

Servicio integral de protección contra riesgos digitales

Kaspersky Digital Footprint Intelligence

kaspersky preparados para el futuro

Introducción

¿Cuál es la forma más rentable de atacarte?

¿Qué información está disponible para los atacantes que eligieron tu empresa como objetivo?

¿Tu infraestructura ya está comprometida y no lo sabes?

Kaspersky Digital Footprint Intelligence responde a estas y otras preguntas, ya que nuestros expertos componen una imagen integral de tu estado de ataque e identifican puntos débiles ideales para su aprovechamiento y revelan pruebas de ataques pasados, presentes e, incluso, planeados.

A medida que tu empresa crece, la complejidad y la distribución de tus entornos de TI también lo hacen, lo que presenta el desafío de proteger una presencia digital ampliamente distribuida sin control ni propiedad directos. Los entornos dinámicos e interconectados permiten a las organizaciones obtener importantes beneficios. Sin embargo, el constante aumento de la interconectividad también está ampliando el área de ataque. Dado que los atacantes son cada vez más hábiles, es vital no solo disponer de una imagen precisa de la presencia en línea de tu organización, sino también poder rastrear sus cambios y reaccionar ante amenazas externas dirigidas a los activos digitales expuestos.

Las organizaciones utilizan una amplia gama de herramientas de seguridad en sus operaciones de seguridad, pero aún existen amenazas externas inminentes que requieren capacidades muy específicas, como detectar y mitigar filtraciones de datos, supervisar los planes y esquemas de ataque de los ciberdelincuentes ubicados en foros de la dark web, etc. Para ayudar a los analistas de seguridad a explorar la visión que tiene el adversario de los recursos corporativos, detectar rápidamente los posibles vectores de ataque a su alcance y ajustar sus defensas en consecuencia, Kaspersky ha creado Kaspersky Digital Footprint Intelligence.

Kaspersky Digital Footprint Intelligence proporciona lo siguiente:

Kaspersky Digital Footprint Intelligence es un servicio integral de protección contra riesgos digitales que te ayuda a supervisar tus activos digitales y detectar amenazas en la red superficial, deep y dark.

Superficie de ataque externa

Supervisión de los activos de los clientes expuestos a Internet, lo que permite la detección temprana de vulnerabilidades y configuraciones incorrectas. Esto ayuda a los equipos de seguridad a centrarse en los riesgos críticos, al tiempo que mantienen una visibilidad completa de la infraestructura de la empresa.

Supervisión de la dark web

Supervisión continua de docenas de recursos de la dark web (foros, blogs sobre ransomware, servicios de mensajería instantánea, sitios Tor, etc.), detectando cualquier referencia y amenaza relacionada con tu organización, clientes y partners. Análisis de ataques dirigidos activos o ataques que se están planificando, campañas APT dirigidas a tu empresa, sector y regiones de operación.

Detección de filtraciones de datos

Detección de credenciales, tarjetas bancarias, números de teléfono y otra información confidencial de empleados, clientes y partners vulnerados, que se puede usar para realizar un ataque o que significa un riesgo para la reputación de la empresa.

Detección de amenazas

Supervisión de actividades fraudulentas que pueden dañar la reputación de tu empresa o engañar a tus clientes.

Kaspersky Digital Footprint Intelligence está disponible directamente a través de Kaspersky Threat Intelligence Portal, una plataforma unificada para acceder a datos sobre amenazas, alertas y análisis en tiempo real.

Cómo funciona

Configura

Detección de información sobre los activos digitales de la organización

Recopila

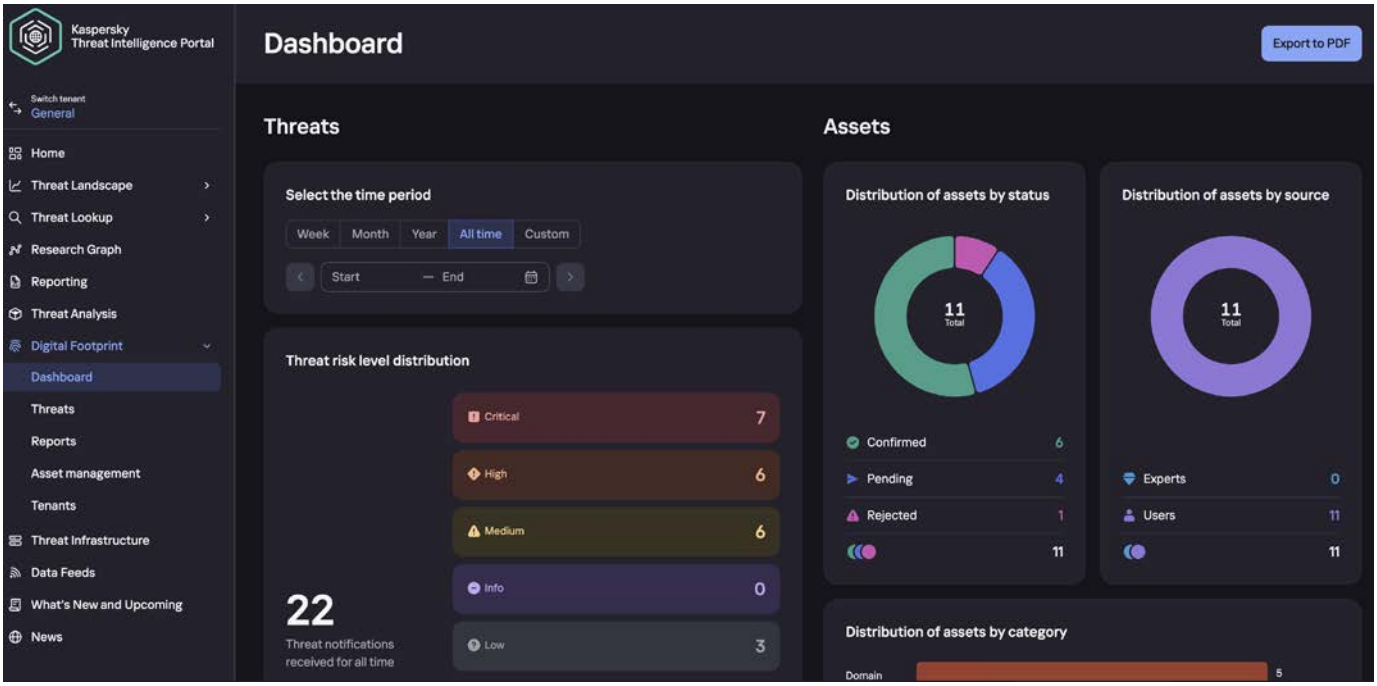
Recopilación automatizada de datos de la red superficial, profunda y oscura, y de la base de conocimientos de Kaspersky

Reacciona

Envío de notificaciones operativas sobre amenazas en Kaspersky Threat Intelligence Portal o a través de la API

Filtra

Detección de amenazas, análisis y priorización administrada por analistas



Resultados clave del servicio

1. Paneles con funciones de resumen y desglose
2. Acceso a la funcionalidad de búsqueda en la red oscura, profunda y superficial
3. Notificaciones sobre amenazas identificadas en Threat Intelligence Portal
4. Cuota de búsqueda en la base de datos de amenazas de Kaspersky (Threat Lookup), incluida la Investigación
5. Presentaciones y sesiones de preguntas y respuestas con expertos
6. Integración a través de API y posibilidad de exportar datos legibles por máquina

Módulos adicionales

7. Informes analíticos* elaborados por nuestros expertos
8. Takedown Service mitiga las amenazas que plantean los dominios de phishing maliciosos, las cuentas falsas en redes sociales y las aplicaciones móviles falsas en el marketplace de aplicaciones móviles
9. Ask the Analyst Acceso directo a los expertos en seguridad de Kaspersky para cada caso concreto
10. Supervisión de marca Supervisa el uso no autorizado de tu marca corporativa en línea. Identificación de sitios web de phishing, cuentas y aplicaciones falsas en redes sociales, y otras actividades fraudulentas que pueden dañar la reputación de tu empresa o engañar a tus clientes

Tipos de amenazas

Kaspersky Digital Footprint Intelligence permite a las organizaciones detectar y responder rápidamente a las amenazas con alertas en tiempo real, minimizando los riesgos para la reputación de la marca, la confianza de los clientes y la continuidad del negocio. Todas las notificaciones enviadas se pueden administrar con estados y asignaciones de usuarios, lo que también permite compartir comentarios entre los miembros del grupo y los analistas de Kaspersky.

Amenazas relacionadas con el perímetro de la red

- Servicios de red mal configurados
- Identificación de vulnerabilidades
- Recursos destruidos o comprometidos

Amenazas relacionadas con la web oculta

- Esquemas de fraude y planes de los ciberdelincuentes
- Ventas por filtración de datos
- Actividades de infiltración

Filtraciones de datos

- Recursos corporativos vulnerados
- Tarjetas de crédito vulneradas
- Credenciales comprometidas

Amenazas relacionadas con malware

- Ataques de phishing
- Ataques dirigidos
- Campañas de APT

* Disponible como complemento de Kaspersky Digital Footprint Intelligence

Fuentes de inteligencia

Es esencial que tengas un conocimiento integral de tu postura de seguridad externa.
Para proporcionar esta información, los analistas de seguridad de Kaspersky recopilan y añaden información de las siguientes fuentes de inteligencia:

Activos

- Direcciones IP
- Rangos de red
- Nombres de dominio
- Números de tarjetas BIN/IIN
- Palabras clave
- Nombres de marca
- Información de empleados
- Enlaces de cuentas en redes sociales
- Enlaces de aplicaciones móviles

Fuentes

- Inventario del perímetro de la red
- Motores de búsqueda de la red superficial, deep y dark
- Búsqueda en la base de conocimientos de Kaspersky

Entregables

- Alertas de amenazas
- Búsqueda en tiempo real en las fuentes de Kaspersky y la red visible y oscura
- Informes analíticos*

Funciones de prestación de servicios

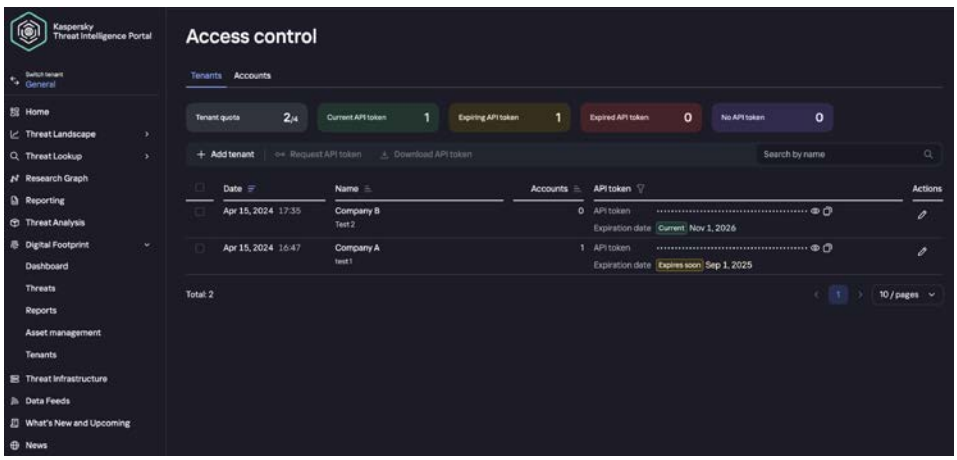
Digital Footprint Intelligence ofrece funciones avanzadas a los proveedores de servicios de seguridad gestionados MSSP y organizaciones grandes con varias sucursales.

La interfaz de Kaspersky Threat Intelligence Portal, a través de la cual se facilita el servicio de DFI, permite a los MSSP diferenciar el acceso a la información relacionada con las filiales de grandes organizaciones o con organizaciones individuales a las que tú, como MSSP, proporcionas servicios de gestión de la seguridad.

Creación de usuarios diferentes y configuración del control del acceso mediante el panel de administración

La administración se logra mediante la creación de usuarios: entidades lógicas creadas para cada estructura nueva, que se deben administrar de forma independiente a las demás.

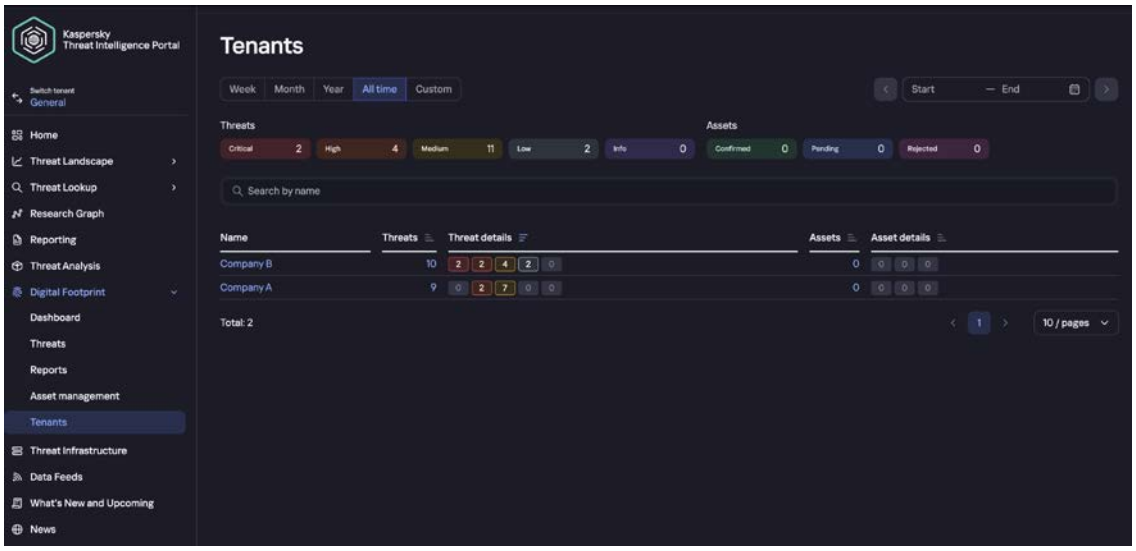
- Acceso a todos los activos y las notificaciones de amenazas específicos del usuario
- Cambio de grupos de usuarios fluido y visualización de información en nombre del usuario
- Control del acceso mediante token de API y TOTP
- Función de cambio de licencias de usuarios



*Servicio complementario

Estadísticas centralizadas sobre las amenazas y los activos de cada usuario

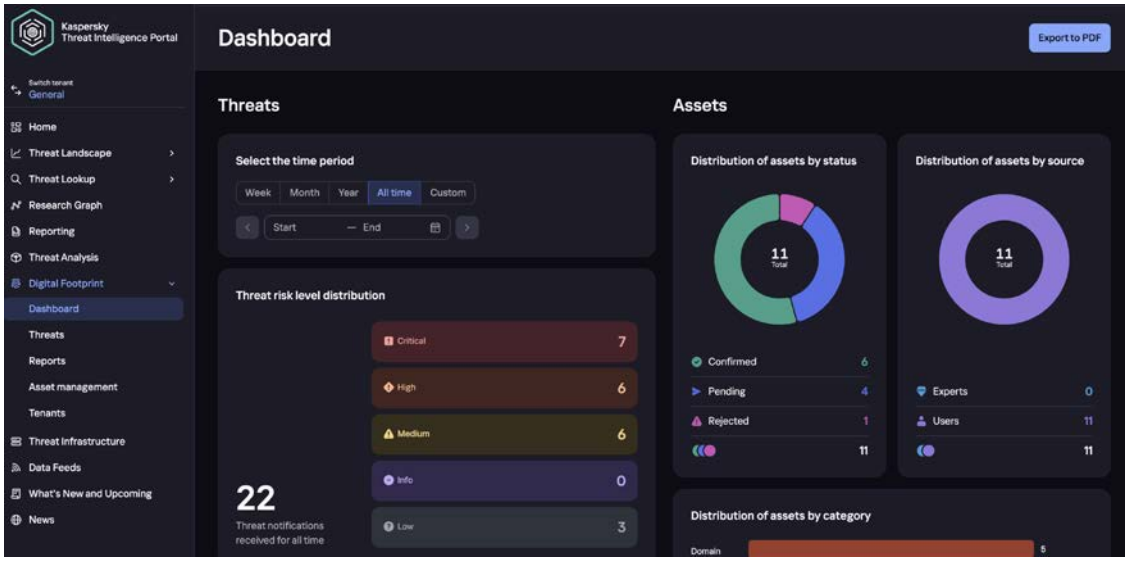
Cuando proporcionas servicios a un gran número de organizaciones, es esencial que dispongas de las herramientas necesarias para supervisar el estado actual de tus tenants. El tenant Center muestra un resumen de cada tenant, incluido el número de amenazas detectadas con su nivel de criticidad, así como información sobre los activos que el inquilino desea supervisar y su estado.



Control detallado

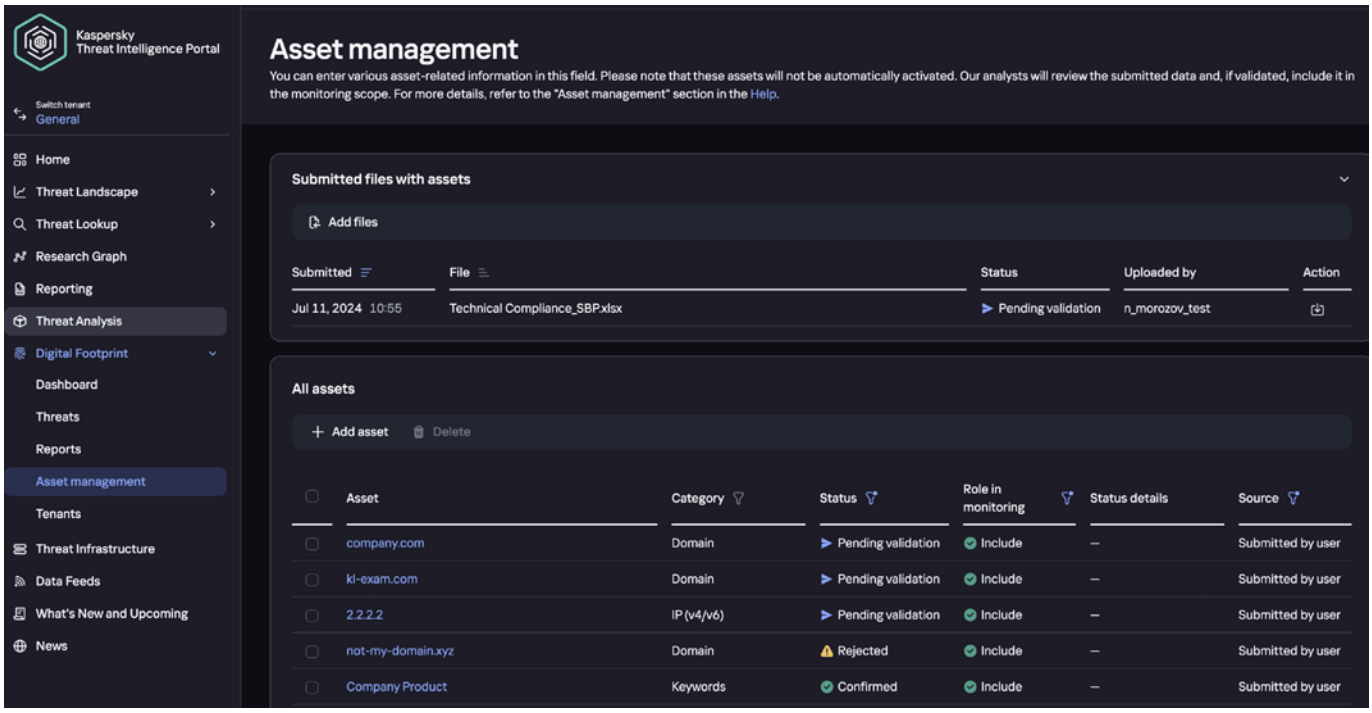
Tú, como MSSP o sede central, puedes ver un resumen detallado de cada tenant:

- La cantidad total de amenazas identificadas durante un período determinado y su severidad para la organización
- Categorización de las amenazas detectadas
- Los activos de los tenants más vulnerables
- El entorno de amenazas cambia con el tiempo



Gestión de activos

El tenant puede añadir nuevos activos para su supervisión tanto de forma individual a través de la interfaz de Kaspersky Threat Intelligence Portal como cargando archivos cuando se trata de una gran cantidad de activos. Básicamente, este enfoque simplifica el proceso de mantener actualizados los activos.



Valores empresariales

La solución Kaspersky Digital Footprint Intelligence ofrece importantes ventajas y valor añadido a tu organización:

Protege tu marca

Detecta amenazas potenciales en tiempo real para proteger la reputación de tu marca, preservar la confianza de tus clientes y reducir el riesgo de pérdidas financieras y daños en las operaciones empresariales.

Reduce los ciberriesgos

Brinda a las partes interesadas (director de experiencia de cliente y Junta Directiva) información sobre dónde ubicar el gasto en ciberseguridad, lo que revelará las brechas de la configuración actual y los riesgos que acarrean.

Reacciona más rápido

El contexto adicional de las alertas de seguridad mejora la respuesta ante incidentes y reduce tu tiempo medio de respuesta (MTTR).

Reduce la superficie de ataque

Gestiona la presencia digital de tu empresa y controla los recursos de red externos para minimizar los vectores de ataque y las vulnerabilidades que pueden usarse en un ataque.

Comprende a tus adversarios

Más vale prevenir que curar: infórmate sobre lo que los ciberdelincuentes están planeando y comentando sobre tu empresa en la red oscura para estar preparado.

Conoce lo desconocido

Mejora tu capacidad de resistencia ante ciberataques e identifica las amenazas externas a la jurisdicción de tus equipos de seguridad internos.

Eficiencia de la prestación de servicios

El inicio rápido y la fácil escalabilidad en modo multitenencia te ahorran tiempo tanto a ti como MSSP como a tus clientes, así como a las grandes organizaciones con múltiples afiliados.

Empieza hoy mismo a supervisar tu superficie de ataque y el entorno de amenazas a través de Kaspersky Threat Intelligence Portal

Visita TIP

Para obtener más información sobre los distintos planes de suscripción, comunícate con nuestro equipo.

Contacta con nosotros



Kaspersky Digital Footprint Intelligence

Más información

www.kaspersky.es

© 2025 AO Kaspersky Lab.
Las marcas comerciales y de servicios registradas pertenecen a sus respectivos propietarios.

#kaspersky
#bringonthefuture