Servicio integral de protección contra riesgos digitales

Kaspersky Digital Footprint Intelligence

kaspersky preparados para el futuro

Preguntas para expertos

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

¿Cuál es la forma más rentable de atacarle?

¿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.

Introducción

A medida que su empresa 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 entornos 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 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 en sus operaciones de seguridad, pero sigue habiendo amenazas digitales al acecho que requieren capacidades muy específicas: detectar y mitigar filtraciones de datos, supervisar planes y esquemas de ataque de cibercriminales ubicados en foros de la red oscura, etc. Para ayudar a los analistas de seguridad a explorar la visión que tiene el adversario de los recursos de tu empresa, detectar rápidamente los posibles vectores de ataque disponibles para ellos 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 ayuda a los clientes a supervisar sus activos digitales y detectar amenazas desde la red superficial, profunda y oscura.

Reconocimiento de redes

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 las 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 red oscura

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

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 una empresa o engañar a los clientes.

Compatibilidad con tenencia múltiple

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

Funcionamiento

Configurar	Recopilar	Reacción	Filtro
Detección de información sobre los activos digitales de la empresa	Recopilación automatizada de datos desde la red superficial, profunda y oscura, así como la base de datos de Kaspersky	Envío de notificaciones sobre amenazas operativas en Kaspersky Threat Intelligence Portal o a través de la API	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 máquinas
7. Informes analíticos elaborados por nuestros especialistas*
8. Solicitudes de ataque*

*Servicio complementario

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 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
- Venta y 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

Fuentesde inteligencia

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

Sus datos no estructurados

- Direcciones IP
- Dominios de empresa
- Nombres de marca
- Palabras clave
- Rangos de red
- Números de tarjetas BIN/IIN
- Información de empleados

Inventario del perímetro de la red

Búsqueda en la red oscura, profunda y superficial

Búsqueda en la base de conocimientos de Kaspersky

Alertas de amenazas

Búsqueda en tiempo real en las fuentes de Kaspersky y la red visible y oscura

Solicitudes de ataque*

Informes analíticos*

Funciones de prestación de servicios

La inteligencia sobre rastro digital ofrece funciones avanzadas a los proveedores de servicios de seguridad gestionados MSSP y organizaciones grandes con varias sucursales.

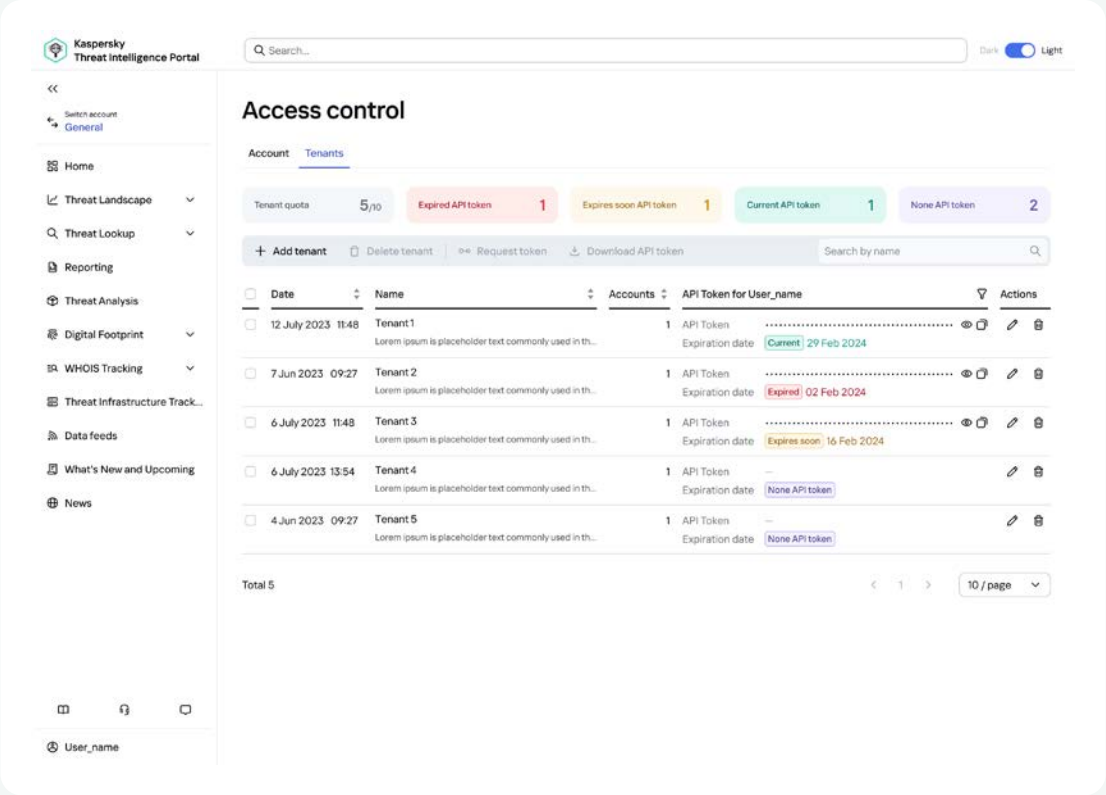
La interfaz del portal de Kaspersky Threat Intelligence, mediante la cual se ofrece el servicio de DFI, les permite a los MSSP tener un acceso diferenciado a la información relacionada con las filiales de organizaciones grandes o con organizaciones individuales a las que los MSSP prestan servicios de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

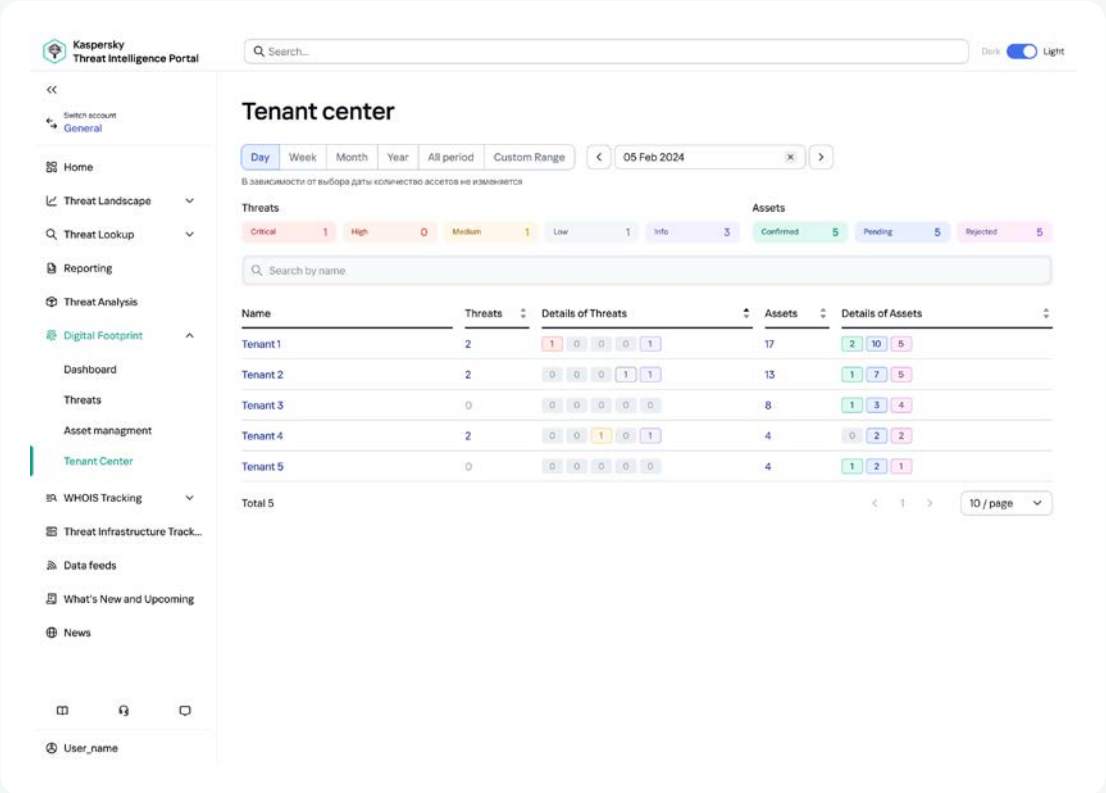
1. Acceso a todos los activos y las notificaciones de amenazas específicos del usuario
2. Cambio de grupos de usuarios fluido y visualización de información en nombre del usuario
3. Control del acceso mediante token de API y TOTP
4. Función de cambio de licencias de usuarios

*Servicio complementario



Estadísticas centralizadassobre las amenazas y los activos de cada usuario

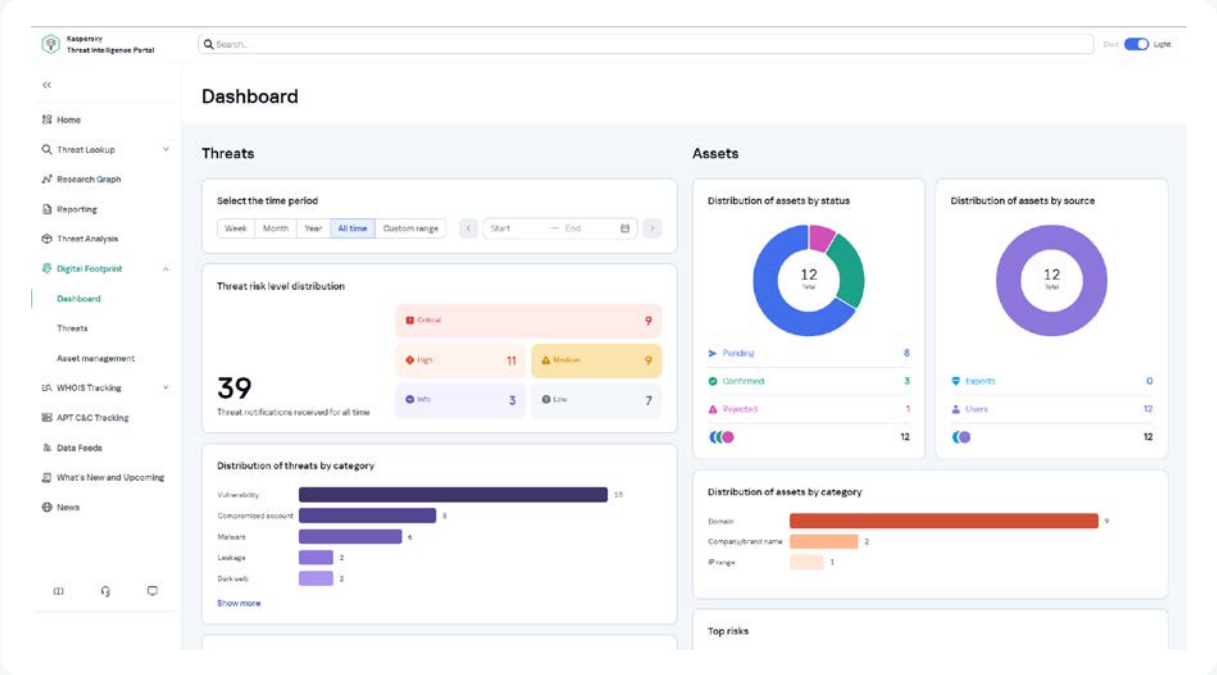
Al prestar el servicio a una gran cantidad de organizaciones, es necesario contar con herramientas para supervisar el estado actual de los usuarios. En el Centro de usuarios, se muestra un resumen de cada usuario, que incluye la cantidad de amenazas detectadas con su nivel de severidad, además de información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



Control detallado

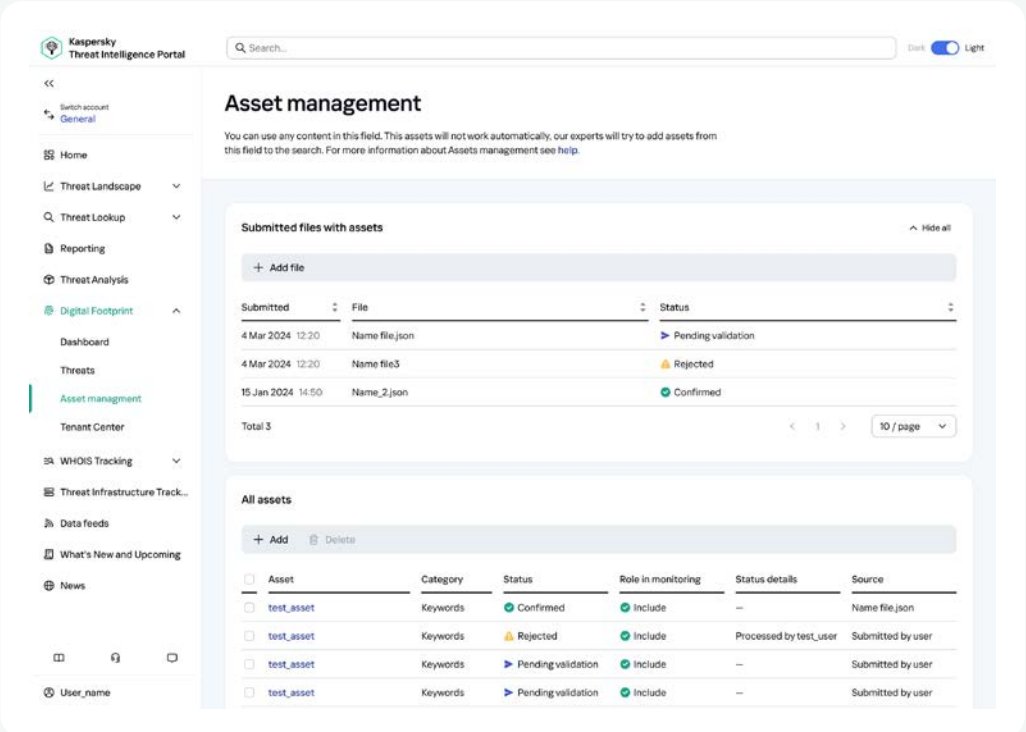
Los MSSP o la oficina central pueden ver un resumen detallado de cada usuario:

- 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 añadir nuevos activos para la supervisión tanto por separado mediante la interfaz de Kaspersky Threat Intelligence Portal como mediante la carga de archivos con una gran cantidad de activos. Básicamente, este enfoque simplifica el proceso de mantener actualizados los activos.



Valores empresariales

Kaspersky Digital Footprint Intelligence ofrece potentes beneficios y un valor significativo 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: debes saber lo que los ciberdelincuentes planean y hablan sobre tu empresa en la red oscura para que la empresa esté preparada.

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

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

Ponte en contacto con nosotros

Kaspersky Digital Footprint Intelligence

Más información

www.kaspersky.es

#kaspersky
#bringonthefuture