(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108702367 B
(45)授权公告日 2021.08.24

(21)申请号 201780013155.0
(22)申请日 2017.02.24
(65)同一申请的已公布的文献号
申请公布号 CN 108702367 A
(43)申请公布日 2018.10.23
(30)优先权数据
62/300,715 2016.02.26 US
62/460,716 2017.02.17 US
15/441,154 2017.02.23 US
(85)PCT国际申请进入国家阶段日
2018.08.24
(86)PCT国际申请的申请数据
PCT/US2017/019508 2017.02.24
(87)PCT国际申请的公布数据
WO2017/147525 EN 2017.08.31
(73)专利权人 甲骨文国际公司
地址 美国加利福尼亚
(72)发明人 G·基尔提 K·比斯瓦斯
S·N·佩雷拉 A·F·西穆
(74)专利代理机构 中国贸促会专利商标事务所有限公司 11038
代理人 张鑫
(51)Int.Cl.
H04L 29/06(2006.01)
(56)对比文件
US 2015347748 A1,2015.12.03
US 2012304249 A1,2012.11.29
US 8495746 B2,2013.07.23
CN 104246785 A,2014.12.24
CN 103180862 A,2013.06.26
CA 2953394 A1,2015.12.30
US 2015319185 A1,2015.11.05
审查员 翟倩倩

权利要求书4页 说明书47页 附图31页

(54)发明名称

用于安全管理的计算机实现的方法、系统及可读介质

(57)摘要

公开了用于在组织的计算环境中发现和管理应用的技术。安全管理系统发现在计算环境中应用的使用以管理对应用的访问,以最小化组织的计算环境中的安全威胁和风险。安全管理系统能够获得关于网络流量的网络数据以识别唯一的应用。安全管理系统能够执行分析和关联,包括使用一个或多个数据源,以确定关于应用的信息。系统能够计算应用的安全性的测量("应用风险得分")和用户的安全性的测量("用户风险得分")。得分可以被分析,以基于应用的使用来确定应用造成的安全威胁。安全系统能够执行一条或多条指令来配置应用允许的访问,无论该访问是被拒绝还是受限制。

CN 108702367 B

1.一种用于安全管理的计算机实现的方法,包括在安全管理系统的计算机系统处:

获得关于在组织的网络上与客户端设备关联的网络活动的数据,其中,网络活动在客户端设备操作为组织的网络的一部分时被生成;

使用关于网络活动的数据来识别在客户端设备操作为组织的网络的一部分时已被客户端设备访问的应用,其中,应用由服务提供者的网络提供给客户端设备,其中组织的网络和服务提供者的网络是不同的网络;

使用关于网络活动的数据来确定与应用关联的访问信息,其中,访问信息包括指示从客户端设备访问应用的网络活动;

使用访问信息来确定关于应用的域信息,其中域信息包括关于服务提供者的信息;

使用域信息来确定关于应用的安全信息,其中,安全信息包括描述与应用关联的安全威胁的一个或多个指示符;

使用安全信息来计算应用的安全性的测量;以及

通过基于所述安全性的测量应用安全策略来执行针对应用的补救动作。

2.如权利要求1所述的计算机实现的方法,其中安全信息包括第一值和第二值,第一值是应用的第一安全威胁的第一指示符,第二值是应用的第二安全威胁的第二指示符,其中第一指示符是从第一数据源获得的,并且其中第二指示符是从第二数据源获得的。

3.如权利要求2所述的计算机实现的方法,其中计算所述安全性的测量包括:

计算基于将第一值乘以第一权重值的第一加权值;

计算基于将第二值乘以第二权重值的第二加权值;

计算基于第一加权值和第二加权值的求和的第一总和;以及

计算基于第一权重值和第二权重值的求和的第二总和,其中所述安全性的测量是基于将第一总和除以第二总和而计算的值。

4.如权利要求3所述的计算机实现的方法,其中第一权重值不同于第二权重值,并且其中第一值不同于第二值。

5.如权利要求1或2中任一项所述的计算机实现的方法,其中获得关于网络活动的数据包括从组织的网络上的一个或多个网络设备获得网络数据,其中组织的网络在组织的计算环境中受到保护,该计算环境不受公共网络的危害。

6.如权利要求1或2中任一项所述的计算机实现的方法,还包括:

为应用确定组织信息;以及

生成显示关于应用的信息的图形界面,其中关于应用的信息是基于组织信息和为应用计算的所述安全性的测量来显示的,并且其中图形界面指示针对应用执行的补救动作。

7.如权利要求1或2中任一项所述的计算机实现的方法,其中关于网络活动的数据用于组织的网络上的通信,其中识别应用包括处理数据以识别与对应用的请求对应的通信,并且其中所述通信指示关于对应用的请求的应用信息,应用信息用于将应用识别为被客户端设备访问。

8.如权利要求7所述的计算机实现的方法,其中使用所述通信来确定访问信息,并且其中访问信息指示网络活动的时间戳、提供应用的系统的互联网协议(IP)地址、用于访问应用的设备的介质访问控制(MAC)地址、以及关于客户端设备的用户的用户信息。

9.如权利要求1或2中任一项所述的计算机实现的方法,其中访问信息指示提供应用的

系统的互联网协议(IP)地址,其中确定域信息包括基于应用的IP地址对与托管应用的域对应的域信息执行查询。

10.如权利要求1或2中任一项所述的计算机实现的方法,其中访问信息指示应用的源信息,该源信息指示由主机提供的应用的位置,并且其中确定域信息包括基于应用的源信息向主机发送对应用的证书的请求。

11.如权利要求1或2中任一项所述的计算机实现的方法,其中应用安全策略包括确定所述安全性的测量是否满足应用的风险阈值,并且其中补救动作是配置组织的网络以防止在客户端设备在组织的网络上操作时从客户端设备访问应用。

12.如权利要求1或2中任一项所述的计算机实现的方法,其中关于网络活动的数据包括与多个用户关联的网络活动,其中所述多个用户是组织的网络上的租户,并且其中补救动作是防止应用被所述多个用户访问。

13.如权利要求1或2中任一项所述的计算机实现的方法,其中针对应用的补救动作包括:

生成图形界面;以及

使图形界面显示请求调整应用的配置操作的提示,其中,所述调整基于应用于所述安全性的测量的安全策略。

14.一种安全管理系统,包括:

一个或多个处理器;以及

所述一个或多个处理器可访问的存储器,其中存储器存储一条或多条指令,所述一条或多条指令在由所述一个或多个处理器执行时使所述一个或多个处理器执行包括以下的操作:

获得关于在组织的网络上与客户端设备关联的网络活动的数据,其中,网络活动在客户端设备操作为组织的网络的一部分时被生成;

使用关于网络活动的数据来识别在客户端设备操作为组织的网络的一部分时已被客户端设备访问的应用,其中,应用由服务提供者的网络提供给客户端设备,其中组织的网络和服务提供者的网络是不同的网络;

使用关于网络活动的数据来确定与应用关联的访问信息,其中,访问信息包括指示从客户端设备访问应用的网络活动;

使用访问信息来执行对与应用关联的域信息的一个或多个查询;

确定关于应用的安全信息,其中,安全信息包括描述与应用关联的安全威胁的一个或多个指示符;

使用域信息和安全信息来计算应用的安全性的测量;以及

通过基于所述安全性的测量应用安全策略来执行针对应用的补救动作。

15.如权利要求14所述的安全管理系统,其中安全信息包括第一值和第二值,第一值是应用的第一安全威胁的第一指示符,第二值是应用的第二安全威胁的第二指示符,并且其中计算所述安全性的测量包括:

计算基于将第一值乘以第一权重值的第一加权值;

计算基于将第二值乘以第二权重值的第二加权值;

计算基于第一加权值和第二加权值的求和的第一总和;以及

计算基于第一权重值和第二权重值的求和的第二总和，其中所述安全性的测量是基于将第一总和除以第二总和而计算的值。

16.一种用于安全管理的计算机实现的方法，包括在安全管理系统的计算机系统处：

从第一服务提供者系统获得关于第一应用的第一数据，其中第一应用被从第一服务提供者系统访问，并且其中对第一应用的访问与用户账户关联；

从第二服务提供者系统获得关于第二应用的第二数据，其中第二应用被从第二服务提供者系统访问，并且其中对第二应用的访问与所述用户账户关联；

使用第一数据和第二数据来确定所述用户账户已访问的第三应用的访问信息；

使用访问信息搜索关于提供第三应用的提供者系统的域信息；

确定关于第三应用的安全信息；

使用域信息和安全信息来计算第三应用的安全性的测量；以及

通过基于所述安全性的测量应用安全策略来执行针对第三应用的补救动作。

17.如权利要求16所述的计算机实现的方法，其中第一服务提供者系统不同于第二服务提供者系统，其中第一服务提供者系统提供对第一应用的访问作为第一云服务，并且其中第二服务提供者系统提供对第二应用的访问作为第二云服务。

18.如权利要求16或17中任一项所述的计算机实现的方法，还包括：

为第三应用确定组织信息；以及

生成显示关于第三应用的信息的图形界面，其中基于组织信息和为第三应用计算的所述安全性的测量来显示关于第三应用的信息，并且其中图形界面指示针对第三应用执行的补救动作。

19.如权利要求16或17中任一项所述的计算机实现的方法，其中第一数据指示用户账户已经通过第三应用访问了第一应用，其中第二数据指示用户账户已经通过第三应用访问了第二应用，并且其中确定访问信息包括确定已经访问了第三应用以提供对第一应用和第二应用的访问。

20.如权利要求16或17中任一项所述的计算机实现的方法，其中安全信息包括第一值，该第一值是第三应用的第一安全威胁的第一指示符，并且安全信息包括第二值，该第二值是第三应用的第二安全威胁的第二指示符，其中第一指示符是从第一源获得的，其中第一值不同于第二值，其中第二指示符是从第二源获得的，并且其中计算所述安全性的测量包括：

计算基于将第一值乘以第一权重值的第一加权值；

计算基于将第二值乘以第二权重值的第二加权值，其中第一权重值不同于第二权重值；

计算基于第一加权值和第二加权值的求和的第一总和；以及

计算基于第一权重值和第二权重值的求和的第二总和，其中所述安全性的测量是基于将第一总和除以第二总和而计算的值。

21.一种非瞬态计算机可读介质，包括存储在其上的指令，所述指令在处理器上执行时执行如权利要求1-13或权利要求16-20中任一项所述的方法。

22.一种安全管理系统，包括：

一个或多个处理器；以及

所述一个或多个处理器可访问的存储器，其中存储器存储一条或多条指令，所述一条或多条指令在由所述一个或多个处理器执行时使所述一个或多个处理器执行如权利要求1-13或权利要求16-20中任一项所述的方法。

23.一种安全管理系统，包括用于执行如权利要求1-13或权利要求16-20中任一项所述的方法的装置。

用于安全管理的计算机实现的方法、系统及可读介质

[0001] 相关申请的交叉引用

[0002] 本申请要求于2017年2月23日提交的标题为“TECHNIQUES FOR DISCOVERING AND MANAGING SECURITY OF APPLICATIONS”的美国非临时专利申请No.15/441,154[代理人案卷号:088325-1032871(185500US)]的优先权和权益,该申请要求以下每项专利申请的优先权和权益:

[0003] 1)于2016年2月26日提交的标题为“Systems and Methods for Discovering and Monitoring Unsanctioned Enterprise Assets”的美国临时申请No.62/300,715[代理人案卷号:088325-1032870(185501US)];以及

[0004] 2)于2017年2月17日提交的标题为“Systems and Methods for Discovering and Monitoring Unsanctioned Enterprise Assets”的美国临时申请No.62/460,716[代理人案卷号:088325-1039197(185502US)]。

[0005] 上述每个专利申请的全部内容通过引用并入本文,用于所有意图和目的。

背景技术

[0006] 组织可以依赖许多技术设备、软件、硬件和/或计算服务来实现计算环境(例如,企业计算环境)。这些计算环境越来越多地被实现为或使用“云”环境。“云”环境可以表示本地和远程托管的计算资源和系统的集合体。术语“云计算”指的是通过网络的分布式计算的各个方面。云计算环境可以实现各种服务模型,包括基础设施即服务 (IaaS)、平台即服务(PaaS)、软件即服务(SaaS)和网络即服务(NaaS)。“云”还可以指单个服务提供者的数据存储和客户端应用。许多应用可以实现云计算环境,以使设备能够获得超出仅仅设备本身上可用的附加功能或能力。可以使用一个或多个服务提供者 (本文也称为“提供者”)来实现这样的应用,每个服务提供者具有一个或多个使用一个或多个计算机系统的服务提供者系统(本文也称为“提供者系统”)。此类服务提供者的示例可以包括诸如Box、Dropbox、Microsoft、Docusign、Salesforce、Oracle、Amazon等公司。每个服务提供者可以提供许多不同的应用或功能,从而使得能够访问作为基于云的服务的应用和/或数据。

[0007] 对计算环境的依赖导致组织广泛使用授权或未授权的应用。授权应用可以是在组织中注册或组织已知的应用。在一些情况下,可以通过组织分发来授权应用。未授权的应用可以是未知的和/或未与组织关联或注册的应用。未经批准的应用可以包括独立于其它应用操作的应用以及作为插件或附件集成到经批准(IT管理)应用中的第三方集成应用。无论是授权还是未授权,许多应用都会给组织的计算环境带来很大的安全风险。安全风险包括以不安全的方式暴露于组织的专用网络或访问私人机密数据,这些数据应通过安全控制进行限制。造成安全风险的应用可以在或可以不在组织的管理之下。照此,这些应用可以以“影子”或隐藏的方式被操作,未知和/或不受组织监管以进行安全控制。另外,未知的应用使用可以导致计算资源(诸如带宽和数据存储装置)的低效和过度使用。未被发现的使用可以影响组织的计算环境中的性能和对关键资源的访问。

[0008] 可以以未授权的方式从服务提供者访问以不受监管的方式操作的应用。例如,组

织的销售人员可以在他的移动设备中使用未经批准的文件共享应用来共享电子表格给他的团队成员以进行协作，而不是通过电子邮件发送。虽然使用此类应用可以提高生产力，但它也会带来安全风险以及组织中的合规性问题。例如，如果应用不够安全，那么具有业务敏感信息的机密文件会容易受到信息泄露的影响。由于这些应用未经组织评估，因此它们不准备对安全漏洞采取行动。而且，一些看似有用的应用可能会故意或不知不觉地分发广告软件甚至恶意软件。许多组织尝试阻止此类应用或网站，但这会使员工因生产力的影响而感到不快。而且，员工尝试绕过这样的障碍，例如，使用外部 VPN服务、移动数据服务等等。但是，组织中的计算环境的管理需要对所有正在使用的应用的可见性，以便他们可以主动地监视和控制可疑或恶意应用。

发明内容

[0009] 本公开一般而言涉及管理计算环境中的安全性，并且更具体而言涉及用于在组织的计算环境中发现和管理应用的技术。这些技术可以使组织能够监视和管理对应用的访问，以最小化组织的计算环境中的安全威胁和风险。发现应用的使用可以使组织有效地监视和管理资源的效率和消耗，由此增强组织的计算环境的性能。

[0010] 安全监视和控制系统(也称为“安全系统”和“安全管理系统”) 可以发现网络或组织内的应用的使用。可以利用各种源(包括但不限于第三方数据源、网络流量和服务提供者系统)来识别在组织的网络中被访问的唯一的应用。安全监视和控制系统可以以分布式方式实现，包括网络上的代理，以发现应用使用。安全监视和控制系统可以与分布式计算系统(诸如多个服务提供者系统(例如，云服务提供者系统))通信，以访问关于在用于组织的设备上使用的应用的数据。安全监视和控制系统可以获得关于网络流量的网络数据，以识别唯一的应用。这些技术可以对在组织中使用的应用的活动提供深入的可见性，这可以有助于检测组织的计算环境中关于应用使用和用户行为方面的异常或新出现的威胁。

[0011] 安全监视和控制系统可以执行分析和关联，包括使用一个或多个数据源，以确定关于应用的信息。信息可以包括关于应用提供者的组织信息。信息可以包括关于应用的安全风险指示符的安全信息。信息可以包括与应用的使用相关的特征的一个或多个指示符(例如，值)，诸如安全性方面。关于应用的信息可以被用于计算应用的安全性测量 (“应用风险得分”)和用户(“用户风险得分”)。可以使用一条或多条信息(例如，指示符)与每条信息的权重值属性组合来计算安全性的测量。可以关于安全策略来分析得分，以基于应用的使用来确定由应用或用户提出的安全威胁。

[0012] 在一些实施例中，可以向用户(例如，安全管理员)提供图形界面，以查看关于应用的使用的信息。该信息可以提供关于应用的服务提供者的细节和/或不同类型的安全风险的可视化，并且可以指示针对每个安全风险的严重性的测量。图形界面可以是交互式的，以基于关于每个安全风险的安全策略来配置要执行的补救动作。对于通过未知的应用使用而难以识别和管理安全风险的组织，图形界面可以使组织能够高效且可靠地发现所有(如果不是大多数)应用的使用，以便在计算环境中最小化安全风险并最大化计算相关资源的资源消耗。在至少一个实施例中，安全监视和控制系统可以被配置为评估与应用使用相关的风险，以自动确定风险的严重性。基于风险的严重性，安全监视和控制系统可以执行一条或多条指令，以配置应用允许的访问，无论该访问是被拒绝还是受限制。

[0013] 在一些实施例中，安全监视和控制系统(也称为安全系统或安全管理系统)可以包括计算机系统，并且可以被配置为实现本文公开的方法和操作。计算机系统可以包括一个或多个处理器和一个或多个处理器可访问并存储一条或多条指令的一个或多个存储器，这些指令在由一个或多个处理器执行时使一个或多个处理器实现本文公开的方法和/或操作。还有其它实施例涉及系统和非瞬态机器可读有形存储介质，其采用或存储用于本文公开的方法和操作的指令。在一些实施例中，可以实现包括存储在其上的指令的非瞬态计算机可读介质，使得当指令在处理器上执行时，可以执行本文公开的方法。在一些实施例中，本文公开了一种系统，包括：一个或多个处理器；以及一个或多个处理器可访问的存储器，其中存储器存储一条或多条指令，这些指令在由一个或多个处理器执行时使得一个或多个处理器执行本文公开的方法。在一些实施例中，公开了一种包括用于执行本文公开的任何方法的装置的系统。

[0014] 在至少一个实施例中，公开了一种在安全管理系统的计算机系统中的计算机实现的方法。所有步骤都可以由安全管理系统执行。该方法可以包括获得关于用户在组织的网络上的网络活动的数据。该方法可以包括使用关于网络活动的数据来识别用户已经在网络上访问的应用。该方法可以包括使用关于网络活动的数据来确定关于与用户已经访问的应用对应的网络活动的访问信息。该方法可以包括使用访问信息搜索关于应用的域信息。该方法可以包括确定关于应用的安全信息。该方法可以包括使用安全信息计算用于已经访问的应用的安全性的测量。该方法可以包括通过基于安全性的测量应用安全策略来执行针对该应用的补救动作。

[0015] 在一些实施例中，安全信息包括第一值，该第一值是应用的第一安全威胁的第一指示符，并且包括第二值，该第二值是应用的第二安全威胁的第二指示符。第一指示符可以从第一数据源获得。第二指示符可以从第二数据源获得。

[0016] 计算安全性的测量可以包括计算基于将第一值乘以第一权重值的第一加权值；计算基于将第二值乘以第二权重值的第二加权值；计算基于第一加权值和第二加权值的总和的加权总和；并且计算基于第一权重值和第二权重值的总和的权重总和。安全性的测量可以是基于将加权总和除以权重总和而计算的值。在一些实施例中，第一权重值不同于第二权重值。在一些实施例中，第一值不同于第二值。

[0017] 在一些实施例中，获得关于网络活动的数据包括从网络上的一个或多个网络设备获得网络数据。网络可以在组织的计算环境中被保护。计算环境可以不受公共网络的危害。

[0018] 在一些实施例中，该方法可以包括确定应用的组织信息并生成显示关于应用的信息的图形界面，其中关于应用的信息是基于组织信息和为应用计算的安全性的测量来显示的。图形界面可以指示为应用执行的补救动作。在一些实施例中，组织信息是关于提供应用的实体，并且组织信息可以指示关于应用的一个或多个属性。

[0019] 在一些实施例中，所获得的数据用于网络上的通信。识别应用可以包括处理数据，以识别数据的与对用户访问的应用的请求对应的部分。数据的该部分可以指示关于对应用的请求的应用信息。应用信息可以用于将应用识别为由用户访问。在一些实施例中，可以使用数据的该部分来确定关于与应用对应的网络活动的访问信息。访问信息可以指示应用的网络活动的时间戳、提供应用的系统的IP地址、用于访问应用的设备的介质访问控制(MAC)地址，以及关于用户的用户信息。在一些实施例中，访问信息指示提供应用的系统的IP地

址。搜索域信息包括基于第一应用的IP地址对与托管该应用的域对应的域信息执行查询。在一些实施例中，访问信息指示应用的源信息，该源信息指示由主机提供的应用的位置。搜索域信息可以包括基于应用的源信息向主机发送对应用的证书的请求。

[0020] 在一些实施例中，基于安全性的测量应用安全策略包括确定安全性的测量是否满足应用的风险阈值。补救动作可以是配置网络以防止应用在网络上被用户访问。

[0021] 在一些实施例中，所获得的数据进一步关于作为组织在网络上的租户的多个用户的网络。该多个用户可以包括所述用户。补救动作是防止多个用户访问应用。

[0022] 在一些实施例中，针对应用的补救动作包括使图形界面基于应用于安全性的测量的安全策略来提示用户调整应用的配置操作。

[0023] 在一些实施例中，公开了在安全管理系统的计算机系统处的计算机实现的方法。所有步骤都可以由安全管理系统执行。该方法可以包括从第一服务提供者系统获得关于用户从第一服务提供者系统访问的第一应用的第一数据。该方法可以包括从第二服务提供者系统获得关于用户从第二服务提供者系统访问的第二应用的第二数据。该方法可以包括使用第一数据和第二数据来确定用户已访问的第三应用的访问信息。该方法可以包括使用访问信息搜索关于提供第三应用的提供者系统的域信息。该方法可以包括确定关于第三应用的安全信息。该方法可以包括使用安全信息来计算已被访问的第三应用的安全性的测量。该方法可以包括通过基于安全性的测量应用安全策略来执行针对第三应用的补救动作。在一些实施例中，第一应用不同于第二应用。第一服务提供者系统不同于第二服务提供者系统。第一服务提供者系统可以提供对第一应用的访问作为第一云服务。第二服务提供者系统可以提供对第二应用的访问作为第二云服务。

[0024] 在一些实施例中，该方法可以包括确定第三应用的组织信息；并生成显示关于第三应用的信息的图形界面。可以基于组织信息和为第三应用计算的安全性的测量来显示关于应用的信息。图形界面可以指示针对第三应用执行的补救动作。

[0025] 在一些实施例中，第一数据指示用户已经通过第三应用访问了第一应用。第二数据可以指示用户已经通过第三应用访问了第二应用。确定访问信息可以包括确定已经访问了第三应用以提供对第一应用和第二应用的访问。

[0026] 在一些实施例中，安全信息包括第一值，该第一值是应用的第一安全威胁的第一指示符，并且包括第二值，该第二值是应用的第二安全威胁的第二指示符。第一指示符可以从第一数据源获得。第一值不同于第二值。第二指示符从第二数据源获得。可以通过以下方式计算安全性的测量：计算基于将第一值乘以第一权重值的第一加权值；计算基于将第二值乘以第二权重值的第二加权值，其中第一权重值不同于第二权重值；计算基于第一加权值和第二加权值的总和的加权总和；并且计算基于第一权重值和第二权重值的总和的权重总和。安全性的测量可以是基于将加权总和除以权重总和而计算的值。

[0027] 通过参考以下说明书、权利要求书和附图，前述内容以及其它特征和实施例将变得更加明显。

附图说明

[0028] 图1A、1B和1C图示了根据实施例的安全监视和控制系统。

[0029] 图2和3示出了图示根据实施例的安全监视和控制系统的框图。

[0030] 图4是图示根据实施例的用于从云服务检索软件定义的安全配置数据的处理的流程图。

[0031] 图5是图示根据实施例的用于从云服务收集活动数据的处理的流程图。

[0032] 图6图示了根据实施例的用于分析应用使用的安全监视和控制系统的部件。

[0033] 图7和8图示了根据一些实施例的用于发现和管理应用的安全性的处理的框图。

[0034] 图9图示了根据一些实施例的用于计算应用的安全性的测量的处理的序列流程图。

[0035] 图10-12示出了图示根据实施例的用于检测和管理应用的安全性的处理的流程图。

[0036] 图13图示了根据一些实施例的用于基于应用使用来计算针对用户的安全性的测量的处理的序列流程图。

[0037] 图14图示了根据一些实施例的用于基于应用使用来评估针对用户的安全性的测量的图表。

[0038] 图15-26图示了根据实施例的用于将存储设备实现为用于管理对资源的访问的安全设备的接口。

[0039] 图27描绘了用于实现实施例的分布式系统的简化图。

[0040] 图28图示了根据本公开的实施例的、其中服务可以作为云服务提供的系统环境的一个或多个部件的简化框图。

[0041] 图29图示了可以被用来实现本公开实施例的示例性计算机系统。

具体实施方式

[0042] 在以下描述中，为了说明的目的，阐述了具体的细节，以便提供对本公开的实施例的透彻理解。但是，显而易见的是，各种实施例可以在没有这些具体细节的情况下实践。例如，电路、系统、算法、结构、技术、网络、处理和其它部件可以以框图形式示为部件，以免用不必要的细节混淆实施例。附图和描述不旨在是限制性的。

[0043] 虽然应用的使用可以有助于提高生产率，但是应用也可以在组织中造成安全风险以及合规性问题。例如，如果应用不够安全，那么具有业务敏感信息的机密文件会容易受到信息泄露的影响。由于这些应用未经组织评估，因此它们不准备对安全漏洞采取行动。而且，一些看似有用的应用可能会故意或不知不觉地分发广告软件甚至恶意软件。

[0044] 许多组织尝试阻止此类应用或网站，但这会使员工因生产力的影响而感到不快。而且，员工尝试绕过这样的障碍，例如，使用外部 VPN服务、移动数据服务等等。最近的行业趋势是不阻止这种服务以确保员工的生产力。但是，IT部门需要对所有正在使用的应用的可见性，以便他们可以主动地监视和控制可疑或恶意应用。

[0045] 用传统工具可以难以检测应用、分析它们造成的任何安全威胁以及校正动作。根据本公开的若干实施例的用于发现和监视应用的处理涉及分析来自各种数据源的信息并关联数据，以发现可以造成敏感数据的未授权披露和/或对组织的计算环境产生负面影响的应用使用。

[0046] 一些实施例(诸如关于本公开中的附图所公开的那些)可以被描述为被绘制为流程图、流图、数据流图、结构图、顺序图或框图的处理。虽然顺序图或流程图可以将操作描述

为顺序处理，但是许多操作可以并行或并发地执行。此外，操作的次序可以被重新安排。处理在其操作完成时终止，但是可以具有图中不包括的附加步骤。处理可以与方法、函数、过程、子例程、子程序等对应。当处理与函数对应时，其终止可以与函数返回到调用函数或主函数对应。

[0047] 本文描述的处理(诸如参考本公开中的附图描述的那些)可以用由一个或多个处理单元(例如，处理器核)、硬件或其组合执行的软件(例如，代码、指令、程序)来实现。软件可以存储在存储器中 (例如，存储在存储设备上、存储在非瞬态计算机可读存储介质上)。在一些实施例中，本文中以序列图和流程图描绘的处理可以通过本文公开的任何系统来实现。本公开中的处理步骤的特定系列并不旨在限制。步骤的其它顺序也可以根据替代实施例执行。例如，本公开的替代实施例可以以不同的次序执行上面概述的步骤。而且，附图中所示的各个步骤可以包括多个子步骤，这些子步骤可以以对个体步骤适当的各种顺序执行。此外，取决于特定的应用，可以添加或移除附加的步骤。本领域的普通技术人员将认识到许多变化、修改和替代。

[0048] 在一些实施例的一方面，本公开的这个图中的每个处理可以由一个或多个处理单元执行。处理单元可以包括一个或多个处理器，包括单核或多核处理器、处理器的一个或多个核，或其组合。在一些实施例中，处理单元可以包括一个或多个专用协处理器，诸如图形处理器、数字信号处理器(DSP)等。在一些实施例中，可以使用定制电路来实现一些或所有处理单元，诸如专用集成电路(ASIC)或现场可编程门阵列(FPGA)。

[0049] I.用于发现和分析应用的计算环境

[0050] 现在转向附图，公开了包括安全监视和控制系统102(本文也称为“安全管理系统”和“安全系统”)的系统100的技术。安全监视和控制系统102可以在具有组织的通信网络104的计算环境内实现。网络104可以是可以与公共网络(例如，互联网)通信以访问应用服务110的专用网络。通信网络的示例可以包括移动网络、无线网络、蜂窝网络、局域网(LAN)、广域网(WAN)、其它无线通信网络或其组合。安全监视和控制系统102可以由服务提供者管理，诸如安全服务提供者(有时称为云访问安全代理(CASB))，其使用安全监视和控制系统102来配置和管理组织的安全性。

[0051] 租户可以是其成员包括由服务提供者(例如，云服务提供者)提供的服务的用户的组织或组。用户可以具有提供者的个人帐户，并且租户可以具有云提供者的企业帐户，这些帐户涵盖或汇总了多个个别的用户帐户。在本公开的许多实施例中，安全监视和控制系统102可以使租户能够查看关于安全帐户的信息，包括对于他们使用的各种服务的那些帐户的控制和活动、审查分析报告，以及通过预设的安全分类级别来配置安全控制。

[0052] 在若干实施例中，安全监视和控制系统102使用机器学习和其它算法来分析关于一个或多个云中的用户活动的信息，以执行威胁检测并提供关于对不同类别的威胁的适当响应的推荐。分析可以包括确定用户活动中正常和/或异常行为的模型，以及检测一个云中或跨多个云的可疑活动的模式。一些模式可以涉及检测与同一用户帐户或IP 地址相关联的多个云中的相同操作或不同操作。分析还可以包括在检测到可疑活动的(一个或多个)云中提供提醒并推荐补救措施，和/ 或在除了显示可疑活动的云之外的云中采取补救措施。在本公开的许多实施例中，用于检测和分析组织的网络内的设备上的应用的处理涉及收集并组合来自各种数据源的信息。

[0053] 根据本公开实施例的用于安全监视和控制的系统包括可以位于单个硬件平台上或者彼此通信的多个硬件平台上的多个部件。部件可以包括配置服务器或其它计算设备以执行用于发现和管理的处理的软件应用和/或模块，如下面将进一步讨论的。

[0054] 在图1A中示出了根据本公开实施例的系统100，该系统100包括安全监视和控制系统102、可以用于访问安全监视和控制系统102 的客户端设备106，以及要被监视的应用服务110。如本文所公开的，“客户端”(本文也称为“客户端系统”或“客户端设备”)可以是设备或在设备上执行的应用。系统100包括多个不同类型的客户端设备106，每个客户端设备106具有通过网络104进行通信的能力。客户端设备106与安全监视和控制系统102通信并呈现用于与服务交互的图形界面。安全监视和控制系统102可以与应用服务110通信，以检索安全配置、应用数据和其它信息并且设置安全控制，如下面将进一步讨论的。

[0055] 图1B图示了具有为组织实现的安全监视和控制系统102的实现的系统150。具体而言，系统150图示了如何实现安全监视和控制系统102以检测组织的用户在通信网络(例如，专用网络(例如，内联网170)和非专用网络(例如，互联网160))上的客户端设备106 上的应用使用。通信网络的示例可以包括移动网络、无线网络、蜂窝网络、局域网(LAN)、广域网(WAN)、其它无线通信网络或其组合。在内联网170中操作的客户端设备106可以在由防火墙142保护的隔离计算环境中。用户(例如，安全管理员)可以管理安全监视和控制系统102的操作。安全监视和控制系统102可以在组织的计算环境、计算环境的外部或两者中实现。可以通过网络160将安全监视和控制系统102作为基于云的服务提供。

[0056] 客户端设备106中的每一个可以用于访问被授权或未授权在组织的设备上使用的应用。应用可以由不同的服务提供者(诸如可信的应用提供者120和未知的应用提供者122)访问。内联网170内部和外部的客户端设备106可以用于访问使得能够访问由不同服务提供者管理的应用和/或数据的第三方服务提供者124的服务。

[0057] 安全监视和控制系统102可以通过来自在网络设备上操作的一个或多个代理的网络数据基于组织的客户端设备的网络活动来监视应用活动。安全监视和控制系统102可以分析并关联来自应用的数据，以提供对组织中的活动的深度可见性，并且有助于基于应用使用来检测异常或新出现的威胁和安全风险。

[0058] 现在转向图1C，系统150被示为可以如何使用客户端设备106 (诸如个人BYOD(“自带设备”)和公司拥有的台式机/笔记本电脑)来访问组织内外的不同类型的应用的另一个示例。应用可以由服务提供者系统180提供。服务提供者系统在本文也可以称为“提供者系统”。本文公开的每个服务提供者系统可以由服务提供者操作和管理。应用可以包括未授权的应用122和第三方未授权的应用124。组织用户可以将许多经批准的应用用于日常工作，诸如Salesforce用于跟踪客户活动、Google Apps/Office 365用于协作、Box用于共享文件，等等。这些应用允许在这些应用内部安装第三方应用，这在内部允许这些第三方应用代表用户访问经批准的应用数据。这些未经认可的(unapproved)第三方应用可以从安全性和合规性角度增加组织风险，因为它们可以访问由于安全数据安全性差或潜在未经授权的数据泄漏而可能易受攻击的业务敏感数据。因此，此类第三方应用发现可以帮助IT团队获得更高的可见性。

[0059] 安全监视和控制系统102可以通过从多个源收集数据、用威胁情报信息关联和分析它们来发现应用使用，包括影子应用。与简单地发现来自网络设备的影子IT信息相比，这

提供了更大深度的可见度和更好的合规性覆盖。当组织的用户从办公室网络访问未经批准的应用时，诸如目的地网络地址、请求者的网络地址、时间戳之类的连接性相关信息由如路由器和防火墙的网络设备(例如，应用防火墙144和网络防火墙142)记录。其中一些应用防火墙还记录请求者身份，这允许查找正在使用该应用的实际用户。当组织用户在如智能电话和平板电脑的移动设备中安装应用时，只要在设备中安装了MDM应用， MDM(移动设备管理)服务182就可以发现已安装的应用的细节。类似地，当用户在公司拥有的设备上安装未经批准的应用时，可以使用集中管理的安全管理工具(例如，应用使用跟踪服务器184)由公司拥有的许可证管理集中发现这样的安装细节。来自这些数据源的日志可以提供对台式/膝上型设备中安装的未授权或影子应用的可见性。

[0060] II.用于安全监视和控制系统的体系架构

[0061] 公开了用于发现和管理计算环境中的应用的安全性的一些实施例，诸如系统、方法和机器可读介质。图2图示了系统200，其中用户可以操作客户端设备(诸如客户端设备106-1、106-2、.....106-N(统称为客户端设备106))，以访问来自一个或多个服务提供者的一个或多个应用(本文也称为“应用”)。例如，系统200可以包括一个或多个服务提供者(诸如服务提供者210和服务提供者212)。每个服务提供者可以经由网络160(例如，互联网)提供一个或多个服务。服务可以包括基于云或网络的服务。例如，服务提供者212可以是“云”服务提供者。服务可以包括提供应用作为服务。每个服务提供者可以具有包括一个或多个计算机系统的服务提供者系统。一个服务提供者系统可以与另一个不同。

[0062] 客户端设备106可以是用户的个人设备(例如，BYOD)或者是组织管理下的设备。如图1C中所示，客户端设备106可以在组织的计算环境的网络、计算环境外部的网络160或其组合上访问服务提供者的应用。可以操作应用，以访问组织的计算环境的数据和/或资源。一些客户端设备可以使用由服务提供者提供的第三方应用214来访问应用和/或用于应用的数据。可以向组织注册应用，以用作那个组织中的用户。一些应用可能未注册，因此可以上组织未经授权或未知的。每个应用可以利用和/或访问组织的计算环境中的资源。安全监视和控制系统102可以发现应用及其关于组织的计算环境的使用。客户端设备106可以由组织的用户(诸如管理员)操作，以利用由安全监视和控制系统102提供的服务。客户端设备106的用户可以是一个或多个租户的一部分，或者组织的组。照此，安全监视和控制系统102可以以每个用户为基础和/或以租户为基础提供发现和管理应用的服务。

[0063] 资源可以包括但不限于文件、网页、文档、web内容、计算资源或应用。例如，系统200可以包括诸如通过那些应用可访问的应用和 /或内容的资源。可以使用应用来请求和访问资源。例如，应用可以基于识别所请求的资源的URL来请求从资源服务器访问网页。资源可以由一个或多个计算系统(例如，提供对一个或多个资源的访问的资源服务器)提供。

[0064] 组织可以具有一个或多个计算环境(诸如计算环境240和计算环境260)。计算环境中的每一个可以是云计算环境或企业计算环境。计算环境中的每一个可以向组织的用户的客户端设备提供对组织的计算资源的访问。每个计算环境可以包括一个或多个计算机和/或服务器(例如，一个或多个访问管理器服务器)，其可以是通用计算机、专用服务器计算机(作为示例，包括PC服务器、UNIX服务器、中程服务器、大型计算机、机架式服务器等等)、服务器场、服务器集群、分布式服务器或任何其它适当的布置和/或组合。计算环境可以运行任何操作系统或各种附加服务器应用和/或中间层应用，包括 HTTP服务器、FTP服务器、CGI

服务器、Java服务器、数据库服务器等。示例性数据库服务器包括但不限于可从Oracle、Microsoft 等商业获得的数据库服务器。计算环境可以使用硬件、固件、软件或其组合来实现。

[0065] 计算环境中的每一个可以被实现为用于组织的安全环境。例如，组织的计算环境240和计算环境260可以被实现为计算防火墙230后面的安全环境(例如，内联网)。可以实现一个或多个防火墙，以保护计算环境。计算环境中的每一个可以用一个或多个网络设备实现。例如，计算环境240可以用一个或多个网络设备242实现，并且计算环境260可以用一个或多个网络设备262实现。网络设备中的每一个可以促进计算环境中的以及与外部网络(例如，网络160)的通信。网络设备可以包括但不限于路由器、网关、接入点、网桥等。可以在计算环境中的每个网络设备处搜集网络数据。可以在日志文件中搜集数据。

[0066] 安全监视和控制系统102可以提供基于web的客户端接口、专用应用程序、应用程序接口(API)、图形接口、通信接口和/或用于促进客户端设备106与安全监视和控制系统102之间的通信的其它工具。例如，安全监视和控制系统102可以包括用于暴露安全监视和控制系统102的服务的接口220。接口220可以生成和/或提供使客户端设备106能够访问安全监视和控制系统102的接口。安全监视和控制系统102可以被实现为执行本文公开的操作，包括参考图1A-1C和 7-14公开的处理。

[0067] 安全监视和控制系统102可以由计算系统实现。计算系统可以包括一个或多个计算机和/或服务器(例如，一个或多个访问管理器服务器)，其可以是通用计算机、专用服务器计算机(作为示例，包括 PC服务器、UNIX服务器、中程服务器、大型计算机、机架式服务器等等)、服务器场、服务器集群、分布式服务器或任何其它适当的布置和/或组合。安全监视和控制系统102可以运行任何操作系统或各种附加的服务器应用和/或中间层应用，包括HTTP服务器、FTP 服务器、CGI服务器、Java服务器、数据库服务器等。示例性数据库服务器包括但不限于可从Oracle、Microsoft等商业获得的数据库服务器。可以使用硬件、固件、软件或其组合来实现安全监视和控制系统102。

[0068] 安全监视和控制系统102可以包括至少一个存储器、一个或多个处理单元(或(一个或多个)处理器)和存储器。(一个或多个)处理单元可以适当地以硬件、计算机可执行指令、固件或其组合来实现。在一些实施例中，安全监视和控制系统102可以包括若干子系统和/ 或模块。安全监视和控制系统102中的这些子系统和/或模块中的每一个可以用硬件、在硬件上执行的软件(例如，程序代码、可由处理器执行的指令)或其组合来实现。在一些实施例中，软件可以存储在存储器(例如，非瞬态计算机可读介质)中、存储器设备上或某种其它物理存储器上，并且可以由一个或多个处理单元(例如，一个或多个处理器、一个或多个处理器核、一个或多个GPU等等)执行。 (一个或多个)处理单元的计算机可执行指令或固件实现可以包括以任何合适的编程语言编写的计算机可执行指令或机器可执行指令，以执行本文描述的各种操作、功能、方法和/或处理。存储器可以存储可在(一个或多个)处理单元上加载并执行的程序指令，以及在执行这些程序期间生成的数据。存储器可以是易失性的(诸如随机存取存储器(RAM))和/或非易失性的(诸如只读存储器(ROM)、闪存等等)。可以使用任何类型的持久存储设备来实现存储器，诸如计算机可读存储介质。在一些实施例中，计算机可读存储介质可以被配置为保护计算机免受包含恶意代码的电子通信的影响。计算机可读存储介质可以包括存储在其上的指令，当指令在处理器上执行时，执行本文描述的操

作。

[0069] 安全监视和控制系统102还可以提供可以包括非虚拟和虚拟环境的服务或软件应用。在一些实施例中，这些服务可以作为基于web 或云的服务或者在软件即服务(SaaS)模型下提供给客户端的用户。由安全监视和控制系统102提供的服务可以包括应用服务。应用服务可以经由SaaS平台由安全监视和控制系统102提供。SaaS平台可以被配置为提供属于SaaS类别的服务。SaaS平台可以管理和控制用于提供SaaS服务的底层软件和基础设施。通过利用由SaaS平台提供的服务，客户可以利用在安全监视和控制系统102中执行的应用，其可以被实现为云基础设施系统。用户可以获取应用服务，而无需客户购买单独的许可证和支持。可以提供各种不同的SaaS服务。操作客户端的用户可以进而利用一个或多个应用与安全监视和控制系统102 交互，以利用由安全监视和控制系统102的子系统和/或模块提供的服务。

[0070] 安全监视和控制系统102还可以包括或耦合到附加的存储装置，该附加的存储装置可以使用任何类型的持久存储设备来实现，诸如存储器存储设备或其它非瞬态计算机可读存储介质。在一些实施例中，本地存储装置可以包括或实现一个或多个数据库(例如，文档数据库、关系数据库或其它类型的数据库)、一个或多个文件存储、一个或多个文件系统或其组合。例如，安全监视和控制系统102耦合到或包括一个或多个用于存储数据的数据存储，诸如存储装置222。存储器和附加的存储装置都是计算机可读存储介质的示例。例如，计算机可读存储介质可以包括以用于存储诸如计算机可读指令、数据结构、程序模块或其它数据之类的信息的任何方法或技术实现的易失性或非易失性、可移动或不可移动介质。

[0071] 在图2所示的示例中，存储装置222可以包括租户配置信息 (“租户配置信息”)224，其可以包括用于租户及其帐户以及与每个租户帐户相关联的用户帐户的配置信息。属于租户组织的用户可以具有各种云应用的用户帐户。租户配置信息还可以具有租户帐户，其中云应用对属于该组织的用户的用户帐户行使管理权限。用户的用户帐户通常与用户所属的租户的租户帐户相关联。根据本发明的实施例，可以以各种方式使用用户帐户与租户帐户的关联，包括检索关于与租户相关联的用户的用户活动的信息。如下面将进一步讨论的，租户帐户的凭证可以用于登录到服务提供者系统，以检索关于与租户帐户相关联的服务的用户帐户和活动的数据。这种配置信息可以包括用于访问、日志设置和访问设置的安全设置(例如，白名单和黑名单)。存储装置222可以包括关于向组织注册的每个用户和/或组织租赁的用户信息。存储装置222可以包括基于关于应用使用的事件和为计算环境中的网络活动搜集的日志信息的应用信息232。应用信息232可以包括从数据源为应用获得的组织信息。存储装置222中的信息可以由安全监视和控制系统102基于用户活动和/或用户输入来维护和策展。例如，存储装置222可以包括诸如本文公开的那些的注册表。存储装置222可以包括关于由安全监视和控制系统102执行的安全性分析的安全信息226。安全信息226可以包括从一个或多个数据源获得的安全信息。存储装置222可以包括用于关于应用的服务提供者的域信息的域信息228。

[0072] 安全监视和控制系统102可以耦合到一个或多个数据源280或与之通信，一个或多个数据源280可以使用任何类型的持久存储设备来实现，诸如存储器存储设备或其它非瞬态计算机可读存储介质。在一些实施例中，本地存储装置可以包括或实现一个或多个数据库(例如，文档数据库、关系数据库或其它类型的数据库)、一个或多个文件存储、一个或多

个文件系统或其组合。例如，数据源280可以包括安全信息数据源282、组织信息数据源284和域信息数据源286。数据源中的每一个可以由服务提供者系统提供的服务实现和/或可作为由服务提供者系统提供的服务访问。每个数据源可以包括用于请求关于应用和/或应用的提供者的数据的接口。例如，安全信息数据源282可以由提供Security Score **Card®**作为服务的公司提供。在另一个示例中，组织信息数据源284可以由**ClearBit®**服务提供。域信息源286 可以由提供域名系统(DNS)查找服务的提供者系统提供。

[0073] 在一些实施例中，安全监视和控制系统102可以包括日志收集器系统234，该系统执行用于收集关于计算环境中的活动的网络数据的操作。网络数据可以从从被监视的一个或多个计算环境获得的日志文件中收集。日志收集器系统234可以被配置为与在每个计算环境中实现的一个或多个模块和/或子系统通信，以收集网络数据。例如，计算环境240和计算环境260中的每一个可以分别包括日志管理器246 和日志管理器266。每个日志管理器可以从被实现为收集关于网络活动的数据的一个或多个代理(例如，计算环境240中的代理244和计算环境260中的代理264)收集和/或汇总数据。可以以日志文件的形式收集数据。每个日志管理器和/或代理可以在网络设备上实现或与网络设备通信。日志收集器系统234可以与日志管理器246、266和/ 或代理244、264通信，以搜集关于计算环境内的网络活动的数据。

[0074] 日志管理器和代理中的每一个可以以硬件、在硬件上执行的软件 (例如，程序代码、可由处理器执行的指令)或其组合来实现。在一些实施例中，软件可以存储在存储器(例如，非瞬态计算机可读介质) 中、存储器设备或某种其它物理存储器上，并且可以由一个或多个处理单元(例如，一个或多个处理器、一个或多个处理器核、一个或多个GPU等等)执行。(一个或多个)处理单元的计算机可执行指令或固件实现可以包括以任何合适的编程语言编写的计算机可执行指令或机器可执行指令，以执行本文描述的各种操作、功能、方法和/或处理。存储器可以存储可在(一个或多个)处理单元上加载并执行的程序指令，以及在执行这些程序期间生成的数据。存储器可以是易失性的(诸如随机存取存储器(RAM))和/或非易失性的(诸如只读存储器(ROM)、闪存等等)。可以使用任何类型的持久存储设备来实现存储器，诸如计算机可读存储介质。在一些实施例中，计算机可读存储介质可以被配置为保护计算机免受包含恶意代码的电子通信的影响。计算机可读存储介质可以包括存储在其上的指令，当指令在处理器上执行时，执行本文描述的操作。

[0075] 日志收集器系统234可以被配置为通过由每个服务提供者提供的接口与每个服务提供者通信。日志收集器系统234可以从服务提供者获得关于由一个或多个用户对服务的使用的日志文件和/或事件数据。日志收集器系统234可以被配置为与客户端设备上的模块(例如，代理)和/或移动设备管理服务通信，以获得关于应用使用的事件信息。

[0076] 关于网络活动和应用使用的数据可以由安全监视和控制系统102 中的数据分析系统236处理。数据分析系统236可以实现本文公开的技术，以分析包括日志文件的网络数据来确定被访问的唯一的应用。数据分析系统236可以执行操作，以识别关于提供应用的服务提供者的域的域信息。域信息可以从一个或多个数据源获得，诸如域信息 286。域信息可以通过执行数据源的查询和/或从应用的服务提供者请求证书来获得。

[0077] 安全监视和控制系统102可以包括信息处理机系统238，其被配置为获得关于应用的使用和/或与应用的使用相关的信息。信息处理机238可以与一个或多个数据源280通信，

以获得信息。信息处理机 238可以管理和策展存储在存储装置222中的信息。存储在存储装置 222中的所有或一些信息可以基于用户的用户输入和/或策展。

[0078] 安全监视和控制系统102中的安全性分析器270可以实现本文公开的技术，以确定关于应用、用户或其组合的安全性的测量。

[0079] 安全监视和控制系统102中的控制管理器272可以处理对计算环境中的应用的访问的管理和控制。安全监视和控制系统可以使用一个或多个策略(例如，安全策略)来控制设备相对于组织的计算环境所允许的对应用的访问。策略可以由用户针对一个或多个用户(或者统称为租赁)配置。策略可以指示基于用户对应用使用的安全性分析来执行的补救动作。补救可以包括发送通知、显示信息(例如，报告)，和/或限制或阻止对应用的访问。控制管理器272可以与计算环境通信，以配置网络设备和/或防火墙来防止或限制对应用的访问。这种控制即使不降低安全风险和/或最小化计算资源的低效或不期望的消耗(例如，带宽和存储器使用)也可以防止这种情况。控制管理器 272可以向计算环境和/或网络设备发送一条或多条指令，以控制对应用的访问。在一些实施例中，安全监视和控制系统102可以在每个客户端设备106上实现被配置为与安全监视和控制系统102通信的模块 (例如，代理)。控制管理器272可以向客户端设备106上的代理发送一条或多条指令，以更改设备的功能来防止或减少对应用的访问。

[0080] 在本公开的许多实施例中，用于安全性的系统包括在硬件平台上执行的管理应用、用户界面部件和存储在硬件平台上的数据仓库。图 3中图示了根据本公开实施例的用于安全性的系统300。系统300可以在如本文所公开的安全监视和控制系统中实现，诸如安全监视和控制系统102。系统300中的云管理应用可以包括云爬虫302、云播种器304和数据加载器306。如将在下面进一步详细讨论的，云爬虫应用302可以从云提供者检索关于安全控制的信息，云播种器应用304 可以修改云提供者的租户帐户的安全控制，以反映期望的安全姿态，并且数据加载器应用306可以检索关于云提供者的租户帐户的活动信息并生成分析。

[0081] 在若干实施例中，由云爬虫应用302检索的数据被输入到应用目录数据库308中，并且由数据加载器应用306检索的数据被输入到登陆储存库310和/或分析和威胁情报储存库数据库311中。进入登陆储存库310的数据可以是不同的格式和/或具有不同的值范围-这种数据可以在移动到分析储存库311之前被重新格式化和/或构造。可以利用关于分析储存库311中的活动信息的数据来生成可以经由用户界面可视地呈现给系统管理员的报告，并生成用于确定威胁级别、检测具体威胁和预测潜在威胁的分析。

[0082] 分析存储库311中关于访问模式和其它事件统计量的活动信息的汇总使得系统能够建立用户行为的基线。然后可以应用机器学习技术来检测威胁并提供关于如何响应威胁的推荐。可以开发威胁模型来检测已知或未知或正在出现的威胁。还可以通过将活动数据与外部威胁情报信息(诸如由第三方提供者提供的信息)进行比较来识别威胁，如将在下面进一步讨论的。

[0083] 不同云应用中的特定用户的帐户(例如，不同的用户身份)可以在用户身份储存库309中关联在一起。云安全系统中的用户身份储存库309和/或其它存储器可以存储关于租户帐户和与每个租户帐户相关联的用户帐户的信息。属于租户组织的用户可以具有各种云应用的用户帐户。租户组织还可以具有云应用的租户帐户，该帐户对属于该组织的用户的

用户帐户行使管理权限。用户的用户帐户通常与该用户所属的租户的租户帐户相关联。根据本公开的实施例，可以以各种方式使用用户帐户与租户帐户的关联，包括检索关于与租户相关联的用户的用户活动的信息。如下面将进一步讨论的，租户帐户的凭证可以用于登录云应用服务，以检索关于与租户帐户相关联的用户帐户的活动数据。

[0084] 如下面将更详细讨论的，用户身份储存库309还可以用于促进跨多个云应用的用户跟踪和简档。此外，收集关于跨多个云服务的用户行为的信息使得系统能够在基于一个或多个云服务上的行为检测到威胁时预先提醒系统管理员关于其它云服务上的威胁和/或主动保护用户通过应用补救措施在其上维护数据的其它服务，诸如向认证添加附加的步骤、改变密码、阻止特定的一个或多个IP地址、阻止电子邮件消息或发件人，或锁定帐户。

[0085] 在本公开的若干实施例中，系统300包括应用或软件模块以对收集的数据执行分析，这将在下面进一步详细讨论。应用或软件模块可以存储在易失性或非易失性存储器中，并且在被执行时配置处理器 301执行某些功能或处理。这些应用可以包括威胁检测和预测分析应用312和/或描述性分析应用313。威胁检测和预测分析应用312可以使用机器学习和其它算法来生成分析，以从活动模式和行为模型中识别并预测安全威胁。描述性分析应用313可以生成分析，诸如但不限于关于用户、用户活动和资源的统计量。可以使用存储在分析和威胁情报储存库311中的数据来执行分析。

[0086] 如下面将进一步讨论的，本公开的实施例可以包括补救功能，其响应于威胁而提供手动和/或自动处理。在一些实施例中，分析可以利用从租户系统接收的描述由租户提供的威胁情报的信息。这些可被称为客户基线317的源可包括诸如但不限于要观看或阻止的具体IP 地址、要观看或阻止的电子邮件地址、易受攻击的浏览器或其版本以及易受攻击的移动设备或者移动硬件或软件的版本之类的信息。在附加的实施例中，分析可以利用从外部第三方馈送318、320和321接收的信息来通过提供安全威胁的外部信息增强威胁情报，其中安全威胁诸如但不限于受感染的节点的识别、来自特定的源IP地址的恶意活动、受恶意软件感染的电子邮件消息、易受攻击的Web浏览器版本以及已知的云攻击。

[0087] 事故补救应用313可以用于响应于检测到的威胁来协调和/或执行补救动作。当在提醒中呈现并选择推荐的补救动作时，它可以被调用。事故补救应用313可以执行所选择的补救动作或指示另一个应用 (诸如云播种器应用304)执行所选择的补救动作。当所选择的补救动作要手动执行或者在云安全系统外部时，事故补救应用313可以跟踪补救动作的状态以及补救事件是否完整。事故补救应用可以用于将手动或自动补救动作的结果保存到存储器中。在若干实施例中，所选择的补救动作将由云安全系统外部的系统执行，诸如由第三方或租户的事件补救系统执行。在这种情况下，事故补救应用313可以指示或调用第三方或租户的事件补救系统来使用自动集成处理执行动作。

[0088] 云播种器应用304可以用于通过在各种云应用中租户的帐户内设置安全控制来实现安全策略。如将在下面进一步详细讨论的，云播种器可以在各种条件下设置安全控制，诸如但不限于威胁的补救的一部分或系统用户的呼叫。可以使用于2014年10月24日提交的标题为“SYSTEMS AND METHODS FOR CLOUD SECURITY MONITORING AND THREAT INTELLIGENCE”的美国专利申请 14/523,804中公开的技术来实现安全控制和调整安全控制的技术的示例。

[0089] 在本公开的其它实施例中，用户界面部件包括管理控制台314，其为用户提供控制

管理,以设置用于一个或多个云的安全控制,以及用于查看由系统生成的分析的分析可视化控制台316。如下面将更详细讨论的,数据仓库中的数据可以用于生成用户界面中显示的信息和报告。下面讨论使用云管理应用从云应用检索安全配置数据。

[0090] Ⅲ.用于从云服务检索软件定义的安全配置数据的处理

[0091] 在本公开的许多实施例中,云爬虫应用从云服务检索软件定义的安全配置数据。软件定义的安全配置数据描述在特定云服务中的安全控制的配置。安全控制是限制对云所容纳的应用和数据的访问的机制。软件定义的安全配置数据可以包括描述以下内容的数据:为用户定义的角色、用户的组和分组、加密密钥、令牌、访问控制、许可、配置、认证策略的类型、移动访问策略以及许多其它类型的安全控制。图4 中图示了从云服务检索软件定义的安全配置数据的处理。

[0092] 该处理包括用于连接到云的步骤402。云可以需要授权或某种其它同意的表示才能访问系统和内部数据。授权可以通过令牌(诸如使用OAuth开放标准进行授权)或通过凭证(诸如用户名和密码)来提供。本领域技术人员将认识到的是,存在可以用于授权访问云提供者的系统和数据的各种其它技术。连接还可以包括提供服务URL (通用资源定位符)。

[0093] 该处理还包括步骤404,用于收集关于云应用的安全控制的软件定义的安全配置数据。可以通过利用由云应用提供的API(应用编程接口)来收集软件定义的安全配置数据。可以根据实施例使用的API 和API的类可以包括REST(代表性状态转移)、J2EE(Java 2平台,企业版)、SOAP(简单对象访问协议)和本机编程方法(诸如用于Java的本机应用API)。还可以使用其它技术请求信息,包括脚本语言(诸如Python和PHP)、部署描述符、日志文件、通过 JDBC(Java数据库连接)或REST的数据库连接,以及常驻应用 (云信标),这将在下面进一步讨论。被发送或接收的信息可以以各种格式表示,包括但不限于JSON(JavaScript对象表示法)、XML (可扩展标记语言)和CSV(逗号分隔值)。本领域技术人员将认识到的是,根据本公开的实施例,可以使用各种格式中适合于特定应用的任何一种。

[0094] 可以在步骤406使用所接收的关于云应用的安全控制的软件定义的安全配置数据来生成安全控制元数据,即,用于将信息输入公共数据库的规格化描述符。安全控制元数据在步骤408被分类(映射到类别中)并被索引。分类可以符合安全组织指定的标准和/或可以由第三方认证和/或审核。此外,安全控制元数据和/或元数据的分类可以围绕特定法规或标准的要求来制定。例如,诸如健康保险流通与责任法案(HIPAA)、Sarbanes-Oxley法案、FedRAMP和支付卡行业数据安全标准(PCI DSS)之类的法规和标准可能需要报告和审计跟踪。安全控制元数据可以以显示法规和标准所需的信息类型的方式被格式化,并促进生成所需的报告。

[0095] 在步骤410将安全控制元数据输入到应用目录数据库中。在本公开的许多实施例中,应用目录数据库是Cassandra数据库。在其它实施例中,应用目录数据库在适于应用的其它类型的数据库中实现。本领域普通技术人员将认识到的是,根据本公开的实施例,可以使用各种数据库中的任何数据库来存储应用目录,以供稍后检索、报告生成和分析生成,如下面将进一步讨论的。

[0096] 以上讨论了根据本公开实施例的用于发现和存储安全控制元数据的具体处理。根据本公开的实施例,可以利用用于检索软件定义的安全配置数据和生成安全控制元数据的各种处理中的任何处理。本领域技术人员将认识到的是,控制的数量和类型以及用于检索

软件定义的安全配置数据的机制可以在由不同云应用支持的本公开的不同实施例中变化。例如，可以使用特定于应用的检索机制来支持其它云应用 (诸如Office 365、GitHub、Workday和各种Google应用)。此外，用于检索软件定义的安全配置数据的处理可以基于目标云提供者支持而被自动化或者是手动的。

[0097] Ⅳ.控件管理平台

[0098] 在本公开的许多实施例中，控件管理平台向用户提供针对多个云的控件的规格化视图。该平台可以包括用户界面，该用户界面在同一屏幕上显示针对不同云的控件的简化视图。可以使用基于元数据的模式映射从应用目录数据库中检索提供给控件管理平台的信息。该平台可以用于跨云指派一致的访问策略。可以根据指定的分类器显示和/ 或设置控件，诸如但不限于：标准、严格、自定义。越高级别的分类与越严格的控件对应。在若干实施例中，安全控制的分类和/或指定符合由诸如国家标准与技术研究院(NIST)、国际标准化组织(ISO) 和/或支付卡行业数据安全标准(PCI DSS)之类的组织规定的标准和/或由一个此类组织提供的具体定认证。在本公开的若干实施例中，控件管理平台还可以提供插件接口以与SaaS、PaaS和本机应用集成。

[0099] 控件管理平台用户界面可以以库格式显示关键安全性指示符，其具有颜色编码的风险因子(诸如红色、绿色、黄色)。可以显示其它统计或度量，诸如但不限于用户登录尝试、具有最多添加用户的组、最多删除的文件、具有最多删除文件的用户以及下载最多文件的用户。一些类型的信息可以特定于特定的云应用提供者，诸如显示谁正在下载机会/预算数据、合同或联系人的Salesforce.com。在本公开的若干实施例中，用户界面为租户的注册云应用提供安全控制的统一视图。用户界面可以显示为针对不同云应用设置的任何或所有安全控制设置的值，以及当前值与预定策略或配置相关联的值的偏差。接下来描述来自云应用提供者的活动数据的集合。

[0100] Ⅴ.用于从云服务收集活动数据的处理

[0101] 在本公开的许多实施例中，云数据加载器应用配置计算设备，以从云服务收集关于租户的用户活动、安全性配置和其它相关信息的活动数据。图5中图示了根据本公开实施例的用于从云服务收集活动数据的处理。

[0102] 该处理包括用于连接到一个或多个云的步骤502和用于从云收集活动数据的步骤504。在许多实施例中，通过加密的通信信道进行连接。在其它实施例中，必须通过令牌或使用登录凭证来认证连接，如在与上面进一步讨论的云爬虫应用进行的连接中一样。在本公开的若干实施例中，收集被调度为周期性地发生(例如，每4小时或每6小时)。在许多实施例中，用于收集的时间表可由租户配置。在其它实施例中，当事件发生时利用实时计算系统(诸如例如Storm)实时地收集和检索数据。该系统可以被配置为将某些事件或活动指定为高风险事件，以便在被调度的检索之外近实时地进行检索。

[0103] 当外部系统保持适当的凭证时(该凭证可以由云应用系统或另一个授权实体发布)，活动数据可以包括由远程托管的云应用系统到云应用系统外部的系统可访问的各种类型的信息。与用户帐户相关联的活动数据可以包括与在云应用处对用户帐户的使用和/或动作相关的信息。活动数据可以包括诸如(一个或多个)用户日志或(一个或多个)审计跟踪之类的信息源。更具体类型的活动数据可以包括但不限于登录和注销统计量(包括尝试和成功)、用于访问应用的IP地址、用于访问应用的设备以及被访问的云资源(包括但不限

于文件管理云应用[诸如Box]中的文件和文件夹,人力资源云应用[诸如Workday] 中的员工和承包商,以及客户关系管理云应用[诸如Salesforce]]中的联系人和帐户)。活动数据可以包括与事件或统计量相关联的用户的用户帐户或其它用户标识符。活动数据可以包括关于云应用系统的系统状态或活动的信息(诸如但不限于服务器活动、服务器重新引导、服务器使用的安全性密钥以及系统凭证),其中这种信息对系统可见或可访问使用授权凭证。

[0104] 活动数据还可以包括关于租户(和相关联用户)帐户的安全性配置的信息。安全性配置可以包括为租户(和/或相关联用户)设置安全控制(在上面进一步讨论)的值。

[0105] 在一些实施例中,某些事件被认为是高风险,并且与这些事件相关的活动数据在被调度的间隔之外近实时地被检索。

[0106] 在步骤506处将检索出的活动数据存储在分析和威胁情报储存库数据库311中。分析和威胁情报储存库数据库311可以是具有查询能力的任何数据库或数据储存库。在本公开的若干实施例中,分析和威胁情报储存库数据库311构建在诸如Cassandra或其它分布式数据处理系统之类的基于NoSQL的基础设施中,但是可以适当地利用任何数据仓库基础设施用于该应用。在一些实施例中,首先将数据输入到登陆储存库310中并在被移动到分析储存库311之前被重新格式化和 /或构造。

[0107] 在本公开的一些实施例中,可以以由不同的云应用使用的不同格式来接收数据。例如,数据可以以JSON(JavaScript Object Notation)或其它数据交换格式来格式化,或者可以作为日志文件或数据库条目使用。在其它实施例中,该处理包括步骤508,用于规格化数据并将数据重新格式化为用于存储在分析和威胁情报储存库数据库311中以及从分析和威胁情报储存库数据库311中检索的公共格式。重新格式化数据可以包括将数据分类并结构化为公共格式。在本公开的若干实施例中,通过运行自动化处理来检查改变的数据,数据库适于结构改变和新值。在一些实施例中,云爬虫应用(如上面进一步讨论的)识别所检索的数据的结构或值的差异,并且在应用目录数据库 308和/或分析和威胁情报储存库数据库311中实现改变。系统报告可以在步骤510处由被调度在数据集上运行的作业预先生成。以上讨论了利用云加载器应用来收集活动数据的具体处理。根据本公开的实施例,可以使用各种处理中的任何处理来收集活动数据。下面讨论根据本公开实施例的可以由系统用户或管理员预先生成或按需生成的报告。

[0108] Ⅵ.报告

[0109] 存储在应用目录数据库和/或分析和威胁情报储存库数据库311 中的数据可以用于生成各种报告。报告的类别可以包括:认证和授权、网络和设备、系统和改变数据、资源访问和可用性、恶意软件活动以及故障和严重错误。报告可以基于各种属性,诸如但不限于每个应用、每个用户、每个受保护的资源以及用于访问的每个设备。报告可以突出显示最近的改变,诸如云应用中的更新特征或新修改的策略。报告可以由被调度的作业预先生成(例如,出于性能原因),或者可以由用户或管理员请求。

[0110] 在本公开的各种实施例中,报告包括关于数据生成的分析。分析可以利用Apache Software Foundation技术,诸如Hadoop、Hive、 Spark和Mahout,或者在所使用的数据存储框架中可用的其它特征。若干实施例利用R编程语言来生成分析。在其它实施例中,分析的生成包括使用机器学习算法、专有算法和/或来自诸如FireEye和Norse之类的外部商业源或者诸如Zeus和Tor之类的公共威胁情报社区的外部威胁情报。下面讨论根据本公开实施

例的用于生成分析的技术。

[0111] Ⅶ.分析和安全性情报

[0112] 根据本公开实施例的安全监视和控制系统可以使用所收集的数据来生成分析。分析可以由分析处理和/或称为分析引擎的分析模块生成。图6中图示了根据本公开实施例的使用威胁情报平台600的部件生成分析的概述。平台600可以在系统200中实现。平台600的全部或部分可以在安全监视和控制系统102中实现。

[0113] 可以生成的一类分析是描述性或统计性分析。可以使用预定义的系统查询集生成统计数据，诸如但不限于MapReduce作业以及 Spark和Apache Hive查询。可以使用关联技术为单个应用或跨多个应用生成描述性分析。可以生成的报告的示例包括但不限于登录统计量(例如，登录失败最多的用户，包括IP信誉、地理位置和其它因素考虑的基于IP地址的登录历史)、用户统计量(例如，资源[文件、EC2机器等等]最多的用户、跨云的权利、改变密码的数量)、活动统计量(例如，用户跨云的活动)、关于密钥轮换的统计量(例如，SSH密钥是否已经过在最近30天内轮换)以及资源统计量(例如，文件夹的数量、用户下载的文件、通过漫游或移动用户下载的文件)。可以识别趋势，诸如某个时间段内的登录活动、基于这些问题的过去历史的密码相关支持问题，或识别在某个时间段内看到最多活动的移动设备的类型。报告中的数据可以作为事件查看器显示在用户界面上，该事件查看器显示事件的“墙”连同用户可以响应或补救事件而采取的动作。可以基于可以包括具体事件和阈值的预定义规则来构建提醒。

[0114] 可以被生成的另一类分析是预测性和启发式分析。这些可以结合机器学习算法以生成威胁模型，诸如但不限于与基线期望的偏离、罕见和不常见事件以及行为分析，以导出用户的可疑行为。可以训练算法和简档，以智能地预测异常行为是否是安全风险。可以集成来自提供者的第三方馈送，诸如但不限于MaxMind、FireEye、Qualys、 Mandiant、AlienVault和Norse STIX，以通过提供潜在安全威胁的和与之相关的外部信息来增强威胁情报，诸如但不限于IP(互联网协议)地址信誉、恶意软件、受感染节点点的标识、易受攻击的 Web浏览器版本、用户对代理或VPN服务器的使用以及对云的已知攻击。在若干实施例中，威胁信息以结构化威胁信息表达(STIX) 数据格式表示。例如，一个或多个服务可以贡献关于特定IP地址的信息，诸如信誉(例如，已知具有软件漏洞、大量恶意软件或攻击源)和/或与IP地址相关联的地理位置。这种信息可以与检索到的涉及IP 地址的活动数据(诸如从该IP地址尝试登录的时间)以及从活动数据导出的信息(诸如登录尝试的距离)组合。这些因素可以用于确定“登录速度”度量。可以为其它活动确定度量标准，诸如文件访问、销售事务或虚拟机实例。

[0115] 在本公开的许多实施例中，各种类型的算法可以对于分析数据特别有用。决策树、时间序列、朴素贝叶斯分析以及用于构建用户行为简档的技术是机器学习技术的示例，其可以用于基于可疑活动和/或外部数据馈送的模式生成预测。诸如聚类之类的技术可以用于检测离群值和异常活动。例如，可以基于访问一个或多个文件的帐户或者从被标记(通过第三方订阅源或其它方式)为恶意的IP地址的一系列登录尝试失败来识别威胁。以类似的方式，威胁也可以基于在一系列时间内一个云中或跨多个云的不同活动模式。如上面进一步讨论的，来自不同云的活动数据可以是不同的格式或具有不同的可能值或值范围。规格化上面讨论的处理中的数据可以包括重新格式化数据，使得它具有可比性、具有相同含义，

和/或在不同云之间承载相同的重要性和相关性。因此，算法可以以有意义的方式聚合和比较来自不同云的数据。例如，在一个云中特定用户帐户的一系列失败登录可以被视为不是威胁。但是，跨多个云与用户相关联的用户帐户的一系列失败登录可以指示协同努力破解用户的密码并因此引发警报。聚类和回归算法可以用于对数据进行分类并查找常见的模式。例如，聚类算法可以通过聚合从移动设备登录的用户的所有条目来将数据放入集群中。预测分析还可以包括基于活动来识别威胁，诸如用户在几个月内未访问特定的云应用，然后在下个月显示高活动，或者用户在过去几周内每周下载一个文件，从而展示潜在的高级持续威胁(APT)场景。在本公开的若干实施例中，随时间收集的数据被用于构建正常行为的模型(例如，事件和活动的模式)并且将偏离正常的行为标记为异常行为。在一个或多个标记的事件或活动被表征为真或假阳性(例如，通过用户反馈)之后，可以将该信息提供回一个或多个机器学习算法，以自动修改系统的参数。因此，机器学习算法可以至少以上面讨论的方式使用，以做出推荐并减少误报(假阳性)。在一段时间内从各种参数收集的活动数据可以与机器学习算法一起使用，以生成被称为用户行为简档的模式。活动数据可以包括诸如IP地址和地理位置之类的上下文信息。

[0116] 用于关联规则学习的算法可以用于生成推荐。在本公开的若干实施例中，简档链接算法被用于通过查找跨应用相关性来链接跨多个云应用的活动。可以使用一个或多个属性或标识元素(诸如跨云共同使用的主用户标识符(ID)或单点登录(SSO)认证机制(例如，Active Directory、Okta))跨多个云识别单个用户。跨应用的活动的关联可以包括在第一云应用中找到具有第一权利的用户，其在第二云应用中具有第二权利，用户从不同的IP地址同时登录到两个云应用，具有多次登录尝试失败然后改变他们的密码的用户，以及在两个云应用中有大量失败登录的共同用户。

[0117] 在本公开的许多实施例中，可以利用用户身份储存库109来促进跨多个云应用的用户跟踪和简档。可以通过将与账户相关联的用户标识符(例如，jdoe、john.doe等等)、通过如上面提到的主(通用) 用户标识符或SSO机制或其它方法关联在一起来链接不同云应用中的特定用户的账户。用户身份储存库109可以包含将与租户相关联的每个用户的帐户关联在一起的信息。利用在租户的控制或所有权下的多个云应用帐户的用户可以被称为“企业用户”。

[0118] 在本公开的若干实施例中，推荐引擎跟踪用户活动的异常行为的，以检测攻击和未知的威胁。推荐引擎可以针对可疑事件跟踪跨多个云的用户活动。事件可以包括预定义的风险操作(例如，下载包含信用卡号的文件、复制加密密钥、提升普通用户的特权)。可以用事件的详细信息和补救推荐来发出警报。

[0119] 可以针对与具体用户/雇员有关的事件生成基于动态策略的提醒。处理可以监视与具体用户相关联的活动数据，并为用户采取的具体操作生成自定义提醒。

[0120] 在本公开的许多实施例中，设计算法以使用分析和威胁情报储存库数据库311中的用户活动数据来模拟正常用户活动。模拟可以用于训练其它机器学习算法以学习用户在系统中的正常行为。一般而言，特定的安全性问题可能并不总是重复，因此可能无法通过纯监督算法检测到。但是，诸如离群值检测之类的技术建立了对检测异常活动有用的基线。这种异常活动连同上下文威胁情报可以提供具有低预测误差的威胁的更准确预测。

[0121] 在本公开的其它实施例中，分析可以用于检测安全控制漂移，其可以指以可以增

加安全风险的看似任意的方式改变一个或多个安全控制。可以响应于一个或多个云应用中的一个或多个安全控制的改变以及与风险事件(在本文也称为“安全风险”、“风险”、“威胁”和“安全威胁”)相关联的可动作情报来生成风险事件。威胁可以包括与应用的使用相关的异常或不合规的活动、事件或安全控制。与其它类型的事件一样,可以向租户、租户系统或其它监视实体发送提醒。例如,云应用中的租户的密码策略可能已被改变,以强加更少的要求 (例如,字符的类型和/或数量)。这可能生成风险事件和提醒,以推荐将密码策略改回原始密码策略。

[0122] 关于上面讨论的任何事件的提醒可以在诸如上面进一步讨论的控件管理平台之类的用户界面上显示。提醒可以包括关于检测到的事件的信息,诸如但不限于事件标识符、日期、时间、风险级别、事件类别、用户帐户和/或与事件相关联的安全控制、与事件相关联的云应用、事件的描述、补救类型(例如,手动或自动)和/或事件状态 (例如,打开、关闭)。关于每个风险事件的提醒中的信息可以包括标识符(ID)、受影响的云应用和实例、类别、优先级、日期和时间、描述、推荐的补救类型和状态。每个风险事件还可以具有用户可选择的动作,诸如编辑、删除、标记状态完成和/或执行补救动作。补救动作的选择可以调用诸如事故补救应用313和/或云播种器应用 304之类的应用来执行所选择的补救。可以将关于识别出的威胁的提醒和/或其它信息发送到安全监视和控制系统102外部的实体。

[0123] 在本发明的许多实施例中,提醒可以是可视的并且可以出现在用户控制台中,诸如上面进一步讨论的控制管理平台。在若干实施例中,通过网络传送警报,诸如通过电子邮件、短消息服务(SMS)或文本消息传递或基于web的用户控制台。提醒可以作为安全消息传送 (例如,通过安全通信信道或需要密钥或登录凭证来查看)。提醒可以包含有关所推荐或可用的(一个或多个)补救动作的信息,诸如实施更强的安全控制,并请求选择要采取的(一个或多个)补救动作。

[0124] 以上讨论了根据本公开实施例的用于检索和分析活动数据的具体处理。根据本公开的实施例,可以使用用于检索和分析活动的各种处理中的任何处理。下面讨论补救识别出的威胁的处理。

[0125] Ⅷ.用于发现和分析应用的系统

[0126] 图7和8图示了根据一些实施例的用于发现和管理应用的安全性的处理的框图。图7图示了安全监视和控制系统102可以如何发现第三方应用并显示具有关于那些应用的信息的图形界面,包括应用和那些应用的用户的安全性的测量。

[0127] 示出了图7中的处理700,用于应用发现和分析与应用使用相关联的应用风险和用户风险。处理700可以被实现用于已经授权的应用,诸如通过向安全监视和控制系统102注册。处理700可以通过用户操作客户端设备(例如,客户端控制台702)在720开始,以提供关于应用(例如,注册应用)的信息。客户端设备702可以使用接口或服务(例如,代表性状态转移(REST)服务)与安全监视和控制系统 102通信。

[0128] 安全监视和控制系统102可以执行处理,以发现应用使用以及用于应用和那些应用的用户的安全性的测量。在722处,可以从提供已经注册的应用的服务提供者系统下载应用事件。应用事件可以以关于已被访问的应用的数据记录的形式提供。在724处,应用事件可以用于发现已被访问的应用和/或已经用于访问另一个应用的其它第三方应用或已注册的应用的数据。在726处,关于第三方应用的事件可以存储在储存库中。事件信息可以包括

关于事件的时间戳、用户信息 (例如,用户名或电子邮件ID)、第三方应用名称(链接->应用细节)、经批准的营与实例名称、IP地址以及地理位置信息。

[0129] 在728处,可以执行处理,以确定关于已被访问的第三方应用的信息。应用事件可以用于确定识别每个应用的唯一的信息。使用关于应用的信息,安全监视和控制系统102可以使用本文公开的技术来计算应用的应用风险得分。在一些实施例中,可以维护应用风险得分注册表704,从中可以获得应用风险得分。可以基于关于应用使用的新的和/或更新后的信息来维护和自动更新注册表。可以基于应用细节和来自使用第三方源(诸如第三方应用注册表706)获得的风险得分馈送740的风险得分指示符来计算应用风险得分。应用细节可以包括关于服务提供者或者提供第三方应用的供应商的供应商信息。供应商信息可以包括供应商名称、供应商徽标、供应商域、供应商描述、供应商类别(业务)和/或安全性指示符(例如,访问安全性得分评估支持数据的得分或链接)。关于应用的信息可以在730处发送到客户端控制台702,以便在诸如图15中描绘的图形界面中显示。

[0130] 在736处,安全监视和控制系统102可以获得关于在应用事件中识别出的应用的用户的用户信息。在734处,可以基于用户信息和应用事件细节来计算用户风险得分。在一些实施例中,可以基于从数据源获得的信息来计算用户风险得分,其中数据源维护关于用户的应用使用的信息。可以将关于用户的信息(包括用户风险得分和应用事件细节)发送到客户端控制台702。在732处,客户端控制台702可以在图形界面中显示关于用户的信息,包括用户风险得分和应用事件细节。处理可以在730和/或732结束。

[0131] 示出了图8中的处理800,用于应用发现和分析与应用使用相关联的应用风险和用户风险。可以实现处理800,以基于日志数据的分析来发现应用。可以从安全监视和控制系统102的一个或多个代理获得日志数据,该代理可以收集关于不同应用和网络活动的日志信息。

[0132] 图8中的处理800可以通过用户操作客户端设备(例如,客户端控制台802)在820开始,以指定识别日志文件的信息。例如,用户可以提供日志文件和/或信息访问日志文件的源。可以在820处摄取日志文件。客户端设备802可以使用接口或服务(例如,代表性状态转移(REST)服务)与安全监视和控制系统102通信。

[0133] 安全监视和控制系统102可以执行处理,以发现应用使用以及用于应用和那些应用的用户的安全性的测量。在822处,可以通过分阶段处理获得日志。在824处,可以处理日志以进行解析,以识别唯一的网络活动。在826处,可以分析网络活动,以发现第三方应用。贯穿处理日志的各个阶段,信息可以由安全监视和控制系统102传送到客户端控制台802,以在830处显示日志处理状态。

[0134] 在826处,日志可以被用于确定识别每个应用的唯一的信息。可以基于日志确定关于应用使用的事件细节。事件细节可以包括时间戳、第三方应用名称(链接->应用细节)、IP地址、地理位置、用户信息(例如,用户名或电子邮件ID),和/或请求应用的源设备的地址(例如,MAC地址)。在840处,使用关于应用的信息,安全监视和控制系统102可以确定关于每个发现的应用的信息。该信息可以包括关于应用的细节和使用本文公开的技术的应用风险得分。

[0135] 在一些实施例中,可以维护应用风险得分注册表804,从中可以获得应用风险得分。可以基于关于应用使用的新的和/或更新后的信息来维护和自动更新注册表。可以基于

应用细节和来自使用第三方源 (诸如第三方应用注册表806)获得的风险得分馈送846的风险得分指示符来计算应用风险得分。应用细节可以包括关于服务提供者或者提供第三方应用的供应商的供应商信息。供应商信息可以包括供应商名称、供应商徽标、供应商域、供应商描述、供应商类别(业务)和 /或安全指示符(例如,访问安全性得分评估支持数据的得分或链接)。关于应用的信息可以在832被发送到客户端控制台802,以在诸如图15中所示的图形界面中显示(例如,关于应用使用的日志发现报告)。

[0136] 在844处,安全监视和控制系统102可以获得关于在应用事件中识别出的应用的用户的用户信息。在842处,可以基于用户信息和应用事件细节来计算用户风险得分。在一些实施例中,可以基于从数据源获得的信息来计算用户风险得分,其中数据源维护关于用户的应用使用的信息。可以将关于用户的信息(包括用户风险得分和应用事件细节)发送到客户端控制台802。在834处,客户端控制台802可以在图形界面中显示关于用户的信息,包括用户风险得分和应用事件细节。处理可以在832和/或834结束。

[0137] Ⅸ.计算应用的安全性的测量

[0138] 图9图示了根据一些实施例的用于计算应用的安全性的测量的处理的序列流程图900。该处理可以由安全监视和控制系统102实现。

[0139] 可以基于由一个或多个第三方源、一个或多个用户、由安全控制和管理系统102管理和策展的源或其组合提供的信息来计算安全性的测量。安全性的测量可以基于关于应用和应用的提供者的信息(“组织信息”)和/或关于应用的安全性的信息(“安全信息”)。安全性的测量可以是定义应用的安全风险的测量的标度(scale)上的值 (在本文中也称为“应用风险得分”)。例如,可以将标度定义为1 到5之间,其中越高的值表示越大的风险。在其它实施例中,可以使用适合于特定评估的各种范围和值中的任何一个。得分可以被安全监视和控制系统102用来提供提醒、提供报告和/或执行补救措施。安全性的测量是用作优先级指示符的值,以帮助用户(例如,安全管理员)减轻由应用造成的安全威胁。在一些实施例中,可以以若干方式计算安全性的测量。

[0140] 用于计算安全性的测量的一种技术可以涉及计算风险得分,该风险得分指示关于由具体应用对组织提出的安全威胁的严重性的安全性措施。可以基于一个或多个指示符(在本文中也称为“威胁指示符”或“安全性指示符”)来计算风险得分。每个指示符可以是指示安全风险的值或信息。例如,在图9中,可以从一个或多个数据源902 (本文也称为“风险得分馈送”)获得唯一的安全性指示符,其中每个数据源(“S”)(在本文统称为数据源“S_1,S_2,.....S_n”902) 提供应用的一个或多个指示符的“馈送”。每个唯一的指示符 (“I”)(在本文统称为指示符“I_1,I_2,...,I_n”904)可以分别由每个数据源902提供。指示符可以是基于安全信息、组织信息或两者的特定类型的指示符。指示符可以是提供应用造成的安全威胁的指示的值。例如,第一指示符可以是指示应用的第一安全威胁的第一值。第二指示符可以是指示应用的第二安全威胁的第二值。第一指示符可以从第一数据源获得,并且第二指示符可以从第二数据源获得。第一数据源可以是图2中的数据源280之一。第二数据源可以与第一数据源相同或者是数据源280中的不同数据源。

[0141] 一种类型的安全威胁指示符是可以由一个或多个第三方源(诸如开源(例如,abuse.ch)或商业源(例如, www.SecurityScoreCard.com))提供的安全威胁指示符。安全威胁指示符可以基于安全信息,诸如但不限于应用的安全状态(诸如具有弱加密算法的不

安全网络设置)、端点安全性(诸如供应商组织中使用的过时设备)、供应商的网络中的IP信誉(诸如恶意软件)、黑客聊天(诸如黑客网络中关于应用的讨论)、泄露的信息(诸如公开暴露的来自供应商的敏感信息)、应用安全性(诸如网站漏洞)以及 DNS设置(诸如可能导致欺骗应用网站的错误设置)。

[0142] 另一种类型的安全性指示符可以是由一个或多个第三方源(诸如开源(例如,Wikipedia.com)或商业源(例如,Clearbit.com))提供的基于组织的指示符。基于组织的指示符可以基于组织信息,诸如但不限于业务类别、供应商的物理地址(其包括诸如国家之类的地理位置信息)、业务运营多长时间、应用互联网域注册年龄、根据网站排名列表(诸如Alexa域名排名)的应用的流行度,或其组合。

[0143] 每个威胁指示符可以表示安全风险得分,该安全风险得分是根据由那个指示符的源定义的标度指示安全风险或威胁的测量的值。在一些实施例中,可以将威胁指示符与标度进行比较,以确定安全风险得分。标度可以由源提供的信息定义或基于源提供的信息。

[0144] 安全监视和控制系统102可以基于一个或多个威胁指示符将安全性的测量计算为值或得分。换句话说,可以将安全性的测量计算为安全风险的组合测量。可以处理每个指示符,以根据要用于所有指示符的标度(例如,从0到100的值的标度)将指示符的值调整(例如,规格化)为调整后的值。一旦被规格化,就可以组合用于每个指示符的值,以确定组合得分。

[0145] 指示风险测量的组合安全性得分908可以基于所有或一些指示符。考虑用于确定组合安全性得分的指示符的数量和/或类型可以是可配置的。照此,安全监视和控制系统102可以被配置为添加或移除从其获得指示符的源902,并且可以被配置为添加或移除从源902获得的指示符904。在一些实施例中,可以呈现图形界面,该图形界面使用户能够配置为得分考虑的指示符的数量和类型。在一些实施例中,组合得分可以基于定义要通过其计算得分的标准的安全策略。标准可以基于安全性的一个或多个属性。这些属性可以用于选择要为得分考虑的指示符。

[0146] 在一些实施例中,组合得分908可以基于使用用于每个指示符的权重值的指示符的组合。例如,可以选择权重("W")(在本文统称为权重"W_1,W_2,...,W_n"904)以应用于用于计算组合得分908的一个或多个具体指示符。权重可以是整数1或1的一部分的值。可以为不同的指示符选择不同的权重。在上面的示例中,第一权重可以是用于第一指示符的第一权重值,并且第二权重可以是用于第二指示符的第二权重值。权重值可以不同。

[0147] 权重可以由用户通过图形界面来配置。在一些实施例中,可以基于安全策略来选择权重,其中安全策略基于特定指示符被给予特定权重来定义。当指示符对安全风险具有更多重要性或建议时,可以考虑更大的权重值。当指示符对安全风险具有较少重要性或建议时,可以考虑较小的权重值。在一些实施例中,可以为来自特定源的所有指示符选择权重。例如,可以基于源的可靠性或信任将权重应用于来自那个源的所有指示符。在一些实施例中,安全监视和控制系统102可以存储关于应用的威胁研究分析的数据。这些数据可以用于选择性地为每个指示符选择权重。

[0148] 可以基于指示符和对那些指示符的权重的考虑来计算组合得分。在至少一个实施例中,可以使用等式908来计算组合得分,以提供组合得分=$(I_1(W_1)+I_2(W_2)+.....I_n(W_n))/(W_{1+}W_2+\cdots W_n)$。在这个等式中,通过将每个指示符乘以相应的权重("W")906来计算每个指示

符 (“I”)904的值。计算第一值,该值是针对每个指示符计算的值的总和($I_1(W_1)+I_2(W_2)+.....I_n(W_n)$)。计算第二值,该值是被应用以获得第一值的每个权重值的总和。可以基于将第一值除以第二值来计算组合得分908。

[0149] 在从上面继续的示例中,可以基于将第一指示符的第一值乘以第一权重值来计算第一加权值。可以基于将第二指示符的第二值乘以第二权重值来计算第二加权值。可以基于第一加权值和第二加权值的总和来计算加权总和值。可以基于第一权重值和第二权重值的总和来计算权重总和值。可以将安全性的测量计算为基于将加权总和除以权重总和的值。

[0150] 在一些实施例中,安全监视和控制系统102可以从一个或多个用户获得关于组合得分908的有效性和准确性的反馈910。反馈910可以通过网络获得,通过图形界面或手动反馈来促进。可以基于反馈 910来调整源、指示符和/或权重中的任何一个。基于反馈910,可以调整组合得分908。可以以与计算组合得分908相同的方式计算新的组合得分912(“调整后的得分”)。除调整后的得分912可以基于基于反馈910选择的指示符和/或权重来计算之外。可以从用于计算组合得分908的内容中添加或移除源、指示符和/或权重。用于指示符的权重值可以基于我们的安全性分析师以及客户反馈来周期性地修订,以改进风险得分。用于指示符权重的修订处理可以通过自动机器学习算法(诸如决策树和神经网络)来执行。

[0151] 可以基于关于特定安全威胁的每个指示符和/或组合得分来执行回归分析914。回归分析可以包括建立并更新线性回归模型。线性回归模型可以提供诸如$S=c_1(I_1)+c_2(I_2)+\cdots+c_n(I_n)$之类的输出。由回归模型计算出的系数$c_i$可以是新的或修改后的权重,其将替换用于计算组合得分908的初始权重。随着更多反馈和更多数据被收集,该模型将提供更高的准确性。

[0152] 以下描述安全监视和控制系统102可以使用来自如abuse.ch(S_1) 的开源服务和如securityscorecard.io(S_2)的商业服务的威胁情报来确定安全性的测量的示例场景。在这个示例中,使用两个源S_1和S_2。源S_1提供域信誉服务,它提供域是否用于托管恶意软件、垃圾邮件程序等等信息。域信誉将是S_1的指示符I_{11}。源S_2提供关于应用安全性(I_{21})(例如,域中托管的应用是否存在安全漏洞)、网络安全性 (I_{22})(例如,使用弱加密算法)的信息。应用安全性将是指示符 I_{21},并且网络安全性将是S_2的指示符I_{22}。

[0153] 在这种场景中,取决于数据源的数据质量和可靠性,可以为每个源指派初始权重值。例如,S_1报告的问题可以有40%的权重,w_{11}。由于S_1有一个指示符I_{11},因此这个指示符将接受整个40%的权重。源S_2具有两个指示符,它们可以共享指派给该源的权重值。为简单起见,我们假设I_{21}和I_{22}共享相同的重量-w_{21}和w_{22}各占30%。使用本文公开的技术,可以如下计算组合得分908:$((I_{11}*\ w_{11})+(I_{21}*w_{21})+(I_{22}*w_{22}))/(w_{11}+w_{21}+w_{22})$。通过插入权重,组合得分可以被反映为$=((I_{11}*0.4)+(I_{21}*0.3)+(I_{22}*0.3))/(0.4+0.3+0.3)$。在这个示例中,威胁情报源指示符被评为$I_{11}=65$,$I_{21}=91$,$I_{22}=90$,域的风险得分将为80(四舍五入)。在另一种场景中,如果客户确认域是合法的并且没有域信誉的问题,那么I_{11}变为0。因此,用于这个客户的域风险得分降至54(四舍五入)。在还有另一种场景中,如果客户确认他们想要将应用列入白名单,因为供应商已解决了所有报告的问题,那么I_{11}、I_{21}将为0。因此,用于客户的域风险得分将为0,指示对于客户没有来自这个应用的风险。当客户继续调整组合得分时,回归模型可以周期性地学习权重与风险得分之间的关系,并相应地调整权重值。

[0154] X.用于检测和分析应用的安全性的处理

[0155] 图10图示了根据实施例的用于发现和管理应用的风险的处理的流程图1000。在许多实施例中，下面讨论的处理的一个或多个特征可以由图1的安全监视和控制系统102执行。

[0156] 流程图1000可以通过收集关于由组织的一个或多个用户访问的应用的信息而在1002开始。可以使用本文公开的技术从一个或多个数据源收集信息。数据源可以包括但不限于路由器、网络防火墙、应用防火墙、云应用、云应用移动设备管理(MDM)服务器以及云应用使用跟踪服务器。在一些实施例中，可以通过使用“拉”型机制请求信息从数据源检索信息。在其它实施例中，信息可以由数据源通过“推送”型机制提供而无需请求。可以从组织环境内的网络流量中的数据来监视信息。环境可以是安全的网络环境，诸如配置有一个或多个网络安全性特征(诸如防火墙)的环境。

[0157] 在各种实施例中，从数据源传送的信息可以是各种格式中的任何一种。一些数据源可以经由指定的应用编程接口(API)与之交互。其它数据源可以将信息存储在数据库表或日志文件中。

[0158] 从路由器和网络防火墙检索的信息可以包括关于被访问的网站或由用户的设备做出的其它连接的信息。这种信息可以包括但不限于源和目的地IP、协议、服务(例如，用于HTTP的443)、HTTP请求内的查询字符串和/或产品(例如，用户正在使用什么平台连接到网络的实例名称)。IP地址可以用于执行地理位置的反向查找和/或评估IP地址的信誉。在一些实施例中，利用深度分组检查(DPI) 来访问网络流量内的附加信息，诸如用户名和其它嵌入的数据。用户设备常常利用虚拟专用网络(VPN)连接到企业网络，因此流量穿过企业网络并且可以由网络内的路由器或防火墙捕获。

[0159] 在某些实施例中，可以从第三方获得关于应用的信息和/或从提供感兴趣的应用的应用或另一个应用获得日志信息。例如，可以从由授权应用提供的数据日志中检索关于授权应用的插件应用的信息。在另一个示例中，线索生成(lead-generation)应用(例如，组织未知的第三方应用)可以与应用(诸如由组织已知的云服务提供者提供的应用)一起使用。第三方应用信息可时以包括但不限于访问时间、用户名、登录URL、应用名称、应用源IP和/或登录时间。此外，可以使用本文公开的技术生成补充信息，诸如URL或IP地址的反向查找。在一些实施例中，可以通过提供应用的服务提供者的接口(例如，应用编程接口)来获得信息。

[0160] 在一些实施例中，服务器可以管理并存储与应用的使用相关的信息。可以从服务器检索这种信息。在一个示例中，跟踪服务器可以存储与组织中的用户对云应用的使用相关的信息。用于移动设备管理 (MDM)的服务器可以管理移动设备(诸如智能电话或平板电脑) 上的应用和其它软件的管理。例如，可以在订阅的基础上向客户提供 Google应用软件套件。Microsoft Server可以管理整个企业中的设备上安装的Microsoft产品。Windows 10应用可以由Windows系统管理员管理。还可以在企业中利用其它跨平台的软件管理系统。

[0161] 在步骤1004处，可以使用在步骤1002获得的信息来确定应用是否与安全风险相关联。安全风险可以用于确定应用是否未授权或未经批准以供组织中的用户使用。例如，关于应用的信息可以用于确定组织是否批准了应用的使用。可以使用诸如图9和11中公开的那些相关技术来处理信息。可以从一个或多个源(包括安全监视和控制系统 102、第三方数据

源,以及在步骤1002获得的信息的处理)获得关于应用的信息。该信息可以包括关于提供应用的组织的组织信息。该信息可以包括关于与应用相关的安全性的安全信息。安全信息可以包括与应用的指示符或安全性方面相关的测量或得分。在一些实施例中,可以直接从应用的提供者获得信息。

[0162] 在步骤1006,可以为正在被评估的应用确定一个或多个特征 (例如,安全性指示符)。特征可以包括但不限于应用是独立的还是对经批准的应用的扩展或插件;扩展或插件应用从经批准的应用访问的数据集(例如,销售数据相对于产品代码);应用的类型或类别(例如,业务内容相对于社交网络);与应用相关联的域名的年龄或注册地点;由第三方信誉或排名服务(例如,Alexa、Google排名或排名因素、市值、公开列出的相对于私营公司,等等)提供的与应用相关联的互联网域的域名信誉和/或互联网站点排名,和/或与应用相关联的网站的IP地址信誉,其指示诸如垃圾邮件或任何恶意软件相关问题历史之类的问题(例如,如由第三方服务提供的)。

[0163] 可以使用从其它源检索出的信息来确定特征。该确定涉及通过为被确定用于评估应用可能对组织造成的安全风险而确定的每个特征指派数值(例如,权重)来进行量化。

[0164] 在一些实施例中,附加特征可以关于与被授权的或安全的应用集成的应用。例如,当第三方应用与流行的经批准的应用(诸如 Salesforce、Google应用等等)集成时,经批准的应用供应商会提供关于如何访问数据的指南。由于这种访问,经批准的应用可以被视为具有增加的风险并且其总体风险得分增加。例如,第三方应用可能无法安全地管理和清除被访问的数据,或者第三方应用中的潜在安全漏洞可以是未授权的数据泄漏的源,这超出了经批准的应用的控制范围。可以针对与授予第三方应用的访问的安全性以及第三方应用与经批准或被授权的应用的界面相关的因素确定特征。

[0165] 在步骤1008处,可以基于所确定的特征为一个或多个应用中的每个应用确定安全性得分或安全性的测量。得分和特征可以存储在数据库中,诸如应用注册表。可以使用本文公开的技术(诸如参考图9 的那些技术)来确定得分。

[0166] 安全得分可以是定义安全风险的测量的标度上的值。例如,可以将标度定义为1到5之间,其中越高的值表示越大的风险。在其它实施例中,可以使用适合于特定评估的各种范围和值中的任何一个。得分可以被安全监视和控制系统102用来提供提醒、提供报告和/或执行补救措施。此外,安全监视和控制系统102可以结合关于更安全 (例如,认可的、授权的或经批准的)应用的信息来利用关于应用安全性的得分和其它信息进行安全性评估并确定威胁级别。

[0167] 流程图1000可以在步骤1010结束。

[0168] 图11图示了根据实施例的用于发现和管理应用风险的处理的流程图1100。在许多实施例中,下面讨论的处理的一个或多个特征可以由图1的安全监视和控制系统102执行。流程图1100图示了图10 中描绘的处理的某些实施例。

[0169] 流程图1100可以通过获得关于用户的网络活动的信息在步骤 1102开始。该信息可以从使用用于监视网络活动的技术(包括参考图8公开的那些技术)获得的数据获得。可以通过监视和/或从网络设备获得数据(例如,日志数据或记录数据)来获得关于网络活动的数据。为了让组织监视应用使用,组织可以监视其内部或受保护的网络(例如,内联网)以进行网络活动。可以通过从组织的网络内部和外部的网络流量的网络资源(例如,网络设

备)获得信息来监视网络活动。

[0170] 在一些实施例中,可以从多个数据源收集关于网络活动的数据。可以通过安全监视和控制系统102摄取和处理来获取日志文件,以识别关于网络活动的信息,诸如应用使用。可以使用图8中公开的技术来获得日志文件。可以使用图7中公开的技术从一个或多个源获得关于应用事件的数据。在一些实施例中,可以从一个或多个第三方源 (诸如应用的服务提供者)获得关于网络活动的信息(诸如具体的服务和应用使用)。安全监视和控制系统102可以利用服务提供者的接口来获得关于一个或多个用户的活动的日志信息。

[0171] 可以以多种不同格式从多个源获得信息。可以处理包含该信息的数据,以准备(例如,规格化)信息成用于处理的格式,以确定应用使用。可以处理数据以进行重复数据删除,以识别网络活动的唯一的实例。

[0172] 在步骤1104处,所获得的关于网络活动的信息被用于确定已被访问的一个或多个应用。所获得的关于网络活动的信息可以从关于网络活动的数据获得。数据可以用于网络上的通信。数据进一步关于作为组织的网络上的租户的多个用户的网络。获得关于网络活动的数据可以包括从网络上的一个或多个网络设备获得网络数据。可以通过本文公开的技术从计算环境中实现的一个或多个代理和/或日志管理器获得网络数据。网络数据可以由安全监视和控制系统的日志收集器获得。可以在组织的计算环境中保护网络,使得计算环境是安全的,免受公共网络影响。

[0173] 访问应用可以包括允许应用的数据由不同的应用访问。例如,应用的数据可以由用户同意以从应用的服务提供者访问用户的数据的第三方应用访问。应用可以由用户访问应用的组织授权(例如,批准) 或未授权(例如,未批准)。该信息可以包括关于所使用的应用的数据。数据可以是应用名称或者指向正被访问的应用的链接。关于应用的信息可以用于从第三方源(例如,应用的提供者)检索信息。该信息可以包括在从提供者的服务提供者系统获得的活动数据中。可以识别每个唯一的应用,以确定用户已访问的应用。在一些实施例中,一些应用可以是相同类型或种类,但是可以与不同的实例和/或不同的访问帐户对应。因为每个唯一的应用可以对所评估的一个或多个特征造成安全漏洞,所以可以确定每个应用用于分析。与每个唯一的应用对应的数据可以关联存储,以供应用进行进一步处理。

[0174] 在步骤1106处,为已被访问的一个或多个应用中的每一个确定访问信息。可以使用在步骤1102获得的信息来确定访问信息。可以通过处理数据来识别应用,以识别数据的与对用户访问过的应用的请求对应的部分。数据的该部分可以指示关于对应用的请求的应用信息,该应用信息用于将应用识别为正被用户访问。数据可以包括关于请求的信息(诸如IP地址、源标识符、到应用的链接),或者与请求的源或与应用所在的目的地相关的其它信息。可以根据与每个应用对应的数据来确定访问信息。可以使用数据的部分来确定关于与应用对应的网络活动的访问信息。访问信息可以包括用于访问应用或与访问应用相关的信息。可以从与每个唯一的应用对应的数据获得访问信息。使用关于每个应用的信息,可以为用户识别关于每个应用的访问信息。访问信息可以包括关于访问应用的请求的网络信息,包括关于请求应用的源(例如,源设备)和请求被发送到的目的地的信息。访问信息可以包括但不限于网络活动的时间戳、应用信息(例如,应用名称、访问应用的源位置和/或关于应用的细节)、源的IP地址、的地的IP 地址、关于源的地理位置信息、用户信息(例如,用户标识或电子邮件标识)以及介质访问控制(MAC)地址。应用的源位置可以是链接(诸如URL或

URI)。可以处理在步骤1102获得的信息,以识别关于在步骤1104识别出的每个唯一的应用的网络活动。

[0175] 在步骤1108处,基于访问信息确定关于提供每个应用的提供者系统的域的域信息。可以使用参考图7和8公开的技术来确定域信息。应用的域可以包括关于提供者和提供应用的提供者的系统的信息(例如,主机系统信息)。例如,域信息可以包括域名、IP地址、系统信息或关于提供者系统中的域的主机系统的其它信息。

[0176] 可以通过使用全部或一些访问信息查询一个或多个数据源来确定域信息。安全监视和控制系统102可以维护关于应用和应用的提供者的信息的数据存储。在一些实施例中,第三方数据源可以用于查找或查询关于应用的域的信息。一个第三方数据源可以是由第三方管理的数据库,使得数据库存储关于域的信息和关于一个或多个应用提供者的系统信息。另一个第三方数据源可以是域名系统(DNS)源或存储关于域或域的实体(例如,提供者)的信息的某个其它源。可以基于访问信息来从第三方数据源查询关于域的信息。例如,可以发出 NSlookup命令,以确定访问信息中IP地址的域。

[0177] 在一些实施例中,可以将请求发送到应用的提供者的系统,以获得域信息。基于访问信息,可以生成请求并将其设置到提供应用的系统。可以基于由访问信息指示的应用的源位置来发送请求。通过查询数据源获得的域信息常常可能不提供关于提供者的系统的域的具体信息。该请求可以是对端点(例如,SQL连接端点)的网络调用,以获得应用的证书。该请求可以包括应用的URI。可以从用于应用的访问信息获得URI。在至少一个示例中,网络调用可以是浏览器调用(例如,HTTPS),以获得关于被托管站点的信息的证书,该被托管站点是应用的提供者的域。通过以这种方式发送调用,站点可能无法防止请求被阻止。证书可以包括关于应用的提供者的被托管站点的域信息。除了查询数据源或者作为对查询数据源的替代,可以实现对提供者的系统的请求。

[0178] 步骤1110和1112可以同时执行,或者基于已经识别出的应用以任何次序执行。在步骤1110处,可以为一个或多个应用中的每一个确定组织信息。组织信息可以包括关于服务提供者的每个组织的信息,其与提供已被访问的一个或多个应用中的每一个的提供者系统明显相关联。组织信息可以包括识别与提供应用的提供者系统相关联的组织的信息。组织信息可以包括业务实体信息(诸如组织的注册信息)。组织信息可以包括关于应用的信息,包括关于应用的细节(诸如应用的源和应用的类型)。组织信息可以包括关于提供者系统的位置的位置信息(诸如托管提供者系统的位置)。在一些实施例中,组织信息可以包括关于被访问的每个应用的统计信息。统计信息可以包括与应用相关的网络活动的数据使用、应用的网络流量(例如,上传和下载流量),以及关于应用的使用或操作的其它统计信息。可以使用域信息来确定组织信息,以识别提供应用的组织。

[0179] 组织信息可以从一个或多个源获得。一个源可以包括汇总关于应用的信息的第三方源,包括提供这些应用的(一个或多个)组织。安全监视和控制系统102可以基于监视网络活动来维护其自己的应用信息的数据存储。在一些实施例中,用户可以提供关于应用的信息。该信息可以由安全监视和控制系统102存储。

[0180] 在步骤1112处,可以确定关于已被访问的一个或多个应用中的每一个的安全信息。安全信息可以包括关于应用的一个或多个安全性相关事件的信息。安全信息可以提供关于与安全性有关的应用的一个或多个特征的安全性的测量(例如,安全性得分)。在至少

一个实施例中，可以经由参考图9公开的一个或多个馈送902来获得安全信息。由馈送提供的安全性的测量可以与应用的安全特征对应。安全性的测量可以基于一个或多个指示符或特征。可以使用域信息、组织信息或其组合来确定安全信息。在一些实施例中，可以基于识别应用的信息来获得安全信息。

[0181] 可以从一个或多个源获得安全信息。一个源可以包括汇总关于应用的安全性相关信息的第三方源，包括提供这些应用的(一个或多个) 组织。安全监视和控制系统102可以基于监视网络活动来维护其自己的应用安全信息的数据存储。在一些实施例中，用户可以提供关于应用的安全信息。该信息可以由安全监视和控制系统102存储。可以在由这些源中的任何一个提供的安全信息中指示安全性的测量。在一些实施例中，可以从不同格式的一个或多个源获得安全信息。每个数据源可以提供具体类型的安全信息。安全信息可以被规格化或处理，以便以特定格式或标度提供安全性的测量。

[0182] 可以基于执行步骤1110和/或1112中的一个或多个来执行步骤 1114。在步骤1114处，计算安全性的测量(例如，应用风险得分)，作为针对一个或多个应用中已被访问的每个应用的单独测量。安全性的测量可以是应用的安全性的值或指示。例如，安全性的测量可以是 1(例如，低安全风险)到5(例如，高安全风险)的标度上的值。用于安全性的测量的标度可以基于安全性的一个或多个特征，或者可以共同基于一组特征。

[0183] 在一些实施例中，可以基于一个或多个特征(诸如应用的类型或安全风险)为多个应用计算安全性的测量。可以使用参考图8和9公开的技术来计算安全性的测量。可以使用在流程图1100的先前步骤中确定的任何信息来计算安全性的测量。例如，可以使用组织信息、安全信息或其组合来计算安全性的测量。可以针对安全性的一个或多个指示符或特征来计算安全性的测量。可以为每个特征确定权重值。基于指示符和权重，可以单独或共同为每个特征计算安全性的测量。在一些实施例中，可以基于多个用户(诸如作为具有访问帐户的租户的一组用户)的使用来为应用计算安全性的测量。可以针对由多个用户访问的应用实现流程图1100中的步骤。可以跨一个或多个提供者和/或一个或多个账户针对一种类型的应用计算安全性的测量。

[0184] 在一些实施例中，在步骤1116处，可以提供显示以显示关于已被访问的一个或多个应用中的每一个的信息。显示可以是在应用或 web浏览器中提供的图形界面。显示可以是交互式的，以监视和管理应用的安全性。显示可以由安全监视和控制系统102生成。提供显示可以包括使显示器在客户端处呈现。在生成时，可以将显示发送到要呈现的客户端。参考图15-26公开各种交互式显示器的示例。在一些实施例中，可以将显示提供为发送给客户端的消息中的报告。报告可以是关于与应用相关的安全性的通知。

[0185] 在步骤1118处，可以为一个或多个被访问的应用中的每一个执行一个或多个补救动作。补救动作是以补救或校正为基础执行的动作，以解决由应用造成的安全性(例如，安全风险或威胁)。补救动作的示例包括但不限于发送关于应用的安全性的通知消息、显示关于应用的安全性的信息、调整应用的操作和/或访问(例如，访问的限制性调整)。

[0186] 例如，控制对应用的访问可以包括阻止或防止用户或用户组访问应用。可以以许多方式实现限制、阻止或防止对应用的访问。可以发送或配置一条或多条指令以调整对应用的访问。例如，可以在组织中的网络上配置一条或多条指令，使得可以拒绝对应用的任何请求，或者可以防止在组织外部传送请求，以便有效地拒绝或阻止访问。可以配置一条或多

条指令以拒绝对应用的某些类型的请求。可以在界面处提示用户，以提供信息来配置对应用的访问，使得其根据策略受到限制。

[0187] 在另一个示例中，动作可以是将关于应用的信息放置在白名单或黑名单上，以分别允许或拒绝对应用的访问。在一些实施例中，可以不基于根据策略评估应用来针对每个应用执行补救动作。

[0188] 可以基于应用的安全性的测量来执行对应用的补救动作。补救动作可以是自动的、手动的、征求用户或管理员参与，或其组合。可以基于来自用户(例如，分析员)的输入配置动作。可以基于一个或多个策略执行补救动作。策略可以是用户可配置的和/或基于安全性的反馈进行调节，诸如参考图9公开的技术。例如，可以基于满足风险阈值(例如，高风险)的应用的安全性的测量来执行补救动作。在一些实施例中，可以基于用于应用的一个或多个特征的安全信息来执行补救动作。可以基于那些特征来计算安全性的测量。照此，补救措动作施可以基于针对为其计算安全性的测量的那些特征的安全性的测量。参考图15-26显示安全性的测量和补救动作的示例。

[0189] 在一些实施例中，可以基于安全策略来执行补救动作。安全策略可以基于安全性的测量和/或安全信息来定义要执行的一个或多个补救动作。可以基于本文所公开的安全性的测量和/或任何信息(例如，组织信息或安全信息)来应用安全策略。可以执行操作以评估安全风险或威胁。安全风险或威胁可以基于安全性的测量和/或安全信息 (例如，一个或多个安全性指示符)。策略可以定义一个或多个标准，诸如定义何时采取补救动作的阈值(例如，安全性阈值或风险阈值)。可以根据安全性测量的标度或由安全性指示符的提供者设置的标度通过一个或多个值来定义标准。例如，应用安全策略可以包括确定安全性的测量是否满足应用的风险阈值。可以将安全性的测量与策略中的一个或多个值进行比较，以评估安全风险的严重性。可以基于一个或多个安全性指示符来定义值。可以基于一个或多个安全性指示符来定义这些值，使得将安全性的测量与基于用于计算安全性的测量的安全性指示符定义的阈值进行比较。还可以比较安全信息中获得的安全指示符，以进一步评估安全风险。

[0190] 在一些实施例中，补救动作可以是配置计算环境的一个或多个方面以防止在计算环境内访问应用。可以将一条或多条指令发送到组织的计算环境的计算机系统和/或网络设备，以指定要阻止哪个应用以及阻止或限制应用的对象。可以通过可以控制计算环境中的访问的策略或其它可配置信息来配置对应用的访问。在一些实施例中，可以将指令发送到由用户操作的客户端设备上的代理。可以指示代理改变操作以防止对特定应用的访问和/或在使用客户端设备的特定环境中改变应用的操作。补救动作可以是防止由多个用户访问应用。在一些实施例中，补救动作可以包括将一条或多条指令发送到服务提供者系统。例如，可以将指令发送到服务提供者系统，以调整用于访问应用的一个或多个安全控制和/或设置。服务提供者系统可以提供访问安全控制和/或设置的接口。补救动作可以包括使用接口(例如，通过进行呼叫)来调整应用的安全控制和/或设置。

[0191] 补救动作可以包括提醒用途。可以向管理员或其他用户的设备发送关于安全风险和/或对应用的访问的改变的提醒。在一些实施例中，针对应用的补救动作包括使图形界面提示用户调整应用的配置操作。

[0192] 流程图1100可以在步骤1120结束。

[0193] 图12图示了根据实施例的用于发现和管理应用风险的处理的流程图1200。在许多实施例中，下面讨论的处理的一个或多个特征可以由图1的安全监视和控制系统102执行。流程图1200可以被实现为参考图10和11公开的技术的一部分或使用所公开的技术来实现。可以实现参考流程图1200公开的处理，以评估和管理已经跨多个服务提供者(例如，云服务提供者)使用的应用的安全性。该应用可以是第一应用，其使能或促进访问由与应用第一应用的服务提供者不同或相同的服务提供者提供的第二应用和/或第二应用的数据。

[0194] 流程图1200可以通过获得关于从组织的网络上的服务提供者系统(例如，第一服务提供者系统)访问的一个或多个应用的数据(例如，“第一数据”)在步骤1202开始。可以通过由服务提供者的第一服务提供者系统提供的编程接口来获得第一数据。数据可以提供访问信息，诸如被访问的应用和/或数据以及关于如何访问应用和/或数据的信息。访问信息可以提供关于从第一服务提供者系统访问应用或其数据的第三方应用的信息。

[0195] 在步骤1204处，可以获得关于从组织的网络上的服务提供者系统(例如，第二服务提供者系统)访问的一个或多个应用的数据(例如，“第二数据”)。可以通过由服务提供者的第二服务提供者系统提供的编程接口来获得第二数据。数据可以提供访问信息，诸如被访问的应用和/或数据以及关于如何访问应用和/或数据的信息。访问信息可以提供关于从第二服务提供者系统访问应用或其数据的第三方应用的信息。

[0196] 可以从若干服务提供者系统汇总访问信息，以评估用户在组织的网络上访问的应用的安全性。来自每个服务提供者系统的访问信息可以被处理，以确定用户在组织的网络上访问的一个或多个应用。应用可以是不同的，但具有一个或多个共同的属性。应用可以是不同的，但可以基于允许第三方应用访问应用和/或其数据的用户而相关。允许第三方应用访问可能存在风险和/或组织不允许。

[0197] 在步骤1206处，可以确定用户访问的应用(例如，第三应用) 的访问信息。在至少一个实施例中，应用可以是通过第一服务提供者系统和第二提供者系统访问的应用的类型。可以处理来自每个服务提供者系统的访问信息，以识别通过第一服务提供者系统和第二提供者系统访问的应用的应用类型。可以基于从每个提供者系统获得的应用信息将应用识别为一种类型的应用。可以使用一个或多个数据源来检索用于所访问的每个应用的应用信息。在步骤1206之后的步骤中，其中用户访问的(一个或多个)应用具有共同类型，可以为每个应用确定在以下步骤中确定的信息。可以为每个应用或应用的组合计算安全性的测量。安全性的测量可以基于平均值或者基于每个应用的安全性的测量组合的测量。

[0198] 在至少一个实施例中，来自每个服务提供者系统的访问信息可以用于确定相同的第三方应用正被用于访问由每个服务提供者系统提供的不同应用和/或其数据。每个服务提供者系统可以提供可以指示通过第三方应用访问应用的信息。

[0199] 在步骤1208处，可以确定关于(一个或多个)应用的提供者系统的域信息。步骤1210和1212可以同时或基于已经识别的应用以任何次序执行。在步骤1210处，可以为应用确定组织信息。在步骤 1212处，可以确定关于应用的安全信息。可以使用本文公开的技术(诸如参考图11公开的技术)来确定针对流程图1200确定的信息。

[0200] 在步骤1214处，可以为已被访问的应用计算安全性的测量。可以为每个应用或者被识别为由用户访问的应用的组合计算安全性的测量。安全性的测量可以基于平均值或基于每个应用的安全性的测量组合的测量。

[0201] 在步骤1216处，提供关于已被访问的(一个或多个)应用的信息的交互式显示。交互式显示可以作为图形界面的一部分包括在内或作为图形界面生成。图形界面可以显示应用的安全性的测量。

[0202] 在步骤1218处，可以对已被访问的(一个或多个)应用执行补救动作。可以如本文所公开的那样执行补救动作，诸如参考图11公开的技术。在应用是在服务提供者系统处提供对应用或其数据的访问的第三方应用的情况下，可以防止第三方应用访问该应用。在一些实施例中，可以向服务提供者系统发送请求，以限制或拒绝由第三方应用对(一个或多个)应用和/或其数据的访问。在一些实施例中，可以修改交互式显示，以提示用户调整用于第三方应用的设置，以限制或撤销从服务提供者系统对应用和/或其数据的访问。

[0203] 流程图1200可以在步骤1220结束。

[0204] XI.基于应用使用计算用户的安全性的测量

[0205] 图13和14图示了根据一些实施例的用于基于应用使用来计算用户的安全性的测量的技术。具体而言，图13图示了处理的序列流程图1300的示例。这些技术可以由安全监视和控制系统102实现。可以使用参考图9公开的技术来计算用户的安全性的测量。

[0206] 用户的安全性的测量(在本文也称为“用户风险得分”)可以提供指示，作为用户可能对组织造成的安全性的风险或威胁。如上面所讨论的，用户可以基于以未授权或不安全的方式使用应用而对组织的网络造成安全威胁。这种使用可能使组织暴露于其专用网络和数据的漏洞。在一些情况下，应用可能会基于组织的资源(诸如公司网络和 /或计算资源)的低效或不当使用而对组织造成威胁。用户风险得分可以提供指示与组织中的用户相关的安全威胁的严重性的测量。可以通过剖析用户对应用的动作来连续生成用户风险得分。

[0207] 在一些实施例中，安全监视和控制系统102可以提供图形界面，该图形界面可以被呈现，以显示关于风险得分和/或与风险得分相关的信息。图形界面的示例在2017年2月17日提交的标题为“Systems and Methods for Discovering and Monitoring Unsanctioned Enterprise Assets”的优先权申请美国临时申请No. 62/460,716[代理人案卷号:088325-1039197(185502US)]中示出。图形界面可以在控制台中呈现为具有风险得分和相关可视化(KSI) 的用户报告。图形界面可以用作单一管理平台(single pane of glass)，其组合来自各种源的风险元素并且对于经批准和未经批准的应用以统一的方式呈现。图形界面使用户(例如，安全管理员)能够查看相关联的风险指示符，以了解为什么一些用户的风险得分高，其中包括在应用中执行的异常动作，访问过有风险的未经批准的应用等等。这有助于用户采取或配置补救动作，如在防火墙中阻止应用、教育用户避开应用或暂停用户帐户。图形界面可以使用户能够基于创建匹配某些条件(诸如风险应用得分、应用类别、用户风险得分等等) 的策略来配置定制提醒。

[0208] 可以基于由一个或多个第三方源、一个或多个用户、由安全控制和管理系统102管理和策展的源或其组合提供的信息来计算用户的安全性的测量。用户的安全性的测量可以基于包括但不限于以下的信息:关于应用和应用的提供者的信息(“组织信息”)、关于应用的安全性的信息(“安全信息”)和/或与应用相关的使用(“应用使用信息”)。组织信息和安全信息可以包括本文公开的信息，诸如关于确定应用的风险的测量。应用使用信息可以指示关于应用的使用的信息，诸如所执行的操作/动作的类型(例如，数据的大量导出或针对应用的联系人下载或过多的文件访问)、被访问的应用的类别(例如，与恶意软件网站、信息

泄露网站或黑客使用的应用/工具相关联的应用将增加用户风险得分)，或者与应用的使用的异常偏差。例如，应用使用信息可以基于很少使用一个提供者系统访问文件的用户突然开始下载大量文档来提供恶意软件活动的指示。

[0209] 用户的安全性的测量可以是定义用户的安全风险的测量的标度上的值(例如，用户风险得分)。例如，可以将标度定义为1到5之间，其中越高的值表示用户的越大风险。在其它实施例中，可以使用适合于特定评估的各种范围和值中的任何一个。得分可以被安全监视和控制系统102用来提供提醒、提供报告和/或执行补救措施。安全性的测量是用作优先级指示符的值，以帮助用户(例如，安全管理员)减轻由应用造成的安全威胁。在一些实施例中，可以以若干方式计算安全性的测量。

[0210] 用户风险得分可以指示关于由具体应用对组织造成的安全威胁的严重性的安全性的测量。可以基于一个或多个指示符(在本文中也称为“威胁指示符”或“安全性指示符”)来计算用户风险得分。每个指示符可以是指示安全风险的值或信息。例如，在图13中，可以从一个或多个数据源(在本文也称为“风险得分馈送”)获得唯一的安全性指示符，提供一个或多个应用指示符的“馈送”。每个唯一的指示符(“I”)(在本文被统称为指示符“I_1，I_2，...，I_n”1304)可以分别由每个数据源提供。指示符可以是基于与应用相关或关于应用的信息的特定类型的指示符，诸如上面指出的信息类型。指示符可以是提供由用户造成的安全威胁的指示的值。例如，第一指示符可以是指示用户的第一安全威胁的第一值。第二指示符可以是指示用户的第二安全威胁的第二值。第一指示符可以从第一源获得，并且第二指示符可以从第二源获得。

[0211] 指示符1302可以包括，例如，用于授权应用的用户风险得分、用于未知/未授权应用的风险得分，或与应用相关联的动作。以下示例图示如何评估用户风险得分。要注意的是，在这个示例中使用的指示符数量有限，但可以将系统配置为使用附加的指示符。在一个示例中，第一指示符I_1可以是从被授权(例如，批准)供组织使用的应用的数据源获得的用户风险得分。可以在经批准的应用中从用户动作计算用户风险得分。这个风险得分组合了经批准的应用中的各种用户活动，诸如文档的上传/下载。第二指示符I_2可以是未经批准的应用的上传量偏差的测量。例如，第二指示符可以被计算为(1天上传量 -30天平均上传量)/(30天上传量标准偏差)。第三指示符I_3可以是指示所访问的站点的风险得分偏差的度量。例如，第三指示符可以被计算为(应用风险得分的1天总和-30天每日平均应用风险得分) /(30天每日应用风险得分标准偏差)。在这个示例中，可以使用所有三个指示符来计算用户风险得分。在一些实施例中，可以使用诸如参考图14描述的那些附加指示符来计算用户风险得分。

[0212] 在一些实施例中，安全监视和控制系统102可以使用用于应用和用户的风险得分来产生图形。可以使用一个或多个图形来导出附加指示符。现在转到图14，改图是访问应用A和B的第一用户集群的图形1402。图14图示了访问应用X、Y和Z的第二用户集群的图形1404。可以使用从一个或多个数据源获得的关于用户和应用使用的信息(诸如本文公开的那些)生成每个图形。可以使用本领域技术人员已知的一种或多种聚类算法来生成图形。集群算法的示例可以包括马尔可夫聚类(MCL)算法。使用一个或多个图形，可以基于一个或多个属性来识别一组用户，诸如访问类似站点的用户。可以使用图形分析来执行这种分析，包括一种或多种已知的图形分析技术，诸如 Girvan-Newman边缘聚类算法。

[0213] 继续上面的指示符I_{1-3}的示例，可以使用图形分析导出第四指示符I_4。例如，I_4可以被计算为(应用风险得分的1天总和-集群的 30天每日平均应用风险得分)/(集群的30天每日应用风险得分标准偏差)。第五指示符I_5可以被计算为(1天上传量-集群的30天平均上传量)/(集群的30天上传量标准偏差)。

[0214] 每个威胁指示符可以表示用户风险得分，该用户风险得分是根据由用于那个指示符的源定义的标度指示用户的安全风险或威胁的测量的值。在一些实施例中，可以将威胁指示符与标度进行比较，以确定用户风险得分。标度可以由源提供的信息定义或基于由源提供的信息。

[0215] 安全监视和控制系统102可以基于一个或多个威胁指示符来计算用户风险得分。换句话说，可以将安全性的测量计算为用户的安全风险的组合测量。可以处理每个指示符，以根据要用于所有指示符的标度(例如，从0到100的值的标度)将指示符的值调整(例如，规格化)到调整后的值。一旦被规格化，就可以组合每个指示符的值以确定组合得分。

[0216] 指示用户风险测量的组合安全性得分1308可以基于所有或一些指示符。为确定组合安全得分而考虑的指示符的数量和/或类型可以是可配置的。照此，安全监视和控制系统102可以被配置为添加或移除从其获得指示符的源，并且可以被配置为添加或移除从源获得的指示符1304。在一些实施例中，可以呈现图形界面，其使得用户能够配置为得分而考虑的指示符的数量和类型。在一些实施例中，组合得分可以基于定义要通过其计算得分的标准的安全策略。标准可以基于安全性的一个或多个属性。这些属性可以用于选择要为得分考虑的指示符。

[0217] 在一些实施例中，组合用户风险得分1308可以基于使用用于每个指示符的权重值的指示符的组合。例如，可以选择权重(“W”) (在本文统称为权重“W_1,W_2,...,W_n”1304)以应用于用于计算组合得分1308的一个或多个具体指示符。权重可以是整数1或1的一部分的值。可以为不同的指示符选择不同的权重。在上面的示例中，第一权重可以是用于第一指示符的第一权重值，并且第二权重可以是用于第二指示符的第二权重值。重量值可以不同。

[0218] 权重可以由用户通过图形界面来配置。在一些实施例中，可以基于安全策略来选择权重，其中安全策略基于特定指示符被给予特定权重来定义。当指示符对安全风险具有更多重要性或建议时，可以考虑更大的权重值。当指示符对安全风险具有较少重要性或建议时，可以考虑较小的权重值。在一些实施例中，可以为来自特定源的所有指示符选择权重。例如，可以基于源的可靠性或信任将权重应用于来自那个源的所有指示符。在一些实施例中，安全监视和控制系统102可以存储关于应用的威胁研究分析的数据。这些数据可以用于选择性地为每个指示符选择权重。

[0219] 可以基于指示符和对那些指示符的权重的考虑来计算组合得分。在至少一个实施例中，可以使用等式1308来计算组合得分，以提供组合得分＝$(I_1(W_1)+I_2(W_2)+.....I_n(W_n))/(W_{1+}W_2+\cdots W_n)$。在这个等式中，通过将每个指示符乘以相应的权重(“W”)1306来计算每个指示符(“I”)1304的值。计算第一值，该值是针对每个指示符计算的值的总和$(I_1(W_1)+I_2(W_2)+.....I_n(W_n))$。计算第二值，该值是被应用以获得第一值的每个权重值的总和。可以基于将第一值除以第二值来计算组合得分1308。在从上面继续的示例中，用户风险得分可以被计算为$(I_1(W_1)+I_2(W_2)+I_3(W_3)+I_4(W_4)+I_5(W_5))/(W_{1+}W_2+W_{3+}W_4+W_5)$。

[0220] 在一些实施例中，安全监视和控制系统102可以从一个或多个用户获得关于组合

得分1308的有效性和准确性的反馈1310。反馈1310 可以通过网络获得，通过图形界面或手动反馈来促进。可以基于反馈 1310来调整源、指示符和/或权重中的任何一个。基于反馈1310，可以调整组合得分1308。可以以与计算组合得分1308相同的方式计算新的组合得分1312(“调整后的得分”)。除调整后的得分1312可以基于基于反馈1310选择的指示符和/或权重来计算之外。可以从用于计算组合得分1308的内容中添加或移除源、指示符和/或权重。用于指示符的权重值可以基于我们的安全性分析师以及客户反馈来周期性地修订，以改进风险得分。用于指示符权重的修订处理可以通过自动机器学习算法(诸如决策树和神经网络)来执行。

[0221] 可以基于关于特定安全威胁的每个指示符和/或组合得分来执行回归分析1314。回归分析可以包括建立并更新线性回归模型。线性回归模型可以提供诸如$S=c_1(I_1)+c_2(I_2)+\cdots+c_n(I_n)$之类的输出。由回归模型计算出的系数$c_i$可以是新的或修改后的权重，其将替换用于计算组合得分1308的初始权重。随着更多反馈和更多数据被收集，该模型将提供更高的准确性。

[0222] 在一些实施例中，计算用户风险得分可以包括缩放针对每个指示符计算的各个得分(或Z得分)。在一个说明性方法中，负z得分被设置为0。其原因是低于平均活动水平被认为在正常范围内。高于 6的Z得分可以缩放到6(z得分3被认为是离群值，并且z得分6 被认为是极端离群值)。0到6之间的Z得分如下在0和100之间缩放：缩放后的z得分＝z得分*(100/6)。

[0223] 继续上面讨论的示例，指示符I_1可以是经批准的应用风险得分 92(0-100的标度)，因此该得分可以不缩放。指示符I_2可以被计算为原始z得分：(100-20)/10＝8，其中今天的上传量是100MB并且最近30天的平均值是20MB并且标准偏差是10MB。由于得分是8，因此可能需要进行缩放。缩放后的得分可以是100.000。指示符I_3可以被计算为原始z得分：(50-20)/5＝6，其中今天访问的站点的平均风险得分是30，过去30天的平均值是20，并且标准差是5。I_3可以被缩放到100.000。指示符I_4可以被计算为原始z得分：(30-25)/10＝0.5，其中今天访问的站点的平均风险得分是30，过去30天的对等组的平均值是25，并且标准偏差是10。I_4的得分可以被缩放到8.3333。指示符I_5可以被计算为原始z得分：(40-60)/30＝-0.667，其中今天的上传量是40MB，过去30天的对等组的平均值是60MB，并且标准偏差是30MB。I_5的得分可以被缩放到0。

[0224] 继续该示例，基于数据质量和数量，可以如下为每个指示符指派数据源权重：W_1＝60％，W_2＝30％，$W_{3=}$5％，$W_{4=}$2％，$W_{5=}$3％。可以使用权重和指示符(其可以被缩放)来计算用户风险得分。在这个示例中，用户风险得分(缩放后的Z得分)可以被计算为(0.60*92) +(0.30*100.0)+(0.05*100.0)+(0.02*8.333)+(0.03*0)＝90(四舍五入)。如果管理员可以验证用户没有其它重大风险，那么管理员可以将最终得分从90调整到25。得分可以通过线性回归算法应用于线性回归分析 1314：特征(I_1,I_2),...)：92,100.0,100.0,8.333,0，目标变量 (调整后的组合得分)：25。对所有用户得分使用这些以及特征和目标变量，回归算法将针对客户的每个指示符计算新的权重(w1， w2,...)，并相应地更新用于所有用户(在客户租户中)的风险得分。

[0225] Ⅻ.用于发现和管理应用的安全性的界面

[0226] 图15-26图示了根据一些实施例的界面，例如，用于发现和管理计算环境中的应用

的安全性的图形界面。诸如图形用户界面(GUI) 之类的每个图形界面可以在客户端处显示,其访问由图中公开的安全监视和控制系统102提供的服务。图形界面可以被显示为访问门户 (诸如网站)的一部分,或者显示在应用中。图形界面的附加示例在于2017年2月17日提交的标题为“Systems and Methods for Discovering and Monitoring Unsanctioned Enterprise Assets”的优先权申请美国临时申请No.62/460,716[代理人案卷号:088325-1039197 (185502US)]中显示。

[0227] 在这个公开中,“元素”可以包括在图形界面中。元素可以是可显示的和/或图形界面的一部分。元素的示例包括但不限于控件、按钮、导航条或其它可见部件,其可以是可以通过声音、视觉、触摸或其组合感知的界面的一部分。元素可以接收输入。例如,交互式元素可以是交互式以接收输入的元素。交互式元素可以接收输入,以使得能够与图形界面交互。例如,交互式元素可以是图形界面中的许多元素之一,诸如为其显示网络数据的热图。

[0228] 在图15中,在应用中示出了GUI 1500,其使得用户能够发现和管理在组织的网络上被访问的应用的安全性。GUI 1500被示为交互式界面(例如,仪表板),其是交互式的,以查看已被发现为在组织的网络上被访问的应用。图15-26中的GUI可以作为应用中仪表板的一部分或基于其与应用中的仪表板的交互来呈现。仪表板可以包括用于交互式界面的一个或多个交互式选项卡,诸如“摘要”、“应用发现”和“关键安全性指示符”。界面中的信息和元素可以是附图的多个GUI中的参考,以图示附加的示例。

[0229] 现在转到图15的示例,示出了GUI 1500,其中选择了“应用发现”。可以基于如何获得信息来显示关于应用的信息。例如,关于应用的信息可以显示在用于基于注册已知的应用的界面“来自已注册的应用”的选项卡下。在另一个示例中,关于应用的信息可以显示在用于基于这里公开的用于识别由用户访问的应用的技术被发现的应用的界面“来自日志”1504的选项卡下。关于任一选项卡中的应用所示出的功能可以被组合成单个选项卡,或者可以在另一个选项卡中实现。

[0230] GUI 1500可以包括是交互式的元素1506,以选择性地提供输入来过滤所发现的应用。可以基于一个或多个属性来执行过滤,诸如时间、日期、应用类型、动作、风险或针对所发现的应用移位 (displated)的任何其它类型的信息。

[0231] 如本文所公开的,可以使用许多技术来发现应用,诸如检查用于网络活动的日志文件(例如,系统日志文件)。GUI 1500可以包括是交互式的元素1510,以提供输入来配置如何收集日志文件以进行分析以发现应用。与元素1510的交互可以使得附加的或修改后的GUI 2000(“系统日志设置”)在GUI 1500旁边或与GUI 1500一起显示。GUI 2000可以使得用户能够配置如何收集日志文件。GUI 2000可以包括一个或多个元素,其可以接收输入来配置用于访问日志文件的令牌、用于日志文件的路径或源、放置所收集的日志文件的位置(例如,端点),以及用于日志文件的一个或多个连接参数(例如,端口)。用于配置日志文件的参数可以包括用于安全位置的一个或多个参数和/或用于存储日志文件的连接。

[0232] GUI 1500可以是交互式的,以显示关于所发现的每个应用的信息的网格或表视图。在所示的示例中,GUI 1500被显示为具有用于已被发现被访问的每个应用的行。每行显示关于已发现的应用的信息,包括提供该应用的主机系统的域、最高风险、(一个或多个)事故和可配置的补救动作。视图中的每个条目或行可以是交互式的,包括每个条目中的字段。最高风险可以显示关于应用的不同类别的安全风险的信息。

[0233] GUI 1500可以包括交互式的元素1508,以导出表中用于任何应用条目的信息的数据文件。数据文件可以用于管理、监视和跟进关于应用安全性的动作。

[0234] 与对应于表的条目中的“事故”的元素的交互可以导致图19中的GUI 1900。该元素可以是交互式的,以选择先前打开的一个或多个事故。GUI 1900可以在GUI 1500的顶部或在其旁边显示。可以呈现GUI以显示关于已经打开的事故的信息。GUI 1900可以包括一个或多个交互式元素,以提供输入来配置应用的事件。与用于打开事故的元素的交互可以特定于与条目的元素对应的应用。图19的GUI 1900可以包括元素1902(“类别”)、1904(“发现的应用名称”)、1906(“供应商域”)、1908(“描述”)、1910(“补救动作”)、1912(“指派给”)、1914(“优先权”)、1916(“认可”)、1918(“新事故”)和1920(“取消”)。

[0235] 元素1902可以指示针对其发现应用的一个或多个安全风险。在发起新事故之前,可能已在GUI 1500中选择了风险。元素1904可以指示应用的名称。元素1906可以指示提供该应用的主机系统的域。元素1908可以是交互式的,以指定关于事故的描述。可以基于安全风险预先填写描述。描述可以用于提供关于应用的使用的描述。元素 1910可以是交互式的,以指定一个或多个补救动作。可以基于安全风险在元素1910中预先选择补救动作。元素1912可以是交互式的,以指定要被通知关于应用的安全性的一个或多个用户。元素1914可以是交互式的,以指定应用的优先级。元素1916可以是交互式的,以指示认可创建事故。元素1918可以是交互式的,以基于对GUI 1900的输入来提交创建事故的请求。元素1920可以是交互式的,以取消创建事故。

[0236] 与对应于表中的条目的元素的交互可以使GUI 1500被修改,以显示关于与那个条目对应的所发现的应用的信息。例如,在图16中, GUI 1500被示为具有用于所发现的应用的条目的扩展的GUI 1600 (例如,图形界面)。GUI 1600可以显示关于应用的组织信息。组织信息可以包括关于与应用相关的使用的信息,诸如用户的数量、网络活动(例如,上传的数据和下载的数据)、应用的类别以及关于提供应用的组织的信息。关于组织的信息可以包括名称、地址、域、网站、组织的描述和/或关于组织对应用的注册的其它信息。

[0237] GUI 1600可以显示关于在GUI 1500中的条目中显示的每个安全风险的信息。每个安全风险可以与描述该安全风险的信息一起显示,并且可以以关于安全风险的视觉外观显示。例如,视觉外观可以具有图像和颜色,以指示风险的严重性。可以基于为发现的应用确定的安全信息中的安全性指示符来确定安全风险。可以显示特定于统计信息的信息或关于安全风险的底层信息。在一些实施例中,安全风险可以基于由第三方源、用户提供的和/或由安全监视和控制系统102策展的信息。在一些实施例中,安全风险可以基于安全性的一个或多个指示符。安全风险可以基于一个或多个安全策略的应用。可以使用针对一个或多个安全风险确定的安全性的测量来应用安全策略。

[0238] 在图16所示的示例中,GUI 1600可以包括用于每个安全风险的元素。与安全风险对应的元素可以是交互式的,以便或者在GUI 1500旁边或者作为GUI 1500的附加显示GUI。在一个示例中,可以基于与用于安全风险(“IP信誉”)的元素1604的交互来显示图17 的GUI 1700。在另一个示例中,可以基于与用于安全风险(“应用安全性”)的元素1606的交互来显示图18的GUI 1800。

[0239] GUI 1700和1800中的每一个显示关于具体安全风险的信息。该信息可以对应于与访问应用的安全风险相关的一个或多个事件。可以基于包括关于实际事件的信息的每个事

件或事件类别来显示信息。可以显示每个安全风险以及关于该问题的信息。可以提供一个或多个补救动作。该信息可以由第三方源、用户提供，和/或由安全监视和控制系统102策展。例如，该信息可以由应用的提供者提供。可以显示每个安全性风险，其具有指示风险严重性的视觉外观。在一些实施例中，可以向元素呈现每个风险，使得元素可以是交互式的，以使得显示另一个GUI以自动化和/或配置补救动作。

[0240] 现在返回图15，对于与唯一发现的应用对应的每个条目，可以在GUI 1500中呈现诸如1512之类的元素。该元素可以是交互式的，以便为应用配置一个或多个补救动作。该元素可以提供一个或多个选项，其可以特定于应用的安全风险。与元素的交互可以使得另一个 GUI在GUI 1500旁边或者作为GUI 150的附加显示，以配置补救动作。可以选择安全风险，以使得为安全风险选择补救选项。在一些实施例中，可以基于安全风险和一个或多个安全策略来呈现一个或多个补救动作。已执行的补救动作也可以与用于已发现的应用的条目一起显示。

[0241] 与元素1502的交互可以使GUI 1500被更新，以显示图21的 GUI 2100。类似于GUI 1500，GUI 2100可以显示关于被发现的应用的信息。该信息可能包括安全风险。GUI 2100可以像GUI 1500那样是交互式的。在GUI 2100中识别出的应用可以是已经向组织注册的应用。与图21中的条目2102的交互可以使GUI 2200被显示。

[0242] 类似于图17和18，图23-25显示具有关于在GUI 2200中显示的安全风险的信息的GUI。GUI 2200可以包括用于端点安全风险的元素2202(“端点安全性”)、用于网络安全风险的元素2204 (“网络安全性”)，以及用于IP信誉安全风险的元素2206 (“IP信誉”)。元素2202、元素2204和元素2206中的每一个可以分别使得图23的GUI 2300、图24的GUI 2400和图25的GUI 2500在GUI 2200旁边或作为GUI 2200的附加显示。

[0243] 图26图示了“应用发现”的GUI 2600，其示出了关于被发现的应用的细节。GUI 2600可以包括交互式视图2602，其针对所发现的每个唯一的应用在表视图中显示条目。类似于图15的GUI 1500，每个条目可以包括关于应用的信息，包括应用名称和应用的提供者。与 GUI 1500一样，每个条目可以是交互式的，以使得显示关于与该条目对应的应用的附加信息。条目可以指示与一个或多个指示符相关联的一个或多个最高风险。与GUI 1500不同，GUI 2600可以示出用于所发现的每个唯一的应用的条目，而不管发现的源(例如，日志或注册)。

[0244] 在一些实施例中，条目可以指示关于与所发现的应用相关的事件的其它信息。条目可以指示关于应用的使用的信息，诸如已经访问应用的用户的数量以及访问应用的日期。

[0245] 在一些实施例中，表视图中的条目可以与作为注册的应用和/或从日志发现的应用对应。每个条目可以包括一个或多个元素以执行补救动作。视图2602可以包括一个或多个是交互式的元素(例如，工具栏)，以配置何时识别已被访问的应用和/或自动发现应用的时间段。工具栏可以是交互式的，以配置已被访问的应用的通知、设置和搜索。

[0246] GUI 2600可以包括区域2604，该区域显示关于应用使用的测量的统计信息的可视化。统计信息可以基于一个或多个安全风险来显示。GUI 2600可以包括基于使用的测量显示应用使用的可视化的区域 2606。GUI 2600可以包括区域2608，基于诸如类别、域、服务提供者、安全风险或与应用相关联的其它类别的信息之类的信息来显示应用的分组的可视

化。

[0247] XIII.用于访问管理系统和客户端系统的通用计算机系统

[0248] 图27描绘了用于实现实施例的分布式系统2700的简化图。在所示的实施例中，分布式系统2700包括一个或多个客户端计算设备 2702、2704、2706和2708，这些客户端计算设备被配置为通过一个或多个网络2710执行和操作客户端应用，诸如web浏览器、专有客户端(例如Oracle Forms)等。服务器2712可以经由网络2710与远程客户端计算设备2702、2704、2706和2708通信地耦合。

[0249] 在各种实施例中，服务器2712可以适于运行一个或多个服务或软件应用。在某些实施例中，服务器2712还可以提供其它服务，或者软件应用可以包括非虚拟和虚拟环境。在一些实施例中，这些服务可以作为基于web的或云服务或者在软件即服务(SaaS)模型下提供给客户端计算设备2702、2704、2706和/或2708的用户。操作客户端计算设备2702、2704、2706和/或2708的用户可以进而利用一个或多个客户端应用与服务器2712交互，以利用由这些部件提供的服务。

[0250] 在图27中描绘的配置中，系统2700的软件部件2718、2720和 2722被示为在服务器2712上实现。在其它实施例中，系统2700的一个或多个部件和/或由这些部件提供的服务也可以由客户端计算设备2702、2704、2706和/或2708中的一个或多个实现。操作客户端计算设备的用户然后可以利用一个或多个客户端应用来使用由这些部件提供的服务。这些部件可以用硬件、固件、软件或其组合实现。应当理解，各种不同的系统配置是可能的，其可以与分布式系统2700 不同。因此，图27中所示的实施例是用于实现实施例系统的分布式系统的一个示例，并且不旨在进行限制。

[0251] 客户端计算设备2702、2704、2706和/或2708可以包括各种类型的计算系统。例如，客户端计算设备可以包括便携式手持设备(例如，**iPhone®**、蜂窝电话、**iPad®**、计算平板、个人数字助理 (PDA))或可穿戴设备(例如，Google**Glass®**头戴式显示器)，其运行诸如Microsoft Windows **Mobile®**之类的软件和/或诸如iOS、Windows Phone、Android、BlackBerry 10，Palm OS之类的各种移动操作系统。设备可以支持各种应用，诸如各种互联网相关的应用、电子邮件、短消息服务(SMS)应用，并且可以使用各种其它通信协议。客户端计算设备还可以包括通用个人计算机，作为示例，运行各种版本的Microsoft**Windows®**、Apple **Macintosh®**和/或Linux操作系统的个人计算机和/或膝上型计算机。客户端计算设备可以是运行任何各种商用的**UNIX®**或类UNIX操作系统(包括但不限于诸如像Google Chrome OS的各种GNU/Linux操作系统)的工作站计算机。客户端计算设备还可以包括能够提供(一个或多个)网络2710通信的电子设备，诸如瘦客户端计算机、启用互联网的游戏系统(例如，具有或不具有**Kinect®**手势输入设备的Microsoft **Xbox®**游戏控制台) 和/或个人消息传送设备。

[0252] 虽然图27中的分布式系统2700被示为具有四个客户端计算设备，但是可以支持任何数量的客户端计算设备。其它设备，诸如具有传感器的设备等，可以与服务器2712交互。

[0253] 分布式系统2700中的(一个或多个)网络2710可以是对本领域技术人员熟悉的可以利用任何各种可用协议支持数据通信的任何类型的网络，其中各种协议包括但不限于TCP/IP(传输控制协议/互联网协议)、SNA(系统网络体系架构)、IPX(互联网分组交换)、

AppleTalk等。仅仅作为示例，(一个或多个)网络2710可以是局域网(LAN)、基于以太网的网络、令牌环、广域网、互联网、虚拟网络、虚拟专用网络(VPN)、内联网、外联网、公共交换电话网络(PSTN)、红外网络、无线网络(例如，在任何电气和电子协会 (IEEE)802.11协议套件、**Bluetooth®**、和/或任何其它无线协议下操作的网络)和/或这些和/或其它网络的任意组合。

[0254] 服务器2712可以由一个或多个通用计算机、专用服务器计算机 (作为示例，包括PC(个人计算机)服务器、**UNIX®**服务器、中档服务器、大型计算机、机架安装的服务器等)、服务器场、服务器集群或任何其它适当的布置和/或组合组成。服务器2712可以包括运行虚拟操作系统的一个或多个虚拟机，或涉及虚拟化的其它计算体系架构。一个或多个灵活的逻辑存储设备池可以被虚拟化，以维护用于服务器的虚拟存储设备。虚拟网络可以由服务器2712利用软件定义的联网来控制。在各种实施例中，服务器2712可以适于运行在前述公开内容中描述的一个或多个服务或软件应用。例如，服务器2712可以与根据本公开的实施例的用于如上所述执行处理的服务器对应。

[0255] 服务器2712可以运行包括以上讨论的任何操作系统的操作系统，以及任何商用的服务器操作系统。服务器2712还可以运行任何各种附加的服务器应用和/或中间层应用，包括HTTP(超文本传输协议) 服务器、FTP(文件传输协议)服务器、CGI(公共网关接口)服务器、**JAVA®**服务器、数据库服务器等。示例性数据库服务器包括但不限于可从Oracle、Microsoft、Sybase、IBM(国际商业机器)等商业获得的数据库服务器。

[0256] 在一些实现中，服务器2712可以包括一个或多个应用，以分析和整合从客户端计算设备2702、2704、2706和2708的用户接收到的数据馈送和/或事件更新。作为示例，数据馈送和/或事件更新可以包括但不限于从一个或多个第三方信息源和持续数据流接收到的**Twitter®**馈送、**Facebook®**更新或实时更新，其可以包括与传感器数据应用、金融报价机、网络性能测量工具(例如，网络监视和流量管理应用)、点击流分析工具、汽车流量监视等相关的实时事件。服务器2712还可以包括经由客户端计算设备2702、2704、2706和2708的一个或多个显示设备显示数据馈送和/或实时事件的一个或多个应用。

[0257] 分布式系统2700也可以包括一个或多个数据库2714和2716。这些数据库可以提供用于存储信息的机制，诸如用户交互信息、使用模式信息、适应规则信息以及由本公开的实施例使用的其它信息。数据库2714和2716可以驻留在各种位置中。作为示例，数据库2714和2716中的一个或多个可以驻留在服务器2712本地(和/或驻留在其中)的非瞬态存储介质上。可替代地，数据库2714和2716可以远离服务器2712，并且经由基于网络的或专用的连接与服务器2712通信。在一组实施例中，数据库2714和2716可以驻留在存储区域网络 (SAN)中。类似地，用于执行服务器2712所具有的功能的任何必要的文件可以适当地在服务器2712本地存储和/或远程存储。在一组实施例中，数据库2714和2716可以包括适于响应于SQL格式的命令存储、更新和检索数据的关系数据库，诸如由Oracle提供的数据库。

[0258] 在一些实施例中，云环境可以提供一个或多个服务。图28是根据本公开内容的实施例、其中服务可以被提供为云服务的系统环境 2800的一个或多个部件的简化框图。在图28所示的实施例中，系统环境2800包括可以被用户用来与提供云服务的云基础设施系统2802 交互的一个或多个客户端计算设备2804、2806和2808。云基础设施系统2802可以包括一个或多个计算机和/或服务器，其可以包括以上针对服务器2712所描述的那些。

[0259] 应当认识到的是，图28中所绘出的云基础设施系统2802可以具有除所绘出的那些之外的其它部件。另外，图28中所示的实施例仅仅是可以结合本公开的实施例的云基础设施系统的一个示例。在一些其它实施例中，云基础设施系统2802可以具有比图中所示出的更多或更少的部件、可以合并两个或更多个部件、或者可以具有不同的部件配置或布置。

[0260] 客户端计算设备2804、2806和2808可以是与以上针对客户端计算设备2702、2704、2706和2708描述的那些设备类似的设备。客户端计算设备2804、2806和2808可以被配置为操作客户端应用，诸如 web浏览器、专有客户端应用(例如，Oracle Forms)或可以被客户端计算设备的用户使用以与云基础设施系统2802交互来使用由云基础设施系统2802提供的服务的一些其它应用。虽然示例性系统环境 2800被示为具有三个客户端计算设备，但是可以支持任何数量的客户端计算设备。诸如具有传感器的设备等的其它设备可以与云基础设施系统2802交互。

[0261] (一个或多个)网络2810可以促进客户端计算设备2804、2806 和2808与云基础设施系统2802之间的通信和数据交换。每个网络可以是对本领域技术人员熟悉的可以利用任何各种商用的协议支持数据通信的任何类型的网络，其中协议包括以上针对(一个或多个)网络 2110所描述的协议。

[0262] 在某些实施例中，由云基础设施系统2802提供的服务可以包括按需对云基础设施系统的用户可用的服务的主机。还可以提供各种其它服务，包括但不限于在线数据存储和备份解决方案、基于Web的电子邮件服务、托管的办公套件和文档协作服务、数据库处理、受管理的技术支持服务等。由云基础设施系统提供的服务可以动态扩展，以满足其用户的需求。

[0263] 在某些实施例中，由云基础设施系统2802提供的服务的具体实例化在本文中可以被称为“服务实例”。一般而言，经由通信网络 (诸如互联网)从云服务提供者的系统使得对用户可用的任何服务被称为“云服务”。通常，在公共云环境中，构成云服务提供者的系统的服务器和系统与消费者自己的本地服务器和系统不同。例如，云服务提供者的系统可以托管应用，并且用户可以经由诸如互联网的通信网络按需订购和使用应用。

[0264] 在一些示例中，计算机网络云基础设施中的服务可以包括对存储装置、托管的数据库、托管的web服务器、软件应用或者由云供应商向用户提供的其它服务的受保护的计算机网络访问，或者如本领域中另外已知的。例如，服务可以包括通过互联网对云上的远程存储的受密码保护的访问。作为另一个示例，服务可以包括基于web服务的托管的关系数据库和脚本语言中间件引擎，用于由联网的开发人员私人使用。作为另一个示例，服务可以包括对在云供应商的网站上托管的电子邮件软件应用的访问。

[0265] 在某些实施例中，云基础设施系统2802可以包括以自助服务、基于订阅、弹性可扩展、可靠、高度可用和安全的方式交付给消费者的应用套件、中间件和数据库服务产品。这种云基础设施系统的示例是由本受让人提供的Oracle Public Cloud(Oracle公共云)。

[0266] 云基础设施系统2802还可以提供与“大数据”相关的计算和分析服务。术语“大数据”一般用来指可由分析员和研究者存储和操纵以可视化大量数据、检测趋势和/或以其它方式与数据交互的极大数据集。这种大数据和相关应用可以在许多级别和不同规模上由基础设施系统托管和/或操纵。并行链接的数十个、数百个或数千个处理器可以作用于这种数据，以便呈现其或者模拟对数据或其所表示的内容的外力。这些数据集可以涉及结构化数

据，诸如在数据库中组织或以其它方式根据结构化模型组织的数据，和/或者非结构化数据(例如，电子邮件、图像、数据blob(二进制大对象)、网页、复杂事件处理)。通过利用实施例相对快速地将更多(或更少)的计算资源聚焦在目标上的能力，云基础设施系统可以更好地用于基于来自企业、政府机构、研究组织、私人个人、一群志同道合的个人或组织或其它实体的需求在大数据集上执行任务。

[0267] 在各种实施例中，云基础设施系统2802可以适于自动地供应、管理和跟踪消费者对由云基础设施系统2802提供的服务的订阅。云基础设施系统2802可以经由不同的部署模型提供云服务。例如，服务可以在公共云模型下提供，其中云基础设施系统2802由销售云服务的组织拥有(例如，由Oracle公司拥有)并且使服务对一般公众或不同的工业企业可用。作为另一个示例，服务可以在私有云模型下提供，其中云基础设施系统2802仅针对单个组织操作，并且可以为组织内的一个或多个实体提供服务。云服务还可以在社区云模型下提供，其中云基础设施系统2802和由云基础设施系统2802提供的服务由相关社区中的若干个组织共享。云服务还可以在混合云模型下提供，混合云模型是两个或更多个不同模型的组合。

[0268] 在一些实施例中，由云基础设施系统2802提供的服务可以包括在软件即服务(SaaS)类别、平台即服务(PaaS)类别、基础设施即服务(IaaS)类别、或包括混合服务的服务的其它类别下提供的一个或多个服务。消费者经由订阅订单可以订购由云基础设施系统2802提供的一个或多个服务。云基础设施系统2802然后执行处理，以提供消费者的订阅订单中的服务。

[0269] 在一些实施例中，由云基础设施系统2802提供的服务可以包括但不限于应用服务、平台服务和基础设施服务。在一些示例中，应用服务可以由云基础设施系统经由SaaS平台提供。SaaS平台可以被配置为提供属于SaaS类别的云服务。例如，SaaS平台可以提供在集成的开发和部署平台上构建和交付点播应用套件的能力。SaaS平台可以管理和控制用于提供SaaS服务的底层软件和基础设施。通过利用由SaaS平台提供的服务，消费者可以利用在云基础设施系统上执行的应用。消费者可以获取应用服务，而无需消费者单独购买许可证和支持。可以提供各种不同的SaaS服务。示例包括但不限于为大型组织提供用于销售绩效管理、企业集成和业务灵活性的解决方案的服务。

[0270] 在一些实施例中，平台服务可以由云基础设施系统2802经由 PaaS平台提供。PaaS平台可以被配置为提供属于PaaS类别的云服务。平台服务的示例可以包括但不限于使组织(诸如Oracle)能够在共享的共同体系架构上整合现有应用的服务，以及利用由平台提供的共享服务构建新应用的能力。PaaS平台可以管理和控制用于提供 PaaS服务的底层软件和基础设施。消费者可以获取由云基础设施系统2802提供的PaaS服务，而无需消费者购买单独的许可证和支持。平台服务的示例包括但不限于Oracle Java云服务(JCS)、Oracle 数据库云服务(DBCS)以及其它。

[0271] 通过利用由PaaS平台提供的服务，消费者可以采用由云基础设施系统支持的编程语言和工具，并且还控制所部署的服务。在一些实施例中，由云基础设施系统提供的平台服务可以包括数据库云服务、中间件云服务(例如，Oracle Fusion Middleware服务)和Java云服务。在一个实施例中，数据库云服务可以支持共享服务部署模型，其使得组织能够汇集数据库资源并且以数据库云的形式向消费者提供数据库即服务。中间件云服务可以为消费

者提供开发和部署各种业务应用的平台，以及Java云服务可以在云基础设施系统中为消费者提供部署Java应用的平台。

[0272] 可以由云基础设施系统中的IaaS平台提供各种不同的基础设施服务。基础设施服务促进底层计算资源(诸如存储装置、网络和其它基本计算资源)的管理和控制，以便消费者利用由SaaS平台和PaaS 平台提供的服务。

[0273] 在某些实施例中，云基础设施系统2802还可以包括基础设施资源2830，用于提供用来向云基础设施系统的消费者提供各种服务的资源。在一个实施例中，基础设施资源2830可以包括执行由PaaS 平台和SaaS平台提供的服务的硬件(诸如服务器、存储装置和联网资源)的预先集成和优化的组合，以及其它资源。

[0274] 在一些实施例中，云基础设施系统2802中的资源可以由多个用户共享并且按需动态地重新分配。此外，资源可以分配给在不同时区中的用户。例如，云基础设施系统2802可以使第一时区内的第一用户集合能够利用云基础设施系统的资源指定的小时数，然后使得能够将相同资源重新分配给位于不同时区中的另一用户集合，从而最大化资源的利用率。

[0275] 在某些实施例中，可以提供由云基础设施系统2802的不同部件或模块共享，以使得能够由云基础设施系统2802供应服务的多个内部共享服务2832。这些内部共享服务可以包括，但不限于，安全和身份服务、集成服务、企业储存库服务、企业管理器服务、病毒扫描和白名单服务、高可用性、备份和恢复服务、用于启用云支持的服务、电子邮件服务、通知服务、文件传输服务等。

[0276] 在某些实施例中，云基础设施系统2802可以在云基础设施系统中提供云服务(例如，SaaS、PaaS和IaaS服务)的综合管理。在一个实施例中，云管理功能可以包括用于供应、管理和跟踪由云基础设施系统2802等接收到的消费者的订阅的能力。

[0277] 在一个实施例中，如图28中所绘出的，云管理功能可以由诸如订单管理模块2820、订单编排模块2828、订单供应模块2824、订单管理和监视模块2826以及身份管理模块2828的一个或多个模块提供。这些模块可以包括或可以利用一个或多个计算机和/或服务器提供，该一个或多个计算机和/或服务器可以是通用计算机、专用服务器计算机、服务器场，服务器集群或任何其它适当的布置和/或组合。

[0278] 在示例性操作中，在2834，使用客户端设备(诸如客户端计算设备2804、2806或2808)的消费者可以通过请求由云基础设施系统 2802提供的一个或多个服务并且对由云基础设施系统2802提供的一个或多个服务的订阅下订单来与云基础设施系统2802交互。在某些实施例中，消费者可以访问诸如云UI 2812、云UI 2814和/或云UI 2822的云用户界面(UI)并经由这些UI下订阅订单。响应于消费者下订单而由云基础设施系统2802接收到的订单信息可以包括识别消费者和消费者打算订阅的由云基础设施系统2802提供的一个或多个服务的信息。

[0279] 在步骤2836处，从消费者接收到的订单信息可以存储在订单数据库2818中。如果这是新的订单，则可以为该订单创建新的记录。在一个实施例中，订单数据库2818可以是由云基础设施系统2818操作以及与其它系统元素结合操作的若干数据库当中的一个。

[0280] 在步骤2838处，订单信息可以被转发到订单管理模块2820，订单管理模块2820可以被配置为执行与订单相关的计费和记帐功能，诸如验证订单，并且在通过验证时，预订订单。

[0281] 在步骤2840处，关于订单的信息可以被传送到订单编排模块 2822，订单编排模块2822被配置为编排用于由消费者下的订单的服务和资源的供应。在一些情况下，订单编排模块2822可以使用订单供应模块2824的服务用于供应。在某些实施例中，订单编排模块2822使得能够管理与每个订单相关联的业务过程，并且应用业务逻辑来确定订单是否应当继续供应。

[0282] 如图28中绘出的实施例所示，在2842处，在接收到新订阅的订单时，订单编排模块2822向订单供应模块2824发送分配资源和配置履行订购订单所需的资源的请求。订单供应模块2824使得能够为由消费者订购的服务分配资源。订单供应模块2824提供由云基础设施系统2800提供的云服务和用来供应用于提供所请求的服务的资源的物理实现层之间的抽象级别。这使得订单编排模块2822能够与实现细节隔离，诸如服务和资源是否实际上实时供应，或者预先供应并且仅在请求时才进行分配/指定。

[0283] 在步骤2844处，一旦供应了服务和资源，就可以向订阅的消费者发送指示所请求的服务现在已准备好用于使用的通知。在一些情况下，可以向消费者发送使得消费者能够开始使用所请求的服务的信息 (例如，链接)。

[0284] 在步骤2846处，可以由订单管理和监视模块2826来管理和跟踪消费者的订阅订单。在一些情况下，订单管理和监视模块2826可以被配置为收集关于消费者使用所订阅的服务的使用统计。例如，可以针对所使用的存储量、所传送的数据量、用户的数量以及系统启动时间和系统停机时间的量等来收集统计数据。

[0285] 在某些实施例中，云基础设施系统2800可以包括身份管理模块 2828，其被配置为提供身份服务，诸如云基础设施系统2800中的访问管理和授权服务。在一些实施例中，身份管理模块2828可以控制关于希望利用由云基础设施系统2802提供的服务的消费者的信息。这种信息可以包括认证这些消费者的身份的信息和描述那些消费者被授权相对于各种系统资源(例如，文件、目录、应用、通信端口、存储器段等)执行的动作的信息。身份管理模块2828还可以包括关于每个消费者的描述性信息以及关于如何和由谁来访问和修改描述性信息的管理。

[0286] 图29图示了可以被用来实现本公开的实施例的示例性计算机系统2900。在一些实施例中，计算机系统2900可以被用来实现上述任何各种服务器和计算机系统。如图29所示，计算机系统2900包括各种子系统，包括经由总线子系统2902与多个外围子系统通信的处理单元2904。这些外围子系统可以包括处理加速单元2906、I/O子系统2908、存储子系统2918和通信子系统2924。存储子系统2918可以包括有形的计算机可读存储介质2922和系统存储器2910。

[0287] 总线子系统2902提供用于使计算机系统2900的各种部件和子系统按照期望彼此通信的机制。虽然总线子系统2902被示意性地示为单条总线，但是总线子系统的可替代实施例可以利用多条总线。总线子系统2902可以是若干种类型的总线结构中的任何一种，包括存储器总线或存储器控制器、外围总线和利用任何各种总线体系架构的局部总线。例如，此类体系架构可以包括工业标准体系架构(ISA)总线、微通道体系架构(MCA)总线、增强型ISA(EISA)总线、视频电子标准协会(VESA)局部总线和外围部件互连(PCI)总线，其可以实现为根据IEEE P1386.1标准制造的夹层(Mezzanine)总线，等等。

[0288] 处理子系统2904控制计算机系统2900的操作并且可以包括一个或多个处理单元

2932、2934等。处理单元可以包括一个或多个处理器，其中包括单核或多核处理器、处理器的一个或多个核、或其组合。在一些实施例中，处理子系统2904可以包括一个或多个专用协处理器，诸如图形处理器、数字信号处理器(DSP)等。在一些实施例中，处理子系统2904的处理单元中的一些或全部可以利用定制电路来实现，诸如专用集成电路(ASIC)或现场可编程门阵列(FPGA)。

[0289] 在一些实施例中，处理子系统2904中的处理单元可以执行存储在系统存储器2910中或计算机可读存储介质2922上的指令。在各种实施例中，处理单元可以执行各种程序或代码指令，并且可以维护多个并发执行的程序或进程。在任何给定的时间，要执行的程序代码中的一些或全部可以驻留在系统存储器2910中和/或计算机可读存储介质2922上，潜在地包括在一个或多个存储设备上。通过适当的编程，处理子系统2904可以提供各种功能。

[0290] 在某些实施例中，可以提供处理加速单元2906，用于执行定制的处理或用于卸载由处理子系统2904执行的一些处理，以便加速由计算机系统2900执行的整体处理。

[0291] I/O子系统2908可以包括用于向计算机系统2900输入信息和/或用于从或经由计算机系统2900输出信息的设备和机制。一般而言，术语“输入设备”的使用旨在包括用于向计算机系统2900输入信息的所有可能类型的设备和机制。用户接口输入设备可以包括，例如，键盘、诸如鼠标或轨迹球的指示设备、结合到显示器中的触摸板或触摸屏、滚轮、点拨轮、拨盘、按钮、开关、键板、具有语音命令识别系统的音频输入设备、麦克风以及其它类型的输入设备。用户接口输入设备也可以包括使用户能够控制输入设备并与其交互的诸如Microsoft **Kinect®**运动传感器的运动感测和/或姿势识别设备、Microsoft **Xbox®** 360游戏控制器、提供用于接收利用姿势和口语命令的输入的接口的设备。用户接口输入设备也可以包括眼睛姿势识别设备，诸如从用户检测眼睛活动(例如，当拍摄图片和/或进行菜单选择时的“眨眼”)并将眼睛姿势转换为到输入设备(例如，Google **Glass®**)中的输入的Google **Glass®**眨眼检测器。此外，用户接口输入设备可以包括使用户能够通过语音命令与语音识别系统(例如，**Siri®**导航器)交互的语音识别感测设备。

[0292] 用户接口输入设备的其它示例包括但不限于，三维(3D)鼠标、操纵杆或指示杆、游戏板和图形平板、以及音频/视频设备，诸如扬声器、数字相机、数字摄像机、便携式媒体播放器、网络摄像机、图像扫描仪、指纹扫描仪、条形码读取器3D扫描仪、3D打印机、激光测距仪、以及眼睛注视跟踪设备。此外，用户接口输入设备可以包括，例如，医疗成像输入设备，诸如计算机断层摄影、磁共振成像、位置发射断层摄影、医疗超声检查设备。用户接口输入设备也可以包括，例如，音频输入设备，诸如MIDI键盘、数字乐器等。

[0293] 用户接口输出设备可以包括显示子系统、指示器灯或诸如音频输出设备的非可视显示器等。显示子系统可以是阴极射线管(CRT)、诸如利用液晶显示器(LCD)或等离子体显示器的平板设备、投影设备、触摸屏等。一般而言，术语“输出设备”的使用旨在包括用于从计算机系统2900向用户或其它计算机输出信息的所有可能类型的设备和机制。例如，用户接口输出设备可以包括但不限于，可视地传达文本、图形和音频/视频信息的各种显示设备，诸如监视器、打印机、扬声器、耳机、汽车导航系统、绘图仪、语音输出设备和调制解调器。

[0294] 存储子系统2918提供用于存储由计算机系统2900使用的信息的储存库或数据存

储。存储子系统2918提供有形非瞬态计算机可读存储介质，用于存储提供一些实施例的功能的基本编程和数据结构。当由处理子系统2904执行时提供上述功能的软件(程序、代码模块、指令)可以存储在存储子系统2918中。软件可以由处理子系统2904 的一个或多个处理单元执行。存储子系统2918也可以提供用于存储根据本公开使用的数据的储存库。

[0295] 存储子系统2918可以包括一个或多个非瞬态存储器设备，包括易失性和非易失性存储器设备。如图29所示，存储子系统2918包括系统存储器2910和计算机可读存储介质2922。系统存储器2910可以包括多个存储器，包括用于在程序执行期间存储指令和数据的易失性主随机存取存储器(RAM)和其中存储固定指令的非易失性只读存储器(ROM)或闪存存储器。在一些实现中，包含帮助在诸如启动期间在计算机系统2900内的元件之间传送信息的基本例程的基本输入/输出系统(BIOS)通常可以存储在ROM中。RAM通常包含当前由处理子系统2904操作和执行的数据和/或程序模块。在一些实现中，系统存储器2910可以包括多个不同类型的存储器，诸如静态随机存取存储器(SRAM)或动态随机存取存储器(DRAM)。

[0296] 作为示例而非限制，如在图29中所绘出的，系统存储器2910可以存储应用程序2912，其可以包括客户端应用、Web浏览器、中间层应用、关系数据库管理系统(RDBMS)等、程序数据2914和操作系统2916。作为示例，操作系统2916可以包括各种版本的 Microsoft **Windows®**、Apple **Macintosh®**和/或Linux操作系统、各种商用**UNIX®**或类UNIX操作系统(包括但不限于各种GNU/Linux 操作系统、Google **Chrome®** OS等)和/或诸如iOS、**Windows®** Phone、**Android®** OS、**BlackBerry®** 8OS和**Palm®** OS操作系统的移动操作系统。

[0297] 计算机可读存储介质2922可以存储提供一些实施例的功能的编程和数据结构。当由处理子系统2904执行时使处理器提供上述功能的软件(程序、代码模块、指令)可以存储在存储子系统2918中。作为示例，计算机可读存储介质2922可以包括非易失性存储器，诸如硬盘驱动器、磁盘驱动器、诸如CD ROM、DVD、**Blu-Ray®** (蓝光)盘或其它光学介质的光盘驱动器。计算机可读存储介质2922可以包括但不限于，**Zip®**驱动器、闪存存储器卡、通用串行总线 (USB)闪存驱动器、安全数字(SD)卡、DVD盘、数字视频带等。计算机可读存储介质2922也可以包括基于非易失性存储器的固态驱动器(SSD)(诸如基于闪存存储器的SSD、企业闪存驱动器、固态 ROM等)、基于易失性存储器的SSD(诸如基于固态RAM、动态 RAM、静态RAM、DRAM的SSD、磁阻RAM(MRAM)SSD)，以及使用基于DRAM和基于闪存存储器的SSD的组合的混合SSD。计算机可读介质2922可以为计算机系统2900提供计算机可读指令、数据结构、程序模块和其它数据的存储。

[0298] 在某些实施例中，存储子系统2900也可以包括计算机可读存储介质读取器2920，其可以进一步连接到计算机可读存储介质2922。可选地，与系统存储器2910一起和组合，计算机可读存储介质2922 可以全面地表示远程、本地、固定和/或可移动存储设备加上用于存储计算机可读信息的存储介质。

[0299] 在某些实施例中，计算机系统2900可以提供对执行一个或多个虚拟机的支持。计算机系统2900可以执行诸如管理程序的程序，以便促进虚拟机的配置和管理。每个虚拟机可以被分配存储器、计算 (例如，处理器、内核)、I/O和联网资源。每个虚拟机通常运行其自己的操作系统，其可以与由计算机系统2900执行的其它虚拟机执行的操作系统相同或不

同。相应地，多个操作系统可以潜在地由计算机系统2900并发地运行。每个虚拟机一般独立于其它虚拟机运行。

[0300] 通信子系统2924提供到其它计算机系统和网络的接口。通信子系统2924用作用于从计算机系统2900的其它系统接收数据和向其发送数据的接口。例如，通信子系统2924可以使计算机系统2900能够经由互联网建立到一个或多个客户端计算设备的通信信道，用于从客户端计算设备接收信息和发送信息到客户端计算设备。

[0301] 通信子系统2924可以支持有线和/或无线通信协议两者。例如，在某些实施例中，通信子系统2924可以包括用于(例如，使用蜂窝电话技术、高级数据网络技术(诸如3G、4G或EDGE(全球演进的增强数据速率)、WiFi(IEEE 802.11族标准)、或其它移动通信技术、或其任意组合)接入无线语音和/或数据网络的射频(RF)收发器部件、全球定位系统(GPS)接收器部件和/或其它部件。在一些实施例中，作为无线接口的附加或替代，通信子系统2924可以提供有线网络连接(例如，以太网)。

[0302] 通信子系统2924可以以各种形式接收和发送数据。例如，在一些实施例中，通信子系统2924可以以结构化和/或非结构化的数据馈送2926、事件流2928、事件更新2930等形式接收输入通信。例如，通信子系统2924可以被配置为实时地从社交媒体网络的用户和/或诸如**Twitter®**馈送、**Facebook®**更新、诸如丰富站点摘要(RSS)馈送的web馈送的其它通信服务接收(或发送)数据馈送2926，和/或来自一个或多个第三方信息源的实时更新。

[0303] 在某些实施例中，通信子系统2924可以被配置为以连续数据流的形式接收本质上可能是连续的或无界的没有明确结束的数据，其中连续数据流可以包括实时事件的事件流2928和/或事件更新2930。生成连续数据的应用的示例可以包括例如传感器数据应用、金融报价机、网络性能测量工具(例如网络监视和流量管理应用)、点击流分析工具、汽车流量监视等。

[0304] 通信子系统2924也可以被配置为向一个或多个数据库输出结构化和/或非结构化的数据馈送2926、事件流2928、事件更新2930等，其中所述一个或多个数据库可以与耦合到计算机系统2900的一个或多个流数据源计算机通信。

[0305] 计算机系统2900可以是各种类型中的一种，包括手持便携式设备(例如，**iPhone®**蜂窝电话、**iPad®**计算平板、PDA)、可穿戴设备(例如，Google**Glass®**头戴式显示器)、个人计算机、工作站、大型机、信息站、服务器机架或任何其它数据处理系统。

[0306] 由于计算机和网络不断变化的性质，对图29中绘出的计算机系统2900的描述旨在仅仅作为具体示例。具有比图29中所绘出的系统更多或更少部件的许多其它配置是可能的。基于本文所提供的公开内容和教导，本领域普通技术人员将理解实现各种实施例的其它方式和 /或方法。

[0307] 虽然已经描述了本公开的具体实施例，但是各种修改、更改、替代构造和等效物也包含在本公开的范围之内。修改包括所公开的特征的任何相关组合。本公开的实施例不限于在某些特定数据处理环境内的操作，而是可以在多个数据处理环境内自由操作。此外，虽然已利用特定系列的事务和步骤描述了本公开的实施例，但是，对本领域技术人员应当显而易见，本公开的范围不限于所描述系列的事务和步骤。上述实施例的各种特征和方面可以被单独或结合使用。

[0308] 另外，虽然已经利用硬件和软件的特定组合描述了本公开的实施例，但是应当认

识到，硬件和软件的其它组合也在本公开的范围之内。本公开的实施例可以只用硬件、或只用软件、或利用其组合来实现。本文描述的各种过程可以在同一处理器或以任何组合的不同处理器上实现。相应地，在部件或模块被描述为被配置为执行某些操作的情况下，这种配置可以例如通过设计电子电路来执行操作、通过对可编程电子电路(诸如微处理器)进行编程来执行操作、或其任意组合来实现。进程可以利用各种技术来通信，包括但不限于用于进程间通信的常规技术，并且不同的进程对可以使用不同的技术，或者同一对进程可以在不同时间使用不同的技术。

[0309] 相应地，说明书和附图应当在说明性而不是限制性的意义上考虑。但是，将显而易见的是，在不背离权利要求中阐述的更广泛精神和范围的情况下，可以对其进行添加、减少、删除和其它修改和改变。因此，虽然已描述了具体的实施例，但是这些实施例不旨在进行限制。各种修改和等效物都在以下权利要求的范围之内。

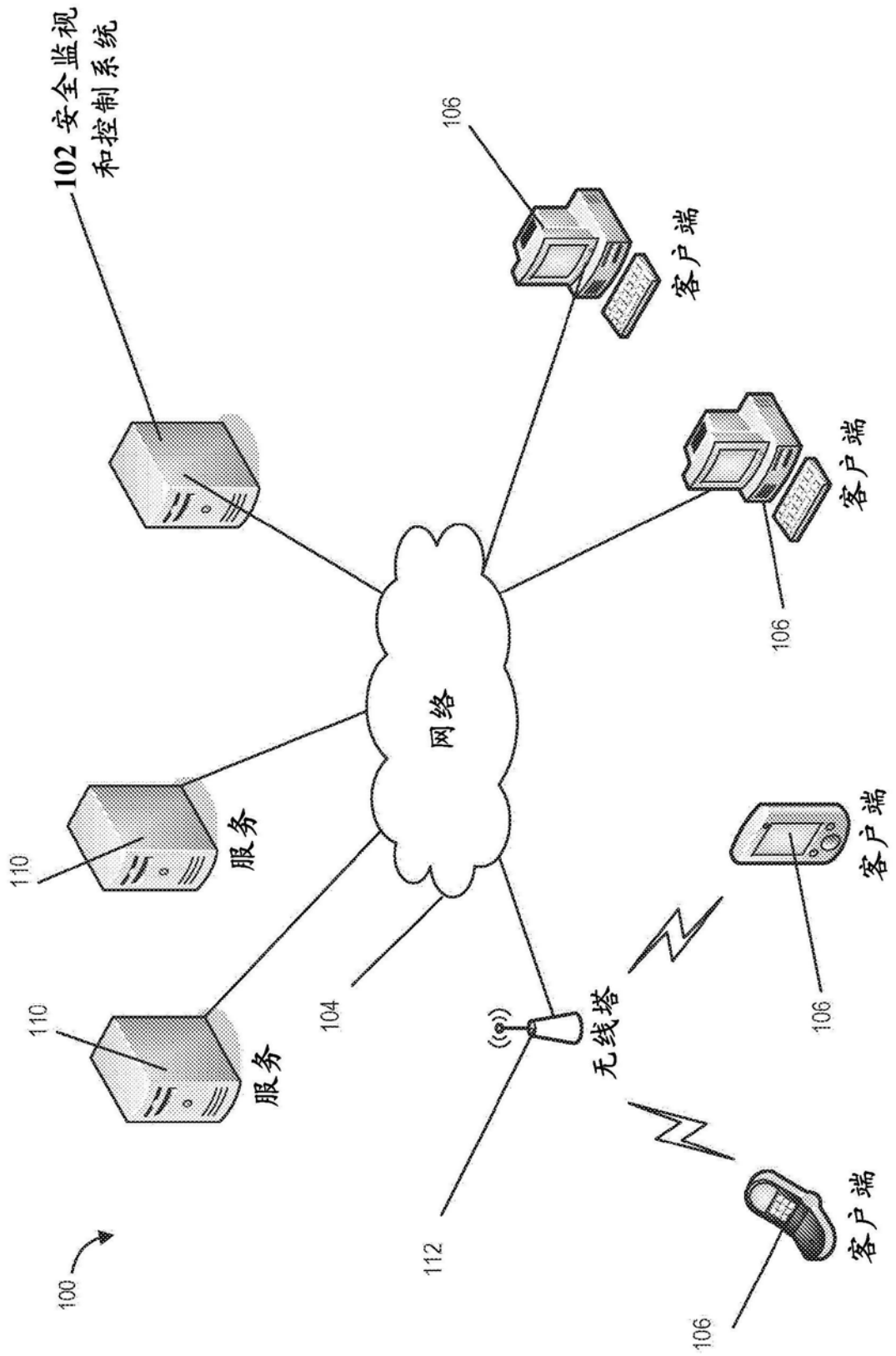
102 安全监视和控制系统
106
客户端
106
客户端
网络
110
服务
110
服务
104
106
客户端
无线塔
112
106
客户端
100

图1A

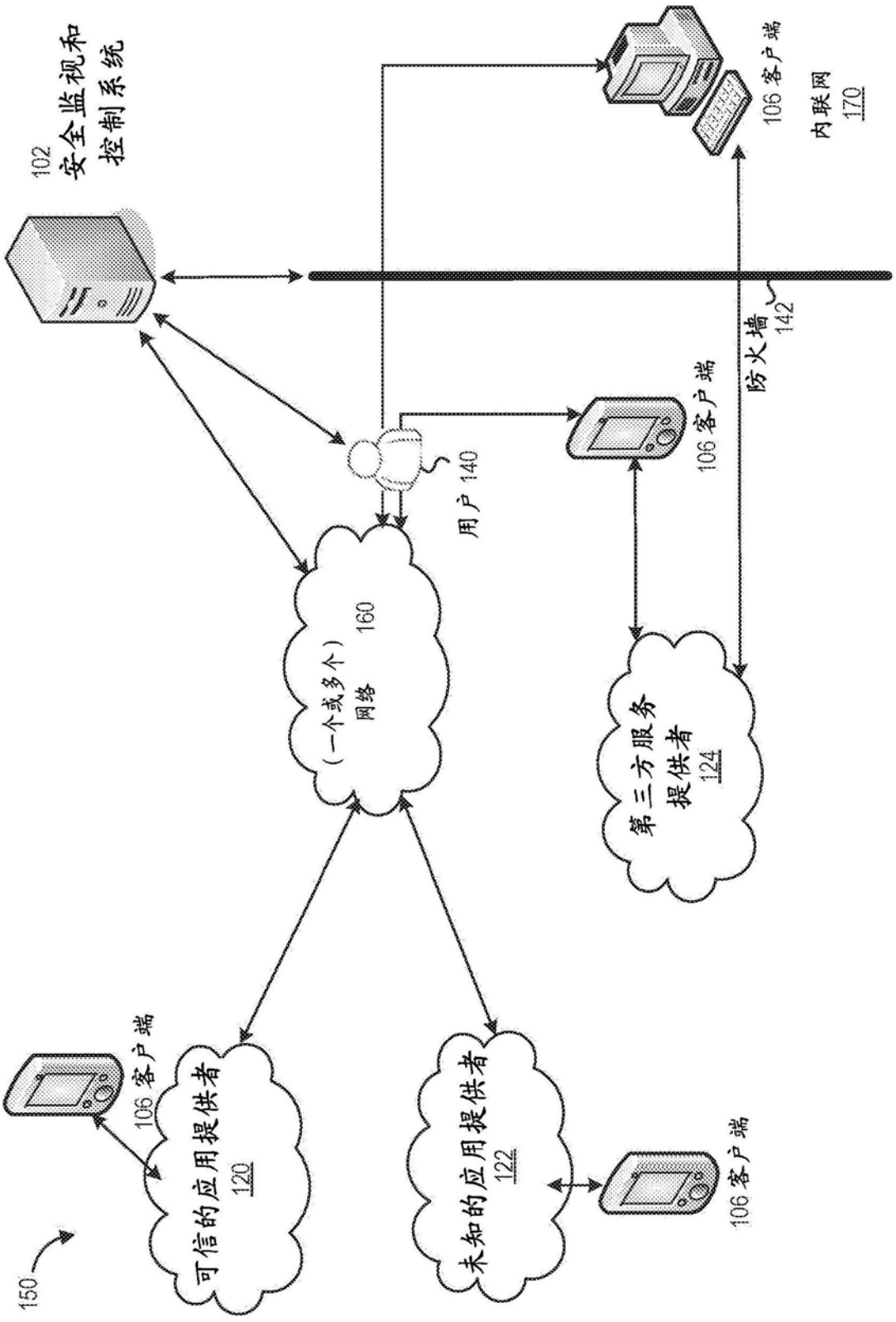
102
安全监视和
控制系统
106 客户端
内联网
170
防火墙
142
106 客户端
用户 140
(一个或多个)
网络
160
第三方服务
提供者
124
106 客户端
可信的应用提供者
120
未知的应用提供者
122
106 客户端
150

图1B

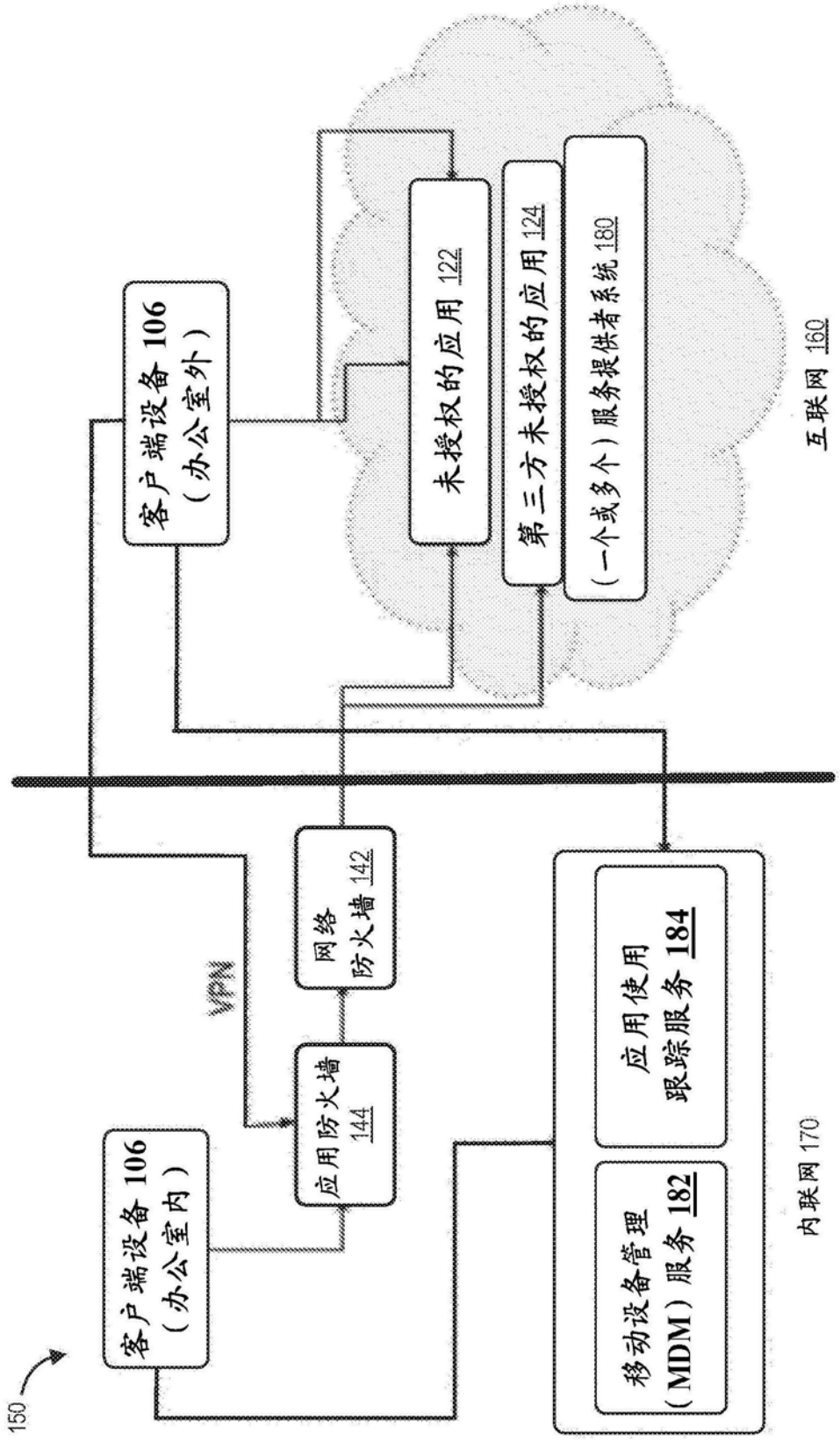
150
客户端设备 106
（办公室内）
客户端设备 106
（办公室外）
VPN
应用防火墙
144
网络
防火墙 142
未授权的应用 122
第三方未授权的应用 124
（一个或多个）服务提供者系统 180
互联网 160
移动设备管理
（MDM）服务 182
应用使用
跟踪服务 184
内联网 170

图1C

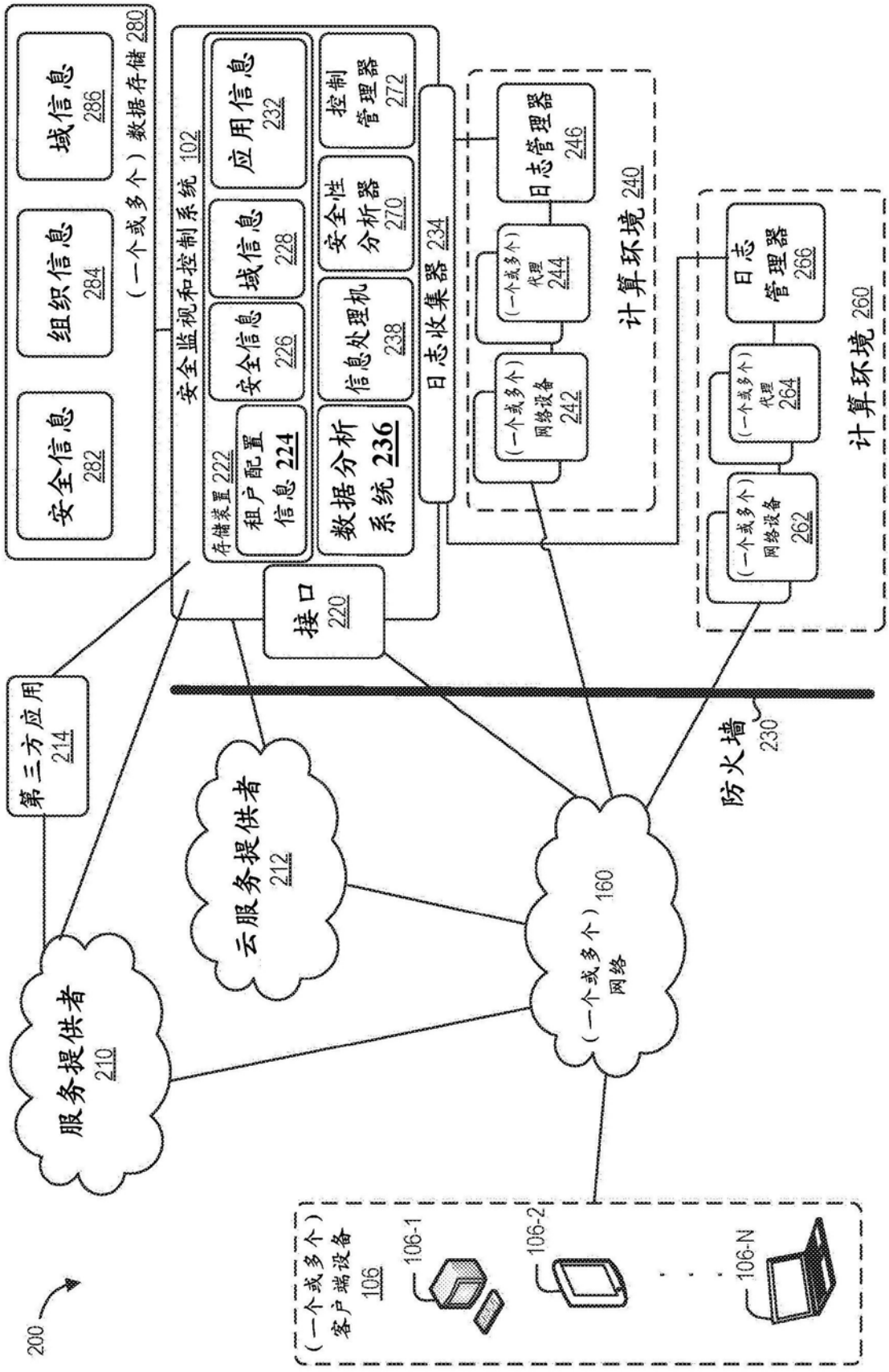
200
(一个或多个)客户端设备 106
106-1
106-2
106-N
服务提供者 210
第三方应用 214
云服务提供者 212
(一个或多个)网络 160
防火墙 230
计算环境 260
日志管理器 266
(一个或多个)代理 264
(一个或多个)网络设备 262
计算环境 240
日志管理器 246
(一个或多个)代理 244
(一个或多个)网络设备 242
日志收集器 234
安全监视和控制系统 102
存储装置 222
租户配置信息 224
安全信息 226
数据分析系统 236
信息处理机 238
域信息 228
应用信息 232
安全性分析器 270
控制管理器 272
接口 220
(一个或多个)数据存储 280
安全信息 282
组织信息 284
域信息 286

图2

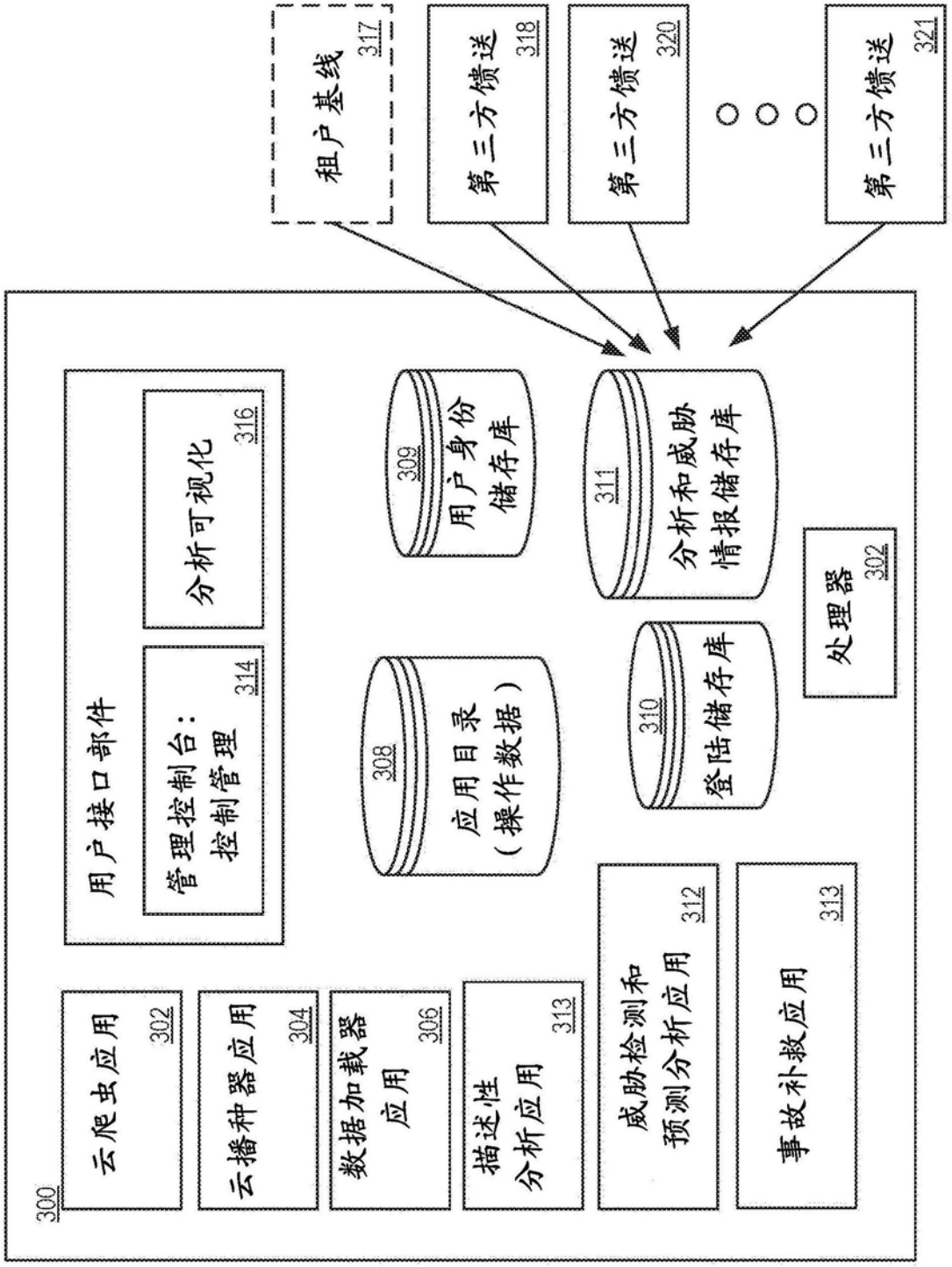
300
云爬虫应用 302
云播种器应用 304
数据加载器应用 306
描述性分析应用 313
威胁检测和预测分析应用 312
事故补救应用 313
用户接口部件
管理控制台：控制管理 314
分析可视化 316
应用目录（操作数据） 308
用户身份储存库 309
登陆储存库 310
分析和威胁情报储存库 311
处理器 302
租户基线 317
第三方馈送 318
第三方馈送 320
第三方馈送 321

图3

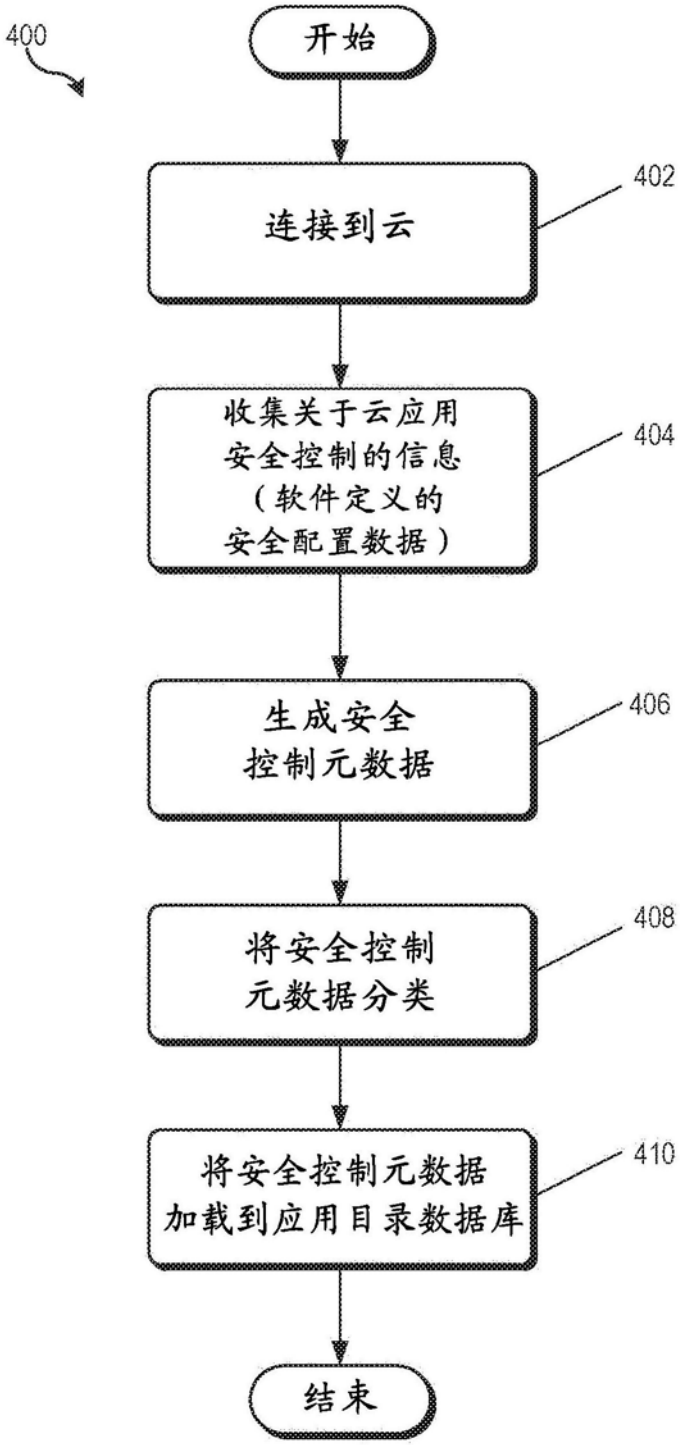
400
开始
连接到云
402
收集关于云应用
安全控制的信息
（软件定义的
安全配置数据）
404
生成安全
控制元数据
406
将安全控制
元数据分类
408
将安全控制元数据
加载到应用目录数据库
410
结束

图4

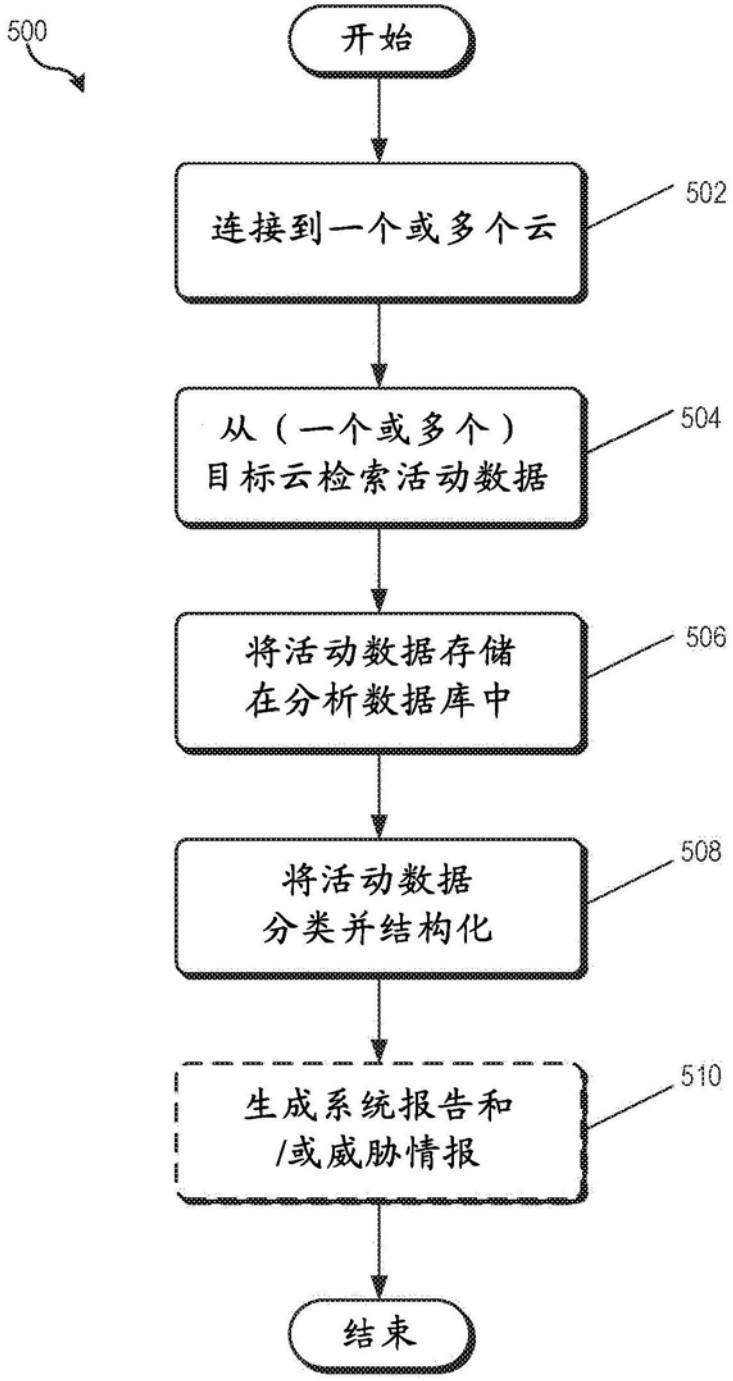
500
开始
连接到一个或多个云
502
从（一个或多个）
目标云检索活动数据
504
将活动数据存储
在分析数据库中
506
将活动数据
分类并结构化
508
生成系统报告和
/或威胁情报
510
结束

图5

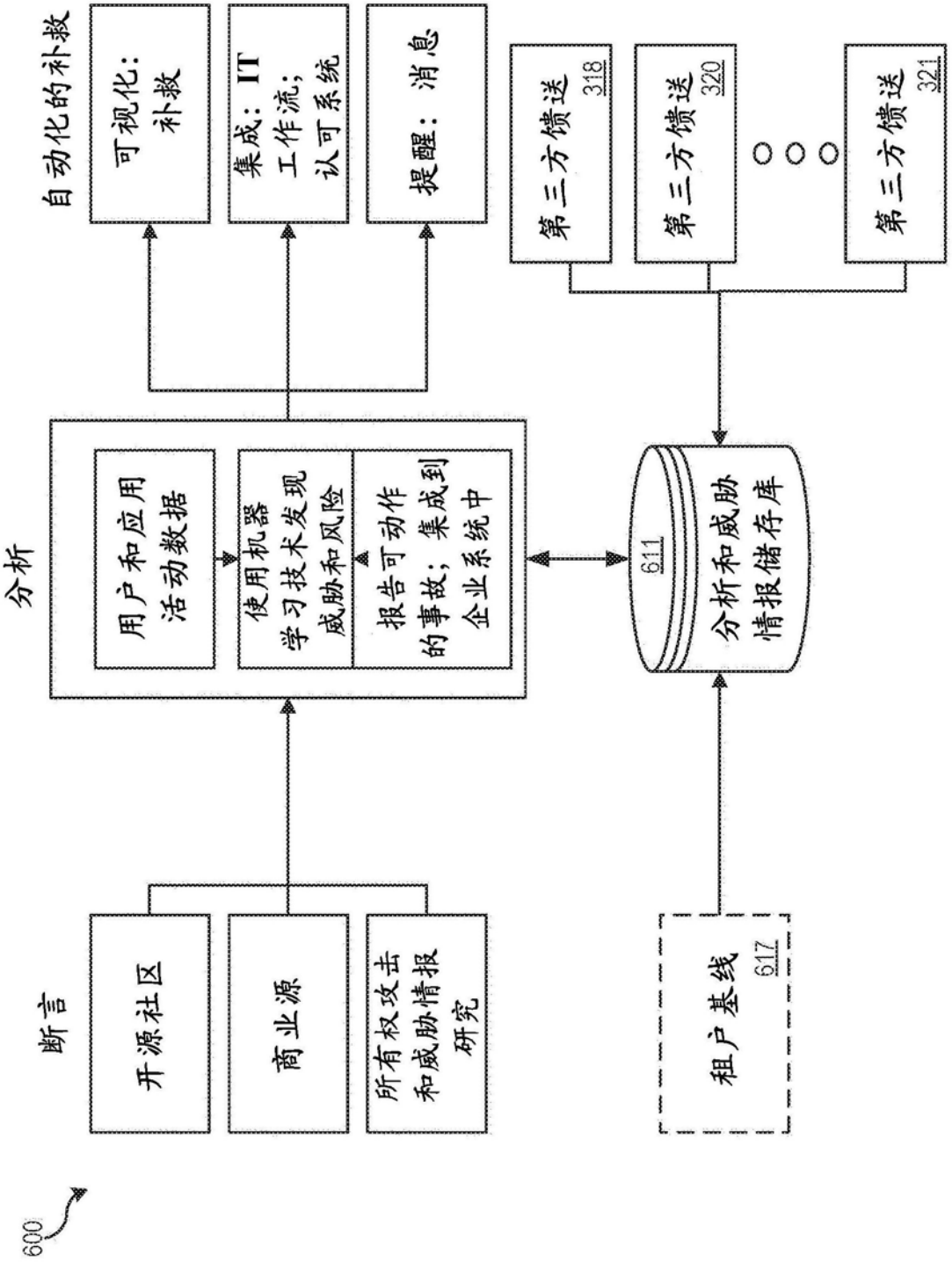
600
断言
开源社区
商业源
所有权攻击和威胁情报研究
分析
用户和应用活动数据
使用机器学习技术发现威胁和风险
报告可动作的事故；集成到企业系统中
611
分析和威胁情报储存库
租户基线
617
自动化的补救
可视化：补救
集成：IT工作流；认可系统
提醒：消息
第三方馈送
318
第三方馈送
320
第三方馈送
321

图6

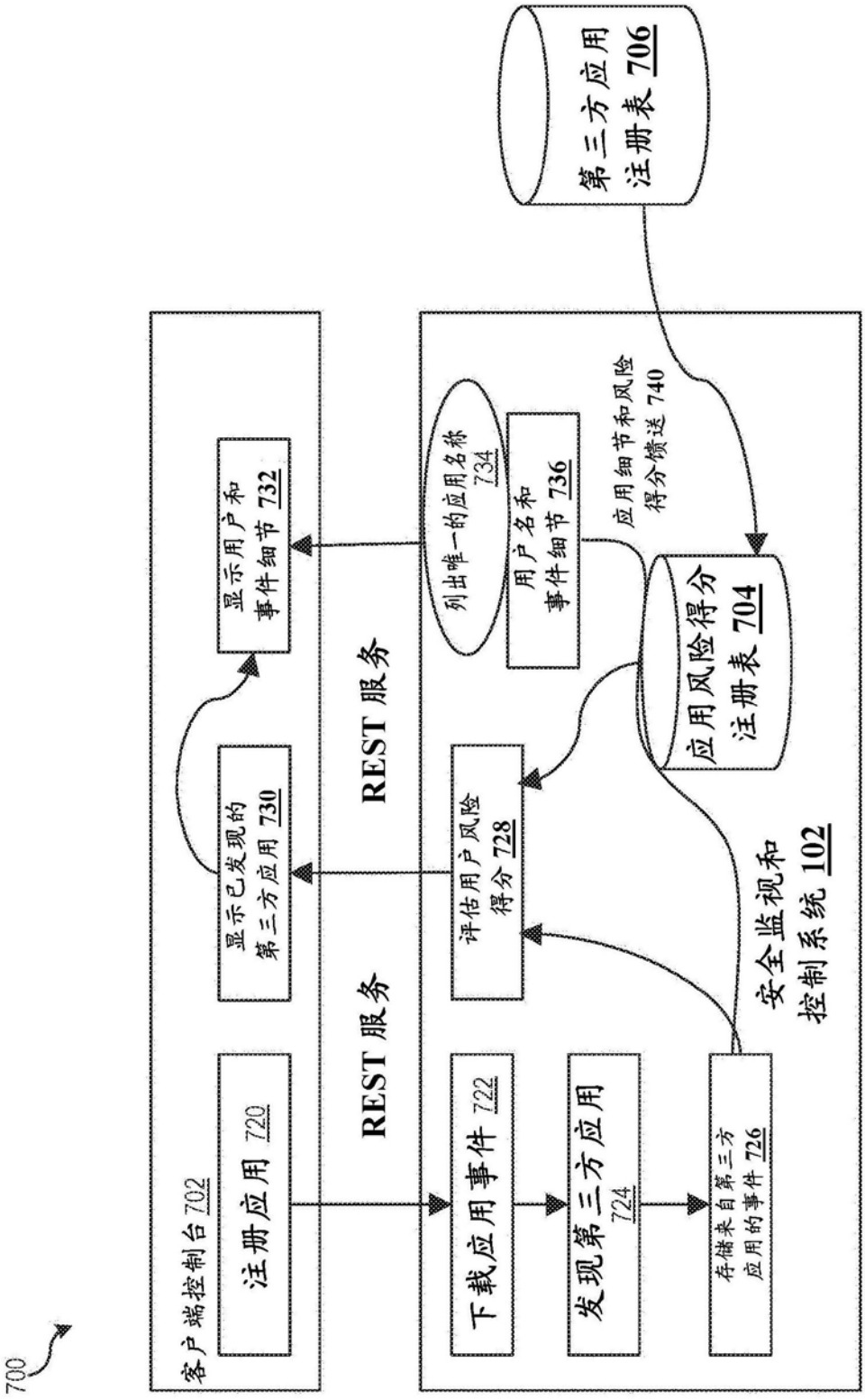
700
客户端控制台 702
注册应用 720
显示已发现的第三方应用 730
显示用户和事件细节 732
REST 服务
REST 服务
下载应用事件 722
发现第三方应用 724
存储来自第三方应用的事件 726
评估用户风险得分 728
列出唯一的应用名称 734
用户名和事件细节 736
应用细节和风险得分馈送 740
第三方应用注册表 706
应用风险得分注册表 704
安全监视和控制系统 102

图7

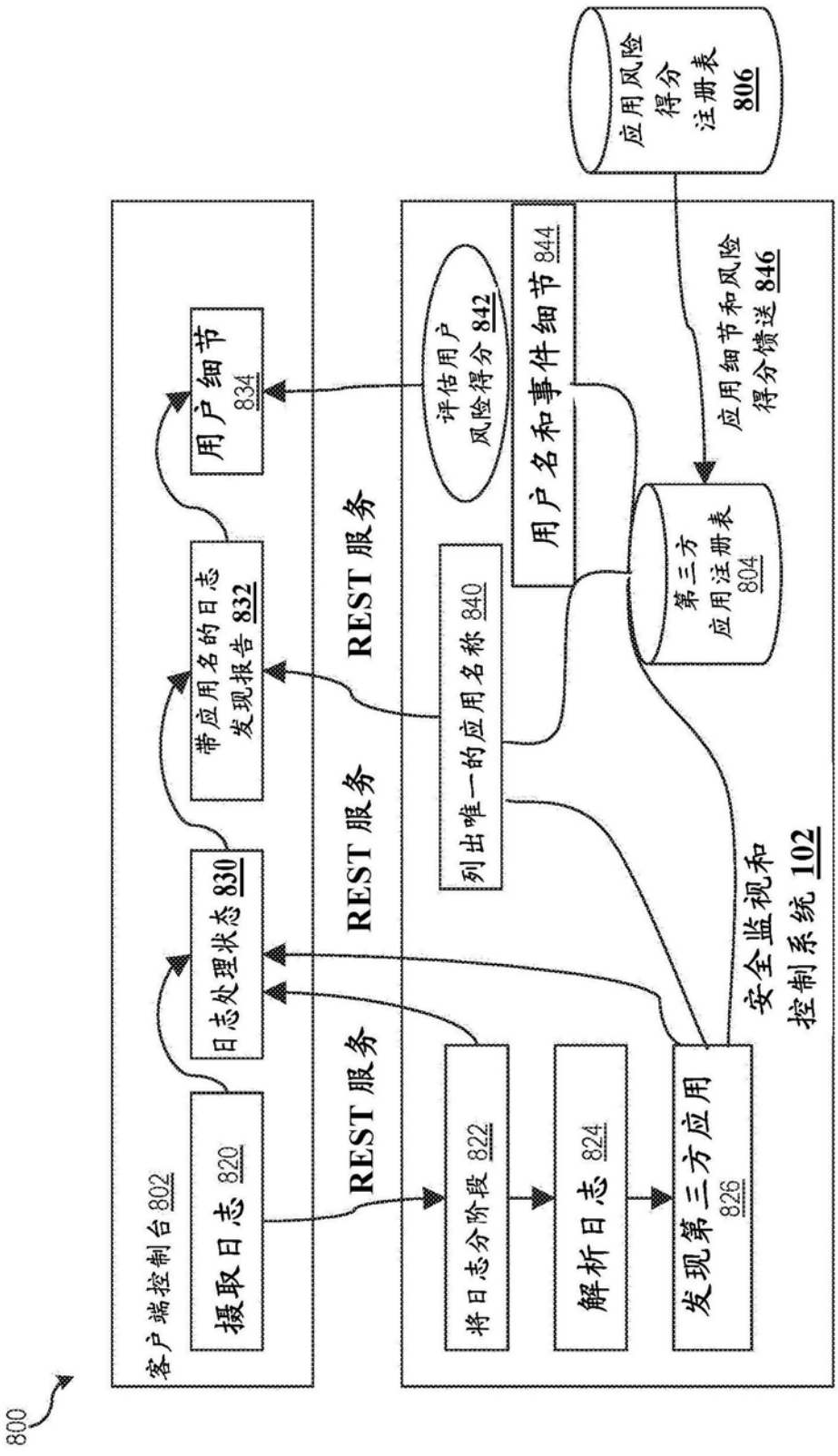
800
客户端控制台 802
摄取日志 820
日志处理状态 830
带应用名的日志发现报告 832
用户细节 834
REST 服务
REST 服务
REST 服务
将日志分阶段 822
解析日志 824
发现第三方应用 826
安全监视和控制系统 102
列出唯一的应用名称 840
评估用户风险得分 842
用户名和事件细节 844
应用细节和风险得分馈送 846
第三方应用注册表 804
应用风险得分注册表 806

图8

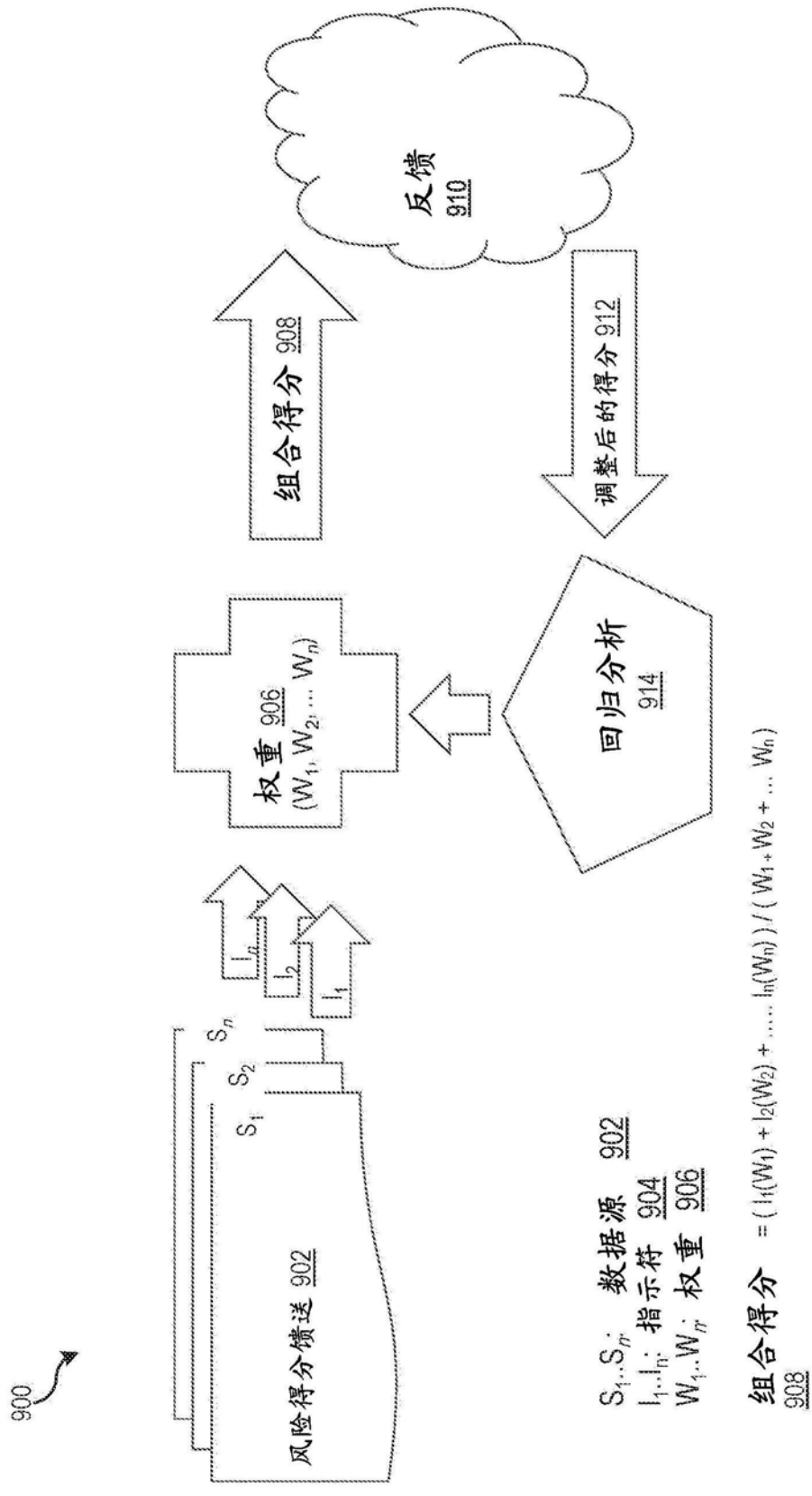
900
风险得分馈送 902
S_1
S_2
S_n
I_1
I_2
I_n
权重 906
$(W_1, W_2, \ldots W_n)$
组合得分 908
反馈
910
调整后的得分 912
回归分析
914
$S_1..S_n$: 数据源 902
$I_1..I_n$: 指示符 904
$W_1..W_n$: 权重 906
组合得分 908 $= (I_1(W_1) + I_2(W_2) + \ldots I_n(W_n)) / (W_1 + W_2 + \ldots W_n)$

图9

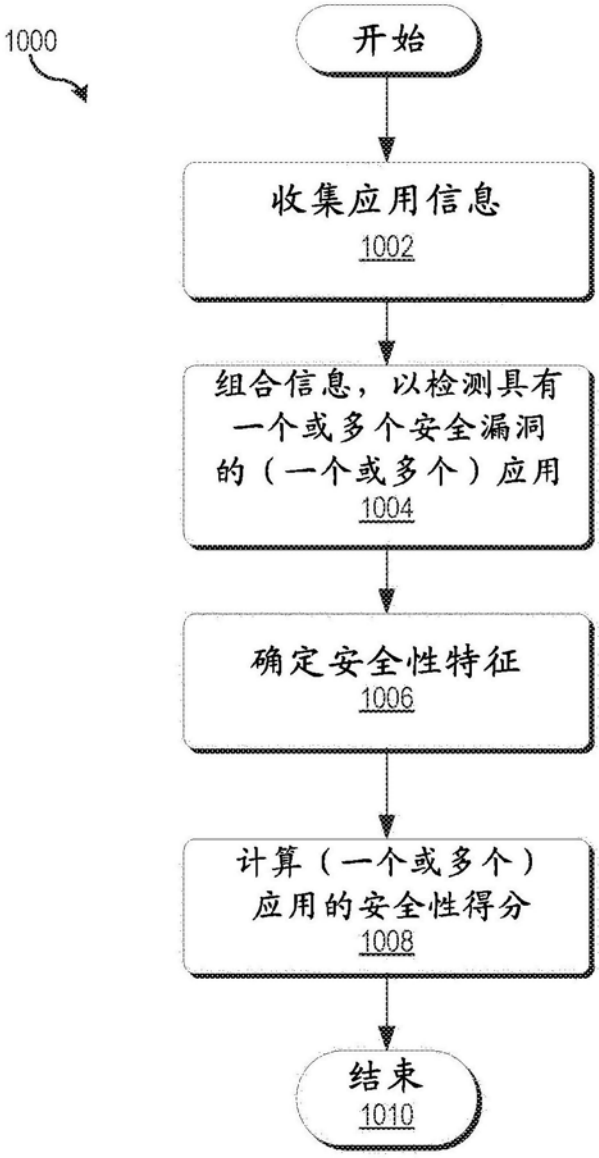
1000
开始
收集应用信息
1002
组合信息，以检测具有一个或多个安全漏洞的（一个或多个）应用
1004
确定安全性特征
1006
计算（一个或多个）应用的安全性得分
1008
结束
1010

图10

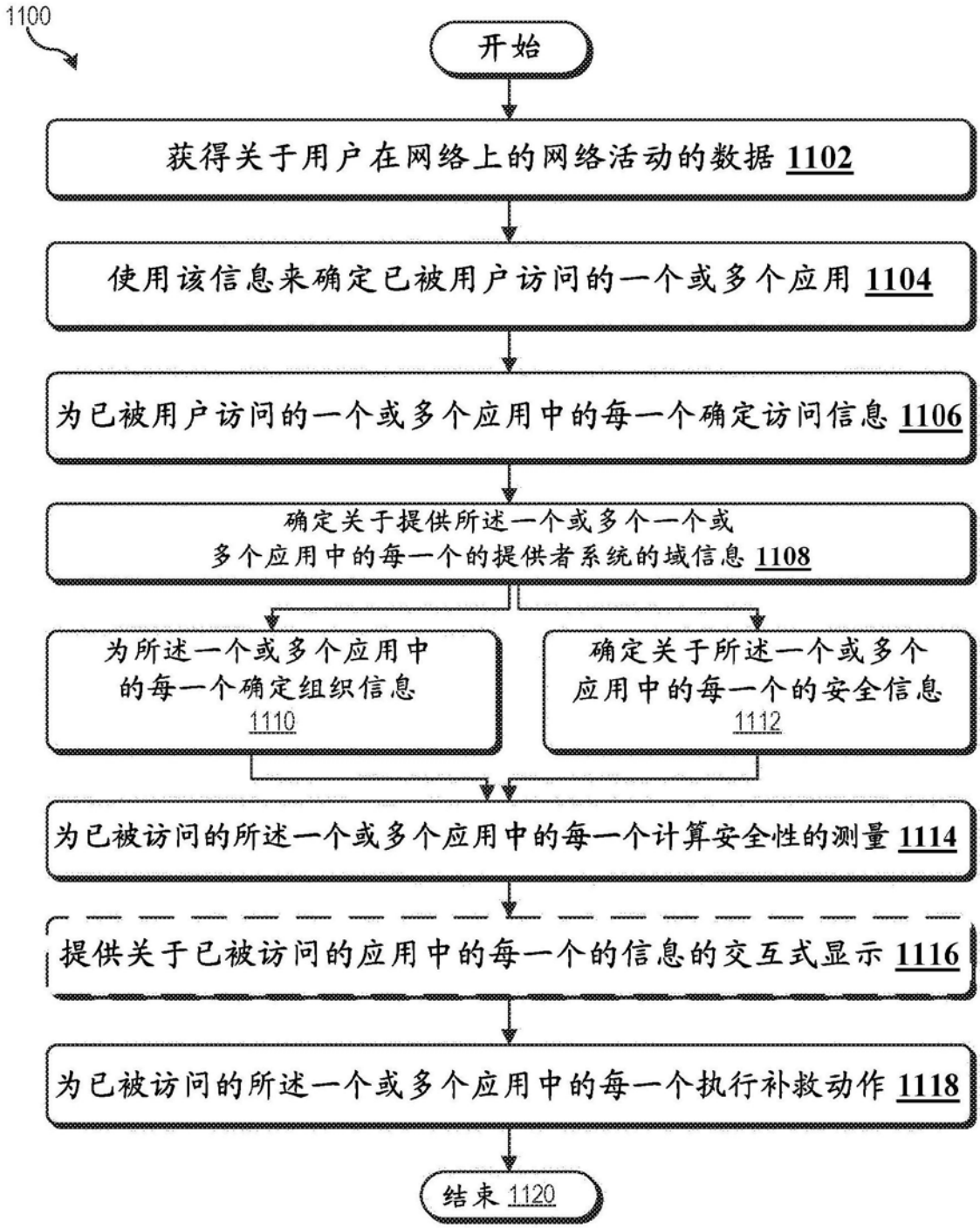
1100
开始
获得关于用户在网络上的网络活动的数据 1102
使用该信息来确定已被用户访问的一个或多个应用 1104
为已被用户访问的一个或多个应用中的每一个确定访问信息 1106
确定关于提供所述一个或多个一个或多个应用中的每一个的提供者系统的域信息 1108
为所述一个或多个应用中的每一个确定组织信息 1110
确定关于所述一个或多个应用中的每一个的安全信息 1112
为已被访问的所述一个或多个应用中的每一个计算安全性的测量 1114
提供关于已被访问的应用中的每一个的信息的交互式显示 1116
为已被访问的所述一个或多个应用中的每一个执行补救动作 1118
结束 1120

图11

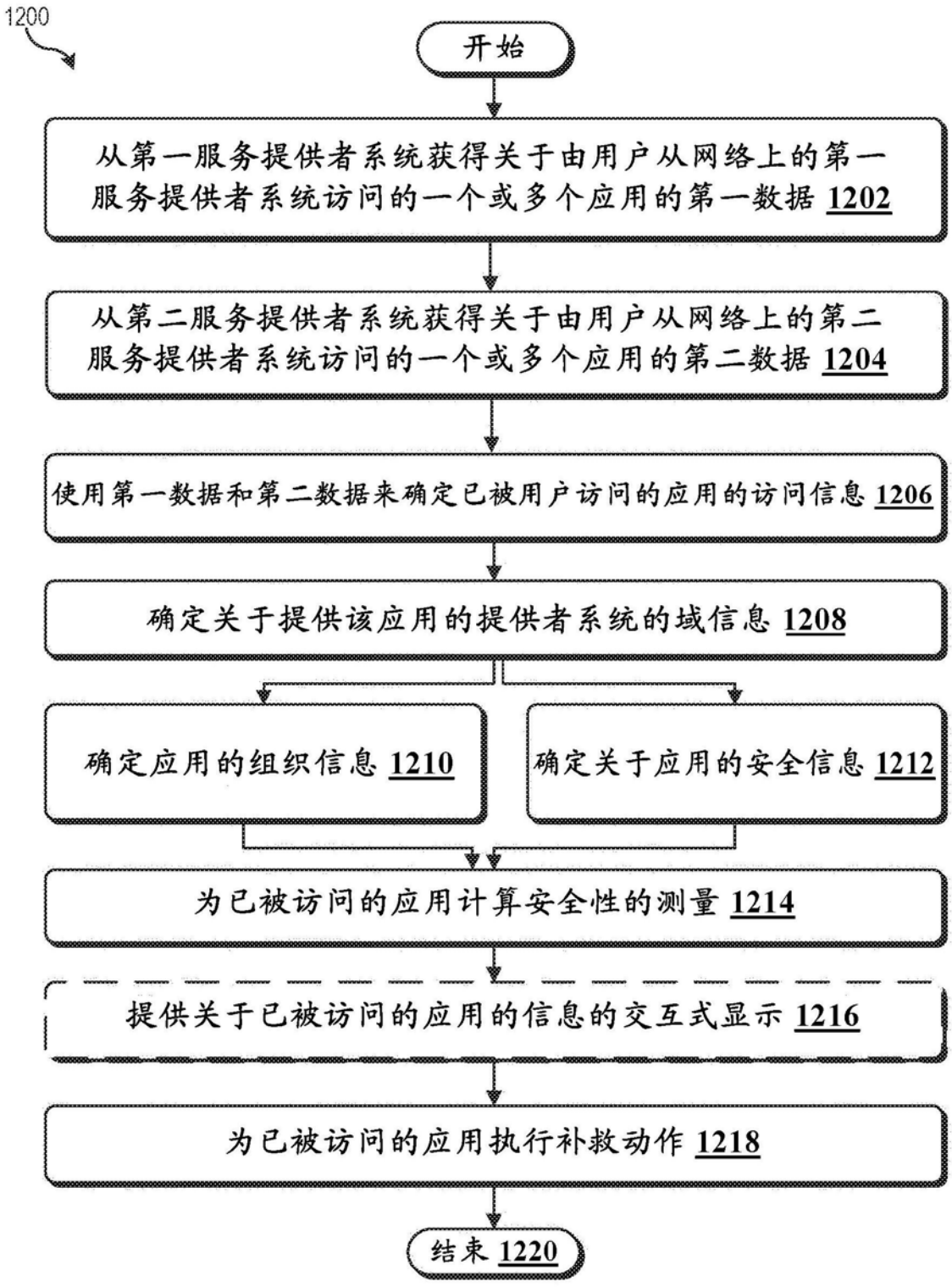
1200
开始
从第一服务提供者系统获得关于由用户从网络上的第一服务提供者系统访问的一个或多个应用的第一数据 1202
从第二服务提供者系统获得关于由用户从网络上的第二服务提供者系统访问的一个或多个应用的第二数据 1204
使用第一数据和第二数据来确定已被用户访问的应用的访问信息 1206
确定关于提供该应用的提供者系统的域信息 1208
确定应用的组织信息 1210
确定关于应用的安全信息 1212
为已被访问的应用计算安全性的测量 1214
提供关于已被访问的应用的信息的交互式显示 1216
为已被访问的应用执行补救动作 1218
结束 1220

图12

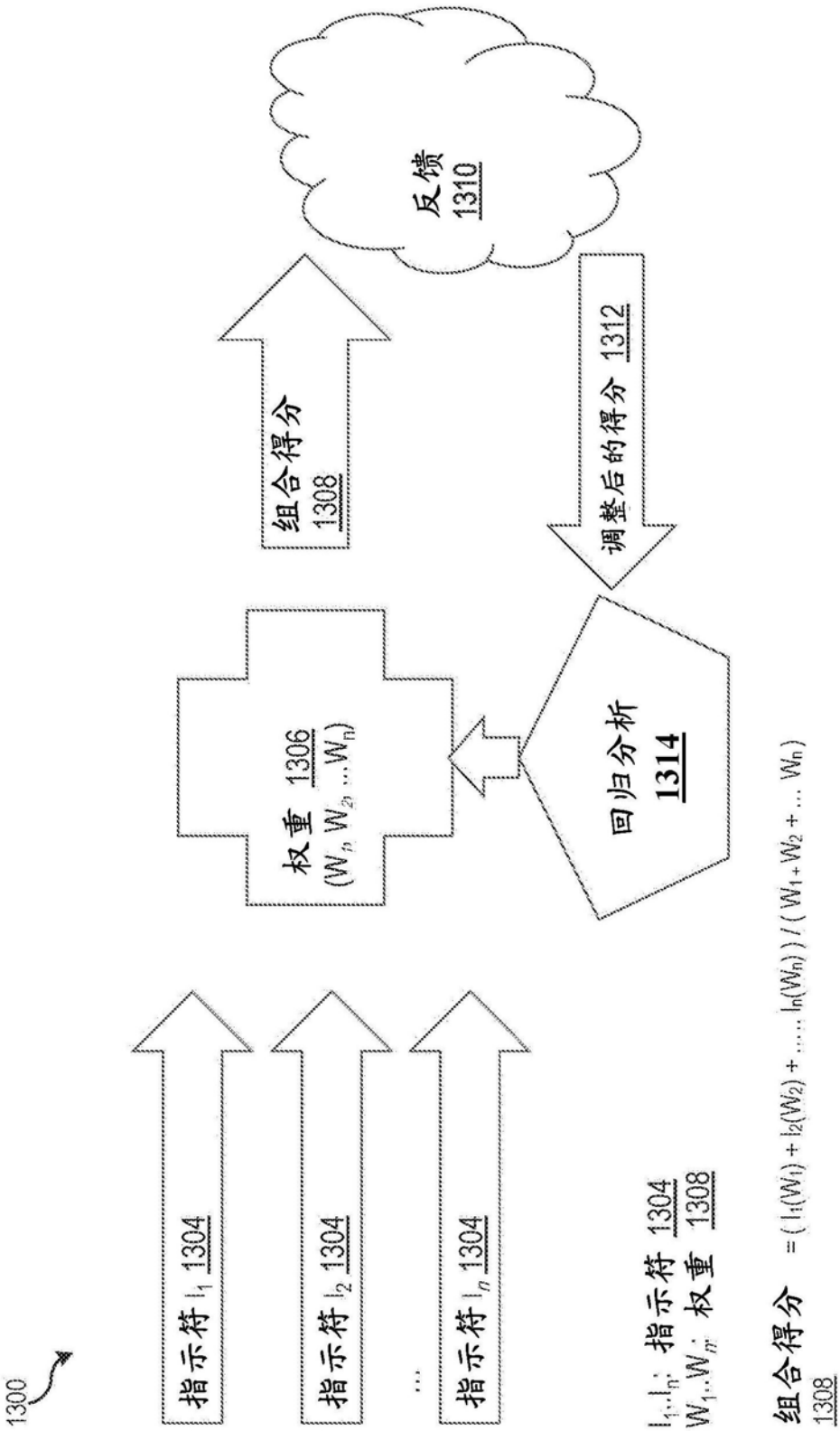
1300
指示符 I_1 1304
指示符 I_2 1304
...
指示符 I_n 1304
权重 1306
(W_1, W_2 ...W_n)
回归分析
1314
组合得分
1308
反馈
1310
调整后的得分 1312
I_1..I_n: 指示符 1304
W_1..W_n: 权重 1308
组合得分 1308
$= (I_1(W_1) + I_2(W_2) + \ldots + I_n(W_n)) / (W_1 + W_2 + \ldots W_n)$

图13

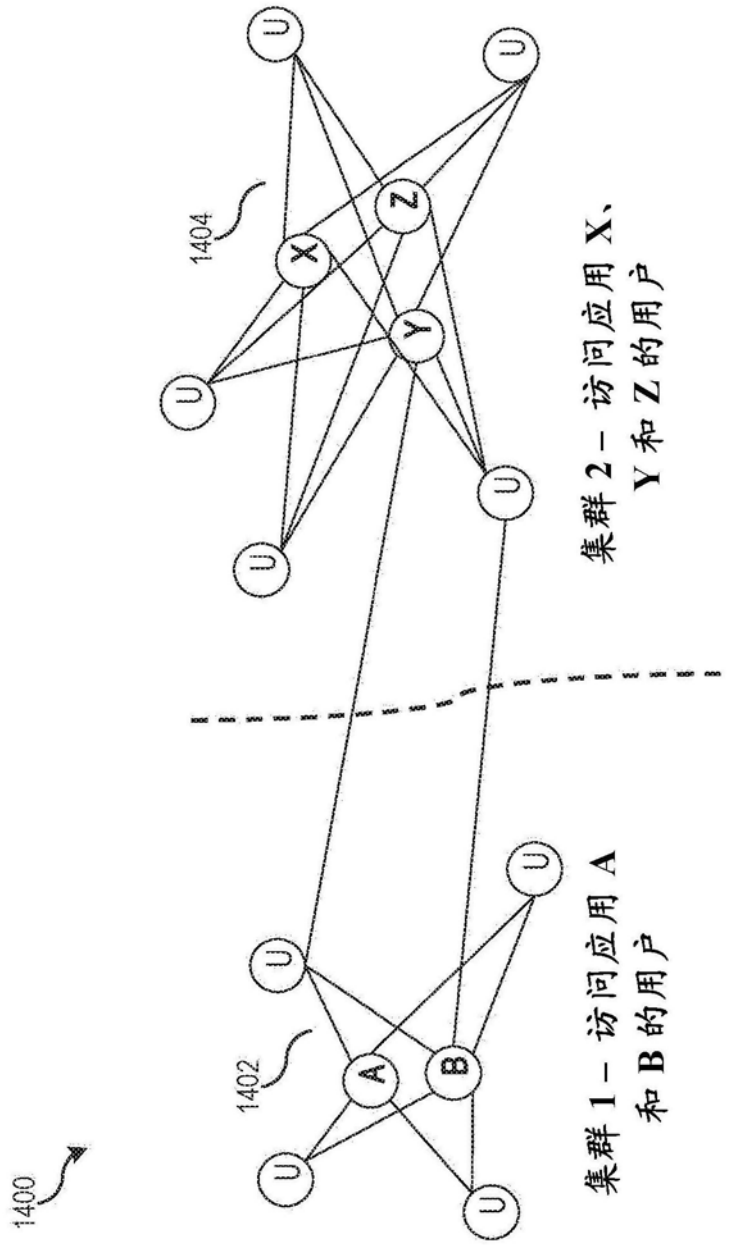

图14

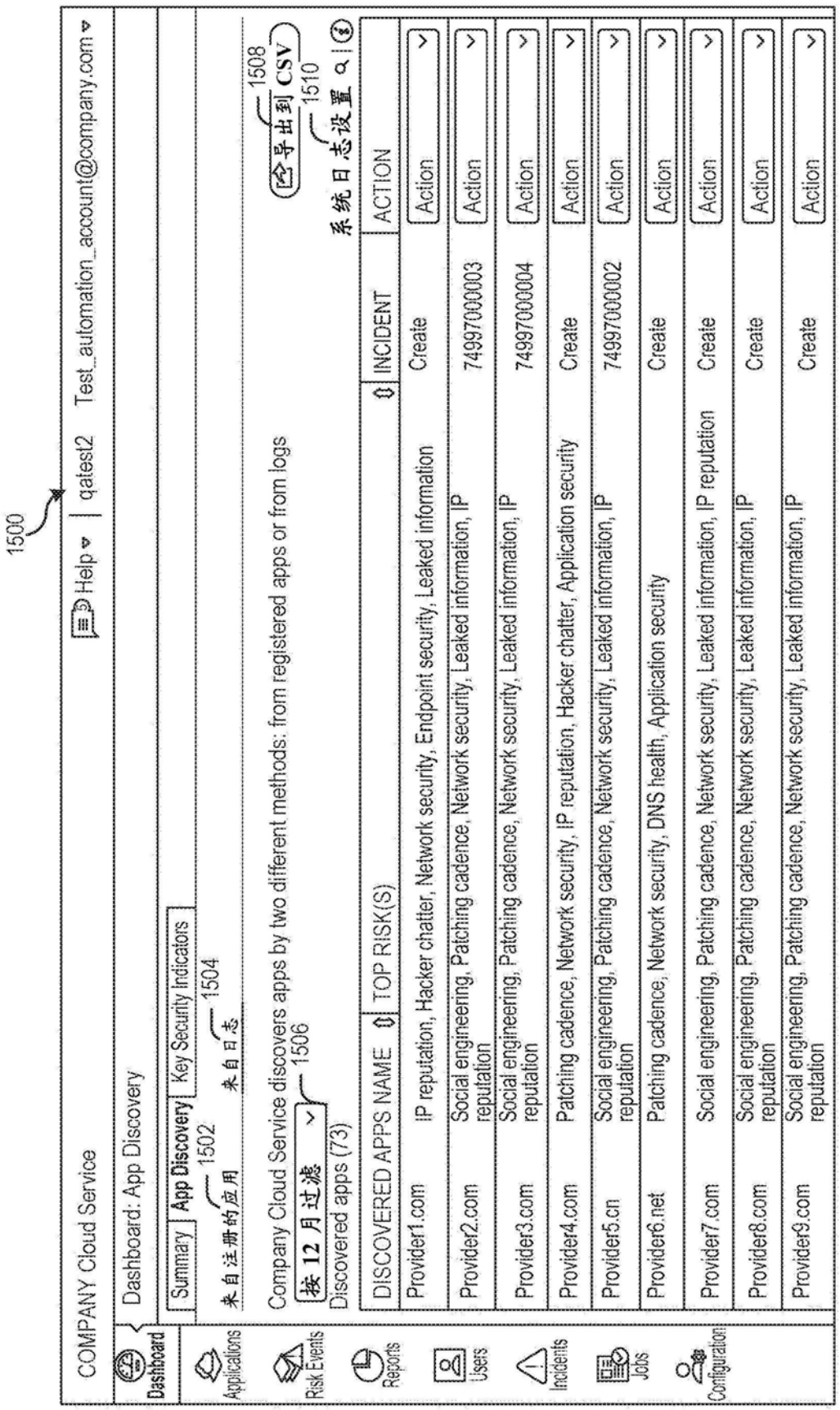
1500
COMPANY Cloud Service
Help
qatest2
Test_automation_account@company.com
Dashboard
Dashboard: App Discovery
Summary
App Discovery
Key Security Indicators
1502
1504
来自注册的应用
来自日志
Applications
Risk Events
Reports
Users
Incidents
Jobs
Configuration
Company Cloud Service discovers apps by two different methods: from registered apps or from logs
1508
导出到 CSV
1510
系统日志设置
按 12 月过滤
1506
Discovered apps (73)
DISCOVERED APPS NAME
TOP RISK(S)
INCIDENT
ACTION
Provider1.com
IP reputation, Hacker chatter, Network security, Endpoint security, Leaked information
Create
Action
Provider2.com
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
74997000003
Action
Provider3.com
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
74997000004
Action
Provider4.com
Patching cadence, Network security, IP reputation, Hacker chatter, Application security
Create
Action
Provider5.cn
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
74997000002
Action
Provider6.net
Patching cadence, Network security, DNS health, Application security
Create
Action
Provider7.com
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
Create
Action
Provider8.com
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
Create
Action
Provider9.com
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
Create
Action

图15

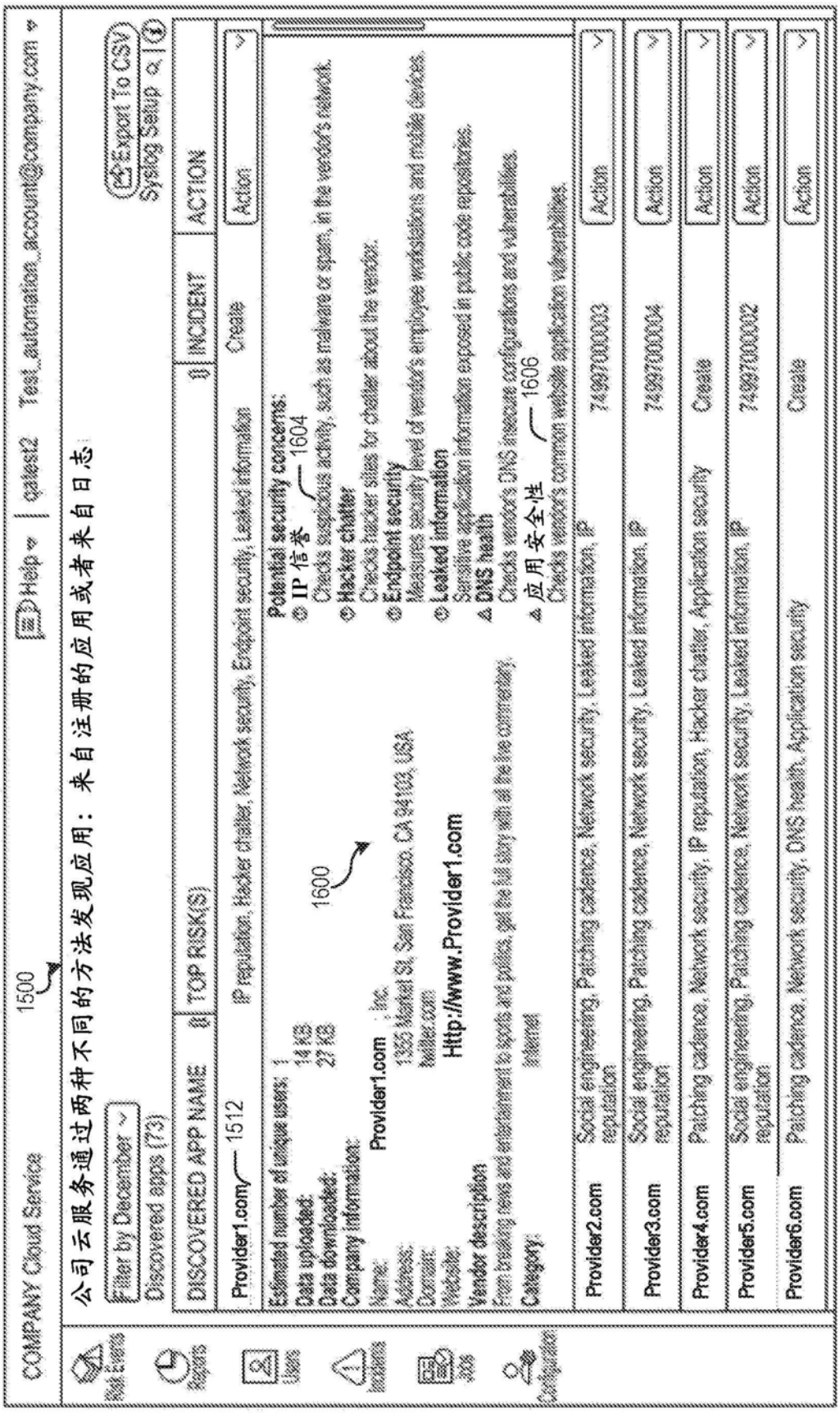
COMPANY Cloud Service
1500
Help
qatest2
Test_automation_account@company.com
Risk Events
Reports
Users
Alarms
Logs
Configuration
公司云服务通过两种不同的方法发现应用：来自注册的应用或者来自日志
Filter by December
Discovered apps (73)
Export To CSV
Syslog Setup
DISCOVERED APP NAME
TOP RISK(S)
INCIDENT
ACTION
Provider1.com 1512
IP reputation, Hacker chatter, Network security, Endpoint security, Leaked information
Create
Action
Estimated number of unique users: 1
Data uploaded: 14 KB
Data downloaded: 27 KB
Company information:
Name: Provider1.com Inc.
Address: 1355 Market St, San Francisco, CA 94103, USA
Domain: twitter.com
Website: Http://www.Provider1.com
Vendor description
From breaking news and entertainment to sports and politics, get the full story with all the live commentary.
Category: Internet
1600
Potential security concerns:
IP 信誉 1604
Checks suspicious activity, such as malware or spam, in the vendor's network.
Hacker chatter
Checks hacker sites for chatter about the vendor.
Endpoint security
Measures security level of vendor's employee workstations and mobile devices.
Leaked information
Sensitive application information exposed in public code repositories.
DNS health
Checks vendor's DNS insecure configurations and vulnerabilities.
应用安全性 1606
Checks vendor's common website application vulnerabilities.
Provider2.com
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
749970000003
Provider3.com
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
749970000004
Provider4.com
Patching cadence, Network security, IP reputation, Hacker chatter, Application security
Create
Provider5.com
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
749970000002
Provider6.com
Patching cadence, Network security, DNS health, Application security

图16

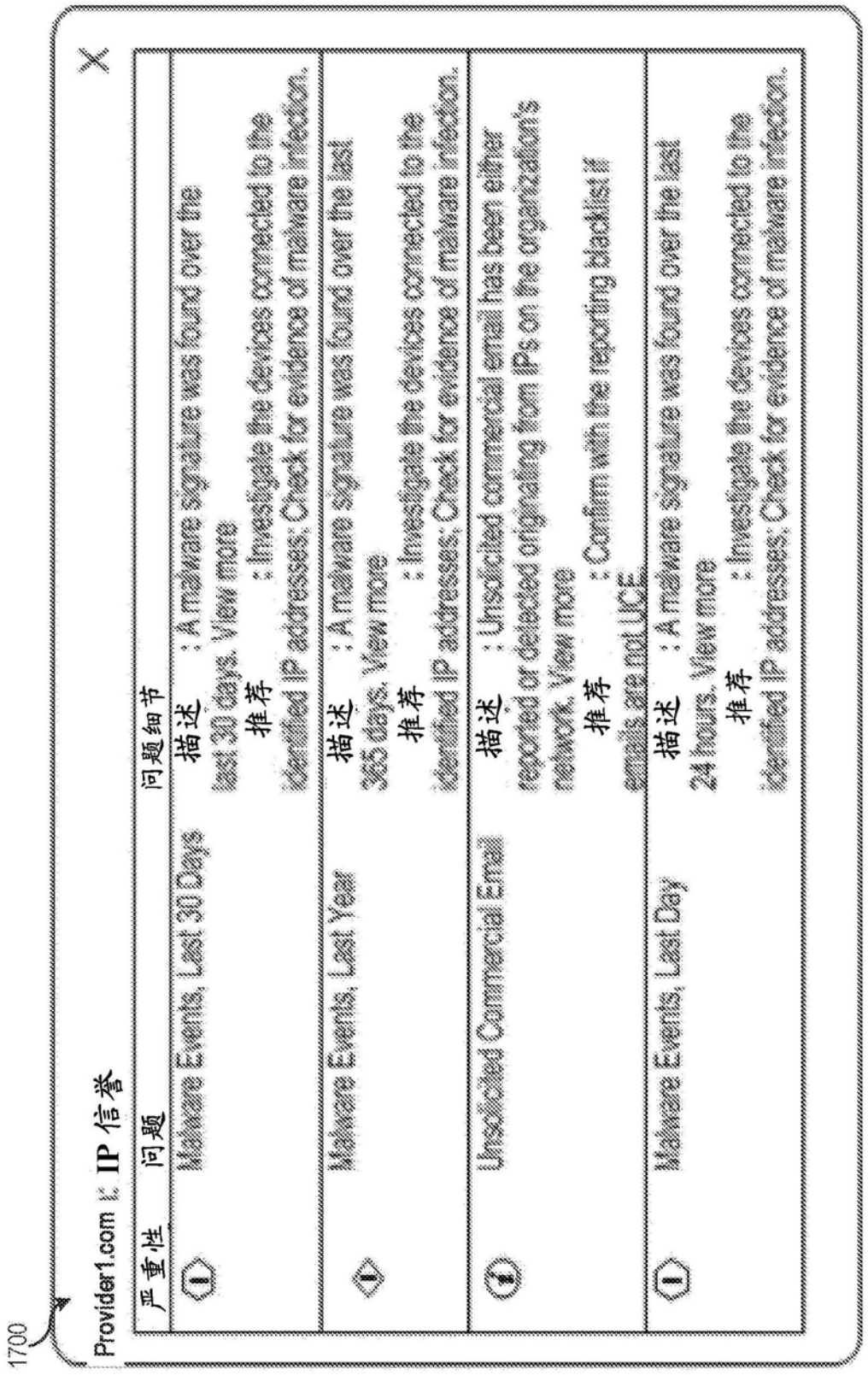
1700
Provider1.com 上 IP 信誉
严重性
问题
问题细节
Malware Events, Last 30 Days
描述 : A malware signature was found over the last 30 days. View more
推荐 : Investigate the devices connected to the identified IP addresses; Check for evidence of malware infection.
Malware Events, Last Year
描述 : A malware signature was found over the last 365 days. View more
推荐 : Investigate the devices connected to the identified IP addresses; Check for evidence of malware infection.
Unsolicited Commercial Email
描述 : Unsolicited commercial email has been either reported or detected originating from IPs on the organization's network. View more
推荐 : Confirm with the reporting blacklist if emails are not UCE
Malware Events, Last Day
描述 : A malware signature was found over the last 24 hours. View more
推荐 : Investigate the devices connected to the identified IP addresses; Check for evidence of malware infection.

图17

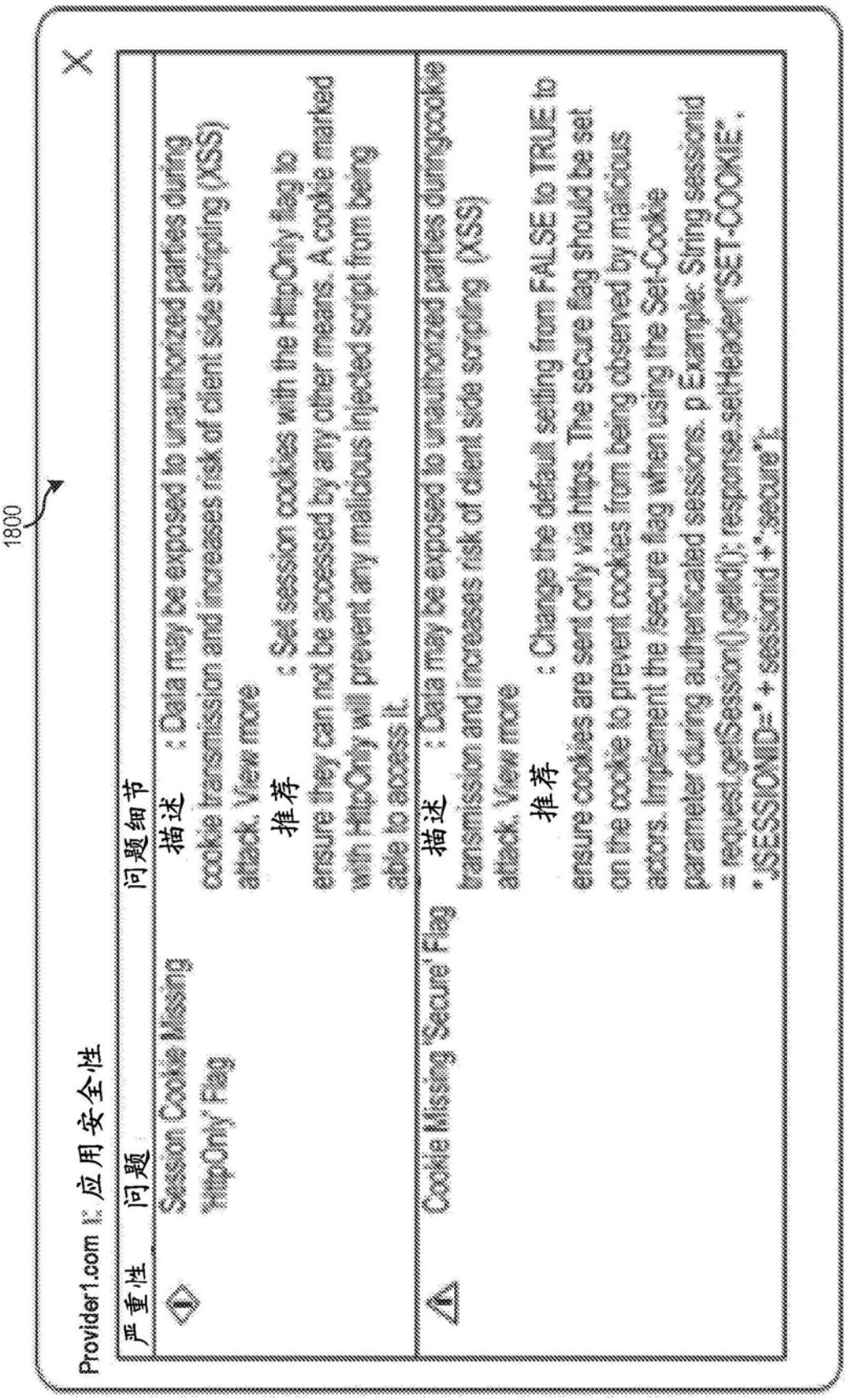
1800
X
Provider1.com 的应用安全性
严重性
问题
问题细节
Session Cookie Missing 'HttpOnly' Flag
描述 : Data may be exposed to unauthorized parties during cookie transmission and increases risk of client side scripting (XSS) attack. View more
推荐 : Set session cookies with the HttpOnly flag to ensure they can not be accessed by any other means. A cookie marked with HttpOnly will prevent any malicious injected script from being able to access it.
Cookie Missing 'Secure' Flag
描述 : Data may be exposed to unauthorized parties duringcookie transmission and increases risk of client side scripting (XSS) attack. View more
推荐 : Change the default setting from FALSE to TRUE to ensure cookies are sent only via https. The secure flag should be set on the cookie to prevent cookies from being observed by malicious actors. Implement the /secure flag when using the Set-Cookie parameter during authenticated sessions. p Example: String sessionid = request.getSession().getId(); response.setHeader("SET-COOKIE", "JSESSIONID=" + sessionid +";secure");

图18

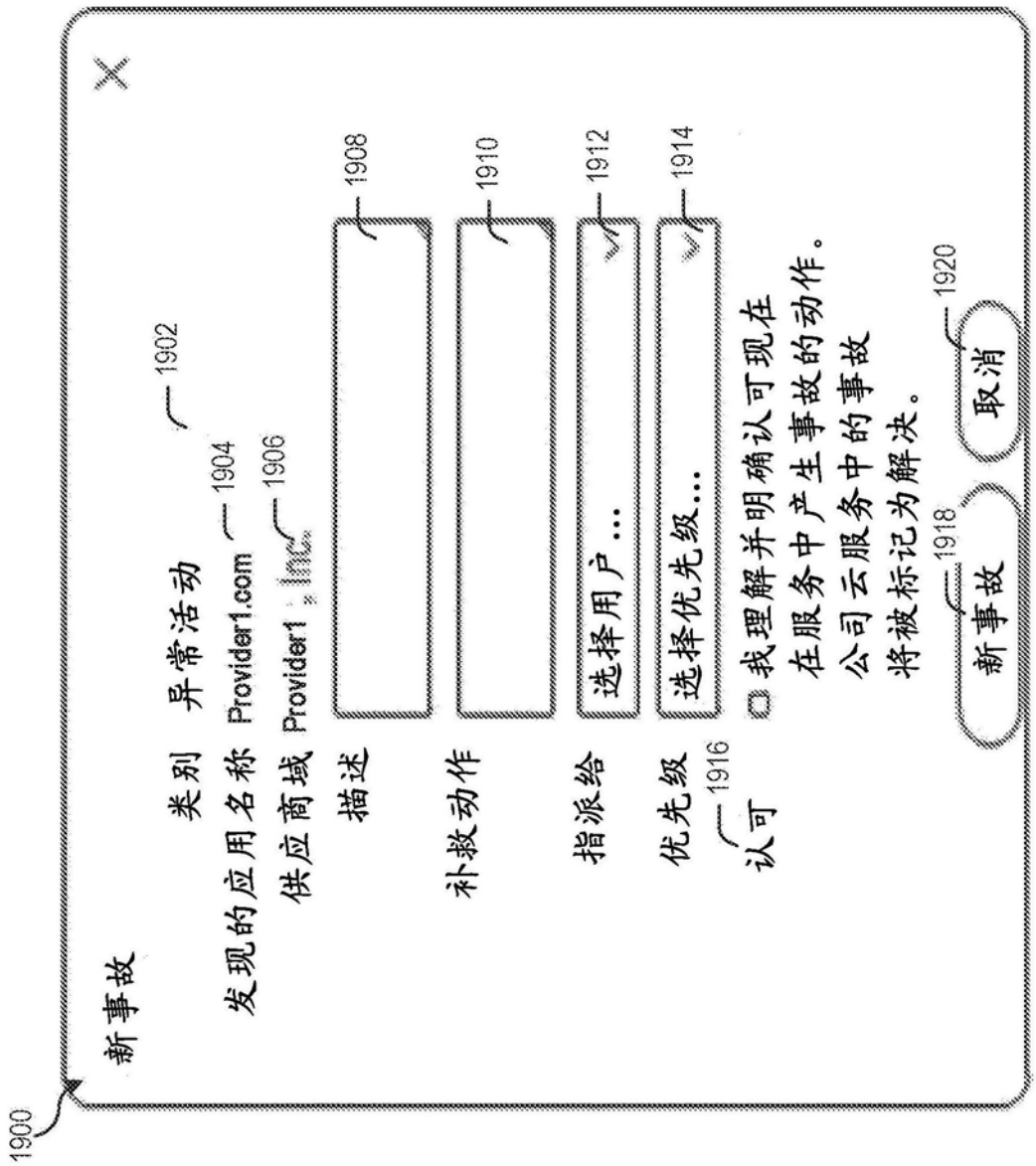
1900
新事故
X
类别 异常活动
1902
发现的应用名称 Provider1.com
1904
供应商域 Provider1 , Inc.
1906
描述
1908
补救动作
1910
指派给 选择用户 ...
1912
优先级 选择优先级...
1914
认可
1916
我理解并明确认可现在
在服务中产生事故的动作。
公司云服务中的事故
将被标记为解决。
1918
新事故
取消
1920

图19

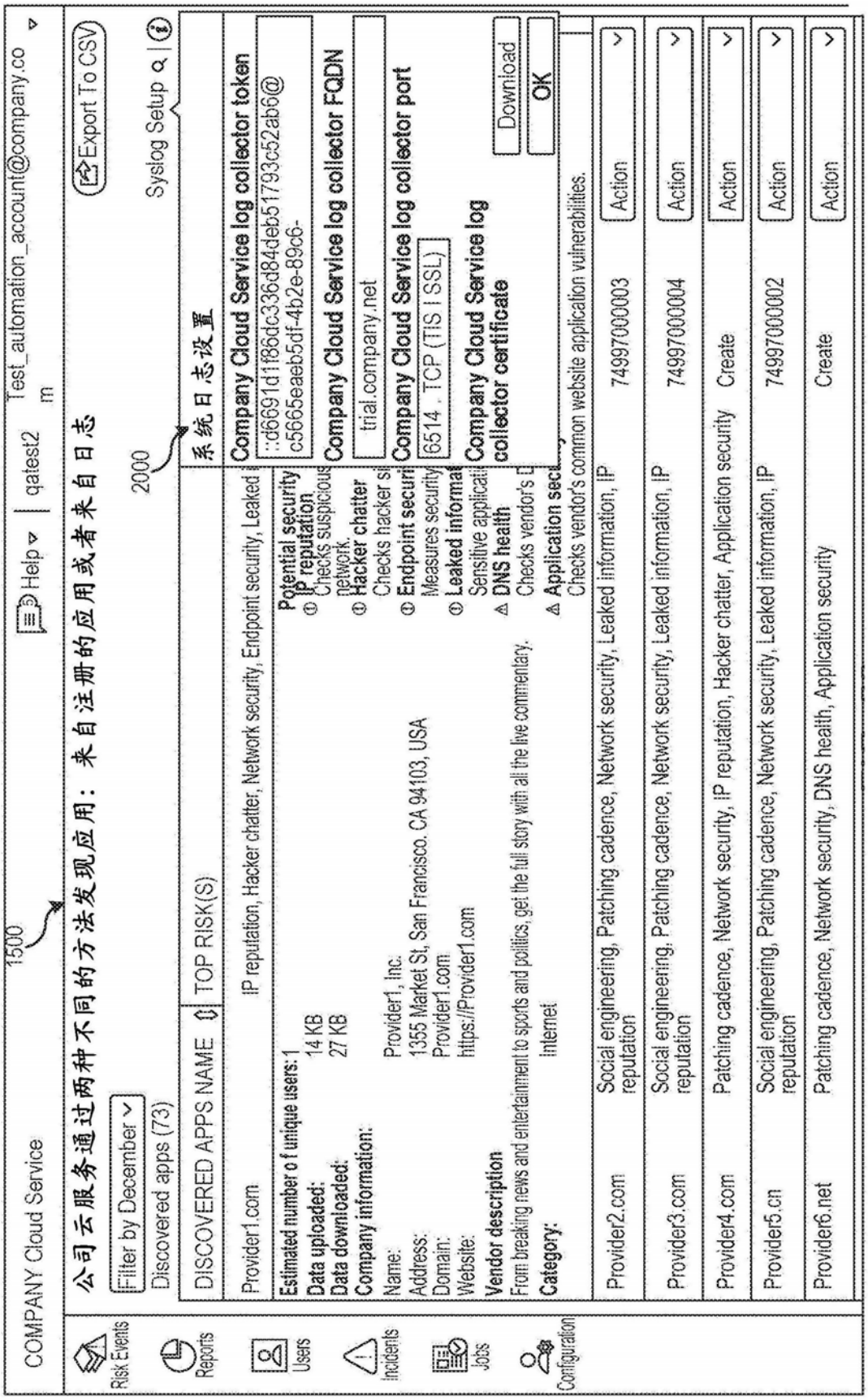
COMPANY Cloud Service
1500
Help
qatest2
Test_automation_account@company.com
公司云服务通过两种不同的方法发现应用：来自注册的应用或者来自日志
Export To CSV
Filter by December
Discovered apps (73)
2000
Syslog Setup
DISCOVERED APPS NAME
TOP RISK(S)
系统日志设置
Risk Events
Reports
Users
Incidents
Jobs
Configuration
Provider1.com
IP reputation, Hacker chatter, Network security, Endpoint security, Leaked
Company Cloud Service log collector token
::d6691d1f86dc336d84deb51793c52ab6@
c5665eaeb5df-4b2e-89c6-
Company Cloud Service log collector FQDN
trial.company.net
Company Cloud Service log collector port
6514 - TCP (TIS I SSL)
Company Cloud Service log collector certificate
Download
OK
Estimated number o f unique users: 1
Data uploaded: 14 KB
Data downloaded: 27 KB
Company information:
Name: Provider1, Inc.
Address: 1355 Market St, San Francisco, CA 94103, USA
Domain: Provider1.com
Website: https://Provider1.com
Vendor description
From breaking news and entertainment to sports and politics, get the full story with all the live commentary.
Category: Internet
Potential security
IP reputation
Checks suspicious network
Hacker chatter
Checks hacker si
Endpoint securi
Measures security
Leaked informat
Sensitive applicati
DNS health
Checks vendor's D
Application sec
Checks vendor's common website application vulnerabilities.
Provider2.com
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
74997000003
Action
Provider3.com
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
74997000004
Action
Provider4.com
Patching cadence, Network security, IP reputation, Hacker chatter, Application security
Create
Action
Provider5.cn
Social engineering, Patching cadence, Network security, Leaked information, IP reputation
74997000002
Action
Provider6.net
Patching cadence, Network security, DNS health, Application security
Create
Action

图20

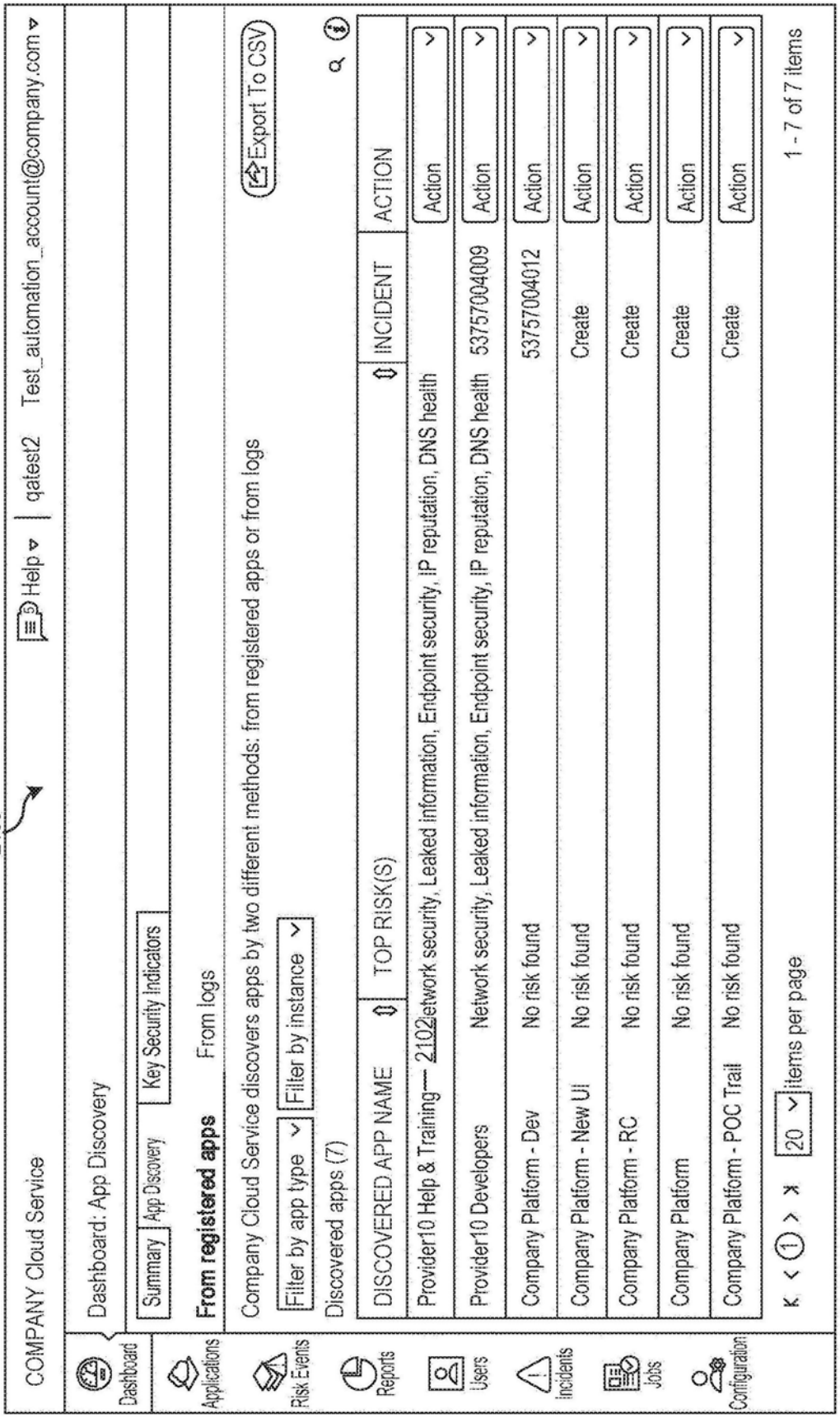
2100
COMPANY Cloud Service
Help
qatest2
Test_automation_account@company.com
Dashboard
Dashboard: App Discovery
Summary
App Discovery
Key Security Indicators
From registered apps
From logs
Company Cloud Service discovers apps by two different methods: from registered apps or from logs
Export To CSV
Filter by app type
Filter by instance
Discovered apps (7)
DISCOVERED APP NAME
TOP RISK(S)
INCIDENT
ACTION
Provider10 Help & Training
2102
etwork security, Leaked information, Endpoint security, IP reputation, DNS heaith
Action
Provider10 Developers
Network security, Leaked information, Endpoint security, IP reputation, DNS health
53757004009
Action
Company Platform - Dev
No risk found
53757004012
Action
Company Platform - New UI
No risk found
Create
Action
Company Platform - RC
No risk found
Create
Action
Company Platform
No risk found
Create
Action
Company Platform - POC Trail
No risk found
Create
Action
items per page
20
1 - 7 of 7 items
Applications
Risk Events
Reports
Users
Incidents
Jobs
Configuration

图21

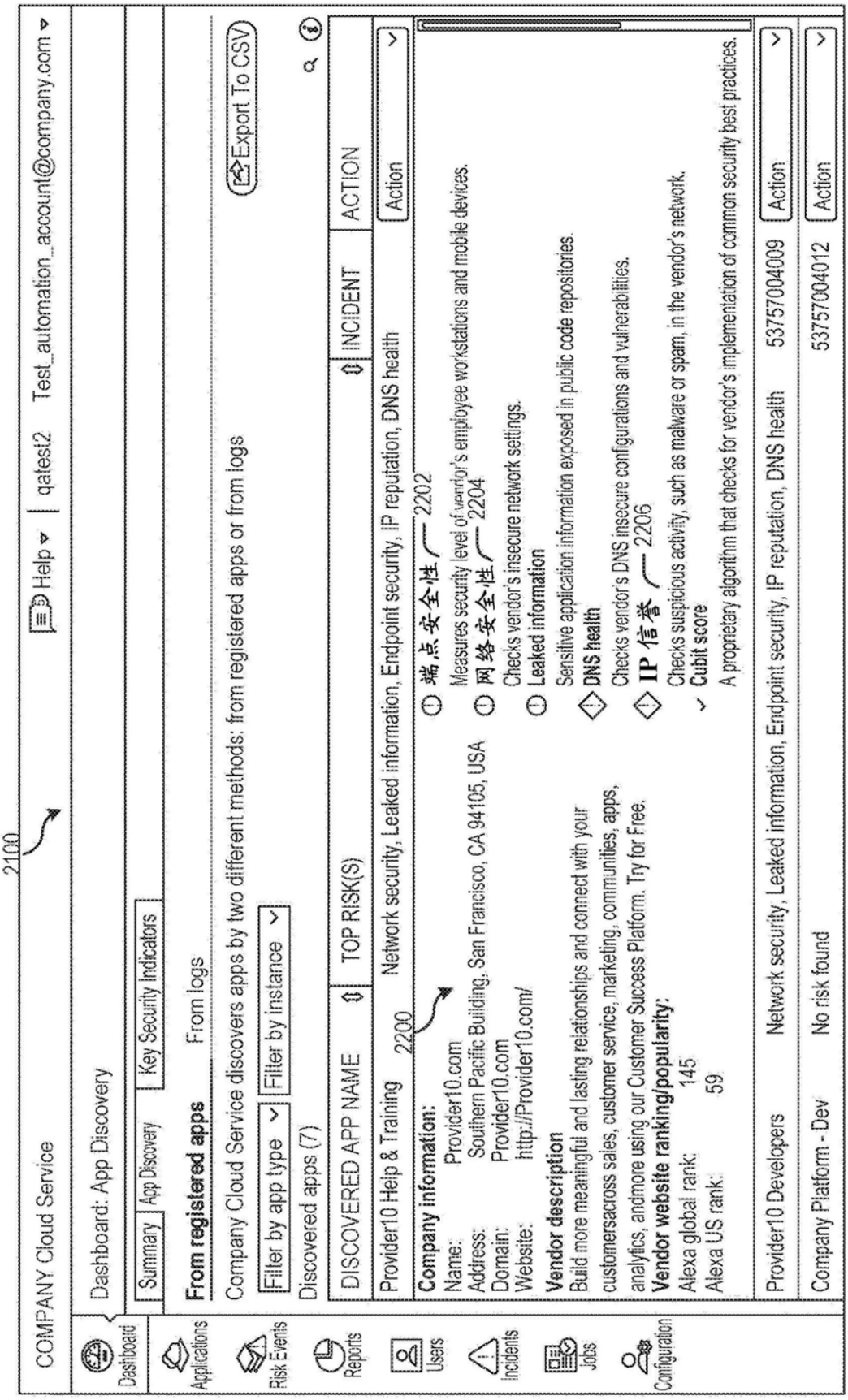
2100
COMPANY Cloud Service
Help
qatest2
Test_automation_account@company.com
Dashboard
Dashboard: App Discovery
Summary
App Discovery
Key Security Indicators
Applications
From registered apps
From logs
Risk Events
Company Cloud Service discovers apps by two different methods: from registered apps or from logs
Export To CSV
Reports
Filter by app type
Filter by instance
Discovered apps (7)
Users
DISCOVERED APP NAME
TOP RISK(S)
INCIDENT
ACTION
Incidents
Provider10 Help & Training
2200
Network security, Leaked information, Endpoint security, IP reputation, DNS health
Action
Jobs
Company information:
Name: Provider10.com
Address: Southern Pacific Building, San Francisco, CA 94105, USA
Domain: Provider10.com
Website: http://Provider10.com/
Vendor description
Build more meaningful and lasting relationships and connect with your customersacross sales, customer service, marketing, communities, apps, analytics, andmore using our Customer Success Platform. Try for Free.
Vendor website ranking/popularity:
Alexa global rank: 145
Alexa US rank: 59
端点安全性
2202
Measures security level of vendor's employee workstations and mobile devices.
网络安全性
2204
Checks vendor's insecure network settings.
Leaked information
Sensitive application information exposed in public code repositories.
DNS health
Checks vendor's DNS insecure configurations and vulnerabilities.
IP 信誉
2206
Checks suspicious activity, such as malware or spam, in the vendor's network.
Cubit score
A proprietary algorithm that checks for vendor's implementation of common security best practices.
Configuration
Provider10 Developers
Network security, Leaked information, Endpoint security, IP reputation, DNS health
53757004009
Action
Company Platform - Dev
No risk found
53757004012
Action

图22

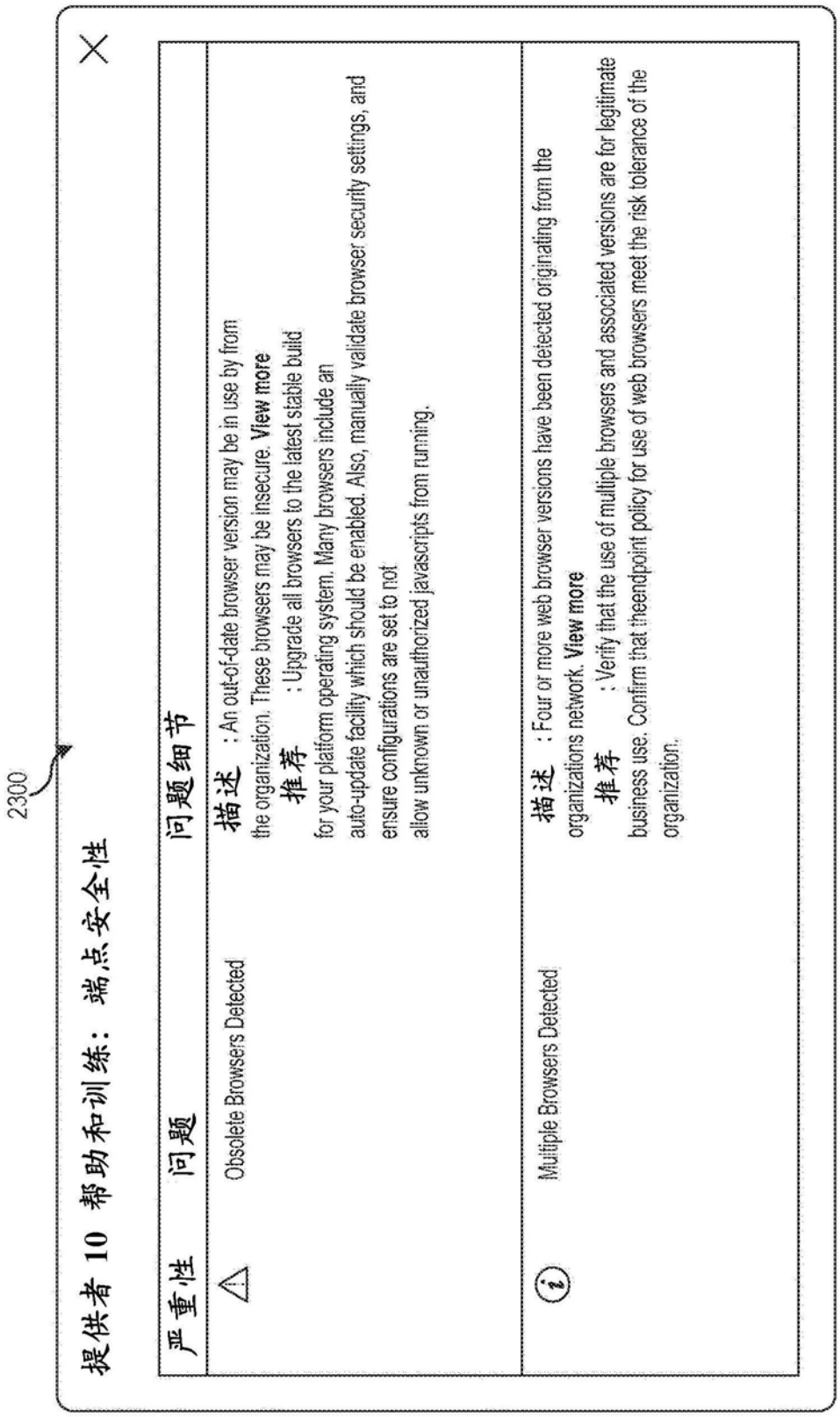
2300
提供者 10 帮助和训练： 端点安全性
严重性
问题
问题细节
Obsolete Browsers Detected
描述 : An out-of-date browser version may be in use by from the organization. These browsers may be insecure. View more
推荐 : Upgrade all browsers to the latest stable build for your platform operating system. Many browsers include an auto-update facility which should be enabled. Also, manually validate browser security settings, and ensure configurations are set to not allow unknown or unauthorized javascripts from running.
Multiple Browsers Detected
描述 : Four or more web browser versions have been detected originating from the organizations network. View more
推荐 : Verify that the use of multiple browsers and associated versions are for legitimate business use. Confirm that theendpoint policy for use of web browsers meet the risk tolerance of the organization.

图23

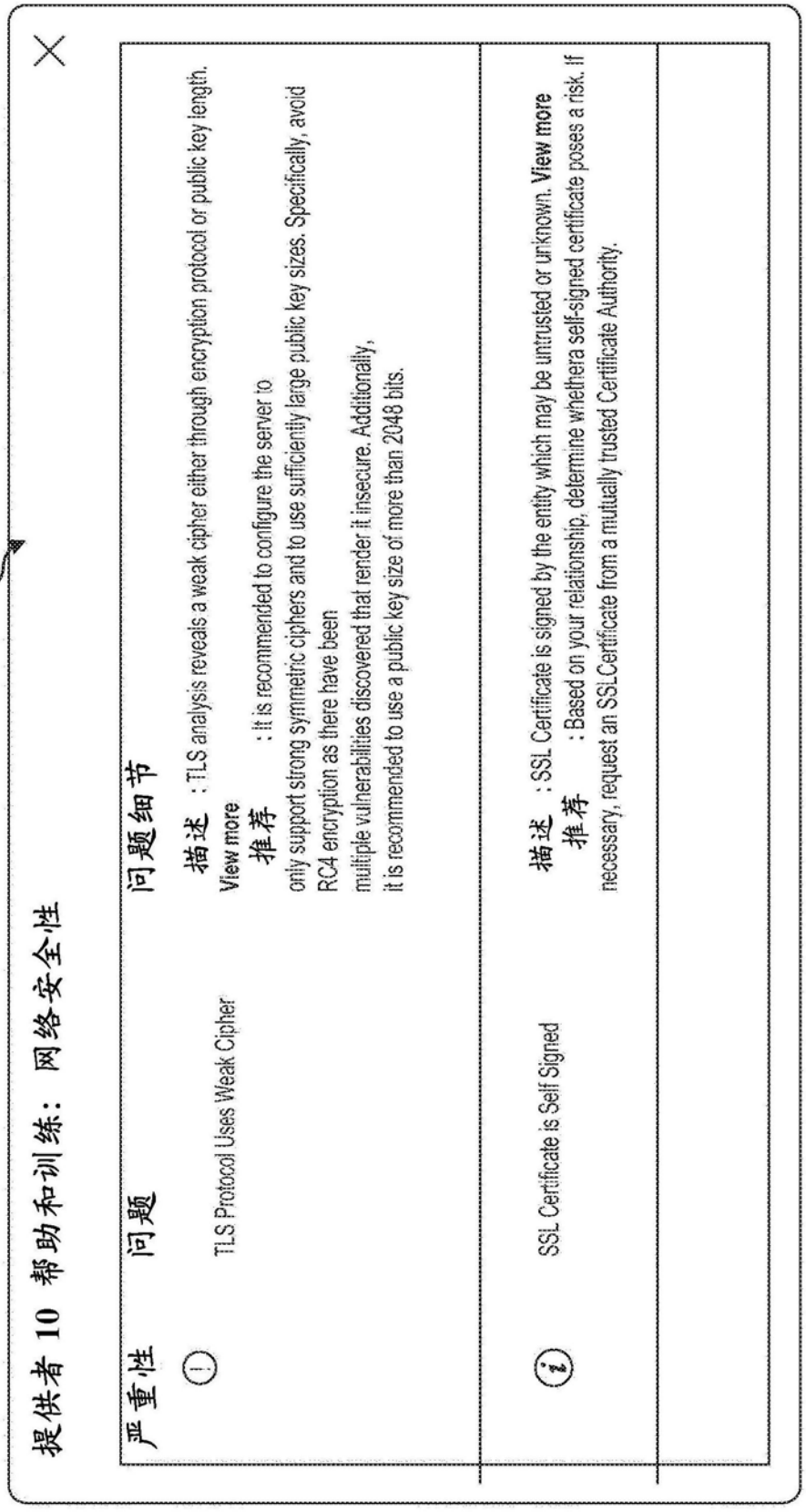
2400
提供者 10 帮助和训练： 网络安全性
严重性
问题
问题细节
TLS Protocol Uses Weak Cipher
描述 : TLS analysis reveals a weak cipher either through encryption protocol or public key length.
View more
推荐 : it is recommended to configure the server to only support strong symmetric ciphers and to use sufficiently large public key sizes. Specifically, avoid RC4 encryption as there have been multiple vulnerabilities discovered that render it insecure. Additionally, it is recommended to use a public key size of more than 2048 bits.
SSL Certificate is Self Signed
描述 : SSL Certificate is signed by the entity which may be untrusted or unknown. View more
推荐 : Based on your relationship, determine whethera self-signed certificate poses a risk. If necessary, request an SSLCertificate from a mutually trusted Certificate Authority.

图24

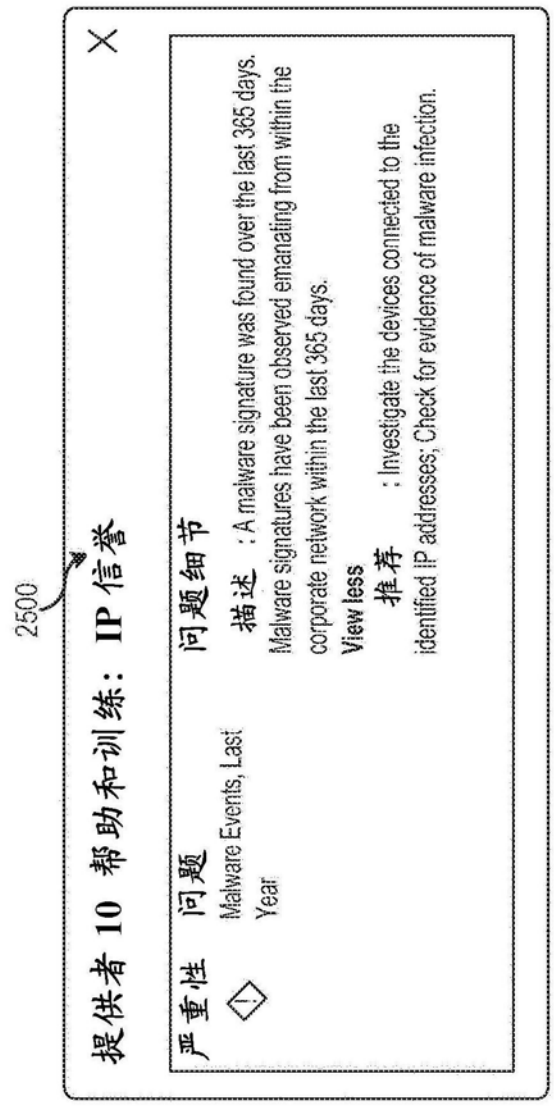
2500
提供者 10 帮助和训练：IP 信誉
严重性
问题
Malware Events, Last Year
问题细节
描述 : A malware signature was found over the last 365 days. Malware signatures have been observed emanating from within the corporate network within the last 365 days.
View less
推荐 : Investigate the devices connected to the identified IP addresses; Check for evidence of malware infection.

图25

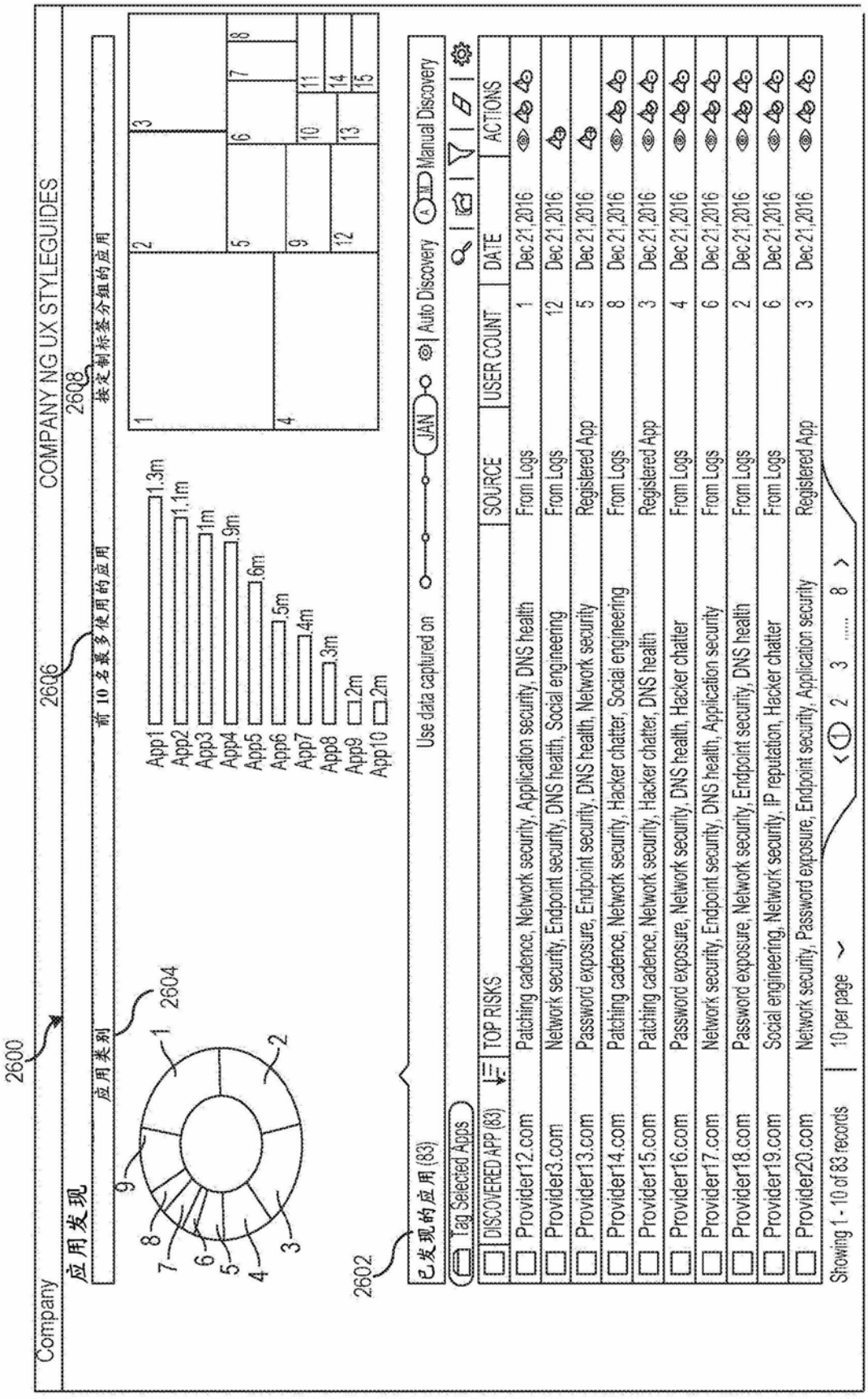
2600
Company
COMPANY NG UX STYLEGUIDES
2606
2608
应用发现
应用类别
前 10 名最多使用的应用
按定制标签分组的应用
2604
1
2
3
4
5
6
7
8
9
App1 1.3m
App2 1.1m
App3 1m
App4 .9m
App5 .6m
App6 .5m
App7 .4m
App8 .3m
App9 .2m
App10 .2m
2602
已发现的应用 (83)
Use data captured on
JAN
Auto Discovery
Manual Discovery
Tag Selected Apps
DISCOVERED APP (83)
TOP RISKS
SOURCE
USER COUNT
DATE
ACTIONS
Provider12.com Patching cadence, Network security, Application security, DNS health From Logs 1 Dec 21, 2016
Provider3.com Network security, Endpoint security, DNS health, Social engineering From Logs 12 Dec 21, 2016
Provider13.com Password exposure, Endpoint security, DNS health, Network security Registered App 5 Dec 21, 2016
Provider14.com Patching cadence, Network security, Hacker chatter, Social engineering From Logs 8 Dec 21, 2016
Provider15.com Patching cadence, Network security, Hacker chatter, DNS health Registered App 3 Dec 21, 2016
Provider16.com Password exposure, Network security, DNS health, Hacker chatter From Logs 4 Dec 21, 2016
Provider17.com Network security, Endpoint security, DNS health, Application security From Logs 6 Dec 21, 2016
Provider18.com Password exposure, Network security, Endpoint security, DNS health From Logs 2 Dec 21, 2016
Provider19.com Social engineering, Network security, IP reputation, Hacker chatter From Logs 6 Dec 21, 2016
Provider20.com Network security, Password exposure, Endpoint security, Application security Registered App 3 Dec 21, 2016
Showing 1 - 10 of 83 records
10 per page
1 2 3 8

图26

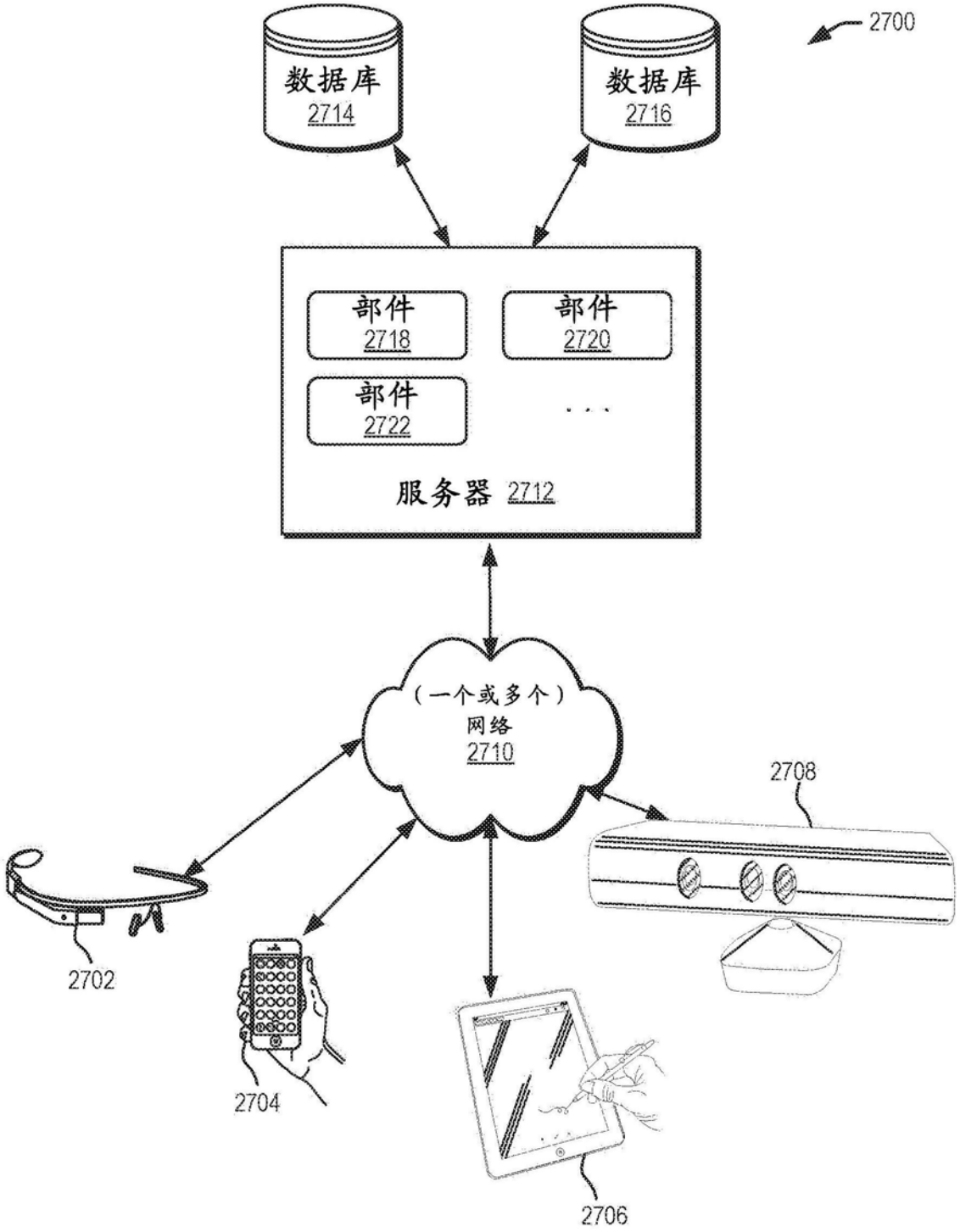
2700
数据库
2714
数据库
2716
部件
2718
部件
2720
部件
2722
. . .
服务器 2712
（一个或多个）
网络
2710
2708
2702
2704
2706

图27

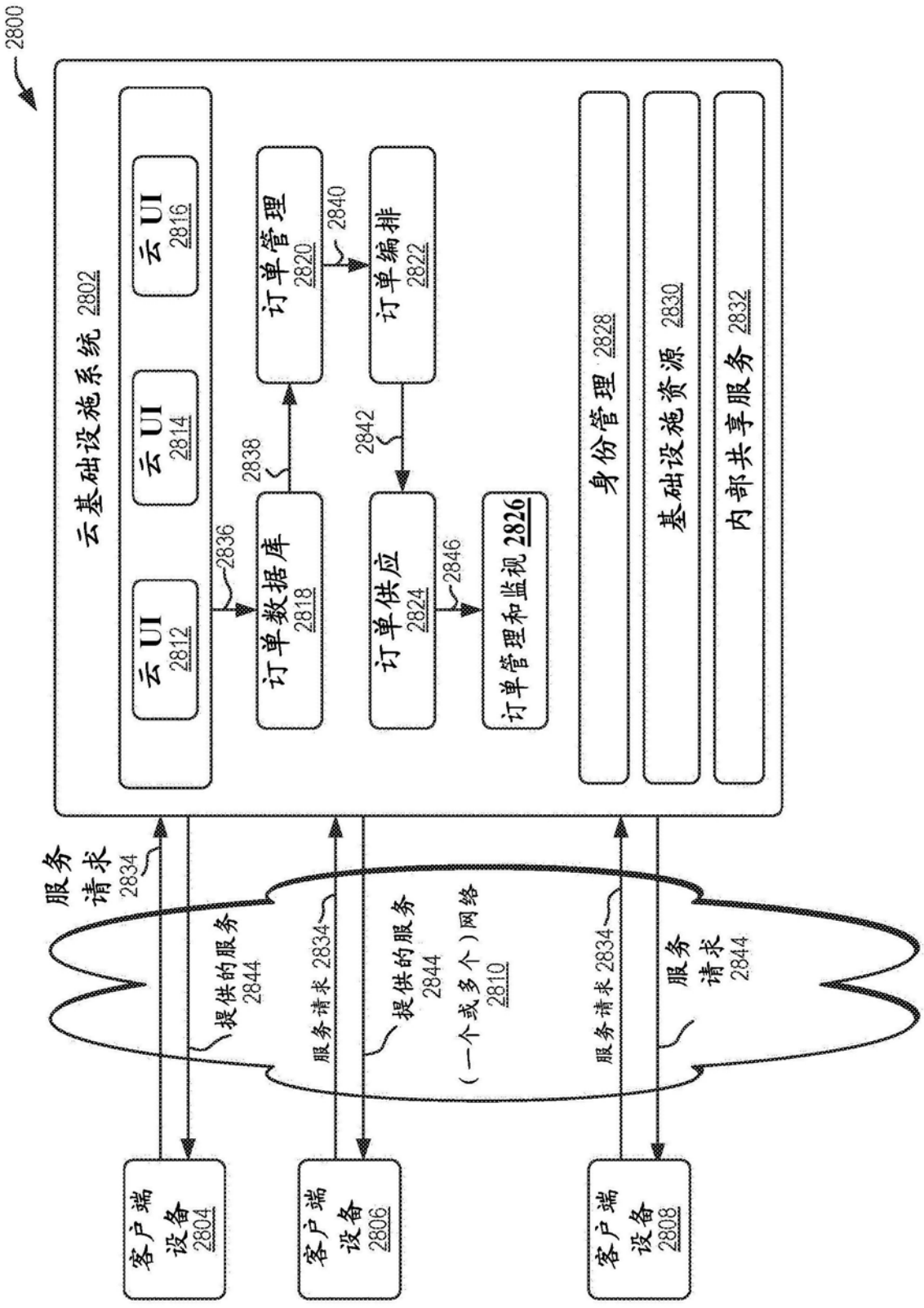
2800
云基础设施系统 2802
云 UI 2812
云 UI 2814
云 UI 2816
订单数据库 2818
订单管理 2820
订单编排 2822
订单供应 2824
订单管理和监视 2826
身份管理 2828
基础设施资源 2830
内部共享服务 2832
2836
2838
2840
2842
2846
服务请求 2834
提供的服务 2844
服务请求 2834
提供的服务 2844
（一个或多个）网络 2810
服务请求 2834
服务请求 2844
客户端设备 2804
客户端设备 2806
客户端设备 2808

图28

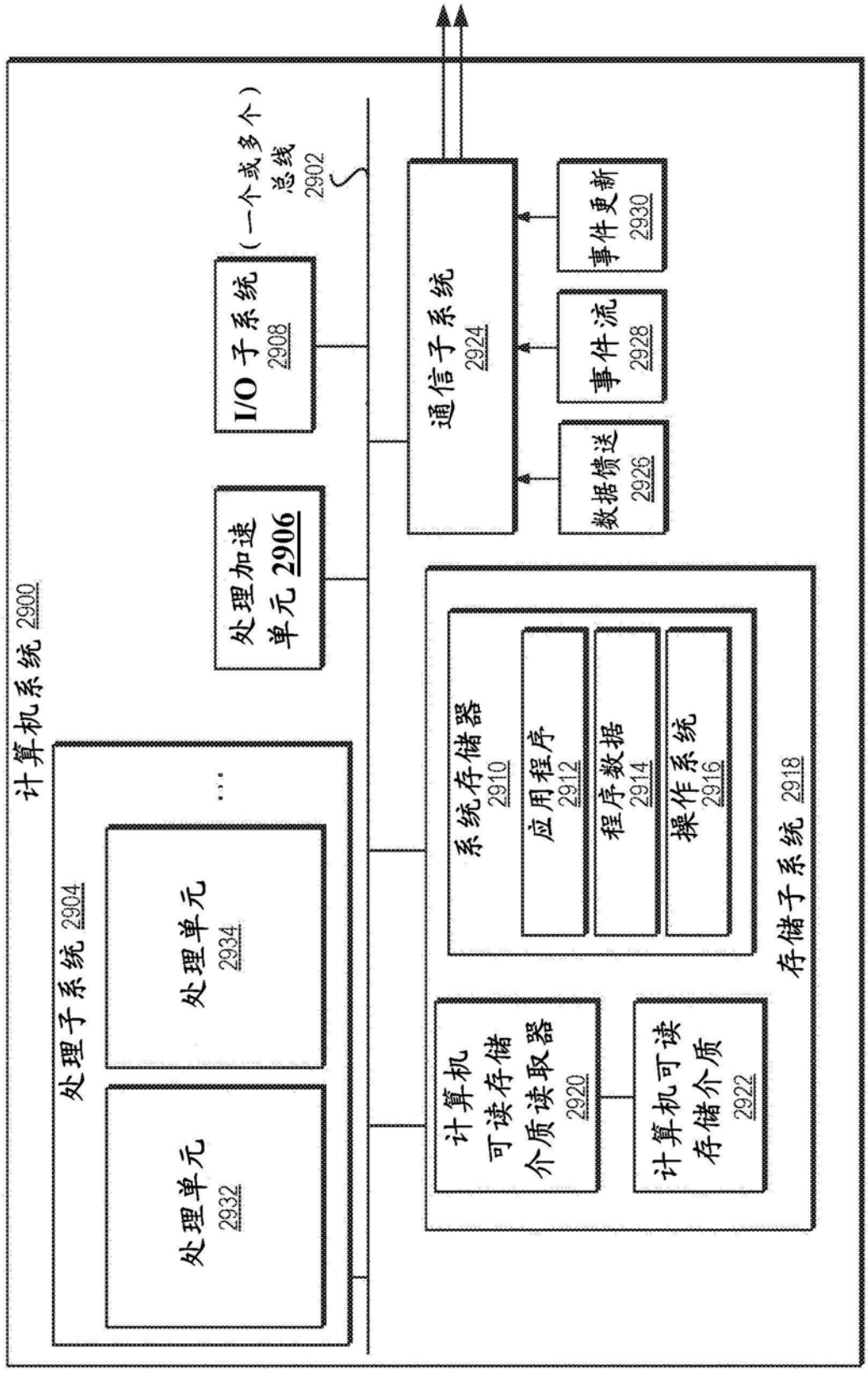
计算机系统 2900
处理子系统 2904
处理单元 2932
处理单元 2934
...
处理加速单元 2906
I/O 子系统 2908
(一个或多个)总线 2902
通信子系统 2924
事件更新 2930
事件流 2928
数据馈送 2926
存储子系统 2918
系统存储器 2910
应用程序 2912
程序数据 2914
操作系统 2916
计算机可读存储介质读取器 2920
计算机可读存储介质 2922

图29