ManageEngine
DataSecurity Plus

Arquitectura

www.datasecurityplus.com

Acerca de DataSecurity Plus

ManageEngine DataSecurity Plus es una plataforma de visibilidad y segurid datos en tiempo real basada en la web. Consta de cinco módulos:

Auditoría de archivos

El módulo de Auditoría de Archivos supervisa las modificaciones y el movimiento d archivos en los servidores de archivos, failover clusters y las estaciones de trabajo alertas en tiempo real en caso de actividades de archivos sospechosas o críticas, respuestas con scripts para detener la propagación del ransomware.

Análisis de archivos

Con el análisis de archivos, los usuarios pueden recuperar el control del almacena de archivos de la empresa mediante la supervisión del crecimiento del almacenam localización de archivos basura, obsoletos y no comerciales, la gestión de archivos duplicados y la identificación de problemas de higiene de permisos, como los perm rotos y los archivos que permiten el acceso abierto.

Evaluación del riesgo de los datos

El módulo de evaluación del riesgo de los datos agiliza el cumplimiento de múltiple mandatos normativos mediante la localización de archivos que contienen datos pe sensibles (PII, PCI y ePHI). Ayuda a analizar la vulnerabilidad y el riesgo asociado esos archivos, a clasificarlos en consecuencia y, por tanto, a permitir el uso seguro archivos críticos.

Prevención de pérdida de datos (DLP)

El módulo DLP audita la actividad de los archivos en las estaciones de trabajo y supervisa las acciones de copia de archivos en dispositivos de almacenamiento ex También ayuda a detectar a los usuarios que adjuntan archivos confidenciales al c electrónico de Outlook, y a frustrar los intentos de robo de datos confidenciales a t de USB, Outlook, impresoras, aplicaciones web, etc.

Protección en la nube

Con el módulo de protección en la nube, los usuarios pueden supervisar el tráfico la empresa, analizar el uso de aplicaciones invisibles, ver las reputaciones web y a políticas para proteger a los empleados contra contenidos web inapropiados o mal

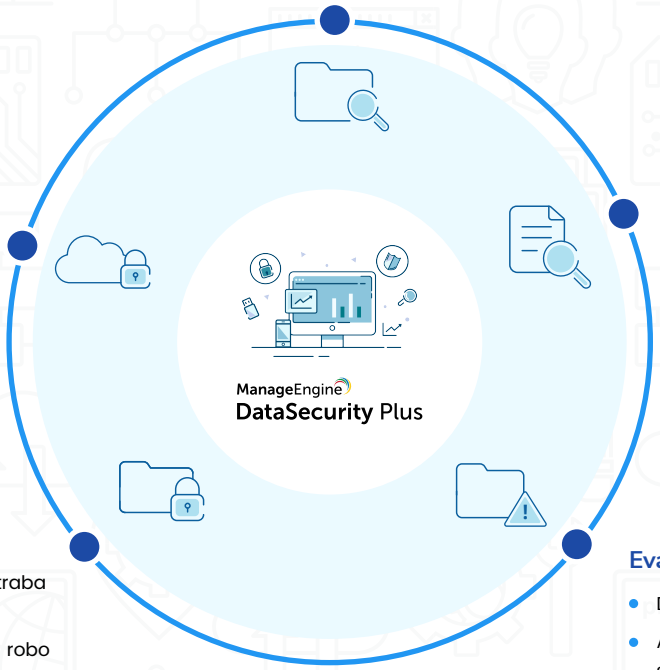
Arquitectura de la plataforma de visibilidad y seguridad de datos

Auditoría de archivos

- Auditoría de archivos en tiempo real y FIM
- Detección y respuesta al ransomware
- Auditoría de cumplimiento y presentación de informes

Protección en la nube

- Supervisión del uso de aplicaciones en la nube
- Descubrimiento y análisis de T invisible
- Lista blanca y lista negra de aplicaciones



Análisis de archivos

- Análisis del uso del disco y de los permisos
- Detección de la vulnerabilidad d los permisos
- Detección y deduplicación de archivos basura

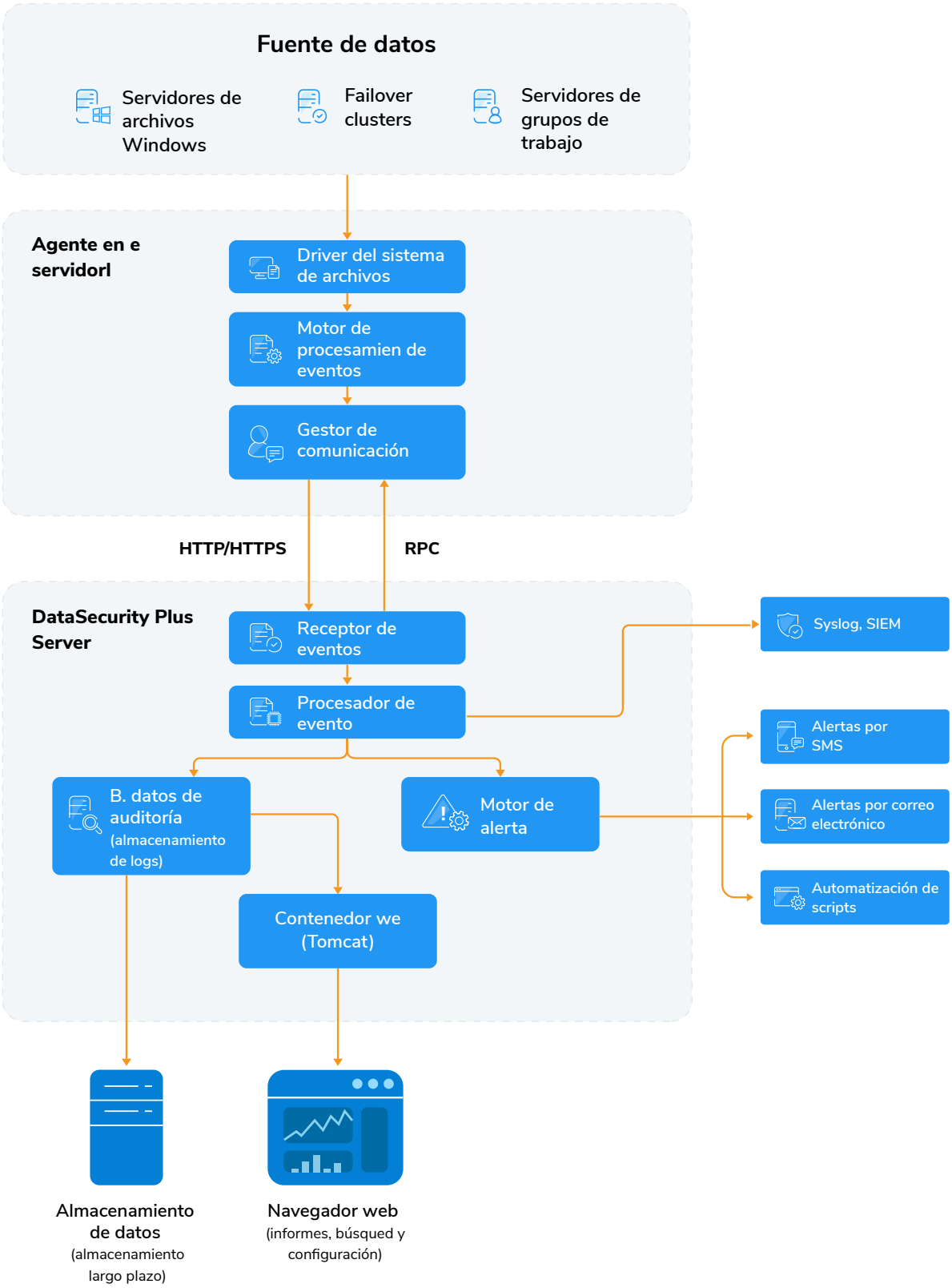
Prevención de la pérdida de datos

- Auditoría de estaciones de traba y archivos USB
- Detección e interrupción del robo de datos
- Políticas y estrategias de DLP integradas

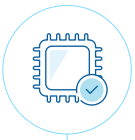
Evaluación del riesgo de los datos

- Descubrimiento de datos sensibl
- Análisis de seguridad de los archivos sensibles
- Calificación dinámica del riesgo

Módulo de auditoría de archivos



Componentes del módulo de Auditoría de Archivos:



Procesador de eventos

Aquí se procesan todos los eventos que se obtienen de la red antes de que s almacenen en la base de datos o se active la alerta correspondiente. Filtra los innecesarios -configurados por el administrador- y normaliza los logs sin proc formatos estándar.

Motor de alerta

Basándose en las reglas configuradas, el motor de alertas automatiza las res pasivas, como el envío de notificaciones por correo electrónico y la ejecución archivos por lotes.

Base de datos de auditoría

DataSecurity Plus incluye una base de datos PostgreSQL que almacena la información de los eventos sin procesar y normalizados de las fuentes de dat configuradas.

Agente DataSecurity Plus

El software implementa un agente ligero en cada servidor de archivos, failove cluster y servidor de grupo de trabajo monitoreado. El agente utiliza un driver minifiltro de Windows para auditar las actividades de los archivos, y la API de Windows para analizar las propiedades de los archivos.

Componentes externos

Consola

Se puede acceder a la interfaz web de DataSecurity Plus a través de un nave (Internet Explorer 9 y superior, Mozilla Firefox, Google Chrome (recomendado Microsoft Edge), y se conecta al componente de servidor web de Tomcat que escucha en el puerto número 8800 por defecto.

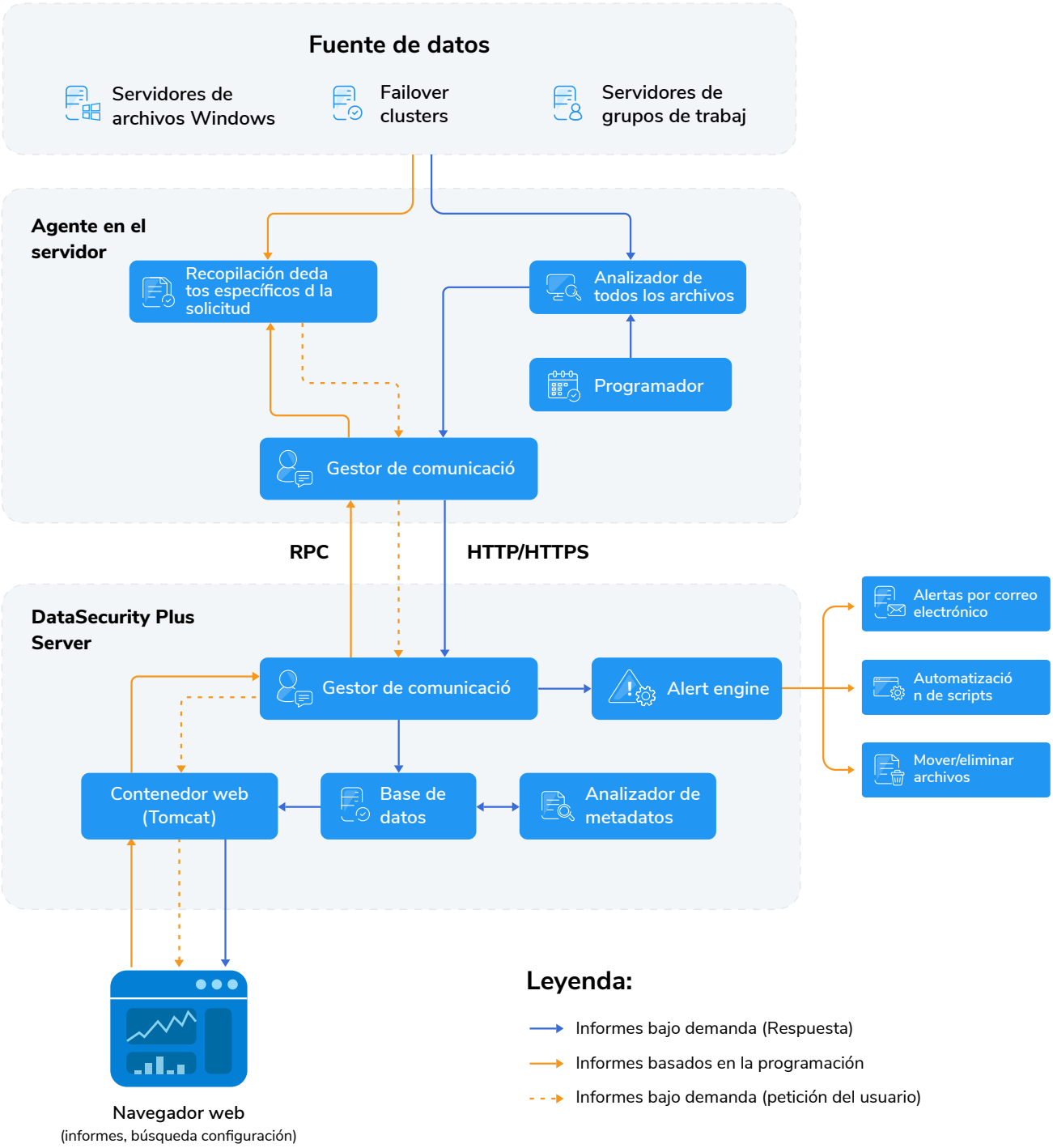
Reenvío de SIEM

DataSecurity Plus le permite reenviar todos los datos de auditoría del servido archivos a su servidor syslog o a Splunk para su posterior análisis.

Alerta por correo electrónico

Para el envío de correos electrónicos de alerta a los destinatarios se utiliza un configuración de servidor de protocolo simple de transferencia de correo (SMTP)

Módulo de análisis de archivos



El módulo de análisis de archivos ofrece dos tipos de informes:

Informes de análisis de archivos basados en la programación

El módulo de Análisis de Archivos recopila los datos para estos informes ejecutando análisis periódicos de me seguridad y espacio en disco a intervalos de tiempo especificados por el usuario.

Informes de análisis de archivos bajo demanda

Los datos para estos informes se recopilan del servidor de archivos a petición, según las entradas proporciona usuario.

Componentes del módulo de análisis de archiv

Motor de alerta

Basándose en las reglas configuradas, el motor de alertas automatiza las resp pasivas, como el envío de notificaciones por correo electrónico, la ejecución d archivos por lotes, la eliminación de archivos o su traslado a una ubicación determinada.

Base de datos

DataSecurity Plus incluye una base de datos PostgreSQL que almacena la información de los eventos sin procesar y normalizados de las fuentes de dato configuradas.

Analizador de metadatos

El módulo de análisis de archivos de DataSecurity Plus utiliza un analizador d metadatos para detectar instancias de incoherencias de permisos, problemas higiene de permisos, archivos no utilizados, archivos duplicados, etc.

Componentes externos

Consola

Se puede acceder a la interfaz web de DataSecurity Plus a través de un naveg (Internet Explorer 9 y superior, Mozilla Firefox, Google Chrome (recomendado Microsoft Edge), y se conecta al componente de servidor web de Tomcat que escucha en el puerto número 8800 por defecto.

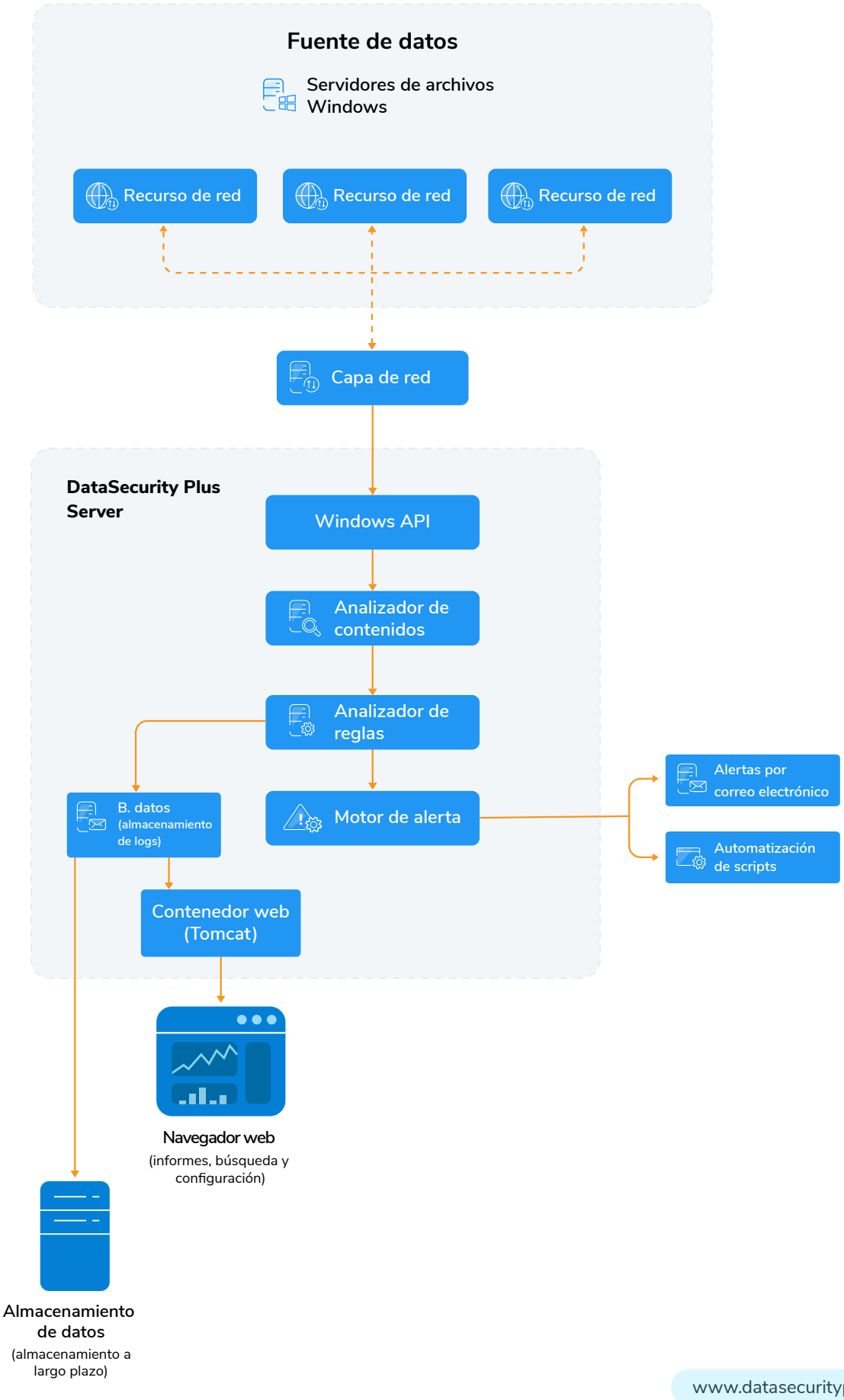
Reenvío de la gestión de incidentes y eventos de seguridad (SIEM)

DataSecurity Plus le permite reenviar todos los datos de auditoría del servidor archivos a su servidor syslog o a Splunk para su posterior análisis.

Alerta por correo electrónico

Para el envío de correos electrónicos de alerta a los destinatarios se utiliza un configuración de servidor de protocolo simple de transferencia de correo (SMTP)

Módulo de evaluación del riesgo de los datos



Componentes del módulo de evaluación de riesgo de dat

Analizador de contenidos

El analizador de contenido extrae y procesa el contenido de los archivos están siendo analizados por el módulo de evaluación de riesgo de datos.

Analizador de reglas

El analizador de reglas compara los datos procesados con las reglas y po de descubrimiento de datos para encontrar hilos de datos que coincidan c expresiones regulares y las frases de palabras clave de esas reglas, y eje acciones definidas en las políticas.

Motor de alerta

Basándose en las reglas configuradas, el motor de alertas automatiza las respuestas pasivas, como el envío de notificaciones por correo electrónic ejecución de archivos por lotes.

Base de datos

DataSecurity Plus incluye una base de datos PostgresQL que almacena datos sensibles y críticos para el negocio descubiertos en las fuentes de configurados.

Componentes externos

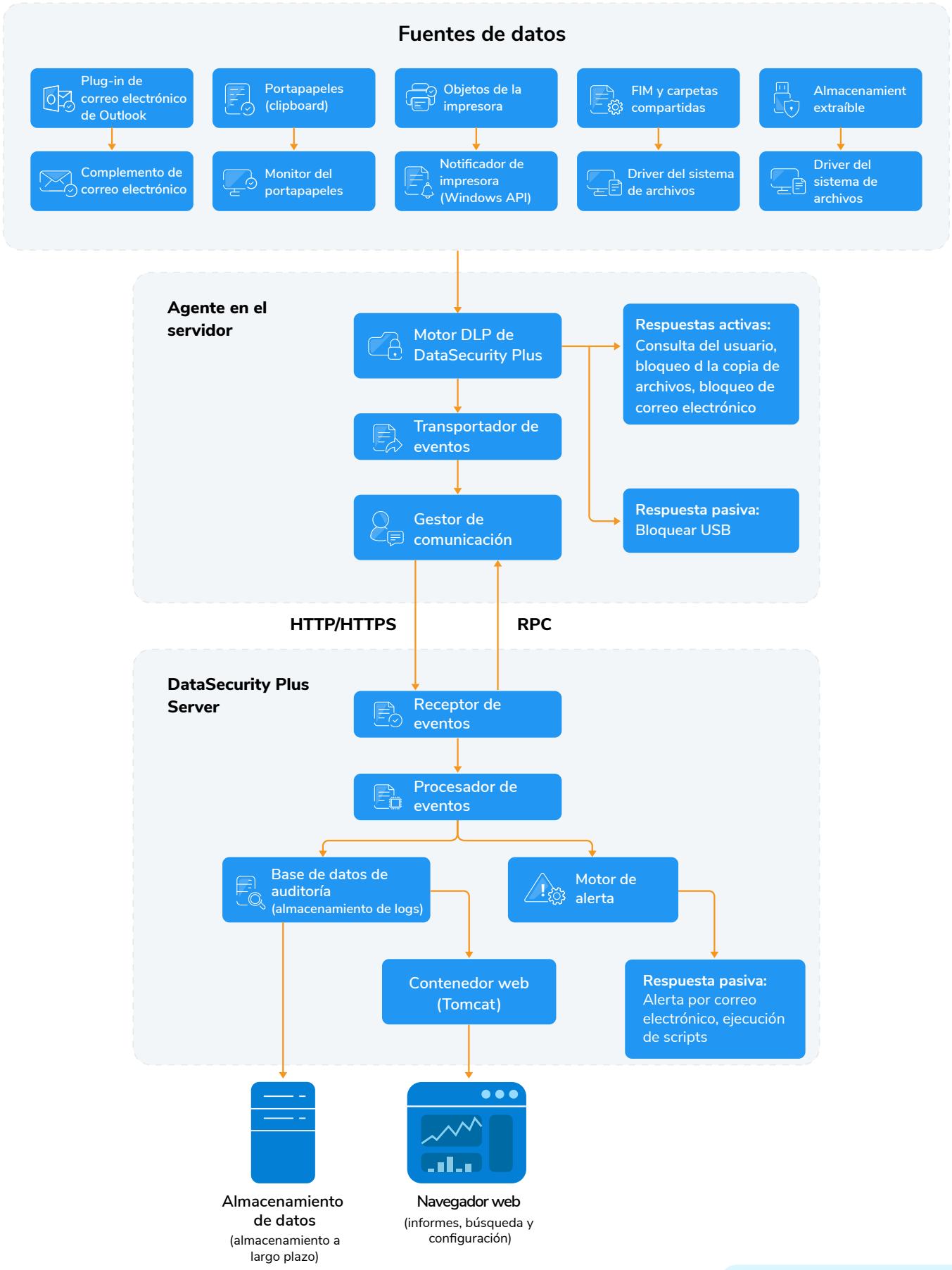
Consola

Se puede acceder a la interfaz web de DataSecurity Plus a través de un navegador (Internet Explorer 9 y superior, Mozilla Firefox, Google Chrome (recomendado) y Microsoft Edge), y se conecta al componente de servido de Tomcat que escucha en el puerto número 8800 por defecto.

Alerta por correo electrónico

La configuración del servidor SMTP se utiliza para enviar correos electrón

Módulo de prevención de pérdida de dat



Componentes del módulo de prevención de pérdida de datos:

Motor de alerta

Basándose en las reglas configuradas, el motor de alertas automatiza las respuestas activas, como la visualización de avisos al usuario y el bloqueo dispositivos USB, así como las respuestas pasivas, como el envío de notificaciones por correo electrónico, la ejecución de archivos por lotes, la eliminación de archivos o su traslado a una ubicación específica.

Base de datos de auditoría

DataSecurity Plus incluye una base de datos PostgreSQL que almacena la información de los eventos sin procesar y normalizados de las fuentes de d configuradas.

Agente DataSecurity Plus

El software implementa un agente ligero en cada estación de trabajo monito El agente utiliza un driver de minifiltro de Windows para auditar las actividad de los archivos, y la API de Windows para analizar las propiedades de los archivos. También permite a los usuarios finales clasificar manualmente los archivos en las estaciones de trabajo.

Motor DLP de DataSecurity Plus

El motor de DLP procesa todos los datos entrantes de las fuentes de datos configuradas, y los compara con un repositorio de políticas de DLP tanto integradas como definidas por el usuario.

Componentes externos

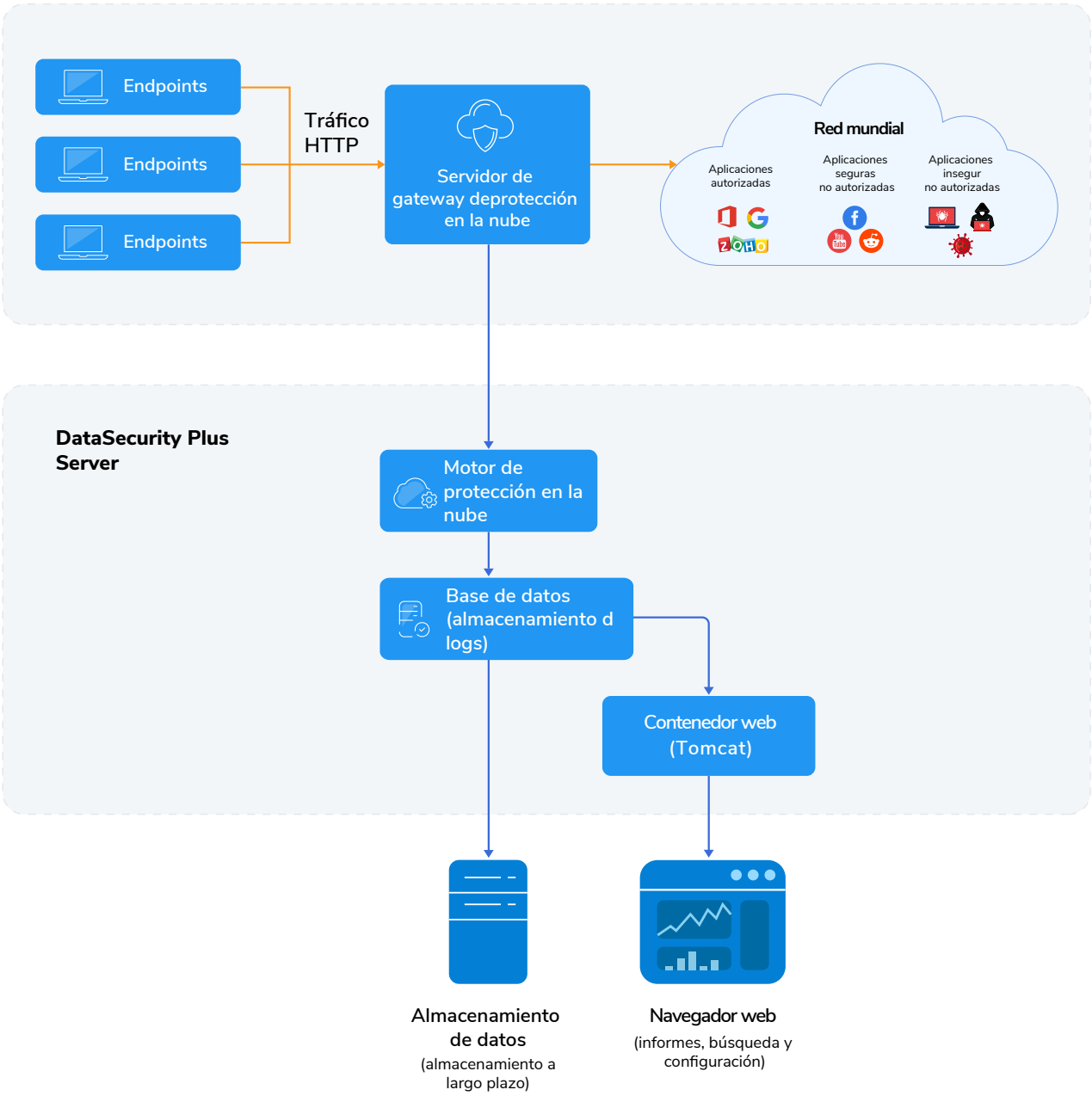
Consola

Se puede acceder a la interfaz web de DataSecurity Plus a través de un navegador (Internet Explorer 9 y superior, Mozilla Firefox, Google Chrome (recomendado) y Microsoft Edge), y se conecta al componente de servido de Tomcat que escucha en el puerto número 8800 por defecto.

Alerta por correo electrónico

La configuración del servidor SMTP se utiliza para enviar correos electrón

Módulo de protección en la nube



Componentes del módulo de protección en la nube:

Servidor de gateway de protección en la nube

El servidor gateway de protección en la nube actúa como un proxy entre usuarios y las aplicaciones de la nube. Monitorea las solicitudes de acce ayuda a los administradores a aplicar las políticas de la organización sob uso de las aplicaciones en la nube por parte de los empleados y envía lo de auditoría al motor de protección en la nube.

Motor de protección en la nube

El motor de protección en la nube gestiona los servidores del gateway, sincroniza las configuraciones entre la consola y el servidor del gateway procesa el uso de la web y los logs de actividad de los usuarios y propor una instantánea del uso de las aplicaciones en la nube de la empresa.

Base de datos

DataSecurity Plus incluye una base de datos PostgreSQL que almacena información de los eventos sin procesar y normalizados de los servidores gateway configurados.

Componentes externos

Console

DataSecurity Plus' web interface can be accessed via a browser (Internet Explorer 9 and above, Mozilla Firefox, Google Chrome (recommended), and Microsoft Edge), and connects to the web server component of Tomcat which listens on port number 8800 by default.