eScan Enterprise EDR - Cloud

eScan Enterprise EDR - Cloud es una solución de ciberseguridad de nivel empresarial basada en plataforma SaaS, diseñada para redes corporativas. eScan EDR (Detección y Respuesta en el Endpoint) proporciona una protección integral, integrada y en capas para los endpoints, ofreciendo visibilidad en tiempo real, análisis, protección y remediación para los equipos conectados en una red. Esto permite obtener información profunda y alertar al administrador sobre actividades maliciosas, facilitando una investigación rápida y restringiendo los ataques en los endpoints tan pronto como son detectados.

Es compatible con acciones automáticas y manuales para restringir amenazas potenciales en el endpoint. Reduce proactivamente los ataques, previene infecciones por malware, detecta y neutraliza amenazas en tiempo real. eScan EDR es una excelente combinación de tecnologías futuristas que protege endpoints con sistemas operativos Windows, Mac y Linux dentro de la red corporativa.

eScan
Enterprise EDR - Cloud

eScan®
Enterprise Security

Why 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 al administrador el estado de los endpoints administrados en formato gráfico, como Estado de Despliegue, Estado de Protección y Estadísticas, Top 10 resumen, Cambios de Activos y Panel EDR.

• Gestión de Activos

El módulo de Gestión de Activos de eScan ayuda al administrador a realizar un seguimiento de la información del hardware y 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 informes detallados para un conocimiento más profundo.

Impulsado por Tecnología Futurista

• Motor de Análisis de Comportamiento Proactivo (PBAE)

PBAE brinda protección en tiempo real a organizaciones y usuarios contra ataques de ransomware. Supervisa la actividad de todos los procesos y bloquea aquellos cuyo comportamiento coincide 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 ataques de fuerza bruta y direcciones IP sospechosas, sino que también permite agregar direcciones IP a una 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 filtrado bayesiano y se basa en principios de Inteligencia Artificial (IA) para analizar cada correo electrónico y prevenir que correos spam y de phishing lleguen a tu bandeja de entrada. Tiene capacidades de autoaprendizaje y se actualiza regularmente mediante fuentes de investigación de los servidores de MicroWorld.

• Capa Winsock de MicroWorld (MWL)

La “Capa MicroWorld-WinSock” (MWL) de eScan es un concepto revolucionario para escanear el tráfico de Internet en tiempo real. Ha transformado la manera en que el mundo enfrenta las amenazas de seguridad de contenido. A diferencia de otros productos y tecnologías, MWL enfrenta las amenazas antes de que lleguen a tus aplicaciones. Técnicamente se sitúa sobre la capa WinSock y actúa como un "Portero Transparente" en esa capa del sistema operativo.

eScan
Enterprise EDR - Cloud

eScan Enterprise Security

Funciones Clave – Consola de Gestión de eScan

• Panel Exclusivo EDR

eScan proporciona un panel resumido de los incidentes que permite a los administradores obtener información más profunda y tomar decisiones rápidas al momento de la detección. Ofrece una vista general de incidentes relacionados con eScan, Windows, Endpoints y Red en formato gráfico y detallado.

• Clientes Excluidos

Esta función permite al administrador restringir que endpoints no administrados se agreguen automáticamente a cualquier grupo. El administrador puede añadir equipos usando nombre de host, comodines, dirección IP o rango de IP. Los equipos listados no serán agregados automáticamente a grupos administrados.

• Configuraciones Avanzadas

eScan ofrece varias configuraciones avanzadas como integración con SIEM, creación de informes con logotipo personalizado, políticas de seguridad avanzadas, entre otras.

• Plantillas de Políticas

Las plantillas de políticas simplifican el despliegue, permitiendo al administrador crear políticas de seguridad y cumplimiento, y aplicarlas a grupos administrados designados.

• Administración Basada en Roles

La administración basada en roles a través de la Consola de Gestión de eScan permite a los administradores crear grupos administrativos con privilegios predefinidos para un acceso más seguro.

eScan
Enterprise EDR - Cloud

eScan®
Enterprise Security

Funciones Clave – eScan EDR

• Investigación Histórica – RCA

Con los eventos de Windows y el Análisis de Amenazas, se realiza un Análisis de Causa Raíz (RCA) contra amenazas detectadas o potenciales. Esto ayuda a identificar los puntos débiles en la red y tomar acciones correctivas antes de que la amenaza se propague.

• Análisis de Amenazas

Todos los registros de eventos son almacenados en un servidor seguro y analizados con base en el tipo de malware y nivel de corrupción. Se contrastan con políticas basadas en reglas y regulaciones, y luego se identifican y clasifican según la naturaleza y nivel de amenaza.

• Recolector de Eventos (Eventos de Seguridad) y Correlación

Todos los eventos de seguridad de Windows (intentos de acceso no autorizados, conexiones RDP, cambios en políticas) son monitoreados para identificar comportamientos sospechosos, violaciones de políticas y excesos de privilegios. Estos eventos se envían al servidor usando protocolos seguros para su análisis y almacenamiento. Además, se recogen todos los logs del sistema operativo y aplicaciones, mejorando la visibilidad en tiempo real, la seguridad de red y la gestión del tiempo.

• Eventos de Violación EDR desde Ransomware Avanzado

eScan EDR recopila registros y eventos de endpoints, protegiendo y bloqueando archivos ejecutables (.exe, .dll, .src) y de scripts (.ps, .vbs, .js) que se autoejecutan al abrir un correo. Utiliza tecnologías heurísticas PBAE para monitorear y bloquear todas las aplicaciones sospechosas de comportamiento tipo ransomware. Además, finaliza la sesión de red si un sistema infectado intenta acceder a un sistema protegido.

• Eventos de Violación EDR desde Endpoints

La solución eScan EDR está equipada con tecnologías avanzadas que recogen información de todos los endpoints, clasificando los ataques de día cero conocidos y desconocidos. Los endpoints de eScan detectan automáticamente y envían registros y eventos a la solución EDR. Los ataques incluyen robo de credenciales, scripts maliciosos en JavaScript o VBScript, archivos ejecutables sin firma desde dispositivos removibles, creación de comandos WMI y PsExec, procesos secundarios desde Office y Adobe, inyección de código y llamadas a API Win32 desde macros. También previene que el malware utilice WMI para persistencia en el dispositivo.

eScan
Enterprise EDR - Cloud

eScan Enterprise Security

Funciones Clave – eScan Endpoints (Windows)

• Informe de Actividad de Sesión

La Consola de Gestión de eScan monitorea y registra la actividad de sesión de los equipos administrados. Muestra un informe de inicio/apagado, inicio/cierre de sesión y conexiones/desconexiones remotas. Los administradores pueden utilizar este informe para rastrear las actividades de inicio de sesión de los usuarios y las sesiones remotas.

• Seguridad Avanzada

eScan incluye políticas de seguridad avanzadas que alertan al administrador sobre actividades maliciosas, ayudando a las organizaciones a identificar y detener brechas en tiempo real de manera eficiente, sin abrumar al equipo de seguridad ni afectar las operaciones.

• Agente de Actualización

Los administradores pueden designar equipos como Agentes de Actualización, lo que reduce el tráfico entre el servidor corporativo y los clientes. Las actualizaciones de firmas y políticas se descargan desde el servidor EDR y se distribuyen a otros equipos del grupo a través del agente. Esto ahorra ancho de banda y mejora el rendimiento.

• Monitoreo de Actividad de Impresión

El módulo de Actividad de Impresión en eScan monitorea eficientemente y registra todas las tareas de impresión realizadas por los endpoints administrados. Proporciona informes detallados en formatos PDF, Excel o HTML sobre dichas actividades mediante cualquier impresora conectada a los equipos, en red o localmente.

• Control de Privacidad

El control de privacidad permite programar el borrado automático de caché, ActiveX, cookies, plugins e historial. También ayuda a eliminar permanentemente archivos y carpetas, evitando que puedan ser recuperados por herramientas de terceros y previniendo la explotación de datos.

• Anti-Spam Avanzado

eScan ofrece protección contra correos spam con su potente tecnología anti-spam. Revisa el contenido de los correos entrantes y salientes, poniendo en cuarentena los mensajes comerciales. Además, utiliza motores antivirus duales con capacidades heurísticas para escanear en tiempo real todos los correos en busca de virus, gusanos, troyanos, spyware, adware y contenido malicioso oculto.

eScan
Enterprise EDR - Cloud

eScan®
Enterprise Security

Funciones Clave – eScan Endpoints (Sistemas Operativos Híbridos)

• Protección Web Avanzada

eScan está equipado con Protección Web Avanzada que bloquea el acceso a páginas peligrosas, de phishing o fraudulentas. Permite al administrador definir listas de sitios para bloquear o permitir en los endpoints conectados a la red. Si una URL lleva a contenido malicioso o sitios falsos, la página se bloquea y se muestra una alerta. También permite restricciones de acceso basadas en horario en endpoints Windows.

• Firewall Bidireccional Mejorado

El firewall bidireccional de eScan filtra todas las solicitudes de red entrantes y salientes, permitiendo monitorear cada conexión establecida. Esto evita conexiones de hackers al sistema y bloquea que aplicaciones no deseadas se conecten a Internet. Permite definir configuraciones de firewall, rangos de IP, aplicaciones permitidas, direcciones MAC de confianza y direcciones IP locales.

• Escaneo Programado

eScan ofrece la opción de escaneo programado, ejecutándose en segundo plano sin interrumpir el trabajo del usuario. Permite programar escaneos para archivos/carpetas específicos o todo el sistema, brindando la mejor protección contra amenazas cibernéticas.

• Control de Aplicaciones

El Control de Aplicaciones de eScan ayuda a prevenir ataques de día cero y amenazas persistentes avanzadas bloqueando la ejecución de aplicaciones no autorizadas. A través de listas blancas, los administradores pueden permitir únicamente aplicaciones confiables, evitando ataques por malware desconocido.

• Reverse Shell

La función Reverse Shell de eScan para endpoints basados en Linux restringe ataques de shell inverso desde máquinas remotas, evitando que atacantes exploten vulnerabilidades de ejecución remota.

• Monitoreo de Integridad de Archivos

El Monitoreo de Integridad de Archivos de eScan valida la integridad de archivos y carpetas comparando el estado actual con el original, detectando posibles compromisos en endpoints Linux.

• Control de Dispositivos

eScan cuenta con Control Avanzado de Dispositivos que permite/bloquea el acceso a dispositivos USB en los endpoints. El acceso a cámaras web, tarjetas SD, dispositivos de imagen, Bluetooth y dispositivos compuestos se restringe en Windows. El acceso a unidades USB puede restringirse en Windows, Mac y Linux. El acceso a CD-ROM puede bloquearse en Windows y Linux.

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