ManageEngine
DataSecurity Plus

Compare

Ediciones de DataSecurity Plus

DataSecurity Plus es una plataforma unificada de visibilidad y seguridad de datos que proporciona funciones de auditoría de archivos, análisis de archivos, evaluación de riesgos de datos, prevención de filtración de datos y protección de la nube. Explore las diferencias entre la edición gratuita y Professional de DataSecurity Plus utilizando la siguiente tabla.

S.No	Funciones de DataSecurity Plus	**Edición gratuita** La edición con funciones limitadas. Una vez finalizado el periodo de prueba de la edición Professional, si no tiene una licencia válida, su instancia pasará de forma predeterminada a la edición gratuita.	**Professional Edition** La edición totalmente funcional de DataSecurity Plus.
1.	**Auditoría de servidores de archivos** Realice auditorías e informes sobre los accesos a los archivos y las modificaciones, con alertas en tiempo real y respuestas automatizadas para las actividades críticas de los archivos.	No se admite. Sólo conserva los datos de auditoría del periodo de evaluación.	Disponible a partir de $745 para 2 servidores de archivos. Solicitar cotización
1.1	**Auditoría de acceso a archivos** Genere informes sobre todos los accesos y modificaciones de archivos con información detallada sobre quién hizo qué, cuándo y desde dónde.	NA	✓
1.2	**Auditoría del copiado de archivos** Supervise las actividades de copiado y pegado de archivos tanto en archivos y carpetas locales como compartidos.	NA	✓
1.3	**Monitoreo de la integridad de los archivos** Detecte y responda a los cambios de archivos sospechosos y de alto riesgo que puedan indicar amenazas para la seguridad.	NA	✓
1.4	**Notificador de cambios en los archivos** Active notificaciones instantáneas ante picos repentinos por actividades críticas de archivos como cambios de SACL, propietario o permisos, borrado de archivos, etc.	NA	✓
1.5	**Monitoreo de usuarios privilegiados** Utilice informes personalizados para supervisar las actividades de archivo de los administradores, las cuentas de usuarios privilegiados y los grupos de AD.	NA	✓

1.6	**Detección y respuesta a ransomware** Detecte e interrumpa los potenciales ataques de ransomware al instante con nuestro mecanismo automatizado de respuesta ante amenazas.	NA	✓
1.7	**Análisis de patrones de acceso** Obtenga información detallada sobre los archivos a los que más se accede, los usuarios más activos, los procesos más utilizados, entre otros, analizando los patrones de acceso a lo largo del tiempo.	NA	✓
1.8	**Informes listos para el cumplimiento** Utilice los múltiples informes listos para auditoría para satisfacer los requisitos exigidos por las normas reguladoras como GDPR, PCI-DSS, HIPAA, etc.	NA	✓
1.9	**Análisis forense** Use pistas de auditoría accionables y precisas para rastrear e identificar la causa raíz de los incidentes de seguridad que involucran el uso indebido de archivos.	✓ Utilizando los datos de auditoría del periodo de evaluación	✓
2.	**Análisis de archivos** Analice el uso del espacio en disco, gestione los datos basura, identifique los datos en riesgo y analice los permisos de los archivos analizando la seguridad de los archivos y los parámetros de almacenamiento.	Tamaño admitido de los datos escaneados: 500GB	Disponible a partir de $95 para 1TB de datos escaneados. Solicitar cotización
2.1	**Análisis del uso de espacio en disco** Supervise las tendencias de crecimiento de los datos y los patrones de uso del disco de los empleados para encontrar a los usuarios que consumen la mayor parte de su espacio en disco.	✓	✓
2.2	**Informes de estado de los archivos** Genere informes sobre archivos abiertos actualmente, carpetas vacías, puntos de unión activos, archivos ocultos, sesiones activas, etc.	✓	✓
2.3	**Análisis de la propiedad del archivo** Realice un análisis cruzado de la peligrosidad de los archivos que contienen datos confidenciales con los datos de su propietario para identificar a los usuarios de alto riesgo, las tendencias alarmantes de los datos y mucho más.	✓	✓
2.4	**Notificador de espacio de almacenamiento críticamente bajo** Active alertas por correo electrónico cuando el espacio libre en los discos de almacenamiento caiga por debajo de los valores preconfigurados.	✓	✓
2.5	**Informes de permisos de seguridad** Genere informes sobre la marcha y encuentre usuarios con privilegios elevados, permisos efectivos y permisos de NTFS sobre archivos y carpetas.	✓	✓

2.6	**Análisis de datos ROT o basura** Encuentre y gestione los datos redundantes, obsoletos y triviales de sus almacenes de datos para recuperar el espacio de almacenamiento desperdiciado.	✓	✓
2.7	**Gestión de los archivos duplicados** Encuentre archivos duplicados comparando sus metadatos, previsualice todas las copias y elimine las instancias innecesarias desde la interfaz de usuario.	✓	✓
2.8	**Descubrimiento de archivos huérfanos** Encuentre la lista de todos los archivos y carpetas que son propiedad de usuarios inactivos, deshabilitados o eliminados.	✓	✓
2.9	**Detección de archivos inactivos** Identifique y analice los archivos antiguos, obsoletos, no modificados, ocultos, etc.	✓	✓
2.10	**Diagnóstico de la integridad de permisos de archivos** Enumere los archivos y carpetas que tienen la herencia de permisos deshabilitada y derechos de acceso excesivos (como control total).	✓	✓
2.11	**Gestión de archivos dañados por ransomware** Localice y elimine los archivos infectados por ransomware utilizando la biblioteca preintegrada de tipos de archivos de ransomware conocidos.	✓	✓
3.	**Evaluación de riesgos** Descubra y clasifique los archivos que contienen datos confidenciales como PII, PCI y ePHI combinando la inspección de contenidos y el análisis contextual.	Tamaño admitido de los datos escaneados: 100GB	Disponible a partir de $395 para 2TB de datos escaneados. Solicitar cotización
3.1	**Descubra los datos confidenciales** Encuentre todas las instancias de datos sensibles en sus repositorios de datos correlacionándolos con frases clave o patrones de expresiones regulares.	✓	✓
3.2	**Clasificación de datos automatizada** Clasifique los archivos con base en su sensibilidad y vulnerabilidad con etiquetas principales y secundarias personalizadas creadas según los requisitos de su organización.	✓	✓
3.3	**Análisis de datos sensibles** Clasifique y analice los archivos que contengan datos confidenciales en función de sus propietarios, tipo de archivo, tipo de fuente, políticas y reglas.	✓	✓

3.4	**Cálculo de la puntuación de riesgo del usuario** Asigne una puntuación de riesgo a todos los usuarios analizando la sensibilidad y vulnerabilidad de los contenidos de su propiedad.	✓	✓
3.5	**Políticas y reglas de descubrimiento de datos integradas** Utilice políticas y reglas integradas y específicas de cumplimiento para encontrar datos controlados por normas reglamentarias como GDPR, PCI DSS, HIPAA, etc.	✓	✓
3.6	**Análisis de la propiedad de los datos y notificador** Utilice notificaciones instantáneas por correo electrónico para alertar a los propietarios de los datos sobre la presencia de datos vulnerables y sensibles de su propiedad.	✓	✓
3.7	**Estimación del nivel de confianza de los datos sensibles** Utilice los filtros de nivel de confianza (es decir, alto, medio y bajo) para indicar la fiabilidad de las instancias de datos sensibles.	✓	✓
3.8	**Reconocimiento del tipo de archivo** Analice el contenido sensible de más de 50 tipos de archivos, incluyendo correo electrónico, texto, archivos comprimidos, etc.	✓	✓
4.	**Prevención de filtración de datos** Detecte e interrumpa las filtraciones de datos a través de USB, correo electrónico, aplicaciones web e impresoras mediante el monitoreo en tiempo real de la actividad de los archivos en los endpoints.	Número de estaciones de trabajo compatibles: 50	Disponible a partir de $345 para 100 estaciones de trabajo. Solicitar cotización
4.1	**Protección del contenido** Utilice etiquetas de clasificación de archivos para proteger los archivos que contengan datos confidenciales: **Equipos distribuidos:** portátiles y desktops **Aplicaciones:** Outlook **Almacenamiento extraíble:** USB, tarjetas SD, etc. **Desktops virtuales:** Citrix, VMWare (siempre que el SO instalado sea Windows 2003 o superior). **Navegadores:** Chrome, Firefox, Internet Explorer, etc. **Otros:** impresora, portapapeles, fax, recursos de red, Wi-Fi y adaptadores Bluetooth.	✓	✓
4.2	**Monitoreo de seguridad de endpoints** Detecte anomalías en el acceso a los archivos y en la transferencia de datos en los endpoints para garantizar la integridad de los archivos.	✓	✓
4.3	**Protección de copia de archivos** Detenga los intentos de robo de datos restringiendo el uso de portapapeles, que bloquea las acciones de copia de archivos en recursos de red, archivos locales y USB.	✓	✓

4.4	**Control de aplicaciones** Supervise el uso de aplicaciones y restrinja el uso de ejecutables sospechosos y de alto riesgo añadiéndolos a listas de bloqueo.	✓	✓
4.5	**Control de dispositivos externos** Limite varias funcionalidades dentro de los dispositivos USB denegando el acceso de lectura, escritura y ejecución.	✓	✓
4.6	**Bloqueo USB** Regule el uso de medios de almacenamiento extraíbles añadiendo dispositivos USB de alto riesgo y no verificados a la lista de bloqueo.	✓	✓
4.7	**Protección contra la filtración de datos adjuntos al correo electrónico** Detecte instantáneamente y bloquee el envío de correos electrónicos (Outlook) que contengan archivos clasificados adjuntos.	✓	✓
4.8	**Auditoría de impresoras** Monitoree el uso del servidor de impresión local y genere informes con detalles sobre quién imprimió qué y cuándo.	✓	✓
4.9	**Auditoría del navegador web** Analice las posibles cargas y descargas de archivos supervisando todas las actividades en archivos iniciadas por los procesos del navegador web.	✓	✓
4.10	**Auditoría de almacenamiento extraíble** Genere informes detallados sobre todas las acciones en archivos USB y supervise las transferencias de archivos con detalles sobre quién hizo qué, desde dónde, a través de qué dispositivo, etc.	✓	✓
4.11	**Clasificación de datos manual** Los administradores y propietarios de datos pueden etiquetar los archivos confidenciales con etiquetas predefinidas como Público, Privado, Confidencial o Restringido.	✓	✓
4.12	**Políticas de respuesta a incidentes** Responda a los eventos de seguridad detectados poniendo en cuarentena los dispositivos infectados, deshabilitando las cuentas de usuarios maliciosos, trasladando los archivos vulnerables a ubicaciones seguras, etc.	✓	✓
4.13	**Educación y concienciación del usuario final** Utilice mensajes emergentes para informar o advertir a los empleados sobre acciones inseguras de transferencia de archivos que podrían provocar una filtración de datos.	✓	✓

5.	**Protección en la nube (Add-on gratuito del módulo de prevención de filtración de datos)** Supervise el tráfico web de su organización, examine el uso de aplicaciones en la sombra y aplique políticas para bloquear las aplicaciones en la nube inapropiadas y maliciosas.	No se admite. Sólo conserva los datos de auditoría del periodo de evaluación.	Ilimitado
5.1	**Descubrimiento de aplicaciones en la nube** Audite el tráfico web de su organización y obtenga información detallada sobre las aplicaciones en la nube en uso, su reputación, categoría de aplicación, etc.	NA	✓
5.2	**Filtrado de contenidos y URL** Impida que sus empleados accedan a aplicaciones en la nube infestadas de malware y que afectan la productividad.	NA	✓
5.3	**Descubrimiento de aplicaciones web en la sombra** Supervise de cerca el uso de aplicaciones web en la sombra (es decir, servicios web no verificados) para encontrar a los principales actores que acceden a ellas y analizar el riesgo que plantean estos servicios.	NA	✓
5.4	**Análisis de aplicaciones en la nube de mala reputación** Encuentre y examine el uso de aplicaciones en la nube poco fiables y de alto riesgo analizando su historial, antigüedad, URL subyacentes, etc.	NA	✓
5.5	**Inspección profunda de paquetes** Inspeccione el tráfico de su red leyendo el contenido de los paquetes de datos cifrados.	NA	✓
5.6	**Monitoreo de la carga de archivos** Genere informes sobre las solicitudes de carga realizadas en SharePoint, OneDrive, Exchange, Box y DropBox, así como en aplicaciones de Zoho como Cliq, WorkDrive, Sheet, Writer, Projects, etc.	NA	✓
5.7	**Supervisión de solicitudes web** Enumere las solicitudes HTTP simples exitosas y fallidas.	NA	✓

* Las funciones y capacidades disponibles para los usuarios en la edición gratuita están sujetas a cambios y pueden ser revisadas sin previo aviso por DataSecurity Plus.