eScan Data Leak Prevention (Prevención de Pérdida de Datos)

La solución de seguridad DLP de eScan es un conjunto de estrategias, tecnologías y técnicas que garantizan que los usuarios finales no transmitan datos críticos o sensibles fuera de una organización. Ya sea que la transmisión de datos se realice a través de mensajes, correos electrónicos, transferencias de archivos u otros medios, la información puede terminar en ubicaciones no autorizadas, lo que puede generar problemas de cumplimiento.

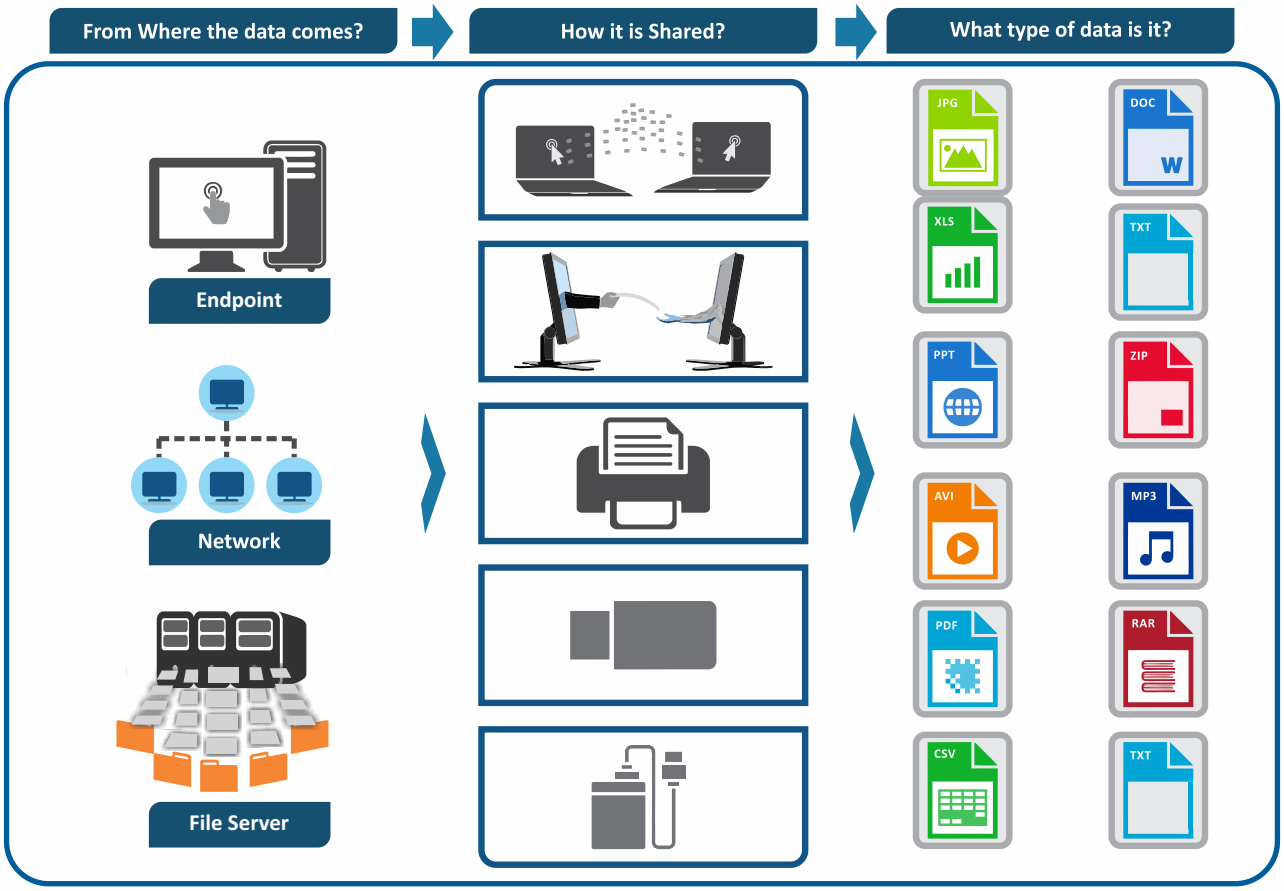
Como solución empresarial, DLP detecta posibles filtraciones de datos/intentos de exfiltración de datos y los previene mediante la supervisión, detección y bloqueo de datos sensibles mientras están en uso (acciones en endpoints), en movimiento (tráfico de red) y en reposo (almacenamiento de datos). Una solución DLP efectiva también emplea reglas empresariales para garantizar el cumplimiento normativo y proteger la información confidencial.

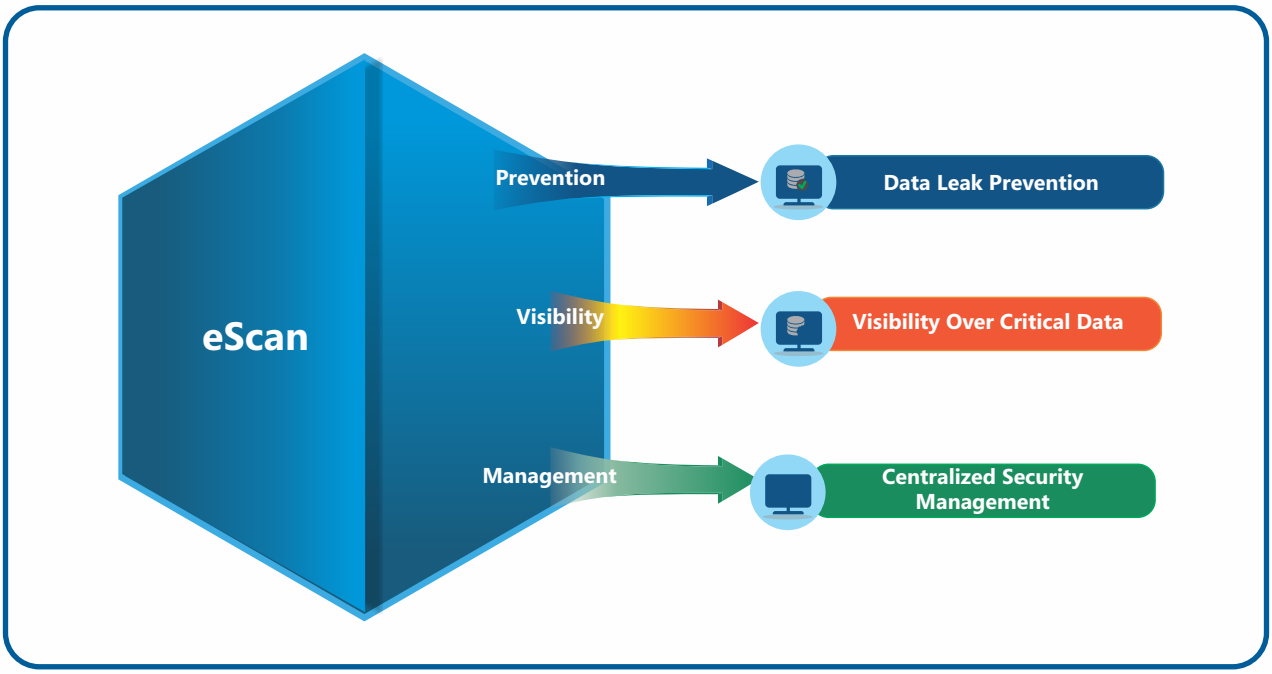
Con sus funciones avanzadas, brinda protección contra intentos de exfiltración, supervisa el acceso y/o filtración de datos sensibles, y permite una visibilidad de 360 grados sobre el uso de archivos confidenciales y la protección de datos etiquetados como críticos por un usuario

eScan
Data Leak Prevention

eScan Enterprise Security

Datos en Reposo y Datos en Movimiento



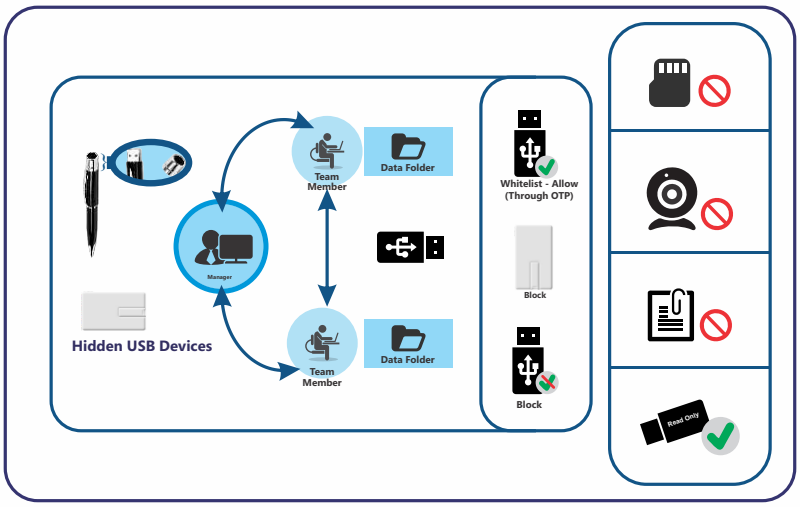


eScan
Data Leak Prevention

eScan Enterprise Security

¿Por qué eScan Enterprise DLP?

eScan Enterprise DLP está equipado con una amplia gama de funciones y tecnologías avanzadas para proteger los datos en movimiento o en reposo. Estas características le ayudan a rastrear, monitorear y proteger datos críticos dentro de su red. Estas funciones pueden configurarse según sus necesidades a través de una Consola de Gestión Centralizada de Nivel Empresarial Segura, que le permite implementar la solución en endpoints conectados a su red. eScan Enterprise DLP también ofrece protección en puertas de enlace de correo para evitar la fuga de datos críticos a través del correo electrónico.



La avanzada función de Control de Dispositivos de eScan Enterprise DLP ayuda a monitorear los dispositivos USB conectados a endpoints con Windows o Mac dentro de la red. En los endpoints con Windows, los administradores pueden permitir o bloquear el acceso a dispositivos USB como cámaras web, unidades de CD-ROM, dispositivos compuestos, teléfonos inteligentes, dispositivos Bluetooth, tarjetas SD o dispositivos de imagen. El acceso no autorizado a dispositivos externos puede bloquearse mediante protección con contraseña, evitando así la filtración de datos a través de dispositivos USB.

Muchas veces, el acceso al puerto USB se usa indebidamente, lo que provoca que el robo de datos se convierta en una práctica común y cause un daño potencial a la organización, ya que la propiedad intelectual puede terminar en manos equivocadas. Una subfunción del Control de Dispositivos en eScan Enterprise DLP permite enviar notificaciones al administrador de la consola web cuando se copia cualquier dato del disco duro del sistema cliente a un dispositivo USB.

El Control de Dispositivos garantiza que el robo de datos se erradique por completo, sin dejar margen para el uso indebido de información confidencial.

La función de protección con contraseña de eScan Enterprise DLP restringe el acceso de los usuarios para evitar que violen una política de seguridad implementada en la red.

Por ejemplo, supongamos que el administrador ha implementado una política de seguridad para bloquear todos los dispositivos USB, pero alguien necesita acceder a uno por una razón legítima, como realizar una presentación de ventas almacenada en una memoria USB.

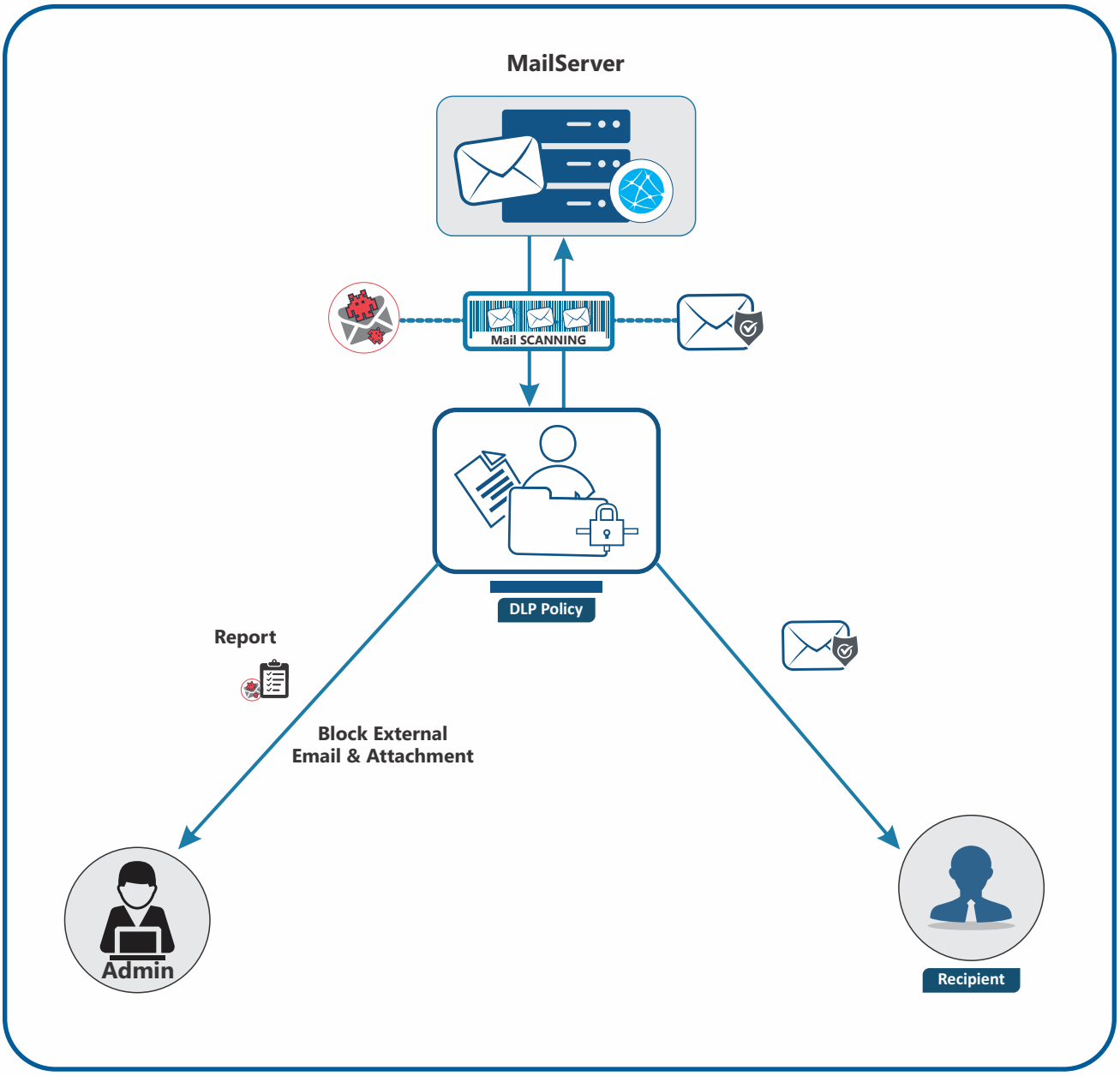
¿Cómo podría el administrador otorgar acceso sin violar la política de seguridad actual?

La respuesta es OTP.

Generando una Contraseña de Un Solo Uso (OTP) de eScan Enterprise DLP por un período de tiempo específico para una computadora cliente en particular, se puede deshabilitar el módulo sin violar la política existente

eScan®
Enterprise Security

Aspectos Clave Control de Adjuntos y Contenido



eScan
Data Leak Prevention

eScan Enterprise Security

Bloqueo de Archivos Adjuntos

La función de bloqueo de adjuntos DLP le permite controlar el flujo de adjuntos dentro de su organización. Puede bloquear/permitir todos los adjuntos que un usuario intente enviar a través de procesos predefinidos específicos. También puede excluir dominios/subdominios específicos de confianza, permitiendo que los adjuntos enviados a través de estos no sean bloqueados, incluso si están dentro de los procesos bloqueados mencionados anteriormente. Un modelo de informe independiente está disponible para recibir información detallada a través del correo electrónico.

Informe de Adjuntos

Esta función proporciona un informe completo que le permite determinar qué adjuntos han sido permitidos o bloqueados por eScan Enterprise DLP. También alerta al administrador sobre los adjuntos que están siendo compartidos o cargados, mostrando la fuente del adjunto y el destino.

Controles en Función del Contenido

Esta función avanzada permite al administrador monitorear y controlar la información confidencial que puede enviarse fuera del endpoint. La información sensible, también conocida como PII (Información de Identificación Personal), que a menudo está regulada por normativas gubernamentales como GDPR, puede clasificarse en las siguientes categorías (nuevas categorías se agregan constantemente y pueden personalizarse según los requisitos del cliente o país):

- **Número de Tarjeta Aadhar**
- **Número de Licencia de Conducir**
- **Número de Pasaporte**
- **Número de Tarjeta PAN**
- **Números de Tarjeta de Crédito (RUPAY, VISA, Amex, MasterCard, etc.)**
- **Números de Cuenta Bancaria Internacional (IBAN)**

El filtrado de PII en eScan Enterprise DLP se puede aplicar a diversos canales como:

- **Dispositivos de Almacenamiento Externo (USB, CD/DVD, Bluetooth)**
- **Impresoras**
- **Comunicación de Red**

eScan
Data Leak Prevention

eScan Enterprise Security

Acceso a Correos Electrónicos, Almacenamiento y Comunicación Corporativa Basados en la Nube

Existen varias formas en las que los empleados que usan servicios como Gmail Corporativo, O365, Slack, WebEx, Dropbox, entre otros, pueden poner en riesgo los datos de la empresa. Para evitar posibles fugas, eScan Enterprise DLP proporciona la funcionalidad para bloquear el acceso a cuentas personales en servicios alojados en la nube.

Esta función garantiza que los miembros del equipo solo puedan acceder a estos servicios usando sus credenciales corporativas y no sus cuentas personales. Se admiten los siguientes servicios alojados (y se están agregando nuevos constantemente):

- **Office365 u O365 (Outlook Corporativo)**
- **Gmail Corporativo**
- **Slack**
- **WebEx**
- **Dropbox**
- **Teams**

Informes de Correo Electrónico

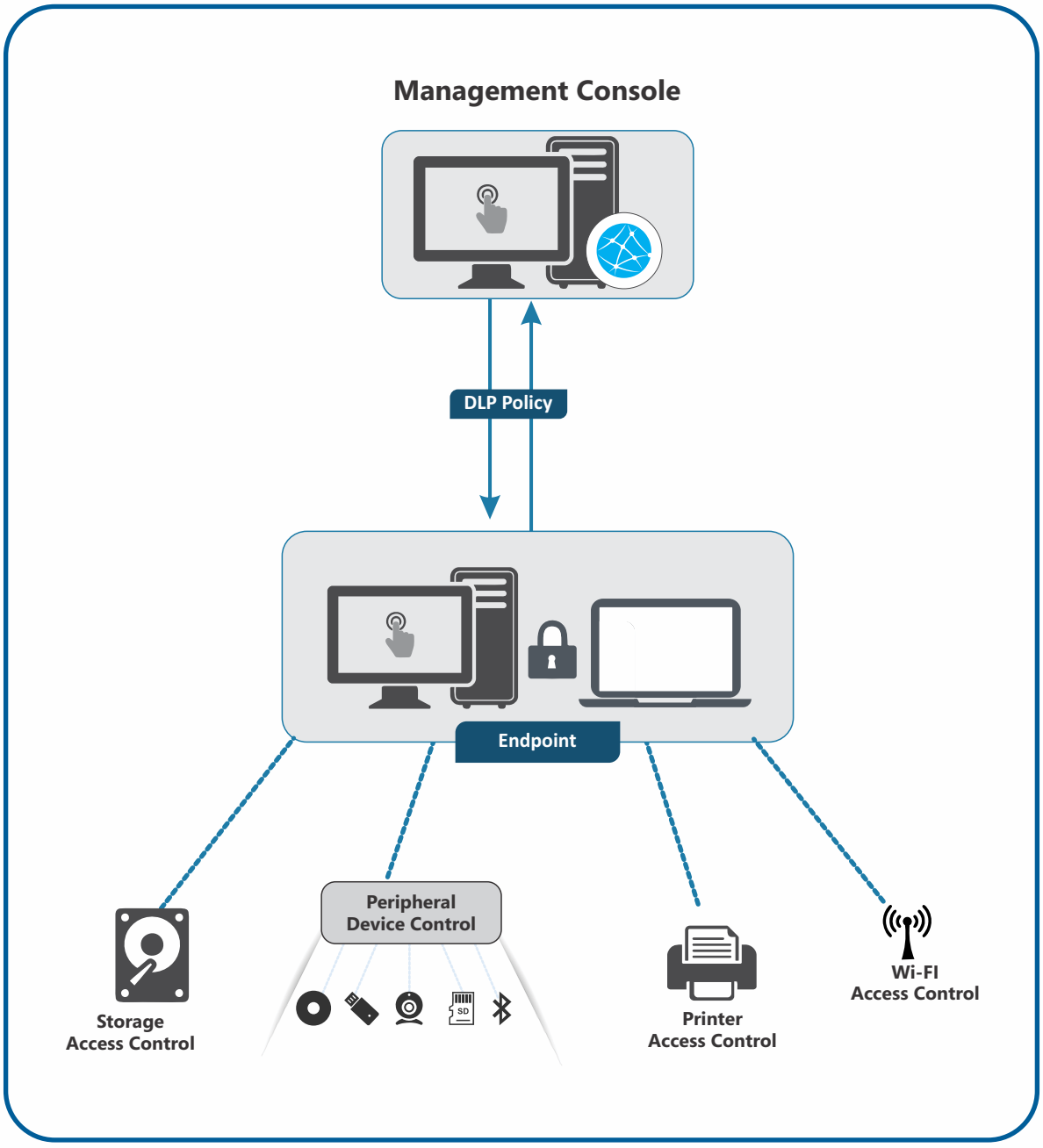
El correo electrónico es una herramienta de comunicación empresarial omnipresente que permite adjuntar archivos, incluir enlaces y compartir detalles corporativos con compañeros de trabajo y clientes. El informe de correo electrónico de eScan Enterprise DLP proporciona al administrador detalles precisos sobre el destinatario, los tipos de adjuntos, el tamaño del correo y mucho más. El administrador puede monitorear y controlar la fuga de datos a través de correos electrónicos.

Copia Sombra de Archivos Permitidos para Carga

eScan Enterprise DLP proporciona copias de los archivos que se transfieren a través de la web, correo electrónico y almacenamiento en línea (Google Drive, OneDrive, Dropbox, etc.).
Cada vez que se transfieren archivos, se pueden crear copias sombra de estos archivos en función de los destinatarios, el nombre del remitente y el tamaño del adjunto, lo que garantiza un monitoreo efectivo de los datos que se comparten o almacenan.

eScan®
Enterprise Security

Control de Dispositivos



Control de Acceso a Impresoras

eScan Enterprise DLP gestiona la actividad de impresión de documentos sensibles. Las opciones de Control de Acceso a Impresoras pueden definir qué datos pueden imprimirse en impresoras específicas y por quién.

Una ventaja de esta solución técnica es que, en caso de actividad no autorizada, el sistema DLP registra el incidente, notifica al usuario sobre los riesgos y también puede bloquear la impresión. Las posibles violaciones generan alertas que se envían al administrador. Este módulo también permite al administrador bloquear total o selectivamente las impresoras en red.

Control de Acceso al Almacenamiento

La protección de Control de Dispositivos en eScan Enterprise DLP evita que los usuarios, endpoints o ambos usen medios de almacenamiento extraíbles no autorizados.
eScan Enterprise DLP impide que un usuario copie un archivo o información a medios extraíbles o dispositivos USB. El control de acceso al almacenamiento bloquea la escritura de datos en unidades extraíbles que no están protegidas.

Control de Dispositivos Periféricos

eScan Enterprise DLP protege los datos críticos de su empresa, evitando que se transfieran a dispositivos periféricos y extraíbles, como unidades USB, dispositivos Bluetooth y CDs o DVDs grabables.
El control de dispositivos proporciona la opción de monitorear y controlar las transferencias de datos desde todas las computadoras de escritorio y portátiles, sin importar dónde se encuentren los usuarios o los datos confidenciales, incluso cuando no están conectados a la red corporativa.

Control de Acceso Wi-Fi

Los puntos de acceso Wi-Fi vienen con un SSID y una contraseña predeterminados que deben actualizarse, aunque con frecuencia se mantienen sin cambios. Esto facilita que un atacante inicie sesión, tome el control del router, configure ajustes o firmware, cargue programas maliciosos o incluso cambie el servidor DNS para redirigir todo el tráfico a la dirección IP del atacante.
El control de acceso Wi-Fi permite bloquear o autorizar redes Wi-Fi específicas para acceder a su red, según una lista de SSIDs permitidos (lista blanca).

Clasificación/Descubrimiento de Datos

Clasificación de Datos

eScan Enterprise DLP proporciona Etiquetas de Sensibilidad, también conocidas como Clasificación de Datos, que constituyen un componente crítico de seguridad de datos. Estas ayudan a las organizaciones a gestionar y proteger su información sensible.

Al categorizar los datos en función de su sensibilidad e importancia, las organizaciones pueden aplicar medidas de seguridad adecuadas según las etiquetas de clasificación de datos y responder rápidamente a posibles fugas de datos, mejorando así su sistema de seguridad general.

Descubrimiento de Datos

El Descubrimiento de Datos en eScan Enterprise DLP se refiere al proceso de detección y gestión de datos sensibles en toda la red de una organización.

Permite escanear y generar un informe detallado de los datos confidenciales presentes en los endpoints. Esto ayuda a tomar decisiones informadas sobre la información detectada y, en última instancia, a mitigar los riesgos asociados con violaciones de datos.

Análisis de Comportamiento de Entidad de Usuario (UEBA) – Monitoreo de Actividad

Monitoreo de Actividad de Archivos (Local, Red, Dispositivos de Almacenamiento)

El módulo de Actividad de Archivos muestra un informe de los archivos creados, copiados, modificados y eliminados en las computadoras administradas.

Además, en caso de uso indebido de archivos oficiales, el responsable puede ser identificado a través de los detalles capturados en el informe. El administrador puede seleccionar y filtrar el informe según cualquiera de los detalles registrados.

Copia Sombra (Actividad de Archivos en USB)

Esta tecnología permite crear una copia de los archivos que un usuario copia en una unidad USB externa. Esta función permite a los administradores auditar los archivos que salen del endpoint.

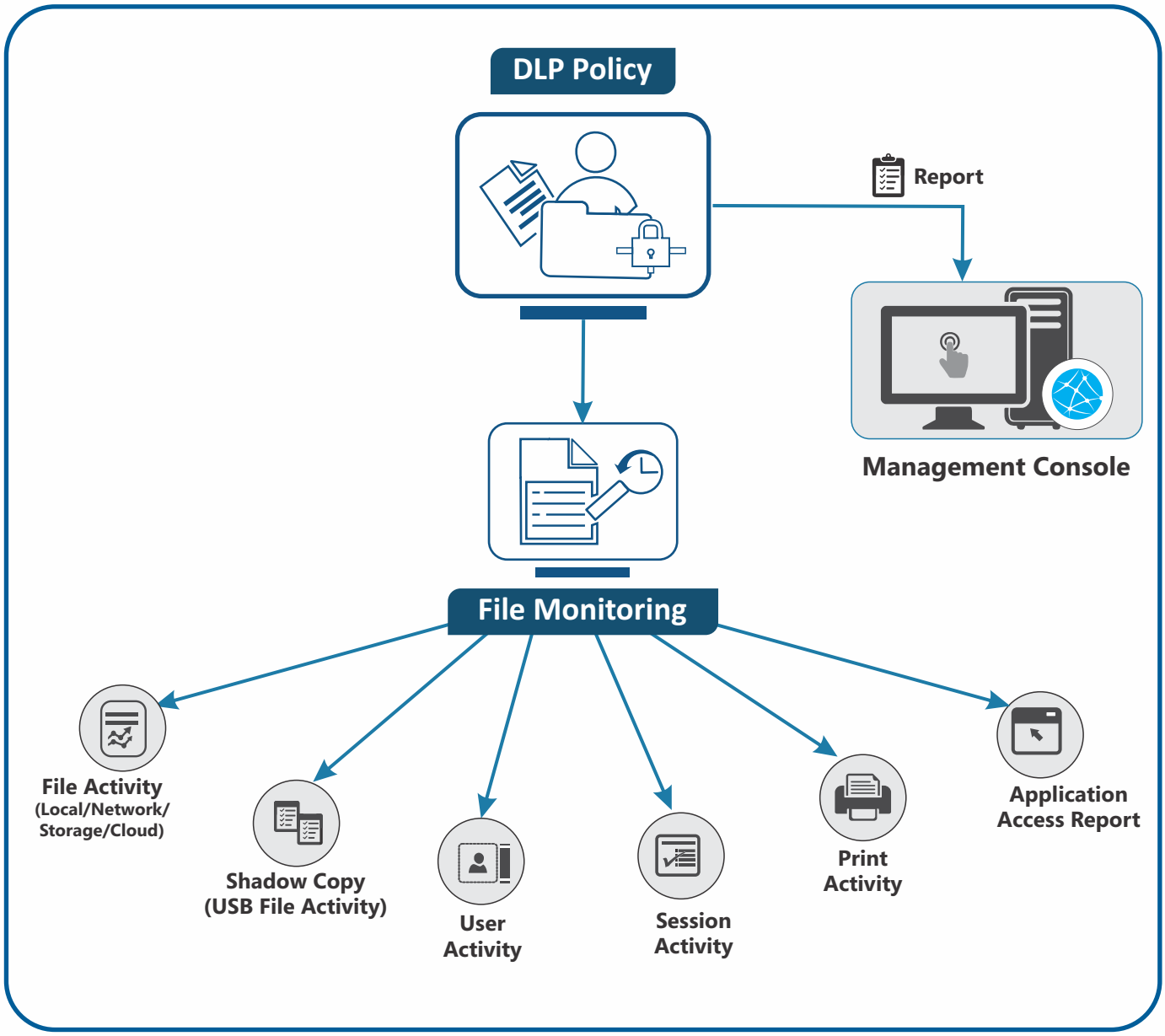
Actividad del Usuario

La función de Actividad del Usuario permite monitorear la actividad de impresión, sesiones, aplicaciones y archivos en las computadoras cliente.
También proporciona informes sobre las aplicaciones en ejecución:

- Actividad de Impresión: monitorea y registra los comandos de impresión enviados desde todas las computadoras.
- Informe de Acceso a Aplicaciones: muestra un informe detallado de todas las aplicaciones utilizadas en las computadoras administradas.
- Informe de Actividad de Archivos: muestra los archivos creados, copiados, modificados y eliminados en las computadoras administradas.

eScan
Data Leak Prevention

eScan Enterprise Security



Actividad de Sesión

Este submódulo monitorea y registra las actividades de sesión en las computadoras administradas.

Muestra un informe con el tipo de operación, fecha, nombre de la computadora, grupo, dirección IP y descripción del evento.

Con este informe, el administrador puede rastrear la actividad de inicio y cierre de sesión del usuario, así como las sesiones remotas realizadas en todas las computadoras administradas.

Actividad de Impresion

La Actividad de Impresión permite hacer un seguimiento de las impresoras agregándolas a un grupo y asignándoles un alias.
Las impresoras pueden agregarse o eliminarse de este grupo alias.
Este módulo monitorea y registra los comandos de impresión enviados desde todas las computadoras y permite filtrar los registros según el nombre de la computadora, impresora y/o usuario.
Además, permite exportar un informe detallado de actividad de impresión en formatos XLS, PDF y HTML. El informe generado contiene:

- Fecha de impresión
- Nombre de la máquina
- Dirección IP
- Nombre de usuario
- Nombre de la impresora
- Nombre del documento
- Número de copias y páginas

Informe de Acceso a Aplicaciones

El módulo de Informe de Acceso a Aplicaciones proporciona una vista detallada de todas las aplicaciones utilizadas en los endpoints que forman parte de las computadoras administradas.

El registro muestra una lista de aplicaciones ejecutadas y la duración durante la cual estuvieron activas.

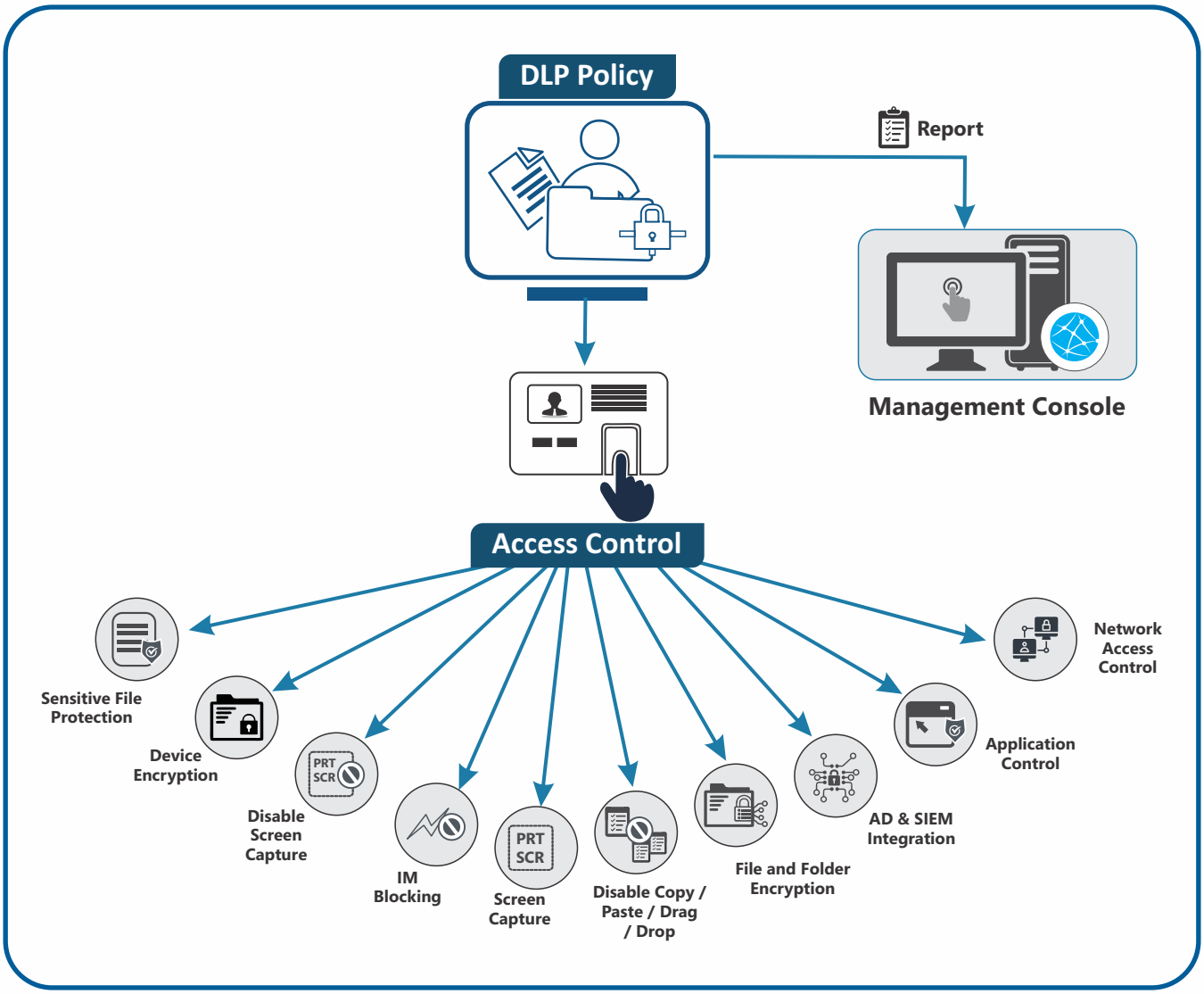
También permite filtrar o exportar el registro en los formatos deseados.

Incluye detalles como:

- Nombre de la computadora que accedió a la aplicación
- Duración de uso

eScan®
Enterprise Security

Control de Acceso



Bloqueo de Mensajería Instantánea (IM Blocking)

Los ciberataques suelen ocurrir a través de transferencias de archivos o mensajes inadvertidos, evitando los sistemas de seguridad tradicionales de las puertas de enlace. Los hackers pueden realizar actividades de exfiltración de información secuestrando navegadores y aplicaciones de mensajería instantánea (como Firefox, Skype, Opera) a través de vulnerabilidades conocidas como desbordamientos de búfer o errores en condiciones de límites.

Las reglas de Mensajería Instantánea (IM) en eScan Enterprise DLP solo funcionarán si los procesos utilizados para la transferencia de archivos son los especificados en la lista de aplicaciones al momento de crear la regla.
La regla IM proporciona un bloqueo total sobre todos los archivos adjuntos y transferencias de archivos a través de aplicaciones de mensajería instantánea

eScan
Data Leak Prevention

eScan Enterprise Security

Captura de Pantalla

La función de Captura de Pantalla facilita la toma de capturas del escritorio. Como propietario de un negocio, es fundamental conocer las actividades de los empleados, especialmente en los equipos de servicio al cliente o mesas de ayuda.
Los empleados pueden trabajar arduamente, pero para comprender claramente su productividad, la captura de pantalla brinda una visión detallada del trabajo realizado.

Deshabilitar (Copiar/Pegar/Arrastrar/Soltar)

En un dispositivo, una vez que los datos se copian en el portapapeles desde cualquier aplicación, pueden ser accedidos por cualquier otra aplicación. Con la opción de Copiar/Pegar deshabilitada, un usuario tiene prohibido copiar información al portapapeles.

Cifrado de Archivos y Carpetas

El Data Vault de DLP cifra archivos y carpetas, protegiendo los datos sensibles y confidenciales contra accesos no autorizados y filtraciones de datos. Brinda un nivel avanzado de protección con contraseña para sus archivos y carpetas importantes.
El Data Vault está cifrado utilizando AES de 256 bits y HMAC-SHA de 256 bits.
Se requiere una contraseña para acceder al vault.

- Cuando un usuario accede al Data Vault con las credenciales correctas, los datos almacenados se descifran automáticamente.
- Cuando el usuario cierra el vault, los datos almacenados se cifran automáticamente.

Control de Aplicaciones

La función de Control de Aplicaciones permite bloquear la ejecución de aplicaciones no deseadas en los endpoints. Esto ayuda al administrador a controlar qué aplicaciones pueden ejecutarse en los dispositivos administrados.
Además, eScan Enterprise DLP refuerza la política de control de aplicaciones para proporcionar monitoreo continuo, evitando violaciones de seguridad, fugas de datos e interrupciones.

Cifrado de Dispositivos Extraíbles

El cifrado de dispositivos extraíbles es una de las características de seguridad que protege sus datos contra accesos no autorizados en caso de que una unidad externa se extravíe o sea robada.

Cuando se activa esta función, el dispositivo se cifra y todos los datos almacenados en él solo pueden ser accedidos por endpoints de confianza, que forman parte del Grupo Administrado de eScan Enterprise DLP.

El cifrado de dispositivos de eScan Enterprise DLP permite administrar el cifrado de dispositivos en endpoints Windows a través de la Consola de Gestión de eScan Enterprise DLP.

eScan
Data Leak Prevention

eScan Enterprise Security

Control de Acceso a la Red

El Control de Acceso a la Red de eScan Enterprise DLP ayuda a una organización a controlar el acceso a unidades de red y carpetas compartidas.

Esta función proporciona acceso granular de solo lectura o acceso completo a recursos compartidos individuales, lo que permite controlar el acceso y modificación de datos confidenciales.

Deshabilitar Captura de Pantalla

Esta función bloquea cualquier captura de pantalla o proceso de captura de imagen, como la herramienta de recortes de Windows, evitando la toma de imágenes del escritorio.
Esta función garantiza que los usuarios no puedan capturar información sensible en formato de imagen para transferirla fuera del sistema, convirtiéndose en un aspecto crítico dentro de una estrategia DLP.

Protección de Archivos Sensibles

Esta función garantiza que los datos sensibles no puedan ser accedidos mediante ninguna otra aplicación excepto la aplicación predeterminada especificada.

- Una vez que una carpeta es clasificada como "Sensible", su contenido no podrá ser modificado ni eliminado de ninguna manera.
- Los archivos solo pueden ser abiertos con las aplicaciones asociadas, y se bloquea cualquier tipo de edición para evitar modificaciones en los datos.

Integración con AD & SIEM

eScan Enterprise DLP permite una integración fluida con Active Directory (AD), Visor de Eventos y SIEM.
La integración con SIEM permite transferir todos los eventos relacionados con DLP a un Servidor SIEM, para un análisis y reporte detallado

Otros Aspectos Destacados

- Consola de Gestión Segura de eScan
- Gestión de Licencias
- Implementación de Tareas
- Plantillas de Políticas
- Criterios de Políticas
- Agente de Actualización
- Agrupación Automática
- Sincronización con Active Directory
- Difusión de Mensajes
- Actividad de Sesión
- Configuración Personalizada
- Gestión de Actualizaciones
- Protección en Tiempo Real contra Malware
- Bloqueo Sofisticado de Archivos y Protección de Carpetas
- Potente Escaneo Heurístico para Protección Proactiva
- Soporte Remoto Integrado de eScan
- Soporte Técnico Gratuito 24x7 a través de correo electrónico, chat y foros

eScan®

Enterprise Security

An ISO 27001 Certified Company

www.latam.escanav.com

MicroWorld Technologies Inc.
Tel.: (+1) 248 374 5020, 248 522 7960
Email: sales@escanav.com

Awards

Partnerships

Comprehensive Protection for

SOHO • BUSINESS • CORPORATE • ENTERPRISE