

From alerts to answers

Get a 360° view of financial crime and risk
with NTT DATA and Splunk



Contents

03 Financial crime and risk are connected. Most defenses are not.

04 Build the foundation for 360° visibility

05 The top four challenges facing today's financial institutions:

- 05 Siloed tools and teams leave the full threat picture out of view
 - 07 Alert noise exhausts teams and hides the threats that matter
 - 09 Manual reporting keeps financial institutions preparing for yesterday's exam
 - 11 Data and tool sprawl make financial crime operations slower and more expensive
-

12 Build an interoperable financial crime and risk operating model with NTT DATA and Splunk

Financial crime and risk are connected. Most defenses are not.

Financial crime moves across accounts, channels, products, entities and jurisdictions without regard for organizational silos. Criminals now use generative and agentic AI, along with automation, to execute increasingly sophisticated attacks at greater speed and scale. When viewed separately, each event can seem explainable. But when events are considered together, they may reveal a coordinated, AI-powered scheme already gaining momentum.

Yet many institutions still fight that threat with fragmented data sources, analytics and teams. Different teams may evaluate the same customer or transaction using incomplete context and inconsistent scoring methods. Meanwhile, analysts become buried in alert noise. Meaningful signals disappear between systems. Technology estates grow more expensive with every new point solution. Compliance teams must reconstruct evidence after the fact.

Financial institutions must make a fundamental shift to keep pace with today's financial crime and risk environment. That starts with a foundation for 360° visibility, supported by models and analytics that connect defenses across the digital ecosystem.

The next era of financial crime operations will depend on four shifts:



Connect data, tools and risk analytics



Cut through alert noise with context and risk scoring



Embed audit readiness into daily operations



Bring technology sprawl under control

\$4.4 trillion

in illicit funds moved through the global financial system in 2025, up \$1.3 trillion in just two years

Source: Nasdaq Verafin, *Global Financial Crime Report*, 2026

Build the foundation for 360° visibility

Start where you are with NTT DATA

Before you can connect your financial crime and risk operations, you need a clear understanding of the systems, data, models and workflows already in place.

NTT DATA can then help map your existing ecosystem to a practical modernization roadmap based on operational readiness and business priorities.

With that roadmap in place, you can define a more integrated operating model that brings data, analytics and risk together around a shared view of financial crime and risk. Instead of another point solution, you need a flexible environment that can connect existing tools, correlate risk across domains and support practitioners with consistent, enterprise-wide visibility.

Discover a comprehensive view of financial crime and risk with the NTT DATA Fraud, Risk and Intelligence Management platform

The NTT DATA Fraud, Risk and Intelligence Management platform, powered by Splunk, provides that foundation. The solution is purpose-built to help you connect financial crime and risk analytics, improve detection quality, strengthen compliance operations and modernize at a pace aligned with your business priorities. It brings financial crime and risk data into a shared environment so practitioners can work from a more consistent enterprise risk picture. It provides a transparent, explainable framework for evaluating risk, refining detection logic, reducing manual work and improving financial crime decision-making over time.

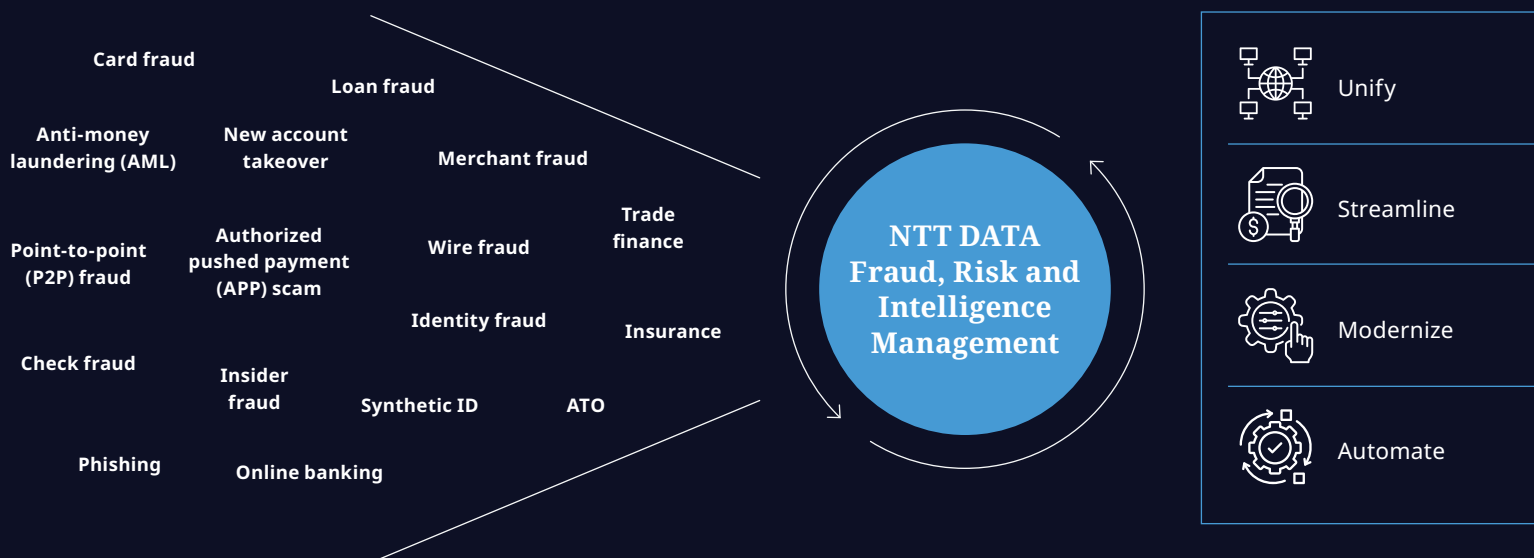
Next, we'll explore four challenges the platform can help institutions address by creating a more connected, enterprise-wide view of risk.

An assessment from NTT DATA can help establish a maturity baseline by identifying:

- Fragmented or duplicated tools
- Siloed data or workflows
- Inconsistent risk-scoring approaches
- Gaps that limit enterprise-wide risk visibility
- Capabilities that should be retained, integrated or consolidated
- Opportunities to improve operational efficiency and regulatory readiness

Journey to 360° visibility

A single attack can span multiple financial crime domains and categories. The NTT DATA Fraud, Risk and Intelligence Management platform unifies fragmented financial crime data, correlating activity across domains to reveal hidden connections and deliver complete visibility across the financial crime landscape.



Siloed tools and teams leave the full threat picture out of view

Challenge 1: When every team sees only one piece

Financial crime rarely stays in one lane, yet financial institutions often view it through separate tools, teams and processes. Criminals can exploit those gaps and move faster than institutions or law enforcement can connect the activity. At the same time, regulators expect banks to identify, investigate and document the risks within their own environments.

Imagine it's 8am and your fraud detection system flags unusual card activity. Based on the available data and scoring, your team marks the activity low risk and closes it. Meanwhile, an AML model identifies an unusual wire transfer involving the same customer. Without visibility into the card activity, the alert appears explainable when evaluated on its own. Later that day, a sanctions screening system flags a related activity, while your risk team observes elevated exposure in the associated geography. Neither team can see the earlier activity, so each addresses the risk in isolation.

No team has enough context to recognize that the customer's activity, entity relationships and geographic exposure may be part of the same coordinated scheme. That fragmentation creates blind spots, duplicates effort, delays escalation and leaves institutions reacting to individual alerts, instead of seeing the coordinated scheme taking shape across accounts and geographies.

5+

NTT DATA assessments find that a typical bank relies on five or more fragmented financial crime data streams, tools and processes, often with limited interoperability or ecosystem-level integration.

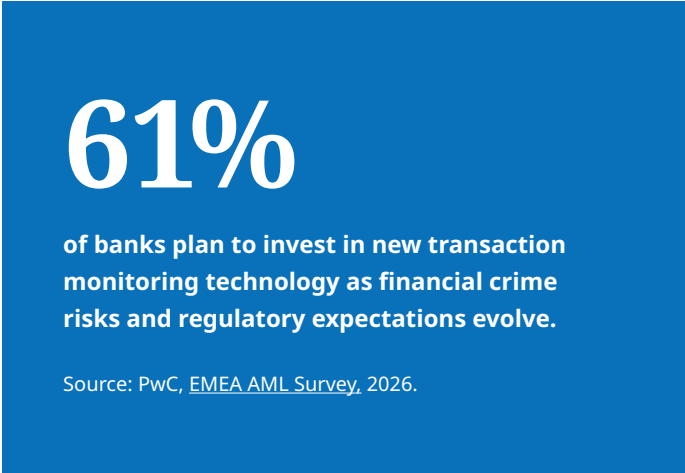
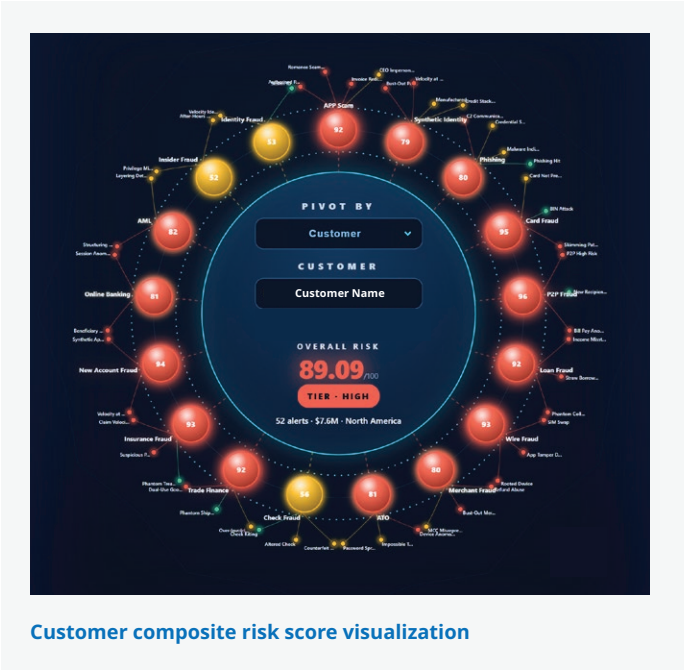


The solution:
Gain a 360° view of risk

Rather than replacing each domain's expertise, the NTT DATA Fraud, Risk and Intelligence Management platform connects data and insights across fraud, AML, sanctions, compliance and risk analytics through a shared data foundation.

Financial crime and risk practitioners need an enterprise-level view of how signals connect across customers, accounts, entities, products, channels and geographies. The platform correlates activity across domains and lets practitioners move from a broad pattern to the underlying evidence without switching between systems.

Risk scoring uses indicators from across financial crime domains, customer and entity activity, products, channels, geographies and third-party data sources. The solution normalizes those signals to help analysts and investigators compare risk consistently and identify connected patterns that individual tools may miss. Role-based views in the platform also give practitioners across risk and security teams the most relevant information tied to their responsibilities while keeping everyone connected to the same underlying risk picture.



The solution supports that shift by bringing fraud, AML, know your customer (KYC), sanctions, payments, account takeover and other domains into a shared data and analytics environment. The result is stronger cross-functional coordination, more consistent risk visibility and decisions grounded in the full context of illicit activity across the enterprise.



Alert noise exhausts teams and hides the threats that matter

Challenge 2: When volume overwhelms judgment

Financial crime and risk teams receive more alerts than they can reasonably investigate. Different tools, models and analytics often score activity independently, making it difficult to distinguish meaningful risk from routine behavior without additional manual work. Detection performance depends on four possible outcomes:

- True positives: meaningful threats correctly identified
- True negatives: routine activity correctly cleared
- False positives: routine activity incorrectly flagged as suspicious
- False negatives: meaningful threats incorrectly dismissed or missed

Focusing only on false positives and false negatives provides an incomplete picture. Improving true-positive and true-negative rates also helps strengthen detection quality. This matters across risk identification and classification, model development and tuning, and transaction monitoring. These decisions must also be defensible to internal auditors and external stakeholders, including clients, shareholders and regulators.

As alert volumes rise, meaningful threats become harder for practitioners to recognize before losses spread across accounts, channels and products. What's more, slower detection and response can increase customer friction and frustration.

59%

2025 saw a significant rise in malicious bot attacks as criminals tested and deployed sophisticated tools.

Source: LexisNexis, [Synthetic Identities and Agentic Bots Posing as Human Contribute to 8% Global Rise in Fraud Attacks, 2026](#).



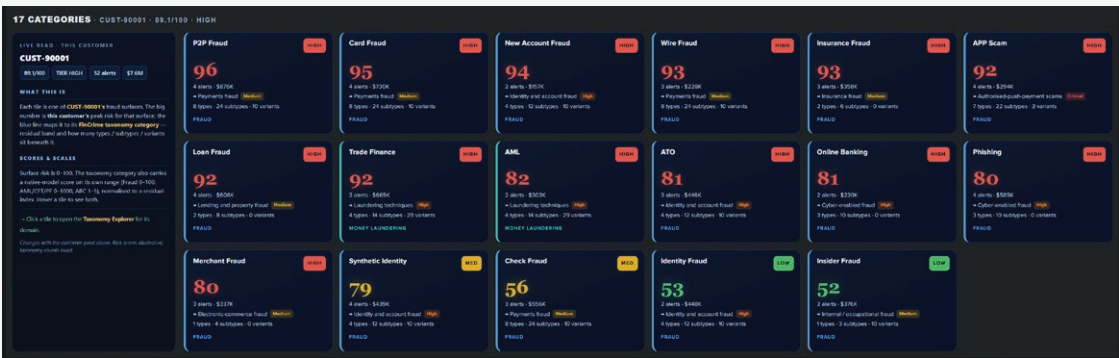
The solution:
Improve detection quality through context

Detection quality is a tradeoff, not a single metric. Institutions often optimize for reducing false positives because that cost is visible in analyst hours, while false negatives — the threats that were never surfaced — remain largely invisible and unmeasured. Evaluating the full confusion matrix and building a feedback loop that makes missed activity measurable is what separates tuning from genuine improvement. Despite decades of investment in financial crime controls, [the scale and sophistication of attacks continue to grow](#).

Financial crime and risk practitioners need to understand how one signal relates to the broader pattern of activity. The Fraud, Risk and Intelligence Management platform uses analytics and automation to connect related activity

across customers, entities, accounts and transactions, bringing together context that practitioners might otherwise assemble manually. Splunk AI can help teams recognize patterns, prioritize higher-risk activity and focus their expertise where it matters most while preserving human oversight and judgment.

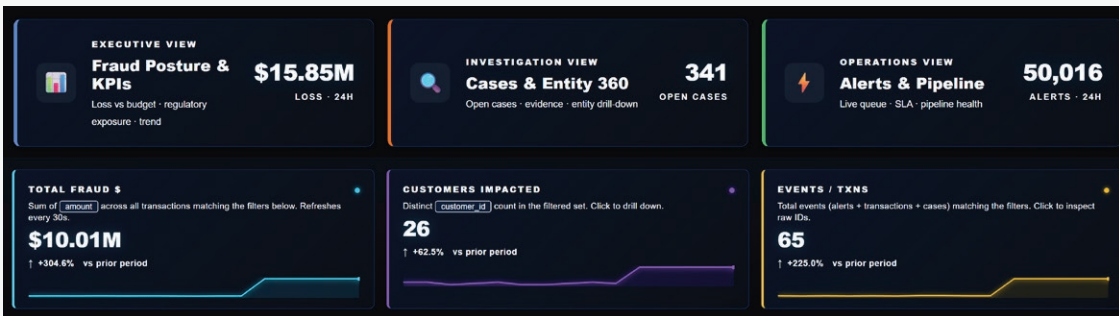
Ecosystem-level risk aggregation with the platform helps executives quantify multidimensional risk across the enterprise. Meanwhile, transparent, explainable analytics show risk teams *which signals* contributed to an outcome. Model developers can use those detection results and practitioner feedback to evaluate performance and refine thresholds, rules and models over time.



Financial crime and risk mitigation across global markets, products and business units

Shared risk views help teams prioritize activity based on broader context rather than the output of a single model or alerting system. Individual data sources may have limited coverage across products, markets or geographies. Ultimately, with NTT DATA and Splunk, risk practitioners across operational teams can move from broad patterns to supporting evidence without repeatedly switching tools.

The Fraud, Risk and Intelligence Management platform also delivers persona-based experiences designed for executives, managers, operations teams, investigators and auditors. Each persona receives a tailored view of the information most relevant to their responsibilities, enabling faster, more informed decisions.



Persona-based interfaces help increase productivity and reduce user fatigue

Manual reporting keeps financial institutions preparing for yesterday's exam

Challenge 3: When compliance becomes a scramble

Compliance and audit readiness processes remain highly manual, even as financial crime data volumes and regulatory expectations continue to grow. When evidence is scattered across multiple data sources, financial institutions must reconstruct customer histories, alerts, controls, decisions and case activity.

Financial crime and risk practitioners may also struggle to show which indicators were available, how risk was scored or how a dynamic or complex model (or series of models) contributed to a decision. Ultimately, this volume of manual work pulls teams away from higher-value activities and increases the risk of inconsistent evidence, delayed suspicious activity or transaction report (SAR/STR) preparation, incomplete audit trails and slower responses to regulatory change across jurisdictions.

Without a shared, time-based record of risks and decisions, organizations may be able to produce a report but still struggle to demonstrate to auditors, shareholders and regulators how their financial crime controls worked in practice.

90%

of financial services institutions believe that compliance requirements have become more complex.

Source: LexisNexis, [5 Trends Poised to Shape the Financial Crime Compliance Landscape in 2026](#), 2026



The solution:
Make audit and examination readiness
part of everyday operations

An AI-enabled compliance model treats evidence as a continuous output of financial crime operations, not something assembled after the fact. As regulatory expectations rise, leaders should evaluate how AI-driven and agentic capabilities can support compliant, auditable workflows.

Financial institutions need a shared record of the alerts, risk scores, investigative decisions, control performance and case activity that can be traced over time. Beyond the result, institutions need evidence showing how each decision was made. They need to know which data fed which analytical process, when it was evaluated and what outcome it produced.

The NTT DATA Fraud, Risk and Intelligence Management platform delivers transparent and explainable analytics that can support stronger governance, auditability and regulatory review. This creates a clear and defensible trail from the original financial crime indicator to the organization's regulatory response. A unified data and analytics foundation makes it easier to reconstruct customer and entity histories, support a consistent view across governance and compliance teams, and reduce manual reporting through greater automation.

The platform can customize views in multiple ways (such as role, market, geography, business unit) to give leaders and teams access to the information most relevant to their responsibilities without separating them from the underlying record.

The platform supports this shift with full time-series audit trails, regulator reporting facilitation, role-based dashboards and other visual analytics that enable faster response, stronger traceability and more time for practitioners to focus on detecting and stopping financial crime.

These capabilities can help financial institutions move from reactive evidence gathering toward more transparent and timely decision-making, giving practitioners more time to analyze emerging risks.

Explainable AI matters
and is now expected

Better detection requires more than accurate models. Financial institutions also need confidence that AI-driven decisions can be understood, validated and defended. Explainable AI helps analysts understand why a model surfaced one risk and not another while supporting the transparency and governance regulators expect.

LLM REASONING TRACES — EVERY AI DECISION, WITH CONFIDENCE + RATIONALE									
TIME	DECISION ID	VERDICT	CONFIDENCE	MODEL	CATEGORY	AMOUNT	COUNTRY	AI REASONING TRACE	LATENCY
2026-09-19T10:28:52Z	DEC269738	REVIEW	75.3%	alo-detect-v5	Account Takeover	\$30,888	UA	Impossible travel NG to GB in 7 minutes, but SCA passed and device is known. \$30,888 pending adjudication.	1681 ms
2026-09-19T08:01:52Z	DEC471314	MONITOR	62.3%	card-risk-v4	Card Fraud	\$514	DE	New device but matching IP and usual spending hour. \$514 is within profile.	649 ms
2026-09-19T06:02:52Z	DEC889462	BLOCK	92.8%	mule-network-v2	Mule Activity	\$381,942	NG	Destination account received from 9 unrelated customers in 72 hours. \$381,942 onward transfer stopped.	810 ms
2026-09-19T04:50:52Z	DEC344846	BLOCK Confirmed finding at or above the auto-action threshold (confidence > 85%). The platform acts without waiting for an analyst.			Card Fraud	\$1,631	AE	Velocity 1.8x this customer's norm at \$1,631, inside segment tolerance.	592 ms
2026-09-19T03:32:52Z	DEC644666				Card Fraud	\$407	AE	New device but matching IP and usual spending hour. \$407 is within profile.	178 ms
2026-09-19T02:39:52Z	DEC823637				Trade Finance	\$547,727	DE	Invoice priced 41% above market for the commodity and route. \$547,727 documentary credit.	981 ms
2026-09-19T01:40:52Z	DEC999067	REVIEW	62.2%	alo-detect-v5	Account Takeover	\$57,067	NG	Impossible travel NG to GB in 7 minutes, but SCA passed and device is known. \$57,067 pending adjudication.	1660 ms
2026-09-18T22:49:52Z	DEC736667	BLOCK	97.8%	sanctions-screen-v3	Sanctions	\$732,456	NG	Beneficiary bank in a comprehensively sanctioned jurisdiction. \$732,456 halted.	1426 ms
2026-09-18T21:45:52Z	DEC298414	REVIEW	74.7%	alo-detect-v5	Account Takeover	\$88,112	UA	Impossible travel NG to GB in 7 minutes, but SCA passed and device is known. \$88,112 pending adjudication.	897 ms
2026-09-18T21:43:52Z	DEC816113	BLOCK	97.1%	card-risk-v4	Card Fraud	\$3,653	NG	Card present in two countries 41 minutes apart. Cloning confirmed on \$3,653 attempt.	1237 ms
2026-09-18T21:10:52Z	DEC638733	BLOCK	92.6%	mule-network-v2	Mule Activity	\$231,739	NG	Destination account received from 9 unrelated customers in 72 hours. \$231,739 onward transfer stopped.	2075 ms
2026-09-18T21:05:52Z	DEC602249	MONITOR	54.9%	card-risk-v4	Card Fraud	\$3,403	NG	Velocity 1.8x this customer's norm at \$3,403, inside segment tolerance.	404 ms
2026-09-18T18:26:52Z	DEC370521	ALLOW	97.0%	kyc-risk-v2	KYC	\$36,012	DE	KYC current, PEP screening clear, source of funds on file. \$36,012 within declared income.	590 ms
2026-09-18T18:26:52Z	DEC721036	BLOCK	92.3%	app-scam-detect-v3	APP Scam	\$134,328	UA	Beneficiary on the Internal mule register with 3 prior confirmed cases. \$134,328 held pre-settlement.	2227 ms
2026-09-18T17:23:52Z	DEC817621	REVIEW	72.2%	sanctions-screen-v3	Sanctions	\$431,388	UA	Fuzzy name match 0.83 against an SDN entry, DOB and nationality do not corroborate. \$431,388 held.	2215 ms

The LLM Reasoning Traces clearly show the verdict, associated metadata and rationale for each AI-based decision on the platform. These capabilities support explainable AI, transparency and governance.

Data and tool sprawl make financial crime and risk operations slower and more expensive

Challenge 4:

When every new problem adds another platform or data source

Financial institutions often build their technology estates one problem at a time. A new threat, regulation, acquisition or business line can introduce another team, point solution, data source or scoring model.

Over time, tech stacks and capabilities become harder to govern, more expensive to operate and slower to change. Different platforms may provide overlapping capabilities or rely on separate data pipelines, leading to inconsistent scoring methods or duplicated capabilities.

But as stakeholders look deeper into the tech stacks and data feeds, it becomes clear that while some capabilities overlap, gaps in visibility persist. Modernization becomes necessary. But how do you know which tools and data sources are most effective? How do you prove efficacy when you cannot yet see the entire ecosystem?

The solution:

Choose the modernization path that fits your institution

Your maturity baseline can guide which capabilities to retain, integrate or consolidate based on demonstrated effectiveness, operational readiness and business priorities.

1 Consolidate what no longer serves the enterprise

Institutions ready to simplify their estates can replace selected point solutions with one Splunk-based platform for monitoring, correlation, investigation and reporting. Consolidation reduces portal switching, overlapping licenses, duplicate integrations and support demands while creating a consistent data and risk model across financial crime domains.

The NTT DATA platform deploys prebuilt detection logic, dashboards, correlation rules and naming conventions on existing Splunk infrastructure. Organizations can start with high-priority domains, expand over time without rebuilding the foundation and consolidate point solutions where it makes business sense. The solution gives organizations the ability to rapidly develop, test and refine detection models as threats evolve, delivering time-to-value in weeks, not months.

2 Connect what still delivers value

Financial institutions do not need to abandon trusted tools to gain cross-domain visibility. Existing platforms can continue detecting activity within their domains while feeding context into the NTT DATA platform as a shared enterprise risk layer.

The approach preserves familiar workflows and prior investments. It helps teams compare signals across vendors, reduce manual reconciliation and investigate related activity without moving repeatedly between systems. The solution can also integrate with existing case management processes. Financial institutions can connect first, measure impact and then modernize selectively over time.

3 Strike the right balance for your organization

Financial institutions can also combine both approaches, consolidating tools that add cost or complexity while retaining those that still deliver value.

A hybrid path allows modernization decisions to reflect demonstrated capability, risk priorities, organizational readiness and broader business priorities. Teams can also modernize in phases while maintaining continuity across critical operations.

This phased path gives IT and enterprise architecture teams greater flexibility to modernize around contract renewals, expected impact, cost savings and operational readiness. Institutions can build one connected risk picture without forcing an all-at-once transformation.

Build an interoperable financial crime and risk operating model with NTT DATA and Splunk

As criminals increasingly leverage AI, the challenges facing financial crime and risk practitioners continue to grow. A more connected operating model can help institutions respond.

Institutions can transform fragmented systems into a shared enterprise foundation, replace alert noise with stronger detection quality and clearer risk priorities, and evolve manual compliance processes into more transparent, audit-ready and intelligence-driven operations.

The NTT DATA Fraud, Risk and Intelligence Management platform helps financial institutions, law enforcement and regulators make that shift with a shared data and analytics foundation across financial crime

and risk domains. By connecting data, models and risk analytics, organizations can gain key context to uncover coordinated threats earlier and act with greater confidence. It also gives institutions room to modernize on their own terms by connecting existing tools, consolidating selected platforms and adding new capabilities without rebuilding the entire environment.

A connected, 360° view of risk gives practitioners the visibility to recognize coordinated threats, the agility to respond as risks evolve and the flexibility to modernize over time.

Ready to get a 360° view of financial crimes and risks?

Connect with our team at na.us.fraim@global.ntt to explore how NTT DATA and Splunk help institutions unify risk intelligence, modernize flexibly and strengthen financial crime operations across the global enterprise.



NTT DATA Fraud, Risk and Intelligence Management.
One platform. Unified intelligence.

NTT DATA is a \$30+ billion business and technology services leader in AI and digital infrastructure. We accelerate client success and positively impact society through responsible innovation. As a Global Top Employer, we have experts in more than 70 countries. NTT DATA is part of NTT Group. Visit nttdata.com to learn more.

