Kaspersky Digital Footprint Intelligence

kaspersky BRING ON THE FUTURE

Kaspersky Digital Footprint Intelligence

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 track its changes and react to up-to-date information about exposed digital assets.

Organizations use a wide range of security tools in their security operations but there are still digital threats that loom: capabilities to detect and mitigate insider activities, plans and attack schemes of cybercriminals located on the 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.

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.

The product provides:

- Network perimeter inventory using non-intrusive methods to identify the customer's network resources and exposed services which are a potential entry point for an attack, such as management interfaces unintentionally left on the perimeter or misconfigured services, devices' interfaces, etc.
- 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).
- Identification, monitoring and analysis of any active targeted attacks or attacks that are being planned, APT campaigns aimed at your company, industry and region of operations.
- Identification of threats targeting your customers, partners and subscribers, whose infected systems could then be used to attack you.
- Discreet monitoring of pastebin sites, public forums, blogs, instant messaging channels, restricted underground online forums and communities to discover compromised accounts, information leakages or attacks against your organization being planned and discussed.

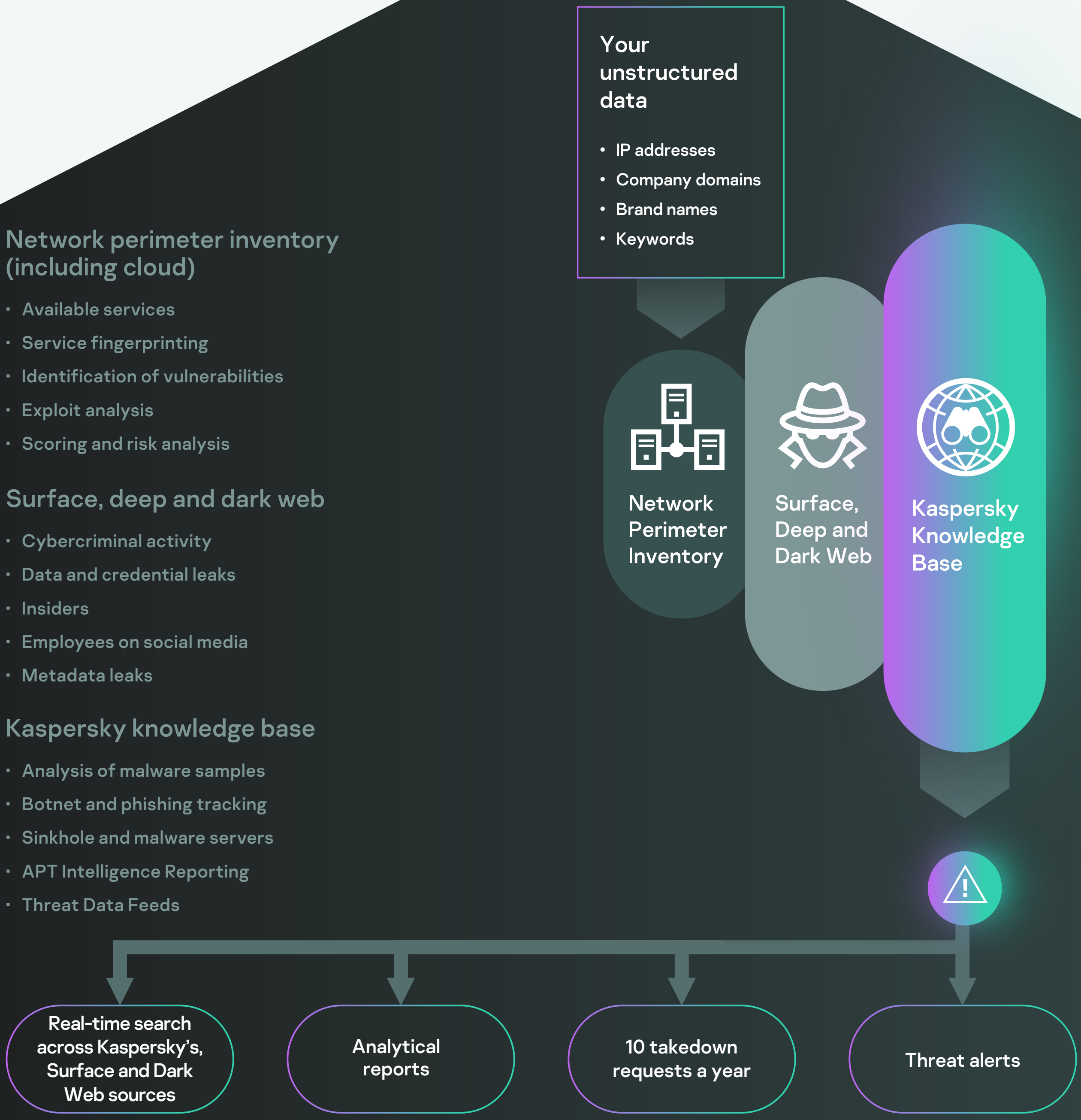
Highlights

Kaspersky Digital Footprint Intelligence uses OSINT techniques combined with automated and manual analysis of the Surface, Deep and Dark Web, plus the internal Kaspersky knowledge base to provide actionable insights and recommendations.

The product is available on the Kaspersky Threat Intelligence Portal. You can purchase four quarterly reports with annual real-time threat alerts or purchase a single report with alerts active for six months.

Search the Surface and Dark Web for near real-time information on global security events that are threatening your assets as well as for exposed sensitive data on restricted underground communities and forums. Annual license includes 50 searches a day across external sources and Kaspersky's knowledge base.

Kaspersky Digital Footprint Intelligence forms a single solution with the Kaspersky Takedown Service. Annual license includes 10 requests for taking down malicious and phishing domains a year.



Network perimeter inventory (including cloud)

- Available services
- Service fingerprinting
- Identification of vulnerabilities
- Exploit analysis
- Scoring and risk analysis

Surface, deep and dark web

- Cybercriminal activity
- Data and credential leaks
- Insiders
- Employees on social media
- Metadata leaks

Kaspersky knowledge base

- Analysis of malware samples
- Botnet and phishing tracking
- Sinkhole and malware servers
- APT Intelligence Reporting
- Threat Data Feeds

Your unstructured data

- IP addresses
- Company domains
- Brand names
- Keywords

Network Perimeter Inventory

Surface, Deep and Dark Web

Kaspersky Knowledge Base

Real-time search across Kaspersky's, Surface and Dark Web sources

Analytical reports

10 takedown requests a year

Threat alerts

Kaspersky Digital Footprint Intelligence

Learn more

www.kaspersky.com