(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 758 755**

(51) Int. CI.:

G06F 21/57 (2013.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.04.2016 PCT/US2016/029462**

(87) Fecha y número de publicación internacional: **08.12.2016 WO16195847**

(96) Fecha de presentación y número de la solicitud europea: **27.04.2016 E 16803903 (0)**

(97) Fecha y número de publicación de la concesión europea: **09.10.2019 EP 3304336**

(54) Título: **Método para aplicar normas de salud de punto final**

(30) Prioridad:

01.06.2015 US 201562169254 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
06.05.2020

(73) Titular/es:

DUO SECURITY, INC. (100.0%)
123 N. Ashley Street Suite 200
Ann Arbor, MI 48104, US

(72) Inventor/es:

OBERHEIDE, JON y
SONG, DOUGLAS

(74) Agente/Representante:

PAZ ESPUCHE, Alberto

DESCRIPCIÓN

Método para aplicar normas de salud de punto final

Referencia cruzada a solicitudes relacionadas

Esta solicitud reivindica el beneficio de la solicitud provisional estadounidense número 62/169.254 presentada el 01 de junio de 2015.

Campo técnico

Esta invención se refiere de manera general al campo de la autenticación, y más específicamente a un método nuevo y útil para aplicar normas de salud de punto final.

Antecedentes

Las contraseñas se suplantan, capturan, reproducen o comprometen de otro modo fácilmente. Para abordar la debilidad en contraseñas, se desarrolló la autenticación de dos factores. Habitualmente se implementa autenticación de múltiples factores (MFA) para aplicaciones delicadas (por ejemplo, correo electrónico, aplicaciones web, VPN) por administradores de sistemas con el fin de proteger mejor los datos empresariales. Desafortunadamente, incluso con un esquema de autenticación de dos factores bien implementado, los datos o redes delicados pueden verse comprometidos si puntos finales de red quedan expuestos a ataque.

Los puntos finales de red (por ejemplo, el portátil o teléfono inteligente de un usuario) pueden verse comprometidos de varias maneras; en particular, vulnerabilidades en sistemas operativos, navegadores de Internet, y complementos pueden conducir a graves violaciones de seguridad. Tradicionalmente, este problema se ha abordado obligando a la instalación de un agente anfitrión (por ejemplo, un programa de software que funciona en un sistema que explora el sistema para detectar vulnerabilidades), pero esta solución tiene varios problemas. En particular, es difícil garantizar el cumplimiento (es decir, que un agente anfitrión se haya instalado y esté actualizado en todos los puntos finales que acceden a la red) a través de la miríada de dispositivos en uso en una red informática. Por tanto, existe una necesidad en el campo de la autenticación de crear un método nuevo y útil para aplicar normas de salud de punto final. Esta invención proporciona un método nuevo y útil de este tipo. La bibliografía de patentes anterior en el campo incluye: los documentos US2013/239168, US2013/0555289 y US2015/163121.

Sumario de la invención

La presente invención se define por la reivindicación independiente 1 adjunta.

Breve descripción de las figuras

La figura 1 es una vista de diagrama de flujo de un método de una realización preferida;

la figura 2 es una vista de diagrama de flujo de un método de una realización preferida;

la figura 3 es una vista de diagrama gráfico de recopilación de intermediario de un método de una realización preferida;

las figuras 4A y 4B son vistas de diagramas gráficos de recopilación de tercera parte de un método de una realización preferida;

la figura 5 es una vista de diagrama gráfico de generación de inteligencia de salud de punto final;

la figura 6 es una vista de ejemplo de un panel de administrador;

la figura 7 es una vista de ejemplo de un panel de administrador;

la figura 8 es una vista de ejemplo de una notificación de administrador; y

la figura 9 es una vista de ejemplo de una notificación de punto final.

Descripción de las realizaciones preferidas

No se pretende que la siguiente descripción de realizaciones preferidas de la invención limite la invención a estas realizaciones preferidas, sino más bien que permita que cualquier experto en la técnica realice y use esta invención.

1. Resumen general

Tal como se muestra en la figura 2, un método 100 para aplicar normas de salud de punto final incluye evaluar la salud de punto final S110 y generar una notificación de salud de punto final S120. El método 100 puede incluir adicional o alternativamente establecer políticas de acceso a red S140.

El método 100 funciona para permitir la aplicación de normas de salud de punto final a través de puntos finales de red. El método 100 funciona preferiblemente en tándem con servicios existentes en una red usada por puntos finales que acceden a la red; por ejemplo, el método 100 puede asociarse con servicios existentes requeridos para el acceso a red (por ejemplo, autenticación de múltiples factores) de tal manera que cualquier punto final que accede a la red debe pasar por una evaluación de salud de punto final.

El método 100 aplica preferiblemente normas de salud de punto final evaluando en primer lugar la salud de punto final (S110) recopilando datos de salud de punto final a partir de dispositivos que se conectan a, o intentan conectarse a, una red (S111) y generando informes de inteligencia de salud (S112) a partir de esos datos. Tras haberse generado inteligencia de salud de punto final, preferiblemente se proporciona a administradores (S132) para permitir la aplicación de políticas de red (por ejemplo, si se permite y cómo se permite que se conecten dispositivos a la red); adicional o alternativamente, puede proporcionarse inteligencia de salud de punto final directamente a usuarios de punto final (S134) y/o puede usarse para establecer automáticamente políticas de acceso a red para puntos finales (S140).

Los puntos finales de red incluyen preferiblemente cualquier dispositivo usado para acceder a información en una red; por ejemplo, ordenadores de sobremesa, ordenadores portátiles, ordenadores de tipo tableta y teléfonos inteligentes. Otros ejemplos de puntos finales de red incluyen servidores informáticos, lectores de códigos de barras, quioscos y terminales de puntos de ventas (POS).

El método 100 se implementa preferiblemente mediante un servicio de salud de punto final que se hace funcionar mediante, o en tándem con, uno o más servicios de autenticación que funcionan en una red informática. Tanto los servicios de autenticación como el servicio de salud de punto final están preferiblemente basados en la nube (por ejemplo, se usan para permitir el acceso a red en una LAN, pero en realidad se ejecutan en servidores basados en la nube), pero adicional o alternativamente pueden estar basados en red local o incluso ser locales. Adicional o alternativamente, cualquier parte del método 100 puede realizarse por un usuario, un administrador de una red, un dispositivo asociado con un usuario, un dispositivo asociado con un administrador y/o cualquier componente adecuado. El método 100 puede implementarse adicional o alternativamente mediante cualquier dispositivo informático adecuado de cualquier manera adecuada.

Tal como se muestra en la figura 1, en una implementación de una realización preferida del método 100, un enfoque para aplicar normas referentes a vulnerabilidades de seguridad para un dispositivo de usuario de punto final asociado con un usuario incluye: recopilar, en un marco incorporado implementado con una aplicación web, datos de salud de punto final del dispositivo de usuario de punto final en respuesta a que el usuario interactúe con la aplicación web a través del dispositivo de usuario de punto final; generar inteligencia de salud de punto final a partir de los datos de salud de punto final, indicando la inteligencia de salud de punto final salud de seguridad de punto final del dispositivo de usuario de punto final; generar una notificación de salud de punto final que comprende la inteligencia de salud de punto final; y notificar a un administrador de una red con la notificación de salud de punto final.

2. Beneficios

En ejemplos específicos, el método 100 puede conferir varios beneficios con respecto a metodologías convencionales para aplicar normas de salud de punto final. El método 100 puede integrarse sin interrupciones con un servicio o red actual. Por ejemplo, el método 100 puede implementarse en el extremo frontal a través de un marco incorporado de una aplicación web usado para la autenticación de dos factores para un servicio. El mismo marco incorporado puede realizar la autenticación y recopilación de datos de salud de punto final de un dispositivo de usuario de punto final. Como tal, el método 100 puede permitir que la aplicación de salud de punto final sea una extensión natural de procesos ya implementados (por ejemplo, un servicio de autenticación de dos factores) sin requerir la adición manual de servicios de aplicación de salud de punto final a una red o dispositivo de usuario de punto final por usuarios o administradores. Tales enfoques pueden facilitar la salud de punto final al tiempo que permiten (1) un cumplimiento de usuario aumentado, (2) aplicación de normas de salud de punto final para todos los dispositivos de usuario de punto final que intentan acceder a un servicio o a una red, y (3) integración sin interrupciones con servicios sin afectar a la experiencia del usuario.

Además, el método 100 puede facilitar mejoras en el funcionamiento de dispositivos de usuario de punto final y redes abordando posibles vulnerabilidades y aumentando la seguridad (por ejemplo, automáticamente en respuesta a vulnerabilidades identificadas de dispositivos de usuario de punto final, mediante la notificación de administradores de vulnerabilidades, etc.). Estos beneficios pueden lograrse en tiempo real, ya que el método 100 puede facilitar la generación en tiempo real y transmisión de información urgente relevante para la seguridad de dispositivos de usuario de punto final y redes. Tal generación y transmisión de información puede prevenir ataques inminentes en redes y servicios, proporcionando de ese modo soluciones para problemas que surgen específicamente con redes

informáticas, concretamente las vulnerabilidades de seguridad de dispositivos de usuario de punto final que acceden a la red.

3. Método

3.1 Evaluar la salud de punto final

La etapa S110 incluye evaluar la salud de punto final. La etapa S110 funciona para determinar si un punto final (o un grupo de puntos finales) cumple normas de salud de punto final. Tal como se muestra en las figuras 1 y 2, la etapa S110 incluye preferiblemente recopilar datos de salud de punto final S111 y generar inteligencia de salud de punto final S112. La etapa S110 puede incluir adicional o alternativamente modificar normas de salud de punto final S120.

3.1.A Recopilar datos de salud de punto final

La etapa S111 incluye recopilar datos de salud de punto final. La etapa S111 funciona para recopilar datos a partir de puntos finales que pueden usarse para evaluar cualquier posible vulnerabilidad de seguridad. Los datos de punto final recopilados mediante la etapa S111 incluyen preferiblemente la presencia y detalles de funcionamiento (por ejemplo, número de versión) de aplicaciones posiblemente vulnerables u otros programas que funcionan en un punto final; por ejemplo, sistemas operativos, navegadores de Internet, complementos (por ejemplo, Java, Flash), software de paquete de oficina (por ejemplo, iWork, Microsoft Office), lectores de documentos (por ejemplo, Adobe Acrobat) y software de conectividad (por ejemplo, aplicaciones de VPN).

Los datos de salud de punto final pueden incluir adicional o alternativamente cualquier dato relativo a vulnerabilidades de seguridad en un punto final, incluyendo datos relativos a hardware de punto final. Por ejemplo, los datos de salud de punto final pueden incluir tráfico de red u otros datos producidos durante el funcionamiento de punto final; estos datos pueden analizarse para determinar posibles vulnerabilidades. Como otro ejemplo, recopilar los datos de salud de punto final puede incluir realizar la toma de huellas digitales de un dispositivo de usuario de punto final con el fin de recopilar propiedades de hardware del dispositivo de usuario de punto final, en el que los datos de salud de punto final pueden incluir las propiedades de hardware. Las propiedades de hardware de un dispositivo pueden incluir uno o más de: propiedades de batería (por ejemplo, tipo de batería, vida de batería, estado de carga, etc.), características de procesador (por ejemplo, velocidad de procesador, etc.), características de visualización, acciones de interfaz de usuario permitidas, almacenamiento, peso, propiedades de sensor (por ejemplo, sensores de ubicación, sensores de movimiento, etc.), tipo de hardware (por ejemplo, teléfono móvil, portátil, ordenador, ordenador de tipo tableta, reloj inteligente, etc.), propiedades de comunicación (por ejemplo, habilitado para Bluetooth, información de transceptor inalámbrico, etc.) y/o cualquier otra propiedad de hardware adecuada de dispositivos.

En una variación de la etapa S111, se recopilan datos de salud de punto final de una manera sin agente. Por ejemplo, recopilar datos de salud de punto final puede incluir recopilar los datos de salud de punto final sin instalar un agente en un dispositivo de usuario de punto final. Como ejemplo, el componente (por ejemplo, un marco incorporado, un servidor de intermediario, etc.) que recopila datos de salud de punto final puede integrarse con una aplicación web usada para acceder a una red, o integrarse con un marco incorporado usado para la autenticación de múltiples factores para un servicio. Adicional o alternativamente, pueden recopilarse datos de salud de punto final mediante un agente instalado en un dispositivo de usuario de punto final, o de cualquier otra manera.

La etapa S111 incluye preferiblemente recopilar datos de salud de punto final a través de un marco incorporado (denominado a partir de ahora “iframe”) integrado en un sitio web; esta técnica se denomina a partir de ahora “recopilación de iframe”. La etapa S111 incluye más preferiblemente recopilar datos de salud de punto final a través de un iframe integrado en uno o más sitios web usados para la autenticación de múltiples factores. Adicional o alternativamente, la etapa S111 puede incluir recopilar datos de salud de punto final de cualquier manera adecuada, por ejemplo, mediante un servidor de intermediario (denominado a partir de ahora “recopilación de intermediario”), mediante una tercera parte (denominado a partir de ahora “recopilación de tercera parte”) y/o mediante un agente anfitrión (denominado a partir de ahora “recopilación de agente anfitrión”).

3.1.A.i Recopilar datos de salud de punto final – Recopilación de marco incorporado.

Recopilar datos de salud de punto final puede incluir adicional o alternativamente recopilar, en un iframe, datos de salud de punto final del dispositivo de usuario de punto final, que funciona para recopilar datos de un dispositivo de punto final en un iframe.

La recopilación de datos de salud de punto final a través de un iframe integrado en un sitio web permite capturar datos de salud de punto final siempre que un usuario de punto final (o programa automatizado que se ejecuta en un punto final) interactúa con el sitio web. Por ejemplo, pueden recopilarse datos de salud de punto final en un iframe en respuesta a que el usuario interactúe con la aplicación web a través del dispositivo de usuario de punto final. El iframe puede integrarse en una aplicación web (por ejemplo, un sitio web, una aplicación accesible a través de Internet, una aplicación que facilita la interacción directa con el usuario de una manera interactiva, etc.), una

aplicación nativa y/o cualquier software adecuado. El iframe puede incluir recursos que pueden presentarse en Silverlight, Flash, HTML 5 y/o cualquier medio y/o reproductor multimedia / complemento adecuado. El iframe puede incluir un elemento de bloque tal como DIV, SPAN u otra etiqueta de HTML, objeto integrado y/o cualquier otro elemento adecuado.

Mientras que la recopilación de iframe incluye preferiblemente recopilar datos usando un objeto de iframe de HTML, la etapa S111 puede incluir adicional o alternativamente cualquier recopilación de datos de salud de punto final a través de una interfaz de web. Por ejemplo, la etapa S111 puede incluir realizar un redireccionamiento de HTTP para enviar en primera vez a usuarios que desean autenticación de red a un sitio diseñado para recopilar datos de salud de punto final antes de permitir que el usuario continúe con la autenticación de red. Como otro ejemplo, la etapa S111 puede incluir recopilar simplemente datos de salud de punto final como parte de una aplicación web; que la aplicación web reenvíe los datos de salud de punto final a un servicio de monitorización de salud de punto final (por ejemplo, mediante una API REST). Sin embargo, la recopilación de datos de salud de punto final puede realizarse en cualquier interfaz integrable adecuada con cualquier anfitrión adecuado para la interfaz integrada.

El iframe se integra preferiblemente en un sitio web usado para autenticar a un usuario para su acceso a una red informática; por ejemplo, el iframe puede integrarse en un sitio web usado para acceder a una red informática desde el exterior de la red física (por ejemplo, mediante VPN). En otro ejemplo, recopilar los primeros datos de salud de punto final puede incluir recopilar los primeros datos de salud de punto final en respuesta a que el primer dispositivo de usuario de punto final intente acceder a la primera red desde la aplicación web. Usar recopilación de iframe en un sitio web requerido para el acceso a red garantiza que los dispositivos que acceden a la red pueden someterse a la aplicación de normas de salud. Adicional o alternativamente, el iframe puede integrarse en cualquier sitio web.

La recopilación de iframe incluye preferiblemente recopilar datos de agente de navegadores web (por ejemplo, recopilando datos de cabecera de agente de usuario de HTTP). Una cabecera de agente de usuario puede ser de la siguiente manera: *Mozilla / 5.0 (Macintosh; Intel Mac OS X 10_9_3) AppleWebKit / 537.75.14 (KHTML,* tal como *Gecko) Versión / 7.0.3 Safari / 7046A194A.* Una cabecera de agente de usuario de este tipo puede usarse para determinar el sistema operativo, versión de sistema operativo, navegador y versión de navegador de un punto final que accede al iframe integrado. Sin embargo, puede recopilarse cualquier dato de salud de punto final adecuado en uno o más iframes. La recopilación de iframe también puede incluir realizar la toma de huellas digitales de dispositivo (por ejemplo, toma de huellas digitales de lienzo). La toma de huellas digitales de dispositivo puede incluir recopilar datos tales como configuración de TCP/IP de cliente, huella digital de OS, ajustes inalámbricos, sesgo de reloj de hardware, dirección MAC de cliente, etc. Sin embargo, puede recopilarse cualquier dato de salud de punto final adecuado en un iframe.

Un iframe puede asociarse con cualquier número de aplicaciones web, redes, administradores de red y/u otra entidad adecuada. Por ejemplo, el método 100 puede incluir recopilar, en un iframe (por ejemplo, el mismo iframe usado para recopilar primeros datos de salud de punto final de un primer dispositivo de usuario de punto final asociado con una primera red), segundos datos de salud de punto final de un segundo dispositivo de usuario de punto final en respuesta a que un segundo usuario interactúe con la aplicación web a través del segundo dispositivo de usuario de punto final; generar segunda inteligencia de salud de punto final a partir de los segundos datos de salud de punto final; generar una segunda notificación de salud de punto final que comprende la segunda inteligencia de salud de punto final; y notificar a un segundo administrador de una segunda red (por ejemplo, en contraposición al primer administrador de una primera red) con la segunda notificación de salud de punto final.

En una primera variación, recopilar datos de salud de punto final en un iframe puede incluir recopilar de manera activa datos de salud de punto final en el iframe. Por ejemplo, recopilar los primeros datos de salud de punto final puede incluir: consultar al dispositivo de usuario de punto final a partir del iframe; y en respuesta a la consulta del dispositivo de usuario de punto final, recibir los datos de salud de punto final a partir del dispositivo de usuario de punto final. Recopilar de manera activa datos de salud de punto final en un iframe puede incluir transmitir sondas de datos de salud de punto final para pedir datos de salud de punto final a partir de una o más entidades incluyendo: una aplicación de tercera parte que funciona en el dispositivo de usuario, una aplicación nativa, el usuario asociado con el dispositivo de usuario (por ejemplo, transmitir una notificación al dispositivo de usuario pidiendo una respuesta por parte del usuario), un servicio asociado con el dispositivo de usuario (por ejemplo, un servicio de seguridad, un servicio de autenticación de dos factores, servicio de cliente, servicio de comunicación, servicio de nómina), un servidor, otra red y/o cualquier entidad adecuada. La recopilación activa de datos de salud de punto final puede realizarse a intervalos de tiempo especificados (por ejemplo, cada día, semana, mes, etc.), en condiciones indicadas (por ejemplo, durante un proceso de autenticación para un usuario que intenta acceder a un servicio, cuando un dispositivo de usuario intenta acceder a una red a través de una aplicación web con un iframe integrado), manualmente (por ejemplo, iniciado por un administrador, por un usuario, etc.) y/o de cualquier manera adecuada.

En la primera variación, la recopilación de iframe puede incluir adicional o alternativamente realizar otras técnicas de interrogación basadas en web. Por ejemplo, la recopilación de iframe puede incluir consultar a un objeto javascript de navigator.plugins para detallar los complementos instalados en el navegador de punto final (por ejemplo, Java, Flash, etc.) incluyendo también posiblemente números de versión. La recopilación de iframe puede incluir cualquier método de consulta de un punto final a través de la interfaz integrada; como otro ejemplo, puede usarse recopilación

de iframe para determinar detalles sobre la conexión a Internet de un usuario (por ejemplo, dirección IP). La recopilación de iframe también puede incluir recopilar información a partir de objetos compartidos de manera local (por ejemplo, cookies flash) o a partir de complementos de navegador (por ejemplo, complementos de OS para soporte remoto). Sin embargo, cualquier dato de salud de punto final adecuado puede recopilarse con recopilación de iframe. Sin embargo, la recopilación de manera activa de datos de salud de punto final en el iframe puede realizarse de otra manera.

En una segunda variación, recopilar los datos de salud de punto final en el iframe puede incluir recopilar de manera pasiva datos de salud de punto final en el iframe. Los datos de salud de punto final recopilados de manera pasiva pueden incluir: peticiones de navegador web, credenciales de usuario (por ejemplo, en un iframe para autenticación de dos factores), cabeceras de HTTP y/o cualquier otro dato de salud de punto final adecuado. Por ejemplo, puede recibirse una cabecera de agente de usuario de HTTP en un iframe integrado dentro de una aplicación web, tal como cuando un navegador web de dispositivo de usuario que se interconecta con la aplicación web envía la cabecera de agente de usuario de HTTP junto con una petición al iframe. En un ejemplo específico, recopilar de manera pasiva datos de salud de punto final puede incluir extraer, en el iframe, el tipo de sistema operativo y versión de sistema operativo a partir de una cabecera de agente de usuario de HTTP, en el que los datos de salud de punto final incluyen el tipo de sistema operativo y la versión de sistema operativo. Adicional o alternativamente, el iframe puede pedir la cabecera de agente de usuario. Sin embargo, la recopilación de manera pasiva de datos de salud de punto final puede realizarse de otra manera.

En una tercera variación, la recopilación de iframe puede aprovechar la existencia de iframes usados para realizar la autenticación de múltiples factores; por ejemplo, la plataforma de Duo Security puede integrar iframes en aplicaciones web para permitir la autenticación de múltiples factores, tal como se describe en la patente estadounidense n.º 8.510.820. En tal caso, el mismo marco integrado usado para realizar la autenticación de múltiples factores (o incluir dispositivos para MFA, gestionar la autenticación de dispositivos para MFA, proporcionar realimentación sobre procesos de MFA, etc.) también puede usarse para recopilar datos de salud de punto final. De esta manera, la recopilación de iframe permite recopilar datos de salud de punto final sin requerir integración de servicio de extremo trasero explícita (por ejemplo, RADIUS, LDAP, etc.). Alternativamente, pueden usarse diferentes iframes integrados dentro del mismo anfitrión de interfaz integrado (por ejemplo, una misma aplicación web) para recopilar datos de salud de punto final y para la autenticación. En un ejemplo específico, el método 100 puede incluir administrar, en un segundo iframe (por ejemplo, en el que el primer iframe es un iframe para recopilar los datos de salud de punto final) implementado con la aplicación web, la autenticación de dos factores para un usuario que interactúa con la aplicación web a través del dispositivo de usuario de punto final. En este ejemplo específico, el segundo iframe puede ser igual que o diferente del primer iframe. Sin embargo, puede integrarse cualquier número adecuado de iframes que presentan cualquier función adecuada a través de cualquier número adecuado de anfitriones de interfaz integrados.

En la tercera variación, la recopilación de datos de salud de punto final en un marco incorporado puede realizarse en cualquier momento adecuado con respecto a la autenticación de un dispositivo de usuario de punto final. Por ejemplo, para un marco incorporado usado para autenticación de un usuario, recopilar los datos de salud de punto final puede incluir recopilar los datos de salud de punto final durante la autenticación del usuario. Además, el uso de un iframe para la autenticación y un iframe para la recopilación de datos de salud de punto final puede realizarse de otra manera.

En una cuarta variación, el método 100 puede incluir adicional o alternativamente implementar un iframe con un anfitrión de interfaz integrado (por ejemplo, una aplicación web). La implementación del iframe puede realizarse, por ejemplo, mediante un administrador de la aplicación web, un servidor remoto asociado con el servicio que recopila los datos de salud de punto final en el marco incorporado y/o cualquier otra entidad adecuada. En un ejemplo específico, el método 100 puede incluir implementar un marco incorporado con la aplicación web, en el que el primer marco incorporado se usa para autenticar al primer usuario, y en el que recopilar los datos de salud de punto final comprende recopilar los primeros datos de salud de punto final únicamente en el marco incorporado. En otro ejemplo específico, el método 100 puede incluir integrar el iframe con una aplicación web usada para acceder a una red (por ejemplo, la red en la que se notifica al administrador con una notificación de salud de punto final que comprende inteligencia de salud de punto final de un dispositivo de usuario de punto final que intenta acceder a la red a través de la aplicación web). En un ejemplo específico adicional que ilustra la recopilación sin agente de datos de salud de punto final, el método 100 puede incluir: implementar un iframe con una aplicación web, en el que la aplicación web se usa para acceder a la red, y en el que recopilar los datos de salud de punto final incluye recopilar los datos de salud de punto final únicamente en el iframe. Sin embargo, la implementación del iframe puede realizarse de cualquier manera adecuada.

3.1.A. ii Recopilar datos de salud de punto final – Recopilación de intermediario.

Tal como se muestra en la figura 3, recopilar datos de salud de punto final puede incluir adicional o alternativamente recopilar, en un servicio de intermediario, datos de salud de punto final del dispositivo de usuario de punto final, que funciona para recopilar datos de un dispositivo de punto final en un servicio de intermediario.

En algunos casos, puede ser deseable realizar la recopilación de datos de salud de punto final para todos los dispositivos que pasan tráfico en una red o subred (en contraposición a dispositivos que intentan la autorización con una aplicación o servicio particular). En este caso, la recopilación de datos de salud de punto final se realiza preferiblemente mediante un servicio de intermediario. Preferiblemente el servicio de intermediario al menos recopila datos de salud de punto final para dispositivos que pasan tráfico a través del mismo, pero puede aplicar adicional o alternativamente políticas de acceso a red para esos dispositivos.

La recopilación de intermediario puede incluir recopilar datos de salud de punto final mediante cabeceras de HTTP o toma de huellas digitales de dispositivo (tal como se describe en la sección de recopilación de iframe), pero puede incluir adicional o alternativamente recopilar datos de salud de punto final de maneras adicionales; por ejemplo, la recopilación de intermediario puede incluir recopilar datos sobre tráfico de red que pasa a través del intermediario, que pueden usarse para determinar la salud de punto final. Por ejemplo, la recopilación de intermediario puede usar análisis de tráfico de red para determinar si un punto final está comprometido.

El servidor de intermediario usado para la recopilación de intermediario está preferiblemente ubicado en una red de área local, pero adicional o alternativamente puede estar ubicado en la nube (o cualquier otra ubicación adecuada).

El servidor de intermediario puede realizar simplemente la recopilación de datos de salud de punto final, pero puede realizar adicional o alternativamente cualquier función adicional (por ejemplo, actuar de cortafuegos). Sin embargo, la recopilación de datos de salud de punto final en un servicio de intermediario puede realizarse de cualquier manera adecuada.

3.1.A.iii Recopilar datos de salud de punto final – Recopilación de tercera parte.

Recopilar datos de salud de punto final puede incluir adicional o alternativamente recopilar datos de salud de punto final del dispositivo de usuario de punto final a partir de una aplicación de tercera parte, que funciona para recopilar datos de salud de punto final a partir de una fuente de tercera parte.

Algunos datos de salud de punto final pueden mantenerse o ser accesibles por partes distintas del punto final (por ejemplo, aplicaciones externas), y estos datos pueden ser accesibles para servicios de monitorización de salud de punto final. En este caso, la etapa S111 puede incluir consultar a estas terceras partes para pedir datos de salud de punto final, tal como se muestra en las figuras 4A y 4B. En algunos casos, pueden recopilarse previamente datos de salud de punto final por terceras partes (por ejemplo, tal como en la figura 4A), mientras que en otros casos pueden recopilarse datos de salud de punto final en respuesta a una consulta (por ejemplo, tal como en la figura 4B). En cualquier caso, la autenticación (si se requiere) del servicio de salud de punto final puede realizarse mediante cualquiera de la tercera parte o del propio punto final. Pueden requerirse terceras partes por uno cualquiera o más de: un servicio (por ejemplo, un servicio de autenticación de dos factores implementado con la aplicación web a la que está accediendo el dispositivo de usuario de punto final), un iframe (por ejemplo, un mismo iframe comentado en la sección 3.1.A.i), un servicio de salud de punto final (por ejemplo, un servidor remoto usado para generar inteligencia de salud de punto final) y/o cualquier otra entidad adecuada.

Los datos recopilados mediante recopilación de tercera parte pueden incluir cualquier dato de salud de punto final recopilado por recopilación de intermediario y de iframe, y pueden incluir adicional o alternativamente cualquier dato de salud de punto final accesible para la tercera parte (en algunos casos, más datos pueden ser accesibles para la tercera parte, particularmente si el servicio o la aplicación de tercera parte tienen un agente anfitrión instalado en el punto final).

Adicional o alternativamente, recopilar datos de salud de punto final puede incluir recibir datos de salud de punto final introducidos a partir de un usuario y/o un administrador. Por ejemplo, puede pedirse a un usuario que introduzca información de sistema operativo del dispositivo de usuario de punto final que intenta acceder a una red de área local de compañía.

Sin embargo, la recopilación de tercera parte de datos de salud de punto final puede realizarse de cualquier otra manera adecuada.

3.1.A.iv Recopilar datos de salud de punto final – Recopilación de agente anfitrión.

Recopilar datos de salud de punto final puede incluir adicional o alternativamente recopilar, en un agente anfitrión, datos de salud de punto final del dispositivo de usuario de punto final, que funciona para recopilar datos de un dispositivo de punto final en un agente anfitrión que funciona en el dispositivo de punto final.

La recopilación de agente anfitrión incluye preferiblemente recopilar datos de salud de punto final a partir de una aplicación o servicio que se ejecuta en el punto final. En este caso, agente anfitrión se refiere a cualquier programa o servicio que se ejecuta en un punto final que permite la recopilación de datos de salud de punto final (por ejemplo, antivirus o software de seguridad, API de gestión de dispositivo integradas con sistemas operativos, etc.).

La recopilación de agente anfitrión puede incluir recopilar datos de salud de punto final con un agente anfitrión específicamente asociado con el servicio de monitorización de salud de punto final que realiza el método 100, o puede incluir adicional o alternativamente recopilar datos de salud de punto final a través de agentes anfitriones de terceras partes o a través de API de gestión de dispositivo que funcionan en puntos finales.

Los datos de salud de punto final recopilados mediante recopilación de agente anfitrión pueden incluir cualquiera de los datos de salud de punto final anteriormente mencionados, pero pueden incluir adicional o alternativamente información accesible para el agente anfitrión pero no para servicios externos (por ejemplo, datos de uso informático, detalles de cifrado de archivos, etc.). En una realización, la recopilación de agente anfitrión es complementaria a la recopilación de iframe; un punto final puede acceder a la red según una primera política de acceso a red sin instalar el agente anfitrión, pero puede acceder a la red según una segunda política de acceso a red (menos restrictiva) tras instalar el agente anfitrión.

Obsérvese que aunque estas técnicas se describen de manera independiente, la recopilación de datos de salud de punto final mediante la etapa S111 puede incluir cualquier combinación de las técnicas anteriores. Por ejemplo, recopilar datos de salud de punto final puede incluir recopilar datos en uno cualquiera o más de un iframe, un servicio de intermediario, mediante una tercera parte, un agente anfitrión y/o cualquier componente adecuado. En un ejemplo específico, para un conjunto de dispositivos de usuario de punto final asociados con una red, pueden recopilarse datos de salud de punto final de un primer dispositivo de usuario de punto final en un iframe de una aplicación web usada para acceder a la red. Pueden recopilarse datos de salud de punto final de un segundo dispositivo de usuario de punto final en un servicio de intermediario que monitoriza tráfico del segundo dispositivo de usuario de punto final. Pueden recopilarse datos de salud de punto final de un tercer dispositivo de usuario de punto final a partir de un agente anfitrión instalado en el tercer dispositivo de usuario de punto final. Pueden recopilarse datos de salud de punto final adicionales de cada uno de los dispositivos de usuario de punto final primero, segundo y tercero a partir de aplicaciones de tercera parte asociadas con los dispositivos de usuario. Sin embargo, puede aprovecharse cualquier combinación de componentes que recopilan datos de salud de punto final.

La etapa S111 recopila preferiblemente datos de salud de punto final almacenando datos de salud de punto final en una base de datos en la nube para su análisis posterior. La etapa S111 puede incluir adicional o alternativamente almacenar datos de salud de punto final en cualquier ubicación adecuada (por ejemplo, en servidores locales con respecto a una red particular).

La etapa S111 puede incluir adicional o alternativamente procesar datos de salud de punto final para preparar los datos para la generación de inteligencia de salud de punto final. Por ejemplo, la etapa S111 puede incluir calcular el promedio de, o agregar, datos de salud de punto final (por ejemplo, para producir un informe de estado de red global), etiquetar datos inesperados/inusuales, y/o agregar datos. En particular, la etapa S111 puede incluir agregar datos de identificación de red. Por ejemplo, la etapa S111 puede incluir agregar información de usuario de red a datos de salud de punto final correspondientes a un usuario particular; por ejemplo, si los datos de salud de punto final recopilados incluyen una dirección IP, la dirección IP puede vincularse a un usuario particular mediante DHCP u otro registro de cuenta ubicado en servidores de red (que pueden consultarse en la etapa S111).

3.2 Generar inteligencia de salud de punto final.

La etapa S112 incluye generar inteligencia de salud de punto final. La etapa S112 funciona para generar datos que describen la salud de punto final. La etapa S112 incluye preferiblemente evaluar datos de salud de punto final frente a normas de salud de punto final (por ejemplo, comparar datos de salud de punto final con normas de salud de punto final), pero puede incluir adicional o alternativamente analizar datos de salud de punto final de cualquier manera adecuada para determinar la salud de punto final (por ejemplo, usando heurística).

La inteligencia de salud de punto final indica preferiblemente la salud de seguridad de punto final de uno o más dispositivos de usuario de punto final, pero puede indicar cualquier otra característica adecuada. La inteligencia de salud de punto final puede incluir informes para acontecimientos específicos (por ejemplo, inicio de sesión satisfactorio o fallido), puntos finales específicos, grupos de puntos finales, la red en su conjunto y/o para cualquier otro objeto adecuado. Generar inteligencia de salud de punto final incluye preferiblemente generar inteligencia de salud de punto final a partir de datos de salud de punto final (por ejemplo, los datos de salud de punto final recopilados en la etapa S111). En un ejemplo, generar la inteligencia de salud de punto final incluye generar la inteligencia de salud de punto final basándose en el tipo de sistema operativo y la versión de sistema operativo. Adicional o alternativamente, puede generarse inteligencia de salud de punto final basándose en información complementaria (por ejemplo, información sobre un usuario, información sobre servicios ofrecidos en la red, etc.). Por ejemplo, puede generarse inteligencia de salud de punto final a partir de procesamiento de datos de salud de punto final de un dispositivo de usuario de punto final con información sobre la adherencia de un usuario a la actualización oportuna de software en diversos dispositivos del usuario. Adicional o alternativamente, puede generarse inteligencia de salud de punto final basándose en propiedades de hardware de dispositivos de usuario de punto final. Por ejemplo, el método 100 puede incluir recopilar propiedades de hardware del dispositivo de usuario de punto final; generar un perfil de dispositivo de punto final a partir de las propiedades de hardware; en el que generar inteligencia de salud de punto final comprende generar inteligencia de salud de punto final a partir del perfil

de dispositivo de punto final. Sin embargo, puede generarse inteligencia de salud de punto final a partir de cualquier información adecuada.

Las normas de salud de punto final incluyen preferiblemente criterios que los datos de salud de punto final deberían (o deben) cumplir para políticas de red particulares. Las normas de salud de punto final incluyen preferiblemente números de versión de sistema operativo, navegador y complementos aceptables (es decir, estos deben ser actuales dentro de algún conjunto de versiones establecidas por las normas de salud de punto final), pero pueden incluir adicional o alternativamente cualquier norma adecuada basándose en datos de salud de punto final. Las normas de salud de punto final pueden incluir datos de salud de punto final esperados (por ejemplo, datos de salud de punto final deseables que reducen vulnerabilidades de seguridad, etc.), datos de salud de punto final inesperados (por ejemplo, un tipo de sistema operativo que no se esperaba de dispositivos de usuario de punto final asociados con una red), normas establecidas por administrador (por ejemplo, normas de salud de punto final seleccionadas por un administrador de red) y/o cualquier otro dato adecuado.

Pueden usarse normas de salud de punto final simplemente para notificar a administradores y/o usuarios de posibles vulnerabilidades, pero adicional o alternativamente pueden vincularse a políticas de acceso a red. Como primer ejemplo, un punto final puede necesitar cumplir un conjunto particular de normas de salud de punto final con el fin de acceder a una red o servicio. Como segundo ejemplo, el nivel de acceso a red concedido a un punto final puede determinarse mediante la clase de normas de salud de punto final que cumple el punto final. Esto se describirá en más detalle en las secciones que describen la etapa S140.

La generación de inteligencia de salud de punto final puede realizarse parcial o totalmente mediante uno o más de: un servidor remoto (por ejemplo, un servidor remoto asociado con un iframe que recopila datos de salud de punto final), un dispositivo asociado con un usuario y/o administrador y/o cualquier otra entidad adecuada.

Desde el punto de vista del tiempo, la generación de inteligencia de salud de punto final se realiza preferiblemente en respuesta a recibir datos de salud de punto final en el componente (por ejemplo, un servidor remoto) que genera inteligencia de salud de punto final. Por ejemplo, en respuesta a recopilar datos de salud de punto final en un iframe integrado en una aplicación web, puede generarse inteligencia de salud de punto final a partir de tales datos de salud de punto final. Adicional o alternativamente, puede generarse inteligencia de salud de punto final tras recogerse un umbral (por ejemplo, por tamaño, tipos de unos datos de salud de punto final, datos de salud de punto final a través de un número umbral de dispositivos, etc.) de datos de salud de punto final. La generación de inteligencia de salud de punto final se genera preferiblemente en tiempo real (por ejemplo, durante una sesión de autenticación de un dispositivo de usuario de punto final en un iframe usado tanto para autenticación como para recopilación de datos de salud de punto final). Sin embargo, puede generarse inteligencia de salud de punto final en cualquier momento adecuado de cualquier manera adecuada.

3.2.A Generar inteligencia de salud de punto final – Comparar datos de salud de punto final con normas de salud de punto final.

En una primera variación, generar inteligencia de salud de punto final puede incluir comparar datos de salud de punto final con normas de salud de punto final. Pueden compararse tipos de datos de salud de punto final específicos (por ejemplo, tipo de navegador, navegador, versión, etc.) con normas de salud de punto final específicas relacionadas con los tipos de datos de salud de punto final. Por ejemplo, pueden compararse datos de salud de punto final de tipo de sistema operativo y versión de sistema operativo con normas de salud de punto final de un tipo de sistema operativo esperado (por ejemplo, un tipo de sistema operativo que un administrador de una red espera que tengan los usuarios de la red) y una versión de sistema operativo esperada. Adicional o alternativamente, pueden compararse perfiles de datos de salud de punto final (por ejemplo, un perfil de las diferentes aplicaciones y sus versiones que funcionan en un dispositivo de usuario de punto final) en su conjunto con normas de salud de punto final para tales perfiles. Sin embargo, puede compararse cualquier granularidad de datos de salud de punto final con cualquier granularidad de normas de salud de punto final en la generación de inteligencia de salud de punto final.

En la primera variación, comparar datos de salud de punto final con normas de salud de punto final puede incluir el grado en el que las normas de salud de punto final se satisfacen por los datos de salud de punto final. En un ejemplo específico, pueden compararse el tipo de navegador y la versión de navegador recopilados a partir de una cabecera de agente de usuario de HTTP recibida en un iframe frente a normas de salud de punto final que especifican tipo de navegador “A” y al menos versión de navegador “5.3”. Los tipos y versiones de navegador recopilados de dispositivos de usuario de punto final pueden compararse con las normas, y puede generarse inteligencia de salud de punto final basándose en la comparación. La falta de satisfacción de una norma de salud de punto final puede indicar una vulnerabilidad de seguridad del dispositivo de usuario de punto final. Por ejemplo, generar la inteligencia de salud de punto final puede incluir identificar una vulnerabilidad de seguridad asociada con los datos de salud de punto final (por ejemplo, basándose en una propiedad de datos de salud de punto final que no logra cumplir una norma de salud de punto final). Puede notificarse a administradores y/o usuarios de vulnerabilidades identificadas, en la que una notificación de salud de punto final puede incluir una indicación de la vulnerabilidad de seguridad. En la primera variación, la inteligencia de salud de punto final puede indicar el número (por ejemplo, número de normas

de salud de punto final no cumplidas), tipo (por ejemplo, tipo de norma de salud de punto final no cumplida), grado (por ejemplo, un nivel de vulnerabilidad de seguridad basándose en el grado en el que no se cumplen las normas de salud de punto final) y/o cualquier característica adecuada referente a no lograr los datos de salud de punto final cumplir las normas de salud de punto final. Sin embargo, la comparación de inteligencia de salud de punto final y normas de salud de punto final puede realizarse de cualquier manera adecuada.

3.2.B Generar inteligencia de salud de punto final – Comparar datos de salud de punto final de múltiples dispositivos de usuario de punto final.

En una segunda variación, generar inteligencia de salud de punto final puede incluir generar una comparación entre datos de salud de punto final de múltiples dispositivos de usuario de punto final. Tales dispositivos de usuario pueden estar asociados con el mismo usuario, con diferentes usuarios y/o cualquier entidad adecuada. Por ejemplo, generar la inteligencia de salud de punto final puede incluir generar una comparación entre primeros datos de salud de punto final de un primer dispositivo de usuario de punto final y segundos datos de salud de punto final de un segundo dispositivo de usuario de punto final, en el que una notificación de salud de punto final generada (por ejemplo, que va a usarse en la notificación a un administrador de una red a la que intentan acceder los dispositivos de usuario de punto final primero y segundo) puede incluir la comparación entre los primeros datos de salud de punto final y los segundos datos de salud de punto final.

En la segunda variación, puede compararse cualquier dato de salud de punto final adecuado a través de dispositivos de usuario de punto final. Por ejemplo, el método 100 puede incluir recopilar información de tipo de navegador a partir de un conjunto de dispositivos de usuario de punto final que intentan acceder a una red de área local. Puede generarse inteligencia de salud de punto final a partir de la comparación de la información de tipo de navegador de los múltiples dispositivos. Esta inteligencia generada puede incluir, como ilustración, que el dispositivo de usuario de punto final “A” usa el navegador “a”, pero el 85% de los demás dispositivos en la red usan el navegador “b”. Sin embargo, puede generarse cualquier inteligencia de salud de punto final adecuada a partir de la comparación de datos de salud de punto final de múltiples dispositivos de usuario (por ejemplo, diferencias y/o similitudes en cuanto al software, en cuanto al hardware, en cuanto al nivel de vulnerabilidad, en cuanto al tráfico, etc.).

En la segunda variación, pueden almacenarse datos de salud de punto final históricos de dispositivos de usuario de punto final (por ejemplo, en un servidor remoto), y tales datos históricos pueden usarse en la generación de inteligencia de salud de punto final con respecto a un dispositivo de usuario de punto final actual (por ejemplo, un dispositivo de usuario de punto final que intenta actualmente acceder a una red). Sin embargo, la generación de una comparación entre datos de salud de punto final de múltiples dispositivos de usuario de punto final puede realizarse de otra manera.

3.2.C Generar inteligencia de salud de punto final – Comparar datos de salud de punto final con datos de salud de punto final históricos.

En una tercera variación, generar inteligencia de salud de punto final puede incluir generar una comparación entre datos de salud de punto final de un dispositivo de usuario de punto final, y datos de salud de punto final históricos del mismo dispositivo de usuario de punto final. La inteligencia de salud de punto final generada basándose en una comparación de este tipo puede incluir: información de versión (por ejemplo, actualizaciones de versión de aplicación, vueltas a versiones anteriores, etc.), información de tipo de aplicación (por ejemplo, cambios en el tipo de aplicaciones presentes en las aplicaciones que funcionan en el dispositivo de usuario de punto final, adiciones de software, borrados de software), información de hardware (por ejemplo, actualizaciones de hardware, vueltas a versiones anteriores, adiciones de hardware de terceras partes, etc.) y/o cualquier otra inteligencia adecuada. Adicional o alternativamente, pueden capturarse datos de salud de punto final capturados a lo largo del tiempo para un usuario (por ejemplo, a través de dispositivos de usuario asociados con el usuario). Por ejemplo, puede generarse inteligencia de salud de punto final basándose en la adición de nuevos dispositivos de usuario asociados con una cuenta de usuario dada. Sin embargo, en la generación de inteligencia de salud de punto final pueden compararse datos de salud de punto final para uno o más de un dispositivo de usuario, un usuario, una red, un administrador y/o cualquier otro componente adecuado. Sin embargo, la comparación de datos de salud de punto final y datos de salud de punto final históricos puede realizarse de cualquier manera adecuada.

3.2.D Generar inteligencia de salud de punto final – Usar un modelo de aprendizaje automático.

En una cuarta variación, generar inteligencia de salud de punto final puede incluir generar inteligencia de salud de punto final usando un modelo de aprendizaje automático. Puede usarse un modelo de aprendizaje automático en la generación de cualquier inteligencia de salud de punto final adecuada. Por ejemplo, generar inteligencia de salud de punto final puede incluir generar una indicación de vulnerabilidad (por ejemplo, un nivel de vulnerabilidad frente a violaciones de seguridad del dispositivo de usuario de punto final) usando un modelo de aprendizaje automático generado a partir de las normas de salud de punto final, en el que la indicación de vulnerabilidad está asociada con los datos de salud de punto final (por ejemplo, los datos de salud de punto final recopilados para un dispositivo de usuario de punto final que intenta acceder a la red), y en el que una notificación de salud de punto final generada puede comprender la indicación de vulnerabilidad. En este ejemplo, el método 100 puede incluir recibir, a partir de

un administrador de la red, verificación de la indicación de vulnerabilidad (por ejemplo, en una interfaz de seguridad proporcionada para el administrador y accesible a través de Internet para ver notificaciones de salud de punto final); y actualizar el modelo de aprendizaje automático con los datos de salud de punto final y la verificación asociada de la indicación de vulnerabilidad. Tales modelos actualizados pueden usarse en casos posteriores de generación de inteligencia de salud de punto final para datos de salud de punto final recopilados. Sin embargo, los modelos de aprendizaje automáticos para generar inteligencia de salud de punto final pueden actualizarse de otra manera.

En un ejemplo específico, tal como se muestra en la figura 5, puede generarse un modelo de aprendizaje automático a partir de datos de entrenamiento incluyendo: perfiles de datos de salud de punto final con vulnerabilidad conocida (por ejemplo, perfiles de datos de salud de punto final recopilados que se han marcado con un nivel de vulnerabilidad por un administrador de red), información de seguridad recopilada a partir de una tercera parte (por ejemplo, información que indica vulnerabilidades de seguridad conocidas asociadas con determinadas versiones de aplicaciones), y normas de salud de punto final recibidas a partir de un administrador (por ejemplo, datos de salud de punto final esperados para la red, datos de salud de punto final inesperados, niveles de vulnerabilidad asociados con tales datos, etc.) y/o cualquier otro dato de entrenamiento adecuado. Los datos de prueba pueden incluir datos de salud de punto final con vulnerabilidad desconocida. Usando el modelo generado, puede determinarse una indicación de vulnerabilidad y/o cualquier otra inteligencia de salud de punto final adecuada para los datos de prueba de salud de punto final. Sin embargo, puede usarse cualquier dato de entrenamiento y/o de prueba adecuado con un modelo de aprendizaje automático.

La etapa S112 y/o cualquier otra parte adecuada del método 100 que puede emplear aprendizaje automático puede usar uno o más de: aprendizaje supervisado (por ejemplo, usando regresión logística, usando redes neuronales con retropropagación, usando bosques aleatorios, árboles de decisión, etc.), aprendizaje no supervisado (por ejemplo, usando un algoritmo a priori, usando agrupamiento de K medias), aprendizaje semisupervisado, aprendizaje con refuerzo (por ejemplo, usando un algoritmo de aprendizaje Q, usando aprendizaje con diferencia temporal), y cualquier otro tipo de aprendizaje adecuado. Cada módulo de la pluralidad puede implementar uno cualquiera o más de: un algoritmo de regresión (por ejemplo, mínimos cuadrados ordinarios, regresión logística, regresión escalonada, tramos de regresión adaptativa de múltiples variables, suavizado de diagrama de dispersión con estimación local, etc.), un método basado en casos (por ejemplo, k vecinos más cercanos, cuantificación de vectores de aprendizaje, mapa de autoorganización, etc.), un método de regularización (por ejemplo, regresión contraída, menor contracción absoluta y operador de selección, red elástica, etc.), un método de aprendizaje de árbol de decisión (por ejemplo, árbol de clasificación y regresión, dicotomizador iterativo 3, C4.5, detección con interacción automática de la chi cuadrado, muñón de decisión, bosque aleatorio, tramos de regresión adaptativa de múltiples variables, máquinas de refuerzo en gradiente, etc.), un método bayesiano (por ejemplo, Bayes ingenuo, factores de estimación monodependientes promediados, red de creencia bayesiana, etc.), un método de kernel (por ejemplo, una máquina de vectores de soporte, una función de base radial, un análisis discriminante lineal, etc.), un método de agrupamiento (por ejemplo, agrupamiento de k medias, maximización de la expectativa, etc.), un algoritmo de aprendizaje de reglas asociadas (por ejemplo, un algoritmo a priori, un algoritmo Eclat, etc.), un modelo de red neuronal artificial (por ejemplo, un método de perceptrón, un método de retropropagación, un método de red de Hopfield, un método de mapa de autoorganización, un método de cuantificación de vectores de aprendizaje, etc.), un algoritmo de aprendizaje profundo (por ejemplo, una máquina de Boltzmann restringida, un método de red de creencias profundas, un método de red de convolución, un método de autocodificadores apilados, etc.), un método de reducción de la dimensionalidad (por ejemplo, análisis de componentes principales, regresión de mínimos cuadrados parcial, mapeo de Sammon, ajuste a escala multidimensional, persecución de proyección, etc.), un método de conjunto (por ejemplo, refuerzo, agregación de arranque primario, AdaBoost, generalización apilada, método de máquina de refuerzo en gradiente, método de bosque aleatorio, etc.), y cualquier forma adecuada de algoritmo de aprendizaje automático. Cada parte de procesamiento del método 100 puede aprovechar adicional o alternativamente: un módulo probabilístico, módulo heurístico, módulo determinista, o cualquier otro módulo adecuado que aprovecha cualquier otro método de cálculo adecuado, método de aprendizaje automático o combinación de los mismos. Sin embargo, cualquier enfoque de aprendizaje automático adecuado puede incorporarse de otra manera en el método 100. Además, puede usarse cualquier modelo adecuado (por ejemplo, aprendizaje automático, aprendizaje no automático, etc.) en la generación de inteligencia de salud de punto final y/u otros datos relevantes para el método 100.

3.3 Modificar normas de salud de punto final.

La etapa S120 incluye modificar normas de salud de punto final. La etapa S120 funciona para modificar y/o crear normas de salud de punto final basándose en inteligencia de salud de punto final y/u otros datos de salud de punto final.

La modificación de normas de salud de punto final puede basarse en información proporcionada por un administrador, por un proveedor de seguridad (por ejemplo, un proveedor de un servicio de autenticación de dos factores), por un usuario, por una tercera parte (por ejemplo, un proveedor de navegador web) y/o cualquier otra entidad adecuada. Por ejemplo, modificar normas de salud de punto final puede incluir: recopilar información de seguridad (por ejemplo, a partir del creador de una aplicación) relacionada con una versión de la aplicación que funciona en el dispositivo de usuario de punto final; y actualizar las normas de salud de punto final (por ejemplo,

datos de salud de punto final esperados) basándose en la información de seguridad.

Las normas de salud de punto final pueden modificarse antes, durante o después de la recopilación de datos de salud de punto final como en la etapa S111 y/o cualquier otra parte adecuada del método 100. Por ejemplo, las normas de salud de punto final pueden actualizarse (por ejemplo, las normas pueden volverse más estrictas) en tiempo real en respuesta a que la generación de inteligencia de salud de punto final indique un alto riesgo de vulnerabilidad para un dispositivo de usuario de punto final que ha accedido recientemente a la red. Sin embargo, la modificación de normas de salud de punto final puede realizarse en cualquier momento adecuado.

Las normas de salud de punto final pueden modificarse en una interfaz de seguridad proporcionada a un administrador de red, a través de mensajes directos (por ejemplo, un administrador que responde a una notificación de salud de punto final), de manera automática (por ejemplo, actualizando automáticamente normas de salud de punto final basándose en inteligencia de salud de punto final recién generada), de manera manual y/o mediante cualquier medio adecuado.

En una primera variación de la etapa S120, las normas de salud de punto final pueden actualizarse basándose en vulnerabilidades identificadas. En un ejemplo, si se detecta una vulnerabilidad anteriormente desconocida (por ejemplo, examinando de manera heurística el tráfico de red) y la vulnerabilidad se correlaciona con un conjunto particular de datos de salud de punto final (por ejemplo, una versión de un navegador particular), pueden modificarse automáticamente las normas de salud de punto final para restringir el acceso a red para puntos finales correlacionados con ese conjunto de datos de salud de punto final (por ejemplo, puntos finales que ejecutan la versión de navegador particular). En un ejemplo específico, el método 100 puede incluir: actualizar automáticamente las normas de salud de punto final basándose en una vulnerabilidad identificada correlacionada con una propiedad de datos de salud de punto final, en el que generar la inteligencia de salud de punto final puede incluir comparar los datos de salud de punto final recopilados con la propiedad de datos de salud de punto final, y en el que notificar al administrador puede incluir notificar al primer administrador de la vulnerabilidad identificada en respuesta a que los datos de salud de punto final incluyan la propiedad de datos de salud de punto final. Sin embargo, la actualización de las normas de salud de punto final basándose en vulnerabilidades identificadas puede realizarse de cualquier manera adecuada.

En una segunda variación, las normas de salud de punto final pueden actualizarse basándose en el etiquetado de datos de salud de punto final como vulnerables. Los administradores de red etiquetan preferiblemente datos de salud de punto final como vulnerables o no vulnerables, pero cualquier entidad adecuada puede realizar el etiquetado. Como ejemplo, un administrador puede etiquetar determinados puntos finales como que son vulnerables o están comprometidos. La etapa S120 puede incluir analizar datos de salud de punto final a partir de estos puntos finales y modificar las normas de salud de punto final para restringir el acceso a red a puntos finales con características de datos de salud de punto final similares (alternativamente, la etapa S120 puede incluir simplemente preparar datos para notificar a un administrador de la similitud en los datos de salud de punto final). En un ejemplo específico, el método 100 puede incluir recibir, a partir de un administrador de red, un etiquetado de datos de salud de punto final como vulnerables; y actualizar automáticamente las normas de salud de punto final con los datos de salud de punto final y el etiquetado. Las normas de salud de punto final utilizadas por una red dada pueden actualizarse utilizando un etiquetado de vulnerabilidad de datos de salud de punto final asociados con cualquier red adecuada. Por ejemplo, el método 100 pude incluir: recibir, a partir de un segundo administrador de una primera red (por ejemplo, en el que el primer administrador es de una primera red), un etiquetado de los segundos datos de salud de punto final como vulnerables; y actualizar automáticamente las normas de salud de punto final con los segundos datos de salud de punto final, en el que las normas de salud de punto final pueden utilizarse en la generación de inteligencia de salud de punto final para dispositivos de usuario de punto final asociados con las redes primera y/o segunda. Sin embargo, la actualización de las normas de salud de punto final puede actualizarse basándose en el etiquetado de datos de salud de punto final de cualquier manera adecuada.

3.4 Generar una notificación

La etapa S130 incluye generar una notificación de salud de punto final, que funciona para generar una notificación que indica salud de punto final de uno o más dispositivos de usuario de punto final. La notificación de salud de punto final se genera preferiblemente a partir de la inteligencia de salud de punto final. Adicional o alternativamente, la notificación de salud de punto final puede incluir cualquier cantidad o combinación de: inteligencia de salud de punto final, normas de salud de punto final, datos de salud de punto final, información de usuario, información de red y/o cualquier otra información adecuada. Por ejemplo, generar la notificación de salud de punto final puede incluir generar una notificación de salud de punto final que incluye una alerta de vulnerabilidad, en respuesta a que los datos de salud de punto final no logren cumplir una norma de salud de punto final. La forma de notificaciones de salud de punto final puede incluir uno o más de: contenido verbal (por ejemplo, el dispositivo de usuario de punto final “A” está utilizando actualmente el navegador web “B”, etc.), contenido numérico (por ejemplo, el 80% de los usuarios en la red a lo largo de la última semana han utilizado el sistema operativo “X” en el acceso a la red, etc.), contenido gráfico (por ejemplo, una notificación destacada en rojo para ilustrar un alto nivel de riesgo de seguridad para un dispositivo de usuario de punto final, etc.), contenido de audio y/o cualquier otra forma adecuada.

La generación de una notificación de salud de punto final es preferiblemente en respuesta a la generación de inteligencia de salud de punto final. Además, la generación de la notificación de salud de punto final se realiza preferiblemente en tiempo real (por ejemplo, durante el intento de un usuario por autenticarse y acceder a red de área local). Adicional o alternativamente, pueden generarse notificaciones de salud de punto final a intervalos de tiempo especificados (por ejemplo, cada hora, cada día, cada semana, etc.), determinarse manualmente (por ejemplo, en respuesta a que un administrador pida inteligencia de salud de punto final), determinarse automáticamente (por ejemplo, en respuesta a que un nivel de vulnerabilidad de un dispositivo de usuario de punto final o una red supere un nivel de vulnerabilidad umbral) y/o generarse de otro modo. Sin embargo, la generación de una notificación de salud de punto final puede realizarse en cualquier momento adecuado.

La generación de una notificación de salud de punto final se realiza preferiblemente mediante la misma entidad (por ejemplo, un servidor remoto) que genera inteligencia de salud de punto final. Sin embargo, las notificaciones de salud de punto final pueden realizarse parcial o totalmente mediante cualquier entidad adecuada.

Puede generarse cualquier número de notificaciones de salud de punto final para cualquier número o tipo de entidad. Por ejemplo, pueden generarse notificaciones de salud de punto final para un administrador de red, para un usuario, para una tercera parte y/u otras entidades adecuadas. En un ejemplo específico, se genera la misma notificación de salud de punto final para diferentes entidades (por ejemplo, una misma notificación de salud de punto final para un usuario y un administrador). Sin embargo, la generación de la notificación de salud de punto final puede realizarse de cualquier manera adecuada.

En una primera variación, las notificaciones de salud de punto final generadas pueden presentarse en una interfaz de seguridad para un administrador de red y/o usuario. La interfaz de seguridad puede ser accesible a través de Internet (por ejemplo, una interfaz web), en una aplicación que funciona en un dispositivo de administrador y/o en cualquier componente adecuado. Por ejemplo, el método 100 puede incluir proporcionar una interfaz de seguridad para un administrador de red, siendo la interfaz de seguridad accesible a través de Internet, en el que notificar al administrador comprende presentar, a través de un enlace de comunicación inalámbrico con un dispositivo de administrador asociado con el administrador, la notificación de salud de punto final en la interfaz de seguridad. Sin embargo, una interfaz de seguridad para presentar notificaciones de salud de punto final puede configurarse de cualquier manera adecuada.

En una segunda variación, las notificaciones de salud de punto final pueden incluir opciones de respuesta para administradores, usuarios y/u otras entidades adecuadas que reciben notificaciones de salud de punto final. Las opciones de respuesta pueden incluir opciones para: actualizar modelos para generar inteligencia de salud de punto final, verificar inteligencia de salud de punto final (por ejemplo, verificar la exactitud de inteligencia de salud de punto final), modificar normas de salud de punto final, modificar políticas de acceso a red, actualizar software que funciona en un dispositivo de usuario de punto final y/o cualquier otra opción adecuada. Las opciones de respuesta pueden presentarse en la notificación de salud de punto final, en la interfaz de seguridad y/o en cualquier componente adecuado. Sin embargo, las opciones de respuesta para realizar acciones relacionadas con la salud de punto final pueden configurarse de cualquier manera adecuada.

3.5 Notificar a un administrador

La etapa S132 incluye proporcionar inteligencia de salud de punto final a administradores. La etapa S132 funciona para proporcionar a administradores (por ejemplo, administradores de red, administradores de servicio, etc.) inteligencia de salud de punto final generada en la etapa S112. Notificar a un administrador incluye preferiblemente notificar a un administrador de una red con una notificación de salud de punto final generada en la etapa S130. Adicional o alternativamente, pueden utilizarse otros tipos de notificaciones en la notificación de un administrador.

La etapa S132 incluye preferiblemente proporcionar a administradores informes de salud de punto final en un panel de administrador; por ejemplo, tal como se muestra en la sección de “acceso” de la figura 6. Adicional o alternativamente, la etapa S132 puede incluir proporcionar inteligencia de salud de punto final a administradores de cualquier manera adecuada (por ejemplo, enviando correos electrónicos de informe agregado una vez al día, enviando notificaciones automáticas al teléfono de un administrador tras un acontecimiento de autenticación de red insatisfactorio, etc.).

La etapa S132 está preferiblemente integrada con una interfaz que permite a los administradores crear normas de salud de punto final y vincular esas normas con políticas de acceso a red específicas; por ejemplo, tal como se muestra en la figura 7. La etapa S132 puede incluir adicional o alternativamente proporcionar cualquier dato de salud de punto final (o inteligencia generada a partir de datos de salud de punto final) a administradores de cualquier manera.

Tal como se comentó anteriormente, la inteligencia de punto final puede incluir informes para acontecimientos específicos (por ejemplo, inicio de sesión satisfactorio o fallido), puntos finales específicos, grupos de puntos finales, la red en su conjunto y/o para cualquier otro objeto adecuado. Por ejemplo, un administrador puede recibir notificación de un posible riesgo de seguridad a través de una interfaz tal como se muestra en la figura 8. Sin

embargo, la notificación a un administrador puede realizarse de cualquier otra manera adecuada.

3.6 Notificar a un usuario

La etapa S134 incluye proporcionar inteligencia de salud de punto final a usuarios de punto final. La etapa S134 funciona para informar a usuarios de información de salud de punto final; en particular, la etapa S134 incluye preferiblemente informar a usuarios si un punto final es vulnerable, pero la etapa S134 puede incluir adicional o alternativamente proporcionar a usuarios cualquier información de salud de punto final para un punto final dado (o para otros puntos finales asociados con el usuario). Notificar a un usuario incluye preferiblemente notificar al usuario con una notificación de salud de punto final generada en la etapa S130. Adicional o alternativamente, pueden utilizarse otros tipos de notificaciones en la notificación a un usuario.

Por ejemplo, tal como se muestra en la figura 9, la etapa S134 puede incluir notificar a un usuario si software en el punto final del usuario está desactualizado. La etapa S134 puede incluir adicional o alternativamente proporcionar a usuarios recursos para resolver vulnerabilidades (por ejemplo, enlaces a parches). La etapa S134 también puede incluir proporcionar a usuarios una opción para resolver automáticamente la vulnerabilidad (por ejemplo, el método 100 puede incluir descargar e instalar un parche de OS a petición del usuario) o para pedir ayuda de un administrador o miembro del personal de asistencia técnica.

En una variación, notificar a un usuario puede incluir notificar a un usuario en el dispositivo de usuario de punto final a través del iframe. Por ejemplo, un usuario puede estar interactuando con una aplicación web implementada con un iframe que recopiló datos de usuario de punto final y/o realiza autenticación de usuario. Puede utilizarse el mismo iframe para notificar a un usuario con una notificación de salud de punto final.

Sin embargo, la notificación a un usuario puede realizarse de cualquier otra manera adecuada

3.7 Establecer políticas de acceso a red

La etapa S140 incluye establecer políticas de acceso a red. La etapa S140 funciona para establecer políticas de acceso a red para puntos finales basándose en cómo se evalúan los datos de salud de punto final con respecto a normas de salud de punto final y políticas de acceso a red asociadas con esas normas de salud de punto final. Las políticas de acceso a red pueden incluir reglas que determinan si se permite que un punto final se conecte a una red, qué clase de conexión puede tener el punto final con la red (por ejemplo, a través de qué VLAN, si la hay; a través de qué puertos, etc.), a qué servicios y/o puertos puede acceder el punto final en la red, a qué datos puede acceder el punto final en la red, ajustes de calidad de servicio (QOS), etc.

El establecimiento de políticas de acceso a red puede realizarse en tiempo real y/o en cualquier momento adecuado en relación con cualquier parte del método.

La etapa S140 incluye preferiblemente establecer políticas de acceso a red según reglas determinadas por administradores (por ejemplo, tal como se muestra en la figura 7, en una interfaz de seguridad proporcionada, etc.), pero puede incluir adicional o alternativamente establecer políticas de acceso a red basándose en reglas derivadas de manera automática (por ejemplo, como parte de la etapa S120). Por ejemplo, la etapa S140 puede incluir bloquear el acceso a red para puntos finales que muestran una vulnerabilidad descubierta mediante la etapa S120 hasta que esté disponible una intervención de administrador. En otro ejemplo, la etapa S140 puede incluir establecer una política de acceso a red para una red basándose en inteligencia de salud de punto final generada para un dispositivo de usuario de punto final que intenta acceder a la red.

La etapa S140 puede incluir establecer políticas de acceso a red basándose en información adicional, tal como tiempo y/o recuento de acontecimientos. Por ejemplo, la etapa S140 puede incluir establecer una política de acceso a red que permite a un usuario con software desactualizado acceder a la red durante 48 horas; se notifica al usuario de que dispone de 48 horas para actualizar su software (tiempo tras el cual se bloqueará el punto final si el software no se ha actualizado). Igualmente, la etapa S140 puede incluir establecer una política de acceso a red que permite a un usuario con software desactualizado iniciar sesión en la red un número limitado de veces antes de bloquearse. Sin embargo, pueden establecerse políticas de acceso a red según cualquier criterio adecuado. Además, el establecimiento de políticas de acceso a red puede realizarse de cualquier manera adecuada.

El método de la realización preferida y variaciones del mismo pueden realizarse y/o implementarse al menos en parte como una máquina configurada para recibir un medio legible por ordenador que almacena instrucciones legibles por ordenador. Las instrucciones se ejecutan preferiblemente mediante componentes ejecutables por ordenador preferiblemente integrados con un servicio de monitorización de salud de punto final. El medio legible por ordenador puede almacenarse en cualquier medio legible por ordenador adecuado tal como RAM, ROM, memoria flash, EEPROM, dispositivos ópticos (CD o DVD), discos duros, discos flexibles o cualquier dispositivo adecuado. El componente ejecutable por ordenador es preferiblemente un procesador general o específico de aplicación, pero cualquier dispositivo de combinación de hardware/firmware o hardware dedicado adecuado puede alternativa o adicionalmente ejecutar las instrucciones.

Tal como reconocerá un experto en la técnica a partir de la descripción detallada anterior y a partir de las figuras y reivindicaciones, pueden realizarse modificaciones y cambios a las realizaciones preferidas de la invención.

REIVINDICACIONES

1. Método para aplicar normas referentes a vulnerabilidades de seguridad para un dispositivo de usuario de punto final asociado con un usuario, comprendiendo el método:

• en un servidor remoto, implementar un marco incorporado;

• integrar el marco incorporado dentro de una aplicación web, en el que la aplicación web comprende una aplicación accesible a través de Internet;

• recopilar de manera activa datos de salud de punto final asociados con un dispositivo de usuario de punto final en el marco incorporado incluyendo transmitir sondas de datos de salud de punto final para pedir los datos de salud de punto final, comprendiendo el dispositivo de usuario de punto final un dispositivo de usuario de punto final sin agente, mediante lo cual la recopilación de los datos de salud de punto final a través del marco incorporado que se implementa por el servidor remoto se realiza sin instalar una aplicación de agente en el dispositivo de usuario de punto final, pidiendo las sondas de datos de salud de datos de punto final de salud de punto final a partir de una o más aplicaciones distintas de agente o servicios distintos de agente que funcionan con el dispositivo de usuario de punto final;

• recopilar, en el marco incorporado, los datos de salud de punto final del dispositivo de usuario de punto final en respuesta a que el usuario interactúe con la aplicación web a través del dispositivo de usuario de punto final, en el que recopilar los datos de salud de punto final comprende:

• recibir, en el marco incorporado, una cabecera de agente de usuario de HTTP que comprende (i) un tipo de sistema operativo y (ii) una versión de sistema operativo del dispositivo de usuario de punto final, en el que los datos de salud de punto final comprenden el tipo de sistema operativo y la versión de sistema operativo;

• generar una comparación de los datos de salud de punto final del dispositivo de usuario de punto final y normas de salud de punto final, comprendiendo las normas de salud de datos de punto final de salud de punto final esperados, en el que generar la comparación comprende:

• comparar el tipo de sistema operativo y la versión de sistema operativo del dispositivo de usuario de punto final con datos de salud de punto final históricos del dispositivo de usuario de punto final;

• generar inteligencia de salud de punto final a partir de la comparación de los datos de salud de punto final y las normas de salud de punto final, indicando la inteligencia de salud de punto final salud de seguridad de punto final del dispositivo de usuario de punto final;

• generar una primera notificación de salud de punto final a partir de la inteligencia de salud de punto final; y

• notificar a un primer administrador de una red informática con la notificación de salud de punto final.

2. Método según la reivindicación 1, en el que generar la inteligencia de salud de punto final comprende generar la inteligencia de salud de punto final basándose en el tipo de sistema operativo y la versión de sistema operativo.

3. Método según la reivindicación 2, en el que recopilar, en el marco incorporado, los datos de salud de punto final incluye recopilar primeros datos de salud de punto final que comprende extraer, en el marco incorporado, el tipo de sistema operativo y la versión de sistema operativo a partir de la cabecera de agente de usuario de HTTP.

4. Método según la reivindicación 1, en el que recopilar los datos de salud de punto final incluye realizar, en el marco incorporado, la toma de huellas digitales del dispositivo de usuario de punto final sin agente para recopilar propiedades de hardware del dispositivo de usuario de punto final sin agente, comprendiendo los datos de salud de punto final las propiedades de hardware.

5. Método según la reivindicación 1, en el que recopilar los datos de salud de punto final comprende recopilar propiedades de hardware del dispositivo de usuario de punto final sin agente; en el que el método comprende además generar un perfil de dispositivo de punto final a partir de las propiedades de hardware; en el que generar inteligencia de salud de punto final comprende generar inteligencia de salud de punto final a partir del perfil de dispositivo de punto final.

6. Método según la reivindicación 1, que comprende además:

• recopilar información de seguridad relacionada con una versión de una aplicación que funciona en el dispositivo de usuario de punto final sin agente; y

• actualizar los datos de salud de punto final esperados basándose en la información de seguridad.

7. Método según la reivindicación 1, que comprende además:

• recopilar, en el marco incorporado, segundos datos de salud de punto final de un segundo dispositivo de usuario de punto final en respuesta a que un segundo usuario interactúe con la aplicación web a través del segundo dispositivo de usuario de punto final;

• generar segunda inteligencia de salud de punto final a partir de los segundos datos de salud de punto final;

• generar una segunda notificación de salud de punto final que comprende la segunda inteligencia de salud de punto final; y

• notificar a un segundo administrador de una segunda red con la segunda notificación de salud de punto final.

8. Método según la reivindicación 1, en el que comparar los primeros datos de salud de punto final con las normas de salud de punto final comprende:

• generar una indicación de vulnerabilidad usando un modelo de aprendizaje automático generado a partir de las normas de salud de punto final, en el que la indicación de vulnerabilidad está asociada con los primeros datos de salud de punto final, y en el que la primera notificación de salud de punto final comprende la indicación de vulnerabilidad.

9. Método según la reivindicación 8, que comprende además:

• recibir, a partir del primer administrador, una verificación de la indicación de vulnerabilidad; y

• actualizar el modelo de aprendizaje automático con los primeros datos de salud de punto final y la verificación.

10. Método según la reivindicación 1, en el que generar la inteligencia de salud de punto final comprende generar una comparación entre los primeros datos de salud de punto final y segundos datos de salud de punto final de un segundo dispositivo de usuario de punto final, y en el que la primera notificación de salud de punto final comprende la comparación entre los primeros datos de salud de punto final y los segundos datos de salud de punto final.

11. Método según la reivindicación 10, en el que el segundo dispositivo de usuario de punto final está asociado con un segundo usuario.

12. Método según la reivindicación 1, en el que generar la inteligencia de salud de punto final comprende identificar una vulnerabilidad de seguridad asociada con los primeros datos de salud de punto final, y en el que la primera notificación de salud de punto final comprende una indicación de la vulnerabilidad de seguridad.

13. Método según la reivindicación 1, que comprende además implementar el marco incorporado con la aplicación web, en el que el marco incorporado se usa para autenticar al usuario, y en el que recopilar los datos de salud de punto final comprende recopilar los datos de salud de punto final únicamente en el marco incorporado.

14. Método según la reivindicación 1, que comprende además proporcionar una interfaz de seguridad con el primer administrador, siendo la interfaz de seguridad accesible a través de Internet, en el que notificar al primer administrador comprende presentar, a través de un enlace de comunicación inalámbrico con un dispositivo de administrador asociado con el primer administrador, la primera notificación de salud de punto final en la interfaz de seguridad.

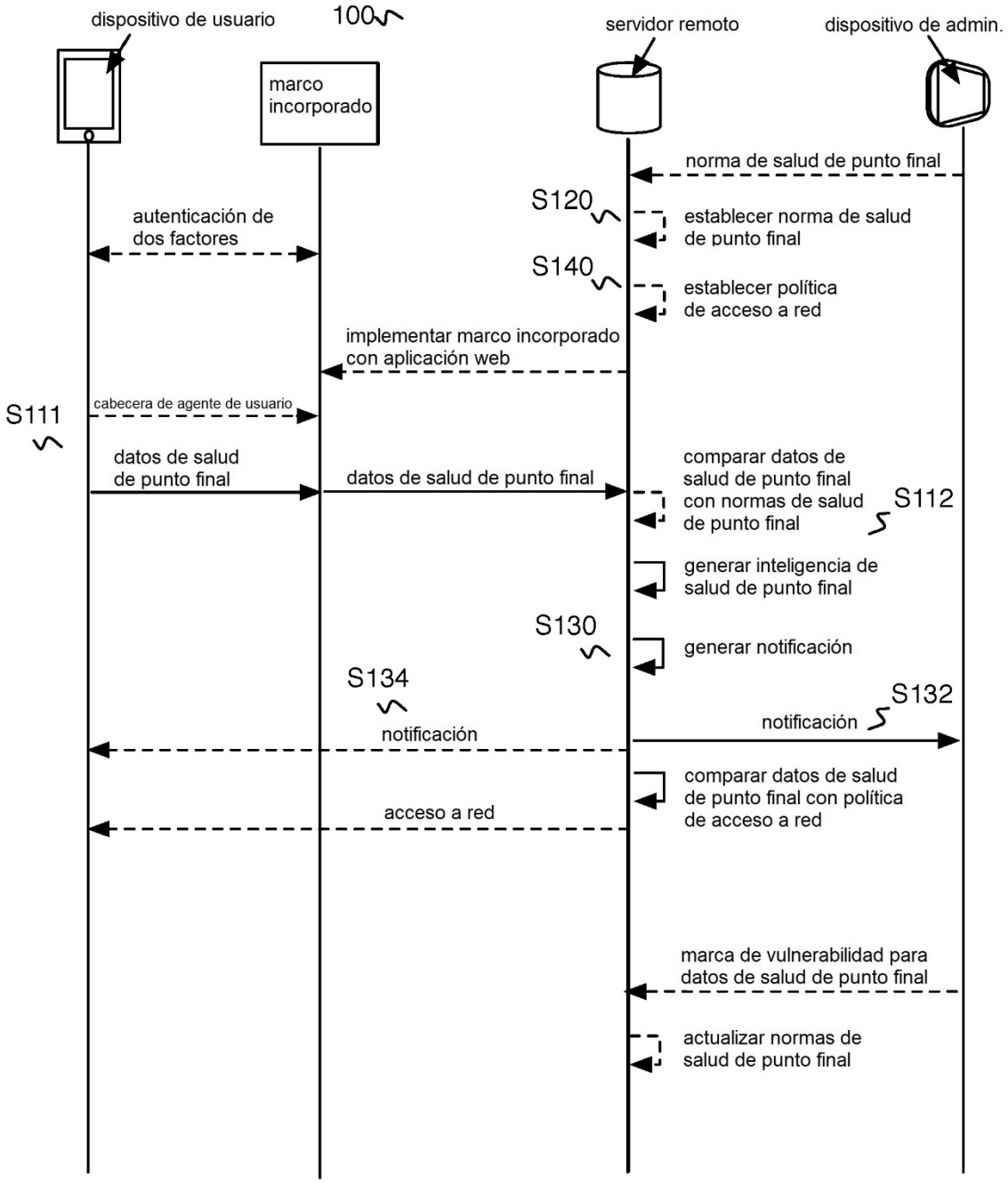
dispositivo de usuario
100
marco incorporado
servidor remoto
dispositivo de admin.
norma de salud de punto final
S120
establecer norma de salud de punto final
autenticación de dos factores
S140
establecer política de acceso a red
implementar marco incorporado con aplicación web
S111
cabecera de agente de usuario
datos de salud de punto final
datos de salud de punto final
comparar datos de salud de punto final con normas de salud de punto final
S112
generar inteligencia de salud de punto final
S130
generar notificación
S134
S132
notificación
notificación
comparar datos de salud de punto final con política de acceso a red
acceso a red
marca de vulnerabilidad para datos de salud de punto final
actualizar normas de salud de punto final

FIGURA 1

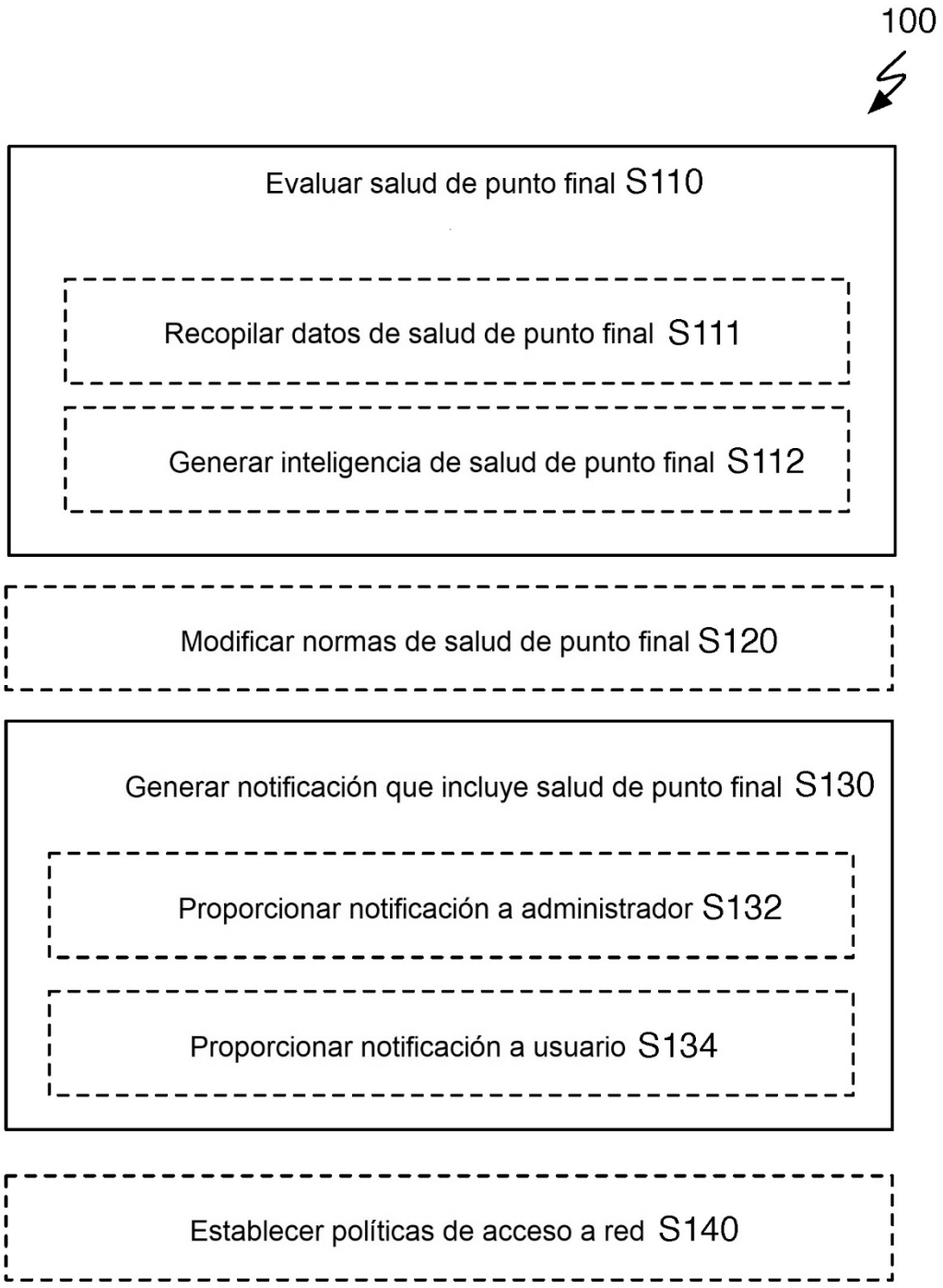
100
Evaluar salud de punto final S110
Recopilar datos de salud de punto final S111
Generar inteligencia de salud de punto final S112
Modificar normas de salud de punto final S120
Generar notificación que incluye salud de punto final S130
Proporcionar notificación a administrador S132
Proporcionar notificación a usuario S134
Establecer políticas de acceso a red S140

FIGURA 2

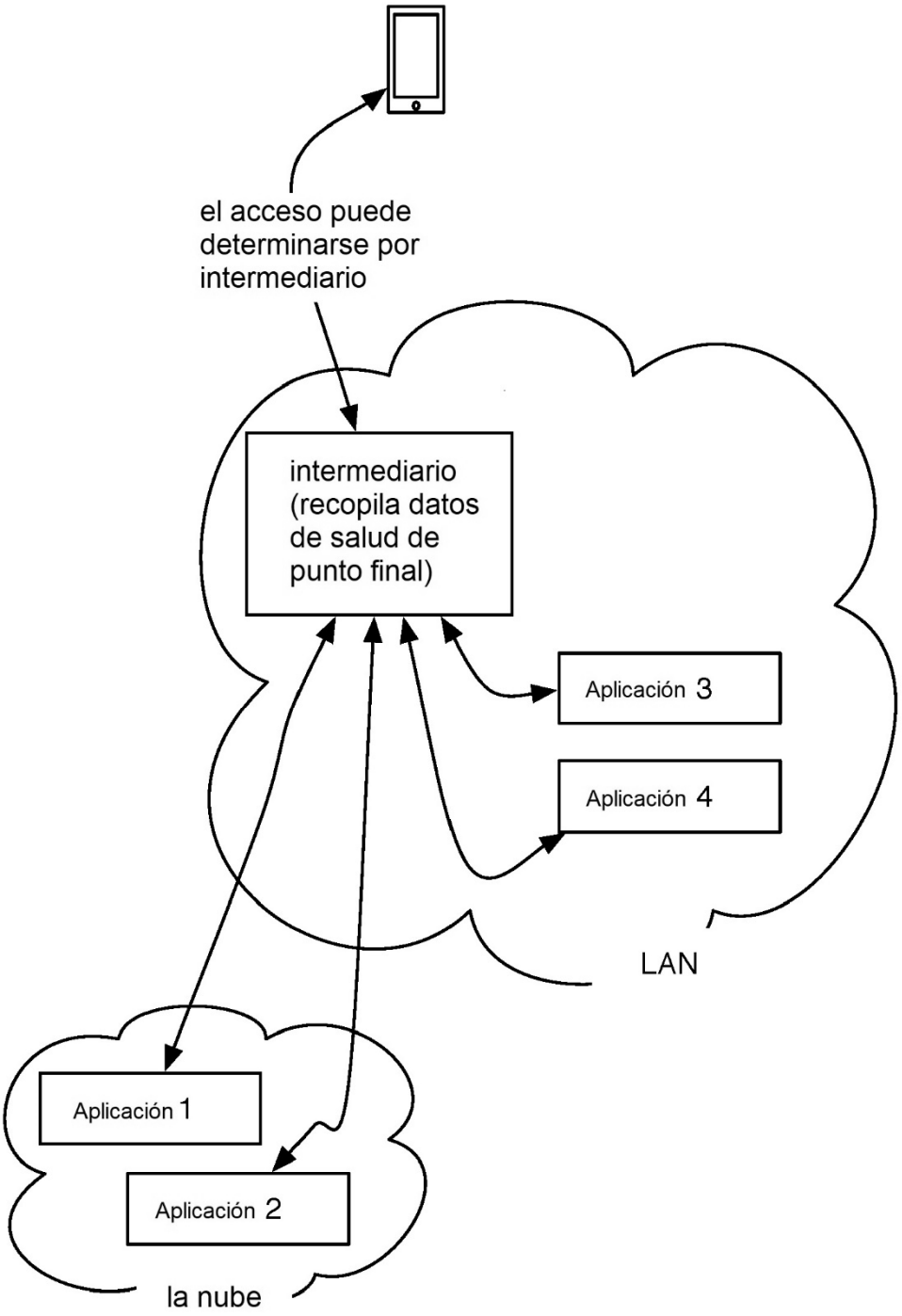
el acceso puede determinarse por intermediario
intermediario (recopila datos de salud de punto final)
Aplicación 3
Aplicación 4
LAN
Aplicación 1
Aplicación 2
la nube

FIGURA 3

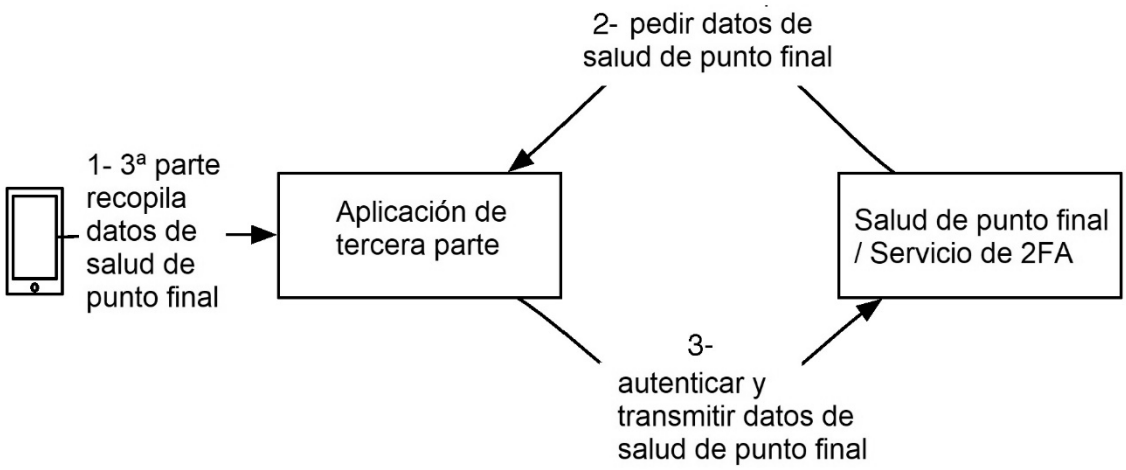

FIGURA 4A

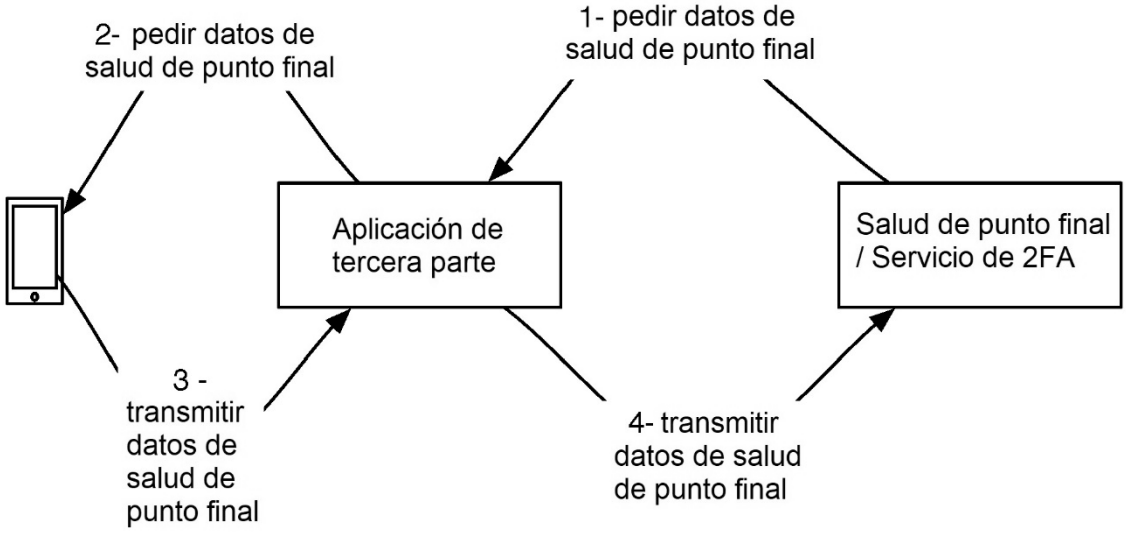

FIGURA 4B

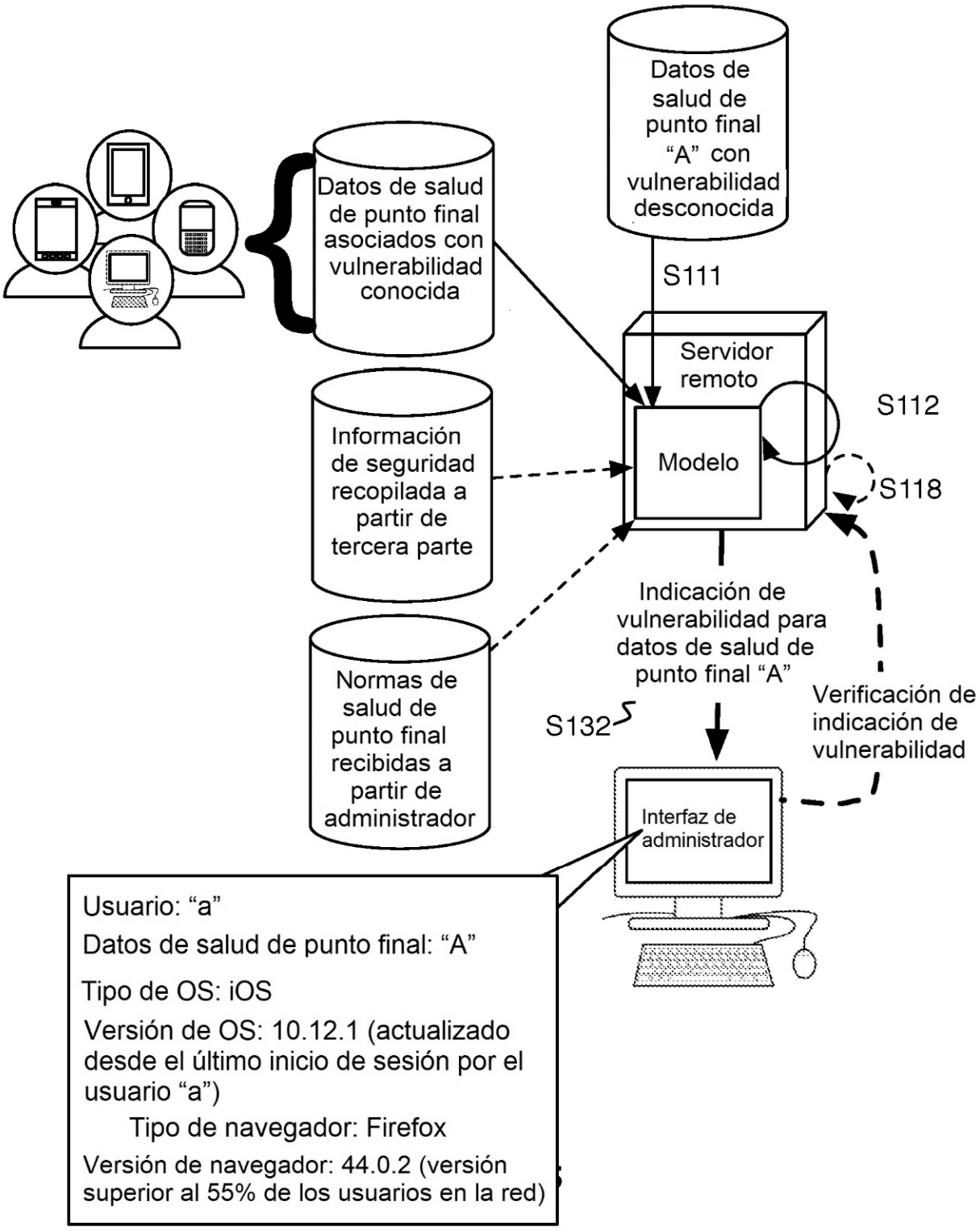
Datos de salud de punto final "A" con vulnerabilidad desconocida
Datos de salud de punto final asociados con vulnerabilidad conocida
S111
Servidor remoto
S112
Información de seguridad recopilada a partir de tercera parte
Modelo
S118
Indicación de vulnerabilidad para datos de salud de punto final "A"
Verificación de indicación de vulnerabilidad
Normas de salud de punto final recibidas a partir de administrador
S132
Interfaz de administrador
Usuario: "a"
Datos de salud de punto final: "A"
Tipo de OS: iOS
Versión de OS: 10.12.1 (actualizado desde el último inicio de sesión por el usuario "a")
Tipo de navegador: Firefox
Versión de navegador: 44.0.2 (versión superior al 55% de los usuarios en la red)

FIGURA 5

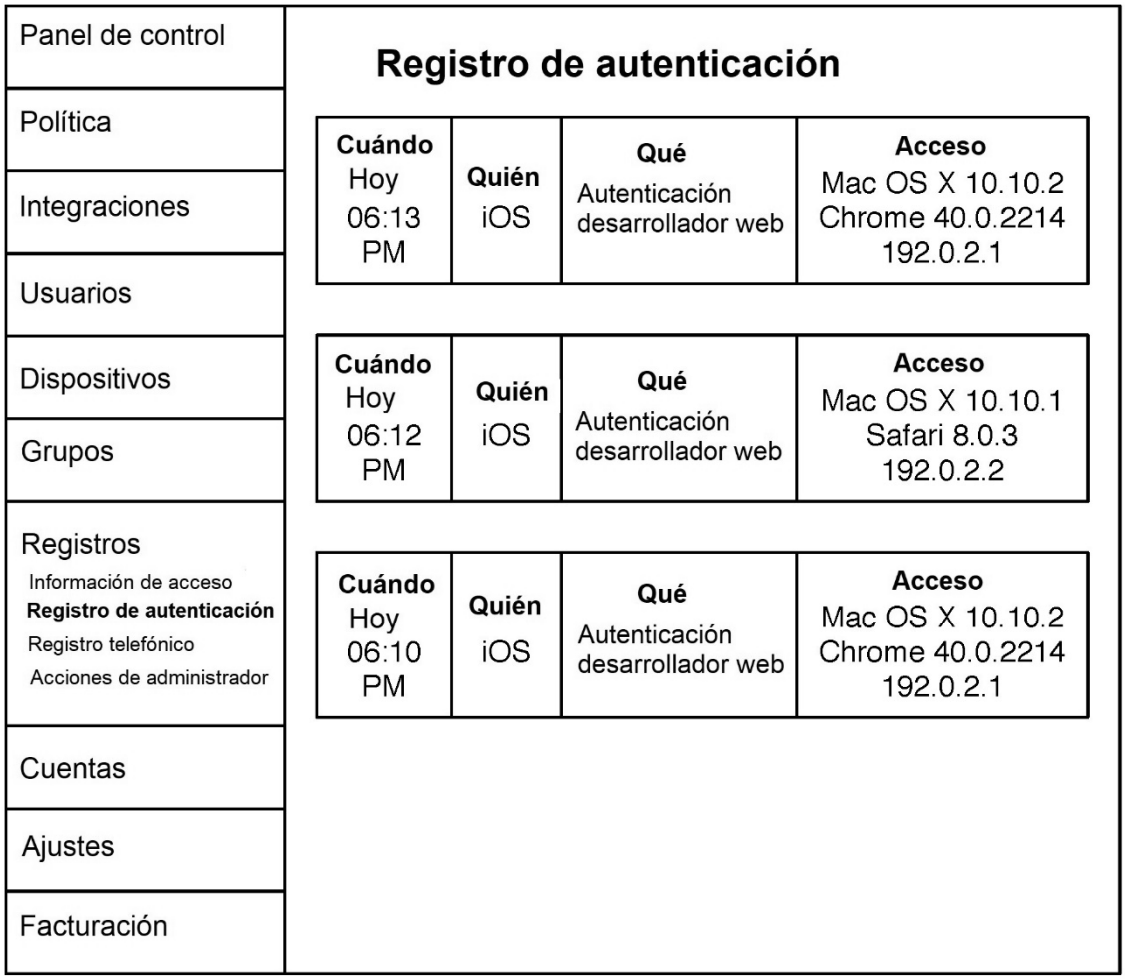
Panel de control
Política
Integraciones
Usuarios
Dispositivos
Grupos
Registros
Información de acceso
Registro de autenticación
Registro telefónico
Acciones de administrador
Cuentas
Ajustes
Facturación
Registro de autenticación
Cuándo Hoy 06:13 PM
Quién iOS
Qué Autenticación desarrollador web
Acceso Mac OS X 10.10.2 Chrome 40.0.2214 192.0.2.1
Cuándo Hoy 06:12 PM
Quién iOS
Qué Autenticación desarrollador web
Acceso Mac OS X 10.10.1 Safari 8.0.3 192.0.2.2
Cuándo Hoy 06:10 PM
Quién iOS
Qué Autenticación desarrollador web
Acceso Mac OS X 10.10.2 Chrome 40.0.2214 192.0.2.1

FIGURA 6

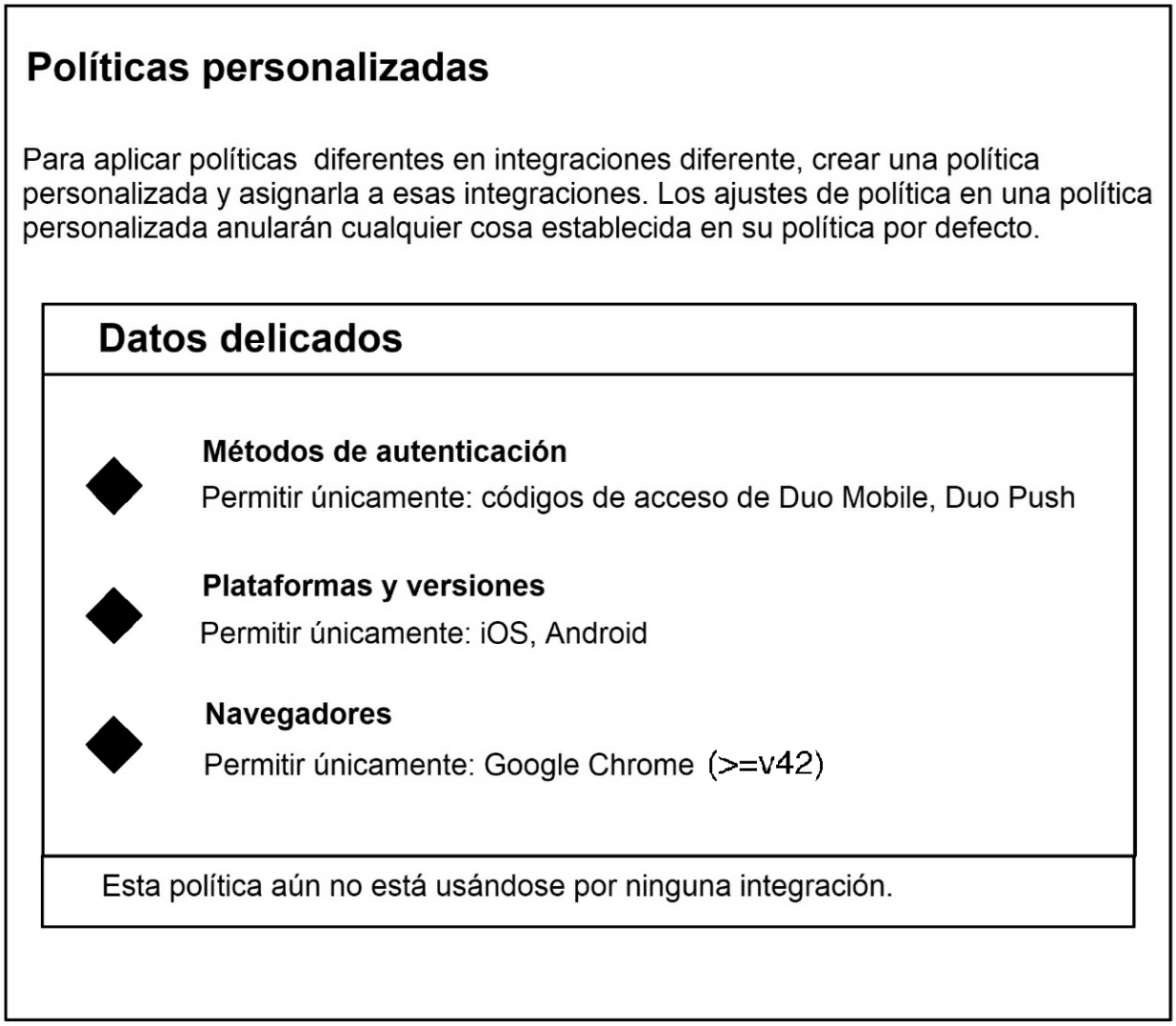
Políticas personalizadas
Para aplicar políticas diferentes en integraciones diferente, crear una política personalizada y asignarla a esas integraciones. Los ajustes de política en una política personalizada anularán cualquier cosa establecida en su política por defecto.
Datos delicados
Métodos de autenticación
Permitir únicamente: códigos de acceso de Duo Mobile, Duo Push
Plataformas y versiones
Permitir únicamente: iOS, Android
Navegadores
Permitir únicamente: Google Chrome (>=v42)
Esta política aún no está usándose por ninguna integración.

FIGURA 7

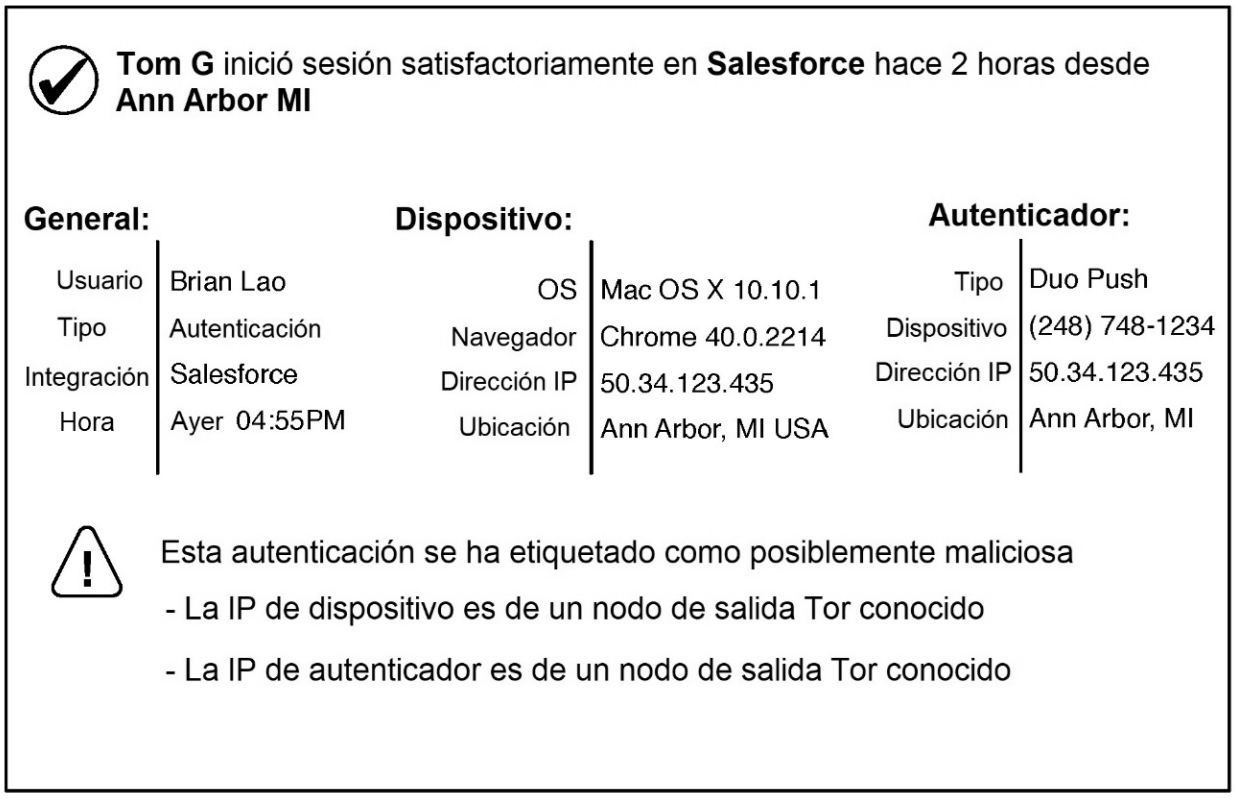
Tom G inició sesión satisfactoriamente en Salesforce hace 2 horas desde Ann Arbor MI
General:
Usuario Brian Lao
Tipo Autenticación
Integración Salesforce
Hora Ayer 04:55PM
Dispositivo:
OS Mac OS X 10.10.1
Navegador Chrome 40.0.2214
Dirección IP 50.34.123.435
Ubicación Ann Arbor, MI USA
Autenticador:
Tipo Duo Push
Dispositivo (248) 748-1234
Dirección IP 50.34.123.435
Ubicación Ann Arbor, MI
Esta autenticación se ha etiquetado como posiblemente maliciosa
- La IP de dispositivo es de un nodo de salida Tor conocido
- La IP de autenticador es de un nodo de salida Tor conocido

FIGURA 8

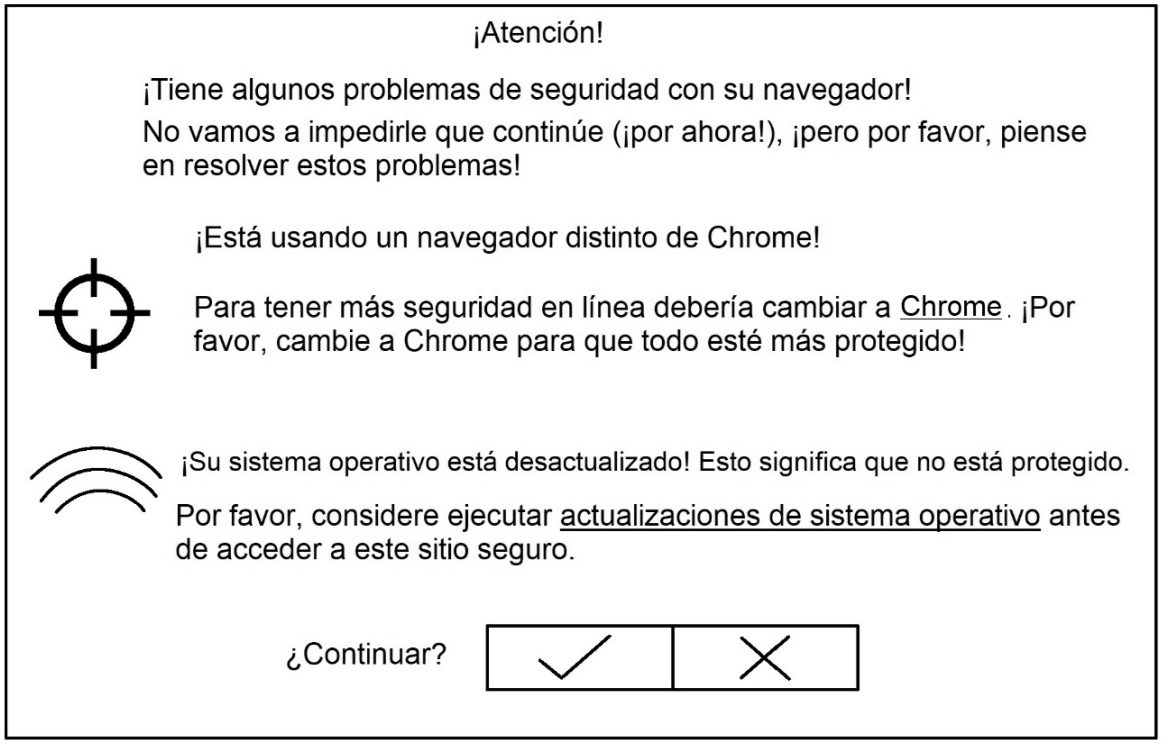
¡Atención!
¡Tiene algunos problemas de seguridad con su navegador!
No vamos a impedirle que continúe (¡por ahora!), ¡pero por favor, piense en resolver estos problemas!
¡Está usando un navegador distinto de Chrome!
Para tener más seguridad en línea debería cambiar a Chrome. ¡Por favor, cambie a Chrome para que todo esté más protegido!
¡Su sistema operativo está desactualizado! Esto significa que no está protegido.
Por favor, considere ejecutar actualizaciones de sistema operativo antes de acceder a este sitio seguro.
¿Continuar?

FIGURA 9