



Servicio integral  
de protección contra  
riesgos digitales

# Kaspersky Digital Footprint Intelligence

**kaspersky** bring on  
the future

## Preguntas para expertos

¿Cuál es la mejor manera de iniciar un ataque contra su empresa?

¿Cuál es la forma más rentable de atacarlo?

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

¿Su infraestructura ya está comprometida y no lo sabe?

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

## Introducción

A medida que su negocio crece, la complejidad y la distribución de sus entornos de TI también lo hacen, lo que presenta el desafío de proteger una presencia digital ampliamente distribuida sin control ni propiedad directos. Los ambientes dinámicos e interconectados permiten que las empresas obtengan grandes 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 su organización, sino también poder llevar un seguimiento de sus cambios y reaccionar ante amenazas externas dirigidas a los activos digitales expuestos.

Si bien las organizaciones utilizan una amplia gama de herramientas en sus operaciones de seguridad, sigue habiendo amenazas digitales al acecho que requieren capacidades muy específicas: detectar y mitigar filtraciones de datos, supervisar planes y esquemas de ataque de ciberdelincuentes ubicados en foros de la web oscura, etc. Para ayudar a los analistas de seguridad a explorar la visión que tiene el adversario de los recursos de su empresa, detectar rápidamente los posibles vectores de ataque disponibles para ellos y ajustar sus defensas en consecuencia, Kaspersky creó [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 ayuda a los clientes a supervisar sus activos digitales y detectar amenazas desde la web superficial, profunda y oscura.



### Reconocimiento de redes

La identificación de los recursos de red del cliente y los servicios expuestos, que son un potencial punto de entrada para un ataque. Análisis personalizado de vulnerabilidades existentes, con una mayor puntuación y evaluación de riesgos integral basada en la puntuación base del CVSS, la disponibilidad de exploits públicos, la experiencia de pruebas de penetración y la ubicación del recurso de red (alojamiento/infraestructura).



### Supervisión de la web oscura

Supervisión constante de decenas de recursos de la web oscura (foros, ransomware, blogs, sistemas de mensajería, sitios de tor, etc.), que detecta todas las referencias y amenazas relacionadas con su empresa, clientes y partners. Análisis de ataques selectivos activos o que se estén planificando, campañas de APT dirigidas a su empresa, sector y regiones de operaciones.



### Descubrimiento de filtraciones de datos

Detección de credenciales, tarjetas bancarias, números de teléfono y otra información confidencial de empleados, clientes y partners en riesgo, 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 una empresa o engañar a los clientes.



### Soporte de tenencia múltiple

Funciones mejoradas para proveedores de servicios de seguridad administrados (MSSP) y organizaciones grandes con una estructura de varias sucursales.

# ¿Cómo funciona?



## Configurar

Descubrimiento de la información sobre los activos digitales de la empresa

## Recopilar

Recopilación automatizada de datos desde la web superficial, profunda y oscura, así como la base de datos de Kaspersky

## Reacción

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

## Filtro

Detección de amenazas, análisis y priorización administrada por analistas

## Resultados clave del servicio

1

Paneles útiles con datos estadísticos detallados

2

Cuota de búsqueda en la base de datos de la red oscura

3

Alertas sobre amenazas en Threat Intelligence Portal

4

Cuota de búsqueda en la base de datos de las redes sociales

5

Presentaciones y sesiones de preguntas y respuestas con expertos

6

Datos legibles por máquina

7

Informes analíticos elaborados por nuestros especialistas\*

8

Solicitudes de ataque\*



## Tipos de amenazas

Kaspersky Digital Footprint Intelligence permite a las organizaciones responder de forma rápida y eficaz ante posibles amenazas con alertas en tiempo real. Reduce la probabilidad de hacerle daño a la reputación de la marca, la confianza de los clientes y las operaciones empresariales en general. Las empresas pueden personalizar las capacidades de supervisión del servicio para satisfacer sus necesidades específicas, y los informes y análisis integrales ofrecen información valiosa sobre el alcance y el impacto del uso no autorizado de la marca y otros riesgos potenciales.

### Amenazas relacionadas con el perímetro de red

- Servicios de red mal configurados
- Identificación de las vulnerabilidades
- Recursos desfigurados o comprometidos

### Filtraciones de datos

- Recursos corporativos en riesgo
- Tarjetas de crédito en riesgo
- Credenciales comprometidas

### Amenazas relacionadas con la web oscura

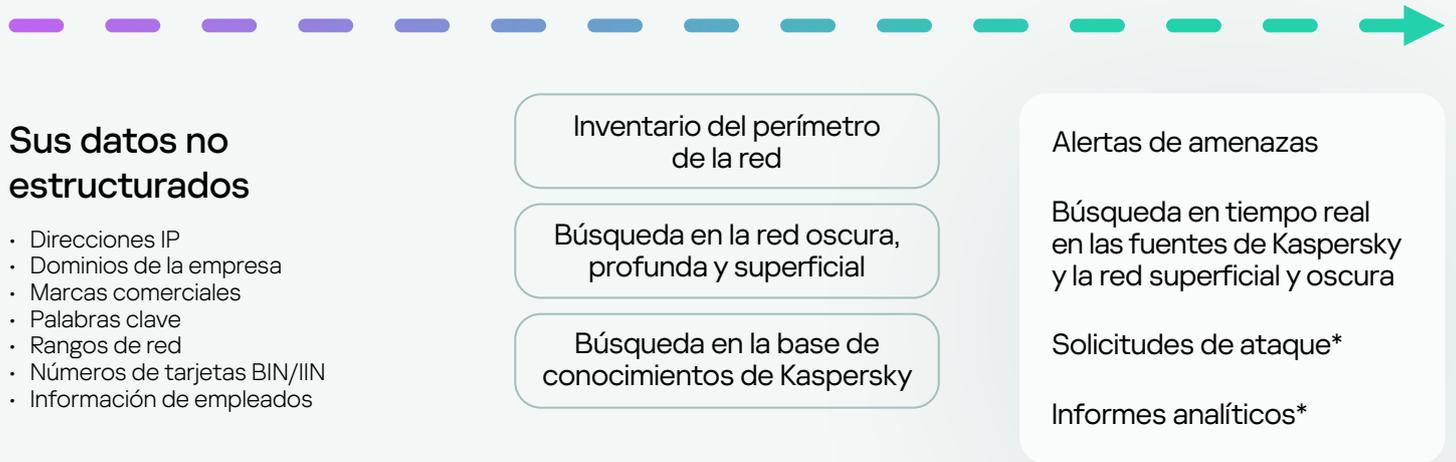
- Estratagemas de fraude y planes de los ciberdelincuentes
- Venta y filtración de datos
- Actividades de informantes internos

### Amenazas relacionadas con el malware

- Ataques de phishing
- Ataques selectivos
- Campañas de APT

## Fuentes de inteligencia

Es esencial que nuestros clientes tengan una comprensión integral de su postura de seguridad externa. Para brindar esta información, los analistas de seguridad de Kaspersky recopilan y agregan información de las siguientes fuentes de inteligencia:



## Funciones de prestación de servicios

La inteligencia sobre presencia digital ofrece funciones avanzadas a los proveedores de servicios de seguridad administrados (MSSP) y organizaciones grandes con varias sucursales.

La interfaz del portal de Kaspersky Threat Intelligence, mediante la cual se ofrece el servicio de DFI, les permite a los MSSP tener un acceso diferenciado a la información relacionada con las filiales de organizaciones grandes o con organizaciones individuales a las que los MSSP prestan servicios de administración 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.

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

**Access control**

Account **Tenants**

Tenant quota: 5/10 | Expired API token: 1 | Expires soon API token: 1 | Current API token: 1 | None API token: 2

+ Add tenant | Delete tenant | Request token | Download API token | Search by name

Date	Name	Accounts	API Token for User_name	Actions
12 July 2023 11:48	Tenant 1 Lorem ipsum is placeholder text commonly used in th...	1	API Token Expiration date: <b>Current</b> 29 Feb 2024	👁️ 🗑️ ✎️
7 Jun 2023 09:27	Tenant 2 Lorem ipsum is placeholder text commonly used in th...	1	API Token Expiration date: <b>Expired</b> 02 Feb 2024	👁️ 🗑️ ✎️
6 July 2023 11:48	Tenant 3 Lorem ipsum is placeholder text commonly used in th...	1	API Token Expiration date: <b>Expires soon</b> 16 Feb 2024	👁️ 🗑️ ✎️
6 July 2023 13:54	Tenant 4 Lorem ipsum is placeholder text commonly used in th...	1	API Token Expiration date: <b>None API token</b>	✎️ 🗑️
4 Jun 2023 09:27	Tenant 5 Lorem ipsum is placeholder text commonly used in th...	1	API Token Expiration date: <b>None API token</b>	✎️ 🗑️

Total 5 | 10 / page

## Estadísticas centralizadas sobre las amenazas y los activos de cada usuario

Al prestar el servicio a una gran cantidad de organizaciones, es necesario contar con herramientas para supervisar el estado actual de los usuarios. En el Centro de usuarios, se muestra un resumen de cada usuario, que incluye la cantidad de amenazas detectadas con su nivel de severidad, además de información sobre los activos que el usuario debe supervisar y sus estados.

**Tenant center**

Day | Week | Month | Year | All period | Custom Range | 05 Feb 2024

В зависимости от выбора даты количество активов не изменяется

Threats: Critical 1 | High 0 | Medium 1 | Low 1 | Info 3

Assets: Confirmed 5 | Pending 5 | Rejected 5

Search by name

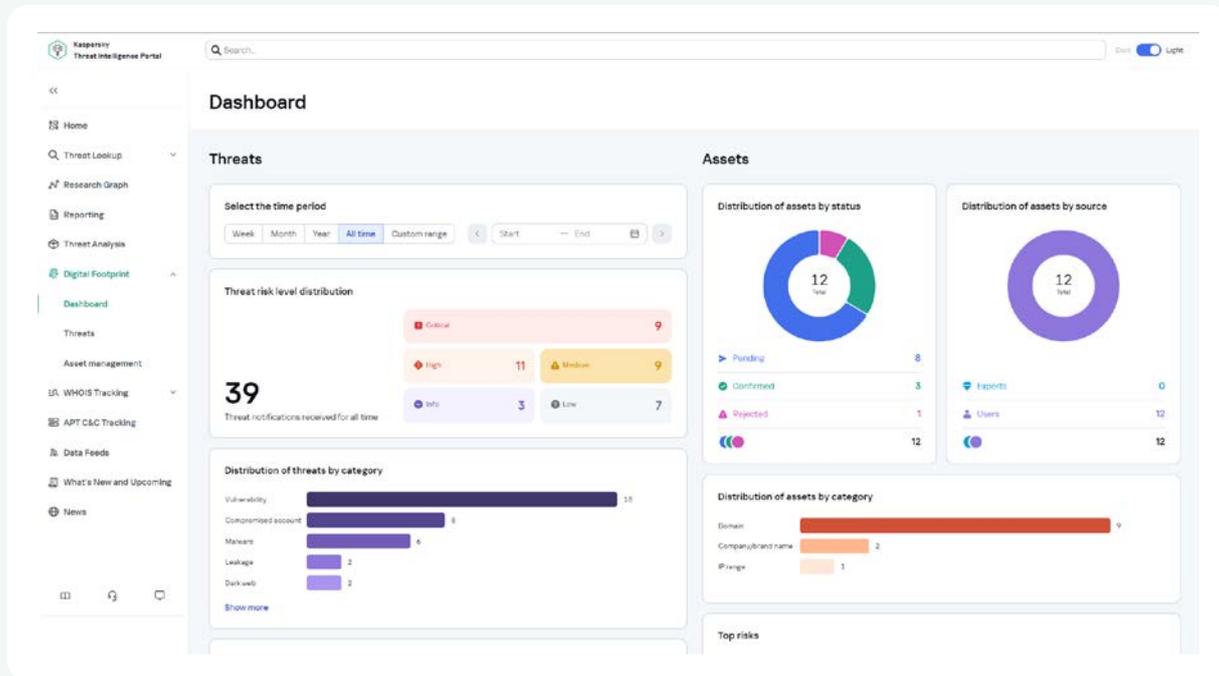
Name	Threats	Details of Threats	Assets	Details of Assets
Tenant 1	2	1 0 0 0 1	17	2 10 5
Tenant 2	2	0 0 0 1 1	13	1 7 5
Tenant 3	0	0 0 0 0 0	8	1 3 4
Tenant 4	2	0 0 1 0 1	4	0 2 2
Tenant 5	0	0 0 0 0 0	4	1 2 1

Total 5 | 10 / page

## Monitoreo detallado.

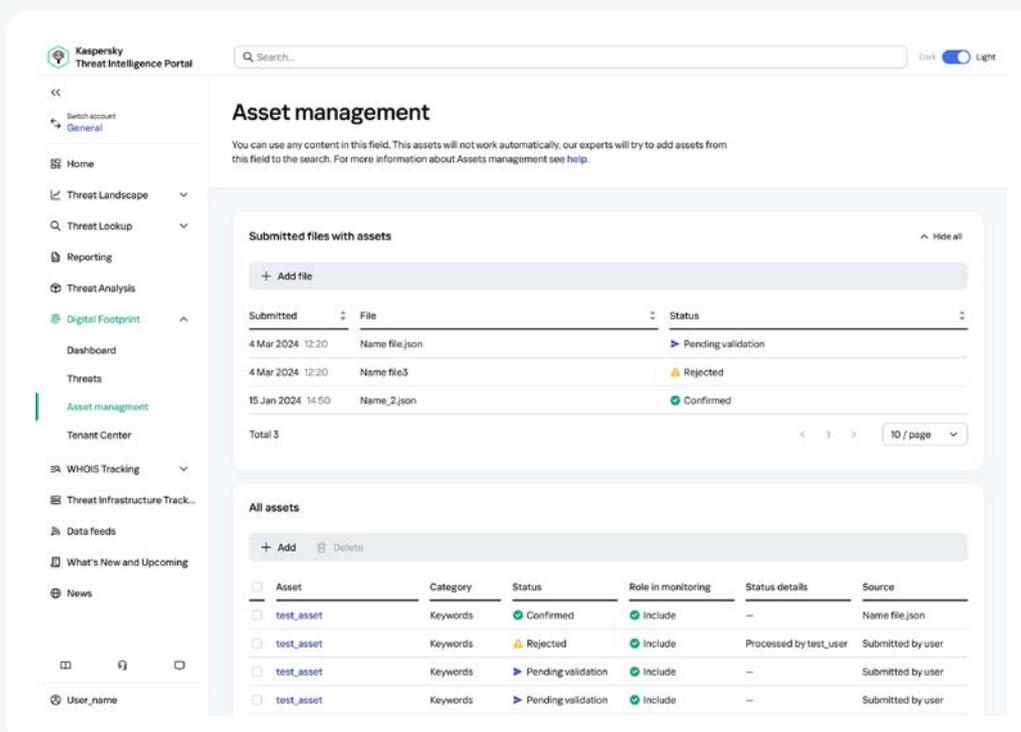
Los MSSP o la oficina central pueden ver un resumen detallado de cada usuario:

- La cantidad total de amenazas identificadas durante un período determinado y su severidad para la organización
- Categorización de las amenazas detectadas
- Los activos del usuario más vulnerable
- Panorama de amenazas que cambia con el tiempo



## Gestión de activos

El usuario puede agregar nuevos activos para la supervisión tanto por separado mediante la interfaz del portal de Kaspersky Threat Intelligence como mediante la carga de archivos con una gran cantidad de activos. Básicamente, este enfoque simplifica el proceso de mantener actualizados los activos.



# Valores comerciales

Kaspersky Digital Footprint Intelligence ofrece potentes beneficios y un valor significativo a su organización:



## Protege su marca

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



## Reduzca los ciberriesgos

Brinde 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 acarrearán.



## Reaccione más rápido

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



## Reduzca la superficie de ataque

Gestione la presencia digital de su empresa y controle los recursos de red externos para minimizar los vectores de ataque y las vulnerabilidades que pueden usarse en un ataque.



## Comprenda a sus adversarios

Más vale prevenir que curar: sepa lo que los ciberdelincuentes planean y hablan sobre su empresa en la red oscura para que la empresa esté preparada.



## Conozca lo desconocido

Mejore su capacidad de resistencia ante ciberataques e identifique las amenazas externas a la jurisdicción de sus equipos de seguridad internos.



## Eficiencia de la prestación de servicios

El inicio rápido y el escalamiento sencillo en el modo de tenencia múltiple ahorra tiempo a los proveedores de servicios de seguridad administrados (MSSP) y sus clientes, además de a las organizaciones grandes de múltiples filiales.

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

Comuníquese  
con nosotros



# Kaspersky Digital Footprint Intelligence

Conozca más

[latam.kaspersky.com](https://latam.kaspersky.com)

© 2024 AO Kaspersky Lab.  
Las marcas comerciales registradas y las marcas  
de servicio pertenecen a sus respectivos propietarios.

#kaspersky  
#bringonthefuture