Comprehensive digital risk protection service

Kaspersky Digital Footprint Intelligence

kaspersky bring on the future

Intro

What's the most cost-efficient way to attack you?

What information is available to an attacker targeting your business?

Has your infrastructure already been compromised without your knowledge?

Kaspersky Digital Footprint Intelligence answers these and other questions as our experts piece together a comprehensive picture of your attack status, identifying weak spots ripe for exploitation and revealing evidence of past, present and even planned attacks.

As your business grows, the complexity and distribution of your IT environments grows too, presenting a challenge: protecting your widely distributed digital presence without direct control or ownership. Dynamic and interconnected environments enable organizations to derive significant benefits. However, ever-increasing interconnectivity is also expanding the attack surface. As attackers become more skilled, it's vital not only to have an accurate picture of your organization's online presence, but also to be able to track its changes and react to external threats aimed at exposed digital assets.

Organizations use a wide range of security tools in their security operations but there are still looming external threats which require very specific capabilities — to detect and mitigate data leakages, monitor plans and attack schemes of cybercriminals located on dark web forums, etc. To help security analysts explore the adversary's view of their corporate resources, promptly discover the potential attack vectors available to them and adjust their defenses accordingly, Kaspersky has created Kaspersky Digital Footprint Intelligence.

Kaspersky Digital Footprint Intelligence provides

Kaspersky Digital Footprint Intelligence is a comprehensive digital risk protection service that helps you monitor your digital assets and detect threats from the surface, deep, and dark webs.

External Attack Surface

Monitoring of customers internet-exposed assets, enabling early detection of vulnerabilities and misconfigurations. That helps security teams to focus on critical risks while maintaining complete visibility of company infrastructure.

Dark Web Monitoring

Continuous monitoring of dozens of dark web resources (forums, ransomware blogs, messengers, tor sites, etc.), detecting any references and threats relating to your organization, clients and partners. Analysis of active targeted attacks or attacks that are being planned, APT campaigns aimed at your business, industry and regions of operation.

Discovery of Data Leaks

Detection of compromised employees, partner and client credentials, bank cards, phone numbers and other sensitive information that can be used to carry out an attack or pose reputational risks for your company.

Threat Detection

Monitoring of fraudulent activities that can damage your corporate reputation and/or deceive your customers.

Kaspersky Digital Footprint Intelligence is available directly via the Kaspersky Threat Intelligence Portal — a unified platform for accessing threat data, alerts and analytics in real time.

How it works

Configure

Information discovery about the organization's digital assets

Collect

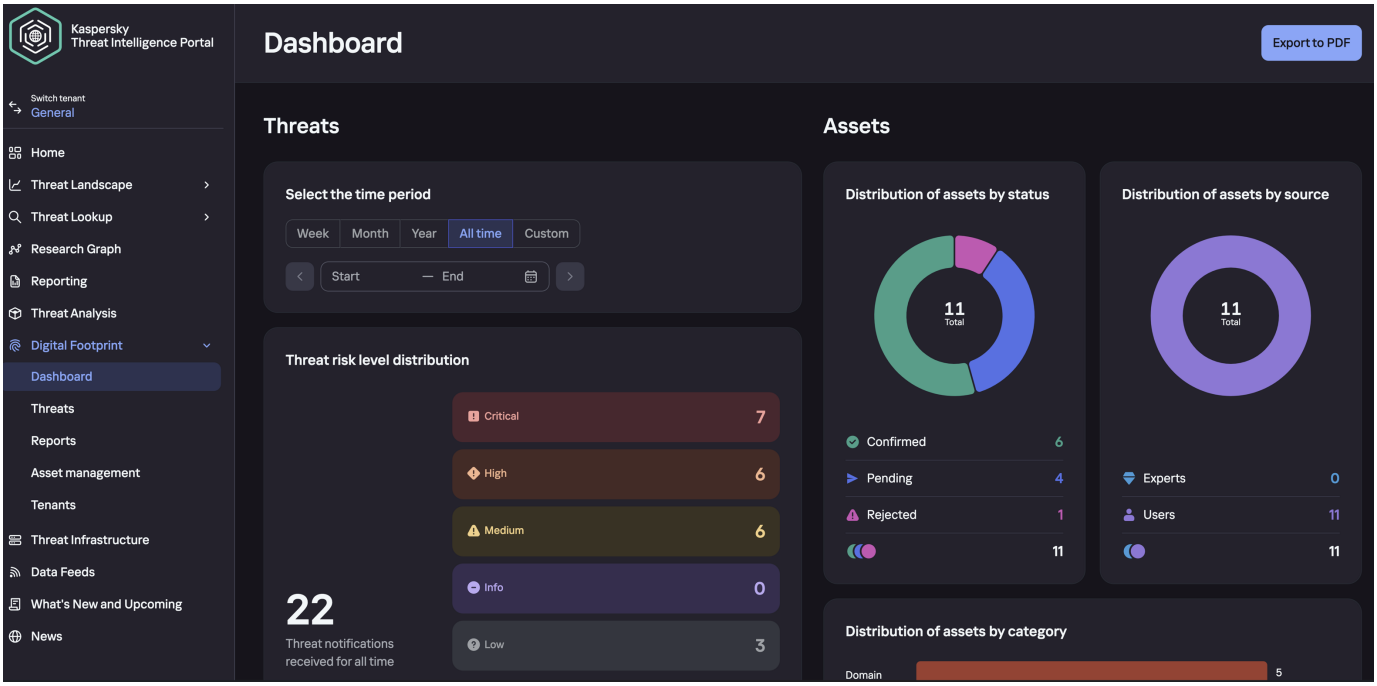
Automated data collection from surface, deep and dark webs, and from the Kaspersky knowledgebase

React

Providing operational threat notifications on Kaspersky Threat Intelligence Portal or via API

Filter

Threat detection, analysis and prioritization managed by analysts



Key service deliverables

1. Dashboards with summary and drilldown capabilities
2. Access to dark, deep, surface web search functionality
3. Notifications about identified threats in Threat Intelligence Portal
4. Search quota in Kaspersky threat database (Threat Lookup) including Research
5. Presentations and Q&A sessions with experts
6. Integration through API and possibility to export machine readable data

Additional modules

7. Analytical reports* compiled by our experts
8. Takedown service mitigates threats posed by malicious phishing domains, fake social media accounts and fake mobile apps in mobile marketplaces
9. Ask the analyst Direct access to Kaspersky security experts on a case-by-case basis
10. Brand Monitoring Monitors unauthorized use of your corporate brand online. Identification of phishing websites, fake social media accounts and applications, and other fraudulent activities that can damage your corporate reputation and/or deceive your customers

Threat types

Kaspersky Digital Footprint Intelligence empowers organizations to rapidly detect and respond to threats with real-time alerts, minimizing risks to brand reputation, customer trust, and business continuity. All delivered notification can be managed with statuses and user assignments, also allowing sharing feedback within group members and Kaspersky analysts.

Network perimeter-related threats

- Misconfigured network services
- Identification of vulnerabilities
- Defaced or compromised resources

Dark web-related threats

- Fraud schemes and cybercriminals' plans
- Data breach sales
- Insider activities

Data leakages

- Compromised corporate resources
- Compromised credit cards
- Compromised credentials

Malware-related threats

- Phishing attacks
- Targeted attacks
- APT campaigns

* Available as add-on to Kaspersky Digital Footprint Intelligence

Intelligence sources

It's essential that you have a comprehensive understanding of their external security posture.
To provide this information, Kaspersky security analysts collect and aggregate information from the following intelligence sources:

Assets

- IP addresses
- Network ranges
- Domain names
- BIN / IIN card numbers
- Keywords
- Brand names
- Employee information
- Social account links
- Mobile app links

Sources

- Network perimeter inventory
- Surface, deep and dark webs search engines
- Kaspersky Knowledge Base search

Deliverables

- Threat alerts
- Real-time search across Kaspersky's surface and dark web sources
- Analytical reports*

Service delivery capabilities

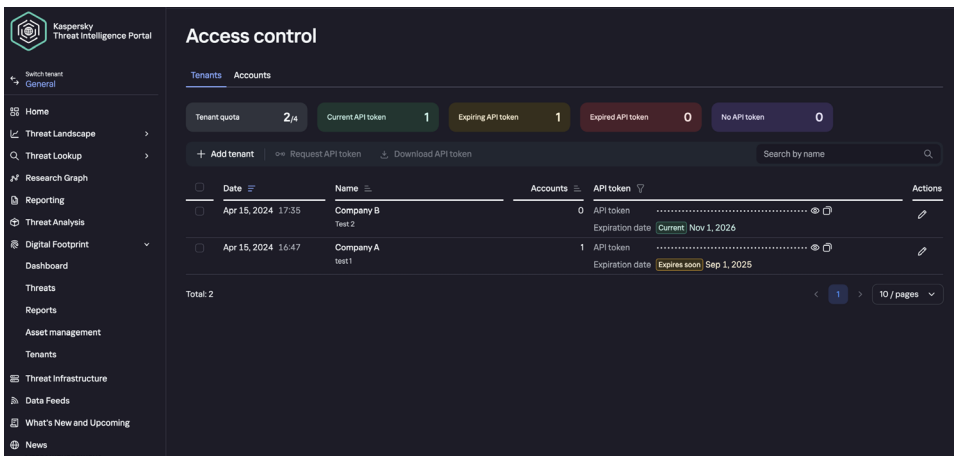
Digital Footprint Intelligence provides advanced capabilities for managed security service providers (MSSPs) and large multi-branch organizations.

Kaspersky Threat Intelligence Portal interface, through which DFI service is provided, allows MSSPs to differentiate access to information relating either to subsidiaries of large organizations or to individual organizations for which you as an MSSP provide security management services.

Creation of separate tenants and access control configuration through administration panel

Management is accomplished by creating tenants — logical entities created for each new structure, which must be managed separately from the others.

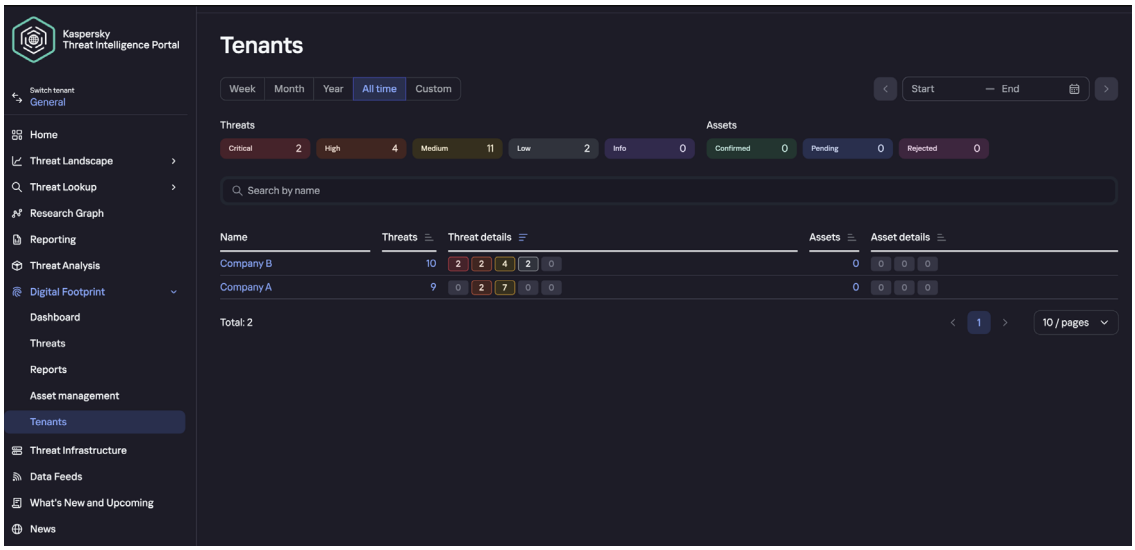
- Access to all tenant-specific threat notifications and assets
- Seamless tenant group switching and viewing information on behalf of the tenant
- Access control by API token and TOTP
- Capability to change tenant licenses



* Add-on service

Centralized statistics on each tenant's threats and assets

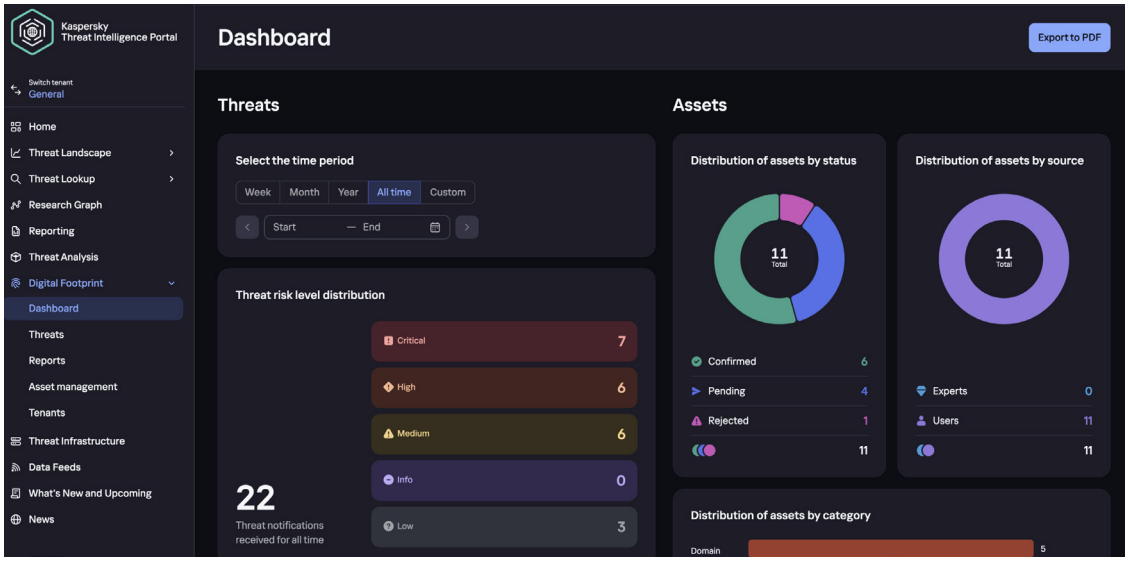
When you're providing the service to a large number of organizations, it's essential you have the tools to monitor the current state of your tenants. The tenant Center displays a summary for each tenant, including the number of detected threats with their criticality level, as well as information on the assets that the tenant would like to monitor and their status.



Detailed monitoring

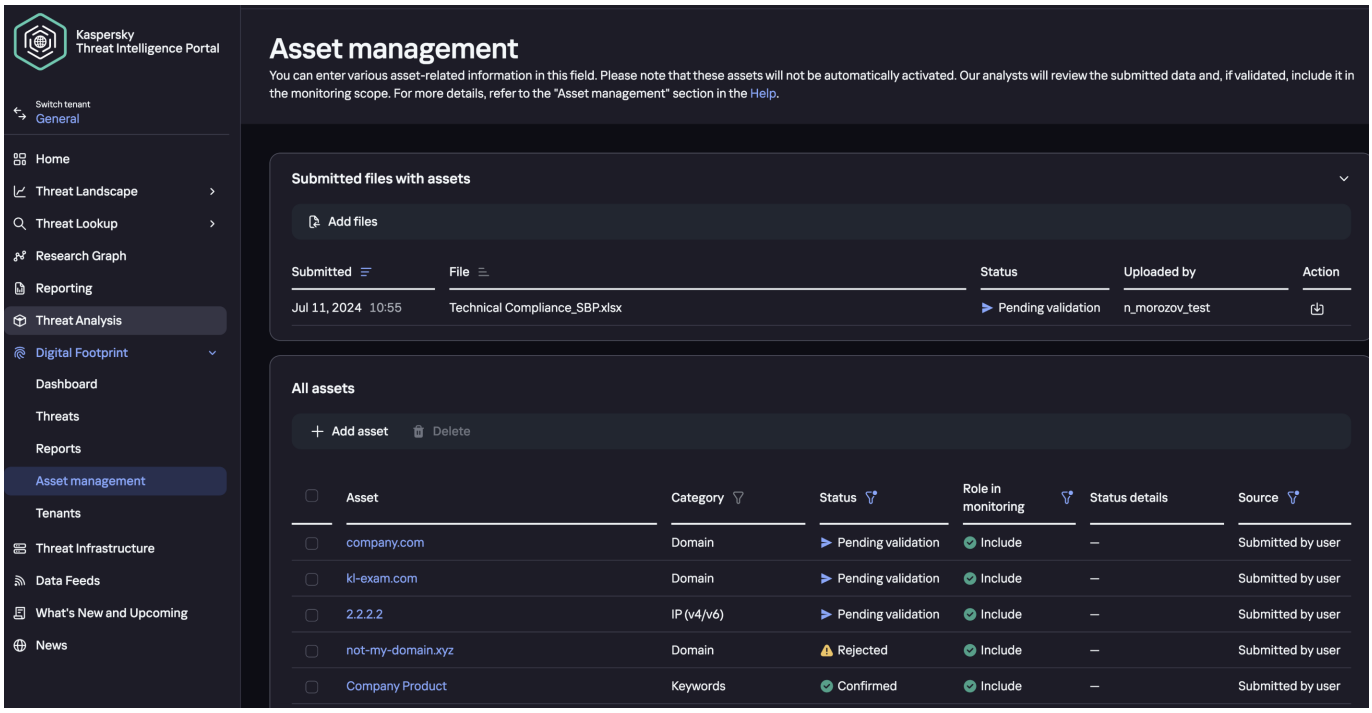
You as an MSSP or the Head Office can view a detailed summary for each tenant:

- The total number of threats identified over a given period and their criticality to the organization
- Categorization of detected threats
- The most vulnerable tenants' assets
- Threat landscape changes over time



Asset management

The tenant can add new assets to be monitored both separately via Kaspersky Threat Intelligence Portal interface and by uploading files where a large amount of assets is involved. This approach essentially simplifies the process of keeping assets up-to-date.



Business values

Kaspersky Digital Footprint Intelligence solution delivers significant benefits and value to your organization:

Protects your brand

Detect potential threats in real-time to protect your brand reputation, preserve customer trust, reduce the risk of financial loss and damage to business operations.

Reduce cyber risks

Equip your key stake holders (CxO and Board) with information on where to focus cybersecurity spending by revealing gaps in the current setup and the risks they bring.

React faster

Additional context for security alerts improves incident response and reduces your Mean Time To Respond (MTTR).

Reduce the attack surface

Manage your company's digital presence and control external network resources to minimize attack vectors and vulnerabilities that can be used for an attack.

Understand your adversaries

Forewarned is forearmed — know what cybercriminals are planning and discussing about your company on the dark web so that you're prepared.

Know the unknown

Improve your ability to withstand cyberattacks and identify threats outside the jurisdiction of your internal security teams.

Service delivery efficiency

Rapid start and easy scaling in multitenancy mode saves time both you as an MSSP and for your customers, as well as large multi-affiliate organizations.

Start monitoring your attack surface and threat landscape today via Kaspersky Threat Intelligence Portal

Visit TIP

To find out more about the various subscription plans, please get in touch with our team

Get in touch

Kaspersky Digital Footprint Intelligence

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture