Use Case: Border Security

Segment: National Security

Products: Rosette

Functions: Name Analytics

Availability: API or SDK

What Better Border Security means

- **Missing even a single match** against a watchlist puts your citizens at risk.
- Border security is **moving beyond watch lists** to combat terrorists using fake or stolen IDs.
- **Skillful mining of big data** is a powerful resource for counter terrorism, cybersecurity, drug policy enforcement, border security, and intelligence gathering.
- **Accurate identity verification** crosses traditional boundaries of geography, language, and culture.
- Border security increasingly requires **social media analytics with the predictive insights** needed to both identify new risks and protect populace during demonstrations and periods of unrest.

A false negative

means you let in a security threat

A false positive

means you deny entry to a legitimate visitor or overload your border officials

Make sure your name matching solution delivers the fastest results possible, while minimizing errors of both types. Assess its ability to scale as watch lists grow and the volume of refugees, migrants, and visitors increases.

Your ability to meet all these expectations depends on a critical technology category—high quality, multilingual, multi-script **text analytics**.

With results that:

- Provide fast identity matching, even where border officials operate with modest resources.
- Supply your agency with the social media analytics needed to identify potential risks that don't yet appear on watch lists.

Nine questions to ask about your software on the next page

Essential Questions to Ask About Border Security Solutions

Serious Consequences:

With millions of people crossing borders every year, can your agents reliably ensure that no terrorist is admitted?

Many Watch Lists:

Has the name of each person at each checkpoint been accurately screened against all available watch lists?

Known Unknowns:

Are you able to identify a potential new threat, even when that person doesn't appear in any existing watch list or database?

1. **How reliable is my current solution's name matching?**
The first hint that a visitor may be on a watch list is a name match. You need a product that can identify individuals through their legal name, nickname(s), initials, truncations, and all possible misspellings and iterations, regardless of language and across scripts.

2. **Why isn't the traditional name matching approach—of generating variations—adequate to match misspelled names?**
A three-component name translated into English can have billions of variations. It's unlikely any software could generate them all. When even a single failure to match a single name can be the difference between life or death, it is simply too risky to rely on outdated methods. A name matching solution based on algorithmic matching of names will miss fewer matches.

3. **How rigorously does my product track identity across languages?**
Border security depends on cross-lingual matching and linguistic capability across non-Latin script language, including difficult languages (i.e. Arabic, Pashto, Persian, Russian, Japanese, Chinese, Korean). In addition, name matching must account for nicknames, spacing errors, misspellings, and even when a name is entered in the wrong field. Your solution must reliably identify "Muhammad Taher Anwari", "Mohammad Tahre Anwari", "Muhammad Tahir Anwari ", "Haji Mudir" "ムハンマド・ターヘル・アヌワリー" and "مُحَمَّد طَاهِر أَنْوَرِي" as the same person.

4. **Can I get reliable watch list screening at border crossings with limited infrastructure?**
You want a solution that provides fast and accurate results, even with a single laptop that can be relied on in case of power outages or borders with minimal infrastructure.

5. **Can my solution scale affordably as name matching demands continue to grow?**
All watch lists are works in progress. As each grows, the number of name matches grows without limit for name-generation solutions, but not for knowledge-based solutions. You want a solution that absorbs change, with minimal additional hardware or cost.

6. **Can my solution match names even when components are entered into the wrong fields?**
When your organization is held accountable for accurately matching names against a growing number of watch lists, it is risky to rely, for example, on a bank employee in Chicago knowing that a Mexican customer's surname is often two words, where one name may be mistakenly entered as a middle name.

7. **Can my solution help me identify new potential threats?**
You want a solution that takes advantage of open source intelligence to gather information from social media on people who are NOT on watch lists. For example, border security can use social media to ask a visitor a few verifiable facts, potentially exposing a fake or stolen passport holder.

   Advanced *text analytics* CAN also spot relationships between people on a watchlist and others, another way to discover new and potential threats. Each time a new entity is flagged, your solution should be able to monitor that person going forward.

8. **Can my solution analyze any textual data?**
The optimum solution will work right out of the box but also be adaptable over time to increase accuracy. Adaptable models allow you to easily improve the quality of your intelligence analysis through training and accommodating different sources (i.e. databases, tweets, blogs, message traffic, chat, etc.)

9. **Is there a way to increase accuracy and cross-lingual matching functionality in the solution I have now?**
There are name matching products designed to seamlessly layer on top of your existing functionality without adding expensive additional hardware. You may even experience a reduction in licensing fees.