Ecosystem thinking: the fraud and risk approach that protects from every angle

BT for financial services institutions

Contents

Cover all bases

Build a global fraud and risk solution with a leading ecosystem that's constantly innovating for the future.

Financial services firms face more and greater digital risks than at any time in their history. The global threat environment is constantly evolving, with new technologies, adversaries, and criminal techniques emerging weekly – and in response more and more regulations are being introduced.

So as digital threats proliferate, as malicious actors become more sophisticated and organised, and as regulations become tighter, the best defence is a multi-layered, fully integrated approach to fraud and digital risk. Staying ahead will require organisations to draw on partnerships that can blend the latest technologies in security to keep their people and customers secure, and keep the company as a whole compliant. We call it ecosystem thinking.

Like the 'embedded finance' or Banking-as-a-Service model that's redefining the industry, ecosystem thinking enables you to approach fraud and risk across the whole organisation. So instead of a fragmented focus on specific parts of the puzzle and several in-country point products as a response, ecosystem thinking allows you to build a consistent, end-to-end, global solution that brings together innovative partners to stay ahead of the threat.

Deploying ecosystem thinking allows organisations to build an anti-fraud and security portfolio that keeps them covered from all angles. By managing fraud and cyber risk across your entire business with an ecosystem of industry-leading partnerships you get: more efficient global fraud solutions, delivered faster and at a lower cost, all backed by our best-in-class resources and expertise.

The finance risk landscape

Your risk environment, though sprawling and complex, can be split into three primary arenas.

Consumer fraud

The problem: consumer fraud is a high-profile fraud risk facing financial services organisations – in fact, 61% of fraud losses involve the contact centre[1] – and it's been exacerbated by an increase in work-from-home practices and the use of online and over-the-phone contact centres. Fraudsters are also using more sophisticated tactics, from 'deepfake' identities to intelligent malware that adapts to its environment to evade detection.

The current solution: there are authentication processes which help to mitigate consumer fraud, such as entering a PIN or answering questions, but many of these can be circumvented by fraudsters with access to leaked or hacked data sources. And although some more advanced institutions have incorporated voice biometrics, metadata analysis and machine learning, research shows that 1.5bn minutes are wasted per year going through the authentication process[2] – so there's work left to do to create a seamless customer experience.

APP (authorised push payment) fraud cost British consumers £355.3m in the first half of 2021 alone, an increase of 71% year-on-year[3]

[1] https://smartnumbers.com/solutions/fraud-prevention/
[2] BT analysis of internal calling data
[3] //www.ukfinance.org.uk/system/files/Half-year-fraud-update-2021-FINAL.pdf

Employee fraud

The problem: ‘insider’ threats are difficult to manage and are unique in both impact and scale. The proliferation of connected devices and a burgeoning ‘work from anywhere’ culture is radically changing the way organisations assess and monitor these risks.

The current solution: current authentication methods which focus on username and password deliver poor security, sub-optimal user experience for your people, and increased support costs. Not to mention when employees forget their details, the average time they’ll spend entering or resetting passwords is 12.6 minutes per week[4]. The challenge is how to introduce robust privilege management and role-based controls, such as multi-factor authentication (MFA) and Zero Trust security models, without stopping legitimate actors such as employees and third-party contractors from doing their jobs.

79% of data is shared internally without encryption[5]

[4] https://resources.yubico.com/53ZDUYE6/at/q3tmql-974v8g-73e8p5/YubicoPonemon_2019_State_of_Password_and_Authentication_Security_Behaviors_Report.pdf?format=pdf
[5] https://www.egress.com/newsroom/data-privacy-survey-2019-uk

Cyber risk

The problem: from speaking to our customers, this is the top non-financial operational risk category in banking; most banking losses are cyber- or tech-related. Cybersecurity threats range from phishing scams and amateur scammers who use existing code to commit cybercrime to nation-state hackers. But it's not just about the threats, it's also about the quantification of those threats. For instance, under Basel III, banks are required to reserve Tier 1 capital to meet these risks – but calculating the risk of cyber exposure in monetary terms is exceptionally difficult.

The current solution: layering security solutions is key to an effective cyber risk response. However, current 'risk matrices' often use ordinal scoring (low, medium, high) rather than quantitative, statistical methods; or they focus on specific controls instead of the organisation holistically. What's more, many risk-quantification methods rely on 'expert' opinion rather than fact.

Only 36% of executives strongly agree that their current cyber risk processes enable them to securely achieve their business objectives[6]

[6] Harvard Business Review: The Necessity of Cyber Risk Quantification, 2020

Our ecosystem approach

Our approach enables financial services organisations to access an anti-fraud and security portfolio that's delivered through a single partner with a single commercial relationship. We've invested in the digital security ecosystem, including building strategic partnerships with the leading specialist vendors in fields such as authentication, biometrics, threat intelligence, analysis, and quantification.

Our ecosystem model changes the blueprint for financial services organisations looking to expand their fraud and security strategy. We can help you to manage and control fraud and risk across your whole organisation, providing access to the most up-to-date thinking and technology through a single point of access.

Protecting your customers

Our layered authentication allows you to combine real-time call validation technology with voice biometrics in the contact centre, providing a secure authentication journey that keeps customers safe and reduces handling time for agents.

Caller authentication and fraud detection

Caller authentication solutions validate inbound calls before the receiver answers, protecting the interactive voice response (IVR) from fraudster reconnaissance.

Benefits:

- analyse the caller's true calling line identification to confirm they're calling from the number they claim
- utilise machine learning to assess the behaviour of fraudsters, log unsecure numbers, and prevent future attacks
- assign calls with a risk score before the call is answered to flag potentially fraudulent calls to agents
- divert high-risk calls to specialist teams, while authenticating legitimate callers to create a frictionless caller experience for genuine customers.

Voice biometrics

This technology works in the background, using voice characteristics and patterns to identify and authenticate callers based on the natural conversations they have with agents or speech-enabled IVR. Built into your contact centre, it can streamline, protect, and personalise every interaction along the customer journey – regardless of channel or device.

Benefits:

- defend against sophisticated spoofing, deepfake, synthetic speech, and replay attacks
- compare call characteristics in real time, flagging suspect activity while continuously authenticating behaviour for ongoing security
- reduce time-consuming authentication and error handling, taking customers where they need to go quicker, and improving agent satisfaction by an average of 60%[7]
- can be layered on top of advanced call validation, environment monitoring, and anti-spoofing technologies.

Large bank delivers 4x ROI on fraud savings

Challenge: this bank was concerned about fraudsters stealing information from customer calls but were struggling to authenticate through audio monitoring only. This had a knock-on effect on customer service due to the resulting authentication times.

Result: our advanced authentication solution identifies fraudsters by determining a call's risk before it even arrives in the IVR by analysing more than 200 features and assigning a risk score for each call. This delivered a sophisticated defence that prevented multiple types of consumer fraud, including card, APP and telephony fraud.

Average call handling time fell by 20-30 seconds and the bank saw a fourfold return on investment.

[7] https://www.nuance.com/en-gb/omni-channel-customer-engagement/authentication-and-fraud-prevention/gatekeeper.html

Protecting from within

Every process, application, and area of your infrastructure relies on the protection of your core assets, including protection from your own employees. We build on our rigorous approach to risk with a comprehensive set of controls to support your Zero Trust journey. And we can layer in market-leading identity management tools without compromising productivity or user journeys.

Zero Trust

Trust no one, authenticate everything. With a Zero Trust policy, you can rely less on network perimeter security and dynamically adapt your security policies as your attack surface widens.

Benefits:

- users and their devices are authenticated, validated, authorised and monitored when accessing data, apps and networks
- provide the lowest level of access to do the job based on persona and context (such as for a third party contractor) to reduce risk of lateral movement
- gain deeper visibility on cyber readiness, resilience, efficacy, and technology to achieve Zero Trust security
- micro-segment non-enterprise systems to prevent unauthorised access to your resources.

Managed Identity

Keep on top of creating and managing accounts for users across apps and devices with a single identity and access management solution, equipped with single sign-on, multi-factor authentication, access provisioning and lifecycle management for both cloud-based and in-house apps. In short, make it easy to do the right thing and hard to do the wrong thing.

Benefits:

- increase security and lower user frustration by reducing password sprawl
- gain visibility and control over user access through modern admin controls
- centralise policies and real-time reporting to shrink identity infrastructure components, costs, and operational burden from legacy solutions
- enhance productivity by automating onboarding and offboarding
- satisfy GDPR and other regulatory requirements with adaptive multi-factor authentication security for all users.

We work with national standards bodies including NIST and the UK NCSC to improve industry knowledge and the delivery of Zero Trust.

Protecting against cyber risk

Effective cyber risk management requires more than identifying and responding to ongoing attacks. What if you could take this a step further by identifying cyber threats before they've even arisen, and objectively quantify the degree of risk?

The next layer in our ecosystem builds in our threat intelligence engine, which identifies the upcoming threats in your industry, assesses which ones are relevant to your business, and quantifies what you stand to lose or gain.

Quantify risk

Minimising cyber risk must be an informed business decision, so you need a solution that objectively quantifies risk and predicts cyber breaches using data science principles - not nebulos scales and expert opinion.

Benefits:

- monitor your cyber risk posture consistently across various technology stacks such as cloud workloads, apps, endpoints and databases, using the same scale and metrics
- quantify the breach likelihood and financial impact using business context and external threat intelligence
- build an integrated risk profile across people, processes, and technology
- maximise your existing cybersecurity investments by drawing from this data.

Threat analysis

The increasing number of endpoint devices attaching to your network gives cybercriminals more opportunities to infiltrate. By constantly monitoring activity at the endpoint, it's easier to keep your business safe.

Benefits:

- drive more accurate, intelligent and faster insights with AI-guided, cloud-based security
- manage complete endpoint security from a single console
- detect and remediate security breaches to maximise protection
- learn adversary tactics and behaviour and adapt fast to new threat approaches.

Why financial services institutions trust us

We knit together multiple layers of security to minimise the holes in your organisation's defence. But that's not the only reason financial institutions put their trust in us.

We're at the heart of the banking and financial services community

For over 50 years we've been an active member of the industry. We're a driving force within the financial services sector, working closely with the Financial Conduct Authority and financial regulators to shape policy and make sure our solutions always deliver risk and compliance outcomes that are fair, explainable and auditable.

Our extensive and experienced partner ecosystem

We offer an ecosystem of partnerships to transform the way you run your operations. Our links with leading security providers deliver flexible and compliant fraud and risk solutions. And, through leading industry partnerships, we blend the latest specialist technologies into what we offer.

We detect threats earlier to keep your business safe

Our Eagle-i cyber defence platform provides automation and orchestration across our existing managed services, allowing them to work together in a cybersecurity mesh architecture. Rather than customers needing to buy a separate service, Eagle-i underpins our existing managed services and will be offered to customers depending on the level of service that they take from us. This enables quicker detection of threats to keep your business safe.

We're continuously innovating

Our innovation teams are researching and developing highly advanced authentication solutions based on the latest developments in biometrics, identity, and cryptography. In particular, we focus on continuous authentication as a key part of the defensive arsenal.

Ecosystem thinking - one approach, leading partners, rigorous protection.

Our experts are ready to guide you through our ecosystem blueprint, helping your organisation to become resilient to fraud and cybercrime.

Visit our website to get started:
www.btireland.com/security