Comprehensive digital risk protection service

Kaspersky Digital Footprint Intelligence

kaspersky bring on the future

Questions for experts

What's the best way to launch an attack against your organization?

What is 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.

Intro

As your business grows, the complexity and distribution of your IT environments grow too, presenting a challenge: protecting your widely distributed digital presence without direct control or ownership. Dynamic and interconnected environments enable companies 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 digital threats that loom 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 company 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 customers monitor their digital assets and detect threats from the surface, deep, and dark webs.

Network Reconnaissance

Identification of the customer's network resources and exposed services which are a potential entry point for an attack. Tailored analysis of existing vulnerabilities, with further scoring and comprehensive risk evaluation based on the CVSS base score, availability of public exploits, penetration testing experience and location of the network resource (hosting/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 company, clients and partners. Analysis of active targeted attacks or attacks that are being planned, APT campaigns aimed at your company, 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.

Threats Detection

Monitoring of fraudulent activities that can damage a company's reputation and/or deceive customers.

Multitenancy support

Enhanced capabilities for managed security service providers (MSSPs) and large organizations with a multi-branch structure.

How it works

Configure	Collect	React	Filter
Information discovery about the company's digital assets	Automated data collection from surface, deep and dark webs, and the Kaspersky knowledgebase	Providing operational threat notifications on Kaspersky Threat Intelligence Portal or via API	Threat detection, analysis and prioritization managed by analysts

Key service deliverables

1. Useful dashboards with detailed statistics
2. Search quota in the dark web database
3. Threat alerts in Threat Intelligence Portal
4. Search quota in the social media database
5. Presentations and Q&A sessions with experts
6. Machine-readable data
7. Analytical reports compiled by our experts*
8. Takedown requests*

* Add-on service

Threat types

Kaspersky Digital Footprint Intelligence empowers organizations to rapidly and efficiently respond to potential threats with real-time alerts. It reduces the likelihood of harm to brand reputation, customer trust, and overall business operations. Companies can customize the service's monitoring capabilities to meet their specific needs, and comprehensive reporting and analytics offer valuable insights into the scope and impact of brand infringement and other potential risks.

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 sale
- Insider activities

Data leakages

- Compromised corporate resources
- Compromised credit cards
- Compromised credentials

Malware-related threats

- Phishing attacks
- Targeted attacks
- APT campaigns

Intelligence sources

It's essential that our customers 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:

Your unstructured data

- IP addresses
- Company domains
- Brand names
- Keywords
- Network ranges
- BIN/IIN card numbers
- Employee information

Network perimeter inventory

Surface, deep and dark web search

Kaspersky Knowledge Base search

Threat alerts

Real-time search across Kaspersky's, surface and dark web sources

Takedown requests*

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 related either to subsidiaries of large organizations or to individual organizations to which MSSP provides 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.

1

Access to all tenant-specific threat notifications and assets

2

Seamless tenant group switching and viewing information on behalf of the tenant

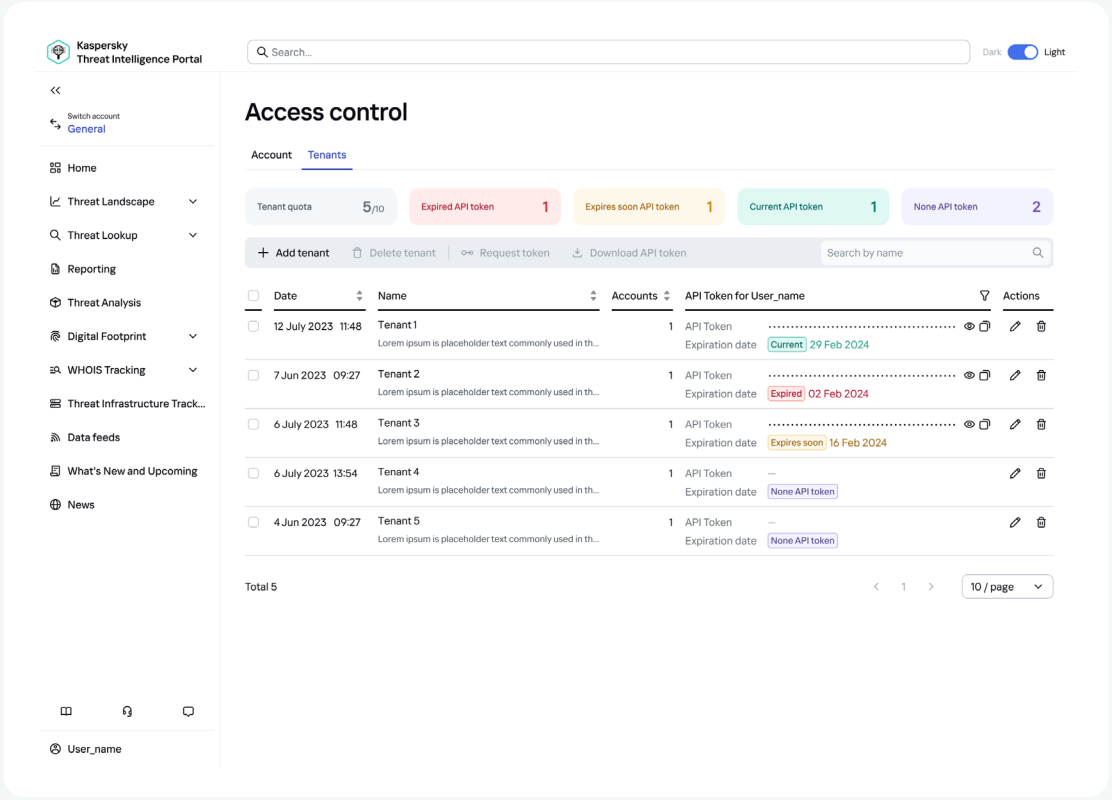
3

Access control by API token and TOTP

4

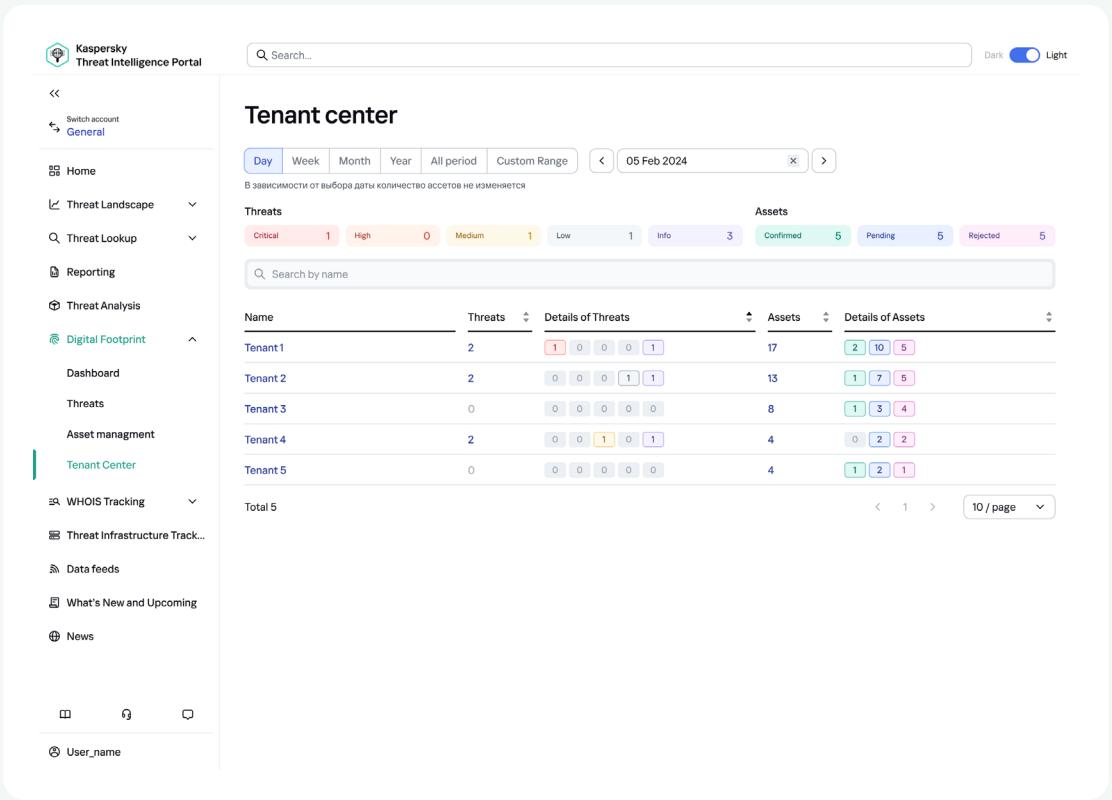
Capability to change tenant licenses

* Add-on service



Centralized statistics on each tenant's threats and assets

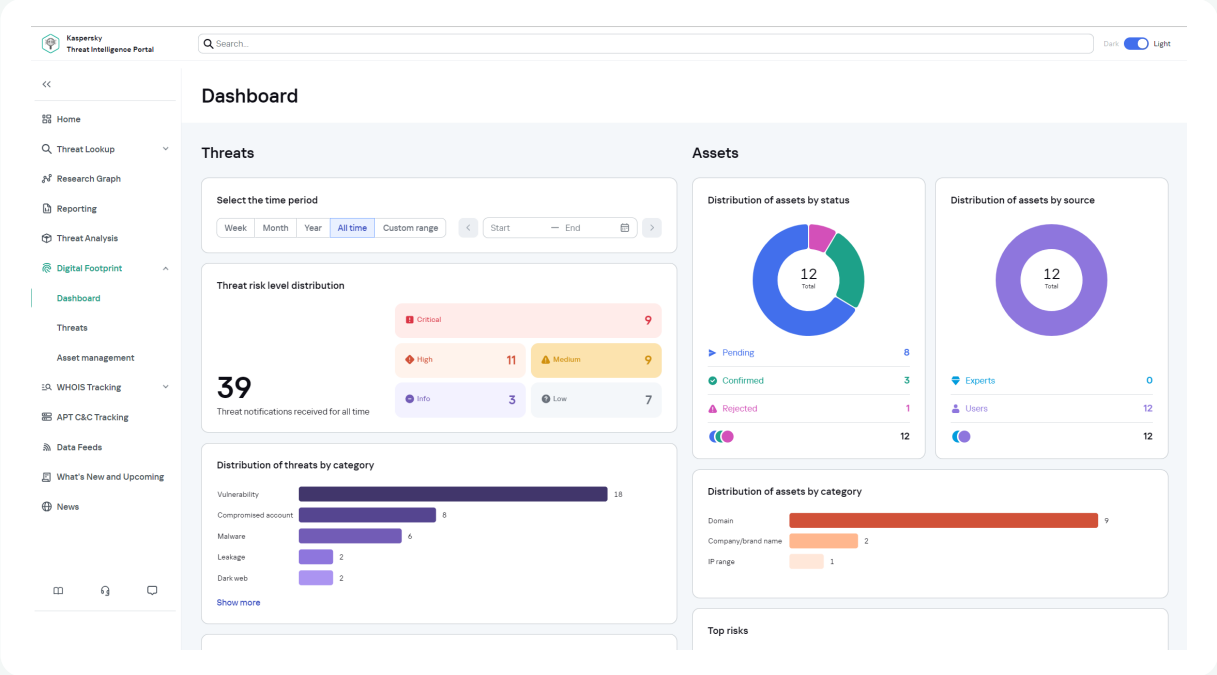
Providing the service to a large number of organizations, it is necessary to have tools for monitoring the current state of tenants. Tenant Center displays summary for each tenant, including number of detected threats with their criticality level, as well as information on the assets that tenant would like to monitor and their statuses.



Detailed monitoring

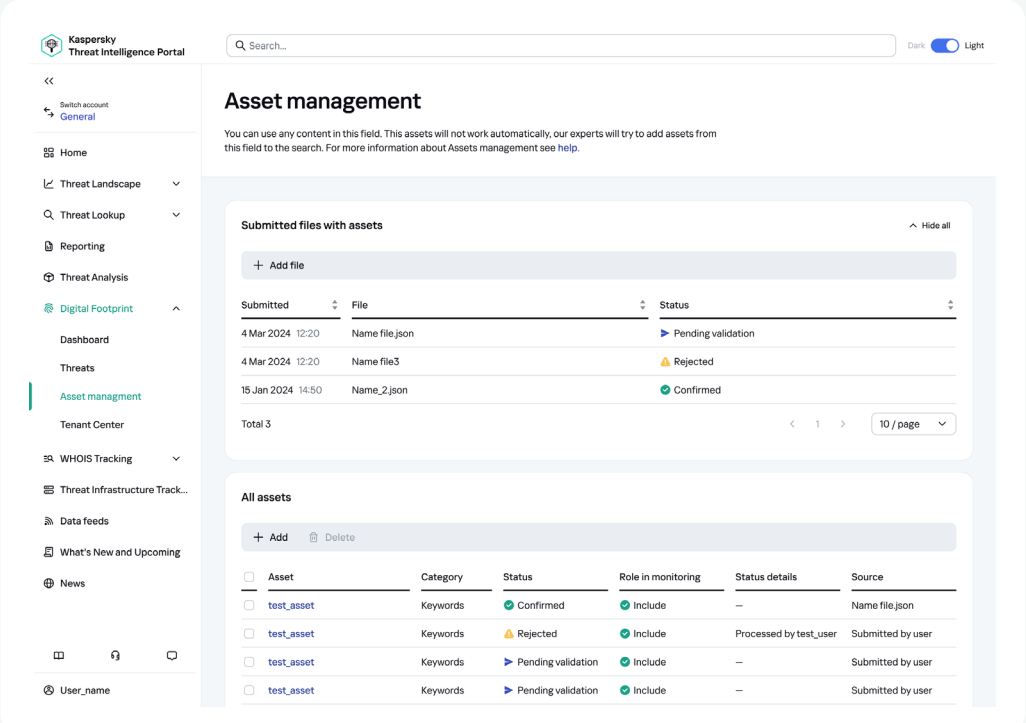
MSSP or head office can view a detailed summary for each tenant:

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



Asset management

Tenant is able to add new assets for monitoring both separately via Kaspersky Threat Intelligence Portal interface and by uploading files with a large amount of assets. This approach essentially simplifies the process of keeping assets up-to-date.



Business values

Kaspersky Digital Footprint Intelligence delivers powerful benefits and significant 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 for it.

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 for managed security service providers (MSSP) and their customers, as well as large multi-affiliate organizations.

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