思科 SecureX 入门指南

首次发布日期: 2020 年 6 月 24 日

上次修改日期: 2020 年 12 月 8 日

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

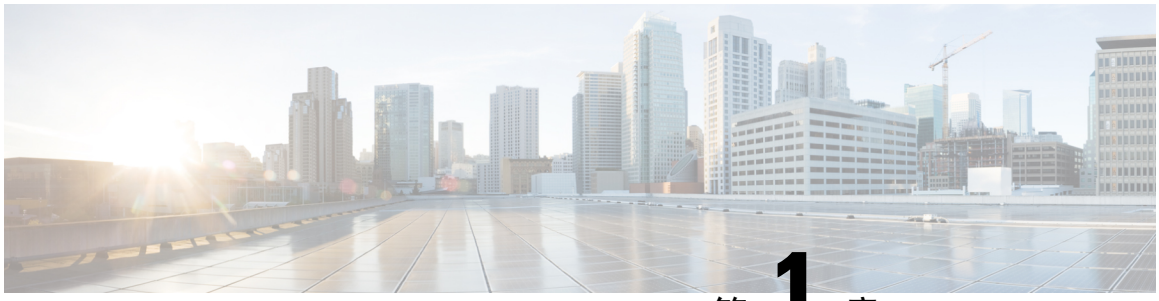
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020 Cisco Systems, Inc. 保留所有权利。

目录



第 1 章

简介

本章概述了思科 SecureX 平台，包括以下内容：

注释 本指南中显示的截图可能并不会总是反映最新的产品名称或用户界面增强功能。

关于思科 SecureX

思科 SecureX 结合了思科的集成安全产品组合以及客户基础设施的优势，旨在提供可统一可视性、实现自动化并增强网络、终端、云和应用安全性的一致体验。通过集成平台中的连接技术，SecureX 提供了可衡量的洞察力、预期成果以及无与伦比的跨团队协作。

通过 SecureX，您可以：

- 整合而不影响性能，减少供应商数量，而不会失去安全功效。
- 利用现有资源提升安全成熟度级别。
- 以更少的工作量实现更大的控制权，让您的团队专注于最重要的事情。
- 获得整个安全环境的可视性，让您知道该保护什么。
- 在共享工作流程中实现比以往更好的协作。
- 改善跨网络、终端、云和应用的主动运行状况检查和响应安全控制。
- 发挥思科安全的全部潜力，并将这些功能扩展到整个安全基础设施。
- 通过可衡量的有意义指标来实现预期结果。
- 放心地保护每家企业，同时节省时间并减少人为错误。

优势

SecureX 平台让您能够：

- 使用涵盖所有入侵载体和接入点的最广泛、集成度最高的安全平台来满足您的安全需求。
- 跨网络、终端、云和应用获取可行的见解，以加速威胁响应并实现预期结果。
- 通过自动化提高现有资源的效率和精确度，进而提升安全成熟度，提前预测不断变化的威胁形势。
- 安全运营团队、IT 运营团队和网络运营团队之间共享情景，协调安全策略，改善工作流程，实现更强的保护效果。
- 提升您购买的思科安全产品的潜力，购买前单击一下即可试用思科产品组合的其他组件，通过产品开箱即用的互通性连接您现有的安全基础设施。

支持的浏览器

以下浏览器的最新版本以及之前一个版本支持 SecureX：

- Google Chrome™
- Microsoft Edge®
- Mozilla Firefox®
- Apple® Safari®

文档

- 思科 SecureX 在线帮助 - 有关 SecureX 的完整文档，请参阅平台中的在线帮助。查看**资源**主题以观看视频，了解有关思科 SecureX 功能的更多信息。
- 思科 SecureX 登录指南 - 有关如何设置 SecureX 帐户和登录平台的信息。

最新产品

本指南中实施了以下更新：

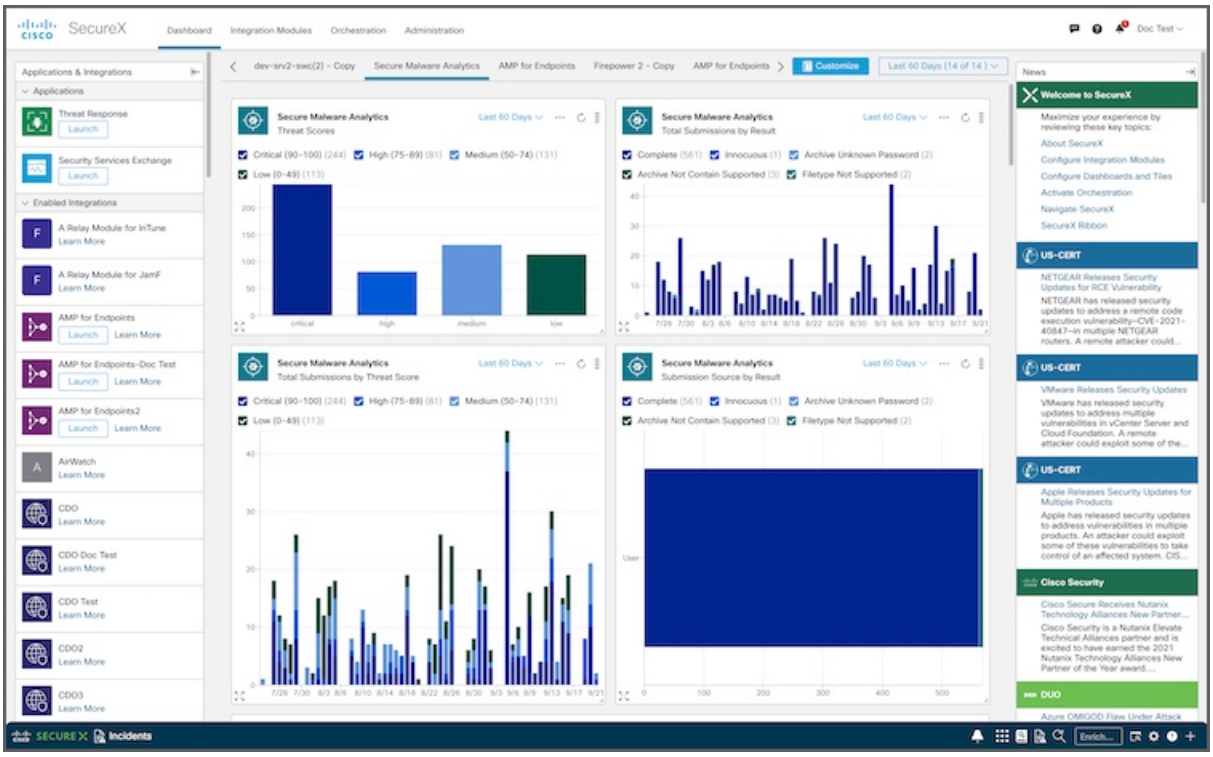
日期	功能或更新	部分
2012 年 12 月 8 日	更新了“导航思科 SecureX”以包括新的键盘快捷键和集成模块的**双向**图标。	导航思科 SecureX，第 3 页
	更新了“添加集成模块”以纳入启用模块。	添加集成模块，第 11 页
	更新了“删除集成模块”以添加有关删除带有**双向**图标的集成模块的说明。	删除集成模块，第 15 页

日期	功能或更新	部分
2021 年 10 月 20 日	更新了指南以纳入最新功能和屏幕截图。	不适用
2020 年 10 月 14 日	更新了指南以纳入最新功能和屏幕截图。	不适用
2020 年 7 月 8 日	更新了“图 1- 思科 SecureX 控制面板”	导航思科 SecureX
2020 年 7 月 23 日	更新了“功能区主页”屏幕截图和新的“思科 SecureX 功能区设置”（主题）。	功能区图标和元素
2020 年 9 月 2 日	更新了“配置集成模块”，包括添加、修改和删除模块。	配置控制面板磁贴
	更新了“配置控制面板磁贴”，以反映添加、修改和删除磁贴的更改。	配置集成模块
	更新了“配置控制面板”以反映对所需唯一控制面板名称（有字符限制）的更改。	配置控制面板
	更新了“思科 SecureX 控制面板”，以反映对磁贴的更改。	控制面板和磁贴面板
	更新了“激活协调”过程；用户现在将在被授予访问权限后收到邮件通知。	激活协调

导航思科 SecureX

本节介绍了如何导航至思科 SecureX 平台的各项主要功能。

图 *1:* 思科 ***SecureX*** 控制面板



控制面板

SecureX 控制面板可在整个组织中提供可视性和汇聚、可执行的情报。

- **应用和集成 (Applications & Integrations)** 面板位于控制面板的左侧，可用于查看集成模块以及可用于集成的模块。您可以折叠或展开该面板。
- 控制面板中心的**磁贴 (Tiles)** 面板会显示来自集成模块的指标和数据，以便让整个安全环境一目了然并加速威胁响应。

  您可以添加要在控制面板上显示的磁贴。有关详细信息，请参阅配置控制面板磁贴和配置控制面板帮助主题。

> **注释** 在 SecureX 演示中，**磁贴 (Tiles)** 面板会显示磁贴以及来自各种集成模块的样本指标和数据。您可以单击示例磁贴中的任何数据，了解有关该产品的更多信息，包括用于启用集成模块的链接和用于访问免费试用版的链接（如果可用）。

- **新闻 (News)** 面板位于控制面板的右侧，提供与您相关的公司范围公告/行业新闻和安全博客帖子的更新。您可以折叠或展开该面板。

色带

SecureX 是集中式控制台和分布式功能集，可统一可视性，实现自动化，加速事件响应工作流程并改善威胁搜索。这些分布式功能以 SecureX 功能区中的应用程序（应用）和工具的形式呈现。

功能区位于页面下方，当您在控制面板和环境中的其他安全产品之间移动时，此功能仍然存在。

图 *2:* 思科 *SecureX* 功能区 - 已折叠

使用功能区访问案例集和其他应用、搜索用于充实的可观察对象，以及查看事件。有关详细信息，请参阅色带。

注释 如果您是 SecureX 演示中未激活的用户，则必须启用集成模块才能激活 SecureX 帐户，然后才能访问功能区。

集成模块

借助思科 SecureX，事件响应者可以通过收集、组合和关联思科 Talos 提供的威胁智能与思科和组织内部署的第三方安全产品的网络和安全数据，从而更好地了解其网络上的威胁。它将威胁智能和本地安全情景与控制整合到一起，以供安全分析师使用。每个全局或本地情报源都由一个模块提供，而该模块会通过 API 密钥来链接。

SecureX 为思科安全产品和第三方解决方案提供集成模块。使用 SecureX 菜单栏上的**集成模块 (Integration Modules)** 选项卡来配置和查看集成模块，以及查看可用于配置的所有集成模块。

为您的环境配置的所有模块都会显示在**我的集成模块 (My Integration Modules)** 页面上。模块面板指示模块是否为**集成 (Integrated)**（已成功配置）或配置是否存在**错误 (Error)**。如果 SecureX 和集成产品通过集成模块接口相互进行双向 API 通信，则还会显示**双向**图标。

所有可用于配置的模块都显示在**可用集成模块 (Available Integration Modules)** 页面上。

注释 在 SecureX 演示中，**集成模块 (Integration Modules)** 页面会显示可用以激活 SecureX 的思科安全产品。

有关详细信息，请参阅配置集成模块。

协调

协调 (Orchestration) 页面提供了一个用于自动化安全过程的框架，例如威胁调查，搜索和补救，以提高运营效率和准确性。

SecureX 协调是一项工作流程自动化功能，可用于定义工作流程以反映典型的安全流程；自动化步骤（活动）、这些步骤之间的逻辑或流程，以及如何将数据从一个步骤传输到下一个步骤。借助 SecureX，您可以利用环境中的思科和第三方多域系统、应用、数据库和网络设备创建这些工作流程。

有关详细信息，请参阅思科 SecureX 在线帮助中的**协调**主题。

注释 您必须激活协调，然后才能访问**协调**页面。有关详细信息，请参阅激活协调。

管理

管理 (Administration) 页面可用于查看您的帐户信息、配置设备和 API 客户端，以及管理现有用户和邀请用户加入您的 SecureX 组织。

有关详细信息，请参阅思科 SecureX 在线帮助中的**管理**主题。

反馈

单击菜单栏右上角的**反馈**图标，打开**提供反馈 (Give Us Feedback)** 表单并向 SecureX 团队提交意见或问题。有关详细信息，请参阅 SecureX 联机帮助中的**反馈**主题。

帮助

单击菜单栏右上角的**帮助**图标，访问在线帮助主题，了解有关思科 SecureX 的更多信息。

要访问集成产品的产品特定文档，请参阅 SecureX 联机帮助中的**集成**主题。

通知

通知 (Notifications) 图标会显示根据严重性进行颜色标记的通知数量。单击此图标以显示通知列表。

键盘快捷键

SecureX 支持以下键盘快捷键：

- 按 **Shift+F** 以打开**提供反馈 (Give Us Feedback)** 表单。
- 按 **?** 或 **Shift+/** 以打开键盘快捷键帮助，了解有关 SecureX 中可用的键盘快捷键的详细信息。

用户配置文件

单击右上角的用户名旁边的下拉箭头，以便查看您的登录凭证、角色和组织。您可以单击凭证区域中的任意位置打开**管理 (Administration)** 页面并查看您的用户帐户。请参阅 SecureX 联机帮助中的**管理**主题。

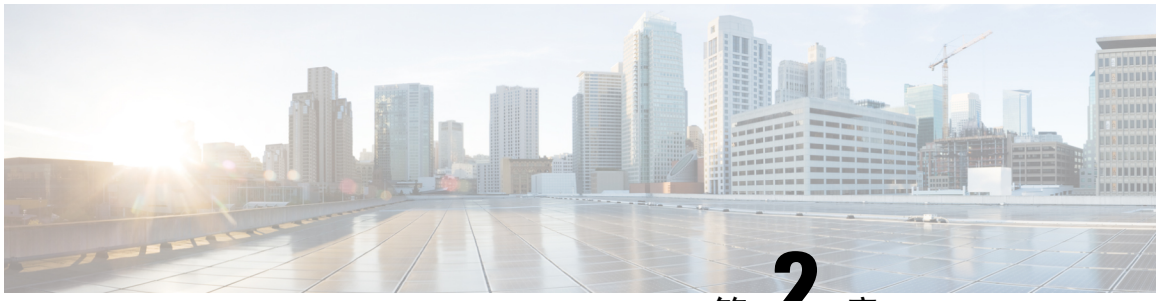
您还可以使用**用户配置文件 (User Profile)** 下拉菜单以更改 SecureX 用户界面的颜色主题、查看系统状态和注销平台。

- **主题 (Theme)** - 您可以选择要显示 SecureX 用户界面的颜色主题。默认颜色主题会显示浅色背景；而黄昏主题会显示深色背景。

  要更改颜色主题，请单击**浅色 (Light)** 或**黄昏 (Dusk)**。

- **系统状态 (System Status)** - 您可以通过**用户配置文件 (User Profile)** 菜单中的**系统状态 (System Status)** 选项来查看系统状态和订用更新。

- **注销 (Logout)** - 在**用户配置文件 (User Profile)** 菜单中选择**注销 (Logout)** 以注销 SecureX。注销页面的下半部分会显示您的身份提供程序。单击链接也会从身份验证提供程序注销。



第 2 章

配置

本章提供有关配置思科 SecureX 环境的说明，包括：

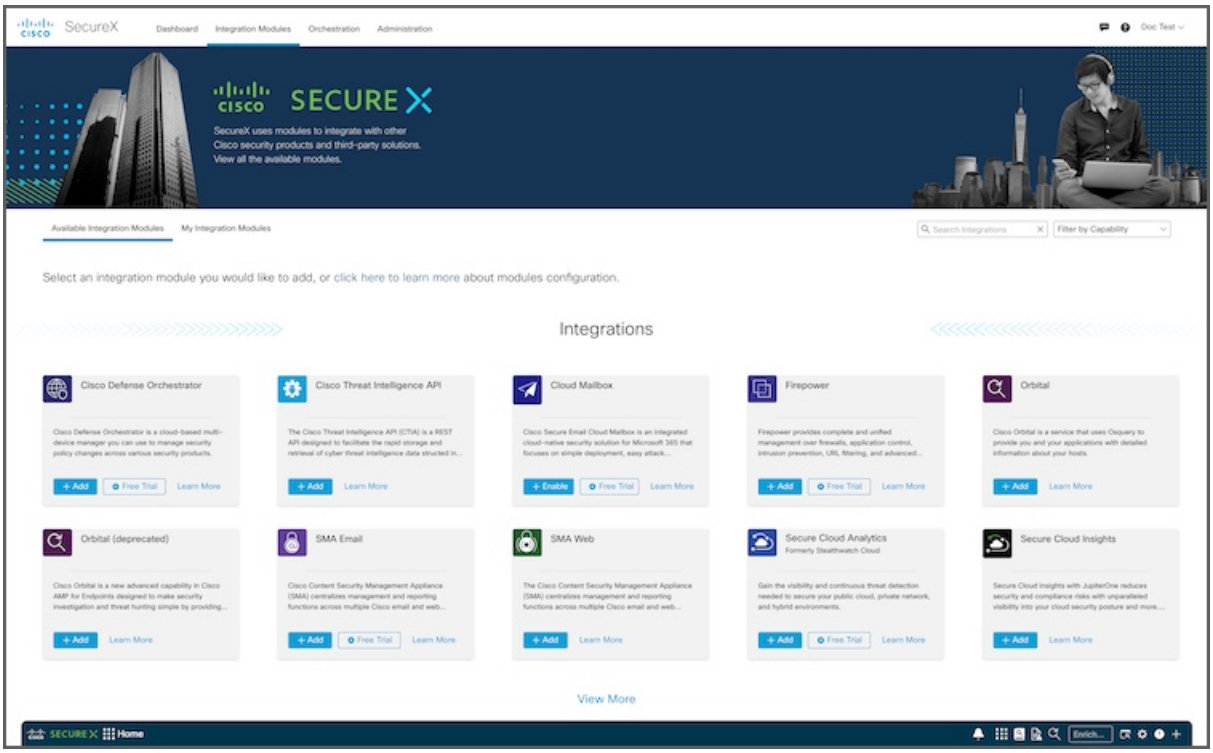
配置集成模块

思科 SecureX 为思科安全产品和第三方解决方案提供集成模块。您必须为产品集成配置模块，以便数据（和响应操作，如果适用）可用在 SecureX 中。本节介绍了如何为您的产品配置新的集成模块的全过程。

注释 只有管理员用户可以添加集成模块。如果您以非管理员用户身份登录，则不会出现**添加 (Add)** 按钮。

使用 SecureX 菜单栏上的**集成模块 (Integration Modules)** 选项卡来配置和查看集成模块，以及查看可用于配置的所有集成模块。

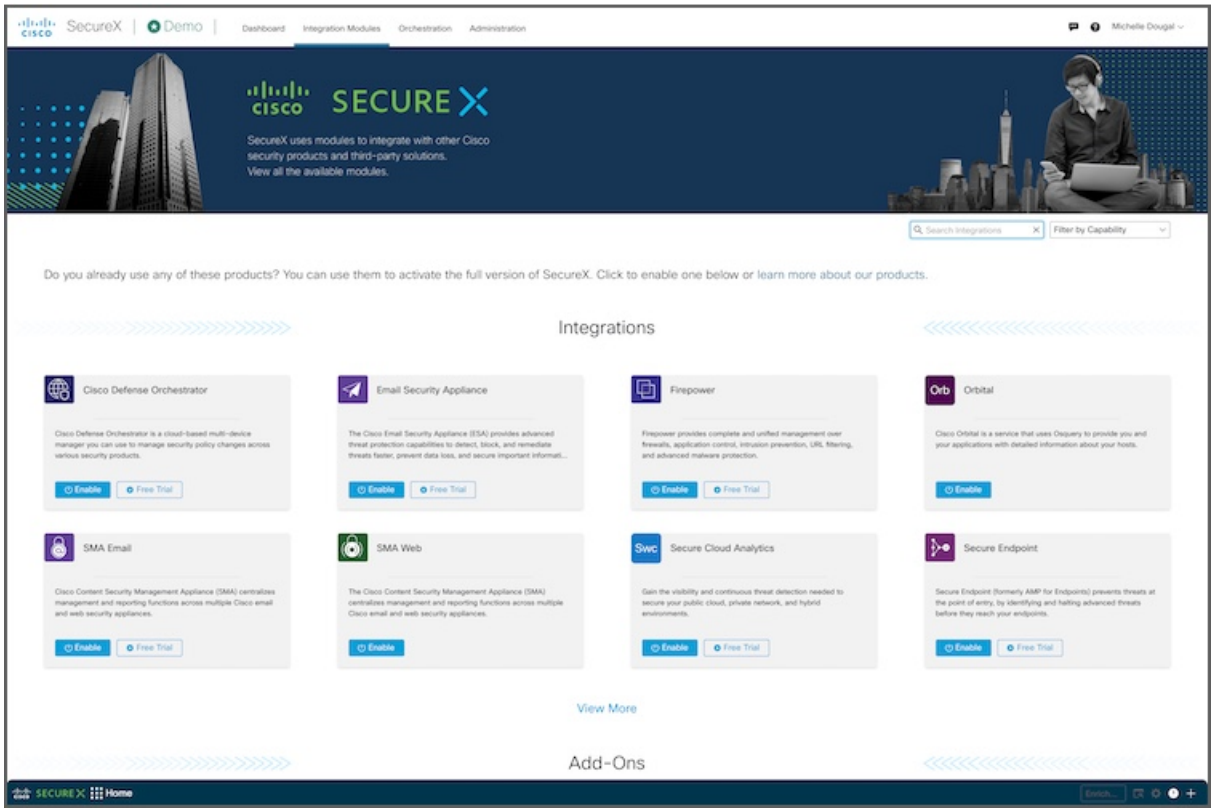
图 *3:* 集成模块



您可以在**我的集成模块 (My Integration Modules)** 页面上查看已配置的集成模块，并在**可用集成模块 (Available Integration Modules)** 页面上查看可用于配置的所有集成模块。

在 SecureX 演示中，您可以在**集成模块 (Integration Modules)** 页面上查看可用于配置的所有集成模块，以便激活 SecureX。

图 *4: SecureX* 演示中的集成模块



注释 如果您的产品是现场设备，则必须在配置集成模块之前在安全服务 Exchange 中注册。有关在 SecureX 中添加集成模块之前配置设备的信息，请参阅特定产品文档。

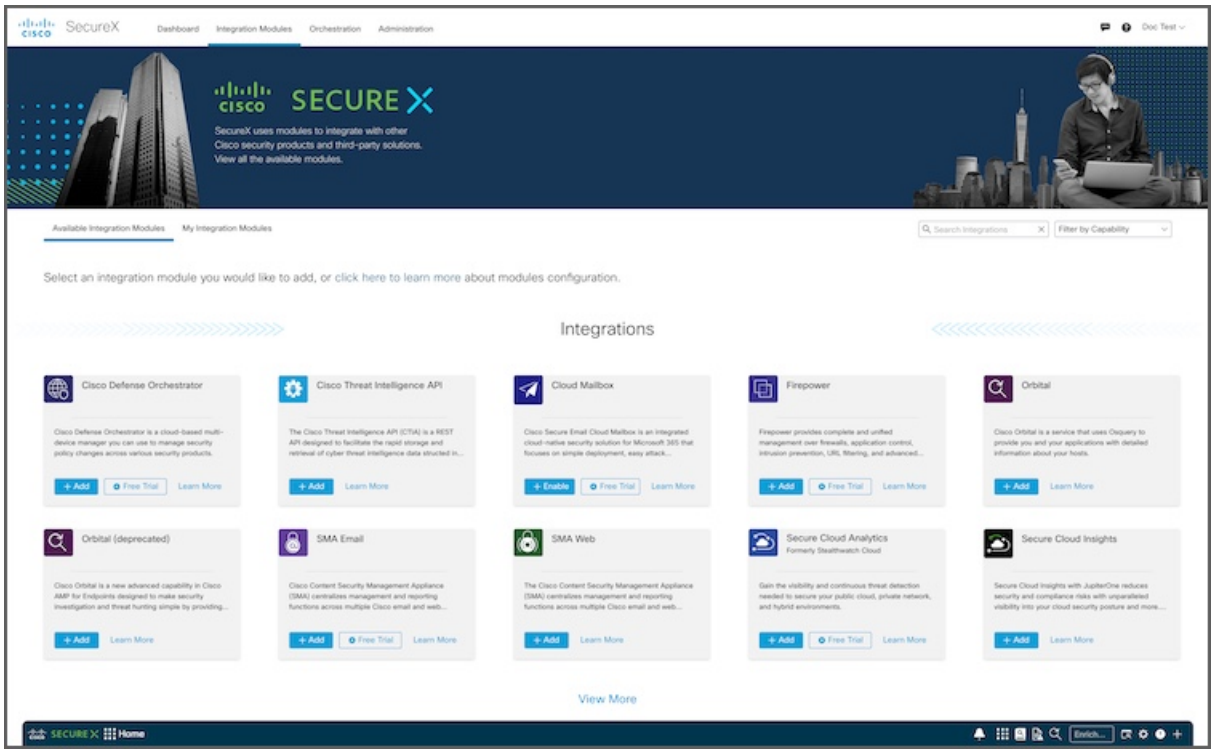
添加集成模块

执行以下步骤以添加集成模块：

步骤 1 登录思科 SecureX。

步骤 2 单击 SecureX 菜单栏中的**集成模块 (Integration Modules)** 选项卡。

图 *5:* 可用的集成模块



您可以根据功能来过滤页面上显示的模块。您还可以根据集成模块名称和说明来搜索页面上显示的模块。

注释　　如果您是 SecureX 演示中未激活的用户，则**集成模块 (Integration Modules)** 页面仅会列出可用的集成模块。

步骤 3　在**可用集成模块 (Available Integration Modules)** 页面上，导航至要配置的集成模块，然后在模块面板中单击**添加 (Add)** 或**启用 (Enable)**。如果您位于**我的集成模块 (My Integration Modules)** 页面中，请单击**添加新集成模块 (Add New Integration Module)** 以打开**可用集成模块 (Available Integration Modules)** 页面。

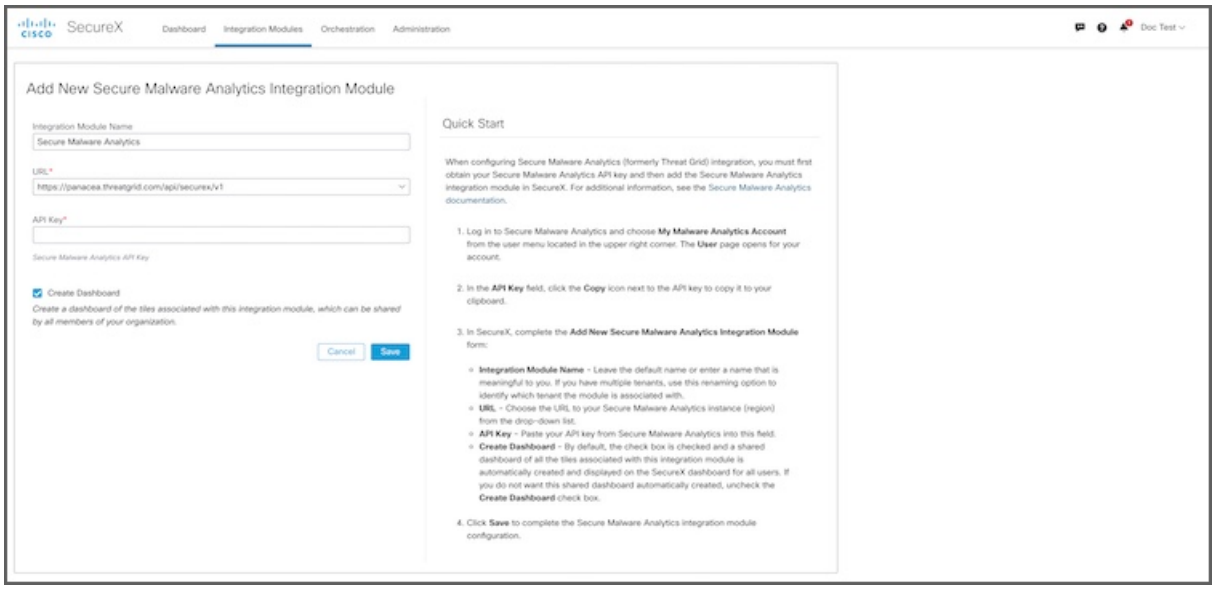
图 *6:* 添加新模块

注释　　如果单击**启用 (Enable)**，则会完成集成产品中的集成模块配置和激活。启用后，它会自动集成到SecureX中，并且集成模块会显示在**我的集成模块 (My Integration Modules)** 页面中并带有**双向**图标。您无需完成其余步骤。

在 SecureX 演示中，导航至要配置的集成模块，然后在模块面板中单击**启用 (Enable)**。

步骤 4 按照**快速启动 (Quick Start)** 面板中的说明，填写**添加新模块 (Add New Module)** 或**启用模块 (Enable Module)**表单。

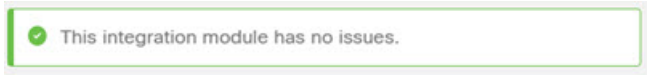
图 *7:* 添加新模块表单



步骤 5 单击**保存 (Save)** 以添加集成模块。执行运行状况检查以确定模块是否配置正确。

系统会在表单的上半部分显示一条消息（由于已保存，表单会变成**编辑模块 (Edit Module)**），从而表明运行状况检查正在运行。完成后，系统会显示一条消息，指明配置没有问题或发现了错误。

图 *8:* 运行状况检查



如果发生错误，请更正配置并单击**保存 (Save)**。

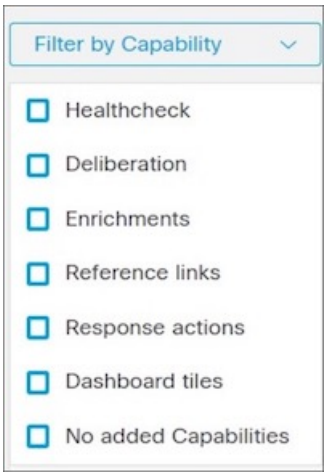
步骤 6 单击**取消 (Cancel)** 退出表单。

模块显示在**我的集成模块 (My Integration Modules)** 页面上，并显示其是否为**集成 (Integrated)** 模块，或者配置是否存在**错误 (Errors)**。

过滤器集成模块

在**可用集成模块 (Available Integration Modules)** 页面上，单击**过滤器 (Filter)** 下拉列表，然后选中功能旁边的复选框以过滤页面上显示的模块。

图 *9:* 按功能过滤



与您的选择匹配的模块会显示在页面上。

搜索集成模块

在**可用集成模块 (Available Integration Modules)** 或**我的集成模块 (My Integration Modules)** 页面上的**搜索集成 (Search Integrations)** 文本框中输入搜索条件，以便按集成模块名称和说明来搜索集成模块。与您的搜索条件匹配的集成模块将显示在**可用集成模块 (Available Integration Modules)** 或**我的集成模块 (My Integration Modules)** 页面上。

更新集成模块

为您的环境配置的所有集成模块都会显示在**我的集成模块 (My Integration Modules)** 页面上。模块面板指示模块是否为**集成 (Integrated)**（已成功配置）或配置是否存在**错误 (Error)**。如果存在错误，您可以编辑模块。

执行以下步骤可编辑集成模块：

步骤 1 登录思科 SecureX。

步骤 2 单击 SecureX 菜单栏中的**集成模块 (Integration Modules)** 选项卡。

步骤 3 导航至**我的集成模块 (My Integration Modules)** 页面上的模块，然后单击模块窗格中的**编辑 (Edit)**。系统将打开**编辑集成模块 (Edit Integration Module)** 表单，其中包含了当前的集成模块设置。

步骤 4 根据需要编辑设置，然后单击**保存 (Save)**。

执行运行状况检查以确定模块是否配置正确。系统会在**编辑模块 (Edit Module)** 表单的上半部分显示一条消息，从而表明运行状况检查正在运行。完成后，系统会显示一条消息，指明配置没有问题或发现了错误。

步骤 5 单击**取消 (Cancel)** 退出表单。

删除集成模块

我的集成模块 (My Integration Modules) 页面上会显示与您的帐户关联的所有模块。您可以删除集成模块，并且该集成中的所有数据将不再可用。

执行以下步骤以删除集成模块：

步骤 1 登录思科 SecureX。

步骤 2 导航至**我的集成模块 (My Integration Modules)** 页面上的模块，然后单击模块面板中的**编辑 (Edit)**。系统将打开**编辑模块 (Edit Module)** 表单，其中包含当前集成模块设置。

步骤 3 单击**删除 (Delete)**。

步骤 4 在确认对话框中，单击**删除 (Delete)**。

集成模块已删除，其数据不再可用。

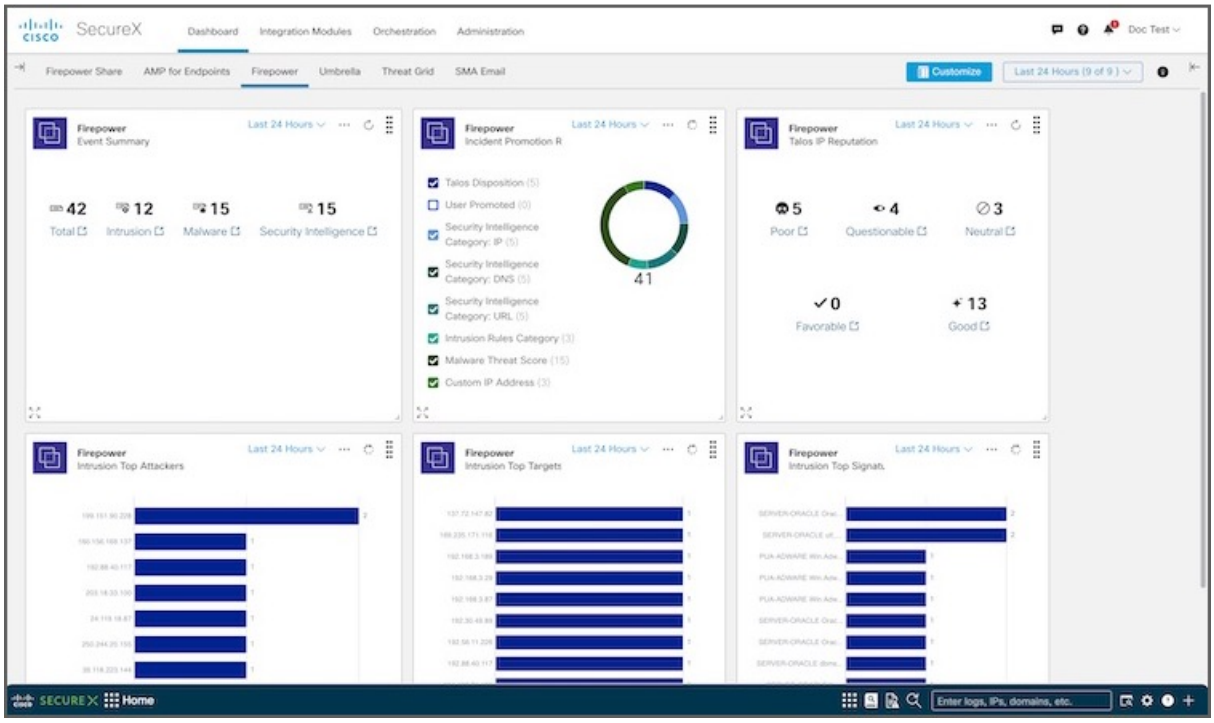
注释 如果要删除带有**双向**图标的集成模块，请确保在集成产品中也禁用了集成。

配置控制面板磁贴

思科 SecureX 控制面板中心的**磁贴 (Tiles)** 面板会显示来自集成产品的指标和数据，以便让整个安全环境一目了然并加速威胁响应。在 SecureX 中添加集成后，基础产品提供的磁贴可用于添加到您的控制面板。如果启用自动创建与集成模块关联的所有磁贴的共享控制面板的选项，则系统会自动为所有用户创建共享控制面板并显示在 SecureX 控制面板上。

您最多可以创建 20 个控制面板（请参阅添加控制面板），并且还可以添加磁贴以自定义视图。例如，您可能需要显示每个集成模块的控制面板，以及特定于该集成的磁贴。

图 *10:* 控制面板磁贴

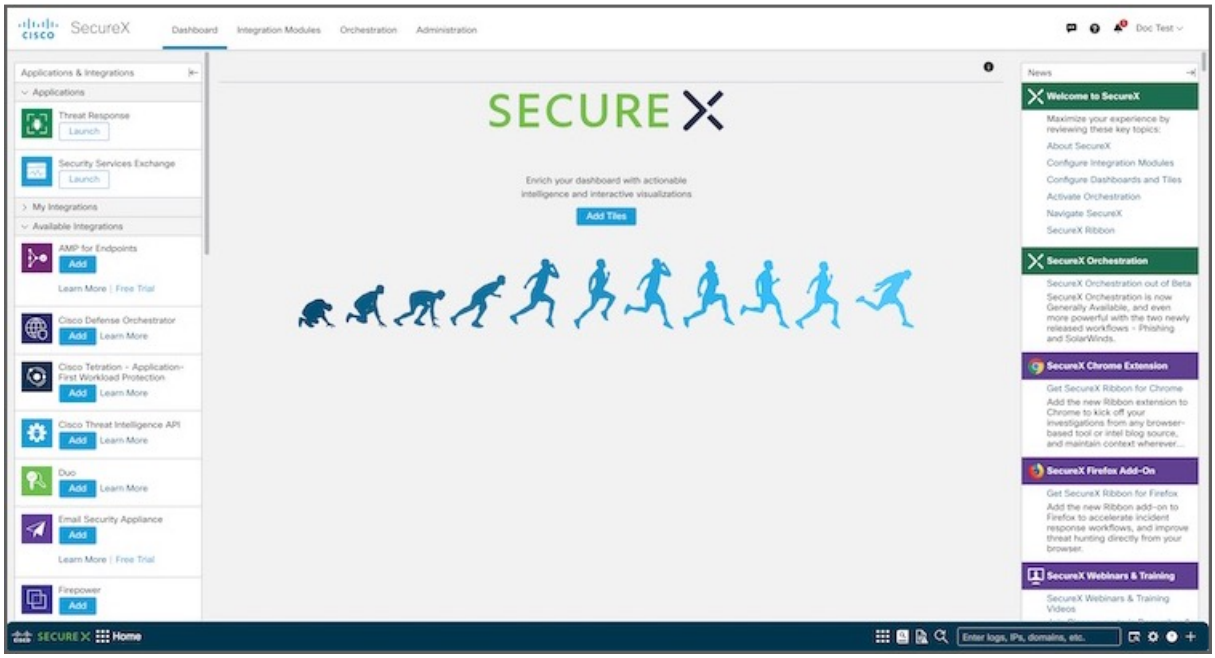


将磁贴添加到控制面板

如果未配置控制面板，则必须添加要在控制面板上显示的磁贴。

步骤 1 在控制面板中心的**磁贴 (Tiles)** 面板中，单击**添加磁贴 (Add Tiles)**。

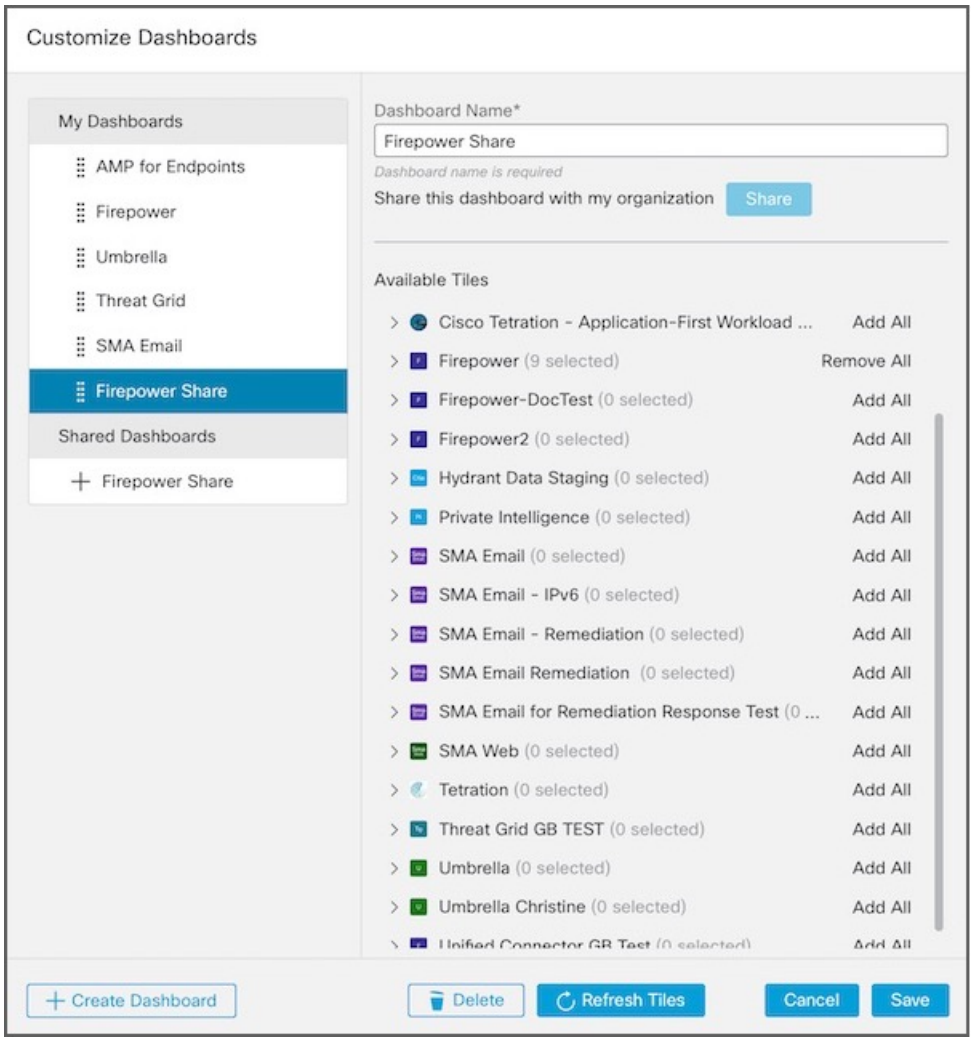
图 *11:* 添加磁贴



注释　　**添加磁贴 (Add Tiles)** 按钮只会在配置控制面板后显示。

您还可以单击控制面板菜单栏上的**自定义 (Customize)** 按钮，以添加、修改和删除控制面板上的磁贴，共享控制面板，以及创建新的控制面板并对其重新排序。

图 *12:* 自定义控制面板



步骤 2 使用默认的**控制面板名称 (Dashboard Name)** 或输入唯一名称（控制面板名称为必填且必须唯一，最多 32 个字符）。

步骤 3 展开集成模块名称，然后选中或取消选中要在控制面板中显示的磁贴的复选框。

您还可以单击特定集成模块的**全部添加 (Add All)**（选中所有复选框）或**全部删除 (Remove All)**（取消选中所有复选框）进行切换。

注释 要更新磁贴定义列表，请单击**刷新磁贴 (Refresh Tiles)**。

所选的磁贴数量会显示在集成模块名称旁边的括号中。

步骤 4 如果您是管理员用户，可以单击右侧面板中的**共享 (Share)** 以便与组织内的其他用户共享控制面板。有关共享控制面板的详细信息，请参阅 共享控制面板，第 23 页。

步骤 5 要添加更多控制面板，请单击**创建控制面板 (Create Dashboard)** 并重复此过程。

步骤 6 或者，将新创建的控制面板重新排序，让它们显示在 SecureX 控制面板上想要的位置。要对控制面板重新排序，请单击左侧面板中的控制面板，然后将其拖动到列表中的所需位置。

步骤 7 单击**保存 (Save)** 以完成流程。

添加磁贴后，您可以调整其大小并将其移至 SecureX 控制面板上的所需位置。

修改控制面板上的磁贴

您可以重命名控制面板、添加磁贴或删除磁贴。执行以下步骤，以便修改控制面板上显示的磁贴：

步骤 1 在 SecureX 控制面板菜单栏上，单击**自定义 (Customize)** 以打开**自定义控制面板 (Customize Dashboard)** 表单。

步骤 2 在左侧面板中选择控制面板。

步骤 3 进行修改：

- **控制面板名称 (Dashboard Name)** - 您可以修改控制面板的名称。控制面板名称是必填字段并且必须是唯一的，最大长度为 32 个字符。
- **可用磁贴 (Available Tiles)** - 选中（添加）或取消选中（删除）要在控制面板上显示的磁贴的复选框。

  您还可以单击特定集成的**全部添加 (Add All)**（选中所有复选框）或**全部删除 (Remove All)**（取消选中所有复选框）进行切换。

步骤 4 如果控制面板已共享，则可以单击右侧面板中的**共享 (Share)**，以便用您的更改来更新控制面板。共享控制面板的其他用户将能够将您的编辑同步到其共享版本。

注释 只有管理员用户可以共享控制面板。

步骤 5 单击**保存 (Save)**。

删除控制面板上的磁贴

要从所选控制面板中删除磁贴，只需单击磁贴右上角的**设置**图标，然后选择**删除磁贴 (Remove Tile)**。

您还可以从**自定义控制面板 (Customize Dashboards)** 表单中删除磁贴：

步骤 1 在 SecureX 控制面板菜单栏上，单击**自定义 (Customize)** 以打开**自定义控制面板 (Customize Dashboards)** 表单。

步骤 2 在左侧面板中选择控制面板。

步骤 3 展开集成模块名称，然后取消选中要从控制面板中删除的磁贴的复选框。

您还可以单击特定集成模块的**全部删除 (Remove All)**（以取消选中所有复选框）。

步骤 4 如果控制面板已共享，您可以单击**共享 (Share)**，以便用您的更改来更新共享的控制面板。共享控制面板的其他用户将能够将您的编辑同步到其共享版本。

注释　只有管理员用户可以共享控制面板。

步骤 5 单击**保存 (Save)**。

配置控制面板

您可以在思科 SecureX 中创建多个控制面板（最多 20 个），以便自定义集成模块提供的数据视图。您还可以共享控制面板，重新排列控制面板的显示方式，以及删除控制面板。

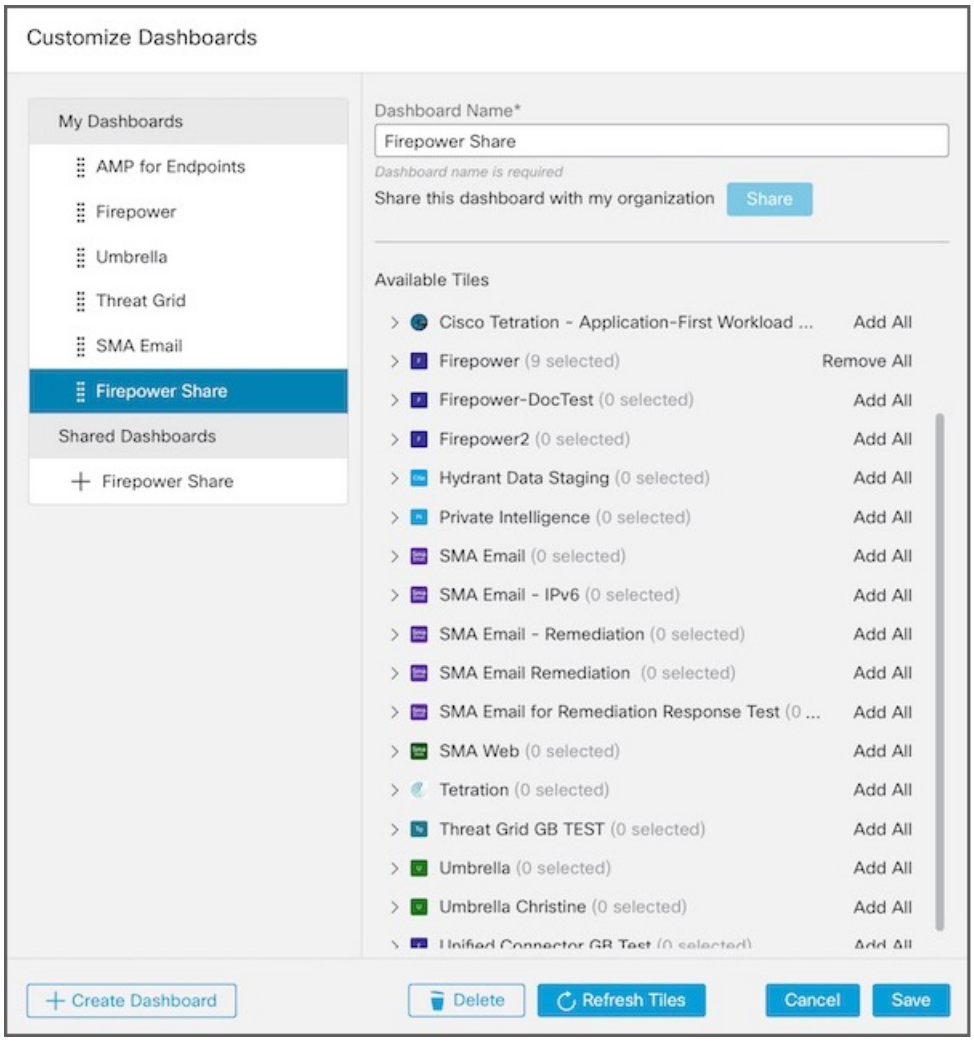
注释　只有管理员用户可以共享控制面板。

添加控制面板

您最多可以创建 20 个控制面板来自定义视图。

步骤 1 在 SecureX 控制面板菜单栏上，单击**自定义 (Customize)** 以打开**自定义控制面板 (Customize Dashboards)** 表单。

图 *13:* 自定义控制面板



步骤 2 单击**创建控制面板 (Create Dashboard)** 并输入唯一的**控制面板名称 (Dashboard Name)**。

注释 控制面板名称是必填字段并且必须是唯一的，最大长度为 32 个字符。

步骤 3 展开**可用磁贴 (Available Tiles)** 列表中的集成模块名称，然后选中要添加到控制面板的磁贴的复选框。

您还可以单击特定集成模块的**全部添加 (Add All)**（选中所有复选框）或**全部删除 (Remove All)**（取消选中所有复选框）进行切换。

注释 要更新磁贴定义列表，请单击**刷新磁贴 (Refresh Tiles)**。

所选的磁贴数量会显示在集成模块名称旁边的括号中。

步骤 4 如果您是管理员用户，并且要与组织内的其他用户共享新控制面板，请单击右侧面板中的**共享 (Share)**。有关共享控制面板的详细信息，请参阅 共享控制面板 ， 第 23 页。

步骤 5 要添加更多控制面板，请单击**创建控制面板 (Create Dashboard)** 并重复此过程。

步骤 6 或者，将新创建的控制面板重新排序，让它们显示在 SecureX 控制面板上想要的位置。要对控制面板重新排序，请单击左侧面板中的控制面板，然后将其拖动到列表中的所需位置。

步骤 7 完成添加控制面板和/或对其重新排序后，单击**保存 (Save)**。

新的自定义控制面板会显示在 SecureX 控制面板上。

添加共享控制面板

您可以将组织内管理员用户共享的控制面板添加到**我的控制面板 (My Dashboards)** 列表，以获取预定义磁贴的自定义视图。添加后，右侧面板中会显示**同步到原始 (Sync to Original)** 图标，您可以将控制面板与原始控制面板的最新版本同步。

有关共享控制面板的详细信息，请参阅 共享控制面板，第 23 页。

步骤 1 在 SecureX 控制面板菜单栏上，单击**自定义 (Customize)** 以打开**自定义控制面板 (Customize Dashboards)** 表单。

步骤 2 在**共享控制面板 (Shared Dashboards)** 列表中，单击要添加到**我的控制面板 (My Dashboards)** 列表中的控制面板列表的控制面板旁边的添加 (+) 按钮。

共享控制面板的副本会被添加到**我的控制面板 (My Dashboards)** 列表中。

步骤 3 您可以选择通过修改名称和/或磁贴来对新添加的共享控制面板进行更改。

步骤 4 完成添加共享控制面板后，单击**保存 (Save)**。

修改控制面板

您可以使用菜单栏上的**自定义 (Customize)** 按钮来修改控制面板名称以及它上面显示的磁贴。

步骤 1 在 SecureX 控制面板菜单栏上，单击**自定义 (Customize)** 以打开**自定义控制面板 (Customize Dashboards)** 表单。

步骤 2 进行修改；您可以修改**控制面板名称**（名称必须唯一），添加或删除要在控制面板上显示的磁贴（请参阅配置控制面板磁贴），并对控制面板重新排序。

步骤 3 单击**保存 (Save)**。

控制面板重新排序

您可以使用 SecureX 控制面板上的**自定义 (Customize)** 按钮重新排列控制面板在菜单栏上的显示方式：

步骤 1 在 SecureX 控制面板菜单栏上，单击**自定义 (Customize)** 以打开**自定义控制面板 (Customize Dashboards)** 表单。

步骤 2 在**我的控制面板 (My Dashboards)** 列表中，单击控制面板并将其拖动到列表中的所需位置。

步骤 3 完成对控制面板的重新排序后，单击**保存 (Save)**。

删除控制面板

使用 SecureX 控制面板上的**自定义 (Customize)** 按钮来删除控制面板：

步骤 1 在 SecureX 控制面板菜单栏上，单击**自定义 (Customize)** 以打开**自定义控制面板 (Customize Dashboards)** 表单。

步骤 2 在**我的控制面板 (My Dashboards)** 列表中选择控制面板，然后单击**删除 (Delete)**。

确认消息会显示在表单的下半部分。

步骤 3 单击**删除 (Delete)** 以确认操作。

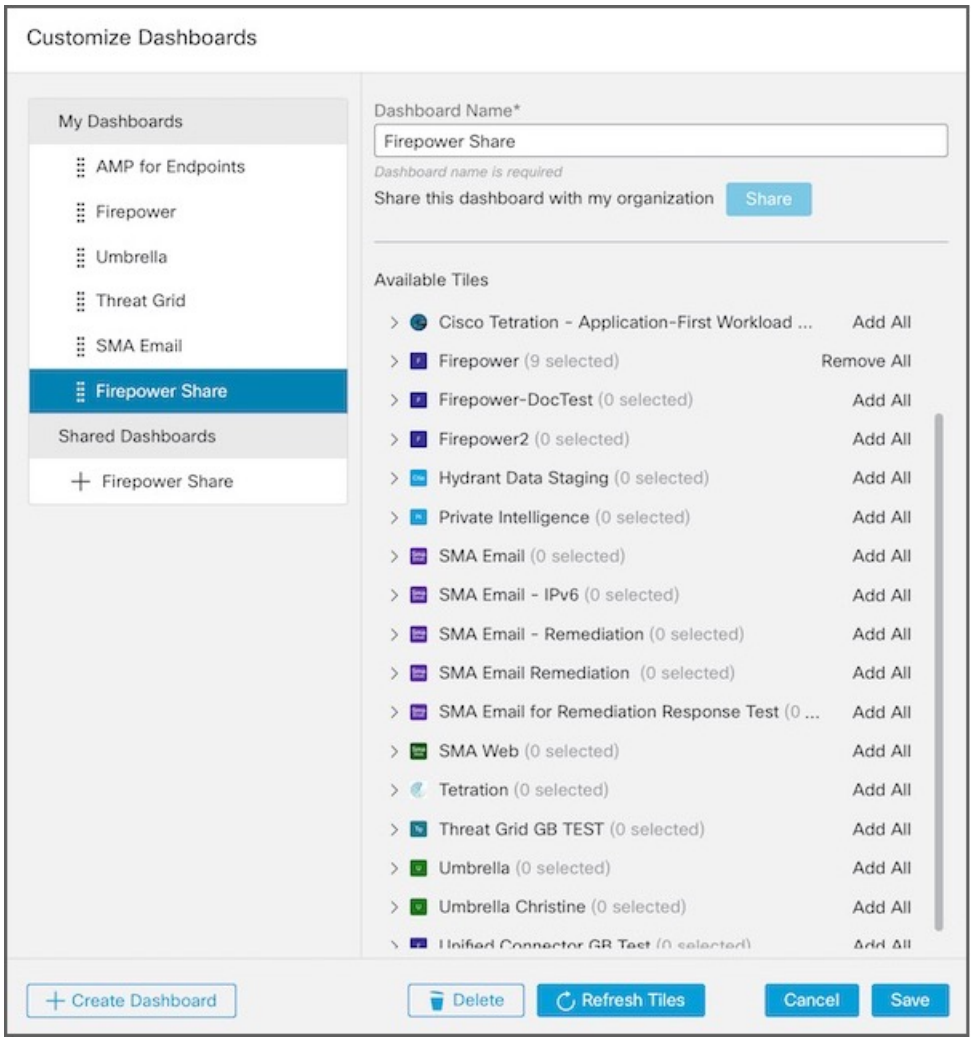
如果已删除的控制面板是共享控制面板，则该控制面板会从**我的控制面板 (My Dashboards)** 列表中删除，但会继续在**共享控制面板 (Shared Dashboards)** 列表中共享。

共享控制面板

管理员用户可以与组织内的其他用户共享控制面板。

步骤 1 在 SecureX 控制面板菜单栏上，单击**自定义 (Customize)** 以打开**自定义控制面板 (Customize Dashboards)** 表单。

图 *14:* 自定义控制面板



步骤 2 在**我的控制面板 (My Dashboards)** 列表中，选择要与组织内其他用户共享的控制面板。

步骤 3 单击右侧面板中的**共享 (Share)**。

控制面板将添加到**共享控制面板 (Shared Dashboards)** 列表。

步骤 4 完成共享控制面板后，单击**保存 (Save)**。

要显示每个控制面板的所选磁贴，请在**共享控制面板 (Shared Dashboards)** 列表中选择控制面板。

激活协调

在思科 SecureX 中提供工作流程自动化之前，组织管理员必须为其组织激活 SecureX 协调。一旦激活后，组织中的所有用户便都可以访问**协调 (Orchestration)** 选项卡和工作流程自动化功能。

步骤 1 在 SecureX 中，单击菜单栏上的**协调 (Orchestration)** 选项卡。

步骤 2 在 **SecureX 协调 (SecureX Orchestration)** 页面上，单击**请求访问 (Request Access)**。

系统将显示一条消息，通知您已收到您的请求，而您将在获得访问权限时收到通知邮件。

注释　如果您是 SecureX 演示中未激活的用户，则必须单击**开始 (Get Started)** 以通过启用集成模块来激活 SecureX 帐户，然后才能激活协调。

步骤 3 单击**返回 SecureX 控制面板 (Back to SecureX Dashboard)** 以返回控制面板。

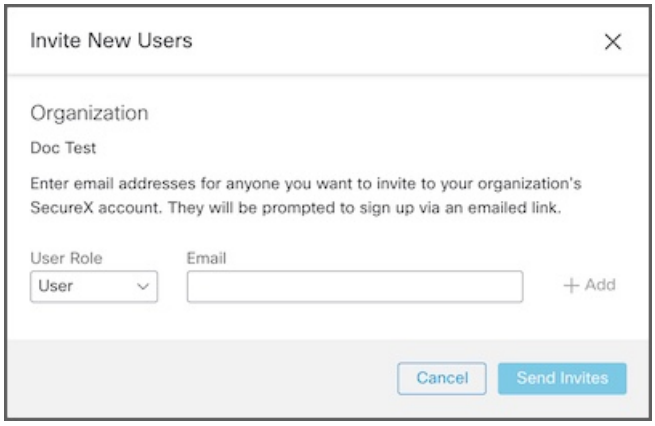
邀请用户

如果您以管理员用户身份使用 SecureX 帐户登录，则可以邀请用户通过思科 SecureX 加入您的组织。使用**管理 (Administration)** 页面上的**用户 (Users)** 选项卡来管理思科 SecureX 组织中的用户，并邀请用户加入您的 SecureX 组织。

步骤 1 在 SecureX 中，单击**管理 (Administration)** 选项卡，然后在导航窗格中选择**用户 (Users)**。

步骤 2 单击**邀请用户 (Invite Users)**。

图 *15:* 邀请新用户



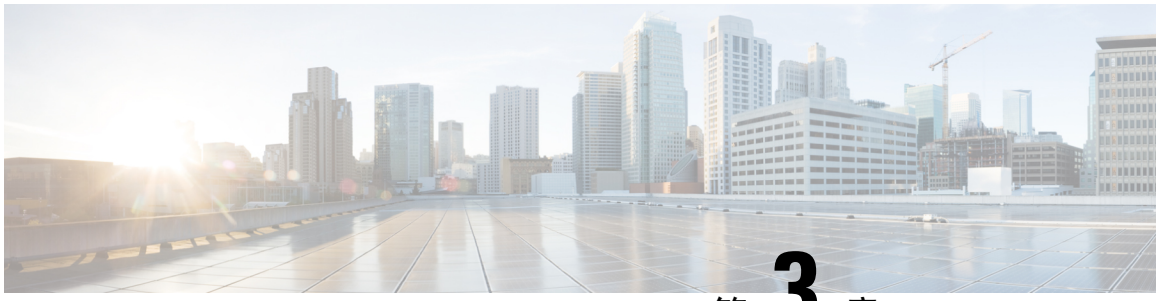
步骤 3 填写**邀请新用户 (Invite New Users)** 表单：

a) 从**用户角色 (User Role)** 下拉列表中选择**用户 (User)** 或**管理员 (Admin)**。

b) 输入要邀请加入您的组织的 SecureX 帐户的人员的**邮件**地址。
c) 单击**添加 (Add)** 将用户添加到邀请中。重复此过程，向邀请中添加其他用户。

步骤 4 将用户添加到邀请列表后，单击**发送邀请 (Send Invites)**。

用户将收到一封邮件，通知他们已被邀请加入您的思科 SecureX 组织帐户。他们应按照邮件中的说明登录思科 SecureX。



第 3 章

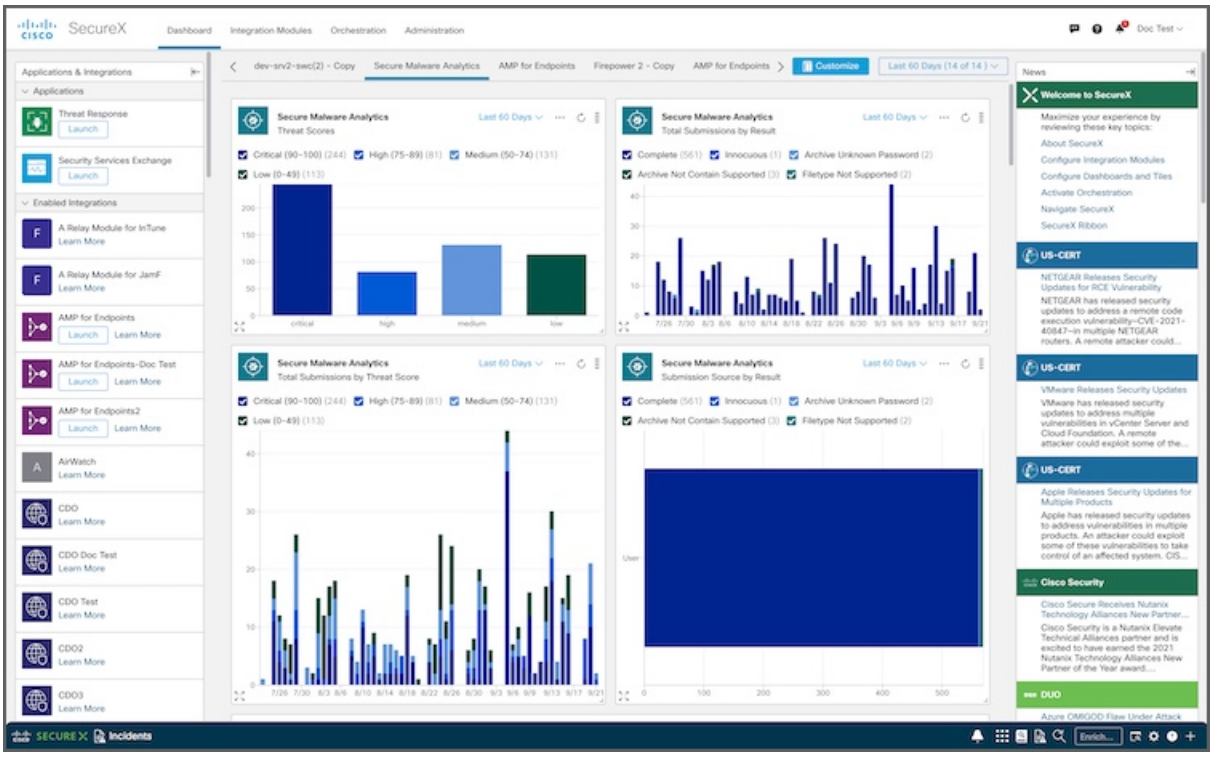
思科 SecureX 控制面板

本章介绍了如何在思科 SecureX 中使用控制面板，包括：

控制面板

思科 SecureX 控制面板可在整个组织中提供可视性和汇聚、可执行的情报。在该页面中，您可以查看和启动集成、查看其他可用的集成（并访问免费试用，如可用）、查看整个安全环境中的指标和数据、采取响应操作，以及查看对您的网络安全重要的相关新闻报道。

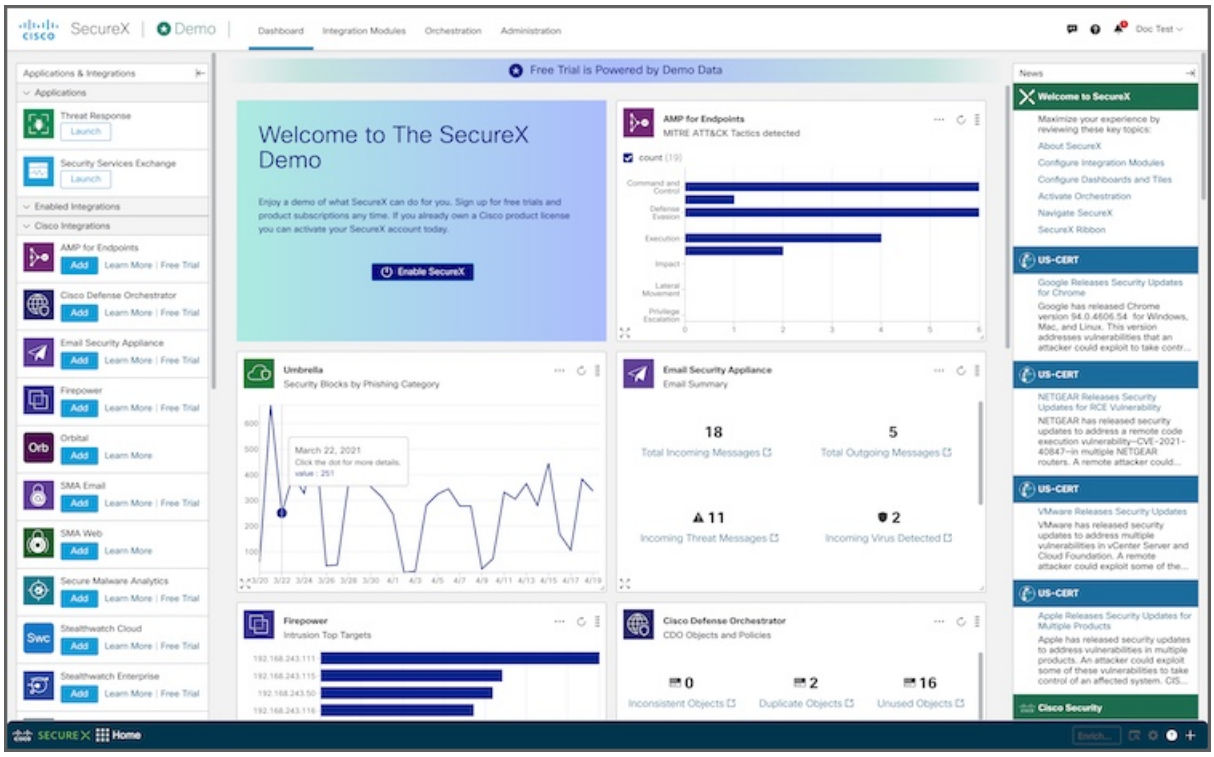
图 *16: SecureX* 控制面板



演示控制面板

思科 SecureX 演示控制面板允许您在激活 SecureX 帐户之前查看 SecureX 的功能和优势。在该页面中，您可以启动应用、添加可用的思科集成、访问免费试用（如可用）、查看样本指标和数据，以及查看对您的网络安全重要的相关新闻报道。

图 *17: SecureX* 演示控制面板



应和用集成

应用和集成 (Applications & Integrations) 面板位于控制面板的左侧，可用于查看思科 SecureX 应用和集成产品以及可用于集成的产品。您可以折叠或展开此面板，以便让控制面板上其他面板显示得更清楚。

- **应用 (Applications)** - 默认启动 SecureX 中可用的应用。这些应用包括用于威胁检测、调查和补救的威胁响应；以及用于管理与 SecureX 集成的设备的安全服务交换。
- **已启用集成 (Enabled Integrations)** - 查看已在 SecureX 中配置和集成的产品。
  - 单击**启动 (Launch)** 按钮，以便在新的浏览器窗口中快速打开产品。
  - 单击**链接 (Links)** 以访问有关产品的更多信息。
- **思科集成 (Cisco Integrations)** - 查看可用于集成的思科安全产品，添加用于集成的思科模块；如果可用，访问免费试用版。
  - 单击**添加 (Add)** 按钮以配置要集成的思科产品模块。有关详细信息，请参阅添加集成模块。

注释 只有管理员用户可以添加集成模块。如果您以非管理员用户身份登录，则不会出现**添加 (Add)** 按钮。

- 单击**了解更多 (Learn More)** 链接，查看思科产品的说明，以及在与 SecureX 集成后可以执行的操作。有关详细信息，请参阅 SecureX 联机帮助中的**集成模块**主题。
- 单击**免费试用 (Free Trial)** 链接（如有）以便试用思科产品。

- **第三方集成 (Third-Party Integrations)** - 查看可用于集成的第三方安全产品，添加用于集成的第三方模块；如果可用，访问免费试用版。
  - 单击**添加 (Add)** 按钮以配置用于集成的第三方产品模块。有关详细信息，请参阅添加集成模块。

  注释 只有管理员用户可以添加集成模块。如果您以非管理员用户身份登录，则不会出现**添加 (Add)** 按钮。

  - 单击**了解更多 (Learn More)** 链接，查看第三方产品的说明，以及在与 SecureX 集成后可以执行的操作。有关详细信息，请参阅 SecureX 联机帮助中的**集成模块**主题。
  - 单击**免费试用 (Free Trial)** 链接（如有）以便试用第三方产品。

控制面板和磁贴面板

在 SecureX 控制面板上，中心面板中配置的控制面板包含**磁贴**，这些磁贴提供来自集成模块的指标和数据，以便让整个安全环境一目了然并加速威胁响应。SecureX 随附了一个默认控制面板，您必须在其上添加要查看的磁贴。您最多可以添加 20 个控制面板以自定义视图。

使用**自定义 (Customize)** 按钮可添加、修改和删除控制面板及其上显示的磁贴，共享控制面板，以及重新排列控制面板的显示方式。

您还可以单击**磁贴 (Tile)** 菜单（磁贴右上角的省略号），然后从下拉菜单中选择**删除磁贴 (Remove Tile)**，将其从当前选定的控制面板中删除。有关详细信息，请参阅配置控制面板和配置控制面板磁贴。

在 SecureX 演示控制面板上，控制面板中间的磁贴会显示样本指标和数据。您可以单击示例磁贴中的任何数据，了解有关该产品的更多信息，包括用于启用集成模块的链接和用于访问免费试用版的链接（如果可用）。

全屏控制面板

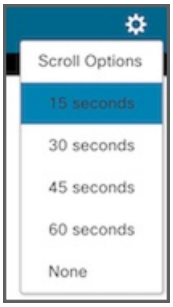
注释 Apple Safari 浏览器不支持此功能。

要将控制面板最大化至全屏，请单击控制面板菜单栏右上角的  （**最大化**）图标；单击右上角的  （**最小化**）图标，或者按键盘上的 **Esc** 键将控制面板折叠为普通视图。

指定滚动选项

在全屏控制面板上，单击 （**设置**）图标并选择在全屏模式下保持不动时控制面板自动上下滚动的速度。如果选择**无 (None)** 选项，则控制面板不会自动上下滚动。

图 *18:* 滚动选项

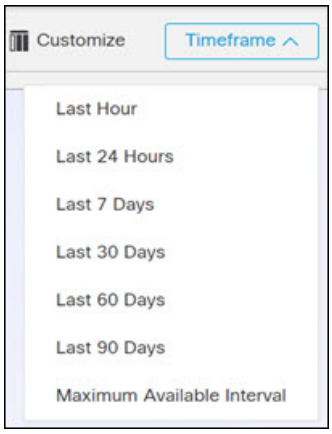


指定磁贴时间范围

在 SecureX 控制面板上，可以为磁贴中显示的数据指定全局时间范围，也可以在每个磁贴上指定时间范围。

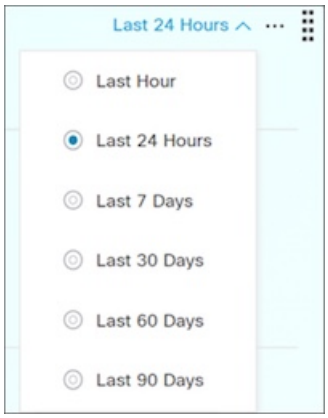
- 单击菜单栏中的**时间范围 (Timeframe)**，然后为磁贴中显示的数据选择全局时间范围（例如，过去 24 小时）。如果选择**最大可用间隔 (Maximum Available Interval)** 选项，则磁贴将显示最长可用时间范围的数据。

  图 *19:* 全局时间范围选择器

- 单击特定磁贴中的**时间范围 (Timeframe)** 链接，为特定磁贴中显示的数据选择时间范围。

图 *20:* 磁贴时间范围选择器



调整磁贴大小

您可以调整磁贴的大小并将其移到控制面板上的任何位置。您还可以让磁贴最大化，以便让细节更清晰。

注释 在 SecureX 演示中，当您刷新页面时，磁贴将恢复为默认大小和位置。

- 要调整磁贴大小，请单击右下角的 （**调整大小**）图标并将其拖动至所需的大小。
- 要将磁贴最大化至全屏，请单击左下角的 （**最大化**）图标；单击右上角或右下角的 （**最小化**）图标将其折叠为正常大小。

刷新磁贴

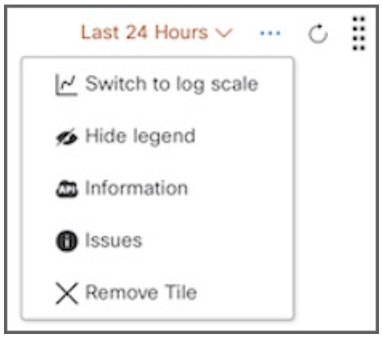
单击磁贴右上角的 （**刷新**）图标以刷新磁贴数据。

磁贴菜单

单击磁贴右上角的**磁贴 (Tile)** 菜单，以便在对数标度和线性标度之间切换，显示或隐藏图例，查看信息和问题，以及删除磁贴。

注释 在 SecureX 演示中，应用到磁贴的任何更改都将在刷新页面时恢复为默认设置。

图 *21:* 磁贴设置



- **切换到对数标度/线性标度 (Switch to log scale/linear scale)** - 选择此选项可在磁贴中以对数标度或线性标度显示数据之间切换（仅适用于图表磁贴）。
- **隐藏/显示图例 (Hide/Show legend)** - 选择此选项可在显示图表图例或隐藏图块中的图例之间切换（仅适用于图表图块）。
- **信息 (Information)** - 选择此选项可打开对话框并查看更多详细信息，例如历史记录和 API 信息。在对话框中单击**复制调试信息 (Copy Debug Information)**，以便将下列信息复制到剪贴板：主机、用户、组织、模块实例、磁贴定义和 API 响应。在提交反馈或向思科支持部门提交支持案例时，复制的调试信息将非常有用。
- **问题 (Issues)** - 选择此选项可打开磁贴问题模式以查看所检测到的问题。
- **删除磁贴 (Remove Tile)** - 选择此选项可将磁贴从当前选定的控制面板中删除。

注释 有关特定磁贴的信息，请参阅磁贴说明列表或相关产品文档。产品文档的链接在思科 SecureX 帮助主题的**集成模块**主题中提供。

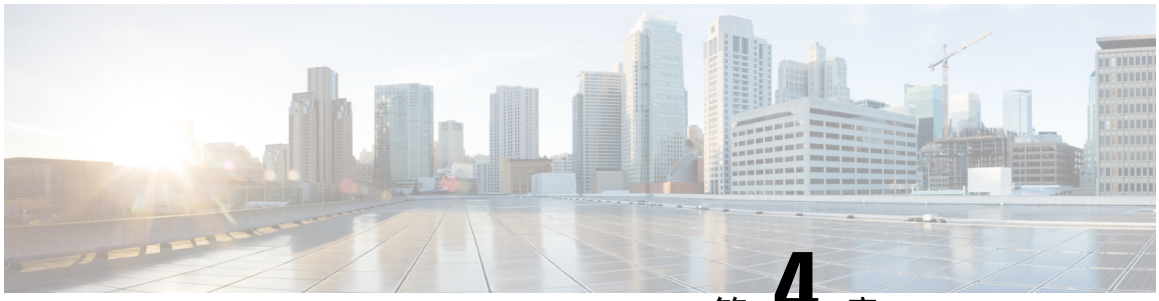
启动应用

单击控制面板磁贴上的模块图标、模块名称或磁贴名称，以便启动应用。

控制面板新闻面板

新闻 (News) 面板位于控制面板的右侧，提供与您相关的公司范围公告/行业新闻和安全博客帖子的更新。信息来自思科 Talos 博客 (https://blog.talosintelligence.com)、美国计算机应急准备小组 (https://us-cert.gov)、Cisco Security Blog (https://feeds.feedburner.com/CiscoBlogSecurity)、Cisco Learning Network (https://learningnetwork.cisco.com) 以及 Cisco Duo Blog (https://duo.com/blog)。

您可以折叠或展开此面板，以便让控制面板上其他面板显示得更清楚。



第 4 章

思科 SecureX 功能区

本章概述了思科 SecureX 中的功能区，包括以下内容：

色带

思科 SecureX 是集中式控制台和分布式功能集，可统一可视性，实现自动化，加速事件响应工作流程并改善威胁搜索。这些分布式功能以 SecureX 功能区中的应用程序（应用）和工具的形式呈现。

功能区位于页面下方，当您在控制面板和环境中的其他安全产品之间移动时，此功能仍然存在。

图 *22: SecureX* 功能区 - 已折叠

使用功能区访问案例集、应用、设置、搜索用于充实的可观察对象、查看通知和查看事件。

注释 如果您是 SecureX 演示中未激活的用户，则必须单击**配置模块 (Configure a Module)** 以通过启用集成模块来激活 SecureX 帐户，然后才能访问功能区。

功能区图标和元素

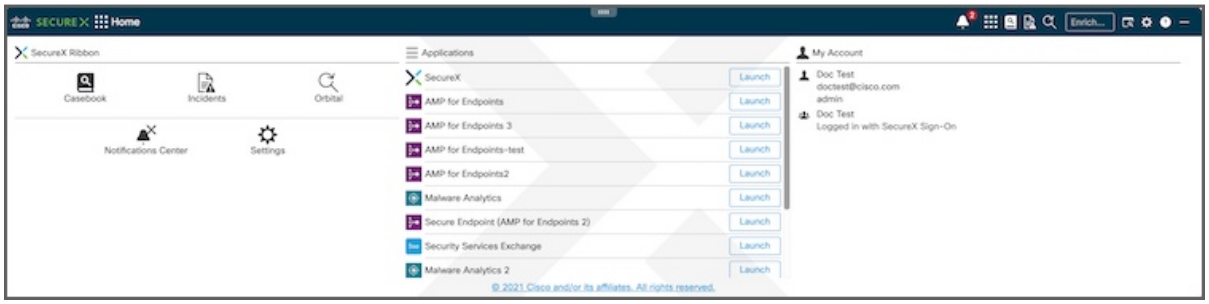
思科 SecureX 功能区上会显示以下图标和元素。

图 *23:* 功能区图标和元素

展开/折叠功能区

单击 +/- 图标以展开或折叠功能区。当功能区展开时，您可以在面板的整个顶面的任意位置上下拖动容器或在任意位置上下拖动双箭头，从而调整面板的高度。

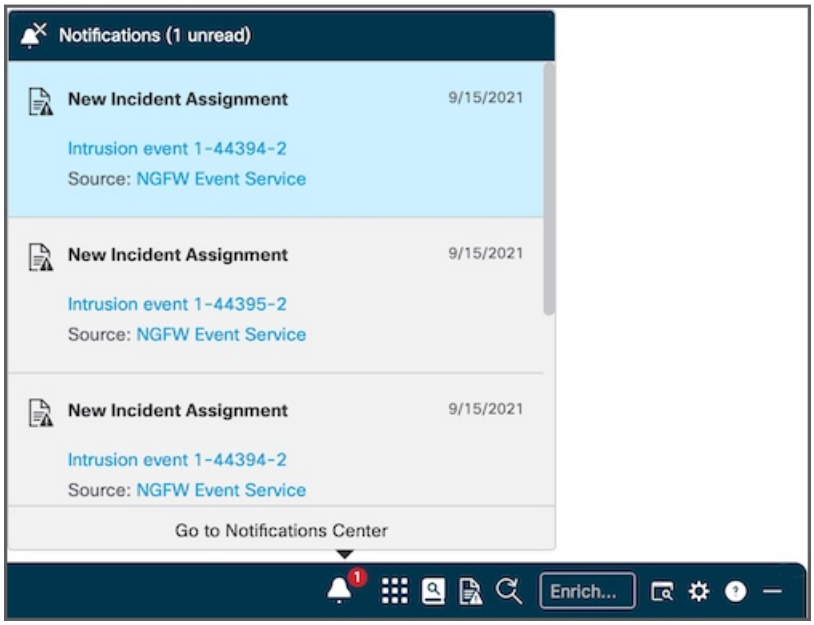
图 *24: SecureX* 功能区 - 已展开



通知

（**通知**）图标会显示未读通知的数量。单击图标以显示其他用户在**通知 (Notifications)** 弹出窗口中分配给您的事件通知。单击图标后，未读通知会被标为已读，而未读通知的数量会重置。

图 *25:* 通知



查看通知详细信息

每个通知都包括通知类型、通知日期、可在**事件应用**中打开事件的事件标题链接，以及打开事件源的源链接（如果适用）。有关事件应用的详细信息，请参阅 SecureX 在线帮助中的**事件应用**主题。

删除通知

要删除通知，请将鼠标悬停在通知上方，然后单击**清除 (Clear)** 图标。这样也会将通知从**通知中心 (Notifications Center)** 删除。

访问通知中心

单击**转到通知中心 (Go to Notifications Center)** 链接以打开**通知中心 (Notifications Center)** 页面并管理通知。有关详细信息，请参阅 SecureX 联机帮助中的**通知中心**主题。

主页

使用功能区**主页 (Home)** 页面打开功能区应用、通知中心和功能区设置，启动集成应用，并查看帐户配置文件，其中包括用于登录的用户名、帐户邮件地址、角色、组织和 IDP。

在移至功能区中的其他页面时，单击**主页**图标可返回到功能区**主页 (Home)** 页面。

案例集应用

单击**案例手册应用**图标以打开案例手册应用并保存有关威胁分析的信息。您还可以将鼠标悬停在图标上，以查看当前案例的相关详细信息。有关详细信息，请参阅 SecureX 联机帮助中的**案例集应用**主题。

事件应用

单击**事件应用**图标以打开事件应用并查看集成产品中的事件。您还可以将鼠标悬停在图标上，以查看分配给当前案例的事件的详细信息。有关详细信息，请参阅 SecureX 联机帮助中的**事件应用**主题。

Orbital 应用

单击 **Orbital 应用**图标以打开 Orbital 应用并执行其他查询。有关详细信息，请参阅 SecureX 联机帮助中的 **Orbital 应用**主题。

增强搜索框

在**充实 (Enrichment)** 搜索框中输入搜索条件，然后按 **Enter** 开始提取可观察对象。然后，您可以单击**添加到案例 (Add to Case)** 或**在威胁响应中调查 (Investigate in Threat Response)**。有关详细信息，请参阅 SecureX 联机帮助中的**搜索可观察对象**主题。

查找可观察对象

单击**查找可观察对象 (Find Observables)** 图标，以便在当前网页中搜索恶意文件散列、可疑域和其他网络可观察对象。然后，您可以单击**将可观察对象添加到案例 (Add Observables to Case)** 或**在威胁响应中调查 (Investigate in Threat Response)**。有关详细信息，请参阅 SecureX 联机帮助。

设置

单击**设置**图标以打开 SecureX 功能区和案例集设置。

- **SecureX 功能区设置**：
  - **主题 (Theme)** - 单击选项以指定功能区的背景颜色：
    - **浅色 (Light)** - 显示浅色背景（默认）。

- **黄昏 (Dusk)** - 显示深色背景。
- **自动 (Automatic)** - 显示自动匹配集成产品主题的背景。

  当选择**自动 (Automatic)** 主题时，您还可以选择将其自动设置为**反转产品主题 (Inverse of the product theme)** 或 **匹配产品主题 (Match the product theme)**。

- **条形图格式 (Bar Format)** - 单击**完整 (Full)** 或**缩小 (Reduced)** 以设置功能区折叠时的大小。根据集成情况，此功能可能会被禁用。
- **存储 (Storage)** - 单击**清除存储 (Clear Storage)** 按钮，以便清除功能区和所有功能区应用的已存储设置和状态。这样不会删除任何数据对象，例如案例和事件。
- **版本 (Version)** - 功能区的发行版本号。
- **重置 (Reset)** - 单击**重置为默认值 (Reset to Defaults)** 按钮，以便将 SecureX 功能区的所有设置都重置为默认值。

- **案例集设置：**
  - **自动打开 (Auto Open)** - 选中此复选框可自动打开案例集中新创建的案例。此复选框会默认选中。如果您不希望在案例集中默认打开新案例，请取消选中此复选框。

    如果要在创建新案例时始终切换到案例集应用，请选中此复选框。此复选框会默认选中。如果不想在创建新案例时切换到案例集应用，请取消选中此复选框。
  - **可观察对象排序 (Observable Sort)** - 单击此选项可对案例中的可观察对象列表进行排序：
    - **最新 (Newest)** - 按可观察对象被添加到案例中的顺序来显示可观察对象的列表（从最新到最旧）。
    - **最旧 (Oldest)** - 按可观察对象被添加到案例中的顺序来显示可观察对象的列表（从最旧到最新）。
    - **字母顺序 (Alphabetical)** - 按字母顺序显示可观察对象列表（从 A 到 Z）。
  - **重置 (Reset)** - 单击**重置为默认值 (Reset to Defaults)** 按钮可将案例集应用的所有设置重置为默认值。

- **通知中心设置：**
  - **请勿打扰 (Do Not Disturb)** - 单击可启用或禁用传入通知以及**通知**图标上显示的未读通知数量。切换开关默认为禁用（关闭）；如要启用此选项，请通过切换为开来启用**请勿打扰 (Do Not Disturb)**。
  - **重置 (Reset)** - 单击**重置为默认值 (Reset to Defaults)** 按钮以将通知中心的设置重置为默认值。

帮助

单击 SecureX 功能区上的**帮助**图标，以便打开 SecureX 在线帮助中的功能区主题，了解有关功能和应用的更多信息。