(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 101632085 B
(45)授权公告日 2012.12.12

(21)申请号 200880008153.3

(22)申请日 2008.03.14

(30)优先权数据
11/724,061 2007.03.14 US

(85)PCT申请进入国家阶段日
2009.09.14

(86)PCT申请的申请数据
PCT/US2008/057164 2008.03.14

(87)PCT申请的公布数据
WO2008/113059 EN 2008.09.18

(73)专利权人 微软公司
地址 美国华盛顿州

(72)发明人 E·胡迪斯 Y·黑尔曼 J·马尔卡 U·巴拉什

(74)专利代理机构 上海专利商标事务所有限公司 31100
代理人 蔡悦 钱静芳

(51)Int.Cl.
G06F 21/00(2006.01)
G06F 15/16(2006.01)
G06F 17/00(2006.01)

(56)对比文件
US 2006031938 A1,2006.02.09, 说明书第40段第3-7行，第42段，第110段第1行,5-7行,15-18行，第115段第8-12行，第161段，第171段，权利要求24.
CN 1618198 A,2005.05.18, 全文.
US 6986060 B1,2006.01.10, 全文.
US 2004010709 A1,2004.01.15, 说明书第24段，第25,26段，表1.
US 2005015626 A1,2005.01.20, 说明书第52段第22-31行.
US 2006031938 A1,2006.02.09, 说明书第40段第3-7行，第42段，第110段第1行,5-7行,15-18行，第115段第8-12行，第161段，第171段，权利要求24.

审查员 马鑫

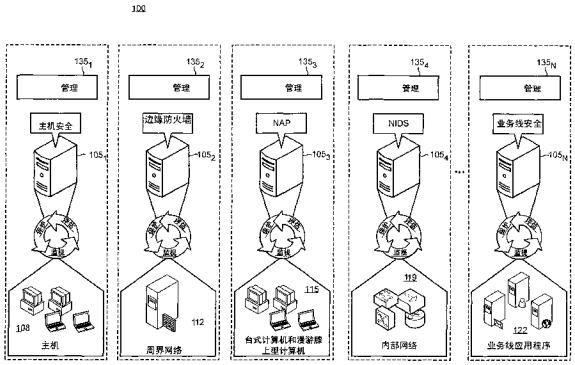
权利要求书 1 页 说明书 13 页 附图 11 页

(54)发明名称

企业安全评估共享

(57)摘要

企业范围共享安排使用被称为安全评估的语义抽象来在被称为端点的不同安全产品之间共享安全相关信息。安全评估被定义为端点将较宽泛的上下文含义向所收集的关于感兴趣对象的信息的试验性指派。其试验性特性反映在其两个分量中:用于表达对评估的置信度水平的保真度字段,以及对应于所估计的评估有效时间段的生存时间字段。端点可将安全评估发布到安全评估信道上,以及订阅由其他端点发布的安全评估的子集。一专用端点耦合到该信道,该专用端点通过订阅所有安全评估、记录安全评估、并且还记录由各端点响应于安全威胁而采取的本地动作来作为集中式审核点来执行。



CN 101632085 B

1. 一种使用安全相关信息共享模型的方法，所述安全相关信息共享模型可用于在企业安全环境中的多个端点之间共享安全相关信息，所述方法包括以下步骤：

使用对于端点可用的安全相关信息的语义抽象来描述所述环境中的对象，所述语义抽象是被安排成由端点使用预定义分类向所述安全相关信息提供上下文指派的安全评估，所述语义抽象 i）按类型来进行分类，并且 ii）由所述端点来共同利用，每个所述端点被配置为接收由其它端点发布的语义抽象，并且每个所述端点被进一步配置为响应于所接收到的语义抽象使用信息来生成新的语义抽象，所述信息对于执行所述生成的端点来说是本地可用的；以及

使用发布端点用于发布订阅端点根据订阅来接收的语义抽象的发布和订阅模型，所述订阅基于语义抽象类型。

2. 如权利要求 1 所述的方法，其特征在于，所述对象类型包括主机、用户、服务、数据或企业中的至少一个。

3. 如权利要求 1 所述的方法，其特征在于，所述评估类别包括易受攻击、已受损、正被攻击、感兴趣、已破坏或恶意中的至少一个。

4. 如权利要求 1 所述的方法，其特征在于，所述评估类别中的特定评估类别被映射到所述对象类型中的特定对象类型。

5. 如权利要求 1 所述的方法，其特征在于，所述安全评估包括多个字段，所述多个字段中的至少一个是被安排成表达端点对所述安全评估的置信度的保真度字段。

6. 如权利要求 1 所述的方法，其特征在于，所述安全评估包括多个字段，所述多个字段中的至少一个是被安排成表达端点对所述安全评估预期有效的时间段的估计的生存时间字段。

7. 如权利要求 1 所述的方法，其特征在于，所述多个端点中的至少一个端点包括安全解决方案对象，所述对象选自安全产品、安全解决方案、管理产品、管理解决方案、安全服务或管理服务中的一个。

8. 一种用于使得端点能够共享企业安全环境中的安全相关数据的方法，所述方法包括以下步骤：

生成用于描述事件的安全评估，其中所述生成至少部分地基于关于由所述端点监视的系统的本地可用信息，所述安全评估被安排成为所述事件提供上下文含义并且用所述安全评估在其上有效的时间间隔来定义；

根据对由所述企业安全环境中的其他端点生成的可用安全评估的子集的订阅来接收当前安全评估；

响应于所接收的当前安全评估生成更新的安全评估；以及

在每一个安全评估的基础上根据响应策略来采取响应。

9. 如权利要求 8 所述的方法，其特征在于，所述响应包括本地动作。

10. 如权利要求 8 所述的方法，其特征在于，所述本地可用信息还包括由所述端点采取的一个或多个过去的本地动作。

11. 如权利要求 8 所述的方法，其特征在于，包括一旦所接收到的安全评估不再有效就回退所述本地动作的进一步的步骤。

企业安全评估共享

[0001] 背景

[0002] 在例如企业办公室的企业计算环境中，多个个人计算机、工作站服务器等，以及诸如大容量存储子系统、内部网络接口和外部网络接口等其他设备通常互相连接以提供其中可生成，从外部源访问并在各个用户之间共享信息的集成环境。通常，用户可执行各种操作，包括定单接收、制造、送货、记帐、库存控制、文档准备和管理、电子邮件、web 浏览、以及其中创建、访问和共享数据是有益的其他操作。

[0003] 当前，通常使用各种不同的安全产品来为企业提供安全性，这些产品各自一般被安排成监视企业范围数据的仅仅一部分。即，安全产品被安排为单独的本地“岛”，其中每一个产品监视、评估企业中的数据的不同部分并对其采取动作。例如，企业可利用诸如保护该企业中的主机计算机的产品、边缘防火墙产品、网络侵入检测系统（“NIDS”）产品、网络接入保护（“NAP”）产品以及其他分立安全产品等安全产品的组合来为该企业的各不同部分提供安全性。

[0004] 虽然这些安全产品在许多应用中通常都令人满意地执行，但对安全事故的检测经常遭受由于只监视部分企业安全数据而导致的不合需要地高的假肯定和假否定出现水平。也难以提供跨所有企业安全产品岛的公共管理。使得企业范围安全数据相关的现有尝试具有高管理和维护成本并且有缩放方面的问题。将需要更有效的企业安全管理来使得单个企业范围视图能够允许安全管理员定义并强制实施用于自动响应安全事故的清楚、简单且统一的企业范围策略。

[0005] 提供本背景来介绍以下概述和详细描述的简要上下文。本背景不旨在帮助确定所要求保护的主题的范围，也不旨在被看作将所要求保护的主题限于解决以上所提出的问题或缺点中的任一个或全部的实现。

[0006] 概述

[0007] 提供被称为“ESAS，即，企业安全评估共享”的企业范围共享安排，其中创建被称为安全评估的语义抽象以允许在企业安全环境中被称为端点的不同安全产品之间共享安全相关信息。安全评估被定义为端点将较宽泛的上下文含义向所收集的关于该环境中诸如计算机、用户、服务（例如，网站）、数据或作为整体的企业等感兴趣对象的信息（即，某些上下文中的数据）的试验性指派。安全评估利用对于端点的简明词汇来声明环境中的对象落入诸如“已受损”或“正被攻击”等特定评估类别以及所检测到的事故的严重性（例如，低、中、高、关键）。

[0008] 安全评估是试验性的，因为它遭受某种不确定性并且在有限时间段内有效。安全评估的试验性特性反映在其两个分量中：保真度字段，其表达端点对其上下文含义指派的置信度水平，以及生存时间（“TTL”）字段，其反映端点对安全评估预期有效的时间段的估计。由此，例如，安全评估可由端点用来根据该端点对一个或多个安全事故的现有理解来声明特定机器已受损，严重性等级为关键、保真度为中且具有 30 分钟的 TTL。可以在任何给定企业安全环境中使用各种类型的安全评估，从而具有例如评估类别和其他类型的各种组合。

[0009] 端点可具有将安全评估发布到在环境中操作的安全评估信道上，以及订阅由其他端点发布的可用安全评估的子集的功能。存在于环境中的活动的安全评估（即，具有指示评估仍然有效的 TTL 的安全评估）用于提供安全上下文，该安全上下文给予这一启用 ESAS 的端点查看其自己的本地可用信息的新的方式。即，该安全上下文允许启用 ESAS 的端点组合或相关来自从各种不同源接收到的且跨对象类型的安全评估的证据以显著提高其对潜在安全事故的检测的质量。该启用 ESAS 的端点然后根据一组响应策略来作出关于对于每一种类型的安全评估（无论是从另一端点接收到的还是由该端点本身内部生成的）什么本地动作或响应是适当的决定。事故判定是高效且经济的，因为安全上下文使得能够以安全评估的形式来对企业范围信息进行分布式处理，而没有在整个企业中共享大量原始数据（其中大多数都由于缺乏任何上下文而是完全无关的）的负担。启用 ESAS 的端点还被安排成在提示本地动作的安全评估到期时（即，在该安全评估超过 TTL 字段中所指定的生存时间时）回退该本地动作。

[0010] 在一说明性示例中，被称为 ESAS 中央服务器的专用端点耦合到安全评估信道，该专用端点通过订阅所有安全评估、记录安全评估、并且还记录由各端点响应于环境中的安全事故而采取的本地动作来作为集中式审核点来执行。该 ESAS 中央服务器向管理员提供作为整体的企业以及每一个启用 ESAS 的端点的历史和当前状态的综合视图。利用安全评估使得管理员能够紧凑且高效地配置对跨整个企业检测到的事故的响应策略。安全评估用作用于定义企业范围安全响应策略的自然锚或起始点。由此启用简化且一致的管理界面来为跨整个企业的每一种类型的安全评估定义所需响应。

[0011] 本发明的 ESAS 共享安排提供了多个优点。通过采用具有简明词汇的安全评估，显著地降低了企业中的总体数据复杂性并且在各端点之间只共享有意义的信息。使用安全评估还消除了在中央存储位置收集大量原始数据的需求，并由此使得能够在非常经济的基础上构建高度可缩放的企业安全解决方案。另外，可容易地用按需可扩展性来部署新端点。安全评估可以在该新端点和现有端点之间共享而无需重新配置现有端点中的响应策略中的任一个。新端点使用现有端点已经理解的语义抽象来担当新的安全评估源即可。利用安全评估还使得能够使用非常紧凑且清楚的方法来建立企业范围安全策略，而无需理解每一个端点可在企业中生成的所有可能的安全事件并然后试图描述对于每一个事件的响应动作。

[0012] 提供本概述是为了以简化的形式介绍将在以下详细描述中进一步描述的一些概念。该概述不旨在标识所要求保护的主题的关键特征或必要特征，也不旨在用于帮助确定所要求保护的主题的范围。

[0013] 附图简述

[0014] 图 1 示出其中可实现本发明的企业安全评估共享的说明性企业安全环境；

[0015] 图 2 示出其中提供信道以使得能够在多个端点之间共享安全评估的说明性企业安全评估共享安排；

[0016] 图 3 示出作为安全评估的基础的说明性术语分层结构；

[0017] 图 4 示出两个说明性端点以及通过利用本发明的安全评估安排来实现的复杂性降低；

[0018] 图 5 示出启用对安全评估的共享的端点中所设置的功能的说明性示例；

[0019] 图 6 是第一说明性情形的图示，其中多个启用 ESAS 的端点耦合到安全评估信道并

且在一个端点处检测到的事故触发多个其他端点处的响应；

[0020] 图 7 是第二说明性情形的图示，其中触发由还执行跨对象映射的接收启用 ESAS 的端点来生成新的高保真评估的低保真安全评估通过安全评估信道来发送；

[0021] 图 8 是示出补救技术的针对性使用的第三说明性情形的图示；

[0022] 图 9 示出由使得诸如管理员等用户能够管理和定义企业中的启用 ESAS 的端点的响应策略的图形用户界面（“GUI”）提供的说明性屏幕；

[0023] 图 10 示出由被安排成补充图 9 所示的 GUI 屏幕或用作对该 GUI 屏幕的替换的 GUI 提供的说明性屏幕；以及

[0024] 图 11 示出其中本发明的 ESAS 特征集提供企业安全管理层功能的说明性企业安全安排。

[0025] 详细描述

[0026] 对现有企业安全解决方案的分析指示仍然存在解决顾客需求的大量机会。例如，每一个单独的安全产品往往具有对诸如通过恶意软件或恶意用户的动作而产生的安全事故的高假肯定和假否定检测率。出现这一低保真检测是因为来自单一类型的源的数据（即，企业范围数据的子集）一般不提供对安全事故作出准确评估所需的上下文。

[0027] 对自动动作或响应的使用由于该低保真检测而是极少见的，因为对所检测到的事故的有效性的置信度很低。另外，对检测到的事故的典型响应往往是非常粗暴的，例如，用户或机器可能从网络断开。因为这些粗暴的动作通常对企业中的商业活动施加大量成本，所以通常不执行基于低保真检测的这些动作的自动化。

[0028] 在检测到感兴趣的事故时，现有安全产品通常执行调查以确定该检测的有效性（即，事故是真还是假）以及作为响应要采取什么动作。在调查上耗费大量资源以审阅所收集的可能与所检测到的事故相关的详细数据。因为始终收集所有数据是不可行的，所以安全产品通过应用由管理员定义的策略来仅收集可用数据的子集。这些策略通常是静态的并且通常基于收集系统的存储容量并且未必按照事故数据或数据源的相关性来定义。

[0029] 在检测到事故时，对策略的应用通常导致对触发该检测的数据的审阅。当该数据被认为不足以生成高保真响应时，通常收集甚至更多的数据。例如，可监视进出被怀疑的已受损机器的所有数据通信。在许多情况下，收集大量数据但从不使用这些数据，并且这些数据具有仅作为噪声的统计重要性。因此，许多现有安全产品收集通常过多的噪声，但未收集足够的相关数据。

[0030] 供改进的另一领域是整个企业中的响应的管理和协调。现有企业安全产品固有地提供对在每一个单独的岛中检测到的事故的本地化响应。因为这些安全产品都是孤立的，所以可能的响应选项被限于企业中该特定安全产品所操作的那部分。即，动作和响应能够针对所检测到的单独事故来在一个安全产品岛中定义，但不存在描述当在企业的另一部分中或在全局的基础上应用时可能更有效的所需动作的能力。当前不存在用于启用对针对安全事故的响应策略的企业范围定义和强制实施的单个管理点。也不存在每一个岛可用于进行通信以由此通知其他岛发生了某件事情或者需要采取动作的统一响应信道和语言 / 协议。缺乏管理和协调的响应导致对于跨企业中的岛的数据的手动集成和相关招致大量成本。

[0031] 现在转向各附图，其中相同的附图标记指示相同的元素，图 1 示出了其中可部署

被称为端点的各种安全产品 105-1,2...N 的说明性企业安全环境 100。要强调的是,图 1 所示的端点 105 的数量和类型仅仅是说明性的,并且取决于企业安全评估共享的具体应用的要求,可增加或减少具体端点数量,且可利用不同类型的安全产品 / 端点。例如,除了图 1 所示且在以下描述的安全产品之外,web 应用程序保护产品、SEM/SIM(安全事件管理 / 安全事故管理) 产品、操作健康监视和配置管理产品 (例如,微软Windows®软件更新服务、微软操作管理器)、或者身份管理产品 (例如,微软现用目录) 也可在某些应用中使用。

[0032] 在企业安全环境 100 中,部署主机安全端点 105_1 以保护、评估和监视企业 100 中的多个主机计算机 108。主机安全端点 105_1 的商用示例是微软 Forefront Client Security® (前线客户机安全),其为企业的台式计算机、膝上型计算机和服务器操作系统提供统一的恶意软件保护。

[0033] 边缘防火墙 105_2 是被安排成保护企业环境 100 以免遭基于因特网的威胁同时向用户提供通过周界网络 112 的对应用程序和数据的远程访问的安全产品。边缘防火墙 105_2 可具体化为例如,微软 Internet Security and Acceleration® (因特网安全和加速,"ISA") 服务器。

[0034] NAP 安全端点 105_3 通过确保正在发生的对由管理员定义的健康策略的遵从来执行健康策略确认。通常,对于由 NAP 安全端点 105_3 监视的、不符合系统健康要求的计算机 (例如,台式计算机和漫游膝上型计算机 115) 限制访问。

[0035] NIDS 安全端点 105_4 分析内部网络 119 上的企业 100 内的通信。NIDS 安全端点 105_4 用于通过监视内部网络 119 上的网络通信来检测诸如服务拒绝攻击端口扫描等恶意活动。

[0036] 业务线安全端点 105_N 保护各个业务线应用程序 122。业务线应用程序 122 包括例如,诸如微软Exchange®等在企业 100 中使用的电子邮件应用程序。安全端点 105_N 通常监视电子邮件以提供反病毒和反垃圾邮件保护。

[0037] 企业 100 中的安全端点 105 中的每一个一般都被安排为单独的岛,如图 1 中的虚线矩形所示。因此,每一个安全端点 105 都被安排成监视企业 100 中的可用数据的子集并响应于所检测到的事故来执行本地化动作。另外,每一个端点通常都包括本地管理功能 135-1,2...N。如上所述,各单独的本地管理功能一般不集成以提供单个管理点。

[0038] 图 2 示出了说明性 ESAS 安排 200,其中提供信道 205 以使得能够使用在每一个端点处共同利用的语言 / 协议来在多个端点之间共享被称为"安全评估"的语义抽象。安全评估信道 205 方便由端点用来将安全评估源 (发布者) 连接到安全评估的消费者 (订阅者) 的发布 / 订阅模型。如图所示,安全评估信道 205 上的发布者和订阅者两者都是端点 105。

[0039] 端点 105 通过被安排成简化与安全评估信道 205 的交互的语义抽象层来与实际传输机构和发布 / 订阅模型的管理隔离开。该抽象层包括描述端点订阅的安全评估类型的表以及描述端点发布的安全评估类型的表 (如下所述,通常并非所有端点都订阅所有安全评估类型)。另外,该抽象层提供用于读取接收到的安全评估的 API(应用程序编程接口) 以及用于生成安全评估的 API。

[0040] 专用端点,即 ESAS 中央服务器 216 耦合到安全评估信道 205,并且作为对于 ESAS 安排 200 的集中式审核点来执行。因此,ESAS 中央服务器 216 订阅所有安全评估并且永久地记录这些安全评估。ESAS 中央服务器 216 还接收并记录来自端点的、指示端点所采取的本地动作的消息。该 ESAS 中央服务器 216 由此向管理员提供安全评估监视功能,该功能给

出了作为整体的企业以及每一个启用 ESAS 的端点的历史和当前状态的综合视图。

[0041] 图 3 示出了作为安全评估的基础的说明性术语分层结构 300。安全评估被定义为安全含义或类别向信息的试验性指派。如此处所使用的信息被定义为具有某些上下文的数据。数据被定义为缺少上下文的离散项目。这些定义可通过示例来进一步描述。如图 3 所示，数据片段 305 是事件日志中诸如失败的登录等事件。信息 310 是具备上下文的数据，该上下文在该示例中是该失败的登录是在同一机器，即命名为膝上型计算机 2 的膝上型计算机上的 10 分钟之内的第六次这样的失败。在该示例中，安全评估 316 指示膝上型计算机 2 以特定方式进行分类，即，该膝上型计算机被评估为具有类别“已受损”、高“严重性”，并且其中这一评估具有低“保真度”（这些术语将在以下更详细地定义和讨论）。

[0042] 可对企业安全环境中诸如用户或设备等任何感兴趣的对象执行安全评估。在该说明性示例中，评估包括四种主要对象类型 :1) 主机 - 关于企业中的计算机的评估 ;2) 用户 - 关于企业中的用户或账户的评估 ;3) 服务 - 关于诸如具有恶意名声的网站的 URL（统一资源定位符）等提供给企业的服务的评估 ;4) 企业 - 关于作为整体的企业或者该企业的诸如部门、子网、站点或分支等明确定义的子集的评估 ;以及 5) 数据 - 关于存在于企业中的或由企业中的对象来访问的业务相关数据（例如，在文档中发现的业务数据、电子邮件、数据库中的业务数据等）的评估。

[0043] 要强调的是，这些对象类型仅仅是说明性的，并且可按特定情形所需使用其他对象类型。在企业安全评估共享的大多数应用中，端点只发布和订阅所有可用安全评估类型的子集，因为特定端点一般将会对企业环境中的特定对象感兴趣。另外，虽然某些端点将会既是发布者又是订阅者，但并不要求每一个端点支持这两个功能。出于这些原因，此处所使用的发布 / 订阅模型被称为是松耦合的。

[0044] 以下的表 1 示出了一组说明性评估类别及其到特定对象类型的映射，该组评估类别可被包含在典型的安全评估中 :

[0045]

对象类型	评估类别	描述
主机	易受攻击的机器	机器具有易受攻击的配置或者遗漏了某些补丁。
	已受损机器	端点检测到机器可能受到恶意软件 / 用户的损害的某些证据。
	正被攻击的机器	检测到攻击尝试但没有成功的证据
	感兴趣的机器	端点对机器有一般怀疑但不具有指出什么出错的能力
用户	已受损用户	端点检测到用户 / 账户可能已受损的某些证据。

	正被攻击的用户	检测到攻击尝试但没有成功的证据
	恶意用户	端点或管理员检测到用户是恶意用户并主动（即，故意）执行非法动作。
	感兴趣的用户	端点对用户／账户有一般怀疑但不具有指出什么出错的能力。
企业	正被攻击的企业	端点检测到企业正被攻击但没有企业的有效部分已受损的证据。
	已受损企业	端点检测到企业的有效部分已受损（机器／用户）。
服务（例如，网站）	恶意	URL（统一资源定位符）具有恶意名声。
数据	已受损	端点检测到企业中的某些业务相关数据已受损的某些证据。
	被破坏	端点检测到企业中的某些业务相关数据已被破坏的某些证据。

[0046] 表 1

[0047] 在本发明的说明性 ESAS 安排中，通常利用四个严重性等级：低、中、高和关键。通常利用三个保真度等级：低、中和高。注意，对于严重性和保真度两者的等级数可被安排成取决于评估类别而不同。例如，对于评估类别“易受攻击的机器”可能使用三个严重性等级，而对于评估类别“已受损机器”使用四个严重性等级。该对要利用的等级数的特定选择将取决于本发明的企业安全评估共享的具体应用的要求。

[0048] 安全评估使用在作出该评估时可用的信息并且依赖于驻留在产生该评估的端点中的特定安全专家经验和知识。安全评估是试验性的，因为对任何特定事件的置信度永远不会是绝对的，并且还因为评估由于其依赖于在产生该评估时存在的信息而在本质上是临时的。在将来某一时刻，其他信息将会是可用的，因此安全评估可能变化。

[0049] 安全评估的试验性特性反映在每一个评估中所包括的两个字段，即保真度和生存时间（“TTL”）中。保真度字段为端点提供表达其对较宽泛的上下文含义向正在分析的信息的指派的置信度水平。TTL 字段使得端点能够反映对安全评估预期有效的时间段的最佳估计。或另选地，TTL 字段提供对将来的安全评估更新的最佳估计。当 TTL 到期时，基于所订阅的安全评估来采取动作的端点预期在该评估的 TTL 到期时回退这些动作。由此，该 TTL 提供安全阀功能，该功能用于防止用户或机器由于假肯定或在企业中的某处丢失消息而不恰当地受制于受限访问。然而，如果这一受限访问的确是适当的，则或者可生成新的安全评

估以继续该限制，或者延长 TTL。

[0050] 安全评估被设计成启用使用紧凑词汇的精确语义（即，由安全评估中所使用的类别赋予的含义）。如图 4 所示，企业中的端点 105 中的两个记录关于其各自感兴趣的领域内所发生的事件的数据。主机事件日志 405 和防火墙事件日志 412 由此包含大量数据。通常，这些数据在各自端点中使用相关规则 420 和 425 来处理以标识感兴趣的事件。通常众多的相关规则定义本地化的发起者或响应于所检测到的事件而采取的动作。

[0051] 通过比较，附图标记 432 所指示的安全评估只包含相对较少的数据。由于安全评估用于将宽泛的上下文指派给信息，因此它们提供对于以下问题的答案：谁创建了评估？何时？为什么？持续多久？以及，对哪一个对象应用评估？由此，为了利用安全评估，端点只需理解相比于由于应用相关规则而产生的无数信息消息的极少数感兴趣的评估类型。因此，由每一个端点收集的数据的复杂性通过将信息映射到一个或多个评估类型来降低。使用安全评估由此使得能够向订阅端点提供相关信息而无需跨企业共享大量数据或信息。

[0052] 以下的表 2 提供了可被包括在典型的安全评估中的一组说明性字段。

[0053]

字段	描述
事故 ID	表示为其创建安全评估的事故的唯一标识符。因为可能存在绑定到同一事故（例如，检测、响应、批准、取消）的若干评估，所以该字段还使用相关值
实例 ID	表示单个安全评估消息的唯一标识符
源	端点类型（例如，主机安全性、边缘防火墙、NAP、NIDS 等）和唯一端点 ID
关于	如果评估是响应于其他安全评估而创建的，则该字段将包含所有评估的事故 ID 的列表
对象类型	主机、用户、名声、企业或其他对象类型
对象 ID	对象的标识符。端点通常以不同的方式来描述相同的对象。例如，主机可由其 FQDN（完全合格域名）、IP（网际协议）、MAC（媒体访问地址）或 SMTP（简单邮件传输协议）地址等来标识
类别	已受损、易受攻击、正被攻击等
操作	已发布（检测到后）、响应、批准、取消等
严重性	事故的严重性
保真度	端点对其事故检测的置信度

创建时间	GMT（格林威治标准时间）和本地时间
TTL	以分钟计的生存时间
描述	解释为何创建评估的人类可读格式
数据	关于为何创建评估的私人信息。其他端点可使用该数据来获取附加相关
响应	（可任选）包含由端点采取的一组响应的复合节点
由	（可任选的）在用户批准 / 取消 / 创建评估的情况下，该字段将包含该用户的名称
版本	评估的模式版本

[0054] 通过使用表 2 中的字段，安全评估能够表达以下事件：

[0055] 1. 检测。端点执行某一分析以推断已发生某一异常行为（已受损机器、易受攻击的机器、已受损的用户等）；

[0056] 2. 响应。端点由于安全评估而采取动作。端点应通知系统（具体而言，图 2 中的 ESAS 中央服务器 216）何时采取动作。响应可包括例如，阻塞通信、触发扫描、重置密码、收集关于机器的更多数据以及类似动作。注意，诸如重置密码或触发扫描等某些响应是间歇性的，而其他响应是持续性的并且需要被回退以便被取消；

[0057] 3. 评估批准。管理员可使用到 ESAS 中央服务器 216 的接口来手动批准评估。应在这一批准之后通知各端点以使得这些端点将执行“必需的手动批准”响应；

[0058] 4. 取消。管理员或端点可取消现有安全评估；

[0059] 5. 响应回退。端点通知系统（图 2 中的 ESAS 中央服务器 216）该端点已回退由于特定评估而采取的所有响应 / 动作；

[0060] 6. 诸如连接验证器、等待时间检查和错误信息等健康信息评估；

[0061] 7. 对调查数据的请求。这是从一端点到另一端点的、发送其在给定时间段内收集的关于对象的所有数据的请求；以及

[0062] 8. 对调查数据的请求完成。这是供端点确认它已执行请求的方法。对请求的响应在存储 / 发送数据后发送。

[0063] 在企业安全评估共享的该说明性示例中，每一个端点都被安排成执行下述任务中的至少某一些。在某些安排中，每一个端点都用通过使用分立 ESAS 代理来执行这些任务所需的附加功能来增强。或者，该增强功能可更紧密地集成到由端点提供的核心功能中，并且单独或分立的代理可不必被包含在该端点中。这些任务包括：

[0064] 1. 基于关于所监视的系统的本地可用信息和安全上下文来生成新安全评估；

[0065] 2. 订阅来自其他端点的可用安全评估的子集；

[0066] 3. 处理传入安全评估以由此影响安全上下文。该处理可导致生成新安全评估；

[0067] 4. 根据响应策略来采取本地动作；

[0068] 5. 在导致本地动作的评估到期（即，相关联的 TTL 到期）时回退（自恢复）该本地动作。

[0069] 图 5 示出了设置在端点中的 ESAS 代理 505 的说明性示例，该端点通过安全评估信道 205 来订阅来自其他端点 105-1，2...N（图 1）的可用评估的子集。如上所述，由 ESAS 代理 505 提供的功能可另选地直接与端点的核心功能集成。

[0070] 多个安全评估 506 对于安全评估类型（即，主机、用户、名声和企业）中的每一个都是可用的。如附图标记 511 所示，在该说明性示例中，ESAS 代理 505 订阅对象类型为“主机”且评估类别为“易受攻击”的安全评估。要强调的是，感兴趣的对象类型和评估类别的特定组合对于不同的端点可以是不同的。同样，通过使用松耦合发布 / 订阅模型，并不要求每一个端点都订阅每一个安全评估。

[0071] 在过程框 514，端点使用可具有某种相关性的相关规则 522 和本地可用数据 527 来处理接收到的安全评估。这一评估过程的输出包括生成新评估 530 和 / 或调用本地动作 535。如上所述，这一本地动作在接收到的评估根据其中所包含的 TTL 字段而到期时经受回退 541（即，自恢复）。

[0072] ESAS 代理 505 根据以下规则来解释安全评估：

[0073] 1. 在生成关于特定对象的安全评估时，端点可将以下各项的任何组合考虑在内：

[0074] a) 关于该对象或该端点监视的任何其他对象的所有本地可用信息；

[0075] b) 该端点接收到的所有当前活动的安全评估（即，具有未到期 TTL 的安全评估）；

[0076] c) 该端点过去所采取的所有本地动作。

[0077] 2. 本发明的企业安全评估共享安排中的所有端点都遵循端点中的所有本地可用信息集都是互斥的原理。即，本发明的安排具有至多一个处理特定本地信息片段的端点。

[0078] 3. 安全评估通常被解释为关于对象的当前和将来安全状态的端点评估。

[0079] 重要的是注意，如上文所定义的信息和数据这两个术语，规则 2 指的是信息而不是数据的排他性。两个端点在它们从数据中提取的并在稍后用于生成评估的信息是排他的情况下可处理相同或重叠的数据源。

[0080] 为了示出规则 3 的暗示，考虑其中机器的排定的反病毒扫描检测到并移除已知恶意软件片段的以下示例。基于该检测，其他本地可用信息、接收到的当前活动评估以及端点的关于当前安全事故的嵌入知识，端点可得出以下结论中的一个：1) 机器在过去受到过感染，但现在是清洁的并且未造成任何其他将来安全风险；2) 该机器已被感染，并且虽然特定恶意软件已被移除，但它仍然可能或很可能造成安全风险。根据规则 3，端点应在后一种情况下生成关于该机器的安全评估但不应在前一种情况下生成安全评估。

[0081] 图 6 是第一说明性情形的图示，其中多个启用 ESAS 的端点耦合到安全评估信道 205，并且在一个端点处检测到的事故触发多个其他端点处的响应。该说明性情形分三个阶段描述。如附图标记 610 所指示的，边缘防火墙 105_2 首先标识可能已受损的客户机，例如这是因为该客户机创建太多的到周界网络 112（图 1）的连接以使得对于该行为的最有可能的解释是安全性损害的存在。其次，如附图标记 620 所指示的，该边缘防火墙 105_2 通过安全信道 205 来将具有高严重性和高保真度的、指示特定客户机“已受损”的安全评估发送到订阅端点。

[0082] 再次，接收该安全评估的订阅端点 105-1，3...N 和 ESAS 中央服务器 216 通过应用

其自己的相关规则和本地可用数据来应用其特定安全专家经验以触发适当的动作。如图 6 中的附图标记 630 所共同指示的，主机安全端点 105_1 执行按需扫描。NAP 端点 105_3 撤消所标识的已受损客户机的 IP 安全证书并实现端口关闭。业务线安全端点 105_N 基于所接收到的安全评估来临时挂起到该已受损客户机的即时消息传递（“IM”）通信。ESAS 中央服务器 216 引发对安全分析员（例如，管理员）的警告并且还记录所有安全评估和所调用的动作。

[0083] 上述第一说明性情形提供其中检测到嫌疑事故的端点生成具有高严重性和高保真度的安全评估（即，该端点对其有效地检测到严重事故具有高置信度）的情况。通过比较，图 7 是第二说明性情形的图示，其中触发由还执行跨对象映射的接收端点来生成新的高保真评估的低保真安全评估通过安全评估信道 205 来发送。

[0084] 该第二说明性情形也分三个阶段描述。如附图标记 710 所指示的，边缘防火墙 105_2 首先检测到到周界网络 112（图 1）的大量客户机连接。然而，与图 6 所示且在所附文本中描述的第一说明性情形不同，客户机所建立的连接数量不是太多从而导致该边缘防火墙 105_2 无法绝对肯定该客户机已受损。在现有企业安全系统中，当端点看见这一数据时，它通常仅丢弃该数据并且不采取动作，因为没有足够的证据来保证诸如断开机器等典型的粗暴响应。通过比较，在当前情形中，在第二阶段中边缘防火墙 105_2 通过安全评估信道 205 来发送具有中严重性和低保真度的、指示该特定客户机已受损的安全评估 715，如附图标记 720 所指示的。

[0085] 在此，对于由边缘防火墙 105_2 生成的安全评估 715 中所引用的特定对象的订阅端点包括主机安全端点 105_1 和 ESAS 中央服务器 216。虽然这一低保真数据在现有安全产品中一般不触发将要在端点处采取的动作，但根据本发明的企业安全评估共享，主机安全端点 105_1 鉴于从边缘防火墙 105_2 接收到的安全评估来不同地考虑其自己的本地数据。在这种情况下，使用由主机安全端点 105_1 处的按需扫描产生的本地数据和来自边缘防火墙 105_2 的安全评估中所包含的信息来生成新的评估 725 和 728。由此，主机安全端点 105_1 具有这样的信息：该信息本身不保证生成新安全评估，但如在这种情况下一样，在用来自另一端点的甚至低保真评估来加强时，有足够的证据证明创建各自具有高保真度的新安全评估 725 和 728 是正确的。

[0086] 主机安全端点 105_1 将该新安全评估 725 和 728 置于安全评估信道 205 上。该新安全评估 725 和 728 由订阅端点通过安全评估信道 205 来接收，该订阅端点在该说明性情形中包括对于安全评估 725 的边缘防火墙 105_2 以及对于安全评估 728 的业务线端点 105_N。

[0087] 注意，业务线端点 105_N 并不是由边缘防火墙 105_2 产生的原始安全评估 715 的订阅者，因为引用对象类型是机器并且业务线端点 105_N 由于其保护电子邮件的角色而通常关心用户。然而，在该第二说明性情形中，主机安全端点 105_1 在其生成新安全评估 728 时从主机对象类型映射到用户对象类型。这一跨对象映射能力在许多情况下都可能是有益的，如可以构想，诸如恶意软件或恶意活动等可能损害主机计算机的数据秘密性或完整性的高严重性事故也可能损害用户。可生成将高严重性事故从主机对象类型跨对象地映射到具有特定保真度的用户对象类型的安全评估。类似地，在其中恶意软件或恶意活动实际上已经导致主机计算机上的数据完整性丢失的关键严重性事故的情况下，可生成具有甚至更高保真度的对于用户对象类型的安全评估。

[0088] 在阶段三，新安全评估 725 和 728 触发接收端点处的各种相应动作，如由附图标记 730 所共同指示的。具体而言，边缘防火墙 105_2 阻塞除了软件更新和 / 或关键任务访问之外的已受损客户机的所有访问。业务线端点 105_N 临时挂起传出电子邮件。并且，如同第一说明性情形，ESAS 中央服务器 216 继续记录所有评估和动作。如上所述，这些限制仅在与新安全评估 725 和 728 相关联的 TTL 保持有效的时间段期间强制实施。当这些新安全评估到期时，回退各自端点所采取的动作，除非延长 TTL 或者接收到调用限制动作的新安全评估。

[0089] 图 8 是示出补救技术的针对性使用的第三说明性情形的图示。该第三说明性情形分三个阶段描述。如附图标记 810 所指示的，边缘防火墙 105_2 首先检测到到周界网络 112（图 1）的大量客户机连接。其次，如附图标记 820 所指示的，该边缘防火墙 105_2 通过安全信道 205 来将具有高严重性和高保真度的、指示特定客户机“已受损”的安全评估 815 发送到订阅端点。该订阅端点包括主机安全端点 105_1、NAP 端点 105_3 和 ESAS 中央服务器 216。

[0090] 主机安全端点 105_1 审阅所接收到的安全评估并使用相关规则和任何相关的本地可用数据来应用其特定安全专家经验。在该说明性示例中，主机安全端点 105_1 作为响应生成新安全评估 825，其包含业务线安全端点 105_N 所订阅的用户对象类型。

[0091] 在该情形的第三阶段中，各端点所采用的补救技术在其对企业 100（图 1）中的业务操作的潜在影响方面被认为是昂贵的。例如，如附图标记 830 所指示的，业务线安全端点 105_N 实现需要临时挂起传出电子邮件的响应策略。另外，主机安全端点 105_1 执行按需扫描并且如果未得到结果，则执行深度扫描。虽然这些补救技术在解决恶意软件、恶意用户和其他问题时可能是非常有效的，但这些技术通常给企业造成了巨大的花费。例如，传出电子邮件被挂起的用户将会是较不多产的，并且深度扫描通常需要会将机器从服务中移除一段时间的一次或多次重启。

[0092] 本发明的 ESAS 安全有利地使得能够以有针对性的方式，而不是仅仅以对于某些机器和 / 或用户可能未被证明是正确的通用方式或全盘应用这些虽然昂贵但有效的补救技术。该环境中只有使用预定义准则来被认为是有嫌疑的对象才将经受这些特定补救技术。

[0093] 图 9 示出了由使得诸如管理员等用户能够管理和定义企业 100（图 1）中的端点的响应策略的图形用户界面（“GUI”）提供的说明性屏幕 900。在某些应用中，该 GUI 被主存在 ESAS 中央服务器 216（图 2）上。有利的是，具体化为安全评估的语义抽象层使得能够使用非常紧凑且清楚的方法来建立企业范围安全策略。即，响应策略可通过将安全评估用作定义的起始点，而不关心企业中的哪一个端点创建了该安全评估或者该端点如何得出该安全评估中所反映的结论来配置。安全评估与其紧凑分类由此用作对于企业范围安全响应策略的自然锚。在没有本发明的 ESAS 安排来简化响应策略的配置的情况下，用户将需要考虑每一个端点可能生成的每一个事件和 / 或警告，并且然后定义对每一个这样的事件做什么。

[0094] 屏幕 900 是使用对应于多个不同端点的字段 903-1，2...N 来示出企业范围响应策略的配置的说明性示例，该配置针对如附图标记 906 所指示的、定义对于该响应策略配置的起始点（即，“锚”点）的具有关键严重性的评估类别已受损机器的情况。要强调的是，对于其他评估类别、对象类型、严重性等级等将利用其他用户界面屏幕以使得允许用户为多个不同起始点定义可能在特定企业安全环境中使用的响应策略。在该特定示例中，响应策

略取决于所设置的严重性等级为“关键”的特定安全评估的保真度来设置。字段 903 包括多个相应的子字段，这些子字段被安排成使用例如典型的 GUI 中所采用的文本输入框、下拉菜单等来反映用户定义的输入。

[0095] 如子字段 910 所指示的，对于具有关键严重性的指示已受损机器的安全评估，边缘防火墙 105_2（图 1）被配置成在安全评估具有低保真度时增加审核量（即，移至与普通审核级别相比增加所收集的数据量的深度审核级别）。子字段 913 示出对于具有中保真度的评估，边缘防火墙 105_2 提高审核级别并且还将对所怀疑的已受损机器的因特网访问仅限于通常包括已知不是恶意的站点的“白名单”URL。在保真度为高时，如子字段 916 所示，完全阻塞对因特网的访问。

[0096] 字段 903_2 示出对应于主机安全端点 105_1（图 1）的响应策略配置。对于具有低保真度并且指示已受损机器且严重性为关键的安全评估，主机安全端点 105_1 将审核量增加至深度审核级别，如子字段 920 所指示的。子字段 923 指示对于中和高保真度的情况，主机安全端点 105_1 增加其审核，并且还增加执行对其主机的深度扫描（其中“深度”扫描可能需要计算机重启一次或多次）。

[0097] 字段 903_N 示出对应于业务线安全端点 105_N（图 1）的响应策略配置。对于具有低保真度并且指示已受损机器且严重性为关键的安全评估，业务线安全端点 105_N 将审核量增加至深度审核级别，如子字段 926 所指示的。子字段 932 指示对于具有中保真度的安全评估，业务线安全端点 105_N 将其数据收集增加至深度审核，并且还限制对于电子邮件的文件附件。子字段 935 指示对于具有高保真度的安全评估，业务线安全端点 105_N 阻塞所有即时消息传递（“IM”）通信。

[0098] 字段 941 示出对应于图 2 中的 ESAS 中央服务器 216 的响应策略配置。对于具有高保真度的安全评估，如子字段 943 所指示的，ESAS 中央服务器 216 执行对于受影响的机器的端口关闭并生成相关联的用户账户已被挂起的警告。如同以上所讨论的子字段，子字段 943 通常被安排成接受用户定义的输入。

[0099] 图 10 示出了由使得诸如管理员等用户能够管理和定义企业 100（图 1）中的端点的响应策略的 GUI 提供的说明性屏幕 1000。该屏幕和 GUI 可用于补充图 9 所示并且在所附文本中描述的安排，或者可用作替换安排。屏幕 1000 提供对应于各种保真度等级和所有严重性等级的评估类别“已受损机器”的响应策略配置的单个视图。在该说明性示例中，具有任意严重性等级的评估类别为“已受损”的安全评估类型 1006 用作对于所示响应策略配置的锚。要强调的是，可构想用于与其他对象类型和评估类别一起使用的类似屏幕。如同图 9 所示且在所附文本中描述的安排，图 10 所示的安排提供了用于整个企业中的端点的响应策略的非常紧凑的管理界面。

[0100] 图 11 示出了说明性企业安全安排 1100，其中本发明的 ESAS 特征集，包括安全评估共享、ESAS 中央服务器的安全评估监视（如图 2 所附文本中所描述的）以及用于企业范围响应策略配置的紧凑分类（如图 9 和 10 所附文本中所描述的，用作企业安全管理层 1105。即，附图标记 1108 所指示的 ESAS 特征集在企业环境中的所有端点之间共享，并且不限于作为单个企业安全产品岛的一部分。由通过安全评估信道 205（图 2）来共享的安全评估形成的语义抽象层使得能够利用单个且一致的管理界面以由此创建针对企业安全的更集成的方法。

[0101] 尽管用对结构特征和/或方法动作专用的语言描述了本主题，但可以理解，所附权利要求书中定义的主题不必限于上述具体特征或动作。相反，上述具体特征和动作是作为实现权利要求的示例形式公开的。

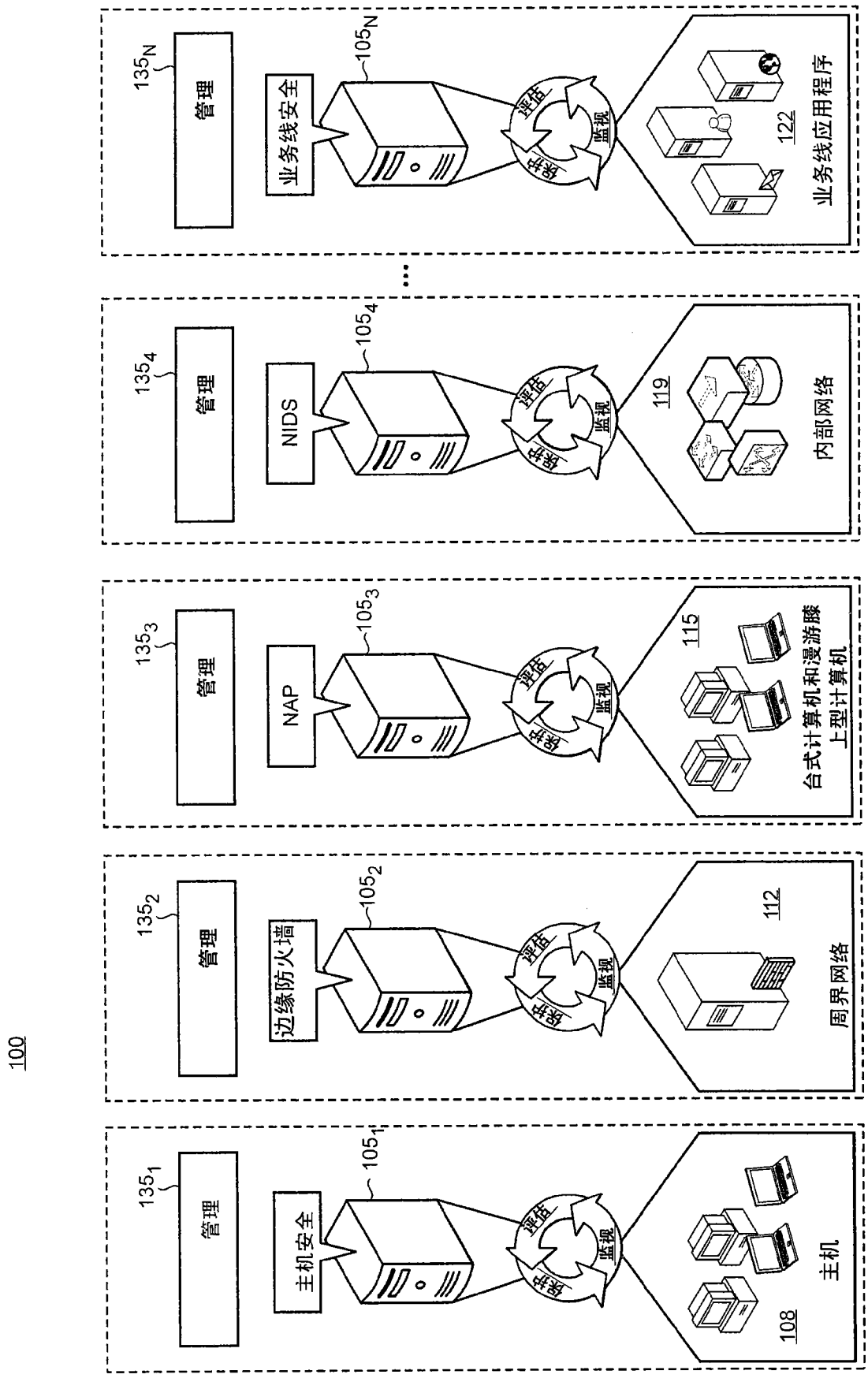

100
135N
管理
业务线安全
105N
评估
监视
122
业务线应用程序
135₄
管理
NIDS
105₄
119
内部网络
135₃
管理
NAP
105₃
115
台式计算机和漫游膝上型计算机
135₂
管理
边缘防火墙
105₂
112
周界网络
135₁
管理
主机安全
105₁
108
主机

图 1

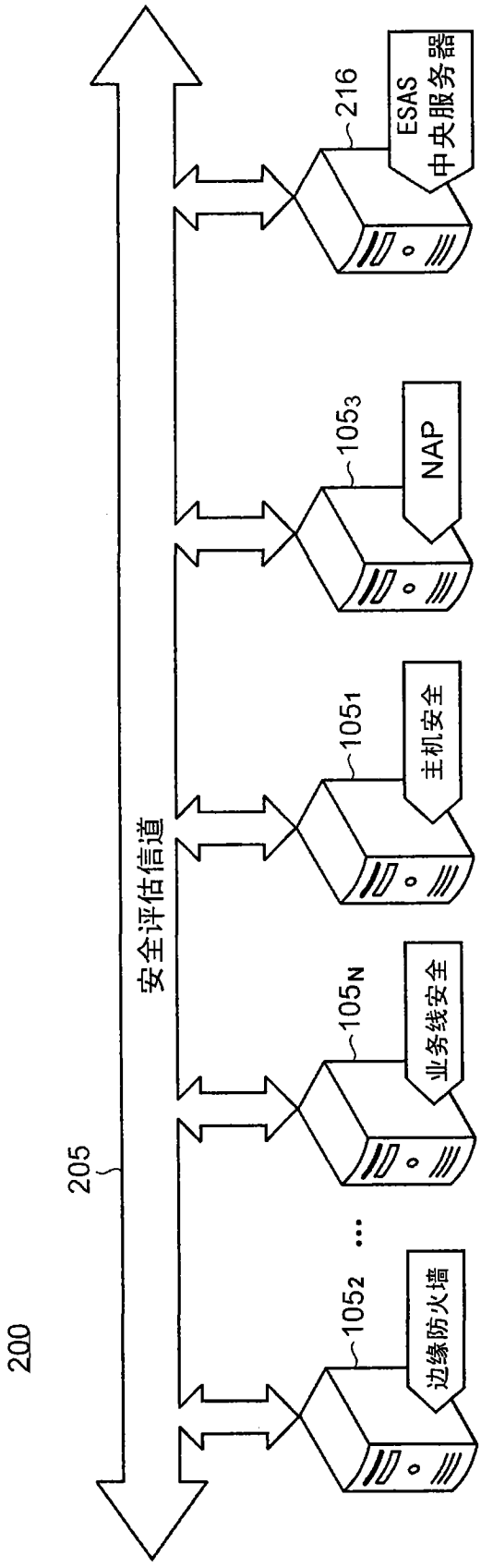

200
205
安全评估信道
1052
边缘防火墙
...
105N
业务线安全
1051
主机安全
1053
NAP
216
ESAS
中央服务器

图 2

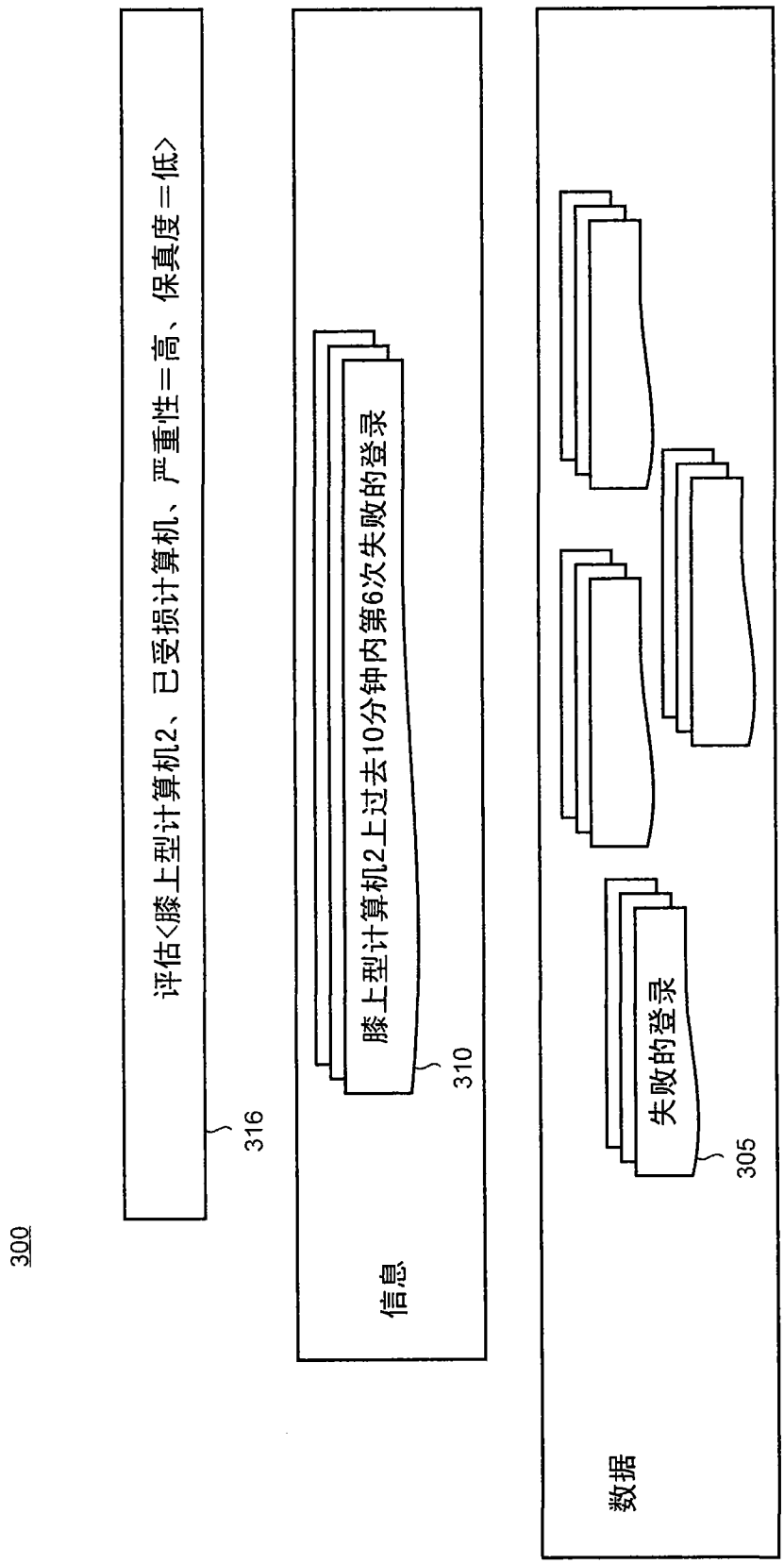

300
评估<膝上型计算机2、已受损计算机、严重性=高、保真度=低>
316
膝上型计算机2上过去10分钟内第6次失败的登录
310
信息
失败的登录
305
数据

图 3

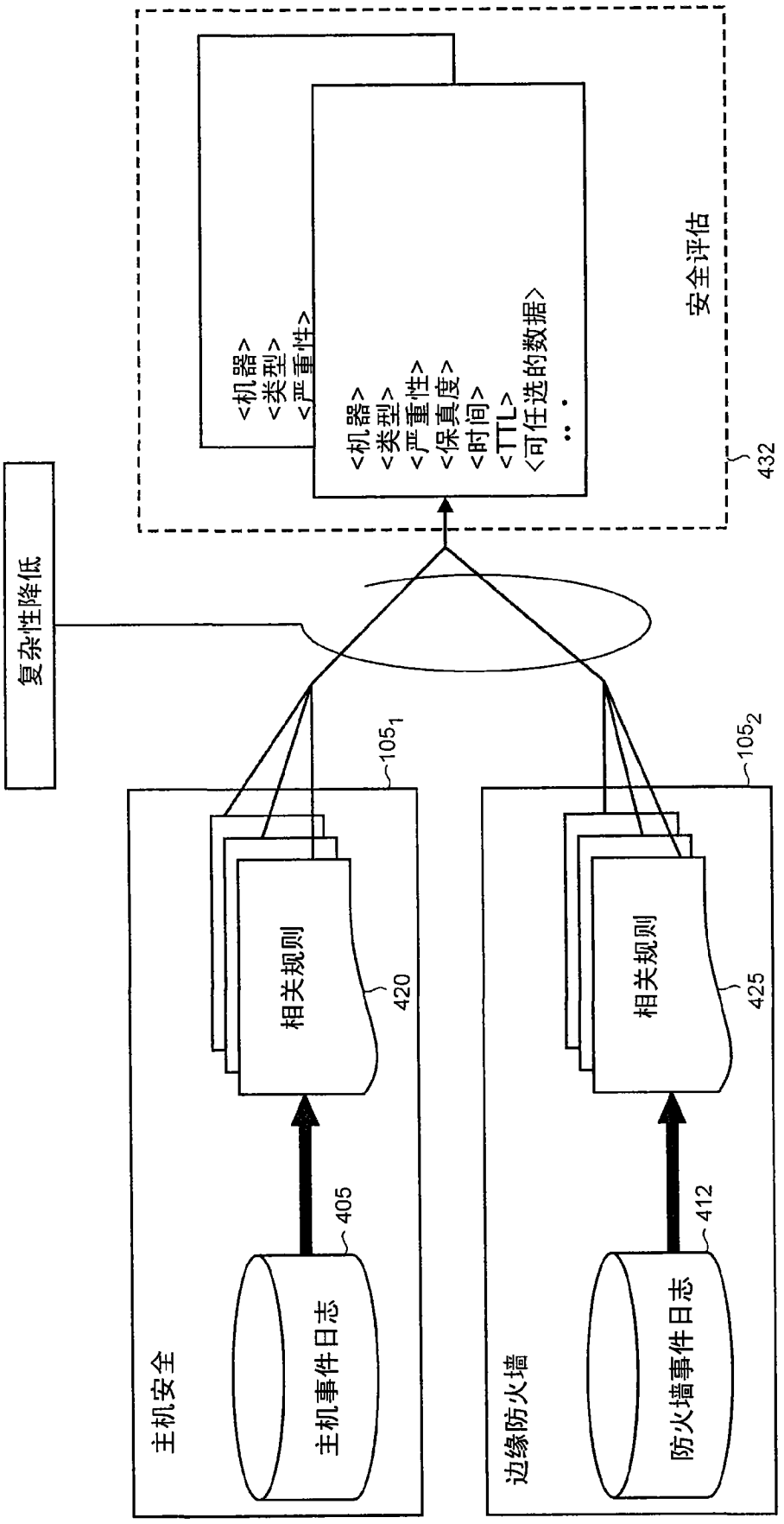

安全评估
<机器>
<类型>
<严重性>
<机器>
<类型>
<严重性>
<保真度>
<时间>
<TTL>
<可任选的数据>
...
432
复杂性降低
105_1
105_2
相关规则
420
相关规则
425
主机安全
主机事件日志
405
边缘防火墙
防火墙事件日志
412

图 4

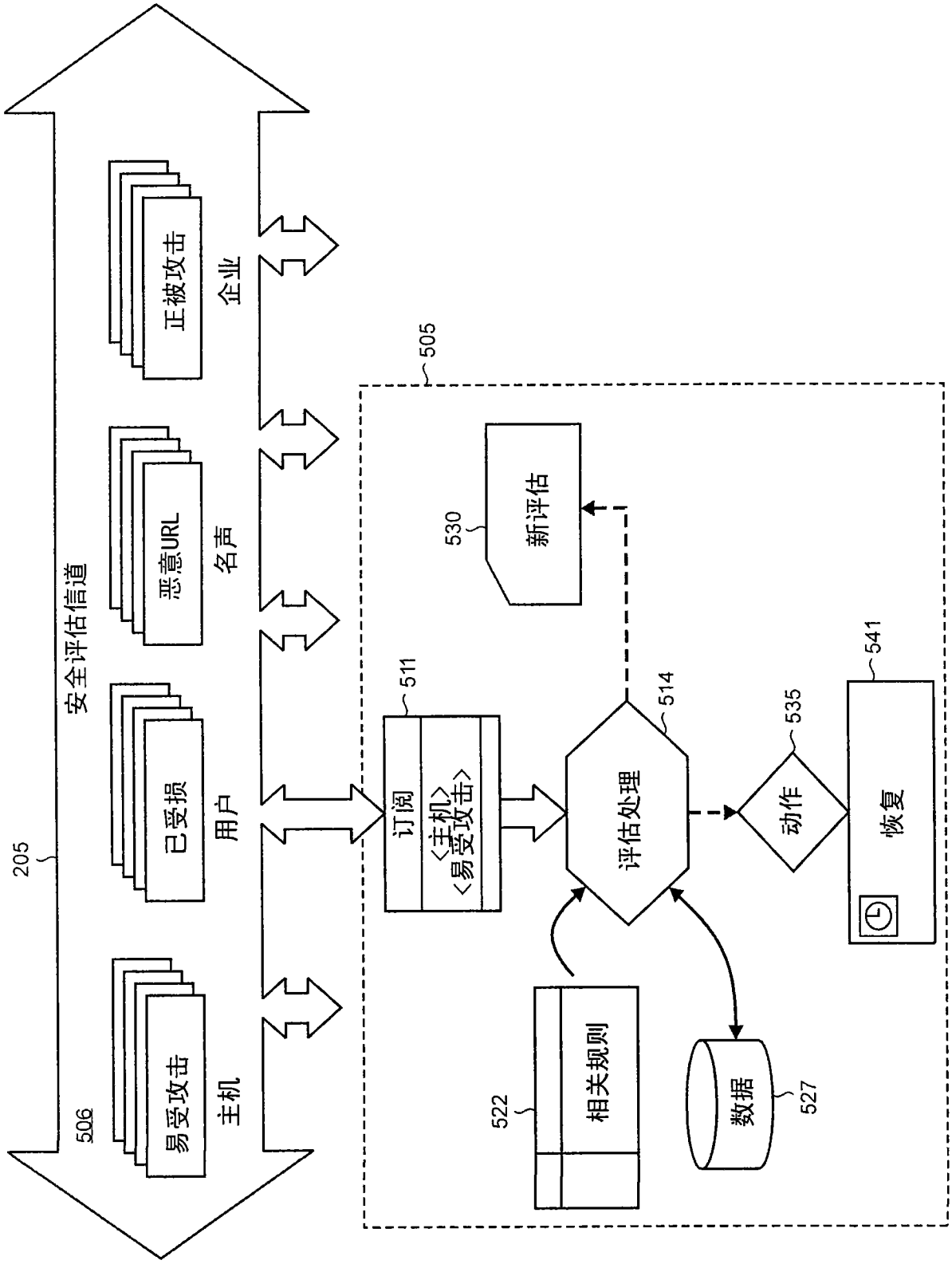

安全评估信道
205
506
易受攻击
主机
已受损
用户
恶意URL
名声
正被攻击
企业
505
530
新评估
511
订阅
〈主机〉
〈易受攻击〉
514
评估处理
535
动作
541
恢复
522
相关规则
数据
527

图 5

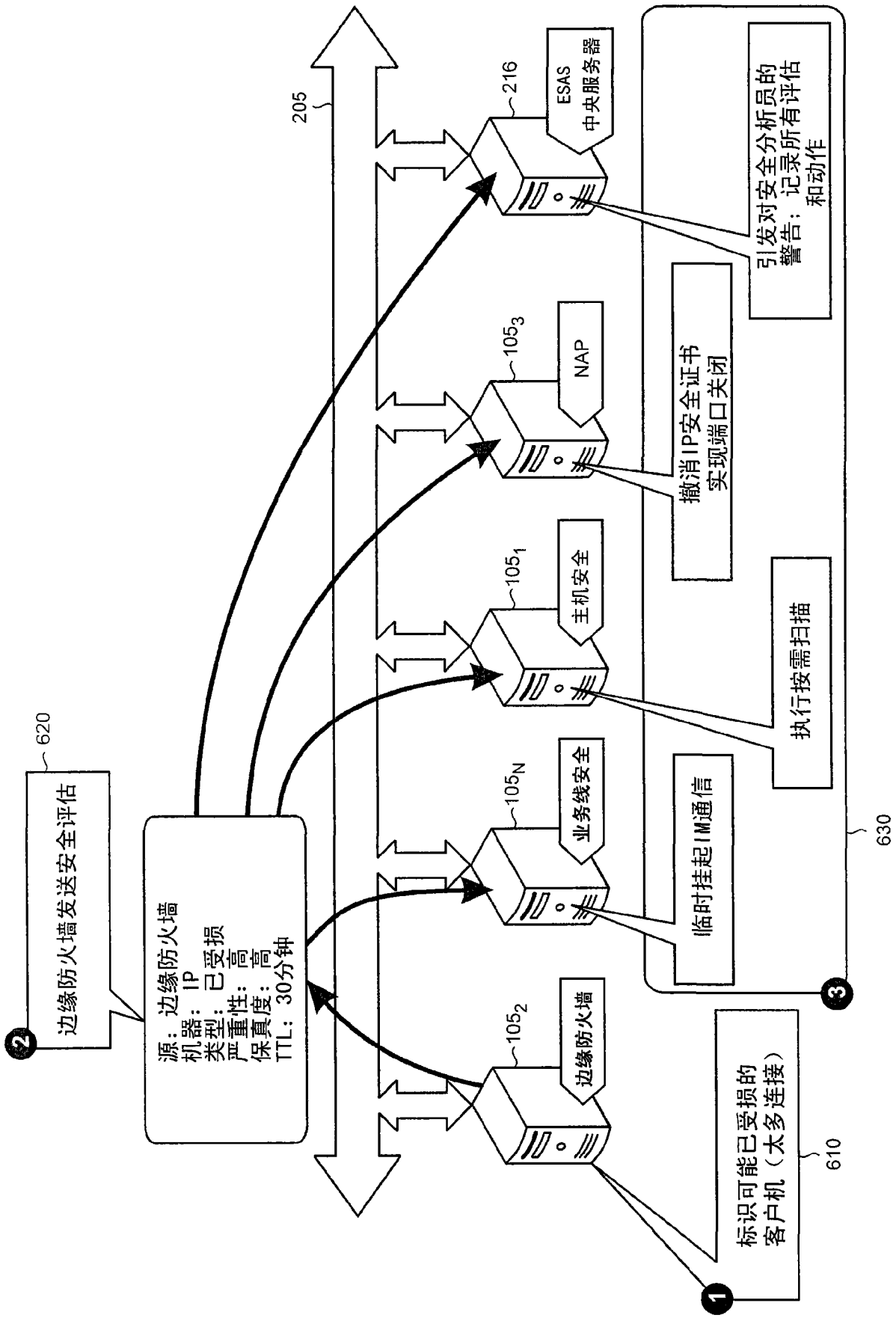

620
边缘防火墙发送安全评估
源：边缘防火墙
机器： IP
类型： 已受损
严重性： 高
保真度： 高
TTL： 30分钟
205
216
ESAS
中央服务器
105_3
NAP
105_1
主机安全
105_N
业务线安全
105_2
边缘防火墙
撤消IP安全证书
实现端口关闭
引发对安全分析员的
警告；记录所有评估
和动作
执行按需扫描
临时挂起IM通信
630
标识可能已受损的
客户机（太多连接）
610
1
2
3

图 6

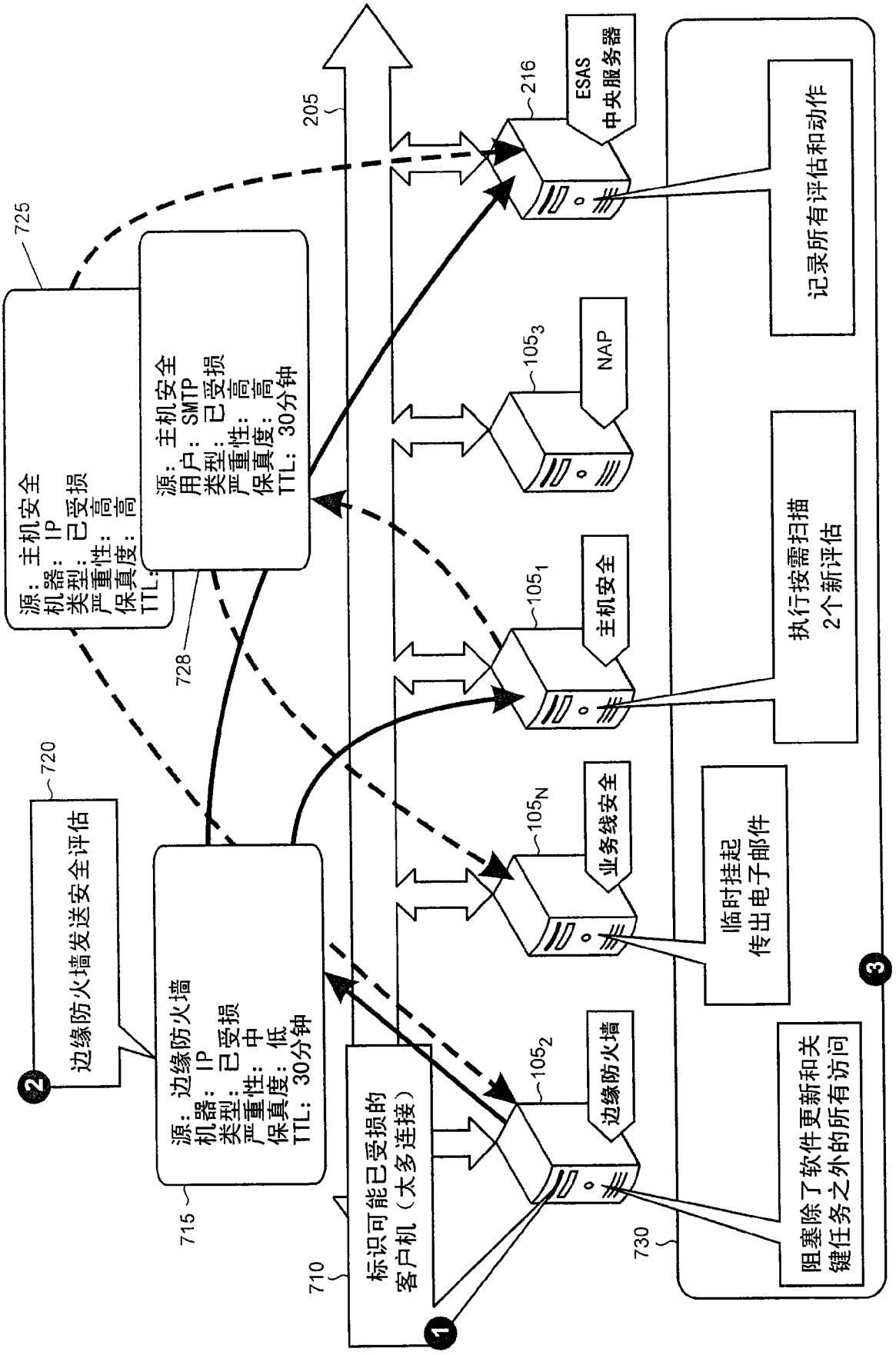

ESAS
中央服务器
216
205
725
源：主机安全
机器：IP
类型：已受损
严重性：高
保真度：高
TTL：
源：主机安全
用户：SMTP
类型：已受损
严重性：高
保真度：高
TTL：30分钟
728
NAP
105_3
主机安全
105_1
业务线安全
105_N
边缘防火墙
105_2
记录所有评估和动作
执行按需扫描
2个新评估
临时挂起
传出电子邮件
阻塞除了软件更新和关
键任务之外的所有访问
730
720
边缘防火墙发送安全评估
源：边缘防火墙
机器：IP
类型：已受损
严重性：中
保真度：低
TTL：30分钟
715
710
标识可能已受损的
客户机（太多连接）
1
2
3

图 7

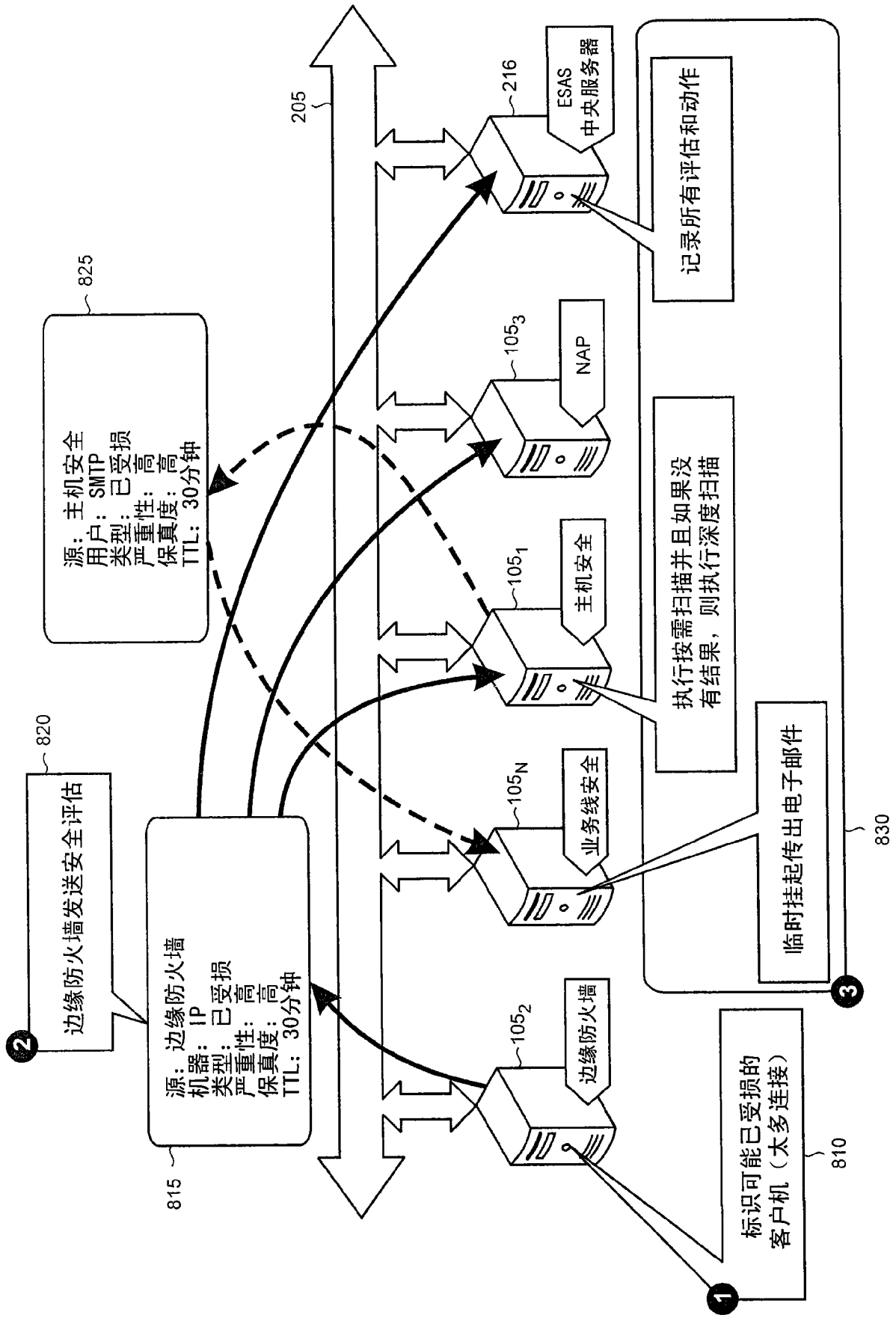

205
216
ESAS
中央服务器
825
源：主机安全
用户：SMTP
类型：已受损
严重性：高
保真度：高
TTL：30分钟
105_3
NAP
105_1
主机安全
105_N
业务线安全
105_2
边缘防火墙
820
边缘防火墙发送安全评估
源：边缘防火墙
机器：IP
类型：已受损
严重性：高
保真度：高
TTL：30分钟
815
记录所有评估和动作
执行按需扫描并且如果没
有结果，则执行深度扫描
临时挂起传出电子邮件
830
标识可能已受损的
客户机（太多连接）
810
1
2
3

图 8

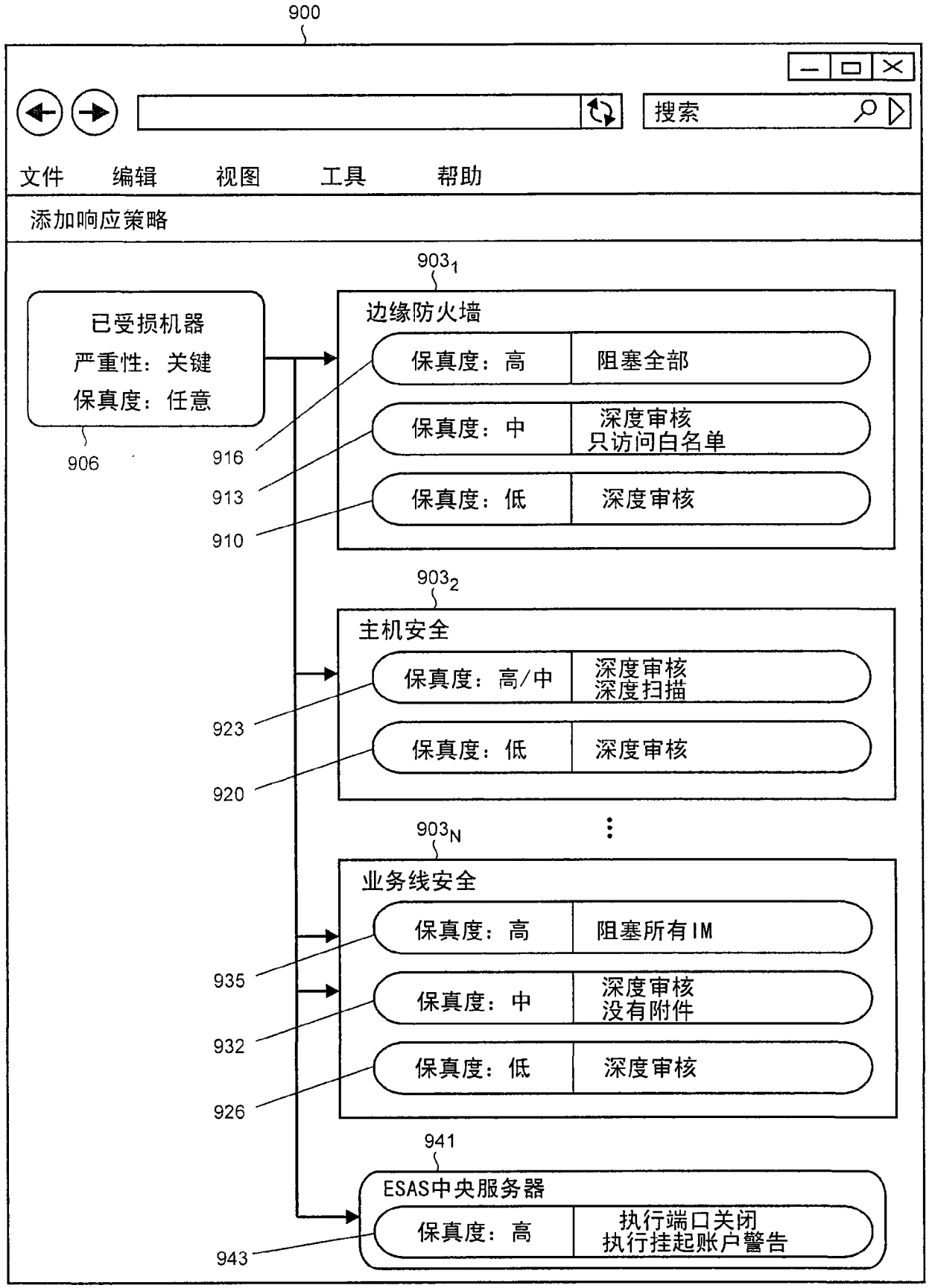

900
搜索
文件
编辑
视图
工具
帮助
添加响应策略
已受损机器
严重性：关键
保真度：任意
906
903_1
边缘防火墙
保真度：高
阻塞全部
保真度：中
深度审核
只访问白名单
保真度：低
深度审核
916
913
910
903_2
主机安全
保真度：高/中
深度审核
深度扫描
保真度：低
深度审核
923
920
903_N
业务线安全
保真度：高
阻塞所有IM
保真度：中
深度审核
没有附件
保真度：低
深度审核
935
932
926
941
ESAS中央服务器
保真度：高
执行端口关闭
执行挂起账户警告
943

图 9

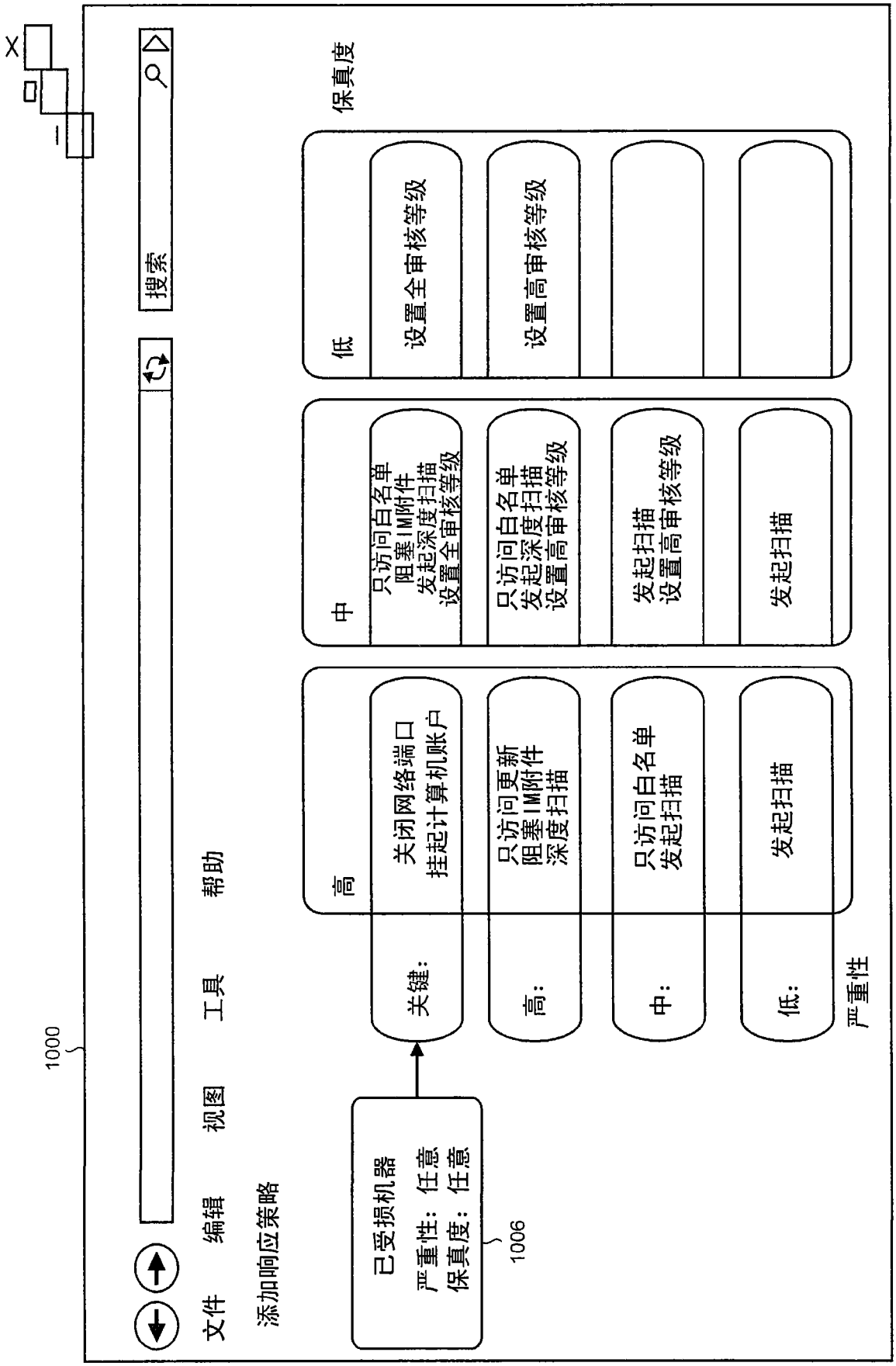

1000
文件 编辑 视图 工具 帮助
添加响应策略
搜索
已受损机器
严重性：任意
保真度：任意
1006
保真度
低
中
高
关键：
高：
中：
低：
严重性
关闭网络端口
挂起计算机账户
只访问更新
阻塞IM附件
深度扫描
只访问白名单
发起扫描
发起扫描
只访问白名单
阻塞IM附件
发起深度扫描
设置全审核等级
只访问白名单
发起深度扫描
设置高审核等级
发起扫描
设置高审核等级
设置全审核等级

图 10

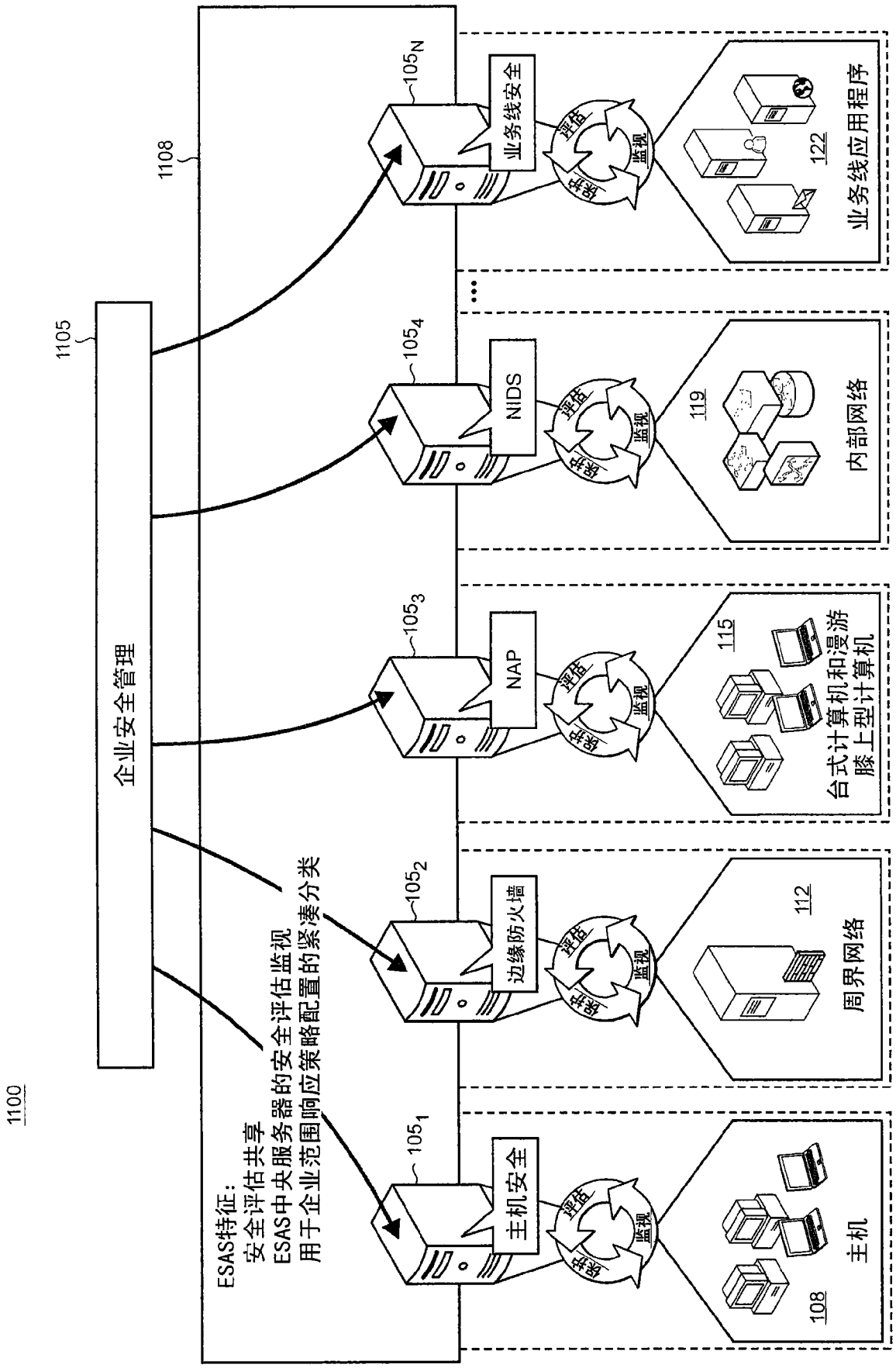

1100
企业安全管理
1105
1108
ESAS特征:
安全评估共享
ESAS中央服务器的安全评估监视
用于企业范围响应策略配置的紧凑分类
105_1
主机安全
105_2
边缘防火墙
105_3
NAP
105_4
NIDS
105_N
业务线安全
评估
监视
实施
108
主机
112
周界网络
115
台式计算机和漫游
膝上型计算机
119
内部网络
122
业务线应用程序

图 11