(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109478263 A
(43)申请公布日 2019.03.15

(21)申请号 201780046179.6

(22)申请日 2017.05.15

(30)优先权数据
15/179,581 2016.06.10 US

(85)PCT国际申请进入国家阶段日
2019.01.28

(86)PCT国际申请的申请数据
PCT/IB2017/052861 2017.05.15

(87)PCT国际申请的公布数据
WO2017/212357 EN 2017.12.14

(71)申请人 欧帕特公司
地址 美国明尼苏达州明尼顿卡市

(72)发明人 菲利普·F·勒纳

(74)专利代理机构 北京博雅睿泉专利代理事务所(特殊普通合伙) 11442
代理人 李慧

(51)Int.Cl.
G06Q 10/06(2006.01)
G06F 21/57(2006.01)

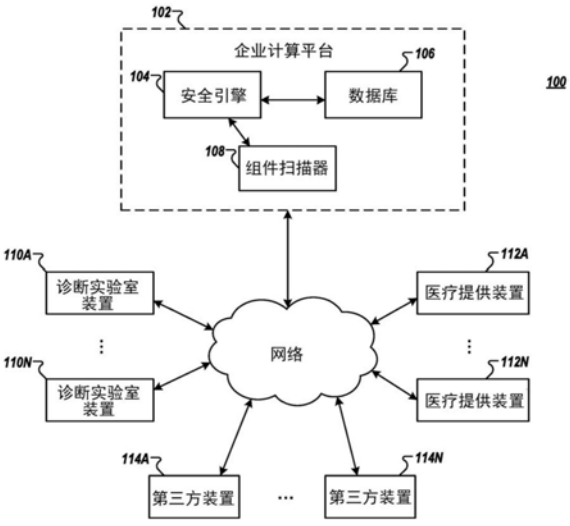
权利要求书3页 说明书14页 附图6页

(54)发明名称

用于体系结构评估和策略执行的系统和设备

(57)摘要

公开了用于企业计算平台内的资产体系结构评估和安全执行的示例实施例。一个示例方法包括接收用于评估的建议体系结构,其中,用于评估的建议体系结构涉及将资产集成到企业计算平台中。该示例方法还包括通过风险评估电路动态地评估针对为企业计算平台建立的嵌入式安全策略、标准、基线或模式的建议体系结构。另外,该示例方法还包括在建议体系结构的动态评估识别安全漏洞的实例中,通过风险评估电路确定将修复所识别的安全漏洞的对建议体系结构的改变。该示例方法还包括生成关于建议体系结构的报告,其中,所述报告标识将修复所识别的安全漏洞的对建议体系结构的任何改变。还提供了对应的设备和计算机程序产品。



CN 109478263 A

1.一种用于企业计算平台内的资产体系结构评估和安全执行的方法,所述方法包括:

引起通过组件扫描器向配备在先前由安全引擎评估的资产上的组件代理器传送一个或多个改变识别消息;

接收对资产的当前体系结构已经进行改变的指示;

生成用于评估的建议体系结构,其中,用于评估的建议体系结构指示包括企业计算平台和基于对资产的当前体系结构的改变的资产的体系结构的修改版本的设计;

通过风险评估电路并使用一个或多个机器学习算法基于为企业计算平台建立的嵌入式安全策略、标准、基线或模式而近乎实时地动态评估建议体系结构;

在对建议体系结构的动态评估识别到安全漏洞的实例中,由风险评估电路确定将修复所识别的安全漏洞的对建议体系结构的改变;

生成关于建议体系结构的报告,其中,所述报告标识将修复所识别的安全漏洞的对建议体系结构的任何改变;以及

引起通过组件扫描器引起向配备在资产上的组件代理器传送关于建议体系结构的报告。

2.根据权利要求1所述的方法,其中,接收对所述体系结构已经进行改变的指示包括:

接收资产的体系结构的指示;以及

将资产的体系结构与先前由安全引擎评估的资产的体系结构的版本进行比较。

3.根据权利要求1所述的方法,其中,所述方法还包括:

训练一个或多个机器学习算法以开发用于企业计算平台的一个或多个基线或模式。

4.根据权利要求3所述的方法,其中,动态地评估建议体系结构包括:

通过风险评估电路并使用一个或多个机器学习算法评估建议体系结构的任何方面是否违反了为企业计算平台开发的基线或模式。

5.根据权利要求1所述的方法,其中,确定将修复所识别的安全漏洞的对建议体系结构的改变包括:

调用人工干预,以识别将修复所识别的安全漏洞的对建议体系结构的改变;或者

识别将使用为企业计算平台建立的嵌入式安全策略、标准、基线或模式中的至少一个来修复所识别的安全漏洞的对建议体系结构的改变。

6.一种用于企业计算平台内的资产体系结构评估和安全执行的设备,所述设备包括至少一个处理器和存储计算机可执行指令的至少一个存储器,当由至少一个处理器执行时,使所述设备:

引起一个或多个改变识别消息传送到配备在先前由安全引擎评估的资产上的组件代理器;

接收对资产的当前体系结构已经进行改变的指示;

生成用于评估的建议体系结构,其中,用于评估的建议体系结构指示包括企业计算平台的设计和基于对资产的当前体系结构的改变的资产的体系结构的修改版本;

使用一个或多个机器学习算法基于为企业计算平台建立的嵌入式安全策略、标准、基线或模式而近乎实时地动态评估建议体系结构;

在对建议体系结构的动态评估识别到安全漏洞的实例中,确定将修复所识别的安全漏洞的对建议体系结构的改变;

生成关于建议体系结构的报告，其中，所述报告标识将修复所识别的安全漏洞的对建议体系结构的任何改变；以及

引起关于建议体系结构的报告传送到配备在资产上的组件代理器。

7.根据权利要求6所述的设备，其中，当由至少一个处理器执行时，所述计算机可执行指令使所述设备执行如下步骤以引起所述设备接收对所述体系结构已经改变的指示：

接收资产的体系结构的指示；以及

将资产的体系结构与先前由安全引擎评估的资产的体系结构的版本进行比较。

8.根据权利要求6所述的设备，其中，当由至少一个处理器执行时，所述计算机可执行指令还使得所述设备：

训练一个或多个机器学习算法以为企业计算平台开发一个或多个基线或模式。

9.根据权利要求8所述的设备，其中，当由至少一个处理器执行时，所述计算机可执行指令使所述设备执行如下步骤以引起所述设备动态地评估建议体系结构：

使用一个或多个机器学习算法评估建议体系结构的任何方面是否违反了为企业计算平台开发的基线或模式。

10.根据权利要求6所述的设备，其中，当由至少一个处理器执行时，所述计算机可执行指令使得所述设备执行如下步骤以引起所述设备确定将修复所识别的安全漏洞的对建议体系结构的改变：

调用人工干预，以识别将修复所识别的安全漏洞的对建议体系结构的改变的；或者

识别将使用为企业计算平台建立的嵌入式安全策略、标准、基线或模式中的至少一个来修复所识别的安全漏洞的对建议体系结构的改变。

11.一种用于企业计算平台内的资产体系结构评估和安全执行的设备，所述设备包括：

用于引起向配备在先前由安全引擎评估的资产上的组件代理器传送一个或多个改变识别消息的装置；

用于接收对资产的当前体系结构已经进行改变的指示的装置；

用于生成用于评估的建议体系结构的装置，其中，用于评估的建议体系结构指示包括企业计算平台的设计和基于资产的当前体系结构的改变的资产的体系结构的修改版本；

用于使用一个或多个机器学习算法基于为企业计算平台建立的嵌入式安全策略、标准、基线或模式而近乎实时地动态评估建议体系结构的装置；

用于在对建议体系结构的动态评估识别安全漏洞的实例中，确定将修复所识别的安全漏洞的对建议体系结构的改变的装置；

用于生成关于建议体系结构的报告的装置，其中，所述报告标识将修复所识别的安全漏洞的对建议体系结构的任何改变；以及

用于引起向配备在资产上的组件代理器传送关于建议体系结构的报告的装置。

12.根据权利要求11所述的设备，其中，用于接收对所述体系结构已经进行改变的指示的装置包括：

用于接收资产的体系结构的指示的装置；以及

用于将资产的体系结构与先前由安全引擎评估的资产的体系结构的版本进行比较的装置。

13.根据权利要求11所述的设备，其中，所述设备还包括：

用于训练一个或多个机器学习算法以开发用于企业计算平台的一个或多个基线或模式的装置。

14.根据权利要求13所述的设备,其中,用于动态地评估建议体系结构的装置包括:

用于使用一个或多个机器学习算法评估建议体系结构的任何方面是否违反为企业计算平台开发的基线或模式的装置。

15.根据权利要求11所述的设备,其中,用于确定将修复所识别的安全漏洞的对建议体系结构的改变的装置包括:

用于调用人工干预的装置,以识别将修复所识别的安全漏洞的对建议体系结构的改变;或者

识别使用为企业计算平台建立的嵌入式安全策略、标准、基线或模式中的至少一个来修复所识别的安全漏洞的对建议体系结构的改变。

用于体系结构评估和策略执行的系统和设备

技术领域

[0001] 本发明的示例实施例总体涉及信息技术体系结构，更具体地涉及用于通过应用程序的自动评估和安全策略的执行来降低安全风险的系统、设备和方法。

背景技术

[0002] 申请人发现用于评估由与企业计算平台接口的资产所造成的安全漏洞的现有技术存在问题。通过付诸努力、独创性和创新，申请人通过开发由本发明所体现并在下面详细描述的解决方案解决了许多这些已经认识到的问题。

发明内容

[0003] 本文描述的示例实施例改进了现有的资产体系结构评估和安全执行技术。本文描述的实施例涉及改进企业计算平台的技术特征、能力和效率。

[0004] 在第一示例实施例中，提供了一种用于企业计算平台内的资产体系结构评估和安全执行的方法。所述方法包括接收用于评估的建议体系结构，其中，用于评估的建议体系结构涉及将资产集成到企业计算平台中。所述方法还包括通过风险评估电路基于为企业计算平台建立的嵌入式安全策略、标准、基线或模式而动态地评估建议体系结构。所述方法还包括，在建议体系结构的动态评估识别到安全漏洞的实例中，通过风险评估电路确定将修复所识别的安全漏洞的对建议体系结构的改变。所述方法还包括生成关于建议体系结构的报告，其中，所述报告标识将修复所识别的安全漏洞的对建议体系结构的任何改变。

[0005] 在一些实施例中，接收用于评估的建议体系结构包括使得通过组件扫描器向配备在资产上的组件代理器传送一个或多个改变识别消息，以及接收从先前由安全引擎评估的资产的体系结构的版本中对资产的体系结构已经进行改变的指示，其中，建议体系结构包括资产的当前体系结构。

[0006] 在一些这样的实施例中，接收对所述体系结构已经进行改变的指示包括接收资产的体系结构的指示；以及将资产的体系结构与先前由安全引擎评估的资产的体系结构的版本进行比较。在这方面，所述方法还可以包括使得通过组件扫描器和配备在资产上的组件代理器传送关于建议体系结构的报告。

[0007] 在一些实施例中，所述方法还包括训练一个或多个机器学习算法以开发用于企业计算平台的一个或多个基线或模式。在一些这样的实施例中，动态评估建议体系结构包括通过风险评估电路和使用一个或多个机器学习算法来评估建议体系结构的任何方面是否违反为企业计算平台开发的基线或模式。

[0008] 在一些实施例中，确定将修复所识别的安全漏洞的对建议体系结构的改变包括调用人工干预以识别将修复所识别的安全漏洞的对建议体系结构的改变、或识别将使用为企业计算平台建立的嵌入式安全策略、标准、基线或模式中的至少一个来修复所识别的安全漏洞的对建议体系结构的改变。

[0009] 在另一个示例实施例中，提供了一种用于企业计算平台内的资产体系结构评估和

安全执行的设备。所述设备包括至少一个处理器和至少一个存储计算机可执行指令的存储器，当由至少一个处理器执行时，所述计算机可执行指令使得所述设备接收用于评估的建议体系结构，其中，用于评估的建议体系结构涉及将资产集成到企业计算平台中。当由至少一个处理器执行时，计算机可执行指令进一步使得所述设备基于为企业计算平台建立的嵌入式安全策略、标准、基线或模式动态地评估建议体系结构，以及在建议体系结构的动态评估识别安全漏洞的实例中，确定将修复所识别的安全漏洞的对建议体系结构的改变。当由至少一个处理器执行时，计算机可执行指令进一步使得所述设备生成关于建议体系结构的报告，其中，所述报告标识将修复所识别的安全漏洞的对建议体系结构的任何改变。

[0010] 在一些实施例中，当由至少一个处理器执行时，计算机可执行指令通过使得设备通过组件扫描器向配备在资产上的组件代理器传送一个或多个改变识别消息，从而使得设备接收用于评估的建议体系结构，以及从先前由安全引擎评估的资产的体系结构的版本中接收对资产的体系结构已经进行改变的指示，其中，建议体系结构包括资产的当前体系结构。

[0011] 在一些这样的实施例中，当由至少一个处理器执行时，计算机可执行指令使得设备通过使设备接收资产的体系结构的指示，从而接收对体系结构已经进行改变的指示，以及将资产的体系结构与先前由安全引擎评估的资产的体系结构的版本进行比较。在这方面，当由至少一个处理器执行时，计算机可执行指令进一步使得设备通过组件扫描器和配备在资产上的组件代理器传送关于建议体系结构的报告。

[0012] 在一些实施例中，当由至少一个处理器执行时，计算机可执行指令进一步使得设备训练一个或多个机器学习算法以开发用于企业计算平台的一个或多个基线或模式。在一些这样的实施例中，当由至少一个处理器执行时，计算机可执行指令使得设备通过使设备使用一个或多个机器学习算法来动态地评估建议体系结构，从而评估建议体系结构的任何方面是否违反了为企业计算平台开发的基线或模式。

[0013] 在一些实施例中，当由至少一个处理器执行时，计算机可执行指令使得设备确定对建议体系结构的改变，这些改变将通过使得设备调用人工干预，以识别将修复所识别的安全漏洞的对建议体系结构的改变、或识别将使用为企业计算平台建立的嵌入式安全策略、标准、基线或模式中的至少一个来修复所识别的安全漏洞的对建议体系结构的改变。

[0014] 在另一个示例实施例中，提供了一种用于企业计算平台内的资产体系结构评估和安全执行的设备。所述设备包括用于接收用于评估的建议体系结构的装置，其中，用于评估的建议体系结构涉及将资产集成到企业计算平台中；用于基于为企业计算平台建立的嵌入式安全策略、标准、基线或模式动态地评估建议体系结构的装置；用于在建议体系结构的动态评估识别安全漏洞的实例中确定将修复所识别的安全漏洞的对建议体系结构的改变的装置；以及用于生成关于建议体系结构的报告的装置，其中，所述报告标识将修复所识别的安全漏洞的对建议体系结构的任何改变。

[0015] 在一些实施例中，用于接收用于评估的建议体系结构的装置包括用于通过组件扫描器向配备在资产上的组件代理器传送一个或多个改变识别消息的装置；以及用于从先前由安全引擎评估的资产的体系结构的版本接收对资产的体系结构已经进行改变的指示的装置，其中，建议体系结构包括资产的当前体系结构。在一些这样的实施例中，用于接收对体系结构已经进行改变的指示的装置包括用于接收资产的体系结构的指示的装置；以及用

于将资产的体系结构与先前由安全引擎评估的资产的体系结构的版本进行比较的装置。在这方面，所述设备还包括用于使得通过组件扫描器和配备在资产上的组件代理器传送关于建议体系结构的报告的装置。

[0016] 在一些实施例中，所述设备还包括用于训练一个或多个机器学习算法以开发用于企业计算平台的一个或多个基线或模式的装置。在一些这样的实施例中，用于动态地评估建议体系结构的装置包括用于使用一个或多个机器学习算法来评估建议体系结构的任何方面是否违反为企业计算平台开发的基线或模式的装置。

[0017] 在一些实施例中，用于确定将修复所识别的安全漏洞的对建议体系结构的改变的装置包括用于调用人工干预的装置，以识别将修复所识别的安全漏洞的对建议体系结构的改变、或识别将使用为企业计算平台建立的嵌入式安全策略、标准、基线或模式中的至少一个来修复所识别的安全漏洞的对建议体系结构的改变。

[0018] 提供上述发明内容仅仅是为了总结一些示例实施例，以提供对本发明的一些方面的基本理解。因此，应该理解，上述实施例仅仅是示例，不应被解释为以任何方式缩小本发明的范围或精神。应该理解，本发明的范围除了这里总结的那些之外还包括许多潜在的实施例，其中一些将在下面进一步描述。

附图说明

[0019] 因此，已经概括地描述了本公开的某些示例实施例，现在将参考附图，所述附图不一定是按比例绘制的。

[0020] 图1示出了根据本发明的示例实施例的示例系统图。

[0021] 图2示出了根据一些示例实施例的与企业计算平台的安全引擎相关联使用的电路的示意性框图。

[0022] 图3示出了根据一些示例实施例的与配管或以其它方式表示企业计算平台与之交互的资产的装置相关联使用的电路的示意性框图。

[0023] 图4示出了根据一些示例实施例的安全引擎的高级设计。

[0024] 图5示出了根据一些示例实施例的安全引擎的系统级设计。

[0025] 图6示出了根据一些示例实施例的描述用于通过应用程序的自动评估和安全策略的执行来降低安全风险的示例操作的流程图。

[0026] 图7示出了根据一些示例实施例的描述用于确保已经评估的变更资产不引入新的安全漏洞的示例操作的流程图。

具体实施方式

[0027] 现在将在下文中参考附图更全面地描述本发明的各种实施例，在附图中示出了本发明的一些但非全部实施例。实际上，本发明可以以许多不同的形式体现，并且不应该被解释为限于本文阐述的实施例；相反，提供这些实施例以使本公开满足适用的法律要求。相同的附图标记始终指代相同的元件。

[0028] 如本文所使用的，术语“数据”、“内容”、“信息”和类似术语可以互换地使用，以指代能够根据本发明的实施例传送、接收和/或存储的数据。因此，不应该考虑使用任何这样的术语来限制本发明的实施例的精神和范围。此外，在本文中描述的计算装置以从另一个

计算装置接收数据的情况下，应该理解，数据可以直接从另一个计算装置接收，或者可以经由一个或多个中间计算装置，例如，一个或多个服务器、中继、路由器、网络接入点、基站、主机和/或类似的装置，本文有时称为“网络”间接接收。类似地，本文描述的计算装置以将数据发送到另一个计算装置的情况下，应该理解，数据可以直接发送到另一个计算装置，或者可以经由一个或多个中间计算装置，例如，一个或多个服务器、中继、路由器、网络接入点、基站、主机和/或类似装置间接发送。

[0029] 概览

[0030] 历史上，企业计算平台中的安全漏洞一直被视为由企业计算平台与外部源资源(例如，应用程序、设施元件、数据库等等)之间交互的持续需求引起的不幸弊端。然而，当这些外源式资源用于访问诸如受保护的健康信息(PHI)、个人身份信息(PII)或支付卡信息(PCI)信息的敏感数据时，保护这种交互的安全尤为重要。因此，这种受保护或被分类的计算资源，在下文中称为“资产”，需要附加的信息安全控制来保护它们使用的数据，并且当从企业计算平台本身检索该数据时尤其如此。虽然企业计算平台通常由信息技术(IT)组管理，它们可以评估资产的风险概况并识别安全漏洞，但人工执行这些功能所需的时间和资源是巨大的。

[0031] 此外，许多企业计算平台出现安全漏洞的一个重要原因源于这样一个事实：即使资产的修改可能会带来同样多的安全缺陷，但对已经授权的资产的更新也不会引发与新资产接口请求相同程度的警报或审查。这种缺乏审查的情况有很多原因。首先，作为一个实际问题，资产的改变并不总是被检测到，因此在安全方面新安全漏洞的出现对企业来说可能是未知的。其次，由于评估任何资产所带来的安全问题所固有的大量时间和资源投入，因此随着时间的推移资产的改变在历史上比作为简单的分类问题新近引入的资产更少受到监管。因此，需要一种系统，其可以促进遵守管理与给定企业计算平台的交互的安全策略，并且同时可以加速对新资产和修改资产的评估。

[0032] 如本文所述，示例系统和设备通过提供被配置成自动评估资产以符合企业计算平台的安全策略的安全引擎来解决这些需求和其它需求。在一些实施例中，安全引擎利用促进关于资产的安全策略相关信息的预处理和分类的机器学习技术，以及连续变量(统计回归)和维度减少(减少无关变量)的随后预测来识别体系结构内的安全漏洞。通过这样做，示例实施例引入了对安全性分析的更严格性，从而确保更好地保护企业计算平台免受可能以其它方式利用安全漏洞的潜在攻击。

[0033] 此外，通过要求在已经被授权与企业计算平台交互的资产上安装组件代理器，并通过引入配置为与组件代理器通信的组件扫描器的使用，可以严格识别和评估对已经授权与企业计算平台交互的资产的改变，从而给予评估资产随着时间的推移而不断发展的安全概况的机会。结合起来，这些概念说明了企业计算平台的配置，该平台能够自动评估新资产和变更资产，从而减轻企业计算平台安全评估中的两个历史弱点。

[0034] 如下面更详细描述的，本文描述的各种实施例改进了现有的资产评估和安全策略执行技术。本文描述的实施例涉及改进企业计算平台的技术特征、能力和效率。

[0035] 系统体系结构和示例设备

[0036] 本发明的方法、设备和计算机程序产品可以由各种装置中的任何一种来体现。例如，示例实施例的方法、设备和计算机程序产品可以由诸如服务器或其它网络实体的联网

装置来体现，该联网装置被配置成与一个或多个装置、例如一个或多个客户端装置通信。附加性地或替代性地，计算装置可以包括诸如个人计算机或计算机工作站的固定计算装置。此外，示例实施例还可以由各种移动终端，例如便携式数字助理(PDA)、移动电话、智能手机、膝上型计算机、平板电脑或上述设备的任何组合中的任何一种来体现。

[0037] 在这方面，图1公开了其中可以操作本发明的实施例的示例计算系统。各种资产可以期望分别使用计算装置110A至110N、112A至112N和114A至114N经由网络(例如，因特网等等)访问和访问企业计算平台102。

[0038] 计算装置110A至110N、112A至112N和114A至114N可以由本领域中已知的任何计算装置来体现。由企业计算平台102从诊断实验室装置110A-110N、医疗提供装置112A-112N和第三方装置114A-114N接收的电子数据可以以各种形式并经由各种方法提供。例如，这些装置可以包括台式计算机、膝上型计算机、智能手机、上网本、平板电脑、可穿戴装置、和/或适于执行本文所述的功能、操作和/或过程的装置或实体的任何组合，以及可以使用与这些装置相关联的各种传送模式和/或协议来提供电子数据。

[0039] 附加性地或替代性地，诊断实验室、医疗提供者和其它第三方可以经由web浏览器与企业计算平台102交互。作为又一个示例，装置110A-110N、112A-112N和114A-114N可以包括被设计成与实验室提取计算系统102接口的各种硬件或固件(例如，其中示例装置110、112、或114是为与诸如信息亭的企业计算平台102通信的主要目的而提供的专用装置)。

[0040] 企业计算平台102可以包括可以与数据库106和组件扫描器108通信的安全引擎104。安全引擎104可以体现为本领域中已知的计算机。安全引擎104可以从各种源(包括但不一定限于装置110A-110N、112A-112N和114A-114N)接收电子数据，并且可以用于分析由这些装置提供和/或表示的资产。

[0041] 数据库106可以体现为诸如网络附连存储(NAS)装置的数据存储装置、或者体现为单独的数据库服务器。数据库106包括由安全引擎104访问和存储的信息，以促进企业计算平台102的操作。例如，数据库106可以包括但不限于：为企业计算平台建立的一个或多个安全策略、标准、基线和/或模式。在这方面，安全策略是一份范围广泛的文档，从业务和技术的角度提供关于某个问题的安全指导，而标准则是更细粒度的，通常是更多技术文档，其中包含的细节通常太过具体，无法包含在更广泛的安全策略中。基线是指在允许技术进入企业之前必须满足的一系列指令或要求。因此，如下面更详细描述的，企业计算平台102包括组件(例如，安全引擎104和组件扫描器108)，以摄取对应于评估中的资产(功能性和非功能性)的设计要求，并基于其对所述策略、标准、基线和模式的遵守情况映射那些要求和正在评估的技术，以确定是否存在可能给企业带来风险的任何安全漏洞。然而，除了这些安全策略、标准、基线和模式之外，数据库106还可以存储其它信息，例如用于数据库和/或应用程序接口(API)集成挂钩的安全相关数据/保护套件。

[0042] 最后，组件扫描器108可以包括促进安全引擎104与安装在与企业计算平台102可以与之交互的资产上的一个或多个组件代理器之间的间接通信的资源。通过避免组件代理器与安全引擎104本身之间的直接通信，组件扫描器108向企业计算平台102提供附加的保护层。在这方面，组件扫描器108可以提供类似于堡垒主机提供的益处，因为即使组件扫描器108由于其经由由特定资产配管的相应组件代理器与资产的交互而受到损害，组件扫描器108本身也不存储或提供对任何敏感信息的访问，以及尽管存在妥协，企业计算平台102

的安全性仍可以保持。

[0043] 应该理解，虽然组件扫描器108使得能够从由各种资产配管的组件代理器检索数据(例如，向安全引擎104提供信息，促进对与资产接口的风险概况的分析)，但是该通信可以是双向的，并且安全代理104可以经由组件扫描器108和资产的组件代理器将信息传送回资产(这种传送可以包括与企业计算平台102的持续互操作性所需的改变的指示)。

[0044] 组件扫描器108还提供附加的功能。它被配置成确定来自资产(由该资产的组件代理器提供)的提案之间的差异，以确定是否有必要对资产的风险概况进行重新评估。通过这样做，组件扫描器108为企业计算平台102提供了避免安全方面的漏洞发展的能力，尽管资产提供的特征集随着时间的推移而不断发展。

[0045] 用于实现本发明的实施例的示例设备

[0046] 安全引擎104可以由一个或多个计算装置、例如图2中所示的设备200来体现。如图2所示，设备200可以包括处理器202、存储器204、输入/输出电路206、通信电路208和风险评估电路210。设备200可以被配置成执行上述关于图1的操作和以下关于图7的操作。尽管关于功能限制描述了这些组件202-210，但是应当理解，特定的实现必然包括特定硬件的使用。还应当理解，这些组件202-210中的某些可以包括类似或共同的硬件。例如，两组电路都可以利用相同的处理器、网络接口、存储介质等等的使用来执行它们的相关联的功能，使得每组电路不需要重复硬件。因此，如本文中关于设备的组件使用的术语“电路”的使用包括被配置成执行与本文描述的特定电路相关联的功能的特定硬件。

[0047] 当然，虽然术语“电路”应该被广义地理解为包括硬件，但是在一些实施例中，它还可以包括用于配置硬件的软件。在一些实施例中，“电路”可以包括处理电路、存储介质、网络接口、输入/输出装置等等。在一些实施例中，设备200的其它元件可以提供或补充特定电路的功能。例如，处理器202可以提供处理功能，存储器204可以提供存储功能，通信电路208可以提供网络接口功能，等等。

[0048] 处理器202(和/或协助或以其它方式与处理器相关联的协处理器或任何其它处理电路)可以经由总线与存储器204通信，用于在设备的组件之间传递信息。存储器204可以是非暂时性的，并且可以包括例如一个或多个易失性和/或非易失性存储器。换句话说，存储器可以是电子存储装置(例如，计算机可读存储介质)。存储器204可以被配置成存储信息、数据、内容、应用程序、指令等等，以使得设备能够根据本发明的示例实施例执行各种功能。

[0049] 处理器202可以以多种不同的方式体现，并且可以例如包括被配置成独立执行的一个或多个处理装置。附加性地或替代性地，处理器可以包括经由总线串联配置的一个或多个处理器，以便能够独立执行指令、流水线操作和/或多线程。术语“处理电路”的使用可以被理解为包括单核处理器、多核处理器、设备内部的多个处理器、和/或远程或“云”处理器。

[0050] 在一个示例实施例中，处理器202可以被配置成执行存储在存储器204中或者以其它方式处理器可访问的指令。替代性地或附加性地，处理器可以被配置成执行硬编码功能。因此，无论是通过硬件还是软件方法配置，还是通过硬件与软件的组合配置，处理器都可以表示能够在相应地配置的同时执行根据本发明的实施例的操作的实体(例如，物理地体现在电路中)。替代性地，作为另一个示例，当处理器被体现为软件指令的执行器时，指令可以具体地配置处理器以在执行指令时执行本文描述的算法和/或操作。

[0051] 在一些实施例中，设备200可以包括输入/输出电路206，所述输入/输出电路又可以与处理器202通信以向用户提供输出，并且在一些实施例中，接收用户输入的指示。输入/输出电路206可以包括用户接口，并且可以包括显示器，并且可以包括web用户接口、移动应用程序、客户端装置、信息亭等等。在一些实施例中，输入/输出电路206还可以包括键盘、鼠标、操纵杆、触摸屏、触摸区域、软键、麦克风、扬声器或其它输入/输出机构。处理器和/或包括处理器的用户接口电路可以被配置成通过存储在处理器可访问的存储器(例如，存储器204和/或类似物)上的计算机程序指令(例如，软件和/或固件)来控制一个或多个用户接口元件的一个或多个功能。

[0052] 通信电路208可以是被配置成在与设备200通信中从或向网络和/或任何其它装置、电路或模块接收和/或传送数据的诸如以或者硬件或者硬件和软件的组合的方式体现的装置或电路的任何装置。在这方面，通信电路208可以包括例如用于实现与有线或无线通信网络通信的网络接口。例如，通信电路208可以包括一个或多个网络接口卡、天线、总线、交换机、路由器、调制解调器和支持硬件和/或软件、或适合于经由网络实现通信的任何其它设备。附加性地或替代性地，通信接口可以包括用于与天线交互以使得经由天线传送信号或者处理经由天线接收到的信号的电路。

[0053] 风险评估电路210包括被配置成实现安全引擎104的硬件。相应地，风险评估电路210被设计成分析关于资产的信息并识别用于潜在补救的安全漏洞。在这方面，风险评估电路210可以利用机器学习来基于为企业计算平台102建立的安全策略、标准、基线或模式来评估资产的体系结构，以便识别安全漏洞。为此，风险评估电路210包括机器学习和/或人工智能组件，其被设计成基于理解建议体系结构和基于例如风险评估电路210本身使用培训数据随着时间的推移开发的基线的该建议体系结构内的任何异常值来捕获安全漏洞。因此，风险评估电路210被配置成使用解释性分析和分析来确定是否存在任何误报以修复不符合策略、标准或基线的破坏的体系结构，这种破坏的体系结构将作为参考点被容纳在逻辑内并且随着这些策略、标准和基线在企业中进行修订而更新。

[0054] 风险评估电路210可以利用诸如处理器202的处理电路来执行上述操作，并且可以利用存储器204来存储每个风险评估的生成结果。还应当理解，在一些实施例中，风险评估电路210可以包括单独的处理器、专门配置的现场可编程门阵列(FPGA)或专用接口电路(ASIC)，以执行其功能。因此，风险评估电路210使用设备的硬件组件来实现，所述硬件组件又由用于实现这些计划的功能的硬件或者软件配置。

[0055] 可以理解，任何这样的计算机程序指令和/或其它类型的代码可以被加载到计算机、处理器或其它可编程设备的电路上，以产生机器，使得在机器上执行代码的计算机、处理器其它可编程电路创建用于实现各种功能、包括本文描述的那些功能的装置。

[0056] 图3示出了根据一些示例实施例的与配管或以其它方式表示企业计算平台与之交互的资产的装置相关联使用的电路的示意性框图。如图3所示，设备300可以包括处理器302、存储器304、输入/输出电路306和通信电路308。当设备300涉及本发明中描述的操作时，这些组件的功能可以类似于上面关于图2所描述的类似命名的组件，为了简洁起见，省略了对这些组件的机械结构的附加描述。然而，一起操作的这些装置元件为设备300提供促进给定资产与企业计算平台102之间的交互所必需的功能。

[0057] 然而，每个设备300另外还可以包括组件代理器310，所述组件代理器包括被配置

成与组件扫描器108交互的硬件。组件代理器310本质上是暂时的，配备在资产上，以在由扫描器确定并报告给安全引擎的资产体系结构中发生改变时，允许从平台到其它解决方案组件的通信更新。组件代理器310可以包括存储在资产上的轻量且不显眼的组件。应当理解，在一些实施例中，组件代理器310可以包括硬件模块，所述硬件模块包括单独的处理器、专门配置的现场可编程门阵列(FPGA)或专用接口电路(ASIC)，以执行这些功能。在一些实施例中，组件代理器310因此使用由硬件或者软件配置的用于实现这些计划的功能的设备的硬件组件来实现，尽管应当理解，在一些实施例中，组件代理器310可以完全在软件中配置并且可以通过利用设备300的先前描述的组件来执行。

[0058] 如上所述并且基于本公开应该理解，本发明的示例实施例可以被配置为方法、移动装置、后端网络装置等等。因此，实施例可以包括各种包括全部硬件或软件和硬件的任何组合的装置。此外，实施例可以在至少一个非暂时性计算机可读存储介质上采用计算机程序产品的形式，所述计算机可读存储介质具有包含在存储介质中的计算机可读程序指令(例如，计算机软件)。任何合适的计算机可读存储介质都可以使用，包括非暂时性硬盘、CD-ROM、闪存、光学存储装置或磁存储装置。

[0059] 示例安全自动化体系结构

[0060] 已经描述了包括本文所设想的一些示例实施例的电路，应当理解，企业计算平台102可以有利地与企业计算平台102的安全策略相关联地评估资产的体系结构。根据示例实施例，图4至6分别示出了高级系统设计、上下文组件设计和系统级设计。

[0061] 首先参见图4，提供高级系统设计，用于评估与企业计算平台102(由策略服务器402配管)的安全策略、标准、基线和模式相关联的资产的体系结构。如图4所示，系统设计依赖于诸如为关于资产安全性的通信提供协议词汇表的安全内容自动化协议-NIST 800-117(SCAP)的TCG/TNC工作组和NIST-行业标准体系结构和协议的使用。依赖于机器学习人工智能的安全引擎404可以嵌入到解决方案的控制平面中，并且可以经由IF-MAP总线406与企业计算平台102中的各种其它元件通信。在一些实施例中，安全引擎404使用的人工智能可以基于Python中的sci-kit学习。这将有助于预处理、数据分类-ID、回归-预测连续变量和降维-减少考虑的随机变量。在其它实施例中，Oryx可以用于机器学习(ML)/AI，因为有可能利用它们的lambda体系结构并且在Hadoop上构建H20，其中HDFS在与服务层和总线交互的计算层上。最后，尽管未在图4中示出，启用SCAP的端点/资产可以使用上面提到的组件代理器310与企业计算平台102接口，以允许使用IF-MAP开放协议与平台和IF-MAP总线404进行持续通信。因此，可以参考存储在策略服务器402上的安全策略、标准和基线，以确定和修复安全漏洞，以降低风险并改进由平台评估的建议体系结构。

[0062] 虽然图4提供了高级设计，但是应该理解，示例企业计算平台102的上下文组件设计(CCD)通常可以在具有不同访问权限和操作角色的各种“区域”中被分段。通常，企业将在其体系结构内提供区域的分段和隔离，以防止从低安全性区域到高安全性区域的访问。这些区域的布置和体系结构可以定制，因为基于资产所在的位置确定每个特定的企业体系结构的需求。因此，安全引擎104可以位于“表示层区域”中，所述“表示层区域”允许容易地访问和与外部资产通信，从而促进基于业务和技术要求的近实时评估。替代性地，安全引擎104可以位于企业体系结构内的更深区域中，从而提供来自外部源的更高安全性。组件扫描器还可以位于呈现区域中，以促进与来自企业计算平台102的核心操作组件在不同层上的

资产交互，以增强整个平台102的安全性。组件代理器将对应地配备在与组件扫描器通信的关键信息资产上，以确定是否在企业计算平台102的当前策略、模式、标准和基线之外进行了改变。应当理解，安全引擎还包含数据库和Web服务器组件，如图4所示，用于保护和报告进出安全引擎的所有通信。

[0063] 图5继而示出了安全引擎的系统级设计。安全引擎使用的实体设施包括Web服务器和数据库服务器。Web服务器可以包括强化的Apache服务器，而数据库服务器可以具有强化的NoSQL设计。安全引擎本身可以使用SE Linux或Slackware来实现，并且在一些实施例中，安全引擎的唯一外部暴露是经由RESTful API实现的。安全引擎可以经由服务总线(例如，图5中所示的虚拟信息总线)进行通信。安全引擎可以利用基于IF-MAP标准的安全协议来实现关于特定区域内的资产分析更新的自动化和报告。同样地，通过将SCAP和XCCDF协议用于可扩展的核对表，可以确定设置、警告、用户指南和元数据。在安全引擎上是运行CMDB的内容/配置管理数据库，其可以基本上用作技术体系结构的轻型数据仓库，并且保持将在其它组件根据需要访问的资产的引用的依赖性相关日期。尽管SCAP和XCCDF协议提供报告和自动化资产分析的能力，但是安全引擎的机器学习组件被配置成执行包括允许生成分析和AI以实际执行评估的“智能”的功能。如下面更详细描述的，机器学习/AI组件的输入将是签名参考，被确定为所述签名的异常值的异常，与诸如策略、标准和基线或技术模式的已知训练数据集有关的人工输入。系统通过查找输入数据集或训练数据集的变体来训练，以确定基线或模式。由于所述基线，输出将是机器学习的。一个示例是使用决策树、支持向量、或经由训练数据集的交叉验证来确定输入体系结构或组件不符合嵌入系统中的基线。

[0064] 为降低安全风险而执行的示例操作

[0065] 现在参见图6，所提供的流程图示出了通过自动评估应用程序和执行安全策略来降低安全风险的一系列操作。如前所述，这些操作可以由企业计算平台102在诸如设备200的计算装置的协助下和/或在其控制下执行。在这方面，设备200配管安全引擎104并因此包括实现安全引擎104的功能的装置。

[0066] 在操作602中，设备200包括诸如输入/输出电路206、通信电路208等的装置，用于接收用于评估的建议体系结构。每个接收到的建议体系结构对应于设计用于与企业计算平台102接口的资产。建议体系结构可以包括具有能够在与资产接口时描述企业计算平台102的建议体系结构的任何格式的文档(例如，文档可以包括Visio图(.vsd)、Word文档(.doc)、Excel电子表格(.xls)、PowerPoint演示文稿(.ppt)等等、或者甚至是原始数据)。建议体系结构可以包括高级和系统级设计以及用于将资产集成到企业计算平台102中的功能性和非功能体系结构要求。

[0067] 在操作604中，设备200包括诸如风险评估电路210等等的装置，用于基于嵌入式企业安全策略、标准、基线和/或模式动态地评估建议体系结构。该操作可以使用一个或多个机器学习算法来执行，该算法使得能够解释用于安全评估的建议。在一些实施例中，该操作可以由实现安全引擎104的功能的风险评估电路210来执行。机器学习算法可以利用监督学习、无监督学习、回归算法(例如，可以基于模型进行的预测，例如，基于实例的算法和决策树算法、或贝叶斯算法)、关联规则学习算法(ARLA)(例如Apriori、Eclat等等)、深度学习或人工神经网络算法(反向传播、RBFN)。

[0068] 在操作606中，设备200包括诸如风险评估电路210等等的装置，用于确定建议体系

结构的动态评估是否包含可能违反为企业计算平台102建立的安全策略、标准、基线或模式的任何安全漏洞。在这方面，安全漏洞包括已知不符合企业计算平台102的安全策略、标准、基线或模式的建议体系结构的一个方面，或者安全引擎104(由风险评估电路210实现)不能确定合规状态的建议体系结构的一个方面。在识别出一个或多个安全漏洞的实例中，过程前进到操作608。然而，如果没有识别出安全漏洞，则过程直接前进到操作616，以生成关于建议体系结构的报告。

[0069] 在操作608中，设备200包括诸如风险评估电路210等等的装置，用于针对所识别的每个安全漏洞确定安全漏洞是否已知不合规或者其合规状态是否不能由安全引擎104确定。如果已知安全漏洞不合规，则过程前进到操作610，以确定可能修复安全漏洞的可能改变。如果安全漏洞是无法确定的状态，则过程前进到操作612，以请求人工干预。

[0070] 接下来参见操作610，设备200包括诸如风险评估电路210等等的装置，用于确定将修复安全漏洞的对建议体系结构的改变。在这方面，当安全引擎104能够识别不合规的安全漏洞时，该识别源于安全引擎104识别被违反的安全策略、标准、基线或模式的特定部分的能力。因此，在一些实施例中，确定将修复安全漏洞的对建议体系结构的改变可以参考被违反的策略、标准、基线或模式，并且识别违规的性质和(通过扩展)可以纠正违规的方式。在这方面，安全漏洞不合规可以由用于为企业生成策略、标准、基线和模式的输入(例如，数据训练集)或异常、签名集和基线相关的数据识别来确定企业的正常或允许的体系结构。因此，该操作可以实时或近实时地执行，而不是如人工实现类似特征所需的批处理或延迟过程执行。

[0071] 然而，如前所述，安全引擎104可能并不总是能够诊断出每个已识别的安全漏洞。在无法进行诊断的实例中，程序从操作608前进到操作612。在操作612中，设备200包括诸如输入/输出电路206、通信电路208等等的装置，用于调用关于将修复未诊断的安全漏洞的对建议体系结构的改变的人工干预。调用人工干预可以包括在接收到来自用户的请求的响应之后传送人工干预请求。如果用户提供来自单独的终端的响应，则这些数据传送可以经由设备200的输入/输出电路206或经由通信电路208进行。受益于该操作的机器学习系统的一个方面是每个否则未诊断的安全漏洞的用户诊断本身将包括训练输入，所述训练输入此后可以由安全引擎104用于预期地诊断建议体系结构的类似方面。以这种方式，虽然在最初利用安全引擎104时人工干预可能更常见，但随着时间的推移，它将变得越来越不必要，因为机器学习组件生成更大的训练数据集，可以挖掘这些数据以诊断稍后建议体系结构的所有方面。

[0072] 在操作614中，设备200包括诸如处理器202、存储器204、风险评估电路210等等的装置，用于确定是否已经识别出附加的安全漏洞，并且如果是，则过程返回到操作608，以处理所识别的安全漏洞的其余部分。然而，如果不是，则过程前进到操作616，以生成关于建议体系结构的报告。

[0073] 最后，在操作616中，设备200包括诸如通信电路208等等的装置，用于生成关于建议体系结构的报告。在这方面，所述报告可以包括描述在评估建议体系结构期间所识别的任何安全漏洞并且指示可能需要对建议体系结构进行哪些改变以修复那些安全漏洞的文档。

[0074] 在一些实施例中，报告可以不仅仅是单个文档，而是可以包括一系列文档(例如，

每个识别的安全漏洞的一个文档)。在其它实施例中,报告可以包括数据流而不是文档,并且数据流可以在批处理的过程中或者在近实时的情况下依次传送描述所识别的安全漏洞的信息,因为安全漏洞是由设备识别的。在这样的实施例中,数据流可以被传递到接收组件(例如,安全引擎104可以以顺序方式将这些改变传送到组件扫描器108),并且从那里可以由开发人员分析安全漏洞,以促进迭代解决在评估建议体系结构期间所识别的任何安全漏洞。通过以这种方式促进自动安全漏洞识别,示例实施例可以在包含Agile或DevOps安全性(也称为DevOpsSec)开发的组织内使用,该开发非常重视迭代改进和自动化。

[0075] Agile和DevOpsSec流程是指开发人员在小团队(即,协作小组)和短时间内协作构建解决方案但仍然可以产生高质量工程交付的流程。DevOpsSec允许开发人员、安全工程师、网络工程师、云工程师和其它人员在跨学科团队中协同工作,以便在管道中创建安全的开发解决方案。DevOpsSec/Agile体系结构通常是流动的,但通常包含开发人员使用的环境(在这种情况下,公共云)以及控制和/或管理风险的方法,例如上面关于识别安全漏洞的那些方法。此外,DevOpsSec或Agile体系结构可以利用开发管道和自动化工具,例如,称为Terraform的工具,其允许脚本自动化和分层访问。因此,DevOpsSec流程可以帮助开发人员在自助服务模型中提供可用的功能,具体取决于对任何给定层的访问权限和级别。

[0076] 具体地,通过提供自动安全漏洞识别,本文描述的示例实施例在某些明确定义的边界内建立安全性,允许实现这种自助服务和自动化,这产生了Agile和DevOps流程所需的更快的上市时间,同时还最小化了在安全性方面的漏洞,从而在可重复的过程中推动对体系结构的改进。换句话说,在操作616中数据流报告的使用通过向在工程流程运行期间和之后识别错误或遗漏的过程中移除人类元素的步骤移近一步来促进Agile和DevOpsSec流程的目标。

[0077] 此外,Agile或DevOpsSec体系结构中的示例实施例的使用通过揭示来自环境的附加的信息进一步参与本文所述的机器学习/深度学习能力,风险评估电路210可以使用该附加的信息来学习其风险评估过程的基线。具体地,因为DevOpsSec/Agile体系结构通常包含开发人员用户(可以是公共云)的环境,所以这样的体系结构可以解锁风险评估电路210对来自相应云服务提供商的更广泛的输入和变量的访问(例如,亚马逊或微软云平台),它深化了可以进行机器学习的数据集,从而可以更准确地对风险进行基线评估。

[0078] 在没有识别到安全漏洞的实例中,报告可能表明建议体系结构已经过验证,在这种情况下,在此过程完成之后,建议体系结构及其相应的资产将被确定为符合要求并且不需要任何修复,允许通过在企业体系结构中持续监控来集成此解决方案。

[0079] 如果建议体系结构表示对先前已经验证的资产的改变,则设备200可以使得报告传送到配备在已经改变的资产上的组件代理器310。如上所述,如果修复安全漏洞所需的对建议体系结构的改变被顺序地传送到组件扫描器108,则组件扫描器108自身可以将这些改变整理成报告以便传递给组件代理器310或者可以以顺序方式将这些改变中继给配备在与建议体系结构相关的资产上的组件代理器310。

[0080] 现在参见图7,提供了流程图,其示出了用于确保已经评估的变更资产不会引入新的安全漏洞的一系列操作。这些操作可以由企业计算平台102执行,该企业计算平台102可以例如包括设备200。在一些实施例中,设备200实现安全引擎104并且另外实现组件扫描器108。在这种情况下,即使同一设备200实现安全引擎104和组件扫描器108,应当理解,这两

个组件可以是由设备执行的不同操作元件，而不是单个应用程序的一部分。然而，应当理解，在一些其它实施例中，设备200实现安全引擎104但不实现组件扫描器108，而是与实现组件扫描器108的单独设备可操作地通信。在任何实施例中，组件扫描器108依次与配备在资产上的组件代理器310通信。

[0081] 在操作702中，设备200可以包括诸如通信电路208、风险评估电路210等等的装置，用于使得通过组件扫描器向配备在资产上的组件代理器传送一个或多个改变识别消息。在设备200包含组件扫描器以及安全引擎的实例中，该操作可以包括直接将改变识别消息传送到组件代理器。当然，在设备200本身不包含组件扫描器的实例中，该操作可以包括向组件扫描器传送消息，指示组件扫描器依次将改变识别消息传送给组件代理器。

[0082] 在操作704中，设备200可以包括诸如处理器202、通信电路208、风险评估电路210等等的装置，用于从组件代理器接收资产的体系结构的指示。与上面的操作702一样，操作704中采取的特定子步骤可以根据设备200本身是否包含组件扫描器而有所不同。

[0083] 在设备200包含组件扫描器以及安全引擎的实例中，操作704包括从组件代理器接收描述资产体系结构的消息，并且还包括评估资产体系结构以从先前由安全引擎评估过的体系结构的版本中识别资产体系结构的改变。

[0084] 替代性地，在设备200本身不包含组件扫描器的情况下，组件扫描器可以从组件代理器接收描述该体系结构的消息，并且可以从先前评估过的体系结构的版本中识别对资产体系结构的任何改变。在这种情况下，在操作704中，设备200可以简单地从组件扫描器接收关于资产体系结构是否已经从先前由安全引擎评估的体系结构的版本进行任何改变的指示。

[0085] 如操作706所示，在资产的体系结构已经改变的实例中，过程移动到操作602，以开始对改变的体系结构的新评估，以确保该改变没有引入安全漏洞。替代性地，在资产体系结构未改变的实例中，不需要执行进一步的动作并且过程可以结束。

[0086] 关于评估新资产或变更资产的示例

[0087] 以下场景示出了当用户希望将新资产集成到企业计算平台102中时可能发生的示例操作。在以下示例中，资产包括允许在企业计算平台102与用户的移动装置(例如，图1中的元件110、112或114)之间传送PHI、PII或PCI数据的新软件模块。对于前两个示例，将假设企业计算平台102的安全策略包括禁止PHI、PII或PCY数据的未加密传送。

[0088] 在第一示例中，结合新资产的建议体系结构促进了PCI数据在企业计算平台102与用户的移动装置之间的未加密传送。在操作602中，用户生成并提交包括该资产的建议体系结构，以供企业计算平台102评估。在操作604中，安全引擎针对嵌入式安全策略、标准、基线和模式动态地评估建议体系结构。在操作606中，企业计算平台102识别安全漏洞：建议体系结构将促进未加密的PCI数据传送。因此，过程前进到操作608，以确定该安全漏洞是否已知。它是，因此该过程前进到操作610以识别哪些改变可以修复该安全漏洞。在操作610中，企业计算平台102确定对要求加密传送PCI数据的建议体系结构的改变将修复问题并使得能够将资产与企业计算平台102一起使用。因为这是在本示例中识别的唯一安全漏洞，所以过程通过操作614前进到操作616，以生成给用户的指示必须对用于与企业计算平台102一起使用的资产加密PCI数据传送的报告。

[0089] 在第二示例中，包含新资产的建议体系结构促进了该数据在企业计算平台102与

用户的移动装置之间的加密传送。在这里，如在第一示例中，在操作602中，用户生成并提交包括该资产的建议体系结构，以供企业计算平台102评估。同样类似于第一示例，在操作604中，安全引擎针对企业计算平台102的嵌入式安全策略、标准、基线和模式动态地评估建议体系结构。然而，在操作606时，企业计算平台102没有识别安全漏洞：因为在本示例中，建议体系结构使用加密的PCI数据传送，因此，该建议没有问题。因此，过程直接前进到操作616，以生成给用户的指示资产被验证并且可以与企业计算平台102一起被使用的报告。

[0090] 在第三示例中，包含资产的建议体系结构促进了PCI数据在企业计算平台102与用户的移动装置之间的加密传送，但是使用了在企业计算平台102的安全策略、标准、基线或模式中未识别的一种加密类型。与前两个示例一样，在操作602中，用户生成并提交包括该资产的建议体系结构，以供企业计算平台102评估。在操作604中，安全引擎针对企业计算平台102的嵌入式安全策略、标准、基线和模式动态地评估建议体系结构。在操作606时，企业计算平台102识别安全漏洞：建议体系结构将促进加密的PCI数据传送，但加密协议未被识别。因此，过程前进到操作608，以确定该安全漏洞是否已知。因为加密协议未被识别，所以安全漏洞是未知的，并且过程前进到操作612以获取人工干预。在操作612中，人工干预可以指示两种情况中的一种：加密协议是足够安全的(在这种情况下没有安全漏洞)，或者加密协议不够安全并且建议体系结构毕竟确实包括安全漏洞。

[0091] 在加密协议不够安全的情况下，人工干预因此将可以提供对安全漏洞的确认，又可以识别将修复安全漏洞的体系结构的改变(替代加密方案的建议)。无论人工干预是否确认存在安全漏洞，这是在本示例中识别的唯一安全漏洞，并且过程通过操作614前进到操作616，以生成给用户的报告。如果没有安全漏洞，则报告验证资产以供企业计算平台102使用。但是，如果仍然存在安全漏洞，则报告指示加密方案所需的改变以使PCI数据传送能够与企业计算平台102一起使用。无论哪种方式，人工干预都代表另一个训练数据点，所述训练数据点随后被安全引擎104所摄取，以便在对未来建议体系结构的动态评估期间使用。

[0092] 最后，在第四示例中，当资产促进了敏感数据在企业计算平台102与用户的移动装置之间的加密传送时，资产已经被验证，但是对资产的体系结构的改变将使得某些类型的PCI数据能够未加密传送。作为初始事项，当资产被验证并与企业计算平台102结合使用时，本文描述的示例实施例可以要求资产在使用时具有存储在其上的组件代理器310，以促进资产与配备在企业计算平台102内并与安全引擎104通信的组件扫描器108之间的通信。因此，将执行以下过程。首先，在操作702中，组件扫描器108将改变识别消息传送到配备在资产上的组件代理器310。作为响应，组件代理器310传送资产的体系结构的指示。在操作706中，组件扫描器108将该当前体系结构与过去验证的资产的体系结构进行比较，并确定已经发生改变。因此，过程前进到操作602，其中组件扫描器108将改变的体系结构提交给安全引擎104，以用于分析。

[0093] 随后，在操作604中，安全引擎针对企业计算平台102的嵌入式安全性策略、标准、基线和模式动态地评估改变的体系结构。在操作606时，企业计算平台102识别安全漏洞：改变的体系结构将促进未加密的PCI数据传送。因此，过程前进到操作608，以确定该安全漏洞是否已知。它是，因此该过程前进到操作610，以识别哪些改变可以修复该安全漏洞。在操作610中，企业计算平台102确定对需要加密传送PCI数据的改变的体系结构的进一步改变将修复该问题并使得能够继续使用该资产与企业计算平台102。因为这是在本示例中唯一识

别的安全漏洞，过程通过操作614前进到操作616，以生成给用户的指示必须对用于继续与企业计算平台102一起使用的资产加密PCI数据传送的报告。

[0094] 如上所述，本发明的示例实施例使得能够提高企业计算平台的安全性。通过实施人工智能安全分析系统，示例实施例加快了安全漏洞识别的过程，同时提高了安全分析的一致性和新近促进了对可能引入企业计算平台的新资产和随着时间的推移而演变的现有资产的已识别的安全漏洞的修复。

[0095] 图6和7示出了根据本发明的示例实施例的设备、方法和计算机程序产品的操作的流程图。应该理解，流程图的每个块以及流程图中的块的组合可以通过诸如硬件、固件、处理器、电路和/或与包括一个或多个计算机程序指令的执行相关联的其它装置的各种装置来实现。例如，上述过程中的一个或多个可以由计算机程序指令来体现。在这方面，体现上述过程的计算机程序指令可以由采用本发明的实施例的设备的存储器存储，并由设备的处理器执行。可以理解，可以将任何这样的计算机程序指令加载到计算机或其它可编程设备(例如，硬件)上以产生机器，使得所得到的计算机或其它可编程设备实现流程图块中指定的功能。这些计算机程序指令也可以存储在计算机可读存储器中，所述计算机可读存储器可以指示计算机或其它可编程设备以特定方式起作用，使得存储在计算机可读存储器中的指令产生制造物品，执行它实现了流程图块中指定的功能。计算机程序指令也可以被加载到计算机或其它可编程设备上，以使得在计算机或其它可编程设备上执行一系列操作，以产生计算机实现的过程，使得在计算机或其它可编程设备上执行的指令提供用于实现流程图块中指定的功能的操作。

[0096] 因此，流程图的块支持用于执行指定功能的装置的组合和用于执行指定功能的操作的组合。应该理解，流程图中的一个或多个块以及流程图中的块的组合可以由执行指定的功能的基于专用硬件的计算机系统、或专用硬件和计算机指令的组合来实现。

[0097] 在一些实施例中，可以修改或进一步放大上述操作中的某些操作。此外，在一些实施例中，还可以包括附加的可选操作。可以以任何顺序和任何组合执行对上述操作的修改、放大或增加。

[0098] 如上所述，本发明的某些示例实施例针对用于改进传统计算装置的技术特性、能力和效率的改进的设备、方法和计算机可读介质。通过使用上面提到的基于数据的启发法，本文描述的实施例使得数据提取操作能够忽略包含无关信息的实验室报告的部分。以这种方式，本文描述的实施例提供了效率的提高，其增加了数据提取工作的吞吐量，并且使得能够生成更多最新的结构化数据集，以用于随后的精算用途(除其它之外)。

[0099] 受益于前述描述和相关附图中呈现的教导，本发明所属领域的技术人员将想到本文所阐述的本发明的许多修改和其它实施例。因此，应当理解，本发明不限于所公开的特定实施例，并且修改和其它实施例旨在包括在所附权利要求的范围内。此外，尽管前面的描述和相关联的附图在元件和/或功能的某些示例组合的上下文中描述了示例实施例，但是应该理解，在不脱离所附权利要求的范围的情况下，可以通过替代性的实施例提供元件和/或功能的不同组合。在这方面，例如，也可以设想不同于上面明确描述的元件和/或功能的元件和/或功能的不同组合，如可以在所附权利要求中的一些中阐述的。尽管本文采用了特定术语，但它们仅用于一般性和描述性意义，而不是用于限制的目的。

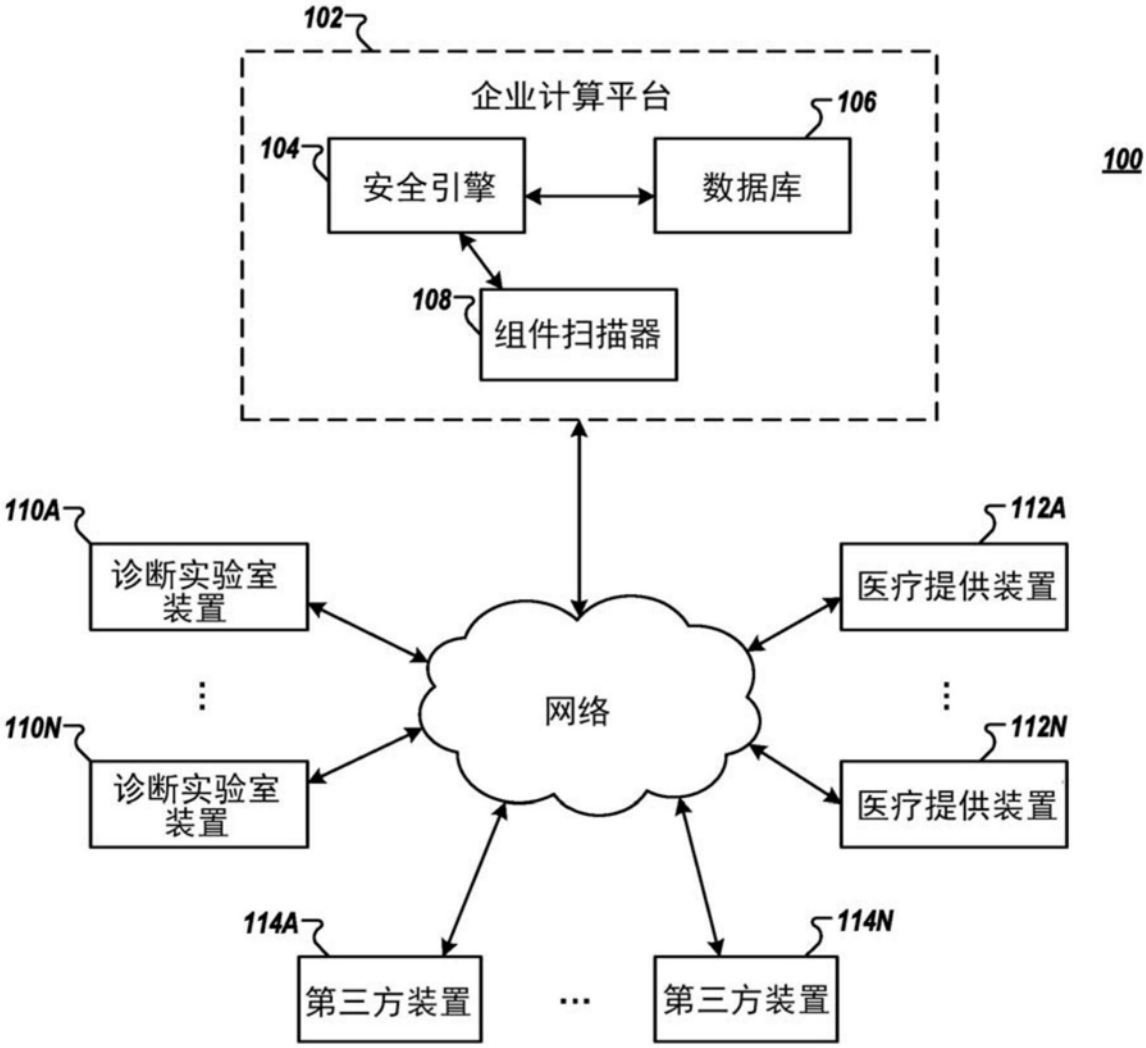

102
企业计算平台
106
104
安全引擎
数据库
100
108
组件扫描器
110A
诊断实验室装置
112A
医疗提供装置
网络
110N
诊断实验室装置
112N
医疗提供装置
114A
第三方装置
114N
第三方装置

图1

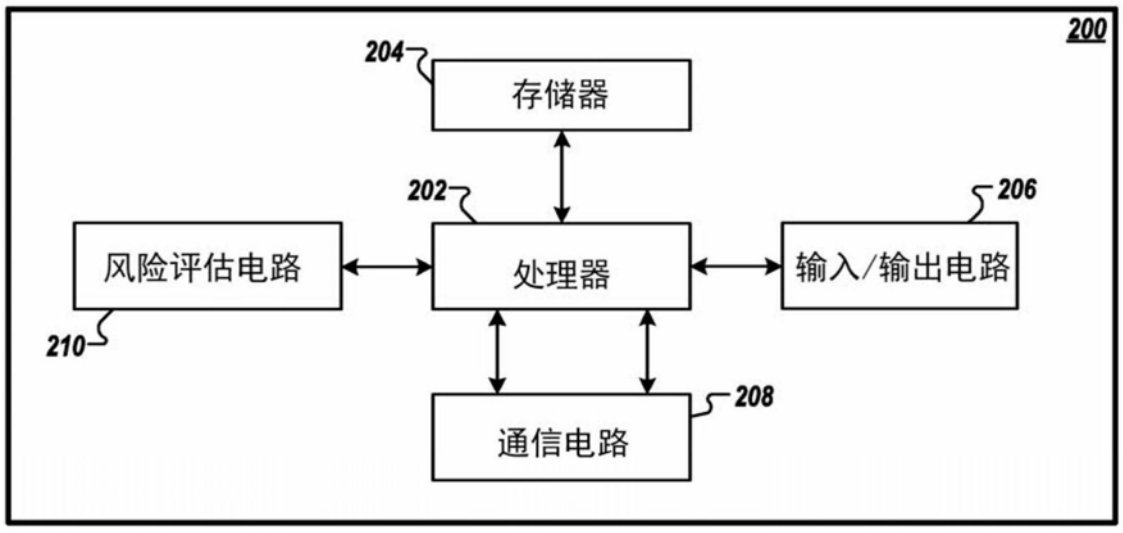

200
204
存储器
202
206
风险评估电路
处理器
输入/输出电路
210
208
通信电路

图2

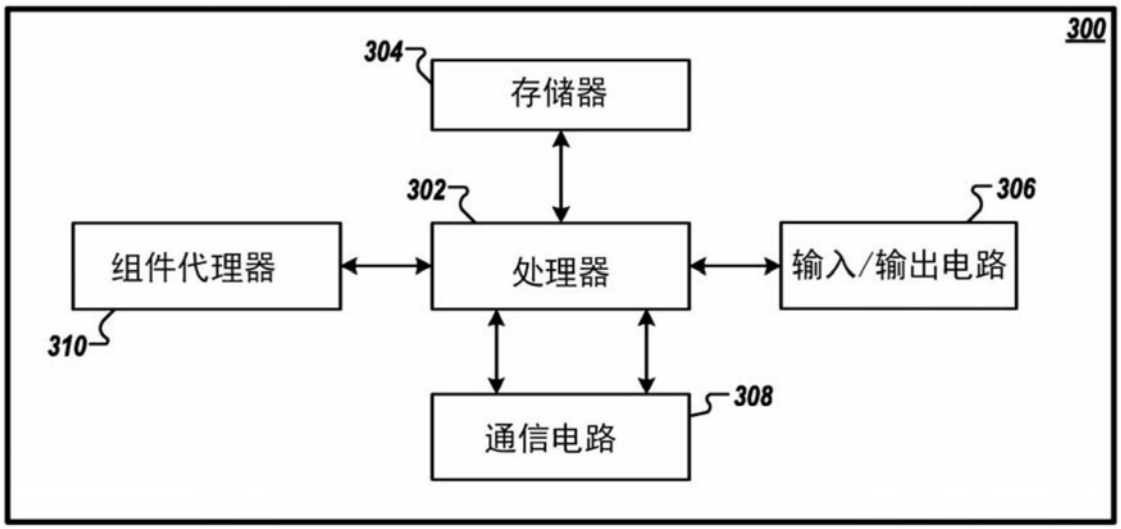


图3

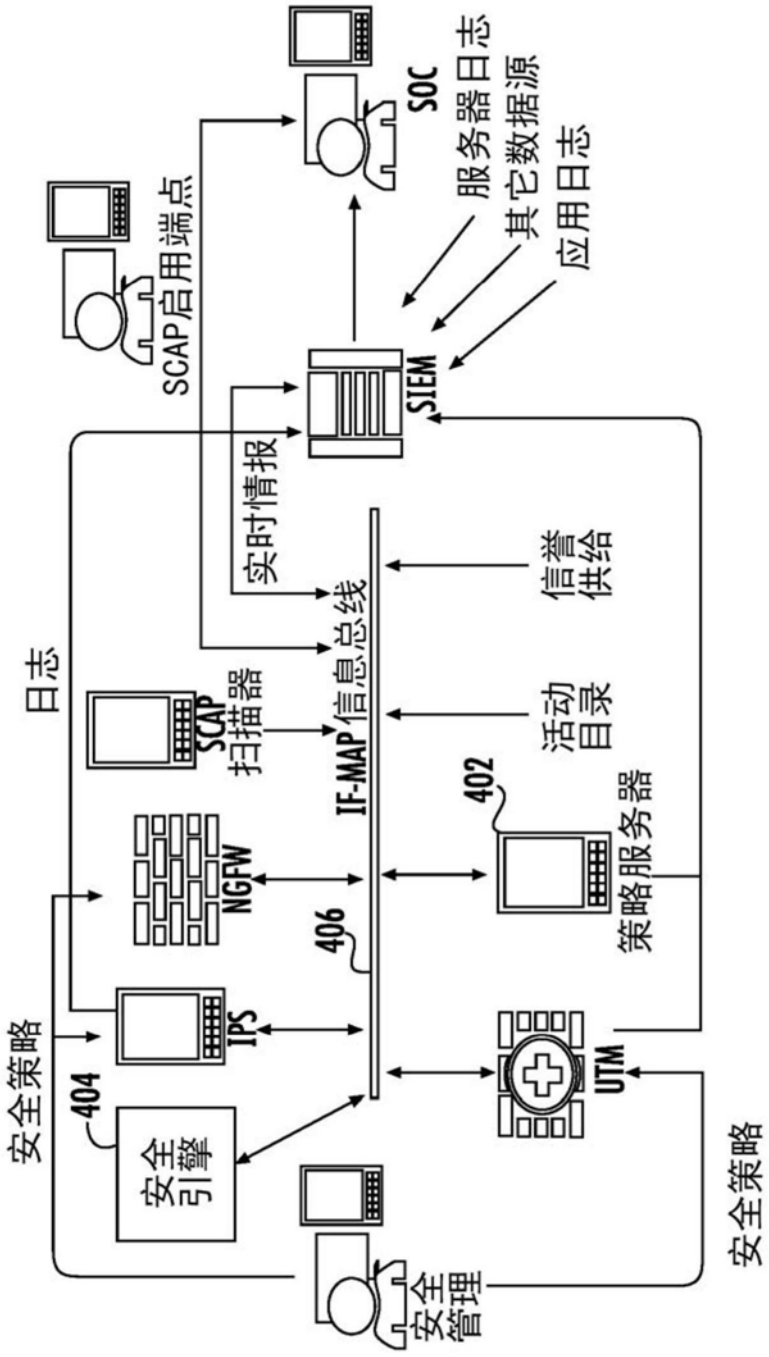

SOC
服务器日志
其它数据源
应用日志
SCAP启用端点
SIEM
实时情报
信誉
供给
日志
SCAP
扫描器
IF-MAP信息总线
活动
目录
402
NGFW
策略服务器
406
IPS
安全策略
404
安全
引擎
UTM
安全策略
安全
管理

图4

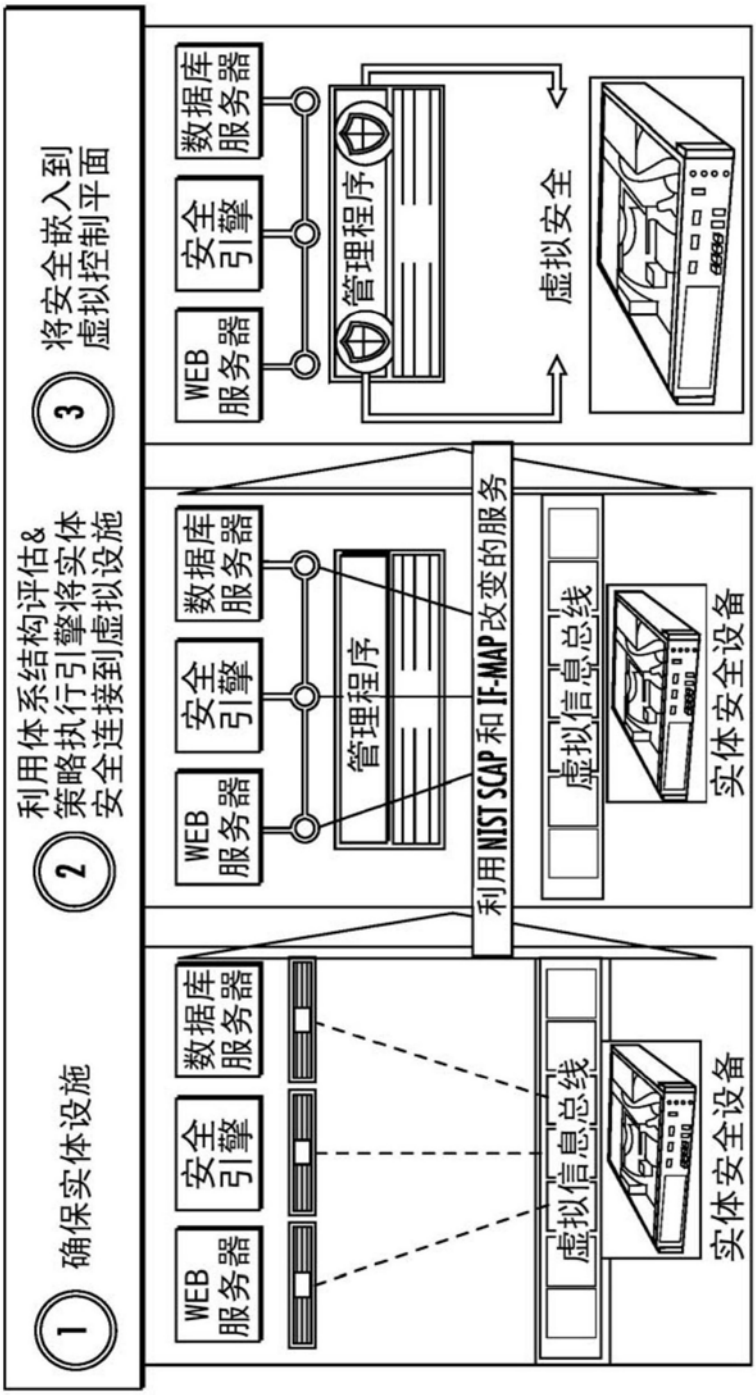

1
确保实体设施
2
利用体系结构评估&
策略执行引擎将实体
安全连接到虚拟设施
3
将安全嵌入到
虚拟控制平面
WEB
服务器
安全
引擎
数据库
服务器
虚拟信息总线
实体安全设备
利用NIST SCAP和IF-MAP改变的服务
管理程序
虚拟安全

图5

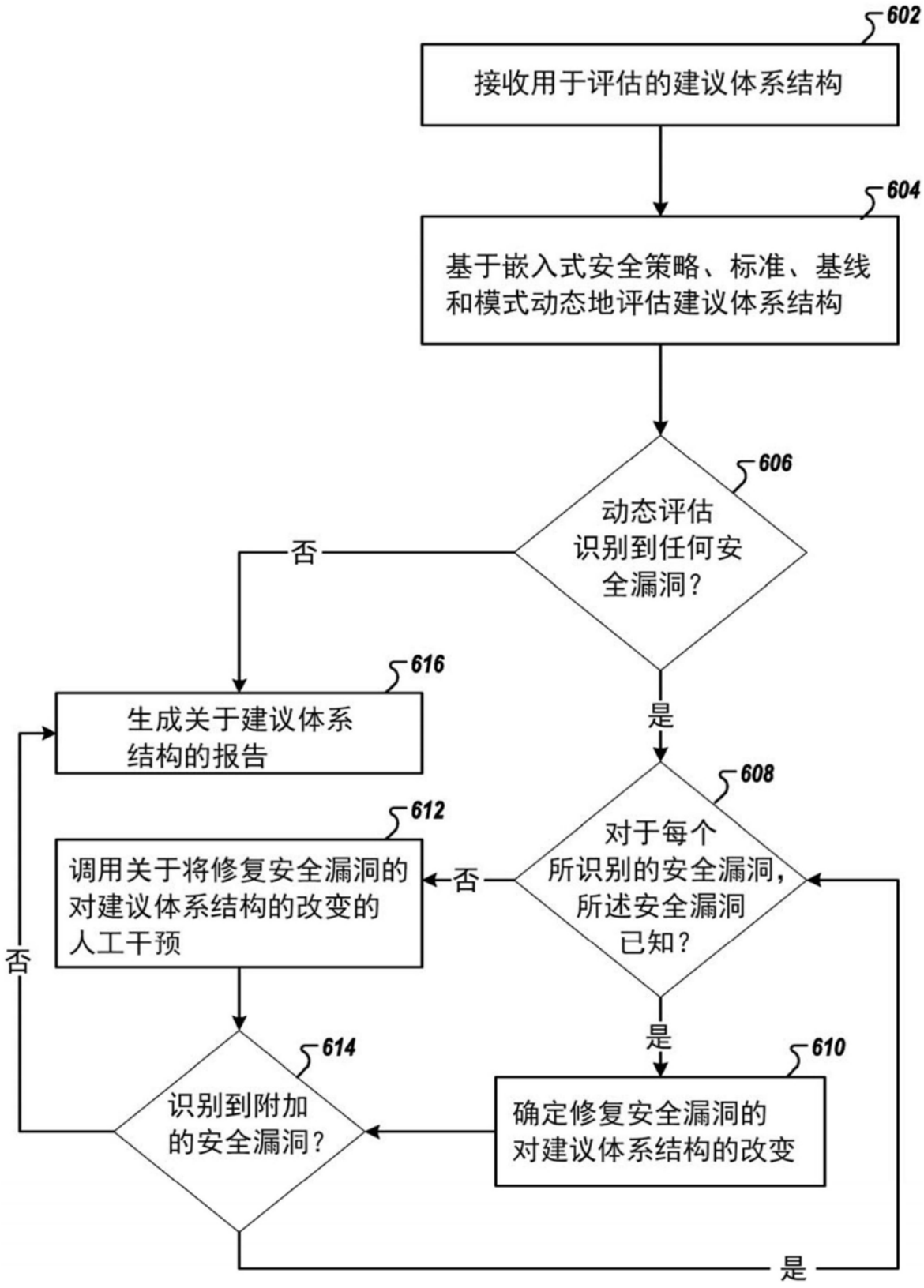

602
接收用于评估的建议体系结构
604
基于嵌入式安全策略、标准、基线和模式动态地评估建议体系结构
606
动态评估识别到任何安全漏洞？
否
是
616
生成关于建议体系结构的报告
608
对于每个所识别的安全漏洞，所述安全漏洞已知？
否
612
调用关于将修复安全漏洞的对建议体系结构的改变的人工干预
是
610
确定修复安全漏洞的对建议体系结构的改变
614
识别到附加的安全漏洞？
否
是

图6

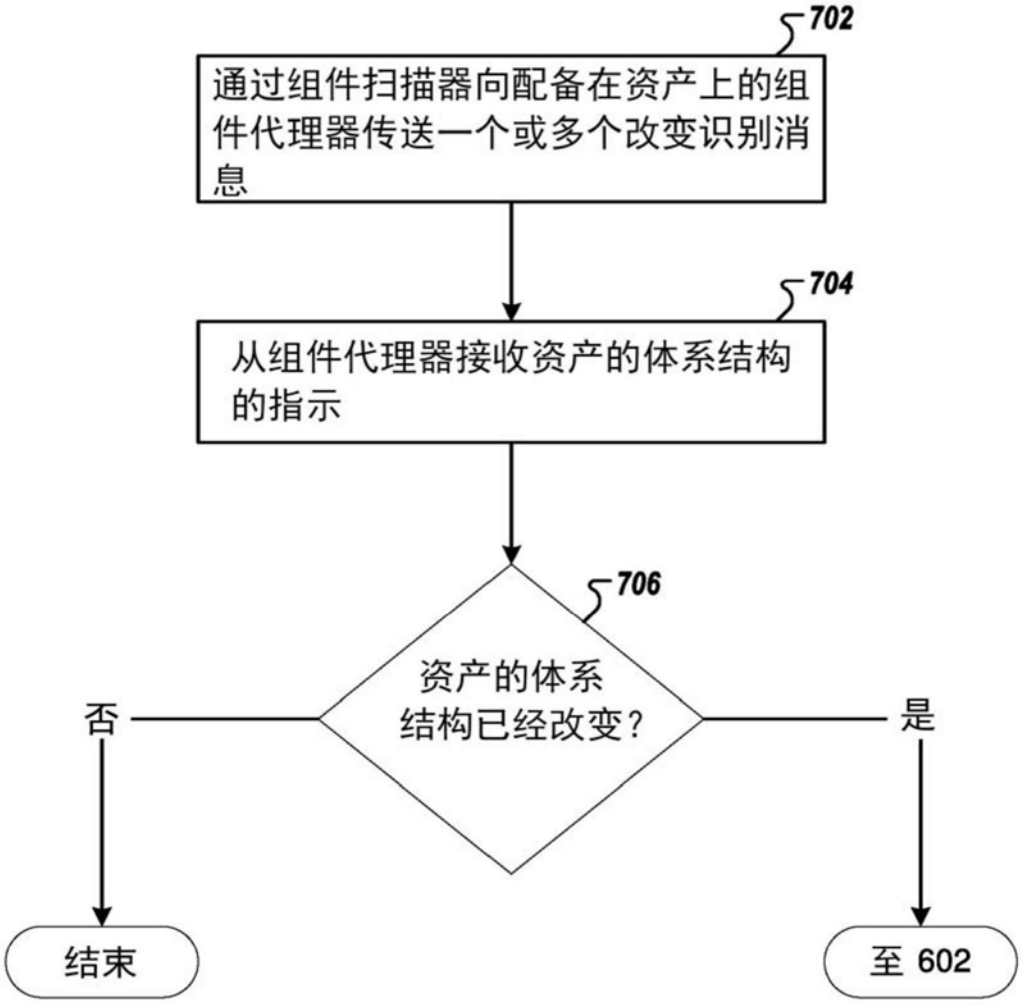

702
通过组件扫描器向配备在资产上的组件代理器传送一个或多个改变识别消息
704
从组件代理器接收资产的体系结构的指示
706
资产的体系结构已经改变?
否
是
结束
至 602

图7