

CASO DE ÉXITO



Rabobank

RiskShield proporciona una solución de monitoreo flexible y multiusuario para gestionar las transacciones financieras y las actividades de los clientes

El fraude en línea es hoy en día una de las principales preocupaciones de los bancos. Rabobank, un pionero de la banca en línea, conoce la importancia de combatir el fraude y proteger a sus clientes al haber experimentado ataques en línea en 2007. Aunque no causaron ningún daño grave, quedó de manifiesto que la naturaleza del fraude en línea estaba cambiando. El fraude es cada vez más sofisticado y, por lo tanto, más difícil de combatir sin las herramientas y una estrategia adecuada de prevención del fraude.

“RiskShield realmente nos ha sorprendido”, comenta Wibout de Klijne, jefe de Crimen Económico Financiero en Rabobank Group. “Conocíamos las capacidades de monitoreo de transacciones de INFORM y realmente nos impresionó la flexibilidad, el rendimiento y la rápida capacidad de respuesta a los constantes cambios en los modus operandi de los cibercriminales”.

Rabobank

Rabobank Group es una de las instituciones financieras líder en el mundo. Con origen en Holanda, se ha expandido en las últimas décadas como un proveedor internacional de servicios financieros que tiene actividades en el campo bancario, gestión de activos, leasing, seguros e inmobiliario.

- Número de titulares de cuentas: 12 millones
- Número de transacciones de pago por mes: 300 millones
- Monitorea entre 750 y 900 millones eventos en tiempo real por mes, con un rendimiento peak hasta 10 veces más rápido

Rabobank usa el software de RiskShield para detectar y evitar transacciones fraudulentas en la banca en línea, las transferencias de pago nacionales e internacionales, las transacciones de tarjetas y cajeros automáticos y en áreas como el monitoreo de la integridad de pago y la identificación de PEP y evaluación de sanciones.

www.rabobank.com



Fue muy rápida la implementación y puesta en marcha de RiskShield para monitorear los complejos sistemas bancarios centrales del banco, la que se realizó en seis meses. Para los canales virtuales, como la Banca en Línea, solo se necesitaron tres meses adicionales para que estuviera en funcionamiento. RiskShield ahora funciona completamente independiente como una capa de seguridad invisible sin tener un impacto en los sistemas bancarios centrales. Cuando se detecta una transacción sospechosa, RiskShield automáticamente solicita una acción en tiempo real para detener el procesamiento del pago en el sistema bancario central. La facilidad de uso y flexibilidad de la tecnología, como también la estrecha colaboración con INFORM, significó que Rabobank fue capaz de superar las expectativas en todos los plazos de implementación, lo que fue impresionante considerando el tamaño del banco y la sofisticación de sus sistemas bancarios.

Combatiendo el cibercrimen

El primer objetivo de Rabobank con RiskShield era identificar y detener transacciones sospechosas dentro de sus servicios bancarios en línea. Rabobank procesa millones de transacciones en línea por día. Para poder identificar ataques fraudulentos o apropiaciones de cuenta, el banco cuenta con RiskShield para crear una vista holística del comportamiento de las transacciones de sus clientes. Una característica clave del software es la manera en que combina una gran cantidad de eventos relacionados y no relacionados en un solo punto de toma de decisiones. Gracias a un análisis minucioso en cada paso de una solicitud de pago en línea, el comportamiento histórico del cliente y otras informaciones relacionadas, como los detalles de la interfaz de usuario, RiskShield puede evaluar el riesgo de cada transacción en cosa de milisegundos. Una gran cantidad de procesos inteligentes de decisiones ocurre en tiempo real para verificar la legitimidad de la transacción. Si hay una gran probabilidad de fraude, el software tiene la capacidad de detener completa y automáticamente la sesión web y el proceso de pago.

“RiskShield permite a nuestro equipo ser capaces de reconocer fácilmente patrones como ataques de intermediario, apropiaciones de cuenta o cualquier otro esquema de patrones fraudulentos” comenta Wibout de Klijne. El software monitorea e identifica automáticamente todos los patrones conocidos de ciberataques. Tan pronto como se identifica un nuevo patrón, el banco es capaz de reaccionar inmediatamente mediante el inicio de nuevas contramedidas para bloquear los nuevos patrones fraudulentos. Los profesionales de gestión de fraude de Rabobank cuentan con las herramientas para ajustar todos los tipos de situaciones antifraude y pueden introducir nuevas reglas para prevenir nuevos ataques sin causar molestias al cliente.

Los profesionales de gestión de fraude tienen la capacidad de incluir todo tipo de información en la lógica de decisiones y pueden crear y activar fácilmente nuevas reglas y escenarios en producción, sin comprometer los sistemas bancarios centrales. “La arquitectura de RiskShield es excepcional. Además de su extremado alto rendimiento en el monitoreo de 3.000 pagos por segundo, estamos impresionados con la manera en que RiskShield encapsula los componentes del motor de reglas”,

comenta Wibout de Klijne. Los profesionales de gestión de fraude cuentan con la facultad de gestionar diferentes escenarios de fraude. Tienen el control total para crear, probar e implementar cualquier regla nueva o configuraciones de algoritmos sin involucrar ningún otro departamento, como el de TI. Esto protege la inteligencia de negocio del banco y evita que acceda cualquier persona no autorizada por el equipo de fraude. Rabobank ha sido capaz de detener más del 99,8% de todas las transacciones fraudulentas durante un gran ataque de cibercrimen.

» **La arquitectura de RiskShield es excepcional. Además, gracias a su extremado alto rendimiento en el monitoreo de 3.000 pagos por segundo, estamos impresionados con la manera en que RiskShield encapsula los componentes del motor de.**

Adaptación de RiskShield para AML, identificación de PEP y normas de sanciones

Luego de ver los resultados positivos de la implementación inicial de RiskShield, Rabobank decidió explorar otras áreas de negocio para expandir el uso de la herramienta. Una de las primeras áreas a evaluar para una posible expansión era la protección contra el lavado de dinero (AML) y la evaluación de la lista de vigilancia. Tras investigar sus requisitos, estaba claro que RiskShield sería ideal para sus necesidades de identificación de PEP y evaluación de la lista de sanciones.

Los profesionales de cumplimiento ahora están mejor facultados para escoger de cualquier fuente de datos y algoritmos de evaluación para ajustar los resultados de comienzo a fin. Los resultados son impresionantes. El número de resultados falsos ha disminuido drásticamente y el rendimiento general de la evaluación de la base de datos de clientes ha incrementado considerablemente. Los profesionales de cumplimiento pueden configurar ellos mismos los algoritmos y crear variables adicionales para enriquecer la fuente de datos. Además, RiskShield les otorgó flexibilidad en comparación con los otros proveedores que evaluaron, los que solamente proporcionarían escenarios y algoritmos como una caja negra. El equipo de cumplimiento utilizó el conjunto de herramientas flexible de RiskShield para personalizar completamente el motor de lógica de decisiones de acuerdo con cada una de sus necesidades y normas.

Se espera que la implementación de RiskShield para identificación de PEP y evaluación de sanciones entre en funcionamiento muy pronto. En las áreas de cumplimiento, Rabobank está evaluando la posibilidad de reemplazar su herramienta actual de monitoreo de transacciones de AML por RiskShield. El plan es eliminar gradualmente la solución anterior y comenzar a usar RiskShield para monitorear comportamientos sospechosos de lavado de dinero.

Integridad de pagos y detección de fraude interno

En 2012, Rabobank implementó otro proyecto para introducir RiskShield como una herramienta de validación para monitorear el procesamiento de pagos. Rabobank buscaba una solución para proteger la integridad de las operaciones de pago. Procesar los pagos es una tarea muy compleja que involucra varios sistemas diferentes. Para poder garantizar que un pago haya seguido los procedimientos correctos, Rabobank quería monitorear todo el flujo del proceso, desde el inicio del



Wibout de Klijne,
jefe de Crimen Económico Financiero
en Rabobank Group



pago hasta cuando los fondos salen del banco. Fueron capaces de verificar cada paso del proceso en la cadena de pago y revisar si es que algo cambió entre la solicitud de pago original y la transferencia final. Si algo ocurría entremedio de los procesos, ya sea por fallas del sistema o por interferencia humana, RiskShield automáticamente alertaría sobre la transacción para mayor investigación. Este proceso permitió a Rabobank monitorear cualquier pérdida de pago producto de un posible fraude interno, incidentes operacionales o fallas de software y hardware. Rabobank incorporó una red de seguridad adicional a través de RiskShield para proteger las operaciones de pago del banco y eliminar cualquier deficiencia en el proceso.

RiskShield es una fuente de poder independiente y multipropósito

RiskShield ofrece una interfaz adaptable, intuitiva y visual para desarrollar, mantener y analizar el software de detección de fraude. Ni el departamento de TI ni ningún especialista de INFORM tiene que involucrarse para ejecutar nuevos escenarios AML y antifraude, lo que significa que los profesionales de gestión de fraude pueden ejecutarlos por su cuenta, lo que los ayudó considerablemente a ajustar los resultados para lograr el mejor resultado posible. Dentro de nuestro entorno de producción, el banco puede usar datos de producción en directo para probar el resultado de nuevas reglas desarrolladas. Esto le otorga una visión muy realista de los resultados de sus pruebas. "Esto es único en el mercado y nunca me he encontrado con otro proveedor con una oferta de esta dimensión", indica Wibout de Klijne. Rabobank reconoce el potencial de RiskShield en muchas áreas diferentes de la organización y firmó un contrato de licencia de software con INFORM que le permite al banco uso ilimitado en una escala global.

Los beneficios

- Hasta 10 millones de transacciones se monitorean diariamente en tiempo real
- La solución flexible RiskShield se puede actualizar y adaptar por profesionales de gestión del fraude para enfrentar nuevas amenazas en cosa de minutos
- La cantidad de falsos positivos se reduce considerablemente gracias a sus capacidades más precisas de monitoreo y ajuste.
- Cada transacción se evalúa automáticamente para identificar potenciales fraudes en milisegundos
- Cualquier modificación o configuración de TI se puede adaptar fácilmente por profesionales de TI de la empresa

Si desea saber más, nos encantaría saber de usted.

INFORM GmbH / Área de negocios Risk & Fraud
Pascalstr. 35, 52076 Aachen
riskshield@inform-software.com / riskshield.co