思科安全邮件威胁防御用户指南

目录

简介

思科安全邮件威胁防御 （之前的 Cisco Secure Email Cloud Mailbox）是面向 Microsoft 365 的集成式云原生安全解决方案，主要特点包括：部署轻松；可简化攻击补救；具有卓越的可视性。

要求

要成功设置和使用 思科安全邮件威胁防御，需要满足以下条件：

- 您已购买 Secure Email Threat Defense 并收到欢迎邮件。
- 以下浏览器之一的最新版本：
  - Google Chrome
  - Microsoft Edge
  - Mozilla Firefox
- 如果您的邮件来源是 Microsoft 365，或者您的可视性和补救模式使用的 Microsoft 365 身份验证：
  - 具有全局管理员权限的 Microsoft 365 帐户。
  - Microsoft 365 环境中能够接收无法传送的日志报告的邮件地址。使用的邮箱地址不会被记录；请勿使用要让 Secure Email Threat Defense 分析的地址。

设置思科安全邮件威胁防御

安全邮件威胁防御设置包括以下内容：

1. 登录您的帐户，第 11 页
2. 指明您是否有 Cisco Secure Email Gateway (SEG)，第 12 页
3. 选择邮件来源、可视性和补救措施，第 12 页
4. 设置邮件来源，第 12 页
5. 查看您的策略设置，第 14 页
6. 导入 Microsoft 邮件域，第 14 页

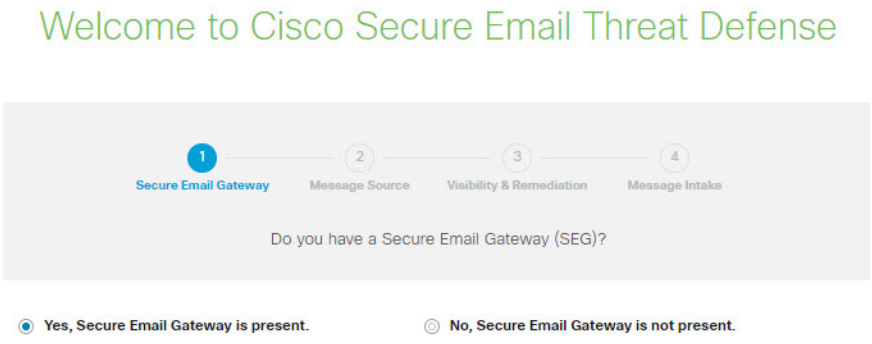
这些步骤将假定您符合**要求，第 9 页**。

登录您的帐户

1. 按照思科欢迎邮件中的说明来设置用户帐户。

   Secure Email Threat Defense 使用 Cisco Security Cloud 登录管理用户身份验证。有关 Cisco Security Cloud 登录的信息，请参阅 https://cisco.com/go/securesignon。如果您是 Cisco SecureX Threat Response、Cisco Secure Malware Analytics（以前称为 Cisco Threat Grid）或 Cisco Secure Endpoint（以前称为 AMP）的客户，请使用现有的凭证进行登录。如果您不是现有用户，则需要创建一个新的 Cisco Security Cloud 登录帐户。

2. 成功登录后，请接受“条款和条件”(Terms and Conditions)。
3. 您现在可以访问**欢迎使用 (Welcome to)思科安全邮件威胁防御** 页面。按照以下各部分中所述的安装向导执行操作。



指明您是否有 Cisco Secure Email Gateway (SEG)

无论您的邮件来源如何（在下一部分中选择），都必须指出存在 Cisco Secure Email Gateway (SEG) 以及哪个信头可用于在传入日志中识别该信头，以便 Secure Email Threat Defense 可以确定邮件的真正源发件人。如果没有此配置，则可能会出现所有邮件都来自 SEG 的情况，从而可能导致误报。

1. 通过选择“是”(Yes) 或“否”(No) 来指示是否存在 Cisco Secure Email Gateway (SEG)，然后点击**下一步 (Next)**。
2. 如果您回答“是”(Yes)，请输入您的 SEG 类型和信头。单击**下一步 (Next)**。

选择邮件来源、可视性和补救措施

1. 选择邮件来源：Microsoft O365 或网关。如果您在上一步中选择了无 SEG，则会假定 Microsoft O365 作为您的邮件来源。
2. 选择您的可视性和补救措施。

   可视性和补救模式定义了可以应用的补救策略的类型。

   Microsoft 365 身份验证

   - **读/写 (Read/Write)** - 允许查看和按需或自动补救（即，移动或删除可疑邮件）。将从 Microsoft 365 请求读/写权限。
   - **读取 (Read)** - 仅允许显示，不允许补救措施。将从 Microsoft 365 请求只读权限。

     注意：如果您选择**读/写 (Read/Write)**，则在设置完成后，您需要在**策略设置，第 15 页**中打开“自动补救策略”(Automated Remediation Policy)。要将自动补救应用于所有内部邮件，请确保在“策略”(Policy) 页面上选中**对不在域列表中的域应用自动补救 (Apply auto-remediation to domains not in the domain list)** 框。

   无身份验证

   如果您使用思科 SEG 作为邮件来源，则会出现此选项。它仅提供可视性。您将无法对邮件进行补救。
3. 如果您选择了 Microsoft 365 身份验证，请连接到 Microsoft 365。
   a. 点击**下一步 (Next)** 以连接到 Microsoft 365。
   b. 根据提示登录您的 Microsoft 365 帐户。此帐户必须具有全局管理员权限；帐户不会被 Secure Email Threat Defense 存储或使用。有关为什么需要这些权限的信息，请参阅思科安全电子邮件威胁防御常见问题解答：为什么设置安全电子邮件威胁防御需要 Microsoft 365 全局管理员权限？。
   c. 点击**接受 (Accept)** 以接受 Secure Email Threat Defense 应用的权限。您将被重定向回 Secure Email Threat Defense 设置页面。
   d. 单击**下一步 (Next)**。

设置邮件来源

为所选的邮件来源完成相关步骤。

Microsoft O365 邮件来源

如果您选择 Microsoft O365 作为邮件来源，则必须将 Microsoft 365 配置为向 Secure Email Threat Defense 发送日志。要执行此操作，请添加日志规则。如果您有网关，请先在 Microsoft 365 中添加连接器，然后再添加日志规则。

1. **对于使用 Cisco Secure Email Gateway (SEG) 的用户**：在 Microsoft 365 中添加一个连接器。

   为了确保日志直接从 Microsoft 365 发送到 Secure Email Threat Defense，而无需通过 Cisco Secure Email Gateway，我们建议在 Microsoft 365 中添加出站连接器。在添加连接器后才能设置日志记录。

   在 Microsoft 365 Exchange 管理中心，使用**添加连接器 (Add a connector)**向导中的以下设置来创建新的连接器：

   - **连接自 (Connection from)**：Office 365
   - **连接至 (Connection to)**：合作伙伴组织
   - **连接器名称 (Connector name)**：出站到思科安全邮件威胁防御（选中**将其打开 (Turn it on)** 复选框）
   - **使用连接器**：仅当邮件被发送到这些域时（为北美环境添加 **mail.cmd.cisco.com**，为欧洲环境添加 **mail.eu.cmd.cisco.com**）
   - **路由 (Routing)**：使用与合作伙伴的域关联的 MX 记录
   - **安全限制 (Security restrictions)**：始终使用传输层安全 (TLS) 来保护连接（推荐）；由受信任的证书颁发机构 (CA) 颁发
   - **验证邮件 (Validation email)**：Secure Email Threat Defense 设置页面中的日志地址

     注意：如果您的O365租户已使用Exchange传输规则配置了条件邮件路由，以便将出站邮件路由到现有连接器，则连接器验证可能会失败。虽然日志邮件具有系统特权，并且不受传输规则的影响，但连接器验证测试邮件没有特权，并且会受传输规则的影响。

     要解决此验证问题，请找到已有的传输规则，并为思科安全邮件威胁防御日志地址添加例外项。等待该更改生效，然后重新测试新的连接器验证。

2. 配置要向 Secure Email Threat Defense 发送日志的 Microsoft 365。要执行此操作，请添加日志规则。

   a. 从 Secure Email Threat Defense 设置页面复制您的日志地址。如果您稍后需要重复此过程，还可以在“管理”(Administration) 页面上找到您的日志地址。

   b. 转至 Microsoft Purview 合规性门户：https://compliance.microsoft.com/homepage。

   c. 导航至**解决方案 (Solutions)** > **数据生命周期管理 (Data lifecycle management)** > **Exchange（传统）(Exchange [legacy])** > **日志规则 (Journal rules)**。

   d. 如果尚未执行此操作，请将 Exchange 收件人添加到**将无法送达的日记报告发送至 (Send undeliverable journal reports to)** 字段中，然后点击**保存 (Save)**。使用的邮箱地址不会被记录；请勿使用要让 Secure Email Threat Defense 分析的地址。如果没有要用于此目的的收件人，则需要创建一个收件人。

   e. 返回**日志规则 (Journal rules)** 页面。点击 **+** 按钮创建新的日志规则。

   f. 将日志地址从 Secure Email Threat Defense 设置页面粘贴到**将日志报告发送至 (Send journal reports to)** 字段。

   g. 在**日志规则名称 (Journal rule name)** 字段中，输入 **Cisco Secure Email Threat Defense**。

   h. 在**从其发送或接收的日志邮件 (Journal messages sent or received from)** 下，选择**每个人 (Everyone)**。

   i. 在**要记录的邮件类型 (Type of message to journal)** 下，选择**所有邮件 (All messages)**。

   j. 单击**下一步 (Next)**。

   k. 查看您的选择，然后点击**提交 (Submit)** 以完成规则创建。

3. 返回 Secure Email Threat Defense 设置页面。点击**查看策略 (Review Policy)**。

网关邮件来源

如果您选择网关作为邮件来源，请启用思科安全邮件云网关的威胁防御连接器，以便将邮件发送到思科安全邮件威胁防御。

1. 从 Secure Email Threat Defense 设置页面复制邮件接收地址。如果您稍后需要重复此过程，则可以在“管理”(Administration) 页面上找到您的邮件接收地址。
2. 从安全邮件云网关用户界面中，选择**安全服务 (Security Services)** > **威胁防御连接器 (Threat Defense Connector)**。
3. 选中**启用威胁防御连接器 (Enable Threat Defense Connector)** 复选框。
4. 输入您在步骤 1 中从思科安全邮件威胁防御中复制的邮件接收地址。
5. 点击**提交 (Submit)** 以确认更改。
6. 返回 Secure Email Threat Defense 设置页面。点击**查看策略 (Review Policy)**。

查看您的策略设置

有关策略设置的信息，请参阅**策略设置，第 15 页**。如果您已选择 **Microsoft O365 身份验证：读取/写入 (Microsoft O365 Authentication:Read/Write)**模式，则应立即验证您的**自动补救(AutomatedRemediation)**设置。要将自动补救应用于所有内部邮件，请确保选中**对不在域列表中的域应用自动补救(Apply auto-remediation to domains not in the domain list)**。一旦导入域，您就可以打开**自动补救策略 (Automated Remediation Policy)** 开关。

导入 Microsoft 邮件域

Secure Email Threat Defense 从 Microsoft 365 租户导入具有邮件功能的域。导入您的域，以便对特定域应用自动补救。根据您是否选中了**对不在域列表中的域应用自动补救 (Apply auto-remediation to domains not in the domain list)** 框，Secure Email Threat Defense 会对新导入的域进行不同的处理：

- 如果选中了**对不在域列表中的域应用自动补救(Apply auto-remediation to domains not in the domain list)**，则自动补救将应用于导入的任何新域。
- 如果未选中**对不在域列表中的域应用自动补救(Apply auto-remediation to domains not in the domain list)**，则则自动补救不会应用于导入的任何新域。

默认情况下不会选中**对不在域列表中的域应用自动补救 (Apply auto-remediation to domains not in the domain list)**。

手动导入

要手动导入 Microsoft 365 邮件域（建议在首次设置 Secure Email Threat Defense 时使用）：

1. 导航至**设置**（齿轮图标）> **策略 (Policy)**。
2. 点击**更新导入的域 (Update Imported Domains)** 按钮，将您的域导入 Secure Email Threat Defense 中。
3. 使用每个域旁边的复选框来调整该域的自动补救设置。
4. 我们还建议选中**对不在域列表中的域应用自动补救(Apply auto-remediation to domains not in the domain list)**，以确保将自动补救应用于所有内部邮件以及以后自动导入的任何域。
5. 点击**保存并应用**。

自动导入

域每 24 小时会自动导入一次，以确保列表保持最新。

策略设置

设置（齿轮图标）> **策略 (Policy)** 页面上的设置确定 Cisco Secure Email Cloud Mailbox 将如何处理邮件。默认设置在您 **设置思科安全邮件威胁防御，第11页**时应用。要更改设置，请进行更改，然后点击**保存并应用(Save and Apply)**按钮。

表 1　　策略设置

设置	说明	选项	默认
消息源	定义邮件的来源。	■ **Microsoft O365** ■ **网关**（仅适用于传入邮件）	在设置思科安全邮件威胁防御时手动选择。
可视性和补救措施	定义可以应用的补救策略的类型。	■ **Microsoft 365 身份验证** - **读/写 (Read/Write)** - 允许查看和按需或自动补救（即，移动或删除可疑邮件）。将从 Microsoft 365 请求读/写权限。 - **读取 (Read)** - 仅允许显示，不允许补救措施。将从 Microsoft 365 请求只读权限。 如果选择**阅读(Read)**，则只需设置**附件分析 (Attachment Analysis)**和**邮件分析 (Message Analysis)**方向。将不会应用补救策略。 ■ **无身份验证** 仅允许可视性。	在设置思科安全邮件威胁防御时手动选择。 如果您更改 Microsoft 365 身份验证设置，则会被重定向以重置 Microsoft 365 权限。系统可能还会指示您设置日志记录；如果您已设置日志记录，则可以跳过此步骤。 **注意：**如果选择 **Microsoft 365 身份验证：读/写 (Microsoft 365 Authentication: Read/Write)**，则您还应验证**自动补救策略 (Automated Remediation Policy)** 设置。
Cisco Secure Email Gateway (SEG)	Cisco Secure Email Gateway(SEG)的存在会影响 Secure Email Threat Defense 识别发件人 IP 的方式。	■ 未选择任何内容（无 SEG） ■ **SEG 存在** - **使用思科 SEG 默认信头** (X-IronPort-RemoteIP). - **使用自定义 SEG 信头**。您必须添加要使用的信头。	在设置思科安全邮件威胁防御时手动选择。 有关详细信息，请参阅使用网关的策略设置，第 17 页。

表 1　　策略设置

设置	说明	选项	默认
邮件分析	要动态分析的邮件，包括： ■ 邮件方向 ■ Cisco Secure Malware Analytics 要分析的邮件附件的方向 ■ 垃圾邮件和灰色邮件分析	■ **邮件方向** – **传入** – **传出** – **内部** ■ **附件方向** – **传入** – **传出** – **内部** ■ **垃圾邮件和灰色邮件** – **开**或**关**	■ **邮件方向** – **全部**，Microsoft O365 邮件来源 – **传入**，网关邮件来源 ■ **附件方向** – **传入** ■ **垃圾邮件和灰色邮件** – 为 2023 年 5 月 9 日之后创建的所有账户**关闭**
自动补救策略	对发现的邮件采取的补救操作： ■ **威胁**（BEC、诈骗、网络钓鱼或恶意邮件） ■ **垃圾邮件** ■ **Graymail**	■ **不执行操作** ■ **移至隔离区** ■ **移至垃圾桶** ■ **移至垃圾邮件** **注意：**如果发件人地址属于Exchange 中的发件人允许列表，或者如果邮件已由 Microsoft 365 进行补救，则不会应用补救操作。	■ **自动补救策略**切换 – **关** ■ 威胁 – **移至隔离区** ■ 垃圾邮件 – **移至垃圾邮件** ■ 灰色邮件 – **无操作**
安全发件人：不使用垃圾邮件或灰色邮件判定来补救 Microsoft 安全发件人邮件。	如果选中此复选框，将不会对 Microsoft 在日志信头中标记为“安全发件人”且被 Secure Email Threat Defense 判定为垃圾邮件或灰色邮件的邮件进行补救。	**选中**或**取消选中**	**已取消选中**
导入的域 – 导入域以帮助确定邮件方向。域可以从自动补救策略中排除。			
应用自动补救	将自动补救应用于特定域。	**选中**或**取消选中**	**取消选中**。在打开**读/写**补救模式时，请选中这些复选框以将自动补救应用于特定域。
对不在上述域列表中的域应用自动补救	当域未明确列出时适用。例如，如果新域已被添加到您的 Microsoft 365 帐户但尚未导入。Secure Email Threat Defense	**选中**或**取消选中**	**取消选中**。当您打开**读/写**模式时，选中此复选框可确保将自动补救应用于所有内部邮件。

使用网关的策略设置

如果您有思科邮件安全设备或类似网关，请考虑使用以下策略设置。

表 2　　建议使用网关的策略设置

设置名称	推荐的选择
Cisco Secure Email Gateway (SEG)	**SEG 存在**，并指示信头
邮件分析	**传出**和**内部**
附件分析	**无**
补救措施	■ 威胁 - **移至隔离区** ■ 垃圾邮件 - **移至垃圾邮件**

务必指明存在安全邮件网关 (SEG)，以及哪个信头可用于在传入日志中识别该网关，以便 Secure Email Threat Defense 可以确定邮件的真实源发件人。如果没有此配置，则可能会出现所有邮件都来自 SEG 的情况，从而可能导致误报。

有关在思科安全邮件云网关（以前称为CES）或CiscoSecureEmailGateway（以前称为ESA）上验证或配置信头的信息，请参阅 https://docs.ces.cisco.com/docs/configuring-asyncos-message-filter-to-add-sender-ip-header-for-cloud-mailbox。

如果您使用 Microsoft 365 作为邮件来源，我们还建议绕过您的设备，以便将日志直接从 Microsoft 365 发送到 Secure Email Threat Defense。您可以通过在 Microsoft 365 中添加连接器来执行此操作，如设置思科安全邮件威胁防御，第 11 页中所述。

切换邮件来源

要更改邮件来源，请导航至**设置**（齿轮图标）> **策略 (Policy)** 页面。

1. 选择新邮件来源的单选按钮。
2. 系统将显示一条通知，指明您正在切换邮件来源。点击**继续 (Continue)**。
3. 系统将显示“切换邮件来源”对话框。您需要配置之前的邮件来源，以便停止向思科安全邮件威胁防御发送邮件。有关如何执行此操作的详细信息，请参阅删除 Secure Email Threat Defense 日志规则，第 55 页或将网关配置为停止发送邮件，第 56 页。
4. 选中表示您已停止发送先前来源的日志或邮件的复选框，然后点击**下一步 (Next)**。
5. 使用对话框中显示的邮件接收地址或日志地址来配置新邮件来源。设置邮件来源，第 12 页中详细介绍了设置每种邮件来源的步骤。

切换邮件来源

消息

“邮件”(Messages) 页面会显示您的邮件和搜索结果，并允许您查找可能的威胁。每页最多可以显示 100 封邮件。

邮件页面图标

下表显示了“邮件”(Messages) 页面上使用的图标及其含义。

表 1　　邮件页面图标

图标	名称	说明
	链接	邮件包含链接。
	附件	邮件包含附件。
	手动补救或手动重新分类	邮件已手动补救或重新分类。如果邮件经过了补救，则会在“操作”(Action) 旁边显示图标；如果对邮件进行了重新分类，则会在“判定”(Verdict) 旁边显示图标。
	追溯性判定	“追溯性判定”已被应用。“追溯性判定”是在 Secure Email Threat Defense 首次扫描邮件后应用的判定。
	允许	根据指示的项目允许邮件：允许列表、MS 允许列表或安全发件人。
	判定覆盖	判定已根据“判定覆盖”邮件规则被覆盖。
	绕过分析	由于存在绕过分析邮件规则，邮件未经过分析。指明规则的类型，即“安全发件人”或“网络钓鱼测试”。
	BEC	邮件已被手动或通过自动补救标记为“商业电子邮件泄露 (BEC)”。
	诈骗	邮件已被手动或通过自动补救标记为“诈骗”。
	网络钓鱼	邮件已被手动或通过自动补救标记为“网络钓鱼”。
	恶意	邮件已被手动或通过自动补救标记为“恶意”。
	垃圾邮件	邮件已被手动或通过自动补救标记为“垃圾邮件”。
	灰色邮件	邮件已被标记为“灰色邮件”。灰色邮件是指已被确定为营销邮件、社交邮件或垃圾邮件。
	一般	邮件已标记为“中性”。

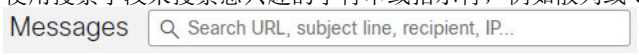
表 1　　邮件页面图标

图标	名称	说明
	传入	从 O365 租户之外收到的邮件。
	内部	发送给您的 O365 租户的邮件。
	混合	内部和外部收件人的邮件。
	传出	发送给 O365 租户之外的收件人的邮件。

搜索和过滤

使用日历控件来显示定义的时间段（最近的日、周或月）或过去 90 天内某个自定义时间范围内的数据。

使用搜索字段来搜索感兴趣的字符串或指示符，例如散列或 URL。

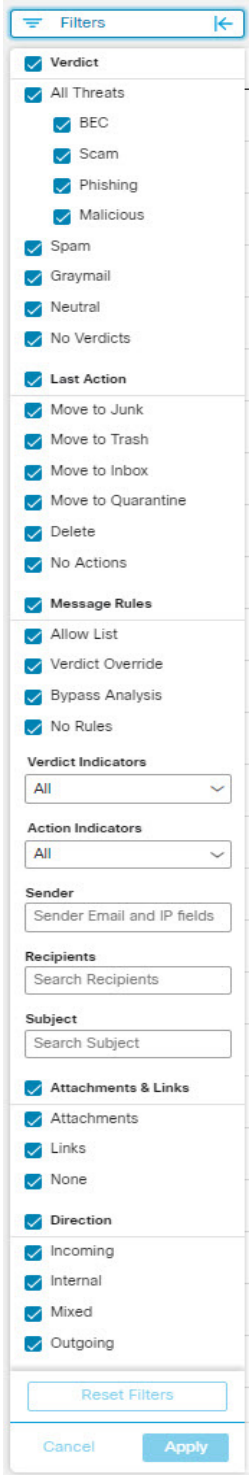


过滤器面板

使用以下过滤器来缩小搜索结果范围：例如，您可能希望查看从特定发件人发送的所有邮件、具有特定判定的邮件、包含附件或链接的邮件、已重新分类的邮件或已移至“垃圾邮件”的邮件。

1. 点击箭头以展开过滤器面板。

2. 进行选择，然后点击**应用 (Apply)**。请注意，您必须在“判定”(Verdict) 下至少选择一个项目。



使用**重置过滤器 (Reset Filters)** 按钮将过滤器重置为其默认设置。

邮件图形和快速过滤器

“邮件”(Messages) 页面顶部的邮件图形和快速过滤器可提供邮件流量的图形视图。使用该图形可快速过滤邮件。该图形包括：

- 威胁和类别分组，用于查看威胁总数并轻松过滤威胁
- 隔离区总数，可用于过滤隔离的项目
- 邮件方向总计，可用于按方向快速进行过滤

判定结果

安全邮件威胁防御会将以下威胁判定应用于邮件：

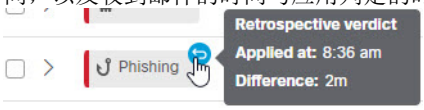
- **BEC：**商业邮件感染 (BEC) 是一种复杂的骗局，它利用社交工程和入侵技术对组织造成经济损失。
- **诈骗：**诈骗的重点是利用彩票或勒索欺诈等手段对个人造成经济损失。
- **网络钓鱼：**这些邮件被判定为欺诈性复制或模仿合法服务，试图获取用户名、密码、信用卡号等敏感信息。
- **恶意：**这些邮件会被判定为包含、提供或支持恶意软件的传送或传播。

追溯性判定

追溯性判定是在 Secure Email Threat Defense 首次扫描邮件后的某个时间应用于邮件的判定。

Secure Email Threat Defense 中的追溯性判定与其他思科安全产品中的判定略有不同。虽然 Secure Email Threat Defense 并非内联邮件处理器，但它具有完成邮件初始分析的固定时间范围。分析时间较长的较新内容引擎（例如 Talos 的深度 URL 分析）会被视为追溯性判定。由于判定被延迟，补救也会随之延迟。因此，Secure Email Threat Defense 可以清楚地标记这些判定。

追溯性判定在判定旁边的“邮件”(Messages) 页面上用蓝色图标表示。将光标悬停在图标上即可查看应用追溯性判定的时间，以及收到邮件的时间与应用判定的时间之间的差异。



追溯性判定邮件通知

要打开或关闭追溯性判定的邮件通知，请执行以下操作：

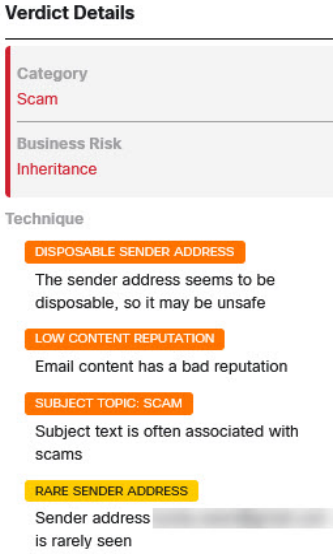
1. 选择**设置**（齿轮图标）> **管理 (Administration)** > **企业 (Business)**。
2. 在**通知邮件地址 (Notification Email Address)** 下，选择或取消选择**发送追溯性判定通知 (Send Notifications for Retrospective Verdicts)**。

如果选中此复选框，则追溯性判定邮件通知将被发送到指定的通知邮件地址。这些通知会默认处于关闭状态。

展开的邮件视图

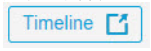
要对“邮件”(Messages) 页面搜索结果中的邮件进行调查，请选择 **>** 图标以展开邮件并查看更多详细信息，包括判定详细信息、发件人 IP、Microsoft 邮件 ID、附件、链接等。通过该视图还可以访问“时间表”(Timeline)、“对话视图”(Conversation View) 和“EML 下载”(EML Downloads)。

“判定详细信息”(Verdict Details) 列将显示判定、业务风险和使用的技术的直观表示。技术采用了颜色编码，以表明其严重性。 恶意文件名/SHA256 和 URL 会在可用时动态显示。如果无法使用动态文本，则会显示静态说明。



时间表

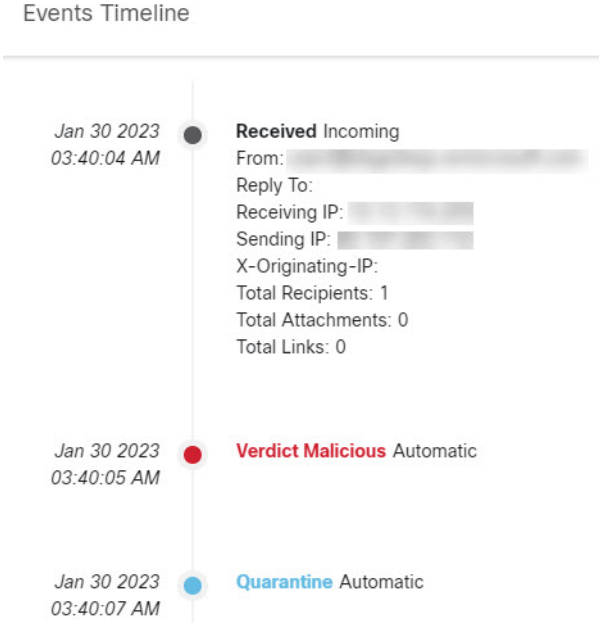
展开邮件后，点击右上角的**时间表 (Timeline)** 按钮即可查看特定邮件的事件时间表。



事件时间表会显示：

- **已接收 (Received)**：收到邮件的时间以及邮件相关详细信息
- **判定 (Verdict)**：有关所呈现的任何判定的信息
- **操作 (Action)**：有关对邮件执行的任何操作的信息

- **规则 (Rule)**：有关已应用的任何邮件规则的信息



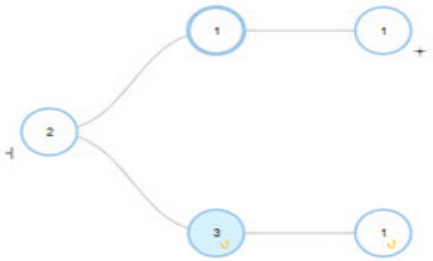
对话视图

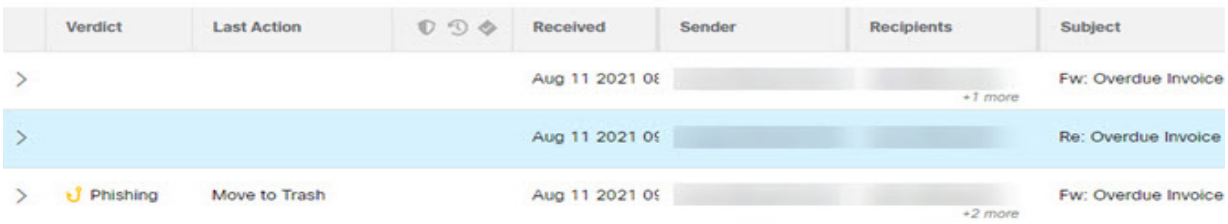
对话视图提供对话的整体视图。使用对话视图可跟踪对话中的邮件，同时全面了解邮件流。这在确定威胁的来源及其在组织内的传播方式时非常有用。

展开邮件后，点击**对话视图 (Conversation View)** 按钮即可查看与特定邮件相关的邮件。

点击 **+** 图标可展开对话的节点，以便您查看对话中更早或更晚的邮件。展开的节点将被添加到节点下方显示的邮件网格中。节点和邮件采用了颜色编码，以表示传入、传出、混合或内部。

节点圆圈内的数字表示邮件被发送到的地址数量。节点中的图标表示是否检测到威胁。在选择节点时，网格中的相应邮件会被突出显示。





SecureX Pivot 菜单

如果您的思科安全邮件威胁防御业务与SecureX集成，则可以从展开的邮件视图中访问SecureX透视菜单。有关与SecureX集成的信息，请参阅SecureX，第 49 页。

移动和重新分类邮件

如果您认为邮件分类不正确，请使用“邮件”(Messages) 页面来移动或重新分类邮件。通过更改每页显示的邮件数，一次最多可以移动或重新分类 100 封邮件。

注意：重新分类只会影响对所选邮件的判定。它不会指明来自所选发件人的未来邮件或基于邮件内容的任何更改。邮件将排队等待思科 Talos 审核。Talos 可能会使用反馈来影响未来的分类。对于误报的垃圾邮件或灰色邮件，请考虑添加判定覆盖规则，第 46 页。

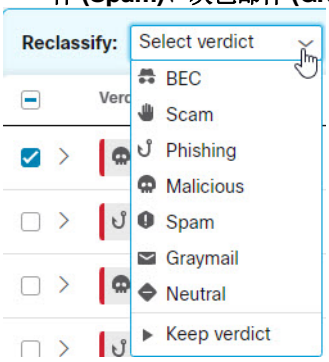
关于混合 Exchange 帐户

Secure Email Threat Defense 只能对 Exchange Online (O365) 中的邮箱执行。如果您正在将邮箱从现场 Exchange 迁移到ExchangeOnline(O365)，则补救（移动或删除）将仅适用于ExchangeOnline(O365)中的邮箱。您不会收到现场Exchange邮箱补救失败的通知。

读取补救模式

如果处于“读取”模式，则可以对邮件重新分类（应用不同的判定）。

1. 选择要重新分类的邮件。
2. 从下拉菜单中选择判定。您可以将邮件重新分类为**BEC**、**诈骗 (Scam)**、**网络钓鱼 (Phishing)**、**恶意 (Malicious)**、**垃圾邮件 (Spam)**、**灰色邮件 (Graymail)** 或**中性 (Neutral)**，或者也可以选择**保留判定 (Keep verdict)**。



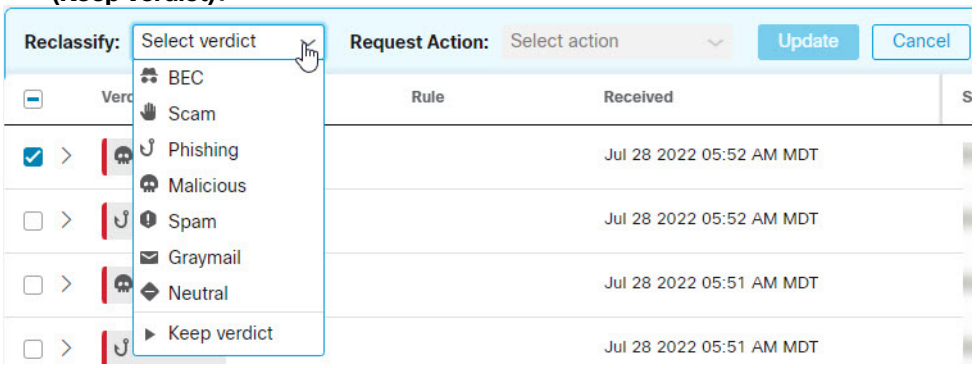
3. 点击**更新 (Update)** 以应用新分类。

读/写补救模式

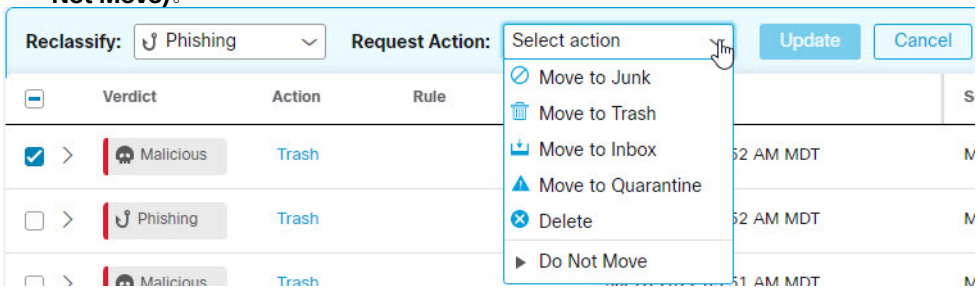
如果处于读/写补救模式，则可以将可疑邮件从用户收件箱移至其垃圾邮件或垃圾桶，或移至其无法访问的隔离区文件夹。同样，如果您确定被移至垃圾邮件、垃圾桶或隔离区的邮件并无可疑之处，则可以将其移回用户的收件箱。您也可以彻底删除邮件。该过程还允许您对邮件重新分类（应用不同的判定）。

1. 选择要移动或重新分类的邮件。

2. 从“重新分类”(Reclassify) 下拉菜单中选择判定。您可以将邮件重新分类为 **BEC**、**诈骗 (Scam)**、**网络钓鱼 (Phishing)**、**恶意 (Malicious)**、**垃圾邮件 (Spam)**、**灰色邮件 (Graymail)** 或**中性 (Neutral)**，或者也可以选择**保留判定 (Keep verdict)**。



3. 从“请求操作”(Request Action) 下拉菜单中选择操作。您可以选择**移至垃圾邮件 (Move to Junk)**、**移至垃圾桶 (Move to Trash)**、**移至收件箱 (Move to Inbox)**、**移至隔离区 (Move to Quarantine)**、**删除 (Delete)**，或者也可以选择**不移动 (Do Not Move)**。



4. 点击**更新 (Update)** 以应用新分类并对邮件执行操作。

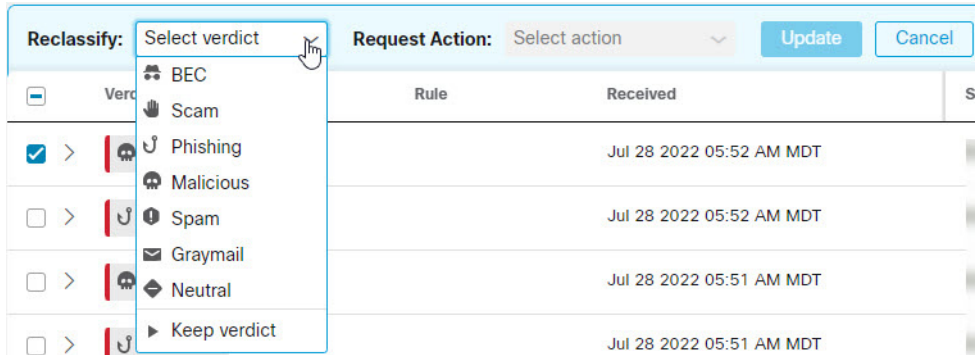
如果邮件已被移动，则会在**上次操作 (Last Action)** 列中指明。

删除邮件

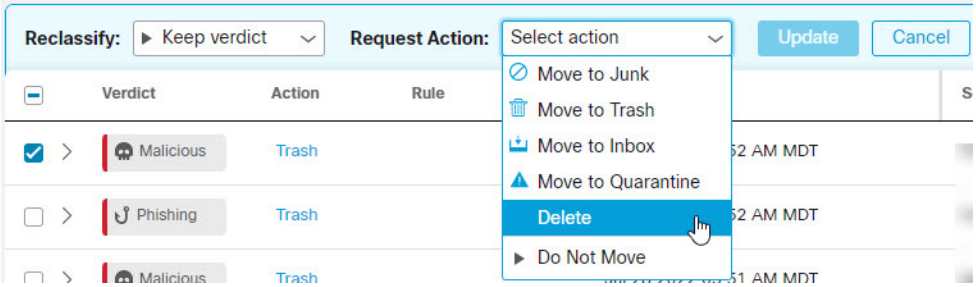
超级管理员和管理员用户可以使用“重新分类/补救”工作流程中的“删除”操作从邮箱中永久删除邮件。已删除的邮件会被移至 **recoverableitemspurges** 文件夹。用户无法访问此文件夹，并且 Secure Email Threat Defense 无法将已删除的邮件恢复到收件箱。

1. 选择要删除的邮件。

2. 从“重新分类”(Reclassify) 下拉菜单中选择判定。您可以将邮件重新分类为 **BEC**、**诈骗 (Scam)**、**网络钓鱼 (Phishing)**、**恶意 (Malicious)**、**垃圾邮件 (Spam)**、**灰色邮件 (Graymail)** 或**中性 (Neutral)**，或者也可以选择**保留判定 (Keep verdict)**。



3. 从“请求操作”(Request Action) 下拉菜单中选择**删除 (Delete)**。



4. 点击**更新 (Update)** 以删除邮件。

5. “确认删除”(Confirm Deletion) 对话框指明邮件无法恢复，并确认是否要继续。点击**删除 (Delete)** 以继续。

上次操作 (Last Action) 列中会指明“删除”(Delete)。

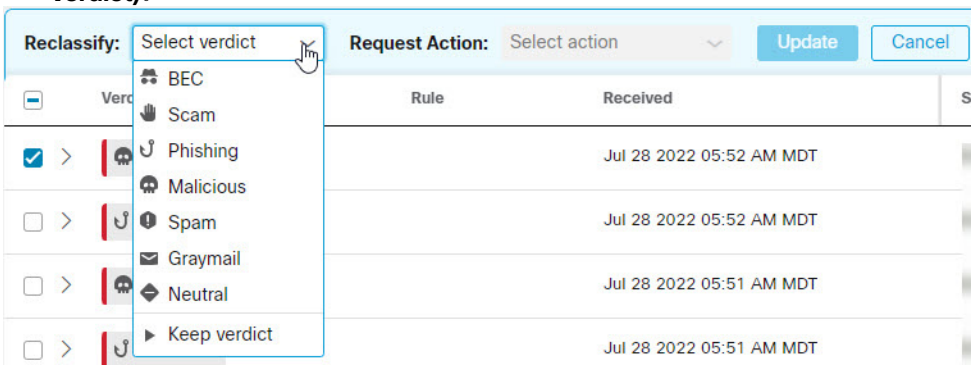
隔离邮件

隔离区文件夹是为每个邮箱自动创建的，并且 Outlook 用户不会看到该文件夹。超级管理员和管理员用户可以在**管理 (Administration) > 企业 (Business)** 页面中看到隐藏文件夹的名称。在 Outlook 中，隔离区文件夹中的邮件将根据您的“已删除邮件”(Deleted Items) 清除设置自动进行清除。Secure Email Threat Defense 当邮件从隔离区文件夹中清除后，其无法再被恢复到用户收件箱。

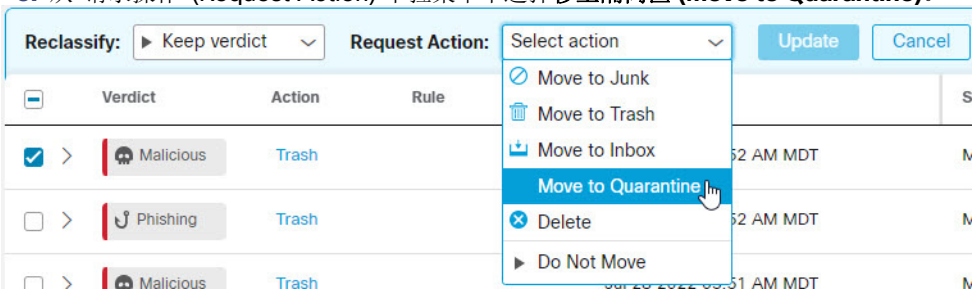
要将邮件手动移动至隔离区，请执行以下操作：

1. 选择要移至隔离区的邮件。

2. 从“重新分类”(Reclassify) 下拉菜单中选择判定。您可以将邮件重新分类为 **BEC**、**诈骗 (Scam)**、**网络钓鱼 (Phishing)**、**恶意 (Malicious)**、**垃圾邮件 (Spam)**、**灰色邮件 (Graymail)** 或**中性 (Neutral)**，或者也可以**保留判定 (Keep verdict)**。



3. 从“请求操作”(Request Action) 下拉菜单中选择**移至隔离区 (Move to Quarantine)**。



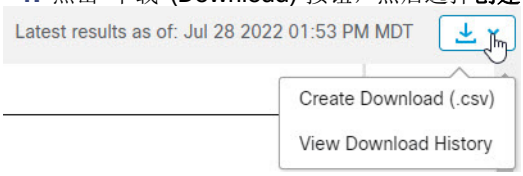
4. 点击**更新 (Update)** 以隔离邮件。

上次操作 (Last Action) 列中会指明“移至隔离区”(Move to Quarantine)。

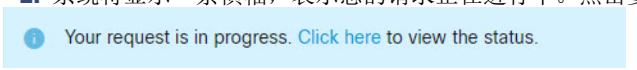
下载搜索结果

您可以将搜索结果中邮件数据作为 CSV 文件进行下载。下载限制为 10,000 封邮件。要下载数据，请完成以下步骤：

1. 点击“下载”(Download) 按钮，然后选择**创建下载 (.csv) (Create Download [.csv])**。



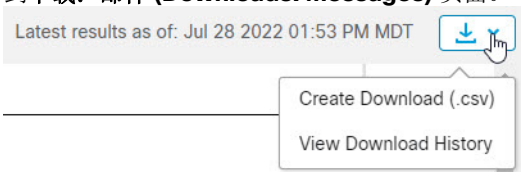
2. 系统将显示一条横幅，表示您的请求正在进行中。点击要转到**下载：邮件 (Downloads: Messages)** 页面的文本。



3. 当下载就绪时，点击“操作”(Actions) 列下的“下载”(Download) 图标以下载文件。

下载历史

您的下载历史记录将保留 90 天。点击“下载”(Download) 按钮，然后选择**查看下载历史记录 (View Download History)** 以转到**下载：邮件 (Downloads: Messages)** 页面。



该页面会显示日期范围、请求下载的用户、启动日期和状态。通过选择“操作”(Actions) 列下的“下载”(Download) 图标下载文件。

下载

通过**设置**（齿轮图标）> **下载 (Downloads)** 页面，您可以创建和/或管理：

- 搜索结果邮件数据 CSV
- 补救错误日志 CSV
- EML 下载请求

消息

您可以通过两种方式来下载邮件数据：

- 从“邮件”(Messages) 页面，如下载搜索结果，第 28 页中所述。如果要下载特定的过滤数据或较长时段的数据，请使用此选项。它将为当前搜索和过滤结果中的邮件创建一个 CSV 文件。
- 通过**设置**（齿轮图标）> **下载 (Downloads)** > **邮件 (Messages)** 选项卡，如下所示。如果要下载特定时段（例如过去 24 小时、过去 7 天或特定日期或周）的所有邮件数据，这将非常有用。

要从“下载”(Downloads) 页面创建并下载邮件数据的 CSV，请执行以下操作：

1. 选择**设置**（齿轮图标）> **下载 (Downloads)**。
2. 选择**邮件 (Messages)**。
3. 点击**创建 CSV (Create CSV)**。
4. 在显示的对话框中，选择要为其创建下载的日期范围，然后点击**创建 CSV (Create CSV)**。
5. 当下载就绪时，点击“操作”(Actions) 列下的“下载”(Download) 图标以下载文件。

EML 下载

超级管理员和管理员用户可以从展开的邮件视图请求 EML 下载。可从“下载”(Downloads) 页面进行下载，直到下载完成或 7 天之后（以先到者为准）。文件可以下载一次。您可以直接从**设置 (Settings)** > **下载 (Downloads)** 访问“下载”(Downloads) 页面。

要请求并下载 EML 文件，请执行以下操作：

1. 展开邮件后，点击**请求 EML 下载 (Request EML Download)** 按钮。
2. 系统将显示一条横幅，表示您的请求正在进行中。点击将要转到**下载：下载 EML(DownloadsDownloadEML)** 页面的文本。

3. 当下载就绪时，点击“操作”(Actions) 列下的“下载”(Download) 图标以下载文件。

补救错误日志

如果发生补救错误，则通知（钟形图标）菜单下会显示一条通知。补救错误日志允许您调查单个邮箱的任何补救失败情况。例如，如果邮件已被邮箱所有者删除，则“移至垃圾桶”(Move to Trash) 请求可能会失败。补救错误日志将显示为*未找到资源 (Resource is not found)*。

您可以通过展开通知并点击**请求下载 (Request Download)**，直接从通知请求下载错误日志。

或者，完成以下步骤以创建和下载补救错误日志：

1. 选择**设置**（齿轮图标）> **下载 (Downloads)**。
2. 选择**补救错误日志 (Remediation Error Log)**。
3. 点击**创建 CSV (Create CSV)**。
4. 在显示的对话框中，选择要为其创建下载的日期范围，然后点击**创建 CSV (Create CSV)**。
5. 当下载就绪时，点击“操作”(Actions) 列下的“下载”(Download) 图标以下载文件。

洞察

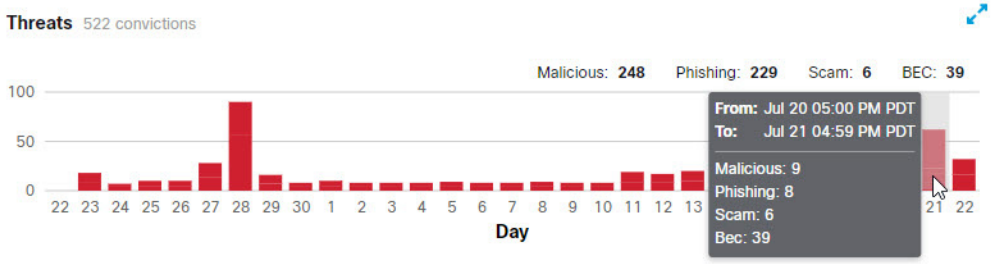
趋势

“趋势”(Trends) 页面会显示有关邮件数据的图形信息。通过选择**见解 (Insights) > 趋势 (Trends)**来查看趋势。

- 使用日历控件来显示特定天、周或月的数据。
- 点击图形中感兴趣的数据，即可转到“邮件”(Messages) 页面上的数据详细信息。
- 点击图例项可转到“邮件”(Messages) 页面上的相关数据。例如，点击传入可查看当前显示在图表上的所有传入邮件。
- 点击下载按钮以下载趋势数据。结果将导出为 CSV 文件，其中包括：
  - 如果您查看的是过去 24 小时或特定日期，则为过去 90 天的每小时汇总数据
  - 如果您查看的是最近 30 天的数据，则为过去 90 天的 24 小时汇总数据
- 点击打印按钮打印趋势图表，或者将其另存为 PDF。

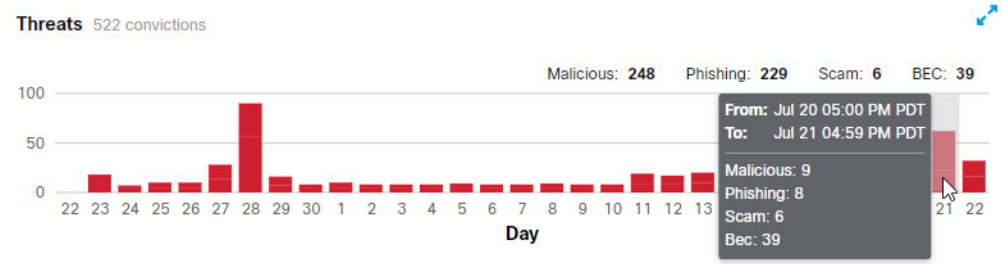
关于时区

“天”(Day) 图表上的每个条形图表示一小时的数据。这些图表会以您的浏览器的本地时区为准。



“周”(Week) 或“月”(Month) 图表上的每个条形图表示一天 24 小时的数据。一天是以世界协调时间的 00:00 至 11:59 为准，然后再转换为浏览器的本地时间。

例如，如果您使用的是太平洋夏令时 (PDT) UTC-07:00，则“月”(Month) 图表上的条形图将表示从太平洋时间 7 月 20 日下午 5:00 到 7 月 21 日下午 4:59。

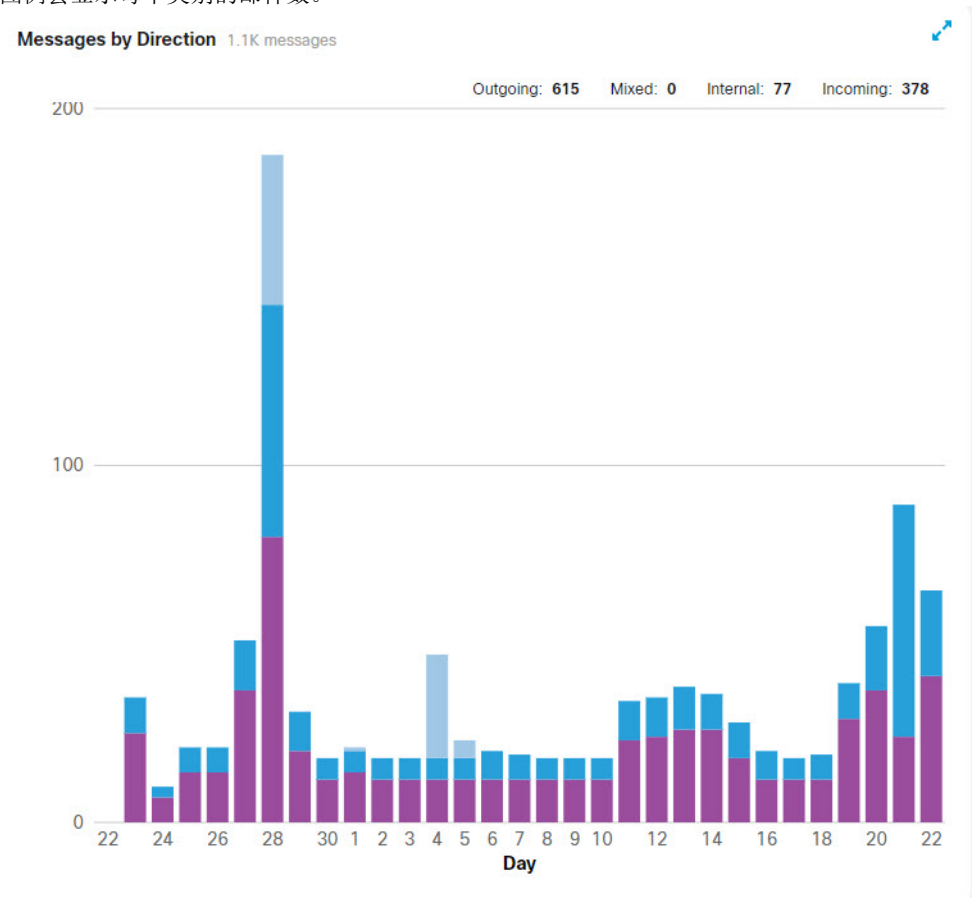


按方向分类的邮件

“按方向分类的邮件”(Messages by Direction) 图形会显示您的邮件总流量。邮件会被分为以下类别：

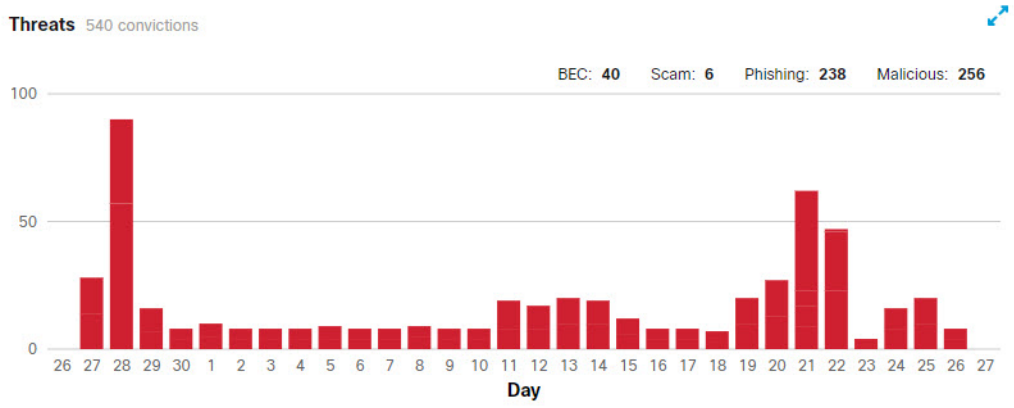
- **传出：**发送给 O365 租户之外的收件人的邮件
- **混合：**包含内部和外部收件人的邮件
- **内部：**发送给您的 O365 租户的邮件
- **传入：**从 O365 租户之外收到的邮件

图例会显示每个类别的邮件数。



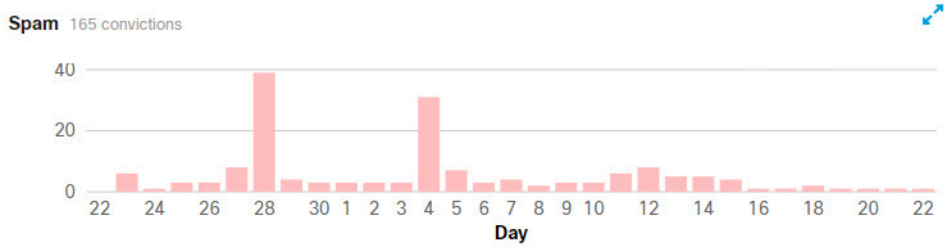
威胁

“威胁”(Threats) 图形会显示被确定存在威胁的邮件的快照。这些邮件包括商业电子邮件泄露 (BEC)、诈骗、网络钓鱼和恶意软件。图例会显示每个类别的邮件数。点击要转到“邮件”(Messages) 页面的数据。



垃圾邮件

“垃圾邮件”(Spam) 图形会显示被确定为垃圾邮件的邮件快照。图例会显示被确定为垃圾邮件的邮件总数。



Graymail

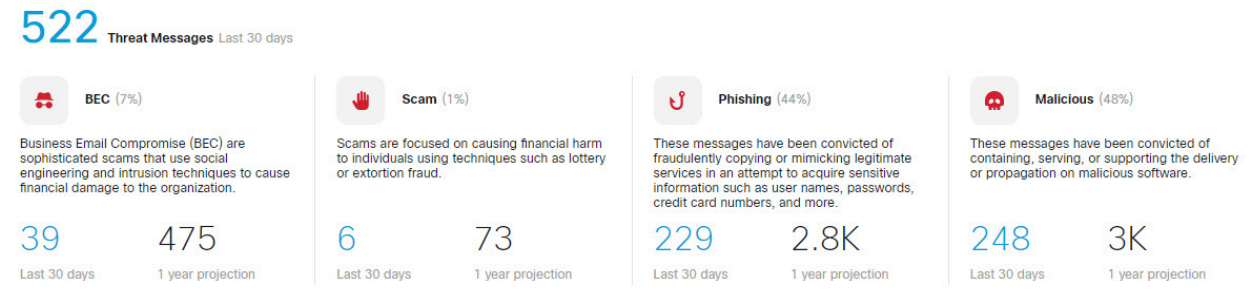
“灰色邮件”(Graymail) 图形会显示被确定为灰色邮件的邮件快照。图例会显示被确定为灰色邮件的邮件总数。

影响报告

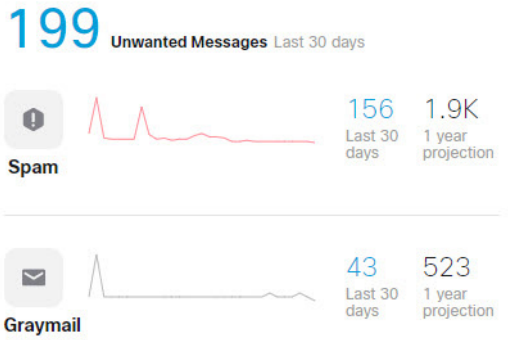
“影响报告”(Impact Report) 会显示过去 30 天内 Secure Email Threat Defense 所带来的好处。选择**见解 (Insights) > 影响报告 (Impact Report)** 以查看报告。点击报告中感兴趣的数据，即可转到“邮件”(Messages) 页面上的数据详细信息。

显示的数据包括：

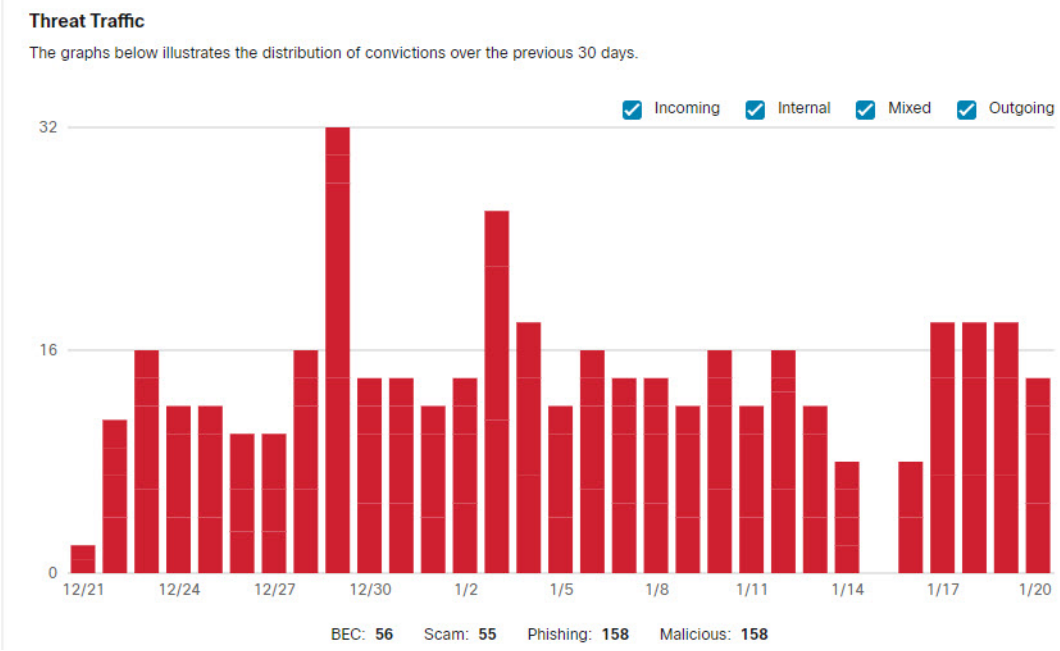
- 在所选的 30 天内由 Secure Email Threat Defense 捕获的威胁邮件，以及此数据的 1 年预测。1 年预测的计算方式为每日平均值乘以 365。



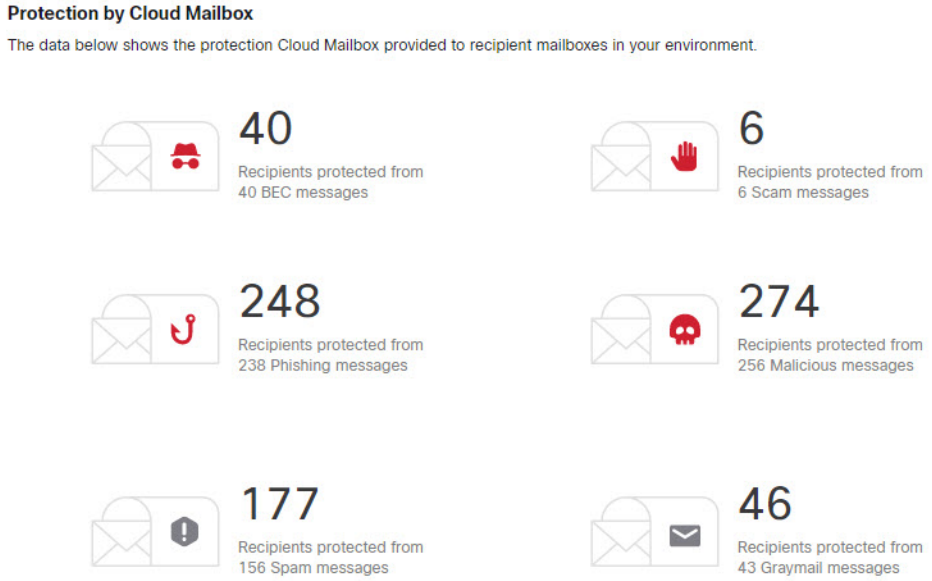
- 不需要的邮件。此图表会显示所选的 30 天内的垃圾邮件和灰色邮件，以及此数据的 1 年预测。1 年预测的计算方式为每日平均值乘以 365。



- 威胁流量。此图表会显示所选 30 天内的认定情况。您可以按方向过滤此图表。



- 由 Secure Email Threat Defense 保护。此图表会显示 Secure Email Threat Defense 为您的环境中的收件人邮箱提供的保护。



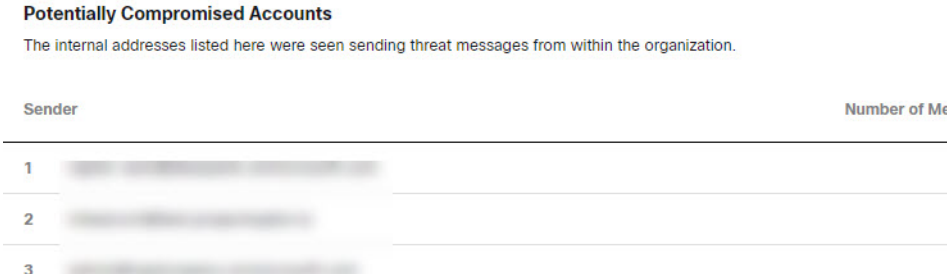
- 主要目标。此图表会显示在所选 30 天内威胁邮件主要针对的前十个内部目标。

Top Targets

The statistics below indicate the addresses which received the most threat messages over the previous 30 days.

	Recipient	BEC	Scam	Phishing	Malicious	Totals
1	[redacted]	1	0	109	107	217
2	[redacted]	0	0	36	36	72
3	[redacted]	0	0	15	30	45
4	[redacted]	0	0	16	22	38
5	[redacted]	0	0	17	17	34
6	[redacted]	0	0	10	19	29
7	[redacted]	0	0	14	14	28
8	[redacted]	0	0	9	18	27
9	[redacted]	0	0	14	9	23
10	[redacted]	12	0	0	0	12

- 内部威胁发件人。此图表会显示威胁邮件的前十个内部发件人。



重大影响人员名单

注意：此功能尚在早期现场试用阶段，并会随着时间的推移不断改进。立即构建您的名单，随着时间的推移，您将在“判定详细信息”(Verdict Details) 中看到“用户模拟”(User Impersonation) 技术。

重要人员（例如执行领导团队的成员）存在被他人冒充以试图危害其他目标的风险。重大影响人员名单有助于思科安全邮件威胁防御抵御假冒攻击。

管理员可以创建一个最多 100 人的名单并将其发送给思科 Talos，以便对显示名称和发件人邮箱地址进行更严格的审查。与个人配置信息的偏差将在判定邮件的判定详细信息”(Verdict Details) 面板中标识为“技术”(Technique)。

将用户添加到重大影响人员名单

完成以下步骤，以便将用户添加到重大影响人员名单：

1. 选择**设置**（齿轮图标）> **重大影响人员 (High Impact Personnel)**。
2. 点击**添加新人员 (Add New Personnel)** 按钮。
3. 输入用户的信息。“名字”(First Name)、“姓氏”(Last Name) 和“电子邮件地址”(Email Address) 为必填。
4. 点击**提交 (Submit)** 以完成将用户添加到名单中的操作。

更新重大影响人员名单中的用户信息

完成以下步骤，以便编辑重大影响人员名单中的用户信息：

1. 选择**设置**（齿轮图标）> **重大影响人员 (High Impact Personnel)**。
2. 在“操作”(Actions) 列下，点击**编辑**（铅笔）按钮。
3. 根据需要更新用户的信息。“名字”(First Name)、“姓氏”(Last Name) 和“电子邮件地址”(Email Address) 为必填。
4. 点击**提交 (Submit)** 以完成编辑用户信息的操作。

从重大影响力人员名单中删除用户

完成以下步骤，以便从重大影响人员名单中删除用户：

1. 选择**设置**（齿轮图标）> **重大影响人员 (High Impact Personnel)**。
2. 在“操作”(Actions) 列下，点击**删除 (Delete)** 按钮。
3. 在“确认删除”(Confirm Removal) 对话框中点击**删除 (Delete)** 以完成操作。

从重大影响力人员名单中删除用户

管理用户

从**设置**（齿轮图标）> **管理 (Administration)** > **用户 (Users)** 页面管理您的用户帐户。

Secure Email Threat Defense 使用思科 SecureX 登录 SSO 解决方案，以便进行用户身份验证管理。有关 Cisco Security Cloud 登录的信息，请参阅 https://cisco.com/go/securesignon。

注意：如果您是 Cisco SecureX Threat Response、Cisco Secure Malware Analytics（以前称为 Cisco Threat Grid）或 Cisco Secure Endpoint（以前称为 AMP）的客户，请务必使用现有的 Cisco Security Cloud 登录凭证进行登录。如果您不是现有用户，则必须创建一个新的 Cisco Security Cloud 登录帐户

虽然 Cisco Security Cloud 登录允许您使用其他类型的帐户进行登录，但我们建议您使用 Cisco Security Cloud 登录帐户，以便保持您的思科安全产品帐户的连接。

多帐户访问

您可以使用同一个 Cisco Security Cloud 登录帐户访问多个 Secure Email Threat Defense 实例。这样可以更轻松地跟踪每个实例，而无需注销并使用单独的 Cisco Security Cloud 登录帐户重新登录。

按照创建新用户，第 39 页中的步骤将用户添加到其他 Secure Email Threat Defense 实例。使用相同 Cisco Security Cloud 登录帐户的帐户将可从其“用户”(User) 菜单来访问。请注意，此访问权限仅限于同一地区（北美、欧洲或亚太及日本）的 Secure Email Threat Defense 实例。

用户角色

基于角色的访问控制 (RBAC) 允许您在应用中为用户提供不同级别的控制或访问权限。Secure Email Threat Defense 可以在下表中描述的角色中创建用户。

表 1　　用户角色

角色	说明
超级管理员	这些用户可以访问 Secure Email Threat Defense 中的所有功能。他们可以更改设置和策略，并对邮件进行重新分类和补救。
管理员	这些用户具有超级管理员的所有功能，但不能创建、编辑或删除超级管理员或管理员用户。
分析师	这些用户可以使用搜索和见解功能。他们可以对邮件进行重新分类和补救，但不能从用户邮箱中删除邮件。他们无法更改帐户设置或策略，也无法创建新用户。
只读	这些用户可以使用搜索和见解功能。他们无法对邮件进行重新分类或补救，无法更改帐户设置或策略，也无法创建新用户。

创建新用户

完成以下步骤以创建新用户：

1. 选择**设置**（齿轮图标）> **管理 (Administration)** > **用户 (Users)**。
2. 点击**添加新用户**。
3. 输入用户的凭证，选择角色，然后点击**创建 (Create)**。

注意：用户的邮箱地址*必须*与其 Cisco Security Cloud 登录帐户使用的邮箱地址相匹配。

用户收到主题为**欢迎使用 (Welcome to)思科安全邮件威胁防御** 的邮件。他们必须按照邮件中的说明来设置 Cisco Security Cloud 登录帐户（如果还没有）并登录。

编辑用户

您可以更新用户的角色。您无法编辑用户的邮件地址。如果用户更改其姓名，则必须在其 Cisco Security Cloud 登录账户中进行更新。

要编辑用户的角色，请执行以下操作：

1. 选择**设置**（齿轮图标）> **管理 (Administration)** > **用户 (Users)**。
2. 在“操作”(Action) 列下点击铅笔。
3. 在“编辑用户”(Edit User) 对话框中，为用户选择新角色，然后点击**保存更改 (Save changes)**。

删除用户

完成以下步骤以删除用户：

1. 选择**设置**（齿轮图标）> **管理 (Administration)** > **用户 (Users)**。
2. 在“操作”(Action) 列下点击 X 图标。
3. 在“确认删除”(Confirm Deletion) 对话框中点击**删除 (Delete)** 以完成操作。

一条状态消息将显示删除已完成。此操作会从 Secure Email Threat Defense 中删除用户的帐户，但不会删除其 Cisco Security Cloud 登录帐户。如果要从多个 Secure Email Threat Defense 实例中删除用户，则必须为每个实例完成这些步骤。

用户设置

可通过**用户 (User)**（配置文件图标）> **用户设置 (User Settings)** 访问各个用户配置文件的设置。

详情

详细信息部分包括您的用户名、角色和组织。

偏好设置

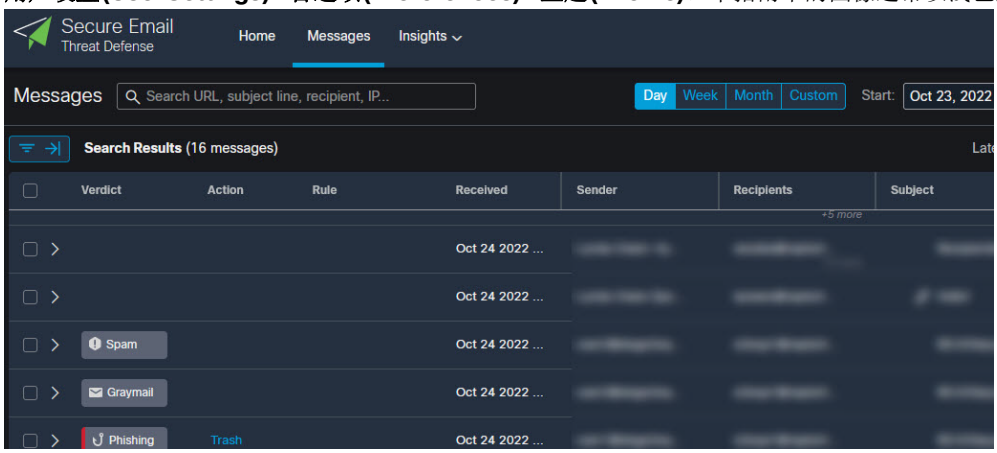
“首选项”(Preferences) 部分包括 SecureX 功能区授权和主题外观设置。

SecureX 功能区

Secure Email Threat Defense 与 SecureX 功能区相集成。功能区让您可以在思科安全产品之间导航、访问案例集、搜索可观察对象以及查看事件。SecureX 功能区按用户进行授权。有关详细信息，请参阅SecureX 集成，第 49 页。

主题

您可以选择使用浅色或深色背景来查看 Secure Email Threat Defense。要切换模式，请转至**用户 (User)**（配置文件图标）> **用户设置(User Settings)**> **首选项(Preferences)**> **主题(Theme)**。本指南中的图像通常以浅色主题显示。深色背景如下所示。



偏好设置

管理设置

可从**设置**（齿轮图标）> **管理 (Administration)** > **企业 (Business)** 访问本部分中介绍的管理设置。

帐户详细信息

“帐户详细信息”(Account Details) 部分显示以下内容：

- Microsoft 365 租户 ID
- 日志地址
- 企业 ID
- 隔离文件夹 ID
- 支持订用 ID
- 许可证信息，包括：
  - 许可证类型
  - 订用 ID
  - 座席数
  - 开始日期
  - 结束日期

偏好设置

“首选项”(Preferences) 部分包括您的通知邮件地址、对审核日志的访问权限以及您的 Google 分析设置。

通知电邮

通知邮件地址是 Secure Email Threat Defense 会将通知邮件发送到的地址。例如，我们可能会发送有关系统更新、新功能、计划维护等的通知。这最初会被设置为您的第一个用户的邮件地址。

您可以选择是否将追溯性判定通知发送到您的通知邮件地址。在将追溯判定应用于邮件时，系统将发送一封邮件。

审核日志

您可以作为 CSV 文件下载前 3 个月的审核日志。从下拉列表中选择日期范围，然后点击**下载 CSV (Download CSV)**。

Google Analytics

当您设置 Secure Email Threat Defense 并接受条款和条件时，最初会启用或禁用 Google 分析。启用后，思科会收集非个人可识别的使用数据，包括但不限于发件人、收件人、主题和URL，并可能与Google分析共享这些数据。这些数据让我们能更好地了解 Secure Email Threat Defense 如何满足您的需求。

SecureX

Secure Email Threat Defense 与 SecureX 集成。SecureX 让您可以在其他思科安全产品的数据旁边查看 Secure Email Threat Defense 信息。有关此设置的详细信息，请参阅**SecureX 集成，第 49 页**。

邮件规则

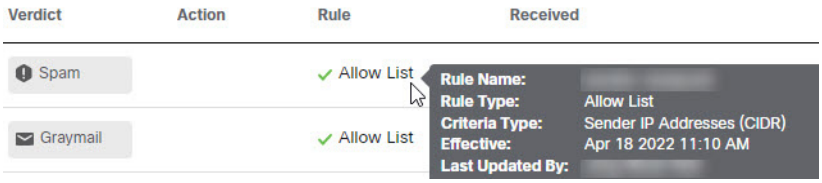
邮件规则允许您指定不应补救或扫描的某些类型的邮件。您可以创建：

- “允许列表”规则
- “判定覆盖”规则
- “绕过分析”规则

注意：“允许列表”和“判定覆盖”规则不适用于无身份验证模式下的企业。

从**设置 (Settings) > 邮件规则 (Message Rules)** 页面创建和管理邮件规则。

“绕过分析”规则优先于“允许列表”和“判定覆盖”规则。如果邮件受规则影响，则会在“邮件”(Messages) 页面的“邮件规则”(Message Rules) 列中指明。将光标悬停在“邮件规则”(Message Rules) 列中的项目上即可查看应用的规则。



注意：规则不会自动应用于子域。域会完全按照规则中的指示进行匹配。

允许列表规则

“允许列表”规则让您能够阻止对来自特定发件人邮件地址、发件人域或发件人 IP 地址的垃圾邮件和灰色邮件进行补救。系统仍会分析邮件，但不会应用自动补救。例如，如果 Secure Email Threat Defense 确定来自某个发件人的项目是垃圾邮件，但您希望将这些项目保留在用户收件箱中，则可以创建“允许列表”规则来覆盖对此类邮件进行补救的任何策略。“允许列表”规则是策略的例外情况。与“允许列表”规则匹配的邮件仍会显示在“影响”(Impact) 报告中。

“允许列表”规则：

- 应用于灰色邮件和/或垃圾邮件。
- 指定允许的发件人邮件地址、发件人域或发件人 IP 地址（IPv4 或 CIDR 块）。
- 每个规则最多可以包含 50 个条件。也就是说，可以包含 50 个邮件地址、域或地址。

活动规则的数量限制为 20。规则可以停用，但不能删除。

判定覆盖规则

“判定覆盖”规则允许您覆盖与规则指定的条件匹配的垃圾邮件和灰色邮件判定。邮件会被标记为“中性”判定，并且不会进行补救。判定被覆盖的邮件不会显示在“影响”(Impact) 报告中。

“判定覆盖”规则：

- 应用于灰色邮件和/或垃圾邮件。
- 指定允许的发件人邮件地址、发件人域或发件人 IP 地址（IPv4 或 CIDR 块）。
- 每个规则最多可以包含 50 个条件。也就是说，可以包含 50 个邮件地址、域或 IP 地址。

活动规则的数量限制为 20。规则可以停用，但不能删除。

绕过分析规则

“绕过分析”规则让您能绕过对网络钓鱼测试或安全邮箱邮件的分析。符合规则条件的邮件将绕过所有引擎分析，因此您可以在不受引擎干扰的情况下处理安全测试。Secure Email Threat Defense 不会打开或扫描附件和链接。

“网络钓鱼测试”规则：

- 应用于来自指定发件人邮件地址、发件人域或 IP 地址的所有传入邮件（IPv4 或 CIDR 块）；邮件不会被分析。
- 每个规则最多可以包含 50 个条件。

“安全邮箱”规则：

- 应用于指定收件人邮件地址的传入邮件；邮件不会被分析。

  注意：如果指定的收件人是邮件的唯一收件人，则会应用“安全邮箱”规则。如果其他收件人被复制或作为密件抄送（密件抄送），则邮件不会绕过分析引擎。

- 每个规则最多可以包含 50 个条件。

活动“绕过分析”规则的数量限制为 20。规则可以停用，但不能删除。

添加邮件规则

添加邮件规则的步骤会因规则类别而异。

添加新的允许列表或判定覆盖规则

完成以下步骤以创建新规则：

1. 选择**设置**（齿轮图标）> **邮件规则 (Message Rules)**。
2. 选择要创建的规则类别：**允许列表 (Allow List)** 或**判定覆盖 (Verdict Override)**。
3. 点击 **Add New Rule** 按钮。
4. 创建规则名称。每个规则必须有唯一名称。
5. 选择条件类型。您可以选择发件人邮件、发件人域、发件人 IP 地址 (IPv4) 或发件人 IP 地址 (CIDR)。
6. 输入允许的项目，以逗号分隔。

7. 根据要允许的判定，选择“垃圾邮件”(Spam)和/或“灰色邮件”(Graymail)。
8. 点击**提交 (Submit)** 完成创建此规则。

您的规则会被添加到列表中。更改最多可能需要 20 分钟即可生效。

添加新的绕过分析规则

完成以下步骤以创建新规则：

1. 选择**设置**（齿轮图标）> **邮件规则 (Message Rules)**。
2. 选择**绕过分析 (Bypass Analysis)**。
3. 点击 **Add New Rule** 按钮。
4. 创建规则名称。每个规则必须有唯一名称。
5. 选择要创建的规则类型：**网络钓鱼测试 (Phish Test)** 或**安全邮箱 (Security Mailbox)**。
6. 对于网络钓鱼测试规则，请选择条件类型：发件人邮件地址、发件人域、发件人 IP 地址 (IPv4) 或 IP 地址 (CIDR)。然后，输入您的项目，以逗号分隔。

   对于安全邮箱规则，请输入收件人邮件地址，以逗号分隔。
7. 点击**提交 (Submit)** 完成创建此规则。

您的规则会被添加到列表中。更改最多可能需要 20 分钟即可生效。

编辑规则

请注意，只能编辑已启用的规则。要编辑规则，请执行以下操作：

1. 选择**设置**（齿轮图标）> **邮件规则 (Message Rules)**。
2. 选择要编辑的规则类型。
3. 在“操作”(Actions) 列下，点击要编辑的规则旁边的铅笔图标。
4. 进行所需的更改，然后点击**保存更改 (Save Changes)**。

您的规则已更新。更改最多可能需要 20 分钟即可生效。

启用或禁用规则

要启用或禁用现有规则，请执行以下操作：

1. 选择**设置**（齿轮图标）> **邮件规则 (Message Rules)**。
2. 选择要启用或禁用的规则类型。
3. 在“操作”(Actions) 列下，点击要更改其状态的规则旁边的启用或禁用图标。

规则的状态已更新。更改最多可能需要 20 分钟即可生效。

Microsoft 允许列表和安全发件人

Secure Email Threat Defense 遵循添加到 Microsoft 365 垃圾邮件和灰色邮件中的垃圾邮件过滤器允许列表中的发件人和域。恶意或网络钓鱼判定不遵循 MS 允许列表。有关详细信息，请参阅思科安全邮件威胁防御常见问题解答：思科安全邮件威胁防御和 Microsoft 365。

如果您的组织允许个人用户在其邮箱中配置允许列表，并且邮件恰好属于用户的允许列表，则 Secure Email Threat Defense 不总是遵循 Microsoft 允许列表。如果要让 Secure Email Threat Defense 遵循这些设置，请在“策略”(Policy) 页面上选中**不补救包含垃圾邮件或灰色邮件判定的Microsoft安全发件人邮件(DonotremediateMicrosoftSafeSendermessages withSpamorGraymailverdicts)**复选框。垃圾邮件和灰色邮件判定会遵循安全发件人标志，但恶意和网络钓鱼判定不会遵循安全发件人标志。也就是说，带有垃圾邮件或灰色邮件判定的安全发件人邮件将不会进行补救。

SecureX 集成

思科 SecureX 将思科安全产品连接到了一个集成平台。Secure Email Threat Defense 与 SecureX 和 SecureX 功能区集成。

- SecureX 让您可以在其他思科安全产品的数据旁边查看 Secure Email Threat Defense 信息。
- SecureX 功能区让您可以在思科安全产品之间导航、访问案例集、搜索可观察对象以及查看事件。

有关本文档中未提供的 SecureX 的详细信息，请参阅 SecureX 文档：https://docs.securex.security.cisco.com/

SecureX

Secure Email Threat Defense 提供可在 SecureX 控制面板中查看的以下磁贴：

- 按方向分类的邮件：按方向显示总邮件流量。邮件被分为传出邮件、混合邮件、内部邮件和传入邮件。
- 威胁：显示被确定为 BEC、诈骗、网络钓鱼或恶意的邮件的快照。
- 垃圾邮件：显示被确定为垃圾邮件的邮件的快照。
- 灰色邮件：显示被确定为灰色邮件的邮件的快照。
- 恶意和网络钓鱼：显示被确定为恶意或网络钓鱼的邮件的快照。

  注意：该磁贴即将被弃用，在未来版本中将被删除。您应从 SecureX 控制面板中删除“恶意和网络钓鱼”磁贴，并改为使用“威胁”磁贴。

有关 SecureX 控制面板的信息，请参阅 SecureX 文档：https://docs.securex.security.cisco.com/

为思科安全邮件威胁防御授权 SecureX

您必须拥有 SecureX 帐户并且是 SecureX 组织的成员，然后才能为 Secure Email Threat Defense 授权 SecureX。有关详细信息，请参阅 SecureX 文档：https://docs.securex.security.cisco.com/SecureX-Help/Content/introduction.html

注意：一个 Secure Email Threat Defense 帐户一次只能与一个 SecureX 组织集成。

Secure Email Threat Defense 超级管理员和管理员用户可以为其 Secure Email Threat Defense 实例授权 SecureX 模块：

1. 选择**设置**（齿轮图标）> **管理 (Administration)** > **企业 (Business)**。
2. 在**首选项 (Preferences)** > **SecureX** 下，点击**授权 SecureX 集成 (Authorize SecureX Integration)**。
3. 完成授权流程。

系统将显示一个横幅，说明 SecureX 配置成功。

现在，您可以将 Secure Email Threat Defense 磁贴添加到 SecureX 控制面板。有关如何执行此操作的信息，请参阅 SecureX 文档：https://docs.securex.security.cisco.com/SecureX-Help/Content/configure-tiles.html

为思科安全邮件威胁防御撤销 SecureX 授权

注意：任何超级管理员或管理员用户均可执行此任务。它不必由为 Secure Email Threat Defense 实例授权 SecureX 的用户执行。

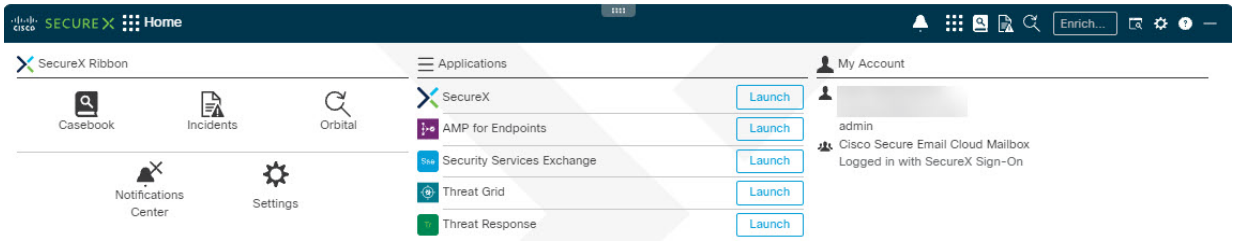
要撤销 SecureX 授权，请执行以下操作：

1. 选择**设置**（齿轮图标）> **管理 (Administration)** > **企业 (Business)**。
2. 在**首选项 (Preferences)** > **SecureX** 下，点击**撤销授权 (Revoke Authorization)**。

系统将显示一个横幅，说明 SecureX 配置已成功更新。

SecureX 功能区

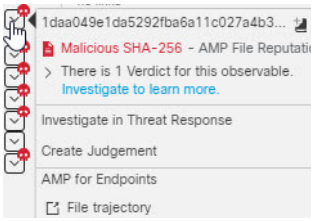
SecureX 功能区位于页面下方，当您在 Secure Email Threat Defense 和环境中的其他思科安全产品之间移动时，此功能仍然存在。任何 Secure Email Threat Defense 用户都可以授权使用 SecureX 功能区。使用功能区在思科安全应用之间导航、访问案例集、搜索可观察对象以及查看事件。



有关 SecureX 功能区的信息，请参阅 SecureX 文档：
https://docs.securex.security.cisco.com/SecureX-Help/Content/ribbon.html

深入调查菜单

如果授权功能区，SecureX 透视菜单将被添加到 Secure Email Threat Defense 展开的邮件视图中。通过这些菜单，您可以集中访问每个可观察对象的其他信息，具体取决于您购买的思科安全产品。



同样，通过思科安全邮件威胁防御与 SecureX 的集成，您可以使用透视菜单来访问思科安全邮件威胁防御。您可以从中透视的可观察对象包括：

- 邮箱地址
- 邮件 ID
- 电子邮件主题
- 文件名
- 发件人 IP
- SHA 256
- URL

使用透视菜单执行以下操作：

- 直接从透视菜单隔离具有特定可观察对象的邮件。以这种方式隔离的项目会在思科安全邮件威胁防御中指明它们是由 SecureX 用户使用 SecureX 手动补救的。
  - **注意**：透视菜单中的隔离区当前限制为 100 封邮件。
- 在思科安全威胁防御中发起搜索。

有关 SecureX 透视菜单的更多信息，请参阅 SecureX 文档：
https://docs.securex.security.cisco.com/SecureX-Help/Content/pivot-menus.html

授权 SecureX 功能区

SecureX 功能区在用户级别进行授权。您可以从功能区中或从“用户首选项”(User Preferences) 菜单中授权功能区。

注意：需要先激活 SecureX 帐户，然后才能授权功能区。您可以按照 为思科安全邮件威胁防御授权 SecureX，第 49 页 中的说明或通过在 SecureX 中集成任何其他模块来执行此操作。

从 SecureX 功能区中授权

要从功能区中授权 SecureX 功能区，请执行以下操作：

1. 点击 SecureX 功能区中的**获取 SecureX (Get SecureX)**。
2. 在“授予应用访问权限”(Grant Application Access) 对话框中，点击**授权安全邮件威胁防御功能区 (Authorize Secure Email Threat Defense Ribbon)**。

您的 SecureX 功能区现已获得授权。系统将显示一个横幅，说明 SecureX 配置已成功更新。

从 Secure Email Threat Defense 用户设置授权

要从“用户设置”(User Settings) 菜单授权 SecureX 功能区，请执行以下操作：

1. 选择**用户**（配置文件图标）> **用户设置 (User Settings)**。
2. 在**首选项(Preferences)**>**SecureX功能区(SecureXRibbon)**下，点击**授权SecureX功能区(AuthorizeSecureXRibbon)**。
3. 在“授予应用访问权限”(Grant Application Access) 对话框中，点击**授权思科安全邮件威胁防御功能区 (Authorize Cisco Secure Email Threat Defense Ribbon)**。

您的 SecureX 功能区现已获得授权。系统将显示一个横幅，说明 SecureX 配置已成功更新。

撤销 SecureX 功能区授权

SecureX 功能区在用户级别进行授权。您可以从功能区中或从“用户首选项”(User Preferences) 菜单中撤销授权。

从 SecureX 功能区中撤销授权

要从功能区中撤销 SecureX 功能区授权，请执行以下操作：

1. 在 SecureX 功能区中选择**设置 (Settings)** > **授权 (Authorization)** > **撤销 (Revoke)**。
2. 在“撤销”(Revoke) 对话框中，点击**确认 (Confirm)**。

您的 Secure Email Threat Defense 用户帐户已不再获得 SecureX 功能区的授权。

从 Secure Email Threat Defense 用户设置撤销授权

要从“用户设置”(User Settings) 菜单撤销 SecureX 功能区授权，请执行以下操作：

1. 选择**用户**（配置文件图标）> **用户设置 (User Settings)**。
2. 在**首选项 (Preferences)** > **SecureX 功能区 (SecureX Ribbon)** 下，点击**撤销授权 (Revoke Authorization)**。

您的 Secure Email Threat Defense 用户帐户已不再获得 SecureX 功能区的授权。系统将显示一个横幅，说明 SecureX 配置已成功更新。

API

安全邮件威胁防御 API 允许您以安全且可扩展的方式以编程方式访问和使用数据。有关详细信息，请参阅 API 文档 https://developer.cisco.com/docs/message-search-api/。

停用思科邮件安全威胁防御

邮件来源：Microsoft 365

要在邮件来源为 Microsoft 时停用 Secure Email Threat Defense，包括两个主要任务：

- 从 Microsoft 365 管理中心删除 Secure Email Threat Defense 日志条目
- 从 Microsoft Azure 租户中删除 Secure Email Threat Defense 应用

删除 Secure Email Threat Defense 日志规则

要删除思科安全邮件威胁防御日志规则，请执行以下操作：

1. 转到 Microsoft 365 管理中心 https://admin.microsoft.com/AdminPortal/Home#/homepage。
2. 导航至**管理中心(Admin centers)**>**合规性(Compliance)**>**数据生命周期管理(Data lifecycle management)**>**Exchange（传统）(Exchange [legacy])** > **日志规则 (Journal rules)**。
3. 选择 Secure Email Threat Defense 日志规则，然后点击**删除 (Delete)**。选择**是 (Yes)** 以确认要删除日志规则。

从 Azure 删除 Secure Email Threat Defense 应用

要从 Azure 中删除思科安全邮件威胁防御应用，请执行以下操作：

1. 转到 portal.azure.com。
2. 搜索并选择**企业应用 (Enterprise applications)**。

   注意：如果您在 Azure 中使用较早的视图，这可能称为**应用注册 (App registrations)**。
3. 找到并选择**思科安全邮件威胁防御 (Cisco Secure Email Threat Defense)** 和/或**思科安全邮件威胁防御（只读）(Cisco Secure Email Threat Defense [Read Only])** 应用。
4. 在左侧窗格中，选择**属性 (Properties)**。
5. 点击**删除 (Delete)** 按钮，然后选择**是 (Yes)** 以确认删除思科安全邮件威胁防御应用。

邮件来源：网关

要在使用网关作为邮件来源时停用思科安全邮件威胁防御，包括两个主要任务：

- 将网关配置为停止向思科安全邮件威胁防御发送邮件
- 从 Microsoft Azure 租户中删除 Secure Email Threat Defense 应用（无身份验证模式则不需要删除）

将网关配置为停止发送邮件

要配置网关以停止向思科安全邮件威胁防御发送邮件，请执行以下操作：

1. 在思科安全邮件云网关控制台中，转至**安全服务 (Security Services) > 威胁防御连接器 (Threat Defense Connector)**。
2. 将**威胁防御连接器 (Threat Defense Connector)** 设置为**已禁用 (Disabled)**。

从 Azure 删除 Secure Email Threat Defense 应用

要从 Azure 中删除思科安全邮件威胁防御应用，请执行以下操作：

1. 转到 portal.azure.com。
2. 搜索并选择**企业应用 (Enterprise applications)**。

   注意：如果您在 Azure 中使用较早的视图，这可能称为**应用注册 (App registrations)**。
3. 找到并选择**思科安全邮件威胁防御 (Cisco Secure Email Threat Defense)** 和/或**思科安全邮件威胁防御（只读）(Cisco Secure Email Threat Defense [Read Only])** 应用。
4. 在左侧窗格中，选择**属性 (Properties)**。
5. 点击**删除 (Delete)** 按钮，然后选择**是 (Yes)** 以确认删除思科安全邮件威胁防御应用。

常见问题解答 (FAQ)

思科安全邮件威胁防御常见问题中提供了常见问题的解答。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。