unisys

Executive brief

Next-generation risk and fraud prevention requires a revolutionary approach

Highlights

- Gain insight in seconds with real-time risk identification, scoring and targeting functionality
- Improve accuracy by combining rules, predictive analytics and machine learning
- Take control of risk profiling by tuning risk scores and thresholds using a highly intuitive interface
- Increase automation and hit rates, thereby reducing false positives
- Ensure all identified "hits" are easily viewed and explained
- Use data science as a service (dsaas) to achieve rapid threat detection and interception
- Perform real-time package testing against live inbound transactions before deployment
- Experience rapid, cost-effective and highly available deployments using cloud or on-premise containerized architectures

As enterprises digitize processes and customer interactions, their expanding digital footprint is leading to increased risks of fraud. Across multiple domains – finance, borders, healthcare, law enforcement and more – much is at risk. When you fall victim to fraud, your customers lose confidence; your borders and perimeters are exposed; and your business may lose money, suffer reputational damage, face potential penalties or even become a victim of organized crime or terrorism.

Expanding volumes

In 2021, cybercriminals inflicted over $6 trillion in damages. While these figures are astounding, cyber fraud is expected to continue growing 15% year-over-year, reaching more than $10 trillion by 2025. Organized criminal gangs and other bad actors employ and share an expanding range of sophisticated techniques and technologies to subvert and circumvent traditional fraud and risk targeting solutions.

Spiraling costs

Organizations spent nearly $27 billion in the global fraud detection and prevention market to deal with fraud volumes in 2021. This amount will reach over $81 billion by 2026, a 24% year-over-year increase. Even at these accelerated investment rates, organizations relying on outdated engines, which can't rapidly adapt to new threats as they develop, simply can't keep up with the spending required to combat risk and fraud.

False-positive drain

As more fraud occurs and less is detected, organizations must take an increasingly conservative approach to risk. This leads to less automation and more human intervention. As a result, organizations experience significant increases in business friction as false-positive hits are amplified and require additional manual checks by overworked teams, resulting in dissatisfied customers who encounter disruption.

A smart approach to risk, fraud and targeting

Unisys is a proven leader in the delivery of security and targeting solutions, protecting borders and finding patterns in vast volumes of airline, passenger and cargo data to intercept criminals, narcotics, drugs and firearms before they can do harm. This expertise is the foundation of the Unisys Risk and Fraud Targeting Solution (RaFTS).

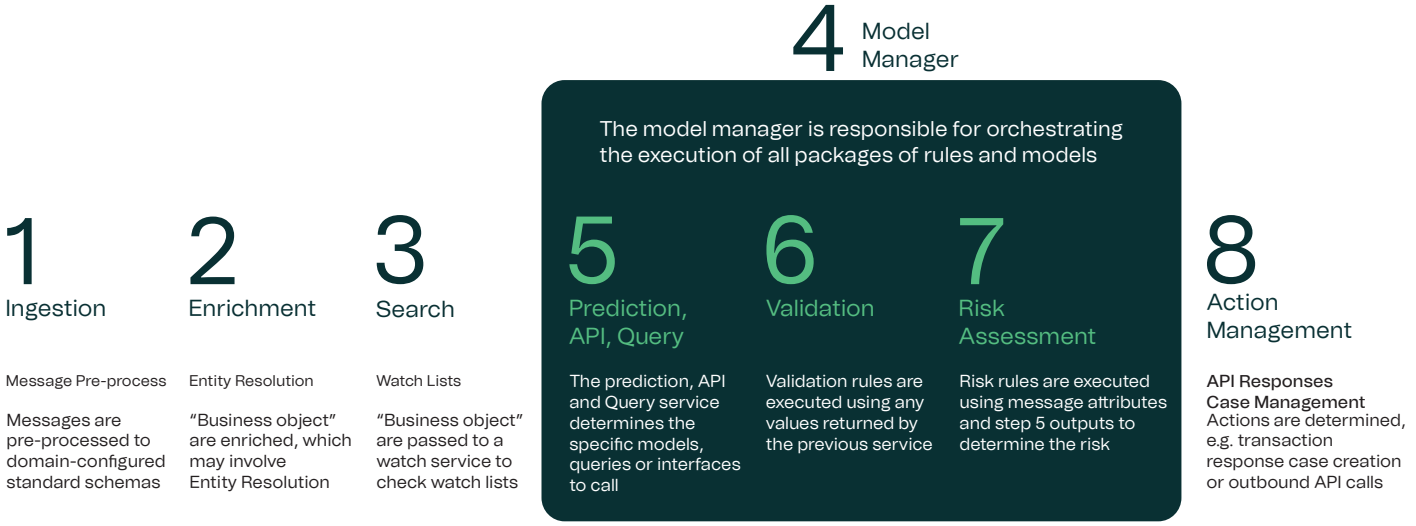
RaFTS is a powerful, open and highly flexible risk-scoring platform. The result is an easily configurable, scalable rules- and AI – based solution – deployed in the cloud or on-premise, with an optional fully managed service offering. It supports large and small institutions alike, allowing organizations to tackle current risks and rapidly adapt to new trends while presenting an intuitive approach to risk presentation, which doesn't bury hit reasons in a "black box."

Single solution, many domains

The flexibility of the RaFTS eight-step workflow process (see the figure) means it can tackle fraud across many operational domains and modalities in a single solution. Some possible scenarios include:

- **Payment fraud**: Apply rules and AI to detect high-risk transactions such as debit and credit card payments.
- **Money laundering**: Analyze patterns in financial transactions to detect money laundering, report suspicious activity to decisionmakers and use historical data to continuously improve.
- **Border-risk targeting**: Protect borders by detecting illegal entries and the importation of unregulated and illegal goods based on the analysis of vast volumes of data from airlines, cargo shippers and government systems.
- **Healthcare fraud**: Minimize the impact of fraud on healthcare costs by analyzing data from healthcare and insurance systems to identify claimant, provider and prescription fraud.
- **Check and signature fraud**: Utilize next-generation image analytics and AI to gather and verify data and signature images to prevent fraud while minimizing false-positive hits.

Figure: RaFTS Workflow Process



RaFTS features

Flexibility and extensibility

Criminals rapidly adapt to evade detection, so solutions must also quickly adapt through configuration without having to wait for a new product release. RaFTS allows new data attributes to be passed in and used without requiring development work. Before deployment, new rules and AI models can be tested against historical and live data feeds. You can edit rules and weightings to fine-tune hit rates. The plug-in model architecture allows the reuse of in-house collateral, and the entire solution can run alongside existing systems to augment legacy capabilities with modern AI techniques to tackle false-positive hits.

Open and explainable

Targeting systems that use a combination of rules and AI cannot afford to be black-box offerings that simply provide a status code for their results. AI must be explainable to prove non-bias and to engender trust. Organizations need to understand why transactions are intercepted with fully logged and user-viewable descriptions of the rules and models that executed. They must also present the risks identified, the weightings applied and the overall output score that led to the final transaction outcome.

Continuously improving

The rules and models for today will not be applicable tomorrow. Waiting for system updates to deal with threats in a fast-paced, ever-changing landscape will not work. Our managed service provides dedicated agile data science teams who work to improve transaction targeting. This team of experts will adapt to new vectors and modify rules and weightings to correctly identify, intercept and review high-risk transactions. This approach allows new rules and models to be developed, tested using Impact Analysis and deployed as Test Packages before publishing changes to the “live” risk-assessment engine.

Self-learning for greater accuracy

RaFTS transcends predefined algorithms to include predictive analytics and machine learning, allowing the system to learn from experience. Models are automatically updated to continuously improve assessment accuracy.

The algorithms are also derived from the data rather than human experience, so RaFTS avoids the problem of actual or perceived bias in the results it provides.

Why is Unisys RaFTS unique?

RaFTS provides you with a different and better approach to risk management that rapidly adapts to how modern criminals think and operate across business areas, technology and borders. What sets this solution apart is that it offers:

- A wide range of features (cloud deployment, AI/ML models, user-configurable flexible rules, DSaaS, market-leading visualization, microservice and containerization)
- An ability to tackle multiple domains and modalities in one offering

When you add to this the heritage that Unisys brings in real-time transaction-based targeting, Unisys stands out with an offering and history that is unique, arming you to face the challenges that lie ahead.

For more information, please visit us online: unisys.com/solutions/business-process-solutions.

unisys

unisys.com

12/22 22-0404