eScan®
Enterprise Security

eScan Enterprise DLP - Cloud

eScan Enterprise DLP (Prevención de Fugas de Datos) – Cloud es una solución de seguridad que consiste en un conjunto de estrategias, tecnologías y técnicas diseñadas para asegurar que los usuarios finales no transmitan datos críticos o sensibles fuera de la infraestructura en la nube de una organización. Ya sea que la transmisión de datos ocurra a través de mensajes, correos electrónicos, transferencia de archivos u otros métodos, la información podría terminar en ubicaciones no autorizadas, de forma intencional o accidental. Esto puede generar problemas de cumplimiento que pueden ser eliminados con eScan Enterprise DLP.

Como solución empresarial, DLP debe detectar posibles brechas de datos o intentos de exfiltración y prevenirlos mediante la supervisión, detección y bloqueo de datos sensibles mientras están en uso (acciones en el endpoint), en tránsito (tráfico de red) y en reposo (almacenamiento de datos). Una solución DLP efectiva también debe aplicar reglas de negocio para hacer cumplir el cumplimiento normativo, la clasificación y la protección de la información confidencial. Con sus funciones avanzadas, brinda protección contra intentos de exfiltración, supervisa el acceso o fuga de datos sensibles y permite una visibilidad total de 360° sobre el uso de archivos confidenciales y la protección de los datos etiquetados como críticos por un usuario.

eScan
Enterprise DLP - Cloud

eScan Enterprise Security

¿Por qué elegir eScan Enterprise DLP?

eScan Enterprise DLP – Cloud está equipado con una amplia gama de funciones y tecnologías avanzadas para proteger los datos en tránsito o en reposo. Estas funciones te permiten rastrear, monitorear y proteger los datos críticos dentro de tu red. Se pueden configurar según tus requerimientos a través de una Consola Centralizada Empresarial de nivel seguro, que permite desplegar la solución en los endpoints conectados a tu red. eScan Enterprise DLP también brinda protección en puertas de enlace de correo electrónico para evitar la fuga de datos críticos por esta vía.

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

Una subfunción del Control de Dispositivos permite enviar notificaciones al administrador desde la consola web cuando se copia cualquier dato del disco duro del sistema cliente a un USB. El Control de Dispositivos garantiza que el robo de datos se erradique por completo, sin dejar espacio para el uso indebido de información confidencial.

Funciones clave

Control de Archivos Adjuntos y Contenido

- **Bloqueo de Archivos Adjuntos**

La función de bloqueo de archivos adjuntos en DLP te permite controlar el flujo de archivos dentro de tu organización. Puedes bloquear o permitir todos los archivos adjuntos que un usuario intente enviar a través de procesos predefinidos. También puedes excluir dominios o subdominios específicos en los que confíes, para que no se bloqueen aunque se utilicen procesos bloqueados. Existe una plantilla de informes separada para recibir información detallada por correo electrónico.

- **Informe de Archivos Adjuntos**

Esta función te ofrece un sistema de informes completo que permite determinar qué archivos adjuntos son permitidos o bloqueados por eScan Enterprise DLP. También alerta al administrador sobre los archivos que están siendo compartidos/subidos, la fuente del archivo adjunto y su destino

eScan
Enterprise DLP - Cloud

eScan®
Enterprise Security

Attachment & Content Control

• Control de Contenido Sensible (Content-Aware Control)

Esta función sobresaliente permite al administrador monitorear y controlar la información confidencial que puede ser enviada fuera del endpoint. La información sensible, también conocida como PII, que muchas veces está regulada por normativas gubernamentales como GDPR, puede clasificarse de la siguiente manera (nuevas categorías se agregan constantemente y pueden personalizarse según el país o cliente):

- Número de tarjeta Aadhar
- Número de licencia de conducir
- Número de pasaporte
- Número de tarjeta PAN
- Número de identificación de votante
- Números de tarjeta de crédito (RUPAY, VISA, Amex, MasterCard, Diners Club, Maestro, etc.)
- Números de cuenta bancaria internacional (IBAN)

El filtrado de eScan Enterprise DLP para la PII anterior puede aplicarse a diversos canales como:

- Dispositivos de almacenamiento externo (USB, CD/DVD, Bluetooth)
- Impresoras
- Comunicación de red

• Acceso a servicios corporativos basados en la nube: Correo, almacenamiento y comunicación

Existen diversas maneras en las que los empleados, al usar Gmail Corporativo, O365, Slack, WebEx, Dropbox, etc., por motivos laborales, ponen en riesgo los datos de la empresa. Para evitar cualquier posible fuga, eScan Enterprise DLP permite bloquear el acceso a cuentas personales de servicios en la nube. Esta función garantiza que los miembros del equipo solo puedan acceder a estos servicios usando sus credenciales corporativas. Se admiten los siguientes servicios:

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

eScan
Enterprise DLP - Cloud

eScan®
Enterprise Security

Attachment & Content Control

• Informe de Correo Electrónico

El correo electrónico es una de las herramientas más comunes de comunicación empresarial que permite adjuntar archivos, compartir enlaces e intercambiar información corporativa. El informe de correo electrónico de eScan Enterprise DLP proporciona al administrador detalles precisos sobre el destinatario, los tipos de archivos adjuntos, el tamaño del correo, entre otros. El administrador puede así monitorear y controlar la posible fuga de información vía correo electrónico.

• Copia Sombra de Archivos Permitidos para Subida

Esta función de eScan Enterprise DLP genera copias de los archivos transferidos por la web, correo electrónico o almacenamiento en línea (Google Drive, OneDrive, Dropbox, etc.). Cuando se realiza cualquier actividad de transferencia de archivos, se pueden crear copias sombra en función del destinatario, nombre del remitente y tamaño del archivo adjunto, lo que garantiza una supervisión efectiva de los datos compartidos o almacenados.

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 permiten definir qué datos se pueden imprimir, en qué impresoras y por quién. Una ventaja de esta solución es que, en caso de actividad no autorizada, el sistema DLP registra el incidente, notifica al usuario sobre los riesgos e incluso puede bloquear la impresión. Las posibles brechas activan alertas que se envían al administrador. Este módulo también permite al administrador bloquear por completo o de forma selectiva las impresoras de red.

• Control de Acceso Wi-Fi

Los puntos de acceso Wi-Fi vienen con un SSID y contraseña predeterminados que deben actualizarse, aunque muchas veces no se hace. Esto facilita que un atacante inicie sesión, tome control del router, modifique configuraciones, cargue programas maliciosos o incluso cambie el servidor DNS para redirigir todo el tráfico a su IP. El control de acceso Wi-Fi permite bloquear o permitir redes Wi-Fi específicas para acceder a tu red, en base a una lista blanca de SSIDs autorizados (Whitelisted).

• Control de Acceso a Almacenamiento

La protección de control de dispositivos en eScan Enterprise DLP evita que los usuarios o endpoints utilicen medios de almacenamiento removibles no autorizados. La solución impide que se copien elementos o información en dispositivos de almacenamiento USB no protegidos, bloqueando así la escritura de datos en unidades removibles que no estén autorizadas

• Control de Dispositivos Periféricos

eScan Enterprise DLP protege los datos críticos para que no salgan de la empresa a través de dispositivos periféricos o removibles como unidades USB, dispositivos Bluetooth, y CDs o DVDs grabables. El control de dispositivos permite monitorear y controlar las transferencias de datos desde todas las computadoras de escritorio y laptops, independientemente de dónde estén los usuarios o los datos confidenciales, incluso cuando no están conectados a la red corporativa.

eScan
Enterprise DLP - Cloud

eScan®
Enterprise Security

Análisis del Comportamiento de Entidades 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 los equipos administrados. Además, en caso de uso indebido de archivos oficiales, se puede rastrear al usuario responsable a través de los detalles capturados en el informe. El administrador puede seleccionar y filtrar el informe con base en cualquiera de los detalles registrados.

• Actividad de Sesión

Este submódulo monitorea y registra las actividades de sesión en los equipos administrados. Muestra un informe del tipo de operación, fecha, nombre del equipo, grupo, dirección IP y descripción del evento. Con este informe, el administrador puede rastrear las actividades de inicio y cierre de sesión de los usuarios, junto con las sesiones remotas que se hayan llevado a cabo en todos los equipos administrados.

• Actividad del Usuario

La Actividad del Usuario permite monitorear la actividad de impresión, sesión, aplicaciones y archivos que ocurre en las computadoras cliente. También proporciona informes de las aplicaciones en ejecución. La Actividad de Impresión monitorea y registra los comandos de impresión enviados desde todos los equipos. El Informe de Acceso a Aplicaciones ofrece una vista detallada de todas las aplicaciones a las que accedieron los equipos administrados. El Informe de Actividad de Archivos muestra un reporte de los archivos creados, copiados, modificados y eliminados en los equipos administrados

• Actividad de Impresión

La Actividad de Impresión te permite llevar un control de las impresoras agregándolas a un grupo y asignándoles un nombre alias. Las impresoras pueden agregarse o eliminarse de este grupo alias. La Actividad de Impresión monitorea y registra los comandos de impresión enviados por todos los equipos. También permite filtrar los registros con base en el nombre del equipo, impresora y/o nombre de usuario. Además, este módulo permite exportar un informe detallado de la actividad de impresión en formatos XLS, PDF y HTML. El informe generado contiene la fecha de impresión, nombre del equipo, dirección IP, nombre de usuario, nombre de la impresora, nombre del documento, junto con el número de copias y páginas.

• Informe de Acceso a Aplicaciones

El módulo Informe de Acceso a Aplicaciones ofrece una vista detallada de todas las aplicaciones utilizadas en los endpoints que forman parte de los Equipos Administrados. El registro muestra la lista de aplicaciones ejecutadas y la duración durante la cual estuvo activa cada una. En la misma interfaz se encuentran opciones para filtrar o exportar el registro en el formato deseado. Se proporcionan detalles como el nombre del equipo que accedió a la aplicación y la duración de uso.

• Copia Sombra (Actividad de Archivos en USB)

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

eScan
Enterprise DLP - Cloud

eScan®
Enterprise Security

Control de Acceso

• Bloqueo de Mensajería Instantánea (IM)

Los robos cibernéticos generalmente ocurren mediante transferencias de archivos o mensajes enviados sin querer, evadiendo la seguridad tradicional del gateway. Las actividades de exfiltración de información son llevadas a cabo por atacantes que secuestran navegadores populares y aplicaciones de mensajería instantánea (como Firefox, Skype, Opera) explotando vulnerabilidades conocidas como desbordamientos de búfer o errores en condiciones de frontera. Las reglas IM de eScan Enterprise DLP solo funcionan si los procesos utilizados para transferir archivos son los que has especificado en tu lista de aplicaciones al crear la regla. La regla IM impone un bloqueo total sobre los archivos adjuntos y transferencias a través de aplicaciones de mensajería instantánea.

• Protección de Archivos Sensibles

Esta función asegura que los datos sensibles no puedan ser accedidos mediante ninguna aplicación diferente a la predeterminada especificada. Una vez que una carpeta se clasifica como "Sensitiva", su contenido no puede modificarse ni eliminarse de ninguna manera. Los archivos solo pueden ser abiertos por las aplicaciones asociadas, y cualquier tipo de edición queda bloqueada para evitar modificaciones de los datos.

• Desactivar Captura de Pantalla (Print Screen)

Esta función bloquea cualquier proceso de captura de pantalla, como la herramienta de recortes de Windows, para evitar que se obtenga una imagen de la pantalla del escritorio. Con esto, se asegura que los usuarios no puedan capturar información sensible en forma de imagen y transferirla fuera. Por lo tanto, es un aspecto fundamental de la protección DLP.

• Desactivar (Copiar/Pegar/Arrastrar/Soltar)

En un dispositivo, una vez que una aplicación copia datos al portapapeles, otra aplicación puede acceder a esa información. Al desactivar la opción de Copiar/Pegar, se impide que el usuario copie cualquier información al portapapeles.

• Encriptación de Archivos y Carpetas

La encriptación de archivos y carpetas en DLP protege los datos sensibles y confidenciales contra accesos no autorizados y fugas de información. Ofrece un nivel avanzado de protección por contraseña para tus archivos y carpetas importantes.

• Control de Aplicaciones

La función de Control de Aplicaciones te permite bloquear la ejecución de aplicaciones no deseadas en los endpoints. Esto ayuda al administrador a controlar qué aplicaciones pueden ejecutarse. Además, eScan Enterprise DLP aplica una política de control de aplicaciones que permite monitoreo continuo para prevenir brechas de seguridad, fuga de datos e interrupciones.

• 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 y carpetas compartidas en la red. Esta función permite configurar accesos granulares de solo lectura o acceso total a compartidos individuales, controlando así el acceso y modificación de datos confidenciales

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