TREND MICRO™

6.0

趋势科技™ 防毒墙控制管理中心

Service Pack 3

联动威胁治理手册

集中式企业安全管理

文档编号：CMCM67184/150909

发布日期：2015 年 7 月

受美国专利号 5,623,600、5,889,943、5,951,698、6,119,165 的保护

趋势科技防毒墙控制管理中心的用户文档介绍该软件的主要功能组件以及针对贵组织生产环境的安装说明。在安装和使用该软件之前，请详细阅读。

有关如何使用软件中具体功能的详细信息，可在联机帮助文件和趋势科技 Web 站点上的在线知识库中获得。

趋势科技一直致力于改进其文档。如对该文档或趋势科技的任何其他文档有任何问题、意见或建议，请通过 service@trendmicro.com.cn 与我们联系。我们始终欢迎您的反馈。

关于联动威胁治理

联动威胁治理

控制管理中心将一系列趋势科技产品与解决方案相结合，帮助您在目标攻击和高级威胁尚未导致长期损害之前将其检测出来，并予以分析和回应。

了解详细信息：

联动威胁治理产品集成

可疑对象和 IOC 文件

目标攻击和高级威胁旨在通过避开现有安全防护措施破坏您的网络。

控制管理中心可通过使用以下项目协助调查目标攻击和高级威胁：

- **可疑对象**：可能会使系统面临危险或遭受损失的文件、IP 地址、域或 URL
- **IOC 文件**：描述在主机或网络中发现的攻击指示符 (IOC)。IOC 文件可帮助管理员和调查人员对威胁数据做出一致的分析和解释。

了解详细信息：

- 可疑对象管理和处理进程
- IOC 管理

终端隔离

您可以通过隔离存在风险的终端来调查原因并解决安全问题。

了解详细信息：

终端隔离

增强的安全威胁监控

使用以下**摘要**选项卡中的小组件来监控整个网络的安全并回应最关键的威胁：

- 关键威胁
- 携带威胁的用户
- 存在威胁的终端

这些小组件提供了指向“安全威胁”窗口的链接。此窗口显示在一定时间段内的威胁（依**用户**或**终端**）。

在“安全威胁”窗口中，可以重点关注特定威胁以查看其近期是否**影响了**其他用户和终端。启动**影响评估**，以查看同一威胁在很长一段时间内是否影响了更多的用户和终端。

通过这些整体视图，您可以查看可能导致攻击的企业级事件链，其中包括用于准备或发起攻击的存在风险的终端。

了解详细信息：

- “安全威胁”窗口（用户）
- “安全威胁”窗口（终端）
- “受影响的用户”窗口
- 影响评估

联动威胁治理产品集成

主要产品

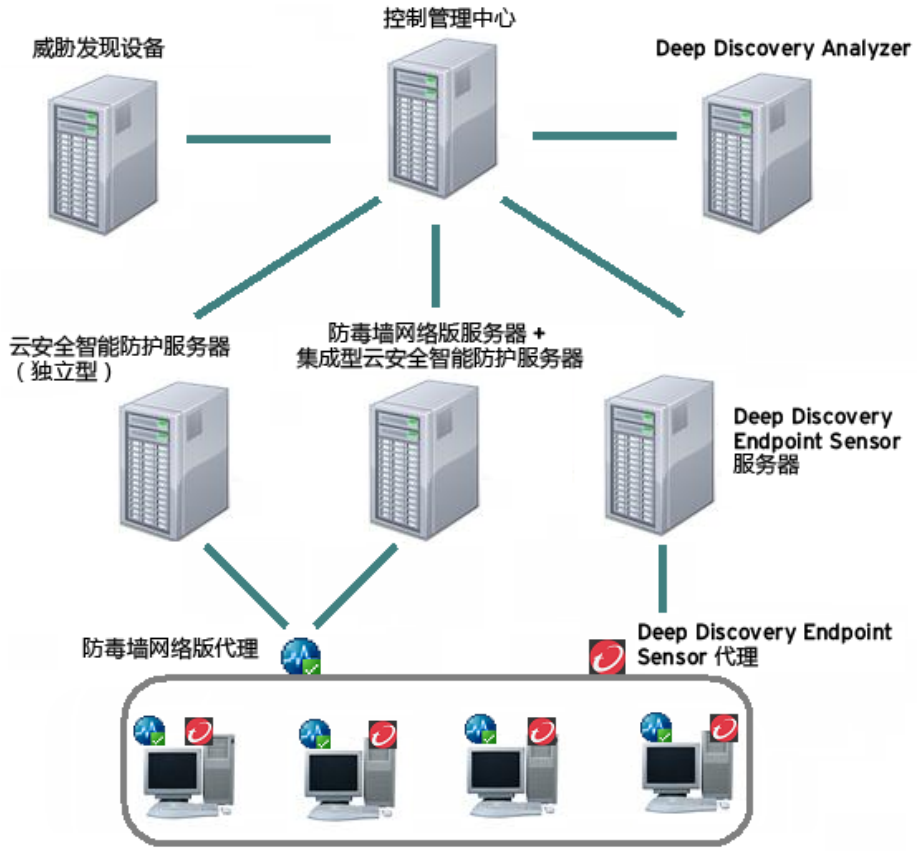
联动威胁治理需要以下趋势科技产品：

- 控制管理中心
- 威胁发现设备
- 防毒墙网络版
- 独立型或与防毒墙网络版集成的云安全智能防护服务器

其他受支持的产品

以下趋势科技产品也可以集成到控制管理中心，以进行联动威胁治理：

- Deep Discovery Endpoint Sensor
- Deep Discovery Analyzer



可疑对象管理和处理进程 第 7 页 和 IOC 管理 第 15 页 对每种产品在联动威胁治理策略中的作用进行了详细说明。

安装这些产品并将其注册到控制管理中心。以下表格列出了各种参考资料和资源，可帮助您安装和注册相关产品。

重要信息

在注册防毒墙网络版**之前**，请先注册威胁发现设备和/或 Deep Discovery Analyzer。如果先注册防毒墙网络版，将无法从威胁发现产品中获取可疑对象。

控制管理中心	
最低版本	6.0 SP3
安装	参考： • 版本 6.0 的安装指南（用于安装产品） • Service Pack 的自述文件（用于安装 Service Pack） http://docs.trendmicro.com/zh-cn/enterprise/control-manager.aspx
控制管理中心信息	某些被管理产品需要以下控制管理中心信息： • **主机名**（最好是 FQDN）或 **IP 地址**：注册威胁发现设备和防毒墙网络版时需要提供。在这些产品的控制台上进行注册。 **注意** 注册其他联动威胁治理产品要在控制管理中心控制台上执行。 • **API 密钥**：威胁发现设备、防毒墙网络版和云安全智能防护服务器同步可疑对象时需要提供 将 API 密钥手动部署到威胁发现设备 3.8 或更高版本、防毒墙网络版 11 SP1 以及云安全智能防护服务器 3.0 Patch 1。要获取 API 密钥，请打开控制管理中心管理控制台，转到**管理** > **可疑对象** > **分布设置**。 对于更高版本的防毒墙网络版和云安全智能防护服务器，在控制管理中心注册后，API 密钥会进行自动部署，前提是须有一个威胁发现产品已注册到控制管理中心。

威胁发现设备	
最低版本	3.8

安装和部署	参考： • 快速入门提示卡 • 安装和部署指南 http://docs.trendmicro.com/zh-cn/enterprise/deep-discovery-inspector.aspx
注册与同步可疑对象	完成注册并通过威胁发现设备管理控制台启用可疑对象同步。 您可以通过控制管理中心内的“托管服务器”窗口轻松启动威胁发现设备管理控制台。 注册和同步说明： http://docs.trendmicro.com/all/ent/ddi/v3.8/en-us/ddi_3.8_olh/admin_int-prods-srvcs_tmcm_register.html

Deep Discovery Analyzer	
最低版本	5.1
安装和部署	参考： • 快速入门提示卡 • 安装和升级指南 http://docs.trendmicro.com/en-us/enterprise/deep-discovery-analyzer.aspx
注册	通过控制管理中心管理控制台完成注册。转至**管理** > **托管服务器**，然后从产品列表中选择 Deep Discovery Analyzer。

防毒墙网络版	
最低版本	11 SP1

安装	参考： • 版本 11 的安装和升级指南（用于安装服务器程序） • Service Pack 的自述文件（用于将 Service Pack 安装到服务器） • 版本 11 或更高版本的联机帮助或管理员指南（用于安装代理和使用集成型云安全智能防护服务器） http://docs.trendmicro.com/zh-cn/enterprise/officescan.aspx
注册与同步可疑对象	注册防毒墙网络版之前，请确保已将至少一个威胁发现设备产品注册到控制管理中心。 完成注册并通过防毒墙网络版服务器 Web 控制台启用可疑对象同步。 您可以通过控制管理中心内的“托管服务器”窗口轻松启动防毒墙网络版服务器 Web 控制台。 • 注册说明： http://docs.trendmicro.com/zh-cn/enterprise/officescan-110-sp1-server/managing-the-product/osce-company_name-co/osce-registering-pro.aspx • 同步说明（仅限防毒墙网络版 11 SP1）： http://docs.trendmicro.com/zh-cn/enterprise/officescan-110-sp1-server/managing-the-product/suspicious-objects-c/configuring-suspicio.aspx **注意** 更高版本的防毒墙网络版或非英语版本的防毒墙网络版 11 SP1 已获得增强，可在注册后与控制管理中心自动同步可疑对象。

云安全智能防护服务器（独立型）	
最低版本	3.0 Patch 1

安装	参考： • 版本 3.0 的安装和升级指南（用于安装产品） • Patch 的自述文件（用于安装 Patch） http://docs.trendmicro.com/zh-cn/enterprise/smart-protection-server.aspx
同步可疑对象	同步说明（仅限云安全智能防护服务器 3.0 Patch 1）： http://docs.trendmicro.com/all/ent/sps/v3.0p1/zh-cn/sps_3.0p1_olh/using_smart_prot_ccca_configure.html **注意** 只有高于 3.0 Patch 1 的云安全智能防护服务器版本才支持在控制管理中心上注册。注册完成后，云安全智能防护服务器会自动与控制管理中心同步可疑对象。

Deep Discovery Endpoint Sensor	
最低版本	1.5（预览版本）
安装	参考： 安装指南（用于服务器和代理安装说明） http://docs.trendmicro.com/en-us/enterprise/deep-discovery-endpoint-sensor.aspx
注册	通过控制管理中心管理控制台完成注册。转至**管理** > **托管服务器**，然后从产品列表中选择 Deep Discovery Endpoint Sensor。

可疑对象管理和处理进程

可疑对象处理进程可细分为以下阶段：

示例提交

内置到被管理产品的沙盒平台负责处理提交的示例：

- **威胁发现设备 3.8**：使用管理员配置的文件提交规则，确定要提交到其沙盒平台的示例
- **Deep Discovery Analyzer 5.1**:接收产品管理员上传或其他趋势科技产品发送的示例

分析

被管理产品中的沙盒平台跟踪并分析提交的示例。沙盒平台会根据相关对象致使系统遭遇危险或损失的可能性来标记**可疑对象**。支持的对象包括文件（SHA-1 散列值）、IP 地址、域和 URL。

分布

控制管理中心会整合可疑对象并扫描此类对象的处理措施，然后将其分布到其他产品。

3.1. 沙盒平台可疑对象 带有沙盒平台的被管理产品向控制管理中心发送可疑对象列表。 控制管理中心会在**管理** > **可疑对象** > **沙盒平台对象**下的**对象**选项卡中显示可疑对象。	**3.3. 用户定义的可疑对象** 控制管理中心管理员可转至**管理** > **可疑对象** > **用户定义的对象**，向沙盒平台可疑对象列表中添加他们认为可疑但当前不在该列表中的对象。

3.2. 沙盒平台可疑对象例外

控制管理中心管理员可从沙盒平台可疑对象（**管理** > **可疑对象** > **沙盒平台对象**）列表中选出认为安全的对象，并将其添加到例外列表。

例外列表显示在**对象**选项卡旁边的**例外**选项卡中。

控制管理中心将例外列表发送回带有沙盒平台的被管理产品。如果被管理产品中的某个可疑对象与例外列表中的某个对象匹配，那么该产品不会再将该对象发送到控制管理中心。

3.4. 可疑对象分布

控制管理中心会整合沙盒平台可疑对象和用户定义的可疑对象（不包括例外），然后将其发送给特定的被管理产品。这些产品会同步和使用这些对象的全部或一部分。

以下是受支持的被管理产品和要求的最低版本：

- **威胁发现设备 3.8**：展开其**可疑对象**列表，以包含用户定义的对象和其他威胁发现产品检测到的对象
- **防毒墙网络版 11 SP1**：在例行扫描过程中搜索可疑**文件**、**IP 地址**和 **URL**
- **独立型或与防毒墙网络版 11 SP1 集成的云安全智能防护服务器 3.0 Patch 1**：将**可疑 URL** 信息转发到发送 Web 信誉查询的趋势科技产品（例如，防毒墙网络版代理、防毒墙群件版和趋势科技服务器深度安全防护系统）

3.5 扫描处理措施

针对影响终端的可疑对象配置扫描处理措施（记录、阻止或隔离）。

“阻止”与“隔离”被视为“主动”处理措施，而“记录”被视为“被动”处理措施。如果产品采取主动处理措施，控制管理中心会宣布受影响的终端**已缓解**。如果是被动处理措施，将宣布终端**存在风险**。

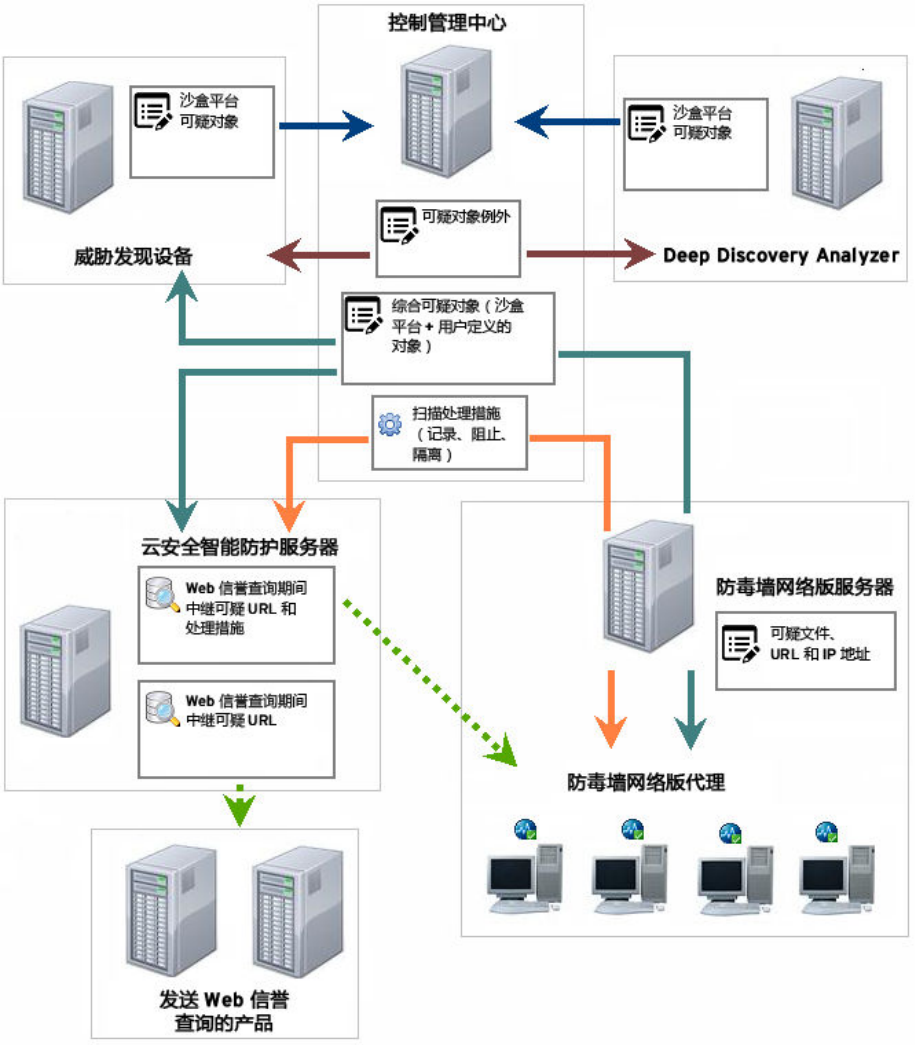
已分别对沙盒平台可疑对象和用户定义的可疑对象配置扫描处理措施。

- **管理** > **可疑对象** > **沙盒平台对象**
- **管理** > **可疑对象** > **用户定义的对象**

控制管理中心会自动将相应处理措施部署到某些被管理产品。

以下是受支持的被管理产品和要求的最低版本：

- **防毒墙网络版 11 SP1**：针对沙盒平台可疑**文件**、**IP 地址**和 **URL** 对象执行处理措施（针对用户定义的对象的处理措施不受支持）
- **独立型或与防毒墙网络版 11 SP1 集成的云安全智能防护服务器 3.0 Patch 1**：将针对可疑 URL 的处理措施转发到发送 Web 信誉查询的防毒墙网络版代理。


控制管理中心
沙盒平台
可疑对象
沙盒平台
可疑对象
可疑对象例外
威胁发现设备
Deep Discovery Analyzer
综合可疑对象（沙盒平台 + 用户定义的对象）
扫描处理措施（记录、阻止、隔离）
云安全智能防护服务器
Web 信誉查询期间中继可疑 URL 和处理措施
Web 信誉查询期间中继可疑 URL
防毒墙网络版服务器
可疑文件、URL 和 IP 地址
防毒墙网络版代理
发送 Web 信誉查询的产品

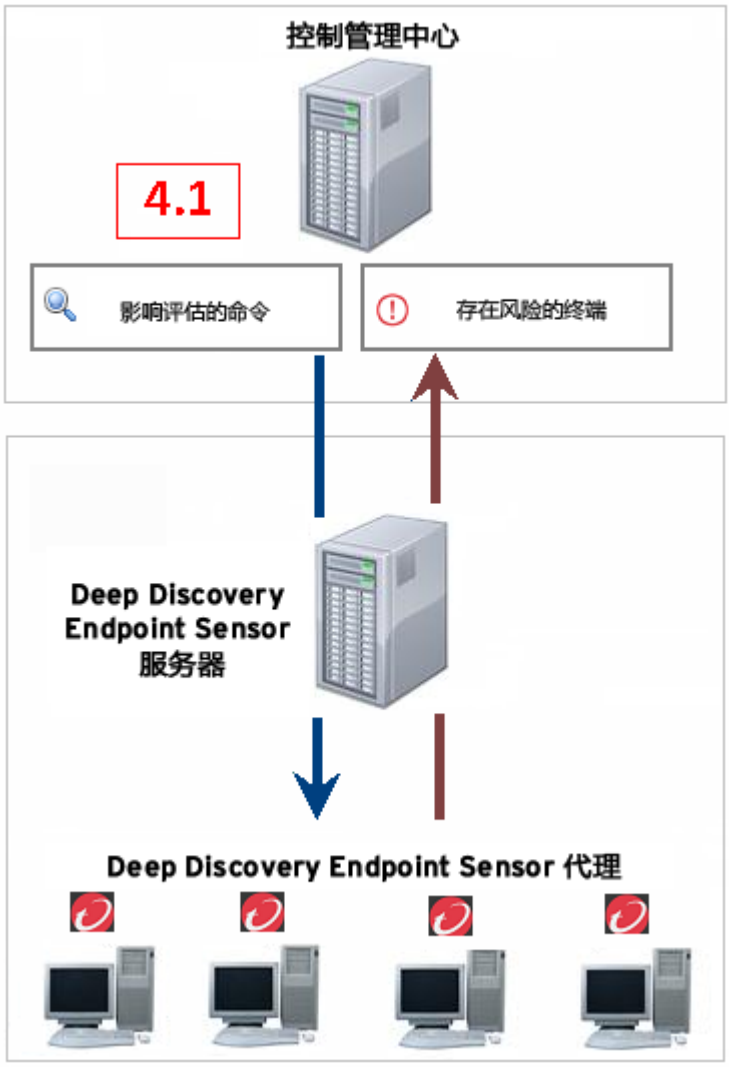
4

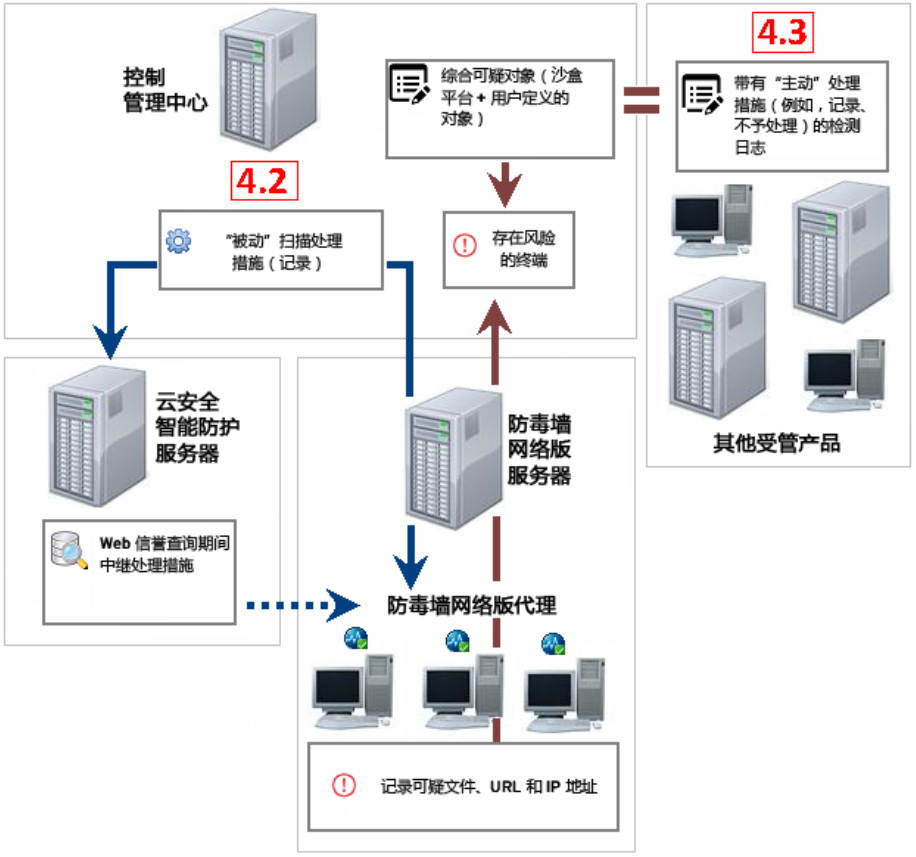
影响评估

影响评估会检查终端内是否存在与可疑对象有关的可疑活动。包含已确认为可疑活动的终端将被视为**存在风险**。

如果产品针对可疑对象采取“被动”处理措施，则控制管理中心也会将终端视为存在风险。

4.1. 影响评估 在**管理** > **可疑对象** > **沙盒平台对象**内的沙盒平台可疑对象列表中，运行影响评估，找出存在风险的终端。 要运行影响评估，需要安装 **Deep Discovery Endpoint Sensor**。所需的最低版本为 **1.5**。 此产品只执行评估，不对存在风险的终端采取处理措施。	**4.3. 检测匹配** 控制管理中心还会检查 Web 信誉、URL 过滤、网络内容检查，以及从所有被管理产品接收的基于规则的检测日志，然后将它们与可疑对象列表进行比较。如果特定终端有匹配，并且被管理产品采取了“被动”处理措施（例如记录、放行或警告并继续），该终端也会被视为存在风险。
4.2. “被动”扫描处理措施 当在控制管理中心内配置和部署到防毒墙网络版代理的扫描处理措施为“被动”（记录）时，受影响的终端将被视为存在风险。	**存在风险的终端** 要查看存在风险的终端数量，请转至**管理** > **可疑对象** > **沙盒平台对象**，查看**存在风险的终端**列。 要查看存在风险的终端的详细信息，请转至**对象**列并单击可疑对象名称前的箭头图标（如果有）。此时相应窗口会展开，以显示包含有关可疑对象和存在风险的终端详细信息的表格。


控制管理中心
4.1
影响评估的命令
存在风险的终端
Deep Discovery
Endpoint Sensor
服务器
Deep Discovery Endpoint Sensor 代理



5

缓解

防毒墙网络版代理和其他被管理产品对可疑对象执行“主动”扫描处理措施。

5.1. 控制管理中心扫描处理措施

从控制管理中心部署“主动”扫描处理措施（阻止或隔离）到防毒墙网络版代理时，对受影响终端的威胁将被视为已缓解。

5.2. 被管理产品扫描处理措施

被管理产品可以对检测到的威胁执行特定于产品的扫描处理措施（例如，阻止、删除、隔离或通过覆盖阻止）。如果控制管理中心在任何被管理产品的日志（Web 信誉、URL 过滤、网络内容检查和基于规则的检测）中匹配某个可疑对象时，将执行威胁评估。如果被管理产品对该可疑对象采取“主动”处理措施时，则控制管理中心将对终端的所有威胁视为已缓解。

注意

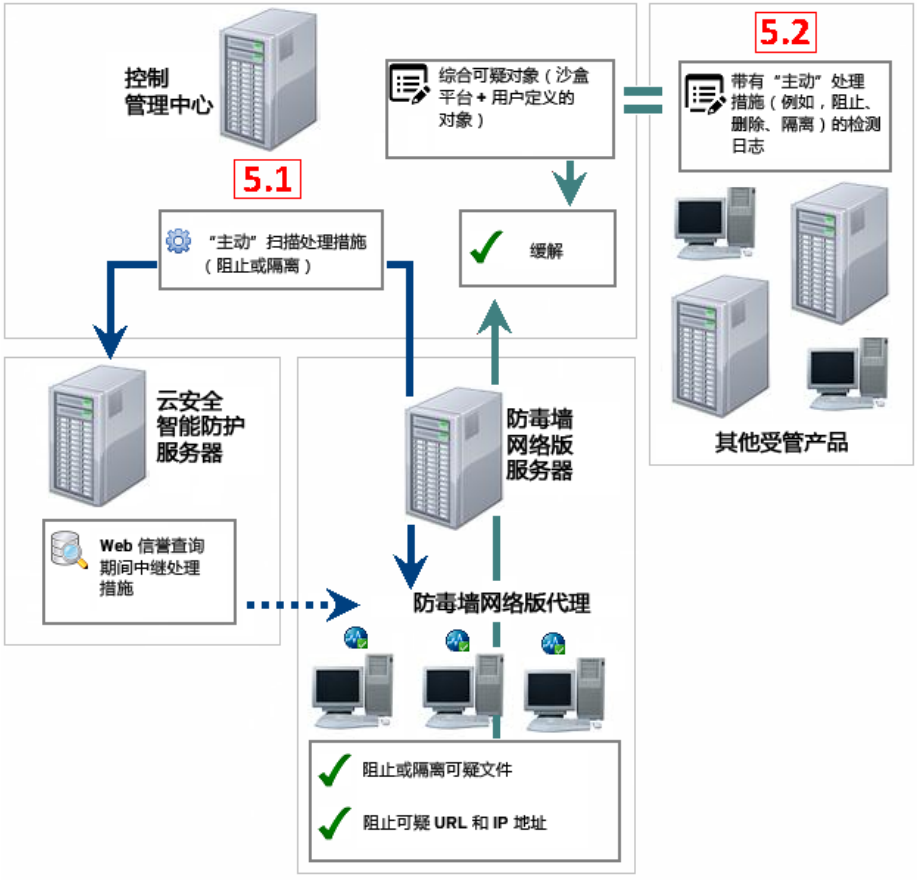
请参阅被管理产品的管理员指南，了解有关特定产品可以对检测到的威胁执行的处理措施类型。

终端隔离

另一种处理措施是隔离存在风险的终端。如需执行详细调查，可执行此处理措施。

只有安装有**防毒墙网络版代理**的终端可被隔离。所需的最低版本为 **11 SP1**。必须启用该代理的防火墙。

关于更多信息，请参阅隔离终端和恢复连接 第 30 页。



IOC 管理

管理 IOC（攻击指示符）涉及以下任务：

1

IOC 文件生成

从对等安全专家和其他安全专家获取 IOC 文件。打开控制管理中心管理控制台，然后转至**管理** > **攻击指示符**以添加 IOC 文件。

如果出于某种原因，来自 Deep Discovery Analyzer 5.1 或威胁发现设备 3.8 的可疑对象并未在沙盒平台可疑对象窗口（**管理** > **可疑对象** > **沙盒平台对象**）中显示，请从被管理产品控制台中下载相应的可疑对象调查包。此调查包（可用的单独压缩文件）包含 IOC 合规文件和其他调查资源。

由于控制管理中心仅需要影响评估的 IOC 文件，所以请从压缩文件中解压 .ioc 文件，然后将其添加到控制管理中心。无法直接添加压缩文件。

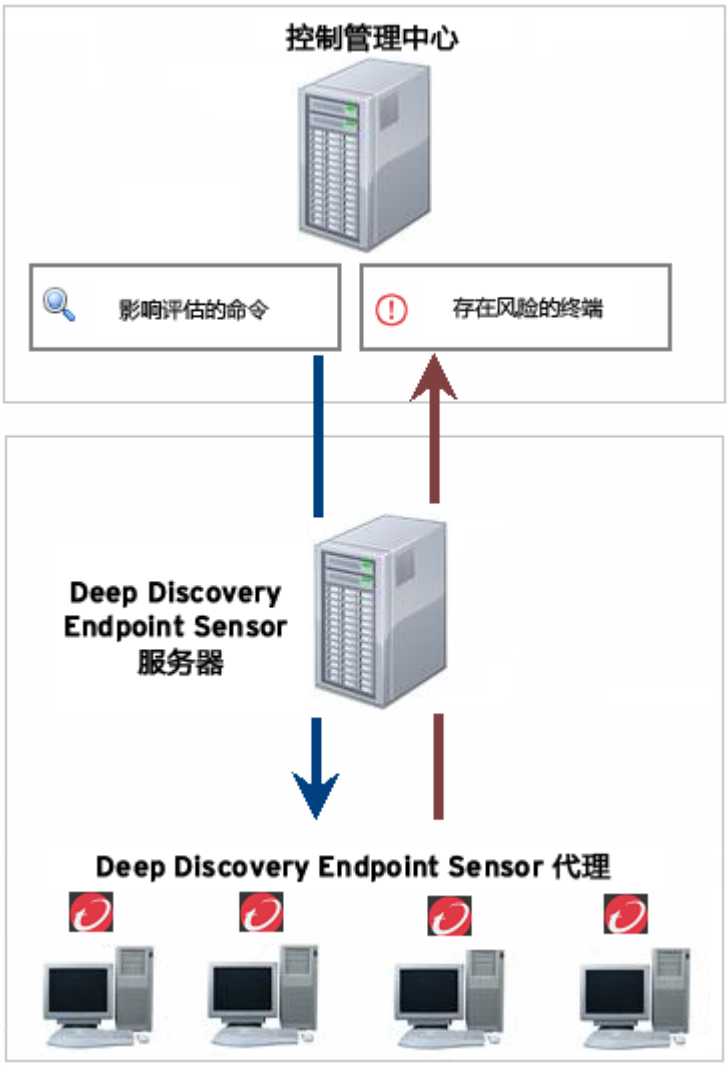
重要信息

解压并添加完 .ioc 文件后，请从计算机中删除该压缩文件，因为其可能包含潜在的恶意文件。

2

影响评估

启动影响评估，根据 IOC 文件中列出的指示符检查可疑活动。包含可疑活动的终端将被视为**存在风险**。



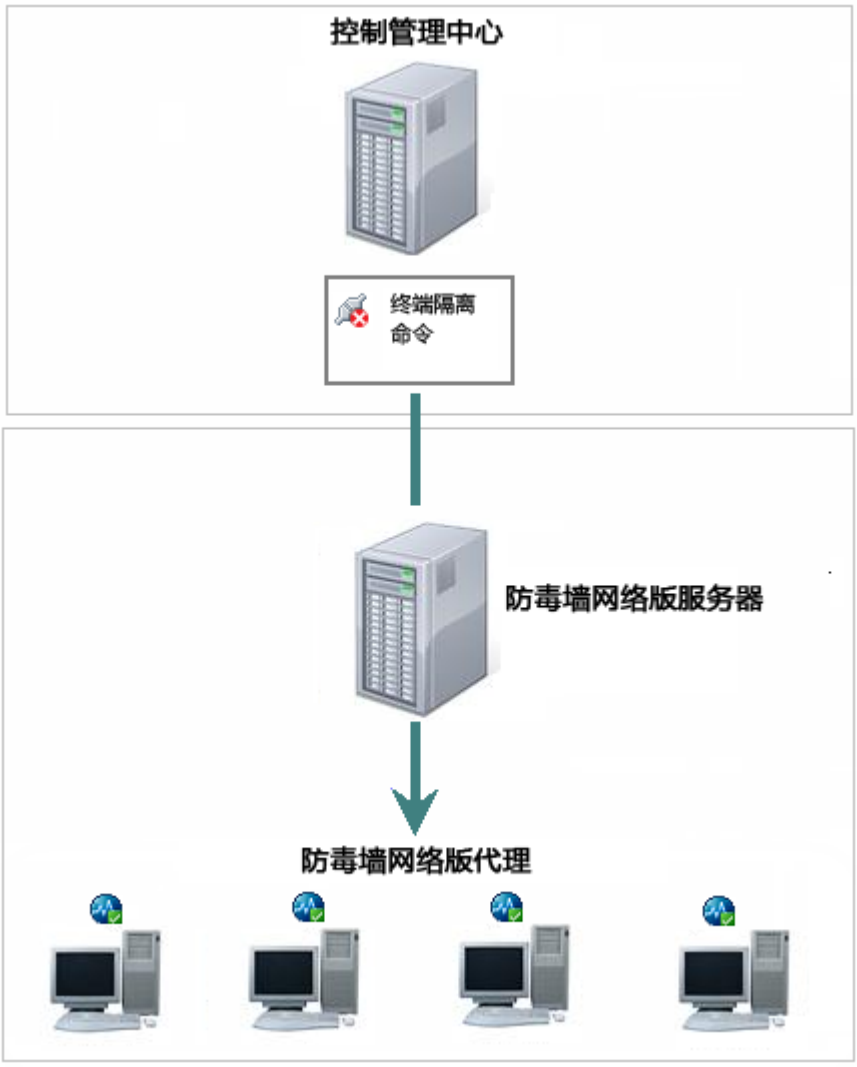
转至**管理** > **攻击指示符**，然后对一个或多个 IOC 文件运行影响评估，以确定存在风险的终端。

评估影响需要使用 **Deep Discovery Endpoint Sensor**。所需的最低版本为 **1.5**。

此产品只执行评估，不对存在风险的终端采取处理措施。

终端隔离

隔离受影响的终端，以进行详细的调查。要执行此任务，请转到**管理** > **攻击指示符**，然后再转到**存在风险**列，并单击表示存在风险的终端个数的数字。



只有安装有**防毒墙网络版代理**的终端可被隔离。所需的最低版本为 **11 SP1**。必须启用该代理的防火墙。

关于更多信息，请参阅隔离终端和恢复连接 第 30 页。

增强的安全威胁监控

使用以下**摘要**选项卡中的小组件来监控整个网络的安全并回应最关键的威胁：

- 关键威胁
- 携带威胁的用户
- 存在威胁的终端

这些小组件提供了指向“安全威胁”窗口的链接。此窗口显示在一定时间段内的威胁（依**用户**或**终端**）。

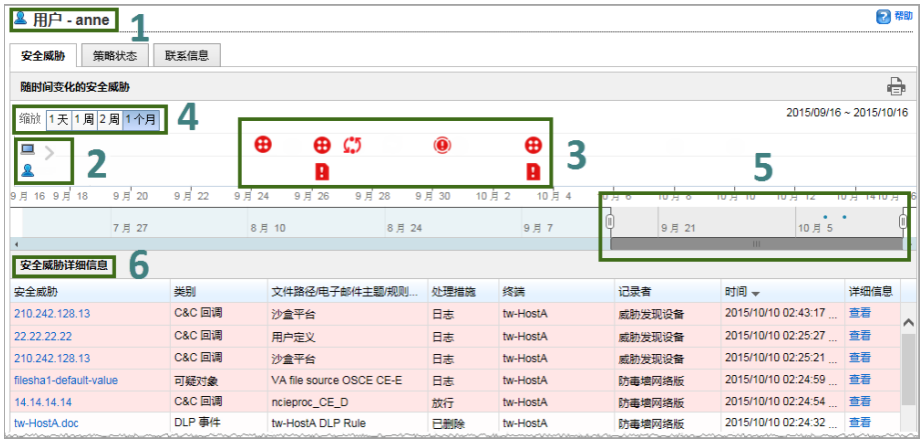
在“安全威胁”窗口中，可以重点关注特定威胁以查看其近期是否**影响了**其他用户和终端。启动**影响评估**，以查看同一威胁在很长一段时间内是否影响了更多的用户和终端。

通过这些整体视图，您可以查看可能导致攻击的企业级事件链，其中包括用于准备或发起攻击的存在风险的终端。

安全威胁（用户）

查看某用户拥有的所有终端上检测到的安全威胁。

您可以通过多种方法访问此窗口。建议的方法是转到控制台上的**携带威胁的用户**小组件，然后单击表示用户拥有的所有终端上检测到的安全威胁个数的值。



窗口中的主要用户界面元素如下：

编号	描述
1	拥有存在安全威胁的终端的用户
2	用户拥有的终端（用监控图标表示）和该用户（用人形图标表示） 缺省情况下，终端的主机名和用户的域名均显示在这些图标旁边。单击灰色箭头可以显示或隐藏主机名和域名。

<table>
<tr><th>编号</th><th colspan="3">描述</th></tr>
<tr><td>3</td><td colspan="3">用图标表示在终端上检测到的安全威胁
将鼠标置于图标上，查看威胁详细信息。</td></tr>
<tr><td></td><td> 
应用程序违例</td><td> 
行为监控违例</td><td> 
C&C 回调</td></tr>
<tr><td></td><td> 
DLP 事件</td><td> 
内容违例</td><td> 
防火墙违例</td></tr>
<tr><td></td><td> 
入侵防护事件</td><td> 
网络内容违例</td><td> 
网络钓鱼电子邮件</td></tr>
<tr><td></td><td> 
垃圾邮件</td><td> 
间谍软件/灰色软件</td><td> 
可疑对象</td></tr>
<tr><td></td><td> 
病毒/恶意软件</td><td> 
Web 违例</td><td> 
多个事件</td></tr>
<tr><td>4 和 5</td><td colspan="3">用于控制特定时间范围内检测到的安全威胁数量的过滤器</td></tr>
<tr><td>6</td><td colspan="3">含有安全威胁详细信息的表格
将关键威胁标为浅红色以便于识别。
要显示详细信息，请执行下列操作之一：
• 单击安全威胁列中的值，查看受威胁影响的用户。
• 单击详细信息列中的值，查看日志条目。</td></tr>
</table>

安全威胁（终端）

查看在特定终端上检测到的安全威胁。

您可以通过多种方法访问此窗口。建议的方式为转至控制台上的**有威胁终端**小组件，然后单击代表在终端上检测到的威胁的数目的值。

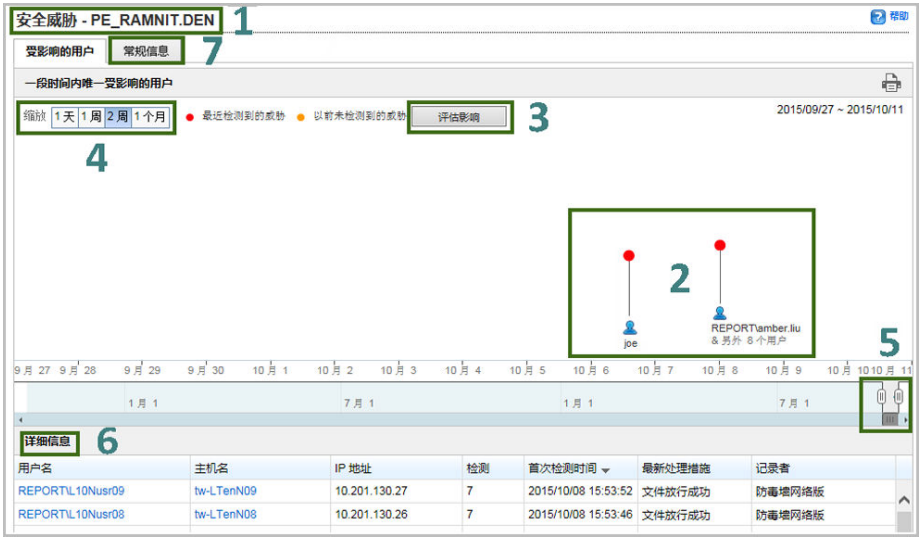
窗口中的主要用户界面元素如下：

编号	描述
1	有安全威胁的终端 如果控制管理中心已隔离了该终端或正在恢复网络连接，终端名后会显示一个图标（如下图所示）. 

<table>
<tr><th>编号</th><th colspan="3">描述</th></tr>
<tr><td>2</td><td colspan="3">用图标表示在终端上检测到的安全威胁
将鼠标置于图标上，查看威胁详细信息。</td></tr>
<tr><td></td><td> 
应用程序违例</td><td> 
行为监控违例</td><td> 
C&C 回调</td></tr>
<tr><td></td><td> 
DLP 事件</td><td> 
内容违例</td><td> 
防火墙违例</td></tr>
<tr><td></td><td> 
入侵防护事件</td><td> 
网络内容违例</td><td> 
网络钓鱼电子邮件</td></tr>
<tr><td></td><td> 
垃圾邮件</td><td> 
间谍软件/灰色软件</td><td> 
可疑对象</td></tr>
<tr><td></td><td> 
病毒/恶意软件</td><td> 
Web 违例</td><td> 
多个事件</td></tr>
<tr><td>3 和 4</td><td colspan="3">用于控制特定时间范围内检测到的安全威胁数量的过滤器</td></tr>
<tr><td>5</td><td colspan="3">可在终端上执行以下任务：
• 分配标签
• 隔离终端</td></tr>
<tr><td>6</td><td colspan="3">含有安全威胁详细信息的表格
将关键威胁标为浅红色以便于识别。
要显示详细信息，请执行下列操作之一：
• 单击安全威胁列中的值，查看受威胁影响的用户。
• 单击详细信息列中的值，查看日志条目。</td></tr>
</table>

受影响的用户

单击安全威胁（用户）或安全威胁（终端）窗口中的威胁名称会打开“受影响的用户”窗口，该窗口显示了受威胁影响的唯一用户列表。



窗口中的主要用户界面元素如下：

编号	描述
1	影响一个或多个用户的安全威胁
2	用图标代表的受影响的用户和检测性质（**最近检测到的威胁**或**以前未检测到的威胁**）。 用特定颜色代表检测的性质。请参阅**评估影响**按钮前的图例，查看每种颜色所代表的性质。 如果某个用户拥有与其他用户相似的检测，那么该用户名下面即会显示一个数字。将鼠标置于该用户名上，查看所有受影响的用户。

编号	描述
3	用来启动安全威胁影响评估的按钮 安全威胁影响评估需要使用 **Deep Discovery Endpoint Sensor** 和**威胁发现设备**。这两个产品都使用逆向扫描来执行评估。 如果只有一个产品注册到控制管理中心，将执行部分影响评估。 评估完成后，图表将使用以前未检测到的威胁列表进行更新。这些都是以前逃避了检测的隐性威胁和复杂威胁。
4 和 5	用于控制显示的受影响的用户数量的时间过滤器
6	含有受影响的用户详情的表格 单击**用户名**或**主机名**列中的值，查看用户终端上的安全威胁。
7	含有安全威胁的常规信息的选项卡

安全威胁的常规信息

查看特定安全威胁的信息。

显示的信息因从被管理产品接收的威胁类型和威胁相关信息而异。

影响评估

可通过多种方法来启动影响评估。

对可疑对象进行的影响评估

启动影响评估，检查与可疑对象相关的可疑活动。包含可疑活动的终端将被视为**存在风险**。

对可疑对象进行影响评估需要使用名为 **Deep Discovery Endpoint Sensor** 的趋势科技产品。

要启动评估，请转至**管理** > **可疑对象** > **沙盒平台对象**。

IOC 文件影响评估

启动影响评估，根据 IOC 文件中列出的指示符检查可疑活动。包含可疑活动的终端将被视为**存在风险**。

对 IOC 文件进行影响评估需要使用名为 **Deep Discovery Endpoint Sensor** 的趋势科技产品。

要启动评估，请转至**管理** > **攻击指示符**。

对安全威胁进行的影响评估

启动对安全威胁进行影响评估，检查受影响的终端。在检查以前逃避了检测的隐性威胁和复杂威胁时，此方式尤其有用。

安全威胁影响评估需要使用 **Deep Discovery Endpoint Sensor** 和**威胁发现设备**。这些产品都使用**逆向扫描**来执行评估。

如果只有一个产品注册到控制管理中心，将执行部分影响评估。

要启动评估：

1. 转至安全威胁（用户）或安全威胁（终端）窗口。
2. 单击威胁名称。此操作将打开受影响的用户窗口，显示**评估影响**选项。

了解详细信息：

逆向扫描

逆向扫描

威胁发现设备中的逆向扫描

逆向扫描是一项基于云的服务，可扫描 C&C 服务器回调尝试的历史 Web 访问日志和您网络中的其他相关活动。Web 访问日志可能会包括近期才发现的未检测到或未阻止的 C&C 服务器连接。检查此类日志是签证调查的重要组成部分，用于确定您的网络是否受攻击影响。

逆向扫描会将以下日志信息存储到云安全智能防护网络：

- 威胁发现设备监控的终端的 IP 地址

- 通过终端访问的 URL
- 威胁发现设备的 GUID

之后，逆向扫描会定期扫描存储的日志条目，以检查以下列表中 C&C 服务器的回调尝试次数：

- 趋势科技全球情报列表：趋势科技根据多个来源汇编该列表并评估每个 C&C 回调地址的风险等级。C&C 列表每天都会更新并传递到支持的产品。
- 用户定义的列表：逆向扫描还可以根据您自己的 C&C 服务器列表来扫描日志。必须将地址存储到文本文件中。

重要信息

威胁发现设备中的“逆向扫描”窗口仅显示有关使用趋势科技全球情报列表的扫描的信息。

Deep Discovery Endpoint Sensor 中的逆向扫描

逆向扫描会基于指定的搜索条件调查历史事件及其活动链。可以将结果视为用于显示任何可疑活动执行流程的 Mind Map。这样有助于分析目标攻击中涉及的企业范围的事件链。

逆向扫描将在其调查中使用以下对象类型：

- DNS 记录
- IP 地址
- 文件名
- 文件夹
- SHA-1 散列值
- MD5 散列值
- 用户帐户

逆向扫描会查询包含终端历史事件的常规数据库。与传统日志文件相比，此方法占用的磁盘空间和资源都相对较少。

隔离终端和恢复连接

隔离存在风险的终端，以调查原因并解决安全问题。在成功解决所有问题后，立即恢复相应连接。

隔离终端和恢复连接需要**防毒墙网络版代理**。所需的最低版本为 **11 SP1**。此外，防毒墙网络版代理必须启用**防火墙**。

1

启动终端隔离

隔离选项可在以下窗口中找到：

1.1 “终端”窗口

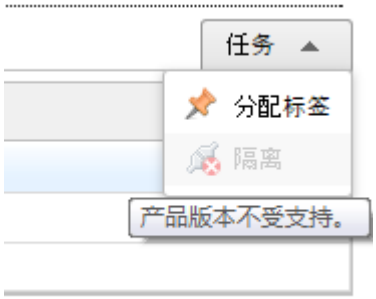
注意

“终端”窗口中的所有选项卡都包含**隔离**选项。

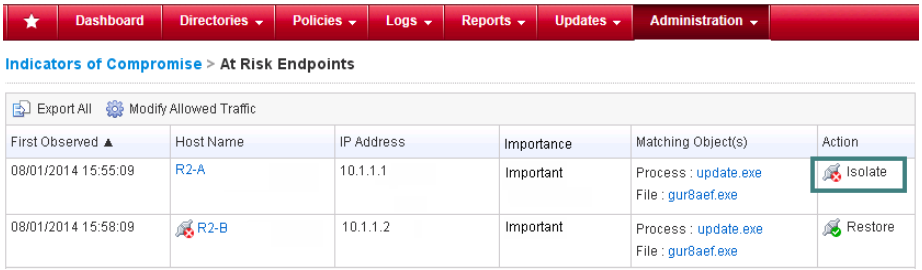
您可以通过多种方法访问此窗口。建议转到**目录** > **用户/终端**，使用窗口中的搜索功能查找要隔离的终端，当搜索结果显示出来后单击相应的终端名称。

如果无法执行隔离，**隔离**选项下方会显示一条消息，指示存在以下问题：

- 终端上的代理运行的是不受支持的版本。
- 登录控制管理中心时所用的用户帐户不具备所需的权限。



1.2 “存在风险的终端”窗口



注意

要访问此窗口，请转到**管理** > **攻击指示符**，然后再转到**存在风险**列，并单击表示存在风险的终端数量的数字。

2

监控隔离状态

隔离终端时，“终端”窗口或“存在风险的终端”窗口顶部会显示一则消息，提示您正在进行终端隔离。

隔离完成后该消息即会消失。终端上会显示一则通知，告知用户相关的隔离情况。

如果出现问题，该消息会有所改变。问题包括：

- 防毒墙网络版代理防火墙已被防毒墙网络版服务器的管理员或有权配置防火墙设置的用户禁用。也有可能防火墙已不再起作用。
- 终端上的防毒墙网络版代理未连接至其父级服务器。
- 防毒墙网络版服务器及代理均已安装到终端。隔离终端将导致防毒墙网络版服务器的功能中断。
- 发生意外错误。

刷新窗口以获取最新状态。

监控隔离终端

选择缺省过滤器**已隔离**后，即可在终端树中找到隔离终端列表。

4

配置允许的网络通信

缺省情况下，终端隔离会阻止除防毒墙网络版代理与其父级服务器之间的网络通信以外的所有入站和出站网络通信。

您可以配置想在隔离终端上允许的入站与出站网络通信。这些设置适用于**所有**隔离终端，无法针对个别终端进行配置。

如果终端上安装了其他趋势科技代理，请确保配置允许的网络通信，以便这些代理继续与其父级服务器通信。

代理	入站网络通信	出站网络通信	其他要求
Vulnerability Protection	**协议**：TCP **源 IP 地址**：父级服务器的 IP 地址 **目标端口**： 4118	**协议**：TCP **目标 IP 地址**：父级服务器的 IP 地址 **目标端口**： 4120	如果安装 Vulnerability Protection 服务器时使用了 DNS 设置，请添加 DNS 服务器的协议、IP 地址和目标端口。
Endpoint Encryption	**协议**：TCP **源 IP 地址**：父级服务器的 IP 地址 **目标端口**： 80, 8080	**协议**：TCP **目标 IP 地址**：父级服务器的 IP 地址 **目标端口**： 80, 8080	如果安装 Endpoint Encryption 服务器时使用了 DNS 设置，请添加 DNS 服务器的协议、IP 地址和目标端口。

代理	入站网络通信	出站网络通信	其他要求
Deep Discovery Endpoint Sensor	**协议**：TCP **源 IP 地址**：父级服务器的 IP 地址 **目标端口**： 8081	**协议**：TCP **目标 IP 地址**：父级服务器的 IP 地址 **目标端口**： 8002, 8003	DNS 设置（入站）： **协议**：UDP **源 IP 地址**：DNS 服务器的 IP 地址 **目标端口**： 53 DNS 设置（出站）： **协议**：UDP **目标 IP 地址**：DNS 服务器的 IP 地址 **目标端口**： 53
Endpoint Application Control	**协议**：TCP **源 IP 地址**：父级服务器的 IP 地址 **目标端口**： 80, 443, 8080, 4343	**协议**：TCP **目标 IP 地址**：父级服务器的 IP 地址 **目标端口**： 8085, 8443	如果安装 Endpoint Application Control 服务器时使用了 DNS 设置，请添加 DNS 服务器的协议、IP 地址和目标端口。

单击**应用到全部**，将这些设置部署到其代理已隔离或正在隔离终端的防毒墙网络版服务器。

恢复终端连接

完成调查并确认相应终端不存在威胁后，请恢复终端的网络连接。**恢复**选项位于“终端”窗口或“存在风险的终端”窗口上。

单击**恢复**之后，窗口顶部将显示一则消息，通知您正在恢复连接。恢复完毕后该消息即会消失。

如果出现问题，该消息会有所改变。问题包括：

- 防毒墙网络版代理防火墙已被防毒墙网络版服务器的管理员或有权配置防火墙设置的用户禁用。也有可能防火墙已不再起作用。因此，网络连接已自动恢复，但该终端仍显示在控制管理中心终端树的**已隔离**过滤器中。

  启用代理防火墙或验证其是否在正常运行，然后通过控制管理中心启动终端隔离（以使终端保持隔离状态）或恢复连接（以将该终端从终端树的**已隔离**过滤器中移除）。

- 终端上的防毒墙网络版代理未连接至其父级服务器。
- 发生意外错误。

刷新窗口以获取最新状态。

隔离终端和恢复连接历史记录

控制管理中心会保存在某个终端上执行的所有隔离和恢复连接任务的记录。要查看这些记录，请转到“终端”窗口，然后单击**附注**选项卡。

趋势科技・中国 趋势科技（中国）有限公司

上海市淮海中路 398 号世纪巴士大厦 8 楼

电话：021-6384 8899　传真：021-6384 1899　service@trendmicro.com.cn

www.trendmicro.com

Item Code: CMCM67184/150909