章节。

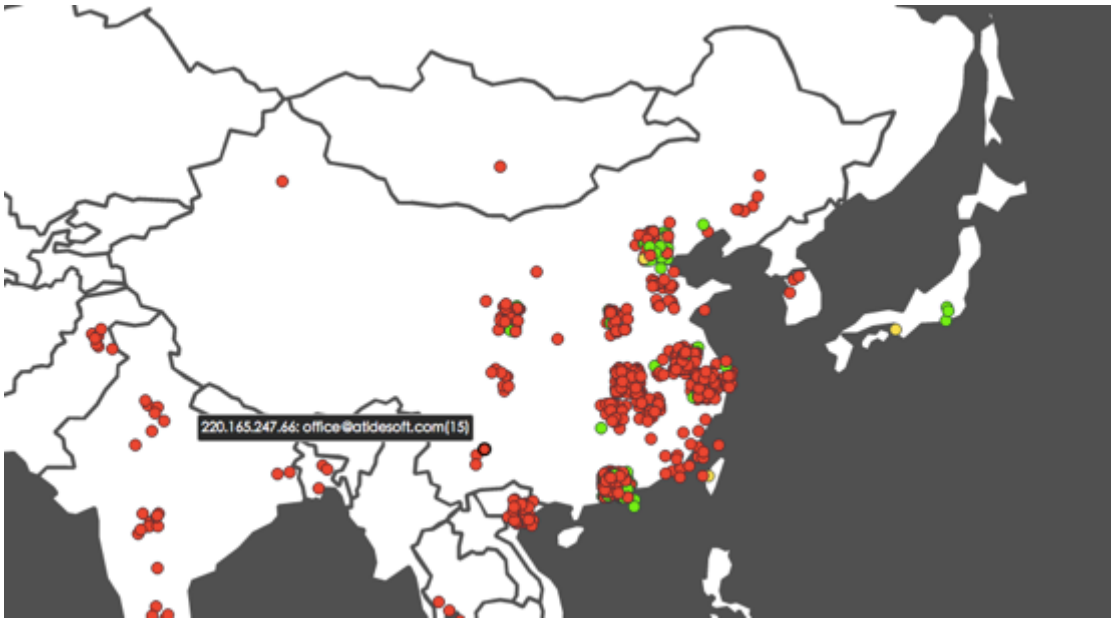
4.5. 邮件溯源

邮件溯源报告显示该用户域名所收到邮件来源 IP（连接邮件服务器 IP）的地理位置信息。要访问“邮件溯源”报告，在“统计报表”页面中点击“邮件溯源”。

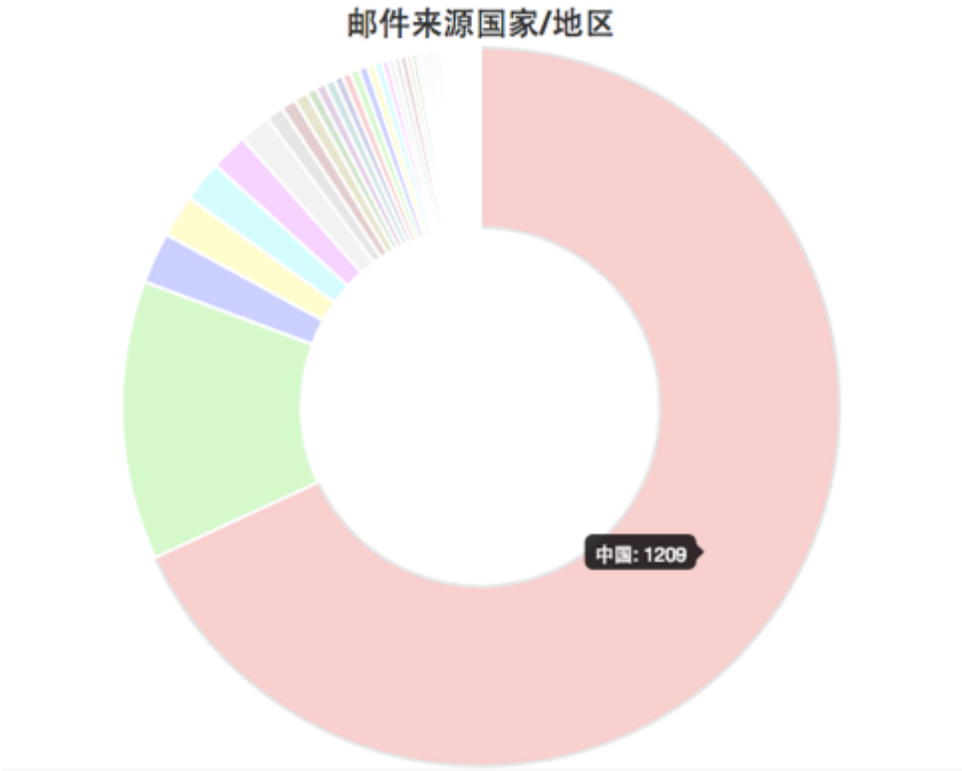
邮件溯源报告将在地图中根据邮件连接 IP 的地理位置信息标记邮件来源，并在地图中该位置的坐标处以圆点显示。红色圆点表示用户所收到威胁邮件的 IP 来源（即已隔离邮件）；绿色圆点表示用户所收到的正常邮件的 IP 来源（即已投递邮件）；黄色圆点表示用户所收到的邮件中其它邮件的 IP 来源（包含正在投递邮件，退信邮件等）。



用户可以点击地图左上放的“＋”或“－”图标放大或缩小一个地图中的范围。此外用户可以将鼠标挪至一个地图中的地理位置标记点，查看该位置的 IP 地址以及来自该 IP 邮件的发件地址。如果在选定时间范围内有多个来自该发件地址的邮件，图示发件地址之后的括号中会显示来自该 IP 该发件地址的邮件数量。



在邮件溯源报告的地图下方，以环形图的形式显示了在一定（“时间”中所选择的）时间范围内该用户域名所收到的邮件中，邮件来源国家和地区的分布情况。



在邮件来源国家/地区环形图中，不同的来源国家/地区将以在图中按比例以不同的颜色呈现，用户可以将鼠标挪至图中一个颜色区域查看该来源国家/地区的具体邮件数量。

5. 邮件追踪

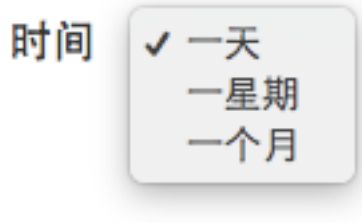
邮件追踪页面显示了所有 ESG 系统处理的邮件。要访问邮件追踪，请单击顶部导航栏中的“邮件追踪”。邮件追踪页面包含了该用户域名下所有邮件的基本信息，状态，以及查看邮件头，ESG 日志操作，报告垃圾邮件的功能。

5.1. 邮件追踪查询

邮件追踪页面的上方提供了针对特定时间范围，特定邮件状态，以及特定关键字的邮件查询，可以帮助用户快速定位符合查询条件的邮件。

时间

ESG 提供了三个时间范围的邮件追踪查询：一天（缺省选择）、一星期、一个月。



需要注意的是，除非特别协定，超过一个月的用户邮件将无法查询，如果对超过一个月前的邮件有特殊查询需求，请联系您的 ESG 销售人员或 ESG 技术支持部门。

邮件状态

ESG 系统支持通过以下邮件状态查询及追踪用户邮件：

已投递：邮件经过 ESG 系统，没有被 ESG 系统阻截或隔离，并且被 ESG 成功投递的邮件。已投递邮件通常有以下两种情况：

1. 邮件经过 ESG 分析，并且判定为正常邮件（未发现垃圾邮件，病毒，高级威胁特征等）
2. 由于用户策略设置，邮件未经过 ESG 分析，或只经过 ESG 部分模块分析，而被投递的邮件

已隔离：邮件经过 ESG 系统，被 ESG 系统所隔离的邮件。邮件被 ESG 系统隔离通常由于以下原因：

1. 垃圾邮件：邮件被 ESG 判定为垃圾邮件（即通过 ESG 垃圾邮件分析，该邮件是垃圾邮件的概率超过用户设定的阈值，缺省为 50%）
2. 病毒：邮件被 ESG 判定为包含病毒
3. 高级威胁（URL）：邮件被 ESG 判定为包含高级威胁 URL/链接，通常为恶意网站，钓鱼网站，和其他危险网页链接等
4. 高级威胁（附件）：邮件被 ESG 判定为包含高级威胁附件文件，通常为恶意软件（勒索软件，APT 等），包含恶意代码的文档等
5. 广告邮件：邮件被 ESG 判定为广告邮件
6. 自定义策略：因为用户设置的策略而被隔离的邮件，由于用户自定义策略在 ESG 其他分析模块之前处理邮件，所以该邮件通常未经过 ESG 其他分析模块扫描。
7. 发件人信誉：邮件被 ESG 发件人信誉系统判定为来自低信誉发件人 / 发件地址。

关于隔离邮件的详细信息，请参考管理员手册中的隔离邮件章节。

已释放：邮件经过 ESG 系统，被 ESG 系统隔离后，被用户/管理员释放的邮件。关于邮件释放操作的详细信息，请参考管理员手册中隔离邮件操作中的“操作—释放”章节。

已删除：邮件经过 ESG 系统，被 ESG 系统隔离后，被用户删除的邮件。关于邮件删除操作的详细信息，请参考管理员手册中隔离邮件操作中的“操作—删除”章节。

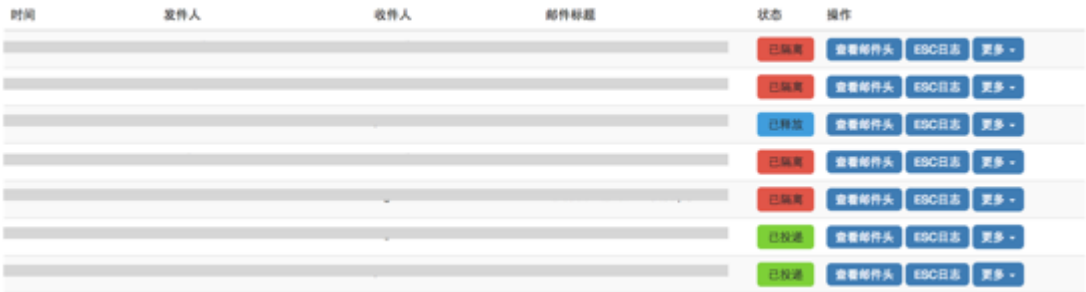
已退信：邮件经过 ESG 系统，没有被 ESG 系统阻截或隔离，由 ESG 系统投递到该邮件的下一跳邮件服务器，但是被下一跳邮件服务器拒绝的邮件。

正在投递：邮件经过 ESG 系统，没有被 ESG 系统阻截或隔离，正在由 ESG 系统投递到该邮件的下一跳邮件服务器的邮件 。

用户可以点击邮件状态下拉菜单，选择需要查询的邮件状态类型，快速定位需要查询的邮件。在查询结果中，ESG 系统也将以不同颜色的标签显示不同的邮件状态，以帮助用户快速区分不同状态的邮件。

5.2. 邮件状态信息

邮件状态信息部分显示了当前查询条件下所有的 ESG 所处理的邮件。



邮件追踪页面显示的信息包括：

- 时间：该邮件被 ESG 系统隔离的时间，时区为 GMT
- 发件人：该邮件的发件人邮件地址（Envelope From）
- 收件人：该邮件的收件人邮件地址（Envelope To）
- 邮件标题：该邮件的标题或主题
- 状态：该邮件在 ESG 系统中的状态。状态包括：已投递，已隔离，已释放，已删除，已退信，和正在投递
- 操作：ESG 系统支持用户对该邮件的操作

邮件追踪页面缺省按时间倒序每页显示最多 50 封隔离邮件信息，如果当前时间范围的隔离邮件超过 50 封，隔离页面将会分页显示。

用户可以点击顶部右侧，或底部右侧的页码选择翻页显示。 用户也可以直接点击跳转到某一页。

5.3. 邮件追踪操作

ESG 系统支持用户对一封邮件追踪中的邮件进行如下操作：

操作 — 查看邮件头

用户可以通过“查看邮件头”操作了解该邮件的邮件头信息 。邮件头通常包含邮件在从发件地址到 ESG 系统中的传递信息。当用户点击“查看邮件头”按钮时，用户浏览器将在一个新的标签页中打开该邮件的邮件头信息页面。邮件头信息页面以纯文本的形式显示了该邮件的原始邮件头。用户/管理员可以通过邮件头信息，了解邮件传递过程中的路径与状态等信息。

```
Received: from sha-mga.maldun.com (unknown [10.21.4.10])
        by sha-prod-esc-scanner01.maldun.local (Postfix) with ESMTP id 228058425B
        for <bigmouth@maldun.com>; Tue, 13 Dec 2016 11:36:27 +0800 (CST)
X-Originating-ClientAddr: 43.242.49.125
Received: from mailserver11.caixinmedia.com (unknown [43.242.49.125])
        by sha-mga.maldun.com (Postfix) with ESMTP id 3td53D0hDMz42rM
        for <bigmouth@maldun.com>; Tue, 13 Dec 2016 11:36:23 +0800 (CST)
Received: from VM-YZ-43.242.49.121 (unknown [43.242.49.121])
        by mailserver11.caixinmedia.com (Postfix) with ESMTPA id A4B6531C97
        for <bigmouth@maldun.com>; Tue, 13 Dec 2016 11:36:41 +0800 (CST)
Message-ID: <1606614174.1481600201363.JavaMail.root@mailserver3.caixinmedia.com>
Date: Tue, 13 Dec 2016 11:36:41 +0800 (CST)
From: =?UTF-8?B?6LSi5paw572R?= <admin1@mailserver3.caixinmedia.com>
To: "bigmouth@maldun.com" <bigmouth@maldun.com>
Subject: =?UTF-8?B?44CQ56S+6K+E44CR44CQ6IiS56uL6KeC5a+f44CR?=
 =?UTF-8?B?5rex5YyW5pS56Z2p56a75LiN5byA546w5Luj57uP?=
 =?UTF-8?B?5rWO5a2m55CG6K66IHwg44CQ6LSi5paw?=
 =?UTF-8?B?5ZCN5a6244CR5Lit5aSu5pS/5rK75bGA5Lya6K6u6YeK?=
 =?UTF-8?B?5pS+5LqG5LuA5LmI5L+h5Y+3IHwg44CQ?=
 =?UTF-8?B?546L54OB5a2m5Lmg5oql5ZGK55uu5b2V44CR6Iul5Y+R?=
 =?UTF-8?B?55Sf5aSn6KeE5qih6YeR6J6N5Y2x5py677yM5Y+X?=
 =?UTF-8?B?5Lyk5pu05aSn55qE5piv5a+M5Lq66L+Y5piv56m35Lq6?=
MIME-Version: 1.0
Content-Type: multipart/alternative;
        boundary="----=_Part_111463947_2051317044.1481600201361"
```

操作 一 ESG 日志

用户可以通过“ESG 日志”操作了解该邮件在 ESG 系统中的处理流程与处理结果 。 当用户点击“查看邮件头”按钮时，用户浏览器将在一个新的标签页中打开该邮件的 ESG 日志页面。ESG 日志页面顺序显示了该邮件进入 ESG 系统后的处理事件，及 ESG 对该邮件所进行的所有处理流程。用户/管理员可以通过 ESG 日志，了解该邮件在 ESG 系统中的处理和分析过程。

时间	事件
2017-03-12 18:07:23	应用用户自定义策略
2017-03-12 18:07:23	查询发件人信誉
2017-03-12 18:07:24	病毒分析
2017-03-12 18:07:25	钓鱼分析
2017-03-12 18:07:25	垃圾邮件分析
2017-03-12 18:07:42	判定为垃圾邮件(确定)
2017-03-12 18:07:42	隔离邮件

ESG 日志记录了所有 ESG 邮件处理事件的时间和事件内容。事件主要包含：

ESG 分析事件：即该邮件经过了哪些 ESG 模块的分析，其中包括用户自定义策略，发件人信誉系统，病毒分析，钓鱼分析，垃圾邮件分析，广告邮件分析，高级威胁分析等。

ESG 处理事件：即通过 ESG 分析而产生的对邮件的处理，如投递、判定、隔离等。
用户操作事件：即通过用户的操作而对邮件产生的处理事件，如释放、删除等。

操作 — 更多

对于已投递（即经过 ESG 分析并被判定为正常邮件而投递）的邮件，在用户点击操作部分的“更多”按钮后，ESG 系统下拉菜单中会显示“报告垃圾邮件”功能，该功能可以帮助 ESG 用户/管理员报告 ESG 系统所遗漏的垃圾邮件。

当用户点击“报告垃圾邮件”后，该邮件将在 ESG 系统中被归类为漏判邮件。ESG 邮件追踪页面将会以不同颜色区分显示已投递，并被用户报告为垃圾邮件的邮件。

如果用户开启了发件人信誉系统，发件人信誉系统将会学习并更新该邮件发件人的综合信誉。需要注意的是，由于 ESG 系统并不保留已投递邮件的邮件副本，ESG 系统的垃圾邮件分析并不能针对该漏判进行有效的改进。我们希望用户可以将漏判的邮件样本发送给我们。关于报告漏判邮件样本，请参考附录 B：报告误判(False Positive) / 漏判(False Negative)。

6. 策略设置

策略设置页面提供 ESG 系统所支持的邮件处理策略以及用户自定义策略功能。要访问策略设置，请单击顶部导航栏中的“策略设置”。策略设置页面支持以下策略配置与邮件订阅的相关功能：

- 基本策略
- 自定义策略
- 高级威胁报告订阅

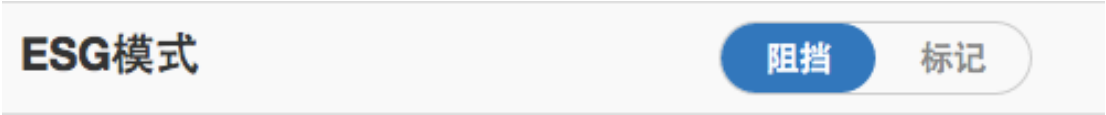
6.1. 基本策略

基本策略页面包含了用户/管理员对 ESG 系统基本功能和策略的设置。要访问基本策略页面，请在“策略设置”标签页左侧菜单栏点击“基本策略”。

基本策略页面支持以下策略的设置：

ESG 模式

ESG 模式为用户选择需要 ESG 邮件安全网关对于判定为威胁的邮件的处理方式，包括：阻挡，标记



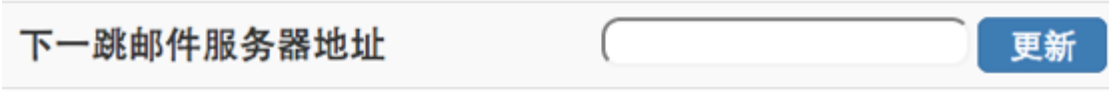
当管理员选择阻挡模式时，邮件将被放入隔离邮件区，而不会被投递给用户，只有当用户选择释放该邮件时，邮件才会被投递。

挡管理员选择标记模式时，邮件将被标注（通常 ESG 将会在邮件标题前加入：[Maldun Detected]标签），并且投递给用户，终端用户可以针对 ESG 所加入邮件标题的标签设立规则。

（注：当管理员选择标记模式时，ESG 仍会将该邮件副本存入隔离邮件区，以便管理员了解标记原因与审核）

下一跳邮件服务器地址

用户可以在“下一跳邮件服务器地址”所对应的输入框中输入您需要 ESG 系统将分析完成的该域名邮箱的邮件投递到的用户内部邮件服务器（注：也可以投递到后续的邮件分析网关或服务器），并点击“更新”按钮，以使用户可以正常接收 ESG 系统分析完成的邮件。



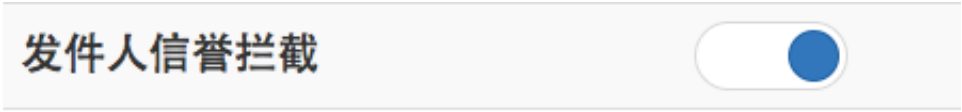
发件人信誉拦截

ESG 发件人信誉拦截将会通过魔盾 ESG 发件人信誉系统的实时信誉等级计算，隔离信誉低的发件地址所发出的邮件。需要注意的是，魔盾 ESG 发件人信誉系统综合分析了包括邮件收件地址与发收件人关系的信息，对于不同的收件地址，同一个发件地址的发件人信誉等级可能会不同。

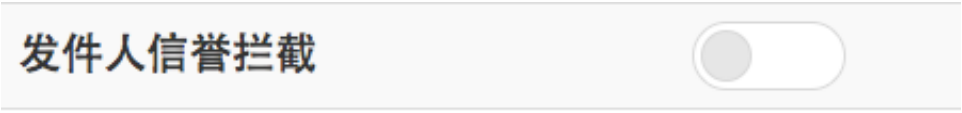
发件人信誉拦截缺省为开启，用户/管理员可以选择开启，或关闭发件人信誉拦截。当关闭发件人信誉拦截时，ESG 系统将不对发件人信誉低的邮件进行单独的隔离处理。需要注意的是当用户在“邮件分析”页面对邮件进行分析时，ESG 发件人信誉系统仍将实时生成针对该邮件的发件人信誉信息。

蓝色的开关圆圈在右代表该功能开启，在左（变为灰色圆圈）代表该功能关闭。

开启



关闭



附件文件类型分析

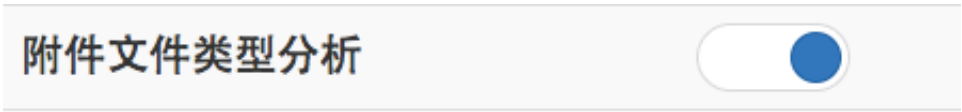
ESG 附件文件类型分析包含了：

- 危险附件类型/威胁文件预警，嵌套压缩文件检查

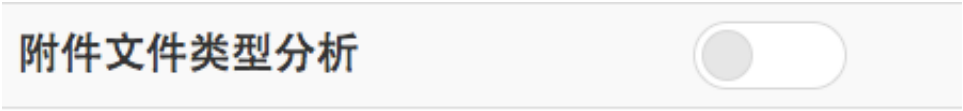
附件文件类型分析缺省为开启，用户/管理员可以选择开启，或关闭附件文件类型分析。当关闭附件文件类型分析时，ESG 系统将不对邮件进行附件文件类型分析和处理。

蓝色的开关圆圈在右代表该功能开启，在左（变为灰色圆圈）代表该功能关闭。

开启



关闭



病毒分析

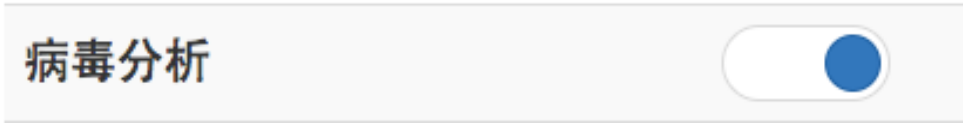
ESG 病毒分析包含了：

- ClamAV 防病毒引擎

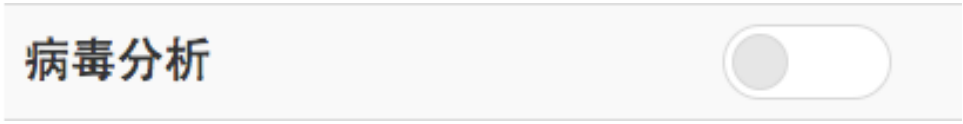
病毒分析缺省为开启，用户/管理员可以选择开启，或关闭病毒分析。当关闭病毒分析时，ESG 系统将不对邮件进行病毒分析和处理。

蓝色的开关圆圈在右代表该功能开启，在左（变为灰色圆圈）代表该功能关闭。

开启



关闭



钓鱼分析

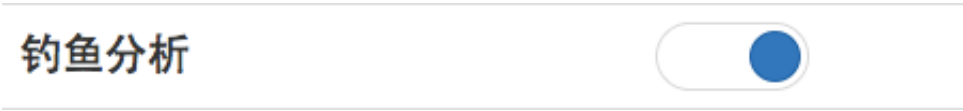
ESG 钓鱼分析包含了：

- 启发式钓鱼站点识别
- 邮件 HTML 隐藏威胁检测
- 发件人一致性检查，发件地址/路径/URL 一致性检查

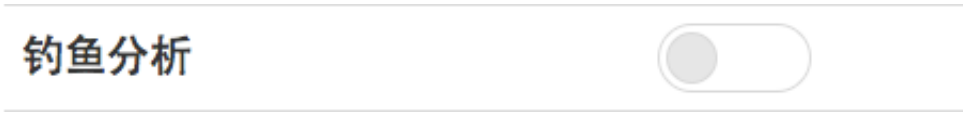
钓鱼分析缺省为开启，用户/管理员可以选择开启，或关闭钓鱼分析。当关闭钓鱼分析时，ESG 系统将不对邮件进行钓鱼分析和处理。

蓝色的开关圆圈在右代表该功能开启，在左（变为灰色圆圈）代表该功能关闭。

开启



关闭



垃圾邮件分析

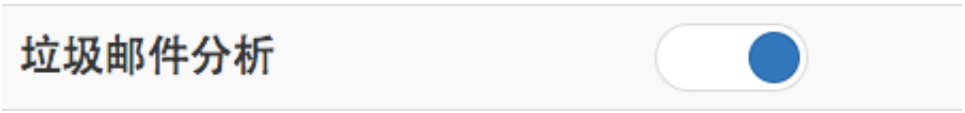
ESG 垃圾邮件分析包含了：

- 魔盾垃圾邮件内容识别规则
- 魔盾机器学习规则
- 全球垃圾邮件样本库检测
- 发件服务器域名、IP 信誉
- 邮件链接 URL 信誉
- 其它基于邮件头、内容、邮件模式的规则

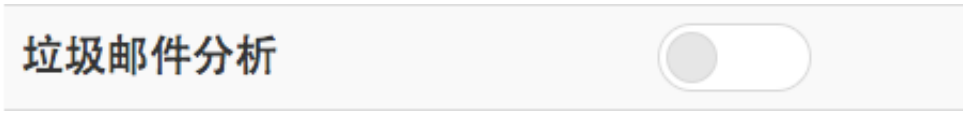
垃圾邮件分析缺省为开启，用户、管理员可以选择开启，或关闭垃圾邮件分析。当关闭钓鱼分析时，ESG 系统将不对邮件进行垃圾邮件分析和处理。

蓝色的开关圆圈在右代表该功能开启，在左（变为灰色圆圈）代表该功能关闭。

开启



关闭

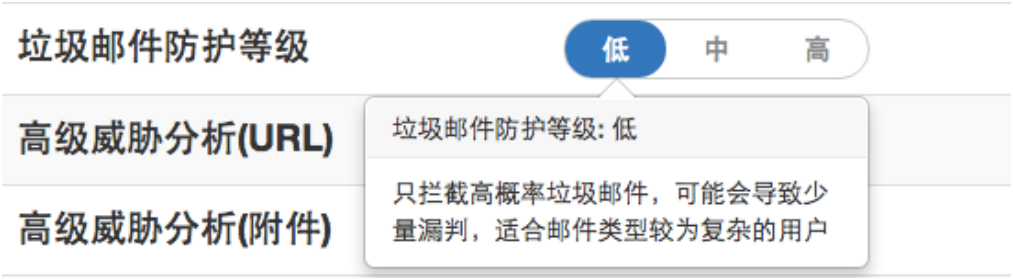


垃圾邮件防护等级

垃圾邮件防护等级设置可以帮助用户智能调整垃圾邮件防护的力度。魔盾 ESG 系统在垃圾邮件分析之后会对每一封邮件生成垃圾邮件概率。垃圾邮件防护等级根据不同的垃圾邮件概率阈值设定操作策略。

用户/管理员可以根据用户企业邮件的不同情况，在三种垃圾邮件防护等级中选择：

垃圾邮件防护等级低：



垃圾邮件防护等级中：

垃圾邮件防护等级高：

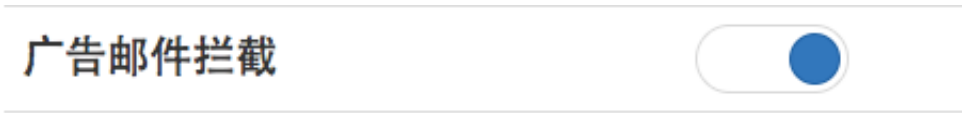
广告邮件拦截

ESG 广告邮件分析通过对邮件发件人的和邮件内容的特征分析，判断该邮件是否为订阅类广告邮件或推广邮件，并针对广告邮件分析结果对邮件进行隔离处理。

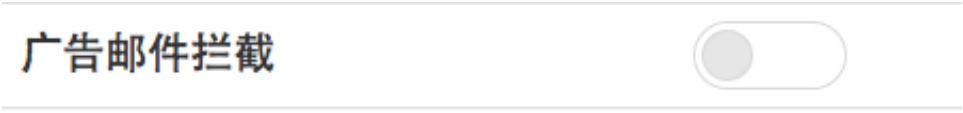
广告邮件拦截缺省为开启，用户/管理员可以选择开启，或关闭广告邮件拦截。当关闭广告邮件拦截时，ESG 系统将不对广告邮件进行处理。

蓝色的开关圆圈在右代表该功能开启，在左（变为灰色圆圈）代表该功能关闭。

开启



关闭



高级威胁分析（URL）

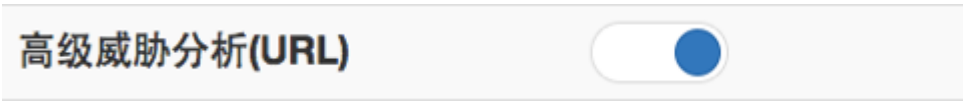
ESG 高级威胁分析（URL）包括对邮件中的所有 URL 进行：

- 网站信誉与黑名单检查
- 魔盾 Threat Analysis Cloud 实时虚拟执行分析

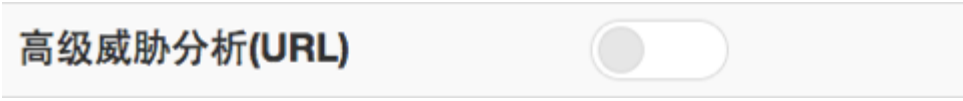
ESG 高级威胁分析（URL）缺省为开启，用户/管理员可以选择开启，或关闭 ESG 高级威胁分析（URL）。当关闭 ESG 高级威胁分析（URL）时，ESG 系统将不对邮件中的 URL 进行高级威胁分析和处理。

蓝色的开关圆圈在右代表该功能开启，在左（变为灰色圆圈）代表该功能关闭。

开启



关闭



高级威胁分析（附件）

ESG 高级威胁分析（附件）包括对邮件中的所有附件进行：

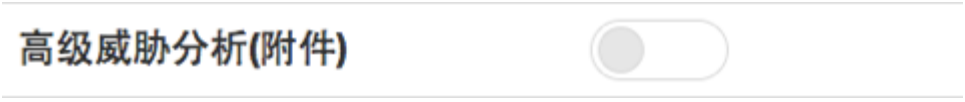
- 文件信誉与黑名单检查
- 魔盾 Threat Analysis Cloud 实时虚拟执行分析

ESG 高级威胁分析（附件）缺省为开启，用户/管理员可以选择开启，或关闭 ESG 高级威胁分析（附件）。当关闭 ESG 高级威胁分析（附件）时，ESG 系统将不对邮件中的附件进行高级威胁分析和处理。

蓝色的开关圆圈在右代表该功能开启，在左（变为灰色圆圈）代表该功能关闭。

开启

关闭



接收隔离邮件报告（收件人）

由于 ESG 系统的分析和策略，终端用户的特定邮件可能会被 ESG 系统隔离，当用户/管理员需要终端用户（即邮件收件人）了解隔离邮件信息，以确保终端用户可以发现并释放 ESG 系统误判或因其它原因隔离的正常邮件时，可以选择允许收件人接收隔离邮件报告。

接收隔离邮件报告（收件人）缺省为关闭，用户/管理员可以选择开启，或关闭 ESG 接收隔离邮件报告（收件人）。当关闭 ESG 接收隔离邮件报告（收件人）时，ESG 系统将不会向收件用户邮箱发送隔离邮件报告。

蓝色的开关圆圈在右代表该功能开启，在左（变为灰色圆圈）代表该功能关闭。

开启

关闭

隔离邮件报告频率

当用户/管理员选择允许终端用户（收件人）接收隔离邮件报告时，可以进一步选择接收隔离邮件报告的频率。ESG 提供四种隔离邮件报告频率选择：2 小时，6 小时，12 小时，24 小时，代表 ESG 系统将分布在每 2/6/12/24 小时，向收件人发送隔离邮件报告，ESG 管理员可以根据具体情况，选择和调整隔离邮件报告频率。

隔离邮件报告由魔盾 ESG 系统邮件地址发出 （魔盾 ESG 通知 <notification@your_ESG_host>），我们建议管理员/用户将魔盾 ESG 系统邮件

地址加入收件邮件服务器或用户终端邮件客户端的白名单，以确保魔盾 ESG 隔离邮件报告的正常投递。

隔离邮件报告包含以下信息：

- 时间：该邮件被 ESG 系统分析与隔离的时间
- 发件地址：该隔离邮件的发件人地址
- 标题：该隔离邮件的标题或主题
- 释放链接：用户可以点击该释放链接从 ESG 邮件隔离区释放该邮件，邮件将从 ESG 系统投递到收件用户

接收每日高级威胁警报（管理员）

经过魔盾 ESG 高级威胁分析的邮件，如果返回高威胁等级，将会生成高级威胁警报。用户/管理员可以选择接收每日高级威胁警报，以确保了解和掌握用户域名 24 小时内收到的邮件中的高级威胁，以及制定相应的安全策略等。

接收每日高级威胁警报（管理员）缺省为关闭，用户/管理员可以选择开启，或关闭 ESG 接收每日高级威胁警报（管理员）。当关闭 ESG 接收每日高级威胁警报（管理员）时，ESG 系统将不会向管理员邮箱发送每日高级威胁警报。

蓝色的开关圆圈在右代表该功能开启，在左（变为灰色圆圈）代表该功能关闭。

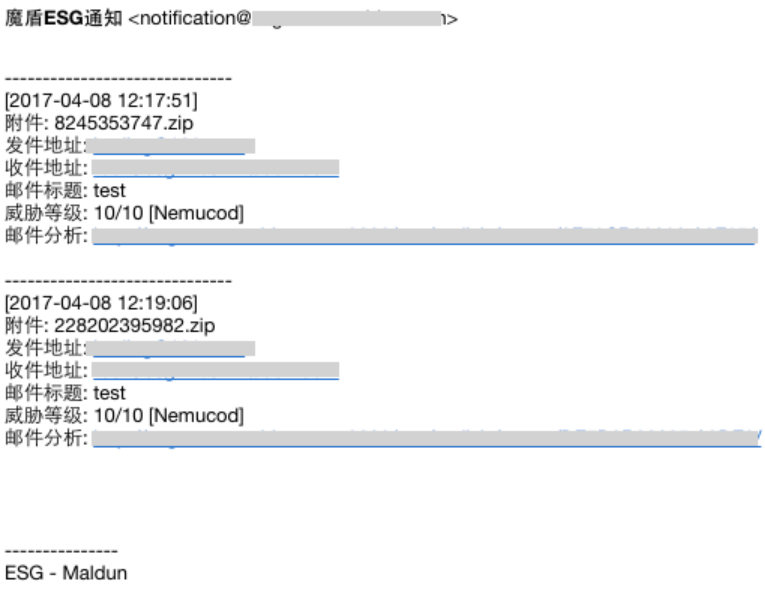
开启

关闭

每日高级威胁警报邮件由魔盾 ESG 系统邮件地址发出 （魔盾 ESG 通知 <notification@your_ESG_host>），我们建议管理员/用户将魔盾 ESG 系统邮件地址加入收件邮件服务器或用户终端邮件客户端的白名单，以确保魔盾 ESG 每日高级威胁警报邮件的正常投递。

每日高级威胁警报邮件中包含了以下信息：

- 时间：ESG 系统发现识别该威胁的时间
- 附件/URL： 包含该高级威胁的附件文件名或 URL 链接地址
- 发件地址：包含该高级威胁的邮件发件人地址
- 收件地址：包含高级威胁的邮件发件人地址
- 邮件标题：包含高级威胁的邮件标题或主题
- 威胁等级：该高级威胁的威胁等级（10 为最高等级），如果 ESG 系统成功识别出威胁类型，威胁等级之后将同时显示威胁类型
- 邮件分析：查看包含高级威胁的邮件信息的链接，方便管理员点击查阅



6.2. 自定义策略

自定义策略页面包含了用户/管理员自行配置的对符合特定条件的邮件的操作策略。要访问自定义策略页面，请在“策略设置”标签页左侧菜单栏点击“自定义策略”。

自定义策略页面支持以下策略的设置：

条件：

- 发件地址
- 收件地址
- 邮件标题

等于 或 包含

关键字

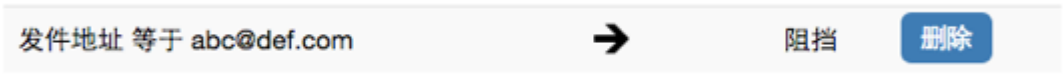
即用户/管理员可以分别设置针对发件地址，收件地址，和邮件标题的策略，策略支持当发件地址，收件地址，或邮件标题等于（完全匹配）或包含（部分匹配）某一用户制定的关键字时生效

策略：

- 阻挡
- 放行
- 仅标记（不阻挡）

即用户/管理员可以选择阻挡（隔离），放行（投递），或标记并投递符合上述条件的邮件。

当用户/管理员设定好策略后，可以点击添加策略，将自定义策略添加到 ESG 系统中。



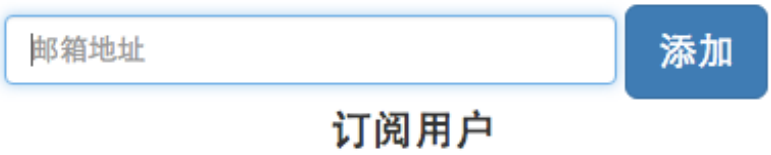
对于已经添加的策略，当用户/管理员可以点击删除，将该自定义策略从系统中删除。

自定义策略的执行将按照已经添加的策略，顺序执行。

6.3. 高级威胁报告订阅

高级威胁报告订阅页面提供了每日高级威胁警报邮件的订阅功能。要访问高级威胁报告订阅页面，请在“策略设置”标签页左侧菜单栏点击“高级威胁报告订阅”。

当用户域名中有其它用户（非管理员用户）需要了解和接收高级威胁报告时，用户/管理员可以在高级威胁报告订阅页面中输入需要添加的邮件地址，并点击添加 。



添加后的订阅用户邮箱地址将会显示在“订阅用户”下方，用户/管理员可以选择删除一个订阅用户的邮箱地址，该用户将不会在收到高级威胁报告邮件。

关于高级威胁报告邮件的具体信息，请参考管理员手册基本策略中的接收每日高级威胁警报（管理员）章节。

附录 A：名词解释

名词术语	解析
高级持续性威胁(APT)	指隐匿而持久的电脑入侵过程，通常由某些人员精心策划，针对特定的目标。其通常是出于商业或政治动机，针对特定组织或国家，并要求在长时间内保持高隐蔽性。高级长期威胁包含三个要素：高级、长期、威胁。高级强调的是使用复杂精密的恶意软件及技术以利用系统中的漏洞。长期暗指某个外部力量会持续监控特定目标，并从其获取数据。威胁则指人为参与策划的攻击。ESG 高级威胁分析主要针对高级持续性威胁。
垃圾邮件	垃圾邮件一般具有批量发送的特征。其内容包括赚钱信息、成人广告、商业或个人网站广告、电子杂志、连环信等。垃圾邮件可以分为良性和恶性的。良性垃圾邮件是各种宣传广告等对收件人影响不大的信息邮件。恶性垃圾邮件是指具有破坏性的电子邮件。例如具有攻击性的广告：夸张不实，包括情色、钓鱼网站。
病毒	计算机病毒是一个程序，一段可执行码。就像生物病毒一样，具有自我繁殖、互相传染以及激活再生等生物病毒特征。计算机病毒有独特的复制能力，它们能够快速蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上，当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。
规则	规则是对工作流的执行进行控制的一种机制，它被看作是申明性的。规则引擎对条件进行判断，然后指挥工作流按照条件处理的结果去执行。在一定程度上，规则类似于脚本代码，与规则引擎一起充当脚本执行环境。防垃圾邮件规则特指根据某些特征（比如单词、词组、位置、大小、附件等）来形成规则，以分析和过滤垃圾邮件。
策略	策略是用户根据自己的实际环境对系统处理细节的微调。可以更有效的贴合企业运营环境。在 ESG 系统中，策略特指用户调节的对邮件处理的方式。
威胁情报	情报(intelligence)一词英文的原意是“瞭解的能力”(the Faculty of Understanding)，从传统情报机构的立场上，情报的本质则是“减少冲突的不确定性”。对情报的重视古已有之，《孙子兵法》中所说“知己知彼，百战不殆”讲的就是情报的重要性，情报就能帮助你做到知彼。在网络空间的战斗中，情报同样有着至关重要的地位
邮件服务器	邮件服务器是一种用来负责电子邮件收发管理的设备。专业的独立的邮件服务器比网络上的免费邮箱更安全和高效，因此一直是企业公司的必备设备。
MX 纪录	邮件交换记录，它指向一个邮件服务器，用于电子邮件系统发邮件时根据 收信人的地址后缀来定位邮件服务器。
隔离	将有问题或者潜在问题的邮件存放在专门的空间内，以保证最终用户的使用安全。隔离是邮件安全中最常采用的方式。
信誉	信誉系统是一种通过一些实体相互给出看法和评价，来试图确定这些实体的等级和类别的合作性筛选算法。这很类似于一种推荐系统，信誉系统是实体间的互相推荐。信誉系统可以使所谓的信任更容易被量化。在 ESG 系统中，信誉特指对发件人，发件服务器，或邮件链接中的网页所评估和计算的信誉。
机器学习	机器学习(Machine Learning, ML)是一门多领域交叉学科，涉及概率论、统计学、逼近论、凸分析、算法复杂度理论等多门学科。专门研究计算机怎样模拟或实现人类的学习行为，以获取新的知识或技能，重新组织已有的知识结构使之不断改善自身的性能。ESG 系统通过机器算法学习垃圾邮件 / 威胁与正常邮件的区别，以帮助更有效的发现和阻截垃圾邮件 / 威胁。
钓鱼	钓鱼式攻击是一种企图从电子通讯中，通过伪装成信誉卓著的法人媒体以获得如用户名、密码和信用卡明细等个人敏感信息的犯罪诈骗过程。这些通信都声称（自己）来自社交网站拍卖网站、网络银行、电子支付网站或网络管理者，以此来诱骗受害人的轻信。网钓通常是通过 Email 或者即时通讯进行。它常常导引用户到 URL 与界面外观与真正网站几无二致的假冒网站输入个人数据。就算使用强式加密的 SSL 服务器认证，要侦测网站是否仿冒实际上仍很困难。ESG 系统采用了多种启发式智能算法分析钓鱼威胁。
钓鲸	钓鲸威胁，或者说针对高管的欺诈攻击，70%的公司企业都见证了这种基于电子邮件的欺诈攻击一直在持续增长。随着年初报税季的来临，诈骗犯们纷纷瞄准公司财务部门，发出貌似来自公司高管的电子邮件，钓鲸欺诈活动越演越烈。

附录 B: 报告误判(False Positive) / 漏判(False Negative)

误判是合法邮件，被错误地归类为垃圾邮件或钓鱼/病毒邮件。
漏判是将垃圾邮件或钓鱼邮件错误地归类为合法邮件。

终端收件用户对错误分类的邮件所提供的反馈有助于提高ESG系统防御垃圾邮件或钓鱼/病毒邮件的准确性。我们希望并邀请终端收件用户对误判和漏判邮件进行报告和提交。

您所报告的邮件必须是RFC822格式的MIME附件。这将保留ESG添加的和排查所需要的邮件头信息。请不要使用转发命令发送错误分类的邮件，这样将生成一封新的邮件并剥离原始邮件的邮件头信息。

魔盾ESG设置了两个电子邮件地址，供终端用户报告误报和漏判邮件。终端用户应使用以下电子邮件地址进行报告和提交：

误判 – 在报告误报（合法邮件被错误地归类为垃圾邮件或钓鱼 / 病毒邮件）时，将邮件作为MIME附件转发到：fp@esg.maldun.com

漏判 - 在报告漏判（垃圾邮件或钓鱼 / 病毒邮件被错误地归类为合法邮件）时，将邮件作为MIME附件转发到：fn@esg.maldun.com

使用Microsoft Outlook或Outlook Express报告错误分类的邮件

1. 从文件菜单中，选择新建>邮件以打开新邮件窗口。
2. 填写误判和漏判相应的ESG电子邮件地址。
3. 将错误分类的邮件拖动到新邮件窗口中以附加它们。虽然您可以附加尽可能多的邮件，但您的电子邮件服务器配置可能拒绝过大的邮件。在构建邮件时，请注意服务器的大小限制。
4. 单击“发送”发送邮件。

使用Thunderbird报告错误分类的邮件

1. 从文件菜单中，选择新建>邮件以打开新邮件窗口。
2. 填写误判和漏判相应的ESG电子邮件地址。
3. 将错误分类的邮件拖动到新邮件窗口中以附加它们。虽然您可以附加尽可能多的邮件，但您的电子邮件服务器配置可能拒绝过大的邮件。在构建邮件时，请注意服务器的大小限制。
4. 单击发送发送消息。

使用Eudora报告错误分类的邮件

1.在邮件列表中，选择错误分类的邮件。
2.从文件菜单中，选择另存为。
3.在“另存为”窗口中，导航到要在其中保存邮件的适当位置。
4.选中包括标题复选框。
5.单击保存。 对每个错误分类的邮件重复步骤1到步骤5。
6.从邮件菜单中，选择新邮件。 将显示一个新邮件窗口。
7.填写误判和漏判相应的ESG电子邮件地址。
8.从邮件菜单中，选择附加文件。
9.在“附加文件”窗口中，导航到保存错误分类邮件的位置，然后选择它。
10.单击附加。虽然您可以附加尽可能多的邮件，但您的电子邮件服务器配置可能拒绝过大的邮件。在构建邮件时，请注意服务器的大小限制。
11.单击发送以发送邮件。

使用Mac OS X Apple Mail报告错误分类的邮件

1.在邮件列表中，选择错误分类的邮件。
2.从文件菜单中，选择另存为。
3.将文件保存在适当的位置。
4.从文件菜单中，选择新邮件以打开新邮件窗口。
5.填写误判和漏判相应的 ESG 电子邮件地址。
6.从文件菜单中，选择附加文件。
7.导航到保存错误分类邮件的位置，然后选择它。
8.单击选择文件以附加保存的文件。虽然您可以附加尽可能多的邮件，但您的电子邮件服务器配置可能拒绝过大的邮件。在构建邮件时，请注意服务器的大小限制。
9.单击发送以发送邮件。

附录 C：联系我们

技术支持：
电话：021 55660866
邮件：support@maldun.com
上海魔盾信息科技有限公司
https://www.maldun.com

Technical Support:
Phone: +86 (21) 55660866
Email: support@maldun.com
Shanghai MalDun Tech. L.L.C
https://www.maldun.com