使用上的报告

本章包含以下部分：

查看报告数据的各种方法

Table 1: 查看报告数据的方式

收件人	请参阅
查看和自定义基于网络的交互式报告页面	• 自定义报告数据的视图 , on page 3 • 使用集中邮件安全报告 • 集中策略、病毒和病毒爆发隔离区
自动生成循环 PDF 或 CSV 报告	• 计划邮件报告 • 计划 Web 报告
按需生成 PDF 或 CSV 报告	• 按需生成邮件报告 • 按需生成 Web 报告

收件人	请参阅
将原始数据导出为 CSV（逗号分隔值）文件	• 并导出报告和跟踪数据 , on page 9 • 将报告数据导出为逗号分隔值 (CSV) 文件 , on page 10
生成 PDF 格式的报告数据	并导出报告和跟踪数据 , on page 9
通过邮件将报告信息发送给自己和他人	• 按需生成邮件报告 • 计划邮件报告 • 按需生成 Web 报告 • 计划 Web 报告
查找有关特定事务的信息	查看报告中包括的邮件或事务的详细信息 , on page 7

Note 有关日志记录和报告之间的差异，请参阅日志记录与报告。

安全管理设备如何收集报告的数据

安全管理设备大约每隔15分钟便会从所有托管设备中提取所有报告的数据，并聚合来自这些设备的数据。将特定消息包含在安全管理设备的报告数据中可能需要一点时间，具体取决于您的设备。有关数据的信息，请查看**系统状态 (System Status)** 页面。

报告数据包括涉及 IPv4 和 IPv6 的事务。

Note 在收集报告数据时，安全管理设备会应用您在安全管理设备上配置时间设置时所设置信息中的时间戳。有关在安全管理设备上设置时间的信息，请参阅配置系统时间。

如何存储报告数据

所有设备都存储报告数据。下表 显示每个设备存储数据的时段。

Table 2: 邮件和 ***Web*** 安全设备中的报告数据存储

	每分钟	每小时	每天	每周	每月	每年
邮件安全设备或网络安全设备 上的本地报告						

	每分钟	每小时	每天	每周	每月	每年
邮件安全设备或网络安全设备上的集中报告						
安全管理设备						

关于报告和升级

新的报告功能可能不适用于在升级之前进行的事务，因为可能没有为这些事务保留所需的数据。有关与报告数据和升级相关的可能限制，请参阅与您的版本对应的版本说明。

自定义报告数据的视图

在 Web 界面中查看报告数据时，可以自定义视图。

收件人	相应操作
查看每个设备或报告组的数据	查看设备或报告组的报告数据, on page 4
指定时间范围。	选择报告的时间范围 , on page 4
（对于 Web 报告）选择要绘制哪些数据的图表	（仅限 Web 报告）选择要绘制哪些数据的图表 , on page 4
自定义表	请参阅自定义报告页面上的表 , on page 5
搜索特定信息或要查看的数据的子集	• 有关邮件报告，请参阅搜索与交互式邮件报告页面。 • 对于 Web 报告，请查找大多数表格底部的“查找 (Find)”或“过滤 (Filter)”选项。 • 有些表格包含指向聚合数据详细信息的链接（蓝色文本）。
指定报告相关的首选项	请参阅设置首选项
创建仅包含您所需图表和表的自定义报告	请参阅自定义报告 , on page 5。

Note 并非每个报告均可使用所有自定义功能。

查看设备或报告组的报告数据

对于邮件和 Web 概述报告，以及邮件的系统容量报告，可查看来自所有设备的数据，或来自任何一个集中托管设备的数据。

对于邮件报告，如果按照创建邮件报告组中所述创建了邮件安全设备组，则可以查看每个报告组的数据。

要指定视图，请从受支持页面上的**查看数据**列表中选择一个设备或组。

如果您正在查看最近将另一个安全管理设备中的数据备份到的安全管理设备的报告数据，则必须首先在 > **管理设备** > **集中服务** > **安全设备**中添加（但不要连接到）每个设备。

选择报告的时间范围

大多数预定义的报告页面支持您选择要包括的数据的时间范围。您选择的时间范围用于所有报告页面，直到您在“时间范围”(Time Range) 菜单中选择不同的值为止。

可用时间范围选项因设备以及有关安全管理设备的邮件和 Web 报告而异：

Note 报告页面上的时间范围以格林威治标准时间 (GMT) 时差显示。例如，太平洋时间是 GMT + 7 小时 (GMT + 07:00)。

Note 所有报告均基于系统配置的时区显示日期和时间信息，并且以格林威治标准时间 (GMT) 时差显示。但是，数据导出会显示 GMT 时间，以适应采用全球多个时区的多个系统。

Tip 您可以指定每次您登录时始终显示的默认时间范围。有关信息，请参阅设置首选项。

（仅限 Web 报告）选择要绘制哪些数据的图表

每个 Web 报告页面上的默认图表会显示通常引用的数据，但是，您可以选择用其他数据绘制图表。如果页面有多个图表，则可以更改每个图表。

通常，图表选项与报告中表格的列相同。但是，某些列无法用于绘制图表。

图表反映表格列中的所有可用数据，无论选择在关联的表格中显示的项目（行）数量是多少都是如此。

步骤 1 单击图表下的**图表选项 (Chart Options)** 链接。

步骤 2 选择要显示的数据。

步骤 3 单击完成 (Done)。

自定义报告页面上的表

Table 3: 自定义 Web 报告页面中的表格

收件人	相应操作	更多信息
• 显示其他列 • 隐藏可见列 • 确定表格的可用列	单击表格下面的**列 (Columns)** 链接，选择要显示的列，然后单击**完成 (Done)**。	对于大多数表格，某些列默认情况下会隐藏。 每个报告页面会提供不同的列。 另请参阅邮件报告页面的表列说明。
对表列重新排序	将列标题拖动到所需的新位置	—
按照所选的标题排序表格。	单击列标题。	—
显示更多或更少的数据行	从表格右上方的**显示的项目 (Items Displayed)** 下拉列表中，选择要显示的行。	对于 Web 报告，您还可以为默认要显示的行设置首选项；请参阅设置首选项。
查看有关表格条目的详细信息（如果可用）	单击表格中的蓝色条目	另请参阅查看报告中包括的邮件或事务的详细信息 , on page 7。
将数据池缩小至特定子集	在表格下方的过滤器设置中选择或输入值（如果可用）	对于 Web 报告，在每个报告页面说明中会介绍可用的过滤器。请参阅 Web 报告页面说明。

自定义报告

可以通过组合现有报告页面中的图表（图形）和表格，创建自定义邮件安全报告页面。

Note 在邮件安全设备上，从 9.6 版本开始，“我的报告”(My Reports) 称为“我的控制面板”(My Dashboard)。

收件人	相应操作
将模块添加到自定义报告页面。	请参阅： • 无法添加到自定义报告的模块 • 创建自定义报告页面 , on page 6

收件人	相应操作
查看自定义报告页面	1. 选择 邮件 > 报告 > 我的报告。 2. 选择要查看的时间范围。所选时间范围会应用到所有报告，包括“我的报告”页面中的所有模块。 新添加的模块显示在自定义报告的顶部。
在自定义报告页面上重新排列模块	将模块拖放到所需的位置。
从您的自定义报告中删除模块	单击模块右上角的 [X]。
生成自定义报告的 CSV 版本	请参阅： • 按需生成邮件报告 • 按需生成 Web 报告
定期生成自定义报告的 CSV 版本	请参阅： • 计划邮件报告 • 计划 Web 报告

无法添加到自定义报告的模块

- 位于**管理设备 (Management Appliance) > 集中服务 (Centralized Services) > 系统状态 (System Status)** 页面上的所有模块
- 位于**邮件 (Email) > 报告 (Reporting) > 报告数据可用性 (Reporting Data Availability)** 页面上的所有模块
- 位于**邮件 (Email) > 邮件跟踪 (Message Tracking) > 邮件跟踪数据可用性 (Message Tracking Data Availability)** 页上的所有模块
- 以下按域的模块来自“发件人配置文件”(Sender Profile) 详细信息报告页：SenderBase 中的当前信息、发件人组信息和网络信息
- “病毒爆发过滤器” (Outbreak Filters) 报告页上的**过去一年病毒爆发摘要 (Past Year Virus Outbreak Summary)** 图表和**过去一年病毒爆发 (Past Year Virus Outbreaks)** 表格

创建自定义报告页面

Before you begin

- 确保您要添加的模块可以添加。请参阅无法添加到自定义报告的模块 。
- 通过单击模块右上角的 [X] 删除不需要的任何默认模块。

步骤 1 使用以下方法之一将模块添加到自定义报告页面：

Note 某些模块仅在使用这些方法中的一种时可用。如果无法使用一种方法添加模块，请尝试另一种方法。

- 导航至具有要添加的模块的“邮件”或下的报告页面，然后单击模块顶部 [+] 按钮。
- 转到邮件> 报告 (Reporting) > 我的报告 (My Reports)，单击 [+] 报告模块按钮（位于一个部分的顶部），然后选择要添加的报告模块您可能需要单击“我的报告”(My Reports) 页面上各个部分中的“+”按钮，以便查找所需的模块。

每个模块只能添加一次；如果您已向报告中添加特定模块，则用于添加该模块的选项将不可用。

步骤 2 如果添加已自定义的模块（例如，通过添加、删除或重新排序列，或者通过在图表中显示非默认数据），则在“我的报告”页面上自定义模块。

添加的模块使用默认设置。原始模块的时间范围无法保留。

步骤 3 如果添加包含单独图例的图表（例如，“概述”(Overview) 页面中的图形），请单独添加图例。如果需要，请将其拖放至所描述数据旁边的位置。

查看报告中包括的邮件或事务的详细信息

步骤 1 单击报告页面上表中的任何蓝色编号。

（并非所有的表格都有这些链接。）

包含在该编号中的消息或事务分别以消息跟踪或 Web 跟踪的形式显示。

步骤 2 向下滚动以查看邮件或事务列表。

What to do next

- 跟踪

提高邮件报告的性能

如果汇聚报告的性能在一个月的时间里因包含大量唯一的条目而下降，请使用报告过滤器限制在涵盖上一年的报告（“去年”(Last Year) 报告）中汇聚数据。这些过滤器可以限制报告中的详细个人 IP、域或用户数据。概述报告和摘要信息仍可用于所有报告。

您可以使用 CLI 中的 **reportingconfig > 过滤器**菜单启用一个或多个报告过滤器。更改必须提交才能生效。

- **IP连接级别详细信息**。启用此过滤器可阻止安全管理设备记录有关各个IP地址的信息。此过滤器适合由于攻击需要处理大量传入 IP 地址的系统。

  此过滤器会影响以下去年的报告：

  - 传入邮件的发件人简档
  - 传入邮件的 IP 地址
  - 传出发件人的 IP 地址

- **用户详细信息**。启用此过滤器可阻止安全管理设备记录有关发送和接收邮件的个人用户以及应用于用户邮件的内容过滤器的信息。此过滤器适合为数以百万计的内部用户处理邮件的设备，或者不能验证收件人地址的系统。

  此过滤器会影响以下去年的报告：

  - “内部用户”(Internal Users)
  - “内部用户详细信息”(Internal User Details)
  - “传出邮件发件人的 IP 地址”(IP Addresses for Outgoing Senders)
  - 内容过滤器

- **邮件流量详细信息**。启用此过滤器可阻止安全管理设备记录有关设备监控的各个域和网络的信息。在数以千万计的域中测量有效的传入或传出域的数量时，此过滤器非常合适。

  此过滤器会影响以下去年的报告：

  - 传入邮件的域
  - 传入邮件的发件人简档
  - 内部用户详细信息
  - “传出邮件发件人的域”(Domains for Outgoing Senders)

Note 要查看上一小时的最新报告数据，必须登录到各个设备并查看其中的数据。

并导出报告和跟踪数据

Table 4: 在新 ***Web*** 界面上导出报告和跟踪数据

要获取的信息	CSV	相应操作	说明
原始数据 另请参阅将报告数据导出为逗号分隔值 (CSV) 文件 , on page 10	•	1. 单击报告页面顶部的**导出 (Export)** 链接。 2. 选择 **CSV** 作为所需格式。 3. 选择要导出的所需报告模块，然后单击**下载 (Download)**。	CSV 文件包含所有适用的数据，包括图表或表中可见的数据。
	•	创建一个计划报告或按需报告。请参阅： • 按需生成邮件报告 • 计划邮件报告	每个CSV文件最多可以包含 100 行。 如果报告包含多个表格，则会为每个表格创建一个单独的 CSV 文件。 一些扩展报告无法使用 CSV 格式。
交互式报告页面的 PDF	•	1. 单击报告页面顶部的**导出 (Export)** 链接。 2. 选择 **PDF** 作为所需格式。 3. 选择要导出的所需报告模块，然后单击**下载 (Download)**。	PDF 会反映当前正在查看的自定义内容。 PDF 经过格式化以便于打印。
PDF 格式的报告数据	•	创建一个计划报告或按需报告。请参阅： • 按需生成邮件报告 • 计划邮件报告	-

要获取的信息	CSV	相应操作	说明
（网络安全）报告数据的自定义子集，例如特定用户的数据。	•	1. 从“产品”下拉列表中选择 **Web**，然后选择**跟踪 > Web 跟踪**。 2. 执行搜索，然后单击搜索结果上方的**导出 (Export)** 链接或**全部导出 (Export All)** 链接	CSV 文件包括符合搜索条件的所有原始数据。
（邮件安全）自定义数据子集，例如特定用户的数据。	•	1. 从产品（Product）下拉列表中选择**邮件**，然后选择**跟踪 > 邮件跟踪**。 2. 执行搜索，然后单击搜索结果上方的**导出 (Export)** 链接或**全部导出 (Export All)** 链接	“导出 (Export)”链接会下载包含显示的搜索结果的 CSV 文件，并且遵循在搜索条件中指定的限制。 “全部导出”(Export All) 链接下载一个包含与您的搜索条件相匹配的最多 50000 封邮件的 CSV 文件。 提示：如果您需要导出超过 50000 封邮件，请为一组较短的时间范围执行一系列的导出。

将报告数据导出为逗号分隔值 (CSV) 文件

可以将原始数据导出为逗号分隔值 (CSV) 文件，该文件可使用 Microsoft Excel 等数据库应用进行访问和操纵。有关导出数据的不同方式，请参阅并导出报告和跟踪数据 , on page 9。

由于 CSV 导出仅包括原始数据，因此从一个基于 Web 的报告页面导出的数据可能不包括计算的数据，例如百分比，即使这些数据显示在基于 Web 的报告中也是如此。

对于邮件跟踪和报告数据，导出的 CSV 数据将显示 GMT 中的所有数据，不管安全管理设备中的设置如何。这简化了独立于设备使用数据，特别是在多个时区中引用设备的数据时。

以下示例是防恶意软件类别报告原始数据导出中的一个条目，其中太平洋夏季时间 (PDT) 显示为 GMT - 7 小时：

Begin Timestamp, End Timestamp, Begin Date, End Date, Name, Transactions Monitored, Transactions Blocked, Transactions Detected

1159772400.0, 1159858799.0, 2006-10-02 07:00 GMT, 2006-10-03 06:59 GMT, Adware, 525, 2100, 2625

Table 5: 查看原始数据条目

类别标题	值	说明
开始时间戳	1159772400.0	以系统纪元以来的秒数表示的查询开始时间。
结束时间戳	1159858799.0	以系统纪元以来的秒数表示的查询结束时间。
开始日期	2006-10-02 07:00 GMT	查询开始的日期。
结束日期	2006/10/3 6:59 GMT	查询结束的日期。
名称	广告软件	恶意软件类别的名称。
监控的事务数	525	受监控的事务数。
阻止的事务数	2100	已阻止的事务数。
检测到的事务数	2625	事务总数： 检测到的事务数 + 阻止的事务数。

Note 每种类型的报告类别标题都是不同的。如果导出本地化的CSV数据，则某些浏览器中的标题可能无法正确呈现。出现该情况是因为某些浏览器可能没有为本地化文本使用正确的字符集。要解决该问题，可以将文件保存到本地计算机，然后在任何 Web 浏览器中使用**文件 (File) > 打开 (Open)** 打开该文件。打开文件时，请选择字符集以显示本地化文本。

报告和跟踪中的子域与二级域

在报告和跟踪搜索中，对二级域（在 http://george.surbl.org/two-level-tlds 中列出的地区域）的处理方式与子域不同，即使两种域类型可能看起来相同。例如：

- 报告不会包含两级域（例如 co.uk）的结果，但是会包含 foo.co.uk 的结果。报告包含主公司域下的子域，例如 cisco.com。
- 对应于地区域 co.uk 的跟踪搜索结果不会包含诸如 foo.co.uk 等域，而对应于 cisco.com 的搜索结果将包含子域，例如 subdomain.cisco.com。

对所有报告进行故障排除

- 无法在备份的安全管理设备上查看报告数据 , on page 12
- 报告功能被禁用, on page 12

无法在备份的安全管理设备上查看报告数据

问题

您无法选择要查看其报告数据的单个邮件安全设备。**查看以下项的数据**选项不会显示在报告页面上。

解决方案

另请参阅备份期间的服务可用性。

报告功能被禁用

问题

取消备份期间会禁用报告。

解决方案

报告功能将在备份完成之后恢复。

邮件和 Web 报告

有关邮件报告特定的信息，请参阅使用集中邮件安全报告。

有关 Web 报告特定的信息，请参阅使用集中 Web 报告和跟踪。