Una plataforma de seguridad para la sostenibilidad de empresas industriales y la transformación digital

Plataforma de Kaspersky Industrial CyberSecurity

kaspersky BRING ON THE FUTURE

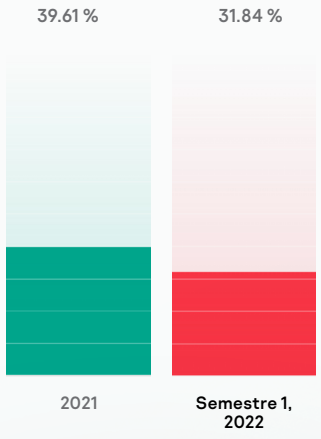
Atacadas por malware

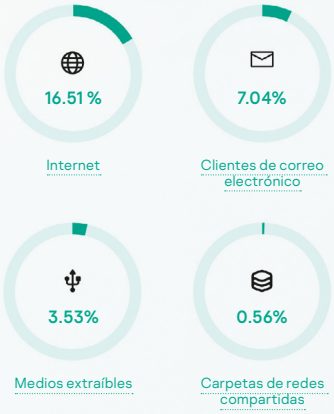
Desde principios de 2022, cerca del 30 % de las computadoras relacionadas con el ICS han sido atacadas por malware: casi un 10% menos que el año pasado

Kaspersky ICS-CERT, junio de 2022

Más información

Porcentaje de computadoras ICS a las que se le bloquearon elementos maliciosos desde que empezó el 2022





Las empresas industriales abordan la ciberseguridad en sus infraestructuras de TI y TO (tecnología operativa) de manera diferente. La mayoría de las empresas ya tienen desarrolladas medidas de detección y respuesta en sus redes corporativas, pero cuando se trata de TO, suelen tener un enfoque desactualizado de aislamiento físico. Las empresas industriales se están volviendo cada vez más "digitales", por lo que invierten más y más en tecnologías inteligentes, nuevos sistemas de automatización y en la adopción de la transformación digital. Esto en realidad elimina la brecha tradicional entre los entornos de TI y TO, una brecha que evitaba que las ciberamenazas alcanzaran la automatización industrial y los sistemas de control.

Usted puede ser un blanco, pero no sea una víctima

No es necesario ser un blanco para convertirse en una víctima de brechas accidentales de aislamiento físico o de una infección de malware. Una sola unidad flash, un celular, un correo electrónico de phishing o un ransomware que se meta en el entorno ICS puede afectar gravemente la actividad principal de una empresa. A su vez, un grupo motivado de hackers puede penetrar las redes de la TO y causar daños importantes a los equipos, los procesos, la producción, la seguridad y la calidad, o robar información valiosa.

Ciberseguridad esencial para la TO

Protección de endpoints

para sistemas independientes y conectados. Una solución segura y probada debe ayudar a ejecutar las políticas de seguridad, respaldar el cumplimiento, realizar auditorías de seguridad, administrar el inventario, llevar a cabo tareas de parches y recopilar telemetría precisa como sensor de endpoints

Protección de redes

para la visibilidad en la comunicación, detección de amenazas y administración de activos. El sistema de detección de intrusiones y análisis del tráfico de red controla la eficacia de los ajustes del firewall, la segmentación de la red y el cumplimiento del uso de la red, y ayuda a proporcionar una respuesta manual segura

Programas de capacitación

para que los empleados reduzcan la cantidad de accidentes y minimicen el factor humano (errores humanos)

Servicios de expertos

para investigar los análisis experimentados de la conducta de la infraestructura o mitigar el impacto de un incidente

Reconocimiento global

Frost & Sullivan reconoció a Kaspersky con el premio a la empresa global del año 2020 según el análisis del mercado de ciberseguridad industrial global (TO/ICS)

En la encuesta global anual de **VDC**, Kaspersky fue el mejor proveedor en la categoría de ciberseguridad industrial, según las puntuaciones generales de más de 250 profesionales calificados de la comunidad de la automatización industrial

Lo que Kaspersky tiene para brindar

La plataforma de Kaspersky Industrial CyberSecurity (KICS) hecha de tecnologías integradas de manera nativa, junto con nuestra cartera de servicios y capacitación experta, se ocupan de todas las necesidades de ciberseguridad de las empresas industriales y los operadores de infraestructura crítica.

La plataforma es un elemento fundamental en un ecosistema único para las empresas industriales que incluye lo siguiente:

- **Soluciones empresariales inmejorables de Kaspersky, que brindan una verdadera convergencia de TI y TO y los múltiples beneficios de tener el enfoque de un solo proveedor**
- **Soluciones especializadas variadas para la seguridad ciberfísica, la seguridad del IoT industrial, el aprendizaje automático, el espacio de trabajo remoto seguro y muchas otras más, que proporcionan una escalabilidad ágil e ilimitada**

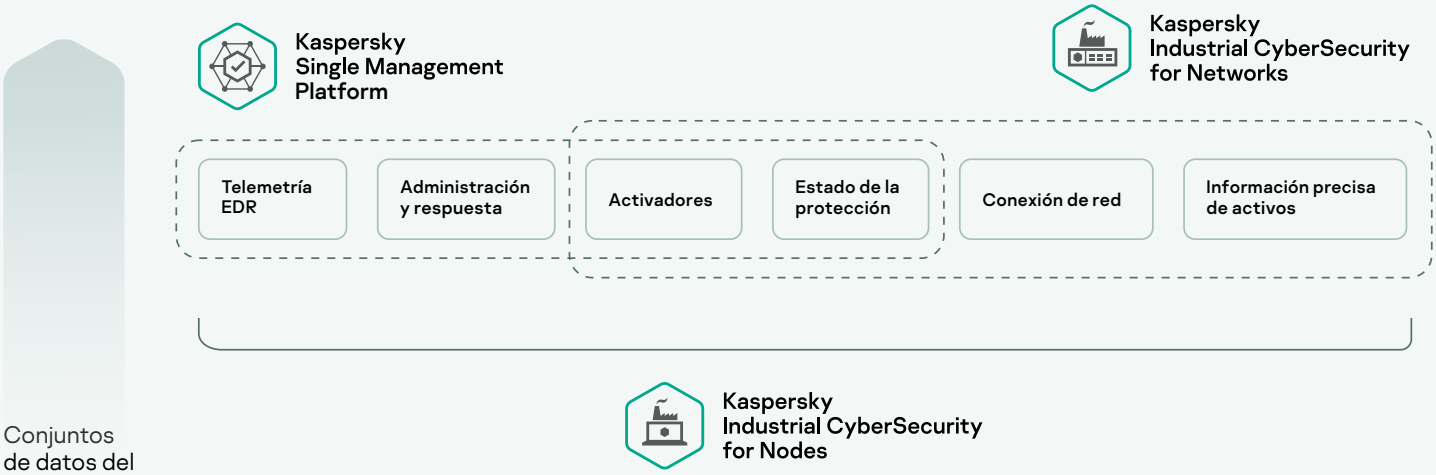
La plataforma de Kaspersky Industrial CyberSecurity lidera las siguientes categorías:

- Seguridad de endpoints en la TO
- Monitoreo y visibilidad de la red en la TO
- Detección de anomalías, respuesta ante incidentes e informes
- Servicios de seguridad en la TO

Cuando se usan en conjunto, el usuario tiene una visión y un contexto más amplios: la cadena de incidentes en el nivel de la red y los endpoints, los parámetros precisos de los activos, la comunicación de la red y los mapas topológicos, incluso de los segmentos donde la duplicación de tráfico aún no está disponible, entre otras cosas.

Productos

KICS es una plataforma de ciberseguridad de TO diseñada para una protección completa de los componentes principales de la automatización industrial y del sistema de control en todos los niveles. La integración continua entre los componentes de la plataforma proporciona una visibilidad completa de las múltiples redes de TO y los sistemas de automatización distribuidos geográficamente. De esta manera, se le brinda al cliente una experiencia mejorada, conocimiento de la situación y flexibilidad en la implementación.



KICS for Nodes es un software de protección, detección y respuesta de endpoints con auditorías de cumplimiento y funcionalidad de sensor de endpoints.

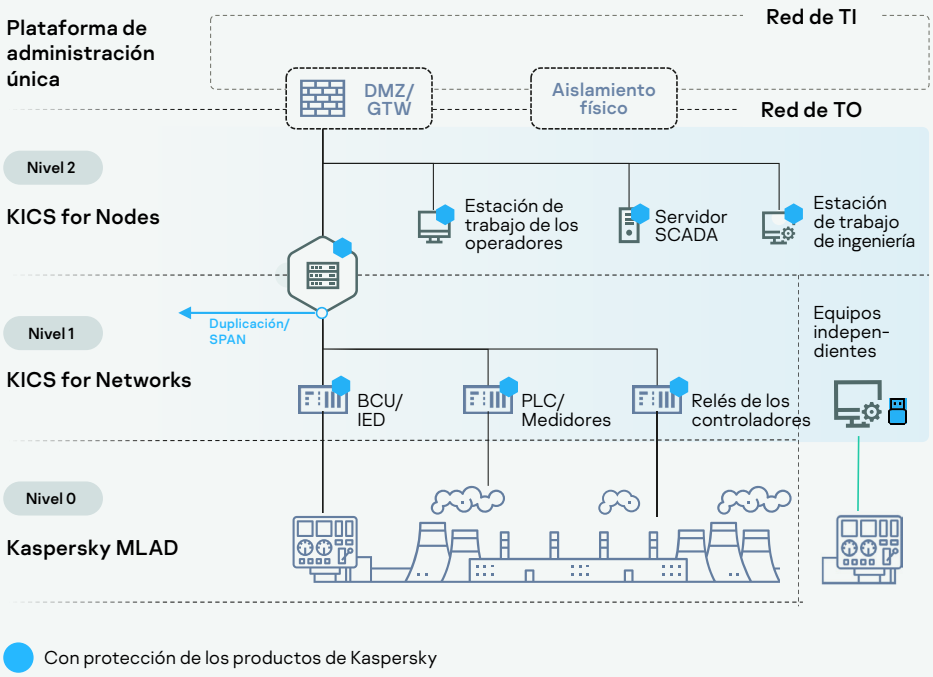
KICS for Networks está diseñado para el análisis, la detección y la respuesta del tráfico en la red de TO.

La plataforma de administración única proporciona una interfaz EDR avanzada y una rápida escalabilidad a numerosas ubicaciones.

Funciones adicionales

Esta solución proporciona numerosas funciones adicionales. La tecnología del **sondeo activo** de red permite una recopilación rápida y precisa de la topología de la red y los ajustes de los activos. La función **auditoría de endpoints** ayuda a garantizar el cumplimiento de la política de seguridad, que incluye la seguridad de los ajustes actuales y las vulnerabilidades del control. El método de distribución **escáner portátil** de KICS for Nodes ayuda a establecer mejores prácticas de auditorías de seguridad de los equipos independientes y con aislamiento físico. **El aprendizaje automático para la detección de anomalías** es un sistema de detección temprana de anomalías en lo profundo del proceso tecnológico.

Arquitectura de la solución



Características

Detección de activos
Inventario e identificación de activos pasivos de TO

Inspección exhaustiva de paquetes
Análisis casi en tiempo real de la telemetría del proceso técnico

Control de integridad de la red
Detecta hosts y flujos no autorizados en la red

Sistema de detección de intrusiones
Envía alertas sobre actividades maliciosas en la red

Control de comandos
Inspecciona los comandos por encima de los protocolos industriales

Integración externa
La integración flexible de la API agrega capacidades de detección y prevención

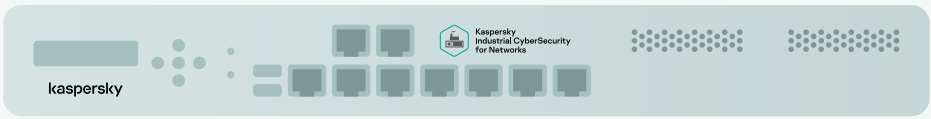
Aprendizaje automático para la detección de anomalías (MLAD)
Busca anomalías cibernéticas o físicas a través de la telemetría en tiempo real y minería de datos históricos (red neuronal recurrente)

Administración de vulnerabilidades
Base de datos actualizable de las vulnerabilidades en los equipos industriales, con tecnología Kaspersky ICS CERT

Kaspersky Industrial CyberSecurity for Networks

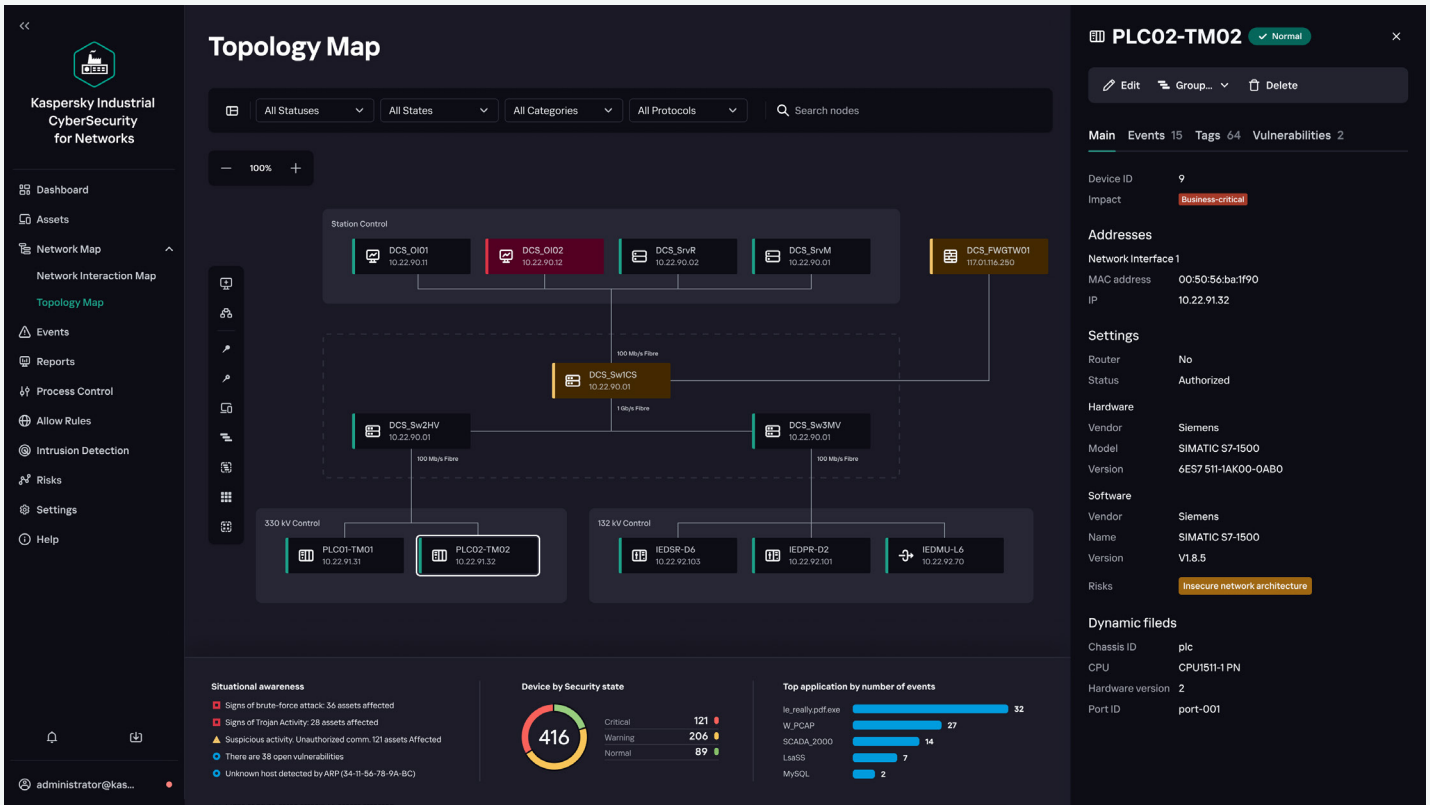
Análisis, detección y respuesta del tráfico en la red de TO. Visibilidad de riesgos clara con monitoreo de tráfico pasivo, sondeo activo y sensores de endpoints.

Detecta anomalías e intrusiones dentro de las redes ICS en sus etapas tempranas y garantiza que se estén llevando a cabo las acciones necesarias para evitar cualquier impacto negativo en los procesos industriales.



Una solución que no depende de ningún dispositivo. Puede integrarse de manera rápida y óptima a las prácticas establecidas de abastecimiento, integración y garantía de nuestros clientes.

Interfaz



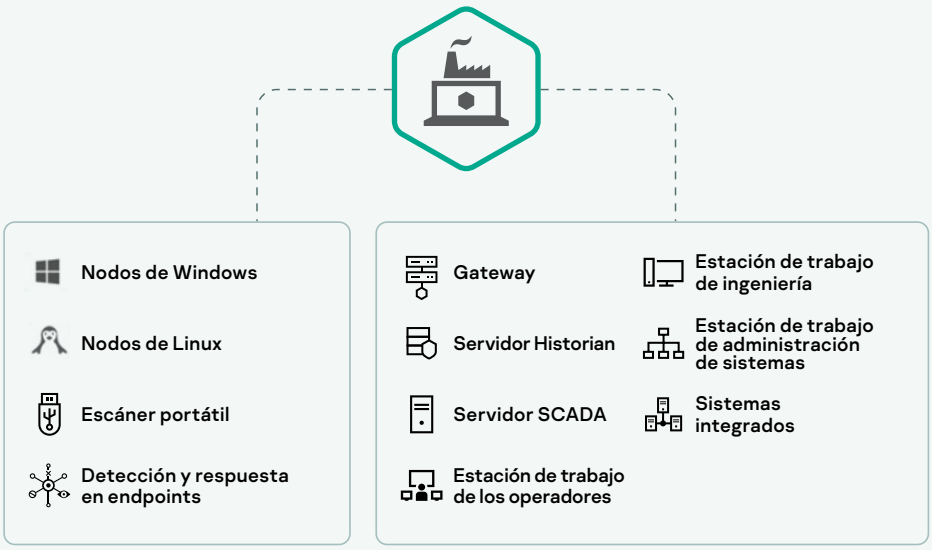
KICS for Nodes se diseñó específicamente para los requisitos estrictos de los sistemas de automatización distribuidos: entornos complicados y mixtos, tiempo ampliado en la operación, casos de uso independientes y conectados, instancias asistidas y libres de mantenimiento y prioridad de la disponibilidad del control a toda costa

Kaspersky Industrial CyberSecurity for Nodes

Protección, detección y respuesta de endpoints de calidad industrial, comprobada y certificada. Una solución estable, de bajo impacto y compatible para Linux, Windows y sistemas independientes.

Protección, detección y respuesta de endpoints industriales

Protege todos los endpoints de un sistema de automatización moderno, digital, administrado y distribuido. Revela nuevos niveles de visibilidad de incidentes en el proceso de análisis de la causa raíz. El agente recopila la telemetría del endpoint para crear una representación visual clara y detallada del progreso de un incidente en las estaciones de trabajo, los servidores, las puertas de enlace y otros endpoints. De este modo, se asegura a los administradores del sistema de automatización que se resolvió el incidente por completo y que no sucederá de nuevo.



Ventajas

Bajo impacto
sobre el dispositivo protegido para un mejor rendimiento del sistema

Compatible
con computadoras de bajo rendimiento de generaciones anteriores y sistemas como Windows XP SP2, Windows Server 2003 SP1 y versiones posteriores

Ciclo de vida extendido
hasta 5 años con licencia y soporte ampliado

Funcionalidad completa
para todos los sistemas operativos MS Desktop, Server y Windows Embedded

Implementación modular
Opciones flexibles y ajustes seguros y no intrusivos

Cubre infraestructuras mixtas
Windows, Linux y variantes portátiles

Escáner portátil de KICS for Nodes
Ejecuta las políticas de ciberseguridad en los mecanismos independientes, los sistemas de automatización o los equipos en los que no se puede instalar un software de seguridad. El mejor conocimiento de la situación y visibilidad de TO incluso desde una infraestructura independiente.

Solución libre de instalaciones
KICS for Nodes se puede activar en varias unidades flash adicionales del escáner portátil. Esto ayuda a realizar análisis a pedido en simultáneo en varias máquinas durante las ventanas de mantenimiento para recopilar datos de los endpoints y organizarlos en un informe de resumen adecuado.

Cumplimiento de las políticas internas y normativas
El escáner portátil de KICS for Nodes realiza verificaciones del cumplimiento del antimalware de los equipos que acceden a un sitio de TO, incluidas las computadoras de contratistas de terceros. Tiene un impacto operativo muy bajo y no interfiere con las soluciones de seguridad existentes.

Ventajas

- Visión de la situación
- Administración de políticas/ sistemas
- Cadena de ataque y respuesta
- Informes y notificaciones
- Integración de SIEM
- Integración de HMI/MES

Kaspersky Single Management Platform

La plataforma de administración única es una solución centralizada de administración de seguridad para la orquestación de la seguridad de toda la infraestructura de TO. Contiene un mapa de todos los activos distribuidos geográficamente que se enriquecen con eventos, análisis de incidentes y más. Aumenta la eficiencia de los equipos de seguridad de TO y TI mixtos. Un lugar donde todos sus controles de seguridad trabajan en armonía, lo que permite una respuesta rápida y precisa.

> Su experiencia en el campo de la ciberseguridad ICS, su profesionalismo y la complejidad de su solución en comparación con otros proveedores, nos aportó un gran valor y nos garantizó un futuro brillante para la estrategia de seguridad de nuestra empresa.
>
> Ondřej Sýkora,
> responsable de C&A,
> Plzeňský Prazdroj

> Mediante la práctica y el aprendizaje de los conocimientos del equipo de Kaspersky, aumentamos nuestra protección frente a las amenazas a la ciberseguridad.
>
> Yu Tat Ming,
> CEO, PacificLight

Servicios de expertos

Nuestro paquete de servicios es una parte importante de la cartera de KICS. Proporcionamos el ciclo completo de servicios de seguridad, desde evaluaciones de la ciberseguridad industrial hasta respuestas a incidentes.

Evaluación de ciberseguridad industrial

Evaluación de la ciberseguridad industrial: Kaspersky brinda una evaluación de ciberseguridad industrial que no es invasiva e incluye pruebas de penetración externas e internas, evaluación de seguridad de TO y evaluación de seguridad de la solución de automatización. Los expertos de Kaspersky proporcionan una perspectiva de gran valor sobre la infraestructura de una empresa y aportan recomendaciones sobre cómo reforzar la postura de ciberseguridad de ICS.

Threat Intelligence

Los análisis actualizados recopilados por los expertos de Kaspersky ayudan a mejorar la protección del cliente contra ciberataques industriales dirigidos. Se entregan como informes personalizados o fuentes de TI, por lo que satisfacen las necesidades específicas del cliente según los parámetros regionales, industriales o del software de ICS.

Respuesta a incidentes

En caso de que haya un incidente, los expertos de Kaspersky recopilan y analizan los datos y el malware, reconstruyen la cronología del incidente, determinan las posibles fuentes y los motivos y desarrollan un plan de corrección detallado. El plan incluye recomendaciones sobre eliminar el malware de los sistemas del cliente y revertir las acciones maliciosas.

Capacitación y concienciación

> Kaspersky fue la mejor empresa posible en ofrecer capacitación en técnicas de ciberseguridad industrial profesional para nuestro grupo de ICS.
>
> Søren Egede Knudsen, director de tecnología

Toma de conciencia sobre la ciberseguridad industrial

Capacitación y juegos de ciberseguridad interactivos en línea y presenciales para los empleados que trabajan con sistemas industriales computarizados y sus gerentes. Los participantes obtienen nuevos conocimientos dentro del panorama de amenazas actual y los vectores de ataque que se dirigen específicamente a entornos industriales. También exploran casos prácticos y adquieren técnicas de ciberseguridad.

Programas de capacitación para expertos

Las pruebas de penetración y los cursos de capacitación sobre ciencia digital forense de ICS están dirigidas a profesionales de la ciberseguridad. Los participantes aprenden todas las técnicas avanzadas que se necesitan para llevar a cabo pruebas de penetración o análisis forenses digitales exhaustivos en entornos industriales.

Ecosistema de soluciones especializadas

Kaspersky IoT Infrastructure Security

Protege el Internet de las cosas en el nivel de la puerta de enlace según el enfoque de ciberinmunidad de Kaspersky

Más información

Kaspersky Antidrone

Protege el espacio aéreo de los drones en instalaciones de cualquier tamaño

Más información

Kaspersky Secure Remote Workspace

Infraestructura de cliente ligero funcional con ciberinmunidad

Más información

Kaspersky Security CAD

Modelado digital de los sistemas de seguridad de la información para las fases de diseño y operación

Más información

Kaspersky Machine Learning for Anomaly Detection

Sistema de detección temprana de anomalías en procesos tecnológicos industriales

Más información

Kaspersky Industrial CyberSecurity

Más información

www.kaspersky.es