eScan®
Enterprise Security

eScan Enterprise EDR
(con defensa de inteligencia neuronal lA/ML)

eScan Endpoint Detection and Response (EDR) es una solución integral, integrada y en capas de protección para endpoints que ofrece visibilidad, análisis, protección y remediación en tiempo real para los endpoints. Esto ayuda a obtener información detallada y alerta al administrador sobre la actividad maliciosa, permitiendo una investigación rápida y restringiendo los ataques en los endpoints tan pronto como son detectados.

Admite acciones automáticas y manuales para restringir las amenazas potenciales en el endpoint. Reduce proactivamente los ataques, previene infecciones de malware, detecta y desactiva amenazas potenciales en tiempo real. eScan EDR es una excelente combinación de tecnologías futuristas que proporciona protección a endpoints basados en Windows, Mac y Linux dentro de la red corporativa

eScan
Enterprise EDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Características Clave - eScan EDR

Recolector de Eventos (Eventos de Seguridad) y Correlación

Todos los eventos de seguridad en Windows (intentos de inicio de sesión no autorizados, conexiones RDP y cambios en políticas) se monitorean para detectar cambios de comportamiento, violaciones de políticas y excesos de derechos otorgados. Estos eventos luego se envían al servidor mediante protocolos seguros para su análisis de amenazas y almacenamiento. Además, se recopilan todos los registros del sistema operativo y de las aplicaciones, lo que también mejora la visibilidad en tiempo real, la seguridad de la red y la gestión del tiempo.

Eventos de Violación de EDR desde Ransomware Avanzado

eScan EDR recopila los registros y eventos de los endpoints para proteger y bloquear archivos ejecutables (.exe, .dll o .src) y archivos de script (.ps, .vbs, .js) que se ejecutan automáticamente tras abrir un correo electrónico. eScan EDR utiliza sus tecnologías heurísticas PBAE para monitorear y bloquear todas las aplicaciones sospechosas de ser ransomware en función de su actividad o comportamiento. Además, finaliza la sesión de red si algún sistema infectado intenta acceder a un sistema protegido..

Análisis de Amenazas

Todos los registros de eventos se almacenan en un servidor seguro y se analizan en busca de amenazas en función del tipo de malware y su nivel de corrupción. Se verifican contra políticas y regulaciones basadas en reglas, luego se identifican y categorizan según la naturaleza y el nivel de la amenaza de seguridad.

Historical Investigation - RCA

With Windows events and Threat Analysis, a deep RCA is carried out against detected and potential threats to identify its root cause. The RCA helps you identify the loose ends in your network and take appropriate action to mitigate threats before the threat takes over the network.

Eventos de Violación de EDR desde los Endpoints

La solución eScan EDR está equipada con tecnologías avanzadas que recopilan información de todos los endpoints, categorizándolos en ataques de día cero conocidos y desconocidos. Los endpoints de eScan detectan automáticamente y envían los registros y eventos a la solución eScan EDR. Los ataques incluyen robo de credenciales, JavaScript o VBScript maliciosos, scripts potencialmente ofuscados, archivos ejecutables no confiables o sin firmar desde dispositivos removibles, creación de comandos WMI y PsExec, bloqueo de aplicaciones de Office y Adobe para la creación de procesos secundarios, inyección de código, creación de contenido ejecutable y llamadas a la API de Win32 desde macros. Los endpoints de eScan también previenen que el malware abuse de WMI para obtener persistencia en un dispositivo.

eScan
Enterprise EDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

¿Por qué eScan Enterprise EDR?

Gestión Uniforme

• Nueva Interfaz Web Segura con Panel Resumido

La nueva Interfaz Web Segura utiliza tecnología SSL para cifrar todas las comunicaciones. El panel resumido de eScan proporciona a los administradores el estado de los endpoints gestionados en formato gráfico, incluyendo Estado de Despliegue, Estado de Protección y Estadísticas, Resumen de los 10 principales, Cambios en los Activos, Panel EDR y Estado en Vivo.

• Gestión de Activos

El módulo de Gestión de Activos de eScan ayuda al administrador a realizar un seguimiento de la información del hardware y de la lista de software instalado en los endpoints. Además, permite ver los cambios de hardware realizados en la configuración de los sistemas dentro de la red. También permite exportar el informe detallado de estos cambios para obtener un conocimiento más profundo

Protección Mejorada para Endpoints

• Prevención de Pérdida de Datos (DLP)*

Con capacidades adicionales como control de adjuntos, control de contenido, protección de archivos/carpetas sensibles, monitoreo de actividad de archivos, aplicaciones de espacio de trabajo y varias otras funciones, eScan protege a las organizaciones del riesgo asociado con la transferencia no autorizada de contenido sensible. Es una función adicional.

• Autenticación de Dos Factores (2FA)*

eScan proporciona una capa adicional de protección al proceso de inicio de sesión que autentica y evita que los delincuentes accedan a la computadora y a los datos personales. Esto ofrece un paso adicional de seguridad, ya que los ciberdelincuentes necesitan más que un nombre de usuario y contraseña para la autenticación. Es una función adicional

eScan
Enterprise EDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

¿Por qué eScan Enterprise EDR?

Impulsado por Tecnologías Futuristas

- **Motor de Análisis de Comportamiento Proactivo (PBAE)**

  PBAE proporciona protección en tiempo real para organizaciones y usuarios contra ataques de ransomware. Monitorea la actividad de todos los procesos y bloquea aquellos cuyo comportamiento coincida con el de un ransomware.

- **Módulo de Protección de Servicios de Terminal (TSPM)**

  eScan está equipado con un TSPM mejorado que no solo detecta y bloquea direcciones IP sospechosas y ataques de fuerza bruta, sino que también permite incluir direcciones IP en la lista blanca para conexiones RDP seguras.

- **Patrón de Aprendizaje No Intrusivo (NILP)**

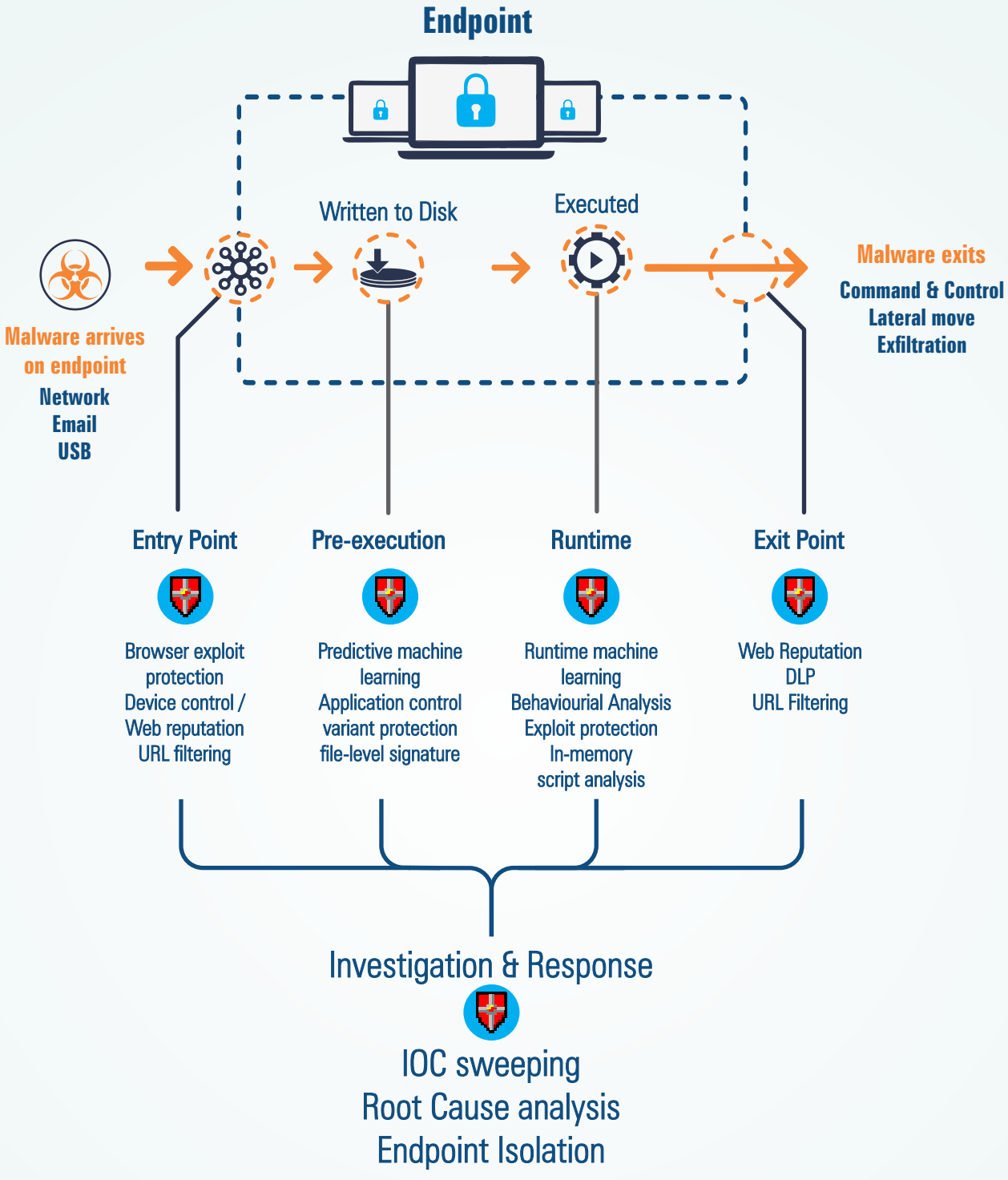
  eScan utiliza el Patrón de Aprendizaje No Intrusivo (NILP), una tecnología revolucionaria que emplea el filtrado bayesiano y opera bajo los principios de la Inteligencia Artificial (IA) para analizar cada correo electrónico y prevenir que los correos no deseados y de phishing lleguen a su bandeja de entrada. Cuenta con capacidades de autoaprendizaje y se actualiza mediante fuentes de investigación regulares de los servidores de MicroWorld. Utiliza un mecanismo adaptativo para analizar cada correo electrónico y categorizarlo como spam o legítimo en función del patrón de comportamiento del usuario.

- **Capa Winsock de MicroWorld (MWL)**

  La "Capa Winsock de MicroWorld" (MWL) de eScan es un concepto revolucionario en el escaneo del tráfico de Internet en tiempo real. Ha cambiado la forma en que el mundo enfrenta las amenazas de seguridad de contenido. A diferencia de otros productos y tecnologías, MWL enfrenta la amenaza antes de que llegue a sus aplicaciones. MWL está técnicamente ubicado por encima de la capa WinSock y actúa como un "Guardián Transparente" en la capa WinSock del sistema operativo

eScan
Enterprise EDR
(con defensa de inteligencia neuronal lA/ML)

eScan®
Enterprise Security



eScan
Enterprise EDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Características Clave - Consola de Gestión de eScan

Panel Exclusivo de EDR

eScan proporciona un panel de control resumido de los incidentes que permite a los administradores obtener información más detallada y tomar acciones rápidas en cuanto se detectan amenazas. Brinda una visión general de incidentes relacionados con eScan, Windows, endpoints y la red en formato gráfico y detallado.

Antirrobo*

eScan le ayuda a bloquear el dispositivo, generar alertas, activar una alarma sonora, borrar datos y localizar los dispositivos. eScan garantiza una protección completa contra accesos no autorizados en caso de que su dispositivo se pierda o sea robado. Es una función adicional para los endpoints con Windows.

Administración Basada en Roles

La Administración Basada en Roles a través de la Consola de Gestión de eScan permite a los administradores crear grupos de administradores con niveles de privilegios predefinidos para un acceso más seguro.

Configuraciones Avanzadas

eScan proporciona diversas configuraciones avanzadas, como Clientes en Itinerancia, Prevención de Brotes, SIEM, creación de informes con logotipo personalizado, Políticas de Seguridad Avanzadas, Plantillas de Criterios de Políticas y muchas más.

ADS (Sincronización con Active Directory)

Con esta función, los administradores pueden sincronizar los grupos de la Consola Centralizada de eScan con los contenedores de Active Directory. Los nuevos equipos y contenedores descubiertos en Active Directory se copian automáticamente en la Consola Centralizada de eScan, y se puede enviar una notificación a los administradores del sistema sobre estos cambios.

Actualizador en Vivo del Cliente

Con la ayuda del Actualizador en Vivo del Cliente de eScan, los eventos relacionados con eScan y el estado de seguridad de todos los endpoints se capturan, registran y pueden ser monitoreados en tiempo real. También puede exportar eventos en un archivo de Excel

eScan
Enterprise EDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Características Clave - Consola de Gestión de eScan

Clientes Excluidos

Esta función permitirá al administrador restringir los endpoints cliente para que no sean agregados automáticamente a ningún grupo desde computadoras no administradas. El administrador debe agregar las computadoras utilizando el nombre de host, nombre de host con comodín, dirección IP o rango de IP en la lista. Ahora, las computadoras listadas no serán agregadas automáticamente en los grupos administrados.

Agrupación Automática

Esta función permite al administrador agregar clientes automáticamente a subgrupos apropiados. Aquí, los administradores deberán crear grupos y luego agregar criterios de clientes basados en host / nombre de host con comodín / dirección IP / rango de IP.

Prevención de Brotes

Si el conteo de virus excede los límites establecidos por el administrador, se enviará una notificación por correo electrónico de brote al destinatario especificado por el usuario. Esto activará simultáneamente un Aislamiento Automático de los endpoints infectados para restringir la infección dentro de la red.

Plantillas de Políticas

Las plantillas de políticas simplifican la implementación de políticas; permiten al administrador crear políticas de seguridad y cumplimiento y hacer cumplir estas políticas en los grupos administrados designados.

eScan
Enterprise EDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Características Clave - eScan Endpoints (Windows)

eBackup & Restore#

eScan permite al administrador realizar copias de seguridad de todos los archivos de forma manual o automática (según un horario programado) y almacenarlas en un formato cifrado y comprimido. También permite realizar copias de seguridad en una unidad local, en una unidad de red o en la nube (función adicional). eScan permite al administrador importar/exportar los datos del servidor, los cuales pueden restaurarse en caso de fallas del sistema o desastres.

Monitoreo y Gestión Remota (RMM)*

El monitoreo y gestión remota (RMM) es un tipo de software de gestión de TI remota utilizado por Proveedores de Servicios Administrados de TI (MSPs) que permite a los administradores rastrear problemas y monitorear activos de TI de forma remota. Ayuda a las organizaciones a obtener información sobre el rendimiento, la salud y el estado de sus endpoints. Es una función adicional.

Gestión de Parches*

eScan verifica la información del sistema operativo y proporciona automáticamente parches de seguridad críticos junto con actualizaciones. El servidor de eScan descarga los parches para diferentes versiones de Windows OS y los distribuye a los distintos endpoints. El módulo de Informes de Parches muestra la cantidad de parches de seguridad de Windows instalados y no instalados en las computadoras administradas. Esto ayudará al administrador a identificar la cantidad de sistemas vulnerables en la red e instalar rápidamente los parches críticos. También es una función adicional.

Informe de Actividad de Sesión

La Consola de Gestión de eScan monitorea y registra la actividad de sesión de las computadoras administradas. Mostrará un informe del inicio/apagado de los endpoints, inicio/cierre de sesión y conexión/desconexión de sesiones remotas. Los administradores pueden usar este informe para rastrear las actividades de inicio y cierre de sesión de los usuarios, así como las sesiones remotas en todas las computadoras administradas.

Actualizaciones sin Conexión

eScan responde a la necesidad de actualizaciones sin conexión en redes aisladas permitiendo que el administrador use una computadora conectada a internet para predescargar todas las actualizaciones necesarias para las computadoras en la red aislada y luego copiar los archivos de actualización a dicha red.

Agente de Actualización

Los administradores pueden agregar computadoras como Agentes de Actualización. Como resultado, se reduce el tráfico entre el Servidor Corporativo de eScan y el cliente. Las actualizaciones de firmas y políticas se descargarán desde el Servidor de eScan EDR y se distribuirán a las demás computadoras administradas en el grupo a través del Agente de Actualización. Esto ahorra ancho de banda y mejora el rendimiento.

eScan
Enterprise EDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Monitoreo de Actividad de Impresión

El módulo de Actividad de Impresión en eScan monitorea y registra de manera eficiente las tareas de impresión realizadas por todos los endpoints administrados. También proporciona un informe detallado en formatos PDF, Excel o HTML de todas las tareas de impresión realizadas por los endpoints administrados a través de cualquier impresora conectada a una computadora en la red o localmente.

Control de Privacidad

El control de privacidad permite programar el borrado automático de la memoria caché, ActiveX, cookies, complementos e historial. También ayuda a eliminar archivos y carpetas de forma permanente sin el riesgo de que sean recuperados por aplicaciones de terceros, evitando así la explotación de datos.

Anti-Spam Avanzado

eScan proporciona protección contra correos electrónicos no deseados con su poderosa tecnología Anti-Spam. Verifica el contenido de los correos electrónicos entrantes y salientes y pone en cuarentena los correos comerciales. Además, eScan utiliza potentes motores antivirus duales basados en heurística para escanear todos los correos electrónicos en busca de virus, gusanos, troyanos, spyware, adware y contenido malicioso oculto en tiempo real.

Política de Seguridad Avanzada

eScan ha incluido una Política de Seguridad Avanzada que alerta a los administradores sobre actividades maliciosas, ayudando a las organizaciones a identificar y detener violaciones en tiempo real de manera automática y eficiente, sin saturar al equipo de seguridad con falsas alarmas ni afectar las operaciones del negocio.

Características Clave - eScan Endpoints (Hybrid OS)

Control de Dispositivos

eScan está equipado con la función avanzada de Control de Dispositivos que permite/bloquea el acceso a dispositivos USB en los endpoints de la red. El acceso a la cámara web, tarjetas SD, imágenes, Bluetooth y dispositivos compuestos está restringido en los endpoints con Windows. El acceso a memorias USB puede ser restringido en Windows, Mac y Linux. El acceso a CD-ROM puede ser restringido en Windows y Linux.

Escaneo Programado

eScan le ofrece una opción para realizar escaneos programados, que se ejecutarán sin problemas en segundo plano sin interrumpir su entorno de trabajo actual. Realiza escaneos programados para archivos/carpetas seleccionados o para todo el sistema durante el período programado, proporcionando así la mejor protección contra amenazas cibernéticas.

eScan
Enterprise EDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Características Clave - eScan Endpoints (Hybrid OS)

Protección Web Avanzada

eScan está equipado con Protección Web Avanzada que protege contra el acceso a páginas peligrosas, de phishing y fraudulentas. Permite al administrador definir la lista de sitios a restringir o incluir en la lista blanca en los endpoints conectados a la red. Como resultado, cuando una URL apunta a un sitio web conocido por phishing o fraude, o a contenido malicioso como spyware o virus, la página web es bloqueada y se muestra una alerta. eScan también proporciona restricciones de acceso basadas en el tiempo en los endpoints con Windows.

Firewall Bidireccional Mejorado

El Firewall Bidireccional de eScan filtra todas las solicitudes de red entrantes y salientes, lo que permite monitorear cada conexión entrante y saliente que se está estableciendo. Esto impide que los hackers se conecten al sistema y defiende la conexión de aplicaciones no deseadas a internet. Proporciona la capacidad de definir la configuración del firewall, así como definir el rango de IP, las aplicaciones permitidas, las direcciones MAC de confianza y las direcciones IP locales.

Control de Aplicaciones

El Control de Aplicaciones de eScan le ayuda a adelantarse a los ciberdelincuentes y mantiene su negocio seguro y productivo. Previene ataques de día cero y ATP bloqueando la ejecución de aplicaciones no autorizadas. Mediante la lista blanca, los administradores pueden prevenir ataques de malware desconocido permitiendo solo aplicaciones conocidas en la lista blanca

Reverse Shell

La función Reverse Shell de eScan para endpoints basados en Linux restringe los ataques de reverse shell desde una máquina remota. De esta manera, se evita que los atacantes exploten una vulnerabilidad de ejecución remota de comandos mediante una sesión de reverse shell.

Monitoreo de Integridad de Archivos

El Monitoreo de Integridad de Archivos de eScan valida la integridad de los valores de archivos y carpetas entre el estado actual y el estado original del archivo para detectar posibles compromisos en endpoints basados en Linux.

eScan
Enterprise EDR
(con defensa de inteligencia neuronal IA/ML)

eScan®
Enterprise Security

Otros Aspectos Destacados

- Anti-Malware de última generación con protección basada en firmas y comportamiento
- ODS (Escaneo Bajo Demanda) para Windows, Mac y Linux
- Gestión de Licencias
- Importación y Exportación de Configuraciones
- Despliegue de Tareas
- Prevención de Brotes Mejorada
- Clientes en Itinerancia (Nuevo)
- Registro de Auditoría (Nuevo)
- Modo de Rescate para Windows y Linux
- Filtro de URLs Maliciosas
- Envío de Mensajes a los Endpoints Cliente
- Informe Forense
- Soporte Remoto de eScan Integrado
- Soporte Técnico en Línea GRATUITO 24x7 a través de Correo Electrónico, Chat y Foros

NOTA

* Esta función requiere una licencia adicional.

Esta función requiere una licencia adicional para utilizar la nube y la unidad de red para copias de seguridad.

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