思科身份服务引擎 - 技术合作伙伴生态系统

合作伙伴生态系统概述

企业网络正变得越来越复杂，需要管理的连接设备和应用比以前任何时候都多。随着设备和应用的日益增多，准确掌握连接到网络的人员和设备的情况变得更加困难，而且安全方面的问题也在迅速增多，因为设备越多，意味着威胁网络的可能方式也越多。一般而言，IT 组织都会通过在其网络中不断引入更多安全系统和供应商来解决这些安全问题。

但是，采用多个供应商提供的多种解决方案，往往会产生各自独立的信息存储库。所有这些不相干的系统就会形成全然不同的数据，需要通过手动方式将它们联系起来，才能准确识别网络威胁，并确定应采取何种修复措施。思科® 身份服务引擎 (ISE) 有助于简化和精简此过程。Cisco ISE 从整个网络中收集有价值的情景数据，并在多个系统和供应商之间进行整合和共享，以便确切了解威胁的根源所在。通过消除将多个系统中的不同数据集中起来的手动耗时过程，您可以更快地查明网络威胁，并在安全事件尚未造成损害之前将其解决掉。

合作伙伴平台还可以使用 Cisco ISE 生成的身份、设备和策略信息，为用户提供其他各种不同的有用功能。通过将这些产品与 Cisco ISE 集成，可以将合作伙伴解决方案融入到思科网络基础设施中，并对用户和设备采取网络访问控制措施。其中包括隔离和阻止访问，为 Cisco ISE 提供输入信息以便决定采取何种访问控制策略。

思科平台交换网格和生态系统要点

Cisco ISE 是市场领先的安全策略管理平台，它可以统一并自动执行安全访问控制，以便对网络和网络资源访问实施基于角色的控制。它提供卓越的用户和设备可视性，并从网络中的众多来源（例如，终端、用户、Active Directory 列表和网络传感器）收集海量情景数据。Cisco ISE 中集成了思科平台交换网格 (pxGrid)。Cisco pxGrid 是一个强大的情景信息共享平台，为了提高内外生态系统合作伙伴解决方案的效力并增强其功能，它会将收集的这些情景数据与这些解决方案进行共享。Cisco ISE 生态系统中的合作伙伴解决方案可通过创新方式利用这些情景数据来改进网络管理并增强安全性。

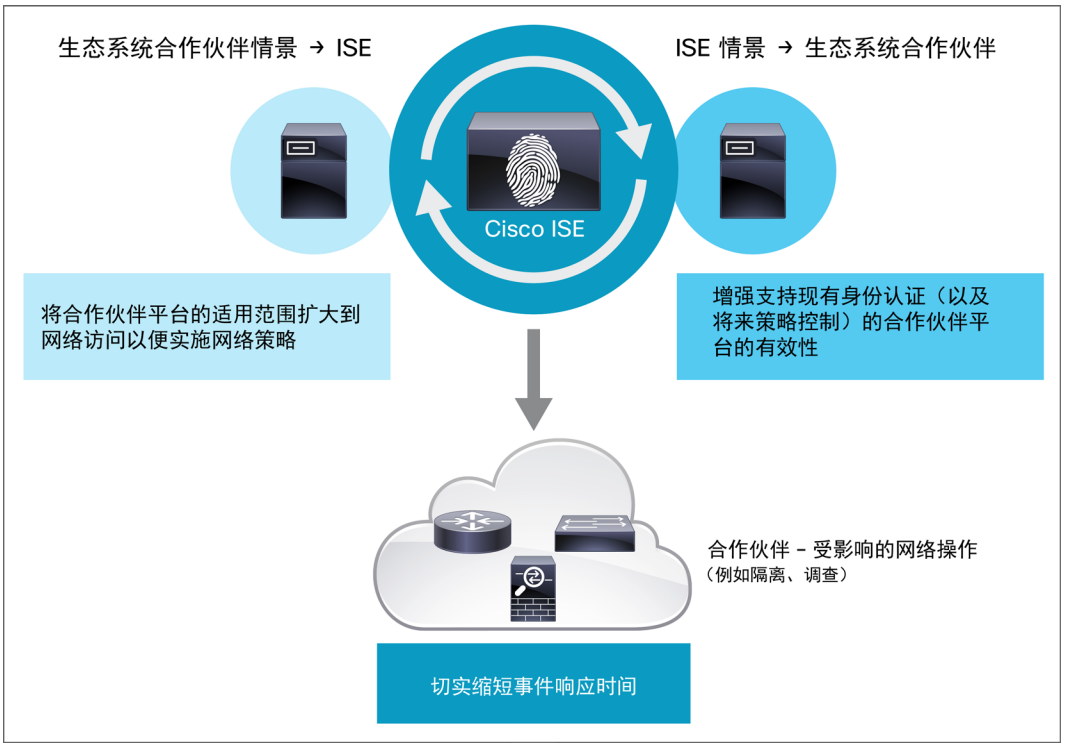
Cisco ISE 生态系统提供以下集成：

- **企业移动性管理和移动设备管理 (EMM/MDM)。**Cisco ISE 与 EMM/MDM 合作伙伴平台之间的集成，不仅有助于进行状态合规性评估，而且还有利于对尝试访问网络的移动终端进行设备控制。将 EMM/MDM 与 Cisco ISE 集成之后，该解决方案可执行持续状态检查，以帮助确保合规性并保持正确的网络访问级别。
- **安全信息和事件管理及威胁防御 (SIEM/TD)。**Cisco ISE 与 SIEM/TD 合作伙伴平台之间的集成，有助于这些平台利用用户身份、网络授权级别、终端设备标识和安全状态信息，进一步增强对整个网络范围内安全事件的了解。此功能可在 SIEM/TD 合作伙伴控制台中提供一个安全事件综合视图。
- **身份访问管理和单点登录 (IAM/SSO)。**通过 IAM/SSO 合作伙伴集成，可以利用网络情景信息进一步增强现有身份验证和授权策略。此功能有助于进行身份验证策略设置，并且可根据网络和设备风险级别对策略进行调整。合作伙伴也可以使用 Cisco ISE 提供的网络情景信息来影响网络应用授权决定，从而提供更有效的关键信息访问控制。您可以根据用户使用的设备、所处的位置以及他们尝试访问的应用，为不同级别的用户建立不同的策略。例如，如果某个移动用户正用 iPad 尝试通过 VPN 连接来访问敏感的人力资源信息，那么为其设置的身份验证策略，可以比为尝试在公司办公室通过公司发放的笔记本电脑连接到同一应用的用户设置的身份验证策略更复杂一些。

- **漏洞评估。**漏洞评估合作伙伴集成可帮助合作伙伴利用 Cisco ISE 提供的用户身份、网络授权级别、网络接入方法和安全状态信息进一步增强漏洞分析。此功能可在漏洞评估管理控制台中提供一个综合视图。这样，分析师只需一个界面即可对严重事件做出响应。
- **网络和安全调查分析。**调查分析和数据包捕获合作伙伴集成支持合作伙伴可利用 Cisco ISE 提供的用户身份、网络授权级别、终端设备标识和安全状态来进一步增强网络流量可视性。此集成会在合作伙伴的管理控制台中提供一个数据包捕获综合视图，而合作伙伴可以使用 Cisco ISE 来对用户或设备实施防范措施，作为对调查分析结果的回应。
- **OT 访问策略和控制/SCADA 网络细分。**运营技术 (OT) 网络有其自己的需求。通过使用 Cisco ISE（用于访问策略）和 Cisco pxGrid（用于情景信息共享），OT 安全合作伙伴可以利用设备和网络情景数据进一步增强其现有 OT 安全策略，以便提供更详细且适应性更强的安全策略。OT 监控和报告功能使用 Cisco ISE 提供的设备和网络情景数据来详细了解哪些不同类型的设备正在访问网络中哪些类型的资源。

通过与 Cisco ISE 的这些集成，合作伙伴解决方案可获得至关重要的情景数据，然后再利用这些数据来更加快速有效地修复威胁或问题，并通过 Cisco ISE 动态实施隔离措施，以便限制受感染用户或设备的访问（见图 1）。

图 1. Cisco ISE 生态系统集成点



好处

- 通过身份和设备感知**提高**当前运营和安全平台的效率。
- **减少**识别、评估和响应网络事件的时间。
- **调整**各种 IT 平台以便从源头上保持用户、设备和策略可视性及网络控制的一致性。

后续计划

有关思科身份服务引擎 (ISE) 的详细信息，请访问 http://www.cisco.com/go/ise。

若要查看 Cisco ISE 生态系统合作伙伴的列表，请访问思科安全合作伙伴生态系统页面：http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html。

有关特定合作伙伴的其他详细信息，请在思科市场解决方案目录中进行搜索，地址：http://marketplace.cisco.com/catalog。

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。

美国印刷 C45-732907-00 09/14