思科安全集成 v1 - 即时演示

最后更新日期：2017 年 11 月 14 日

关于本演示

本预配置演示指南包括以下内容：

- 要求
- 关于此解决方案
- 开始演示
- 场景 1：思科的有效安全集成

要求

下表列出了本预配置演示的要求。

表 1. 要求

必需	可选
• 笔记本电脑	• 无

关于此解决方案

思科的安全产品开发始于一个纯粹从实用角度出发的问题：我们如何构建最有效的安全架构？

我们认为，当安全堆叠的各个部分能够无缝地协同工作时，才能提供有效的安全保护。

当今的许多攻击响应都涉及依赖于人类活动的复杂工作流程。对漏洞做出的响应可能需要数月才能付诸实施。为什么？因为我们担心我们的响应可能比攻击更具破坏性。设想一下，如果您在一台远程笔记本电脑上发现恶意软件，系统可以自动实时在您的所有网络和笔记本电脑上实施响应措施，发现一次，永绝后患，情况会怎样？

思科可以将典型的客户检测时间从数月缩短到数小时。然后，做出近乎实时的系统化响应。现在，把这个想法扩展到其他领域。想像这样一个地方：您可以查看来自网络、恶意软件、Web 和邮件的所有遥感勘测数据。您可以在这里毫不费力地透视数据，通过分析攻击者自己的 IT 基础设施了解有关攻击的更多信息。您的分析师可以进入一个高效的流程：在一个位置使用他们掌握的所有情报来研究攻击，并随着威胁形势的演变迅速做出响应。简而言之，我们正在积累这些遥感勘测数据，并采用能够让您简化工作流程并自动做出响应的方式将这些数据整合到一起。

开始演示

演示前的准备

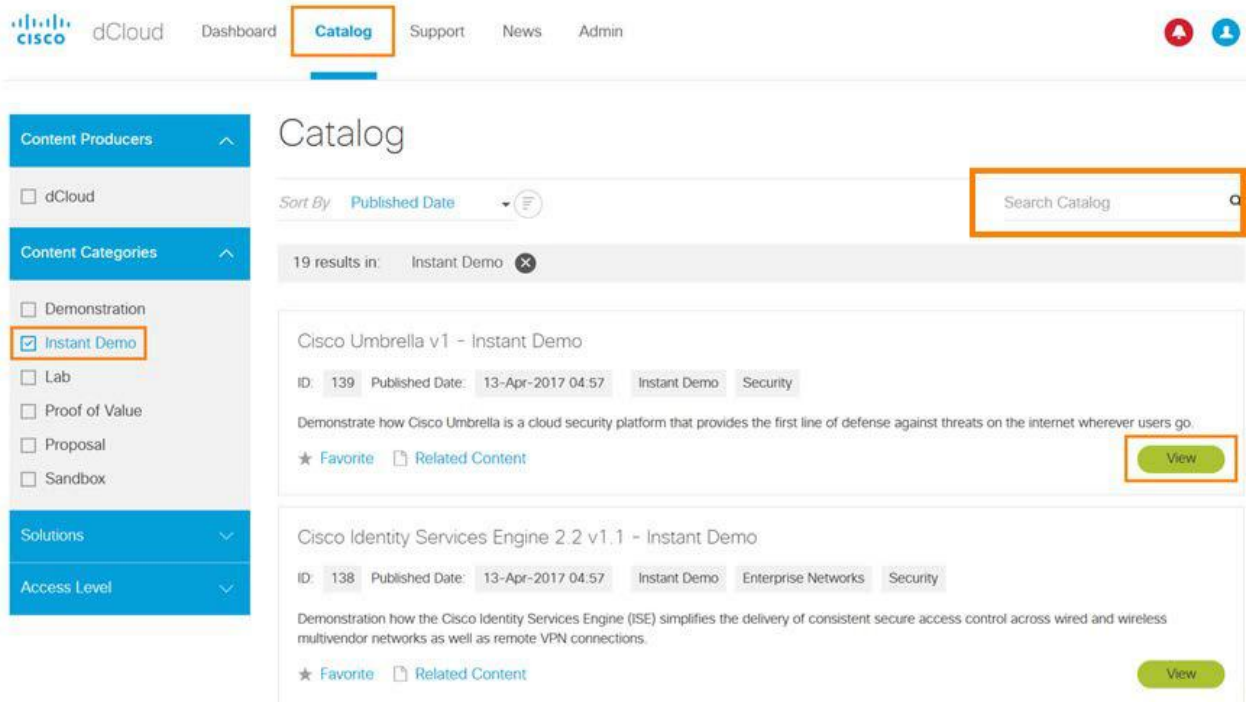
思科 dCloud 强烈建议您事先使用活动会话执行本文档中的任务，然后再给现场观众演示。这样您将熟悉文档和内容的结构。

遵循本指南后，有必要安排一个新会话，以将环境重置为其原始配置。

细致的准备对于一场成功的演示至关重要。

按照步骤安排内容会话并配置演示环境。

1. 点击**目录**并从侧栏中选择**即时演示**。这将列出所有 dCloud 即时演示。
2. 在目录中**搜索或滚动**查找思科安全集成。点击相应的**查看**按钮。



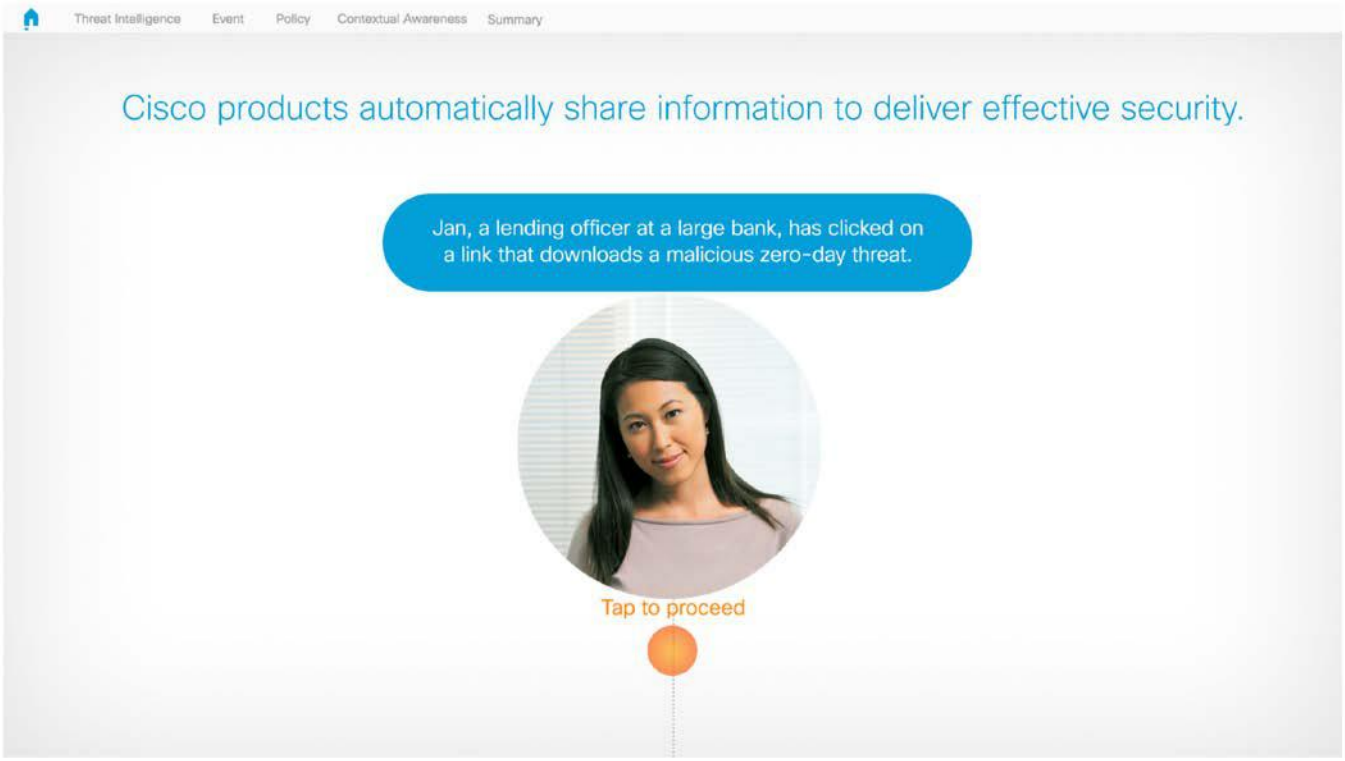
3. 系统会将您自动定向至思科安全集成演示。

场景 1： 思科的有效安全集成

步骤

在接下来的几分钟内，您将通过一个示例了解思科的安全解决方案如何在本地协同工作，从而提高安全性并缩短检测时间。

认识 Jan。



点击橙色的点开始演示。

Jan 是旧金山银行的一名新员工。她收到一封邮件，看起来像是她的经理发来的，包含她的新薪酬计划。她点击了链接，但文件无法打开。由于忙着应付新工作，她关闭了窗口，继续完成当天的工作。

尽管我们不愿意承认，但这种情况实在是太普遍了，并非有意造成，而是因为太忙，又将注意力集中到下一项就要截止的工作上，因而错过了一些细节。

但是 Jan 很不幸，她点击的链接指向一个通过鱼叉式网络钓鱼活动投放的零日恶意软件攻击。如果使用的是旧式安全产品，此攻击就会得逞，因为每个安全解决方案只检查自己这一部分受到的攻击，而不了解其他部分的情况，并且只在威胁通过控制点时检查一次。

威胁情报

点击橙色的点继续演示。

我们认为，当各个部分能够无缝地协同工作时，才能提供有效的安全保护。思科通过安全架构共享事件、策略、威胁情报和情景感知，因此我们可以针对高级威胁提供更强大的检测功能和更快的补救速度。

点击橙色的点继续演示。

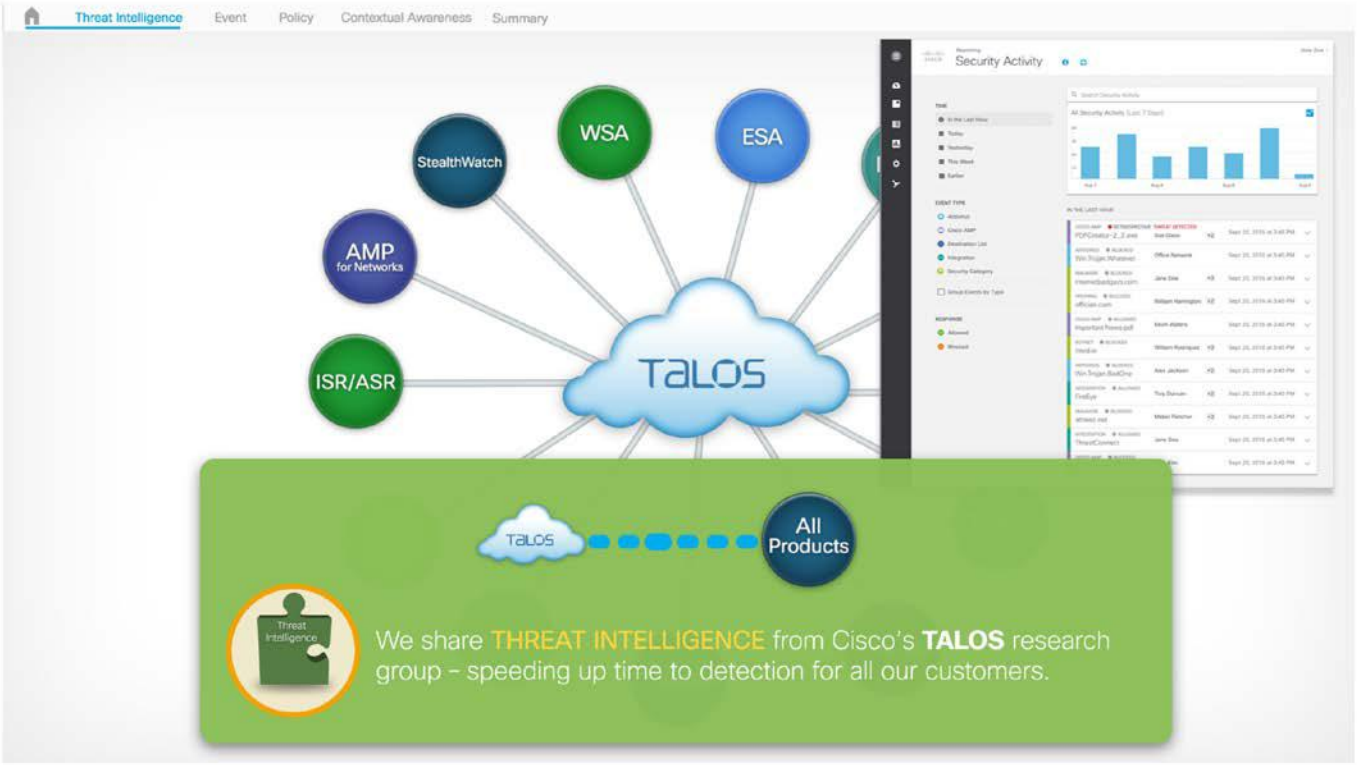
当 Jan 下载文件后，文件性质最初是未知。AMP 自动将文件发送到 Threatgrid，并在我们发现该文件是恶意软件时触发追溯性警报。这样，面向终端的 AMP 就可以清理感染，而下一代防火墙 (NGFW) 则可以阻止新的攻击。

点击橙色的点继续演示。

每个威胁内部有大量信息可供我们与整个思科安全架构共享，从而使整个网络都能通过学习变得更智能。这是我们共享的第一种信息 - 威胁情报。

点击橙色的点继续演示。

例如，Threatgrid 可以为思科 Umbrella 提供威胁发出的 DNS 信息，这就是我们共享的一种数据类型。然后，Umbrella 将阻止与命令和控制服务器（也称为 C2 或 C&C）的进一步通信或新的下载尝试，进一步缩小受攻击面。只有思科才能实现这些信息的共享，因为思科具有开放性，支持可简化安全运营的自动化功能。

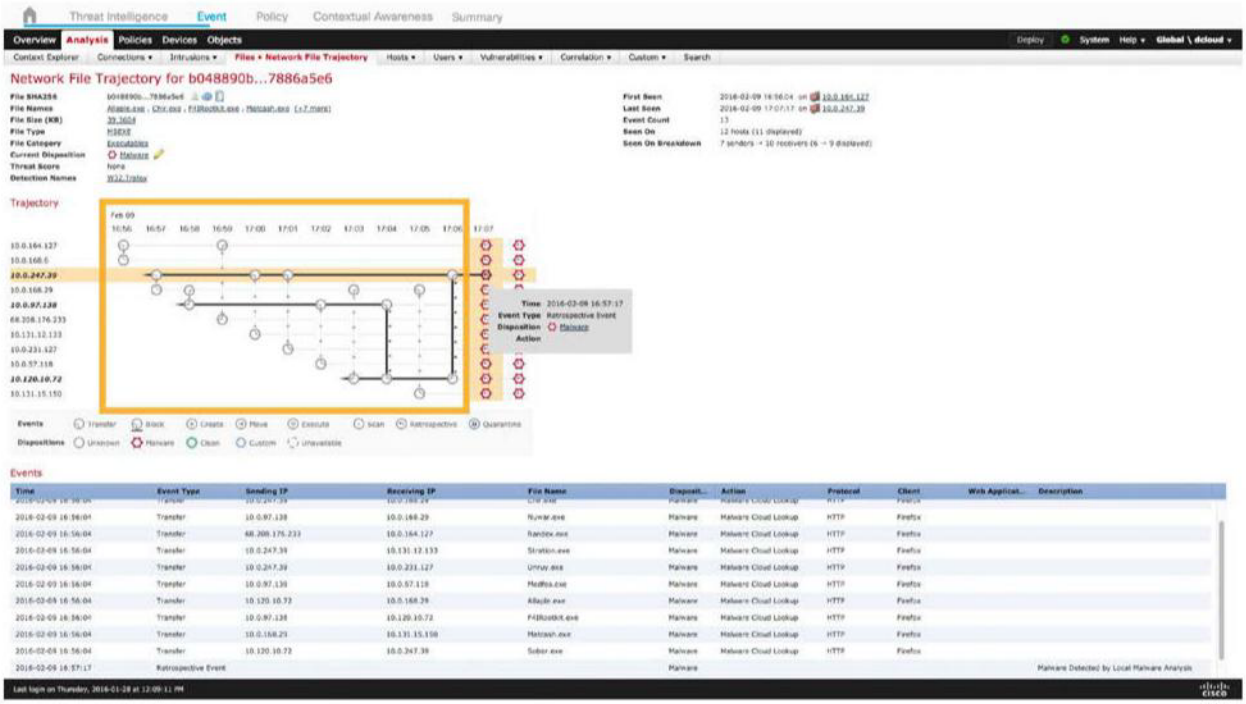


事件

点击橙色的点继续演示。

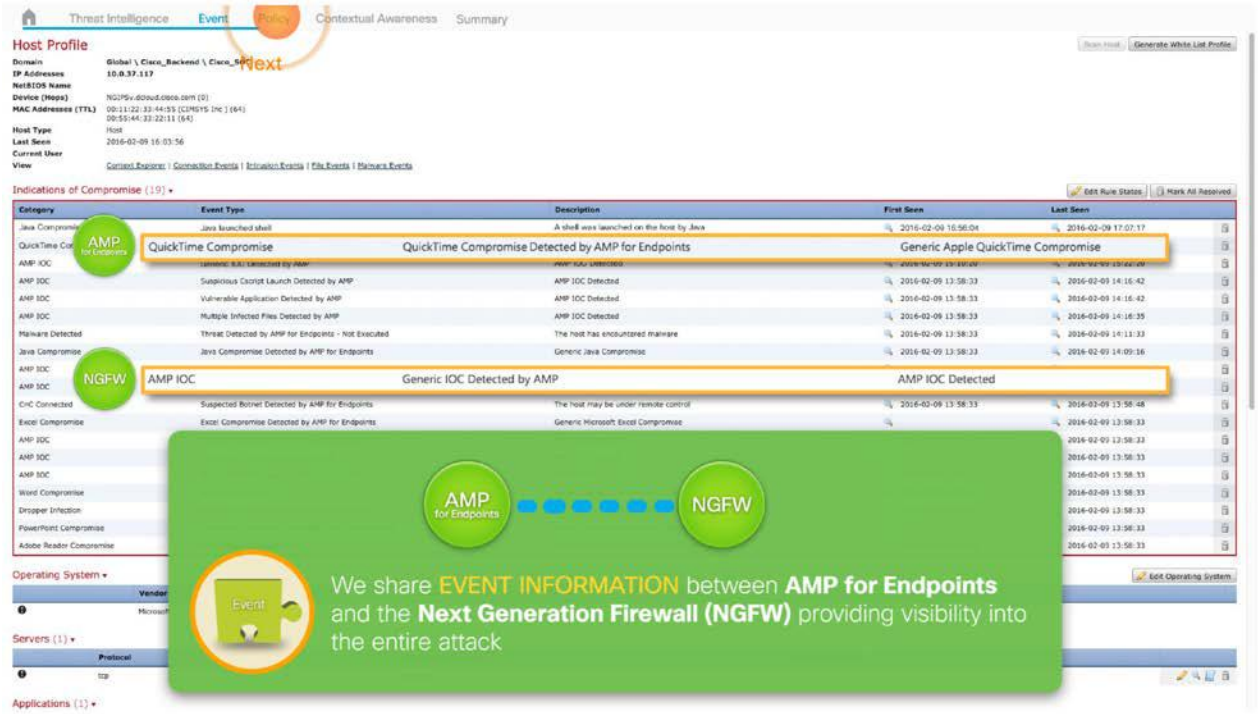
让我们看看下一代防火墙发生了什么情况。从此处可以看出，当 Jan 首次下载该文件时，文件被列为未知文件，因为它是零日攻击。随后，文件被自动发送到 AMP Threatgrid 进行分析。Threatgrid 发现该文件是恶意软件，并在防火墙和面向终端的 AMP 上同时更改了文件在 AMP 中的性质，这触发了追溯性警报。

由于 AMP 可以跟踪一段时间内的文件，因此我们能够看到文件在网络中的移动轨迹。



点击橙色的点继续演示。

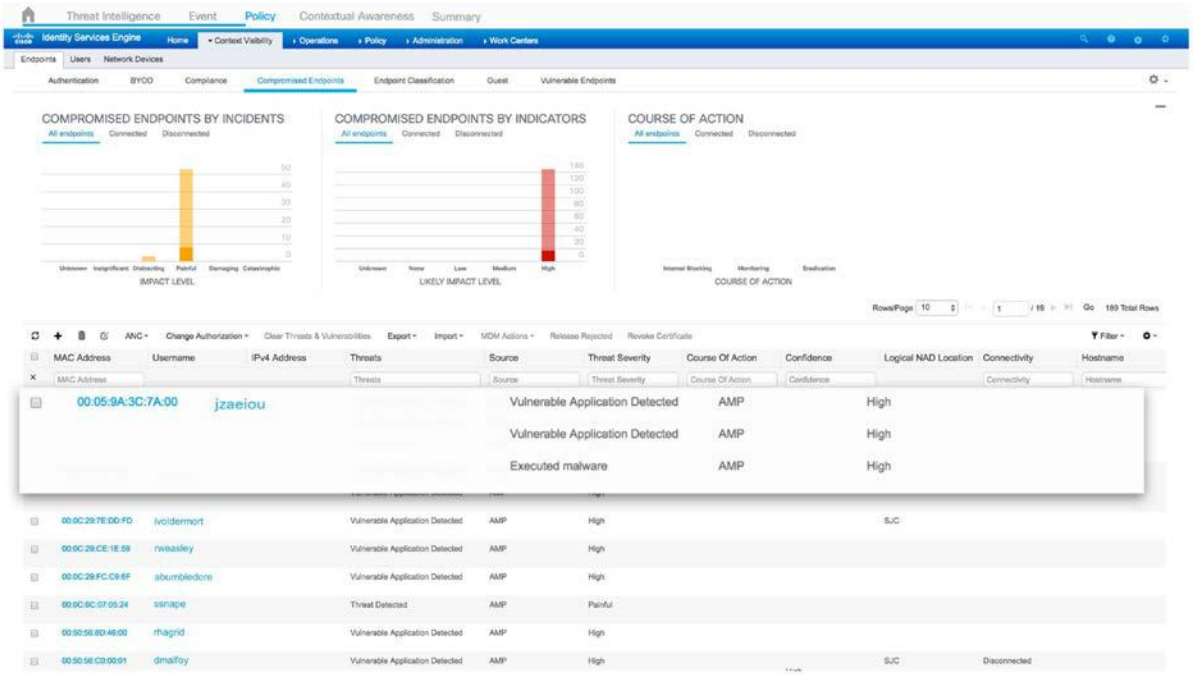
我们共享的第二种数据是事件信息。AMP 是一个可以跨网络和终端使用的平台。在此情况下，我们在下一代防火墙 (NGFW) 与面向终端的 AMP 之间共享事件数据，从而提供对网络内外系统上的整体攻击情况的可视性。只有思科才能实现这些信息的共享，因为思科具有开放性，支持可简化安全运营的自动化功能。



策略

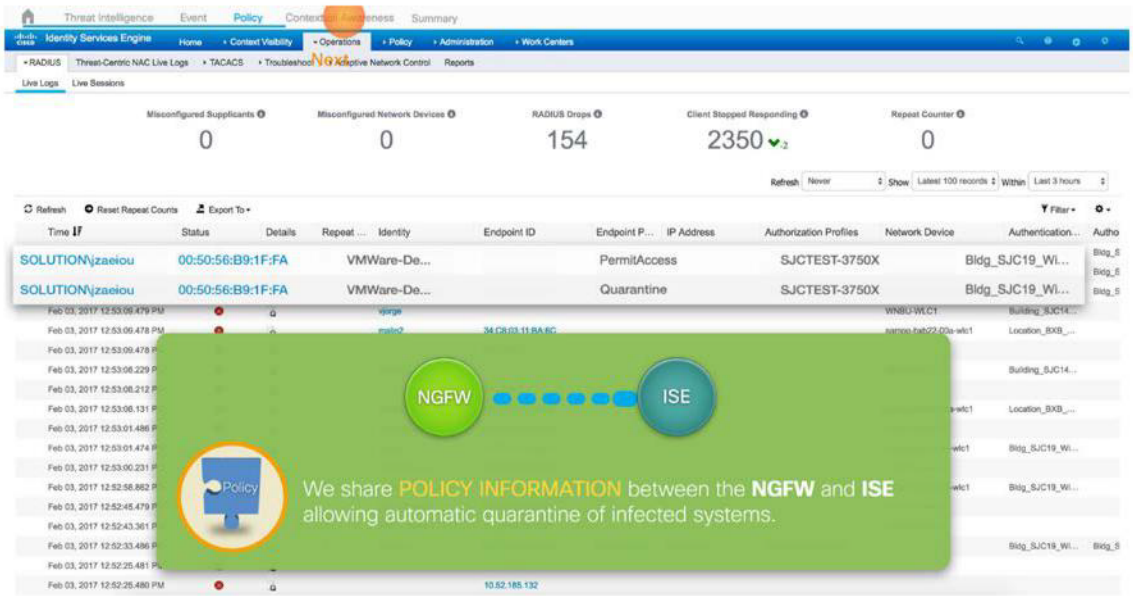
点击橙色的点继续演示。

我们可以进一步使用思科的身份服务引擎 (ISE) 来控制网络访问，自动执行对威胁的响应。



点击橙色的点继续演示。

我们共享的第三种信息是策略信息。正如此处所示，NGFW 与 ISE 共享策略信息，让我们得以自动隔离系统。这就是我前面提到的系统化响应。我们实现了工作流程的自动化，因此我们可以近乎实时地阻止威胁，从而遏制感染并最大限度地减少损害。只有思科才能实现这些信息的共享，因为思科具有开放性，支持可简化安全运营的自动化功能。

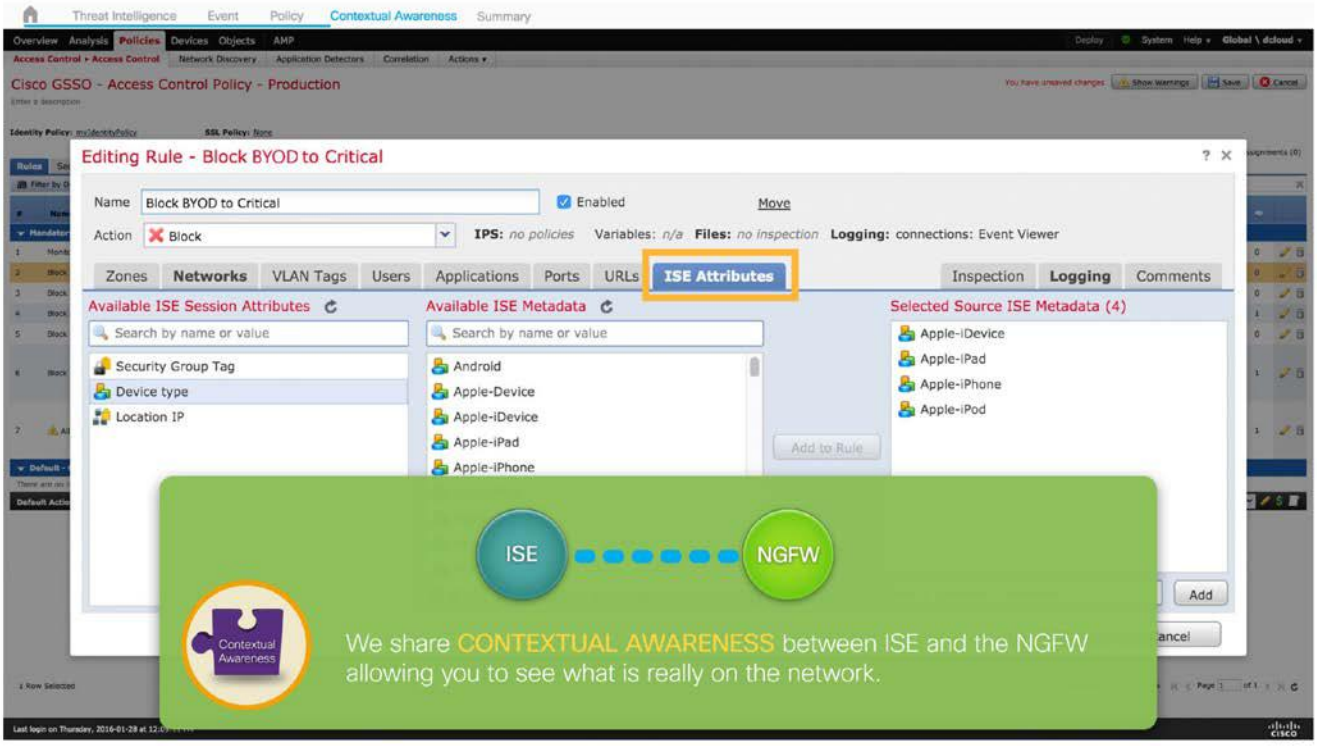


注意：虽然此演示显示的是对系统进行完全隔离，但也许其他补救方案更切合您的客户的实际情况。

情景感知

点击橙色的点继续演示。

再来看 NGFW，您可以看到 ISE 与 NGFW 之间的通信是如何双向工作的。NGFW 可以共享策略信息以便 ISE 采取行动，而 ISE 也可以与防火墙共享对网络中真正存在的设备的情景感知。情景感知是我们共享的第四种信息，管理员可以根据它做出更明智的决策。只有思科才能实现这些信息的共享，因为思科具有开放性，支持可简化安全运营的自动化功能。



总结

点击橙色的点继续演示。

综上所述，思科拥有唯一能够提供更有效的安全功能并缩短检测时间的集成产品组合。我们之所以能够做到这一点，是因为我们的产品具有开放性并且专为在本地协同工作而设计，旨在自动做出安全响应并简化工作流程，从而创建更有效的安全架构。

点击橙色的点继续演示。

您应该记得我们开始提出的问题：“我们如何构建最有效的安全架构？”

在过去的几分钟内，您看到了思科的安全解决方案如何通过互相通信提高安全效力并缩短检测时间。

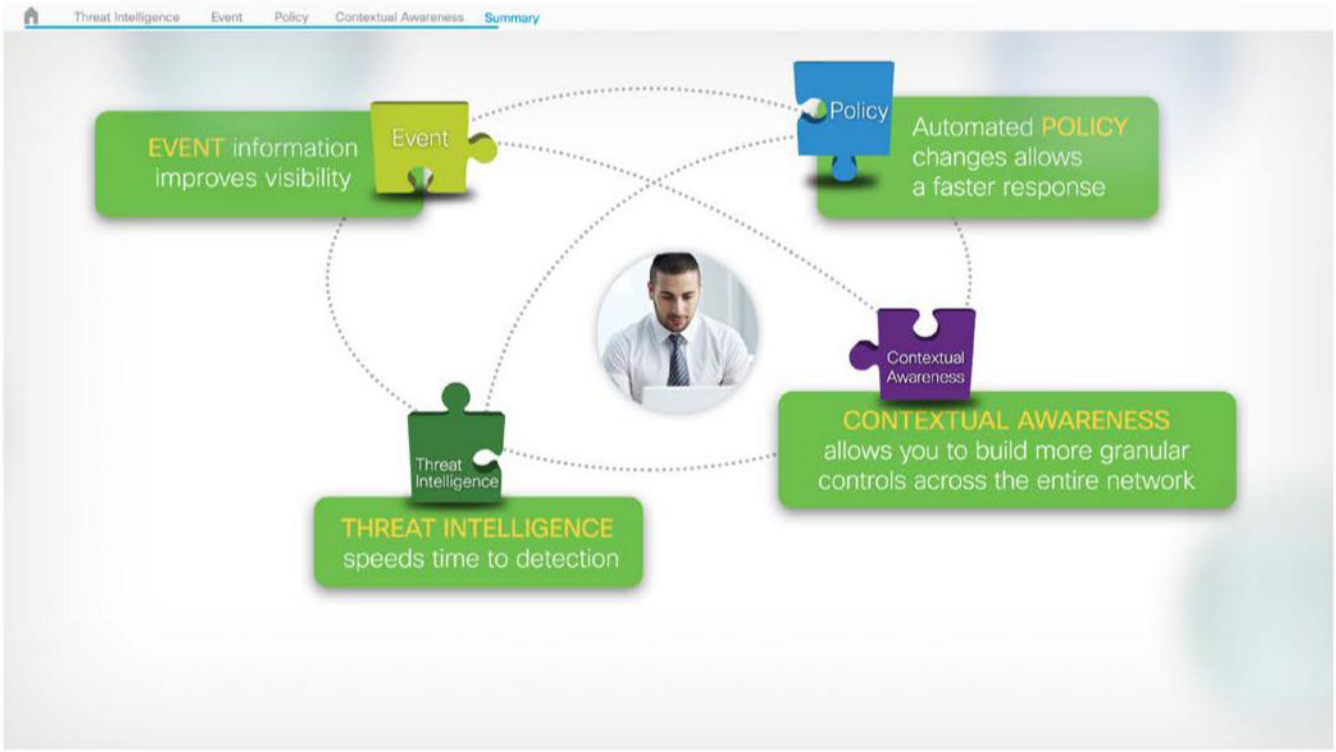
这个小例子说明了我们如何提供旨在共享四种信息的服务，以便简化安全运营并自动做出响应，从而跨终端或网络和云缩短检测时间。

第一种信息是事件信息，它可以提高我们对威胁的可视性。

第二种信息是策略信息，可以实现更快的响应。

我们共享的第三种信息是威胁情报，可以提高整个安全架构的智能化。

最后，我们共享的第四种信息是情景感知，您可以借助它在整个网络中构建更加智能、一致和精细的策略。



我们相信，通过此解决方案，我们可以提供一个功能强大的安全架构来简化检测并做出自动响应，从而提供更有效的安全保护。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。 地址、电话号码和传真号码均列在思科网站 **www.cisco.com/go/offices** 中。