



Intellectual Solution for Deal Transparency

Kaspersky
Transparent Deal

Companies face threats and suffer direct, indirect, and other losses due to conflict of interest



The scoring model helps calculate the risk for discovered connections and prioritize them based on the final score

The model provides a sum of 4 factors, with the result landing in one of three zones:

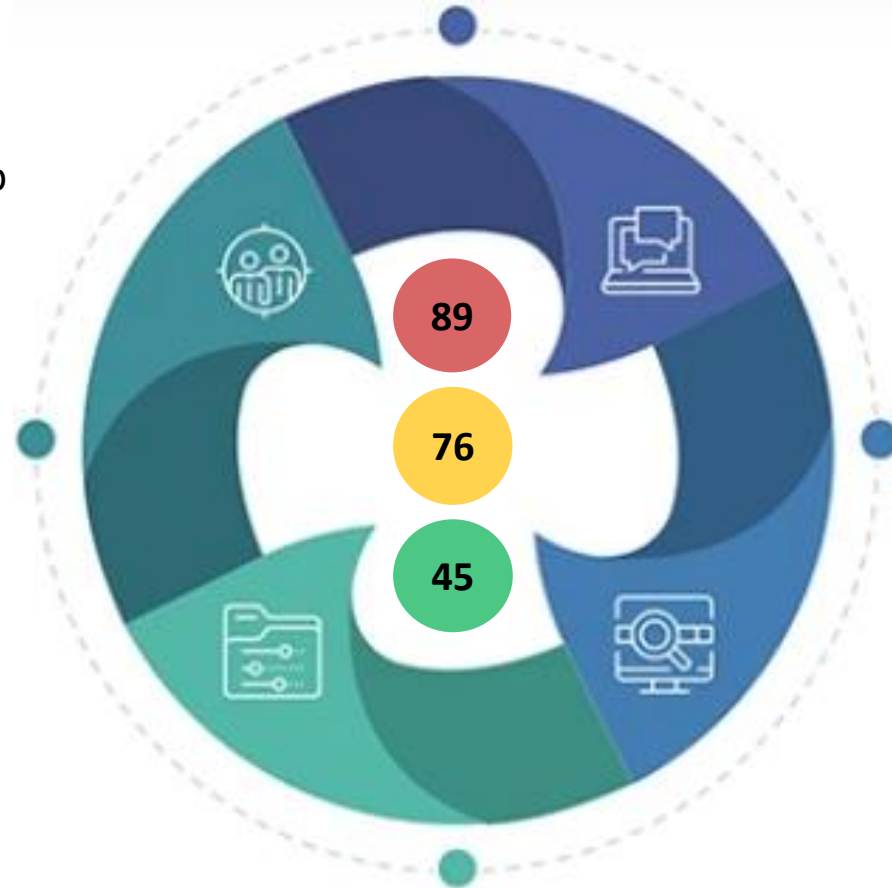
red – risks with a high probability of verification, **yellow** – risks with a high possibility of false positives, **green** – risks with specific types of relationships

RELATIONSHIPS

- The dynamic of the relationship
- Duration of the relationship
- Time interval;

PAST

- Suspicion of an employee previously engaging in dubious transactions;



WORK

- Nature of business (subdivision, department);

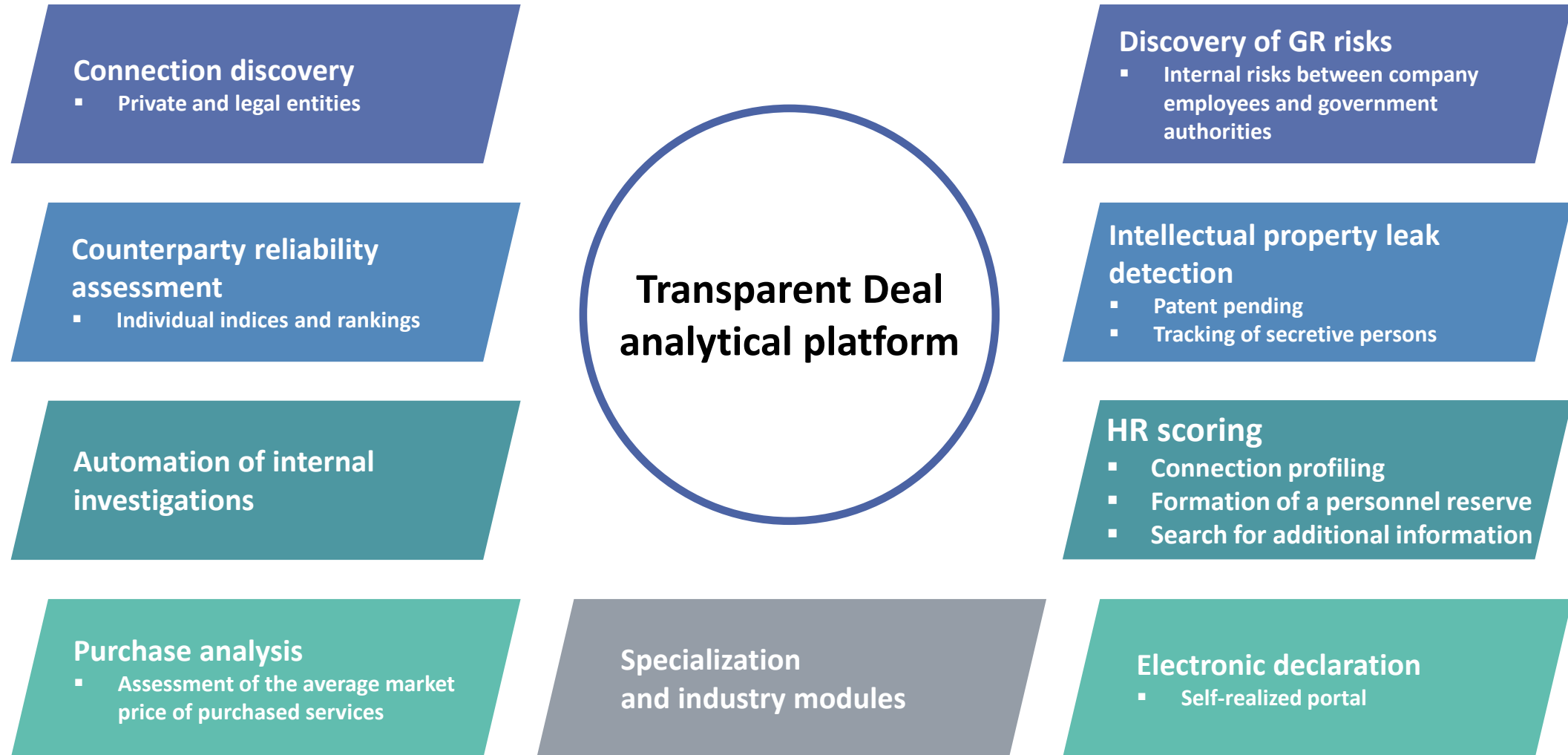
POSITION

- Risk of corruption within the employee's range of responsibilities;
- Level of impact on the transaction;

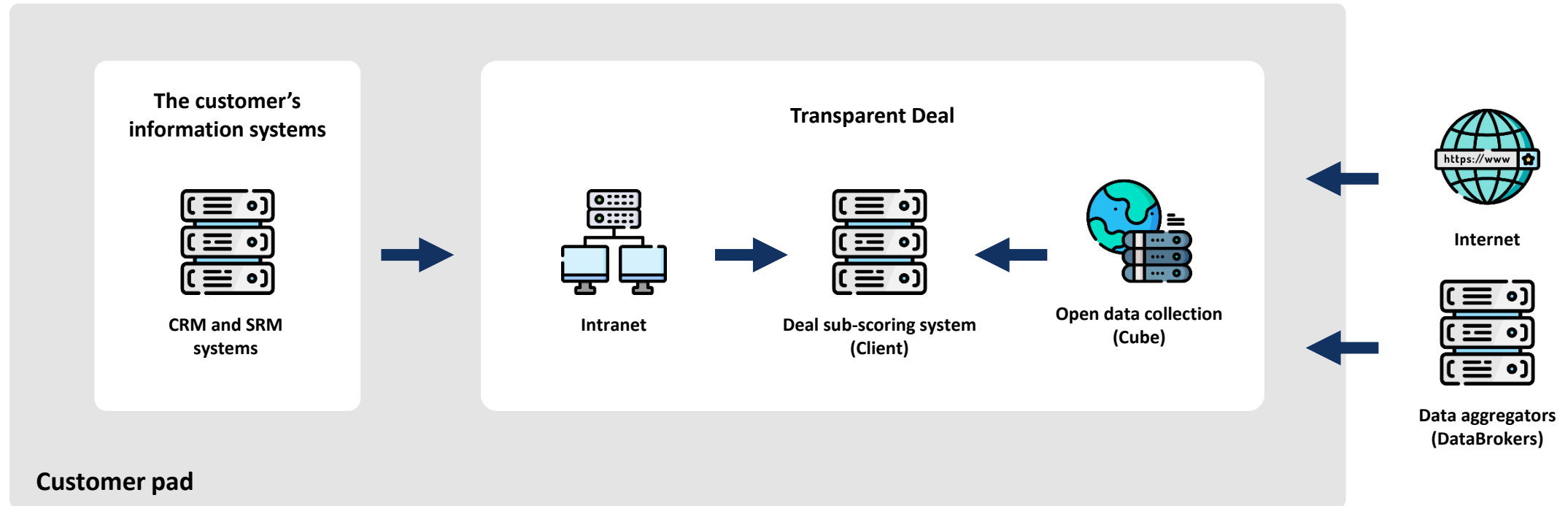
Functional customers automate department processes thanks to the analytics of the Transparent Deal platform



Modules of the Transparent Deal platform automate disparate company processes and converts them into a transparent system

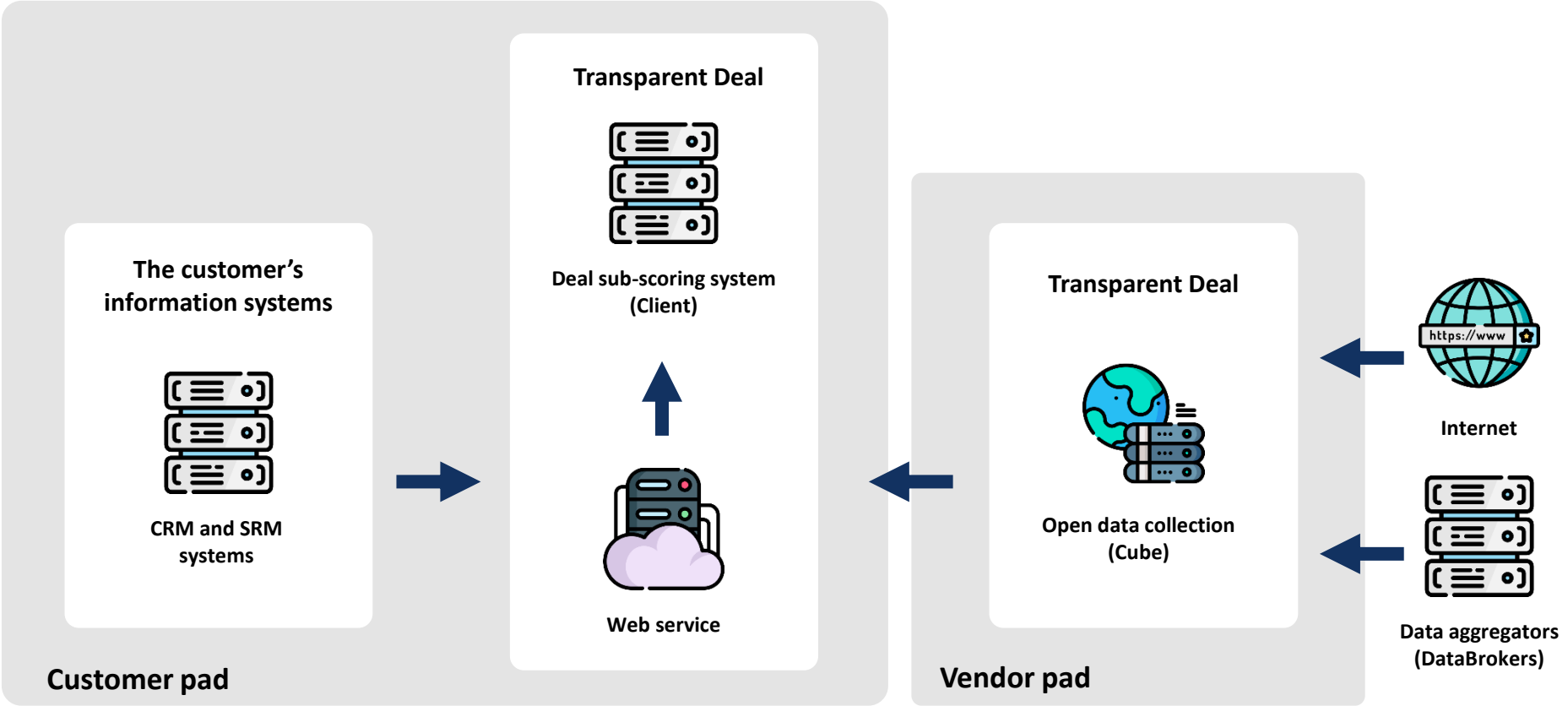


The on-premise format presents individual customization for the customer and offers deep process automation



Example of on-premise actualization

The hybrid solution offers various integration options with the customer's information systems and databases



Example of hybrid actualization

We measure project results and improve process automation for our customers



World leader in cybersecurity



4500 employees, ~ 800 in the risk zone



3500 counteragents



Over 60 000 deals



Hybrid integration format

Customer problems:

- No automation to verify compliance with procurement procedures;
- No verification of data compliance in various systems;
- No automation for contract verification;
- Security services waste significant time on manual information analysis.

The objective:

- Conducting automatic verification of employee and counteragent connections to discover conflict of interest when analyzing expense and revenue contracts;
- Checking deal data compliance in various systems and finding discrepancies in procurement procedures;
- Analyzing deals in accordance with procurement procedures and discovering contract fragmentation factors.

The results of integrating the system:

- The security service prevented contractual transactions with inflated prices and bad faith participants;
- The workplace efficiency of security service employees increased as they managed to automate the identification of connections with conflict of interest and sped up the verification process.
- The security service prevented procurement violations with purchases above the approved cost, the fragmentation of contracts, and the involvement of insider affiliated counterparties discovered by the system.



Transparent Deal Business Processes Analysis and Clarity Check

Analyzing business processes related to economic security does not only offer opportunities for automation, but also to receive the full benefits of the system within 1,5 months of exploitation.

The main value of the project is to solve the client's key problems and to offer automation options within a short period of time

1. **We approach the client's problem-solving process when finding interconnections quickly and efficiently** – the large number of employees and counteragents at the company highlights the need to automate current processes

2. **We offer the implementation of new approaches to solve the task** – we don't only collect and analyze the company's current experience, but we also aggregate all the needed sources in a unified system to achieve a complete solution

3. **We share our experience and methods for analyzing interconnections:** we increase the effectiveness of source usage, optimize the process by tuning the scoring model, and place the discovered connections in different groups for a high-quality analysis

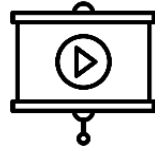
4. **We develop and prepare unique automation solutions** based on the results that we get from analyzing **your data**

The TD system will conduct a real connection search between physical entities and counteragents by using various data sources

The system finds the type of connection:



Work



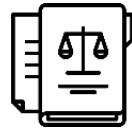
Education



Social networks



Ownership by legal entities



Intellectual property



Familial relations

Open sources

- business and IS registries
- Social networks and HR services

Additional sources are discussed individually

With the use of open sources we conduct:

- Profiling of the customer's employees
- A connection search between the customer's employees and counteragents
- A connection search between the customer's employees and affiliated counteragents

With the use of additional sources we conduct:

- An analysis of a physical entity's telephone and email
- A bankruptcy or debt verification of a physical entity
- A search on the base of a physical entity's leak of offshore jurisdictions
- An analysis of the counteragent's financial welfare
- A verification of the counteragent in the database of untrustworthy counteragents
- An analysis of reputational risks
- A verification of counteragents on the customer's own indices



Thank you

Andrey.Shpurik@kaspersky.com

Kaspersky
Transparent Deal