Author: Annie Bailey

KuppingerCole ANALYSTS

Buyer's Compass

Identity Verification

Daon

Chapter 1

The Challenge

Organizations face a range of challenges that impact both institutions and their customers, particularly in areas like compliance for Know Your Customer (KYC) and Anti-Money Laundering (AML) regulation, fraud prevention, and customer experience. These challenges don't exist individually; each impacts and complicates the others. For example, regulatory obligations and rising fraud add requirements to an onboarding experience that customers already have strong opinions about. Balancing the growing threat of fraud with the high customer demand for seamless, secure digital experiences creates a challenging environment for institutions trying to evolve their digital services.

Organizations from a multitude of industries often face the following challenges:

Stringent Requirements for Compliance

Organizations in regulated industries such as financial institutions are obligated to comply with KYC regulations. KYC processes typically include identity verification. If not modernized, KYC can be a high-effort step for both customers and institutions during onboarding, rely on manual processes, and degrade the overall customer experience. Without modern approaches, KYC requirements have prevented many industries from onboarding customers with all-digital flows, which made for choppy and lengthy onboarding experiences and increased drop-offs. Related measures are AML regulation and Customer Due Diligence (CDD).

Increasing Fraud Attempts

Any business may be targeted by fraudsters, and banking, finance, payment services, and retail are some of the most frequent targets. According to the ENISA Threat Landscape report (2024), attacks from stolen and synthetic credentials are worsening, especially due to the use of Generative AI (GenAI) and Large Language Models (LLMs)[1]. Account Takeover Fraud (ATO) and Account Opening (AO), also called New Account Fraud or Synthetic Fraud, are two potential fraud attempts that organizations face.

Reputational and Financial Loss from Fraud

There are clear monetary losses from fraud or failed compliance – criminals intend to make a profit, after all. The accompanying reputational damage from well publicized fraud incidents or failed compliance may be less tangible but have long-reaching impacts on customer trust and new business. Businesses in any industry including telecommunications, finance and banking, gambling, trading and brokerage, and crypto-currencies face significant fines for deficiencies AML or KYC controls[2].

High Customer Expectations

Users have the expectation for smooth, quick, and secure digital interactions, regardless of the challenges that organizations may face in delivering those experiences to users. While a manual, effort and time intensive, or less-than-modern user experience to onboard, authenticate, or verify transactions may not lose an organization existing customers, it certainly will miss out on new customers who are choosier about how easy it is to do business with. Given the increasing fraud attempts on new accounts and requirements such as KYC, AML, and increasingly the purchase of age-restricted goods and services require high levels of security and identity assurance but must still match customer expectations of a smooth user journey, quick onboarding processes, and the feeling of security. Crafting remote onboarding flows that meet all these needs is a challenge.

1 ENISA, 2024. *Threat Landscape 2024*.
2 *AML Intelligence (2024).*

Chapter 2

The Solution

Remote identity verification is designed to meet these requirements, moving not only the banking and financial services, but also insurance, gaming and gambling, healthcare, and telecommunications away from manual identification processes and enables them to use all-digital flows for onboarding, verification of high-value transactions, and authentication, as well as other use cases.

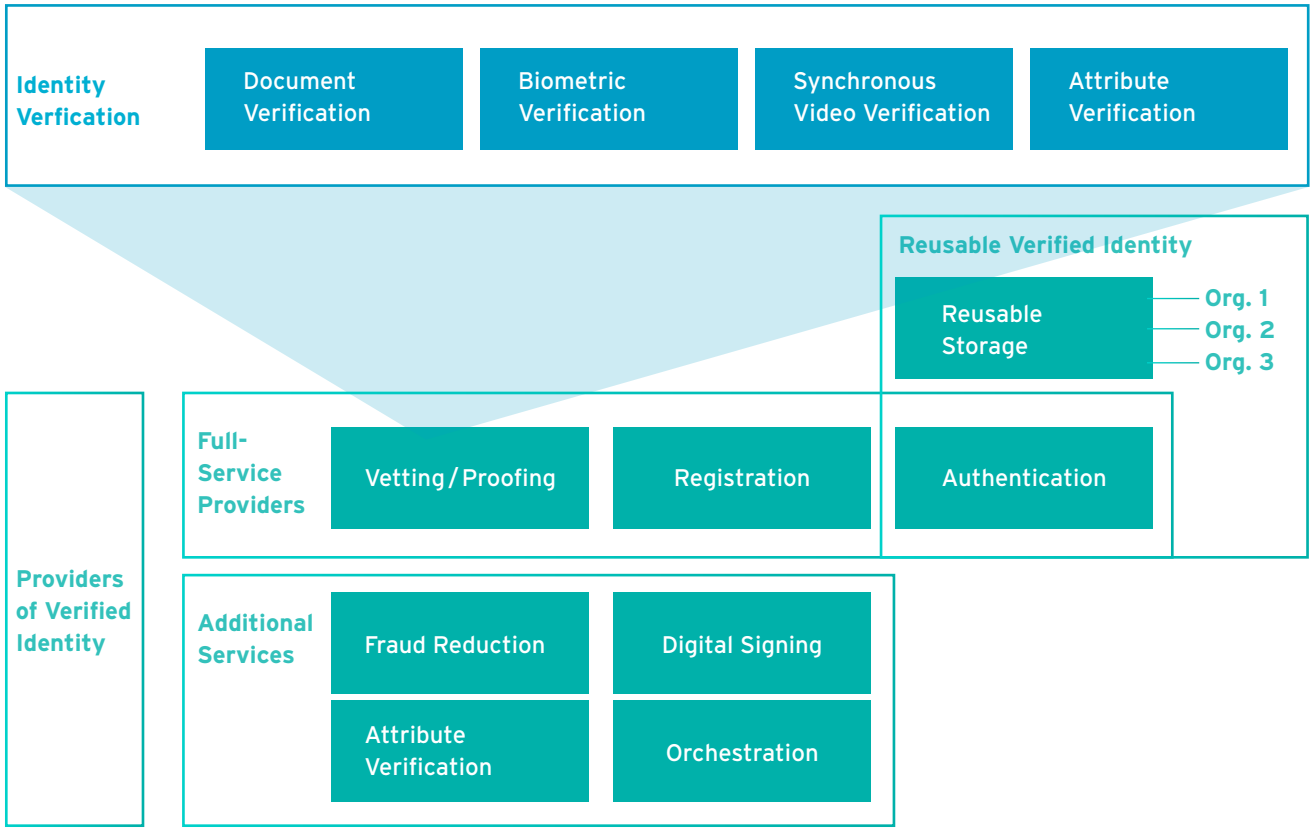
How the solution works

While other technology methods exist, most vendors remotely verify identity by guiding the user through the following steps:

- The user scans a government-issued identity document with their mobile device
- The user takes a selfie photo or video with their mobile device
- The collected information is triangulated against government repositories and with each other, fraud checks are performed, and sometimes additional checks made for Politically Exposed Persons (PEPs), and against various sanctions lists.

Other methods include verifying identity via the customer's bank, or by issuing a Verifiable Credential that holds a high level of assurance.

These methods are underpinned by a few important components:



Document Verification

Verification of government-issued and/or real-world documents. Ability to process multiple types of identity documents, from different regions, in different forms (updates, versions) and be checked for authenticity against authoritative sources such as a national registry database for eIDs and other government data. Triangulate from data collected and analyzed by optical character recognition (OCR), smartphone or hardware near-field communication (NFC) of embedded chip, and the machine-readable zone (MRZ) of identity documents to increase the confidence level that the document is valid and authentic.

Biometric Verification

Collect and process an authoritative sample for face, voice, and/or behavioral biometrics for initial verification and for optional later use in authentication. Secure storage, appropriate use of 1:1 and 1:n matching for adequate privacy protection and identification purposes.

Synchronous Video Verification

The use of a secure, synchronous video call between the user and a trained specialist to manually verify the identity. The user presents their identity document to the specialist via the video call, and the specialist makes a decision if the holder of the document matches the individual described in the document.

Attribute Verification

Collect, verify, and share standard identity attributes (name, date of birth, address, contact info, identification numbers, account numbers) and nontypical identity attributes (education credentials, employment credentials, health records, etc.).

Fraud Reduction

Ensure that the identity documents, biometrics, attributes, or context is valid, held by the individual it describes, and not falsified through a variety of methods: IP address collection, GPS, data aggregation, sanctions lists, behavioral features, keystroke analysis, and more. Confidence scoring should provide a recommendation on the identity's reliability, and may be supported with AI/ML.

Chapter 3

Top Use Cases

Know Your Customer (KYC) Measures

Many regulated industries like financial services, gaming, age-specific services, or travel and hospitality require that certain checks be made on potential customers or periodically after account creation. Remote digital identity verification solutions are able to gather the required information and verify that it is correct, valid, and untampered with.

Occasionally, it is required for a customer to recomplete a KYC when the ID documents on file expires or to address new risks. To ensure that this requirement does not negatively impact the user experience, it must be a smooth and low-effort process for the user, but still adhere to high security standards.

Passwordless Authentication

One method of passwordless authentication leverages biometrics. Unifying identity verification with authentication means that the biometric template that is collected at onboarding can be registered for authentication purposes. This adds additional strength and usability to the authenticator, since it is matched against the biometric data collected from the user's government-issued document, providing identification capacity alongside each authentication.

Elevating Trust

Existing customers will from time to time go through a higher-risk activity such as credential changes, account updates, or elevated risk signals may flag a user for closer inspection. It must be ensured that these activities are conducted by the customer, not by a malicious actor. To not penalize the customer with additional effort or time lost, additional checks must be done in a smooth process. Remote identity verification elevates trust in customers while preventing fraud by malicious actors.

Account Take Over Prevention

ATO attacks are often motivated by stealing money, or assets that can be converted into money such as points in customer loyalty programs. Preventing ATO can be managed with remote identity verification and with strong authentication, ideally supported by the information collected during the identity verification flow. High-risk scenarios such as registering or using a new device are perfectly normal for a well-intentioned customer but can also indicate a fraud attempt.

Age Assurance

Not every action requires a full identity verification, and it is critical to privacy best practice and preserving a good user experience to not over-collect information. For age-restricted activities, remote identity verification solutions can verify or estimate the user's age with various methods, ranging from identity verification, selective disclosure or age estimation with a facial image.

Chapter 4

Top Functional Selection Criteria

Document Verification

Ability to scan identity documents using OCR, MRZ, NFC, and ability to validate it against an authoritative source. Must be accompanied by checks for fraudulent spoofed documents, expiration, etc.

Biometric Verification

Use of facial analysis for 1:1 matching against the scanned identity document. Other forms may include voice.

Use of 1:n biometric searches to check watchlists of known bad actors or recent applicants looking for duplicate accounts and/or 1:N full database searches to find actors with multiple identities or multiple attempts to register.

Additional Verification Methods

Use of other verification methods, including federation of an electronic ID (eID), mobile driving license (mDL), BankID, trusted government data sources (some governments will allow financial services firms to check a face capture against a face record on file for passports, drivers license or national ID) and other financial information, attribute verification such as name or address, synchronous video verification, or leveraging Verifiable Credentials to present already verified information.

Geographical Coverage

Adequate ability to provide document verification and biometric verification in the regions where the implementor has customers.

Automation and Machine Learning (ML)

Use of automation and Machine Learning (ML) to improve the functionality and user experience, accompanied by appropriate governance of algorithms used for matching, decisioning, and fraud detection.

Privacy

Specific attention to end-user privacy in solution design, information collection, storage, and transactions.

Orchestration

The automated coordination and management of the identity verification components with enterprise systems, services, and processes. The ability to use identity verification to support onboarding, KYC, authentication, and fraud reduction processes is a large value-add which orchestration helps to facilitate.

Use Case / Capabilities Mapping

Chapter 5

Vendor Spotlight

Daon, known as the digital identity trust company, was founded in 2000 and headquartered in the USA with offices in Ireland, UK, Australia, Hong Kong, Serbia, Singapore, and Japan. Daon provides identity proofing and authentication solutions to help customers achieve identity continuity across the user identity lifecycle. Their identity verification product, xProof, combines with and supports a suite of other products covering authentication, facial and voice authentication, voice detection, and travel document validation. Daon's solutions are available as SaaS, a hosted platform, or an on-premises deployment. These services are hosted in AWS across global data centers. The pricing model is on per-transaction rates.

Daon operates on a concept of identity continuity, where the same information collected during an onboarding process / identity verification can be used to authenticate and establish more trust during later higher-risk actions across all channels of the organization, including mobile apps, web browsers, and in-person at a store / branch counter or kiosk. Identity verification is established with a customizable flow that typically includes verification of a government-issued ID, capture and matching of facial biometrics, and liveness detection. Daon's suite of identity verification and authentication products are focused on serving consumer use cases, particularly identity proofing of new customers for account opening, fulfilling KYC/AML requirements, and for verification of existing customers to elevate trust for higher-risk activities.

xProof is being used by regulated organizations, including financial services providers, to meet AML/KYC guidelines around the world. It can achieve up to NIST 800-63-3 identity assurance level (IAL) 3 with its identity verification processes, as well as being certified with UK DIATF and is awaiting ratification of Spain's CCN-STIC-140 Video Identification. While in-person presence is still the primary method for IAL3, supervised remote proofing provides a compliant alternative for scenarios where in-person presence might be impractical, provided the CSP's setup meets all NIST security and verification standards to ensure an equivalently high assurance level.

Remote capture and verification of physical documents in a variety of methods is possible. Document verification may be done for passports with or without embedded chips, eID cards, physical identity cards, physical driver's licenses, and with some preliminary support for ISO/IEC 18013-7 mDL. Documents from over 200 countries may be verified, covering North and South America, Europe, Middle East, Africa, and Asia. Video verification is achieved through a partner solution. Verification can incorporate data checks from various external data sources to verify that the document matches that issued by the governing authority. These data checks use a flexible framework that can extend to legal name, date of birth, address, phone number, identification number, proof of address, and bank account verification. More support for mDL and verifiable credentials is planned.

Biometric verification is possible for face and voice. In cases where a fingerprint reference database is available, fingerprint can be verified through a technology partnership. Biometric data can be captured in various ways, including a user's personal device using app or web browser or for in-person scenarios, a kiosk or other capture device. The capture flow can be integrated in the customer's onboarding process via SDK, API, or embeddable web app. Liveness detection is completed during the biometric capture, using methods that appear passive to the customer to protect against spoofing, masks, replay attacks, and injection attacks.

Biometric template data is encrypted before storage, are non-reversible, and may not be presented for identity verification or authentication. Storage of biometric templates is not required but can be used to enable authentication use cases. Flexible storage options are available including storage with Daon, the customer, or in some cases on the user's device. Biometric matching algorithms are certified by BixeLab for lack of bias and liveness detection is certified for ISO 30107 Presentation Attack Detection, level 2. Daon also submits its facial matching algorithms to NIST Face Recognition Vendor Test (FRVT). Algorithms are regularly improved on and distributed on a continuous update cycle. Daon has an internal committee responsible for implementing the EU AI Act in the organization, supported by an in-house lawyer, research team, and external consultation. Document processing algorithms are submitted on a regular, annual basis for external independent testing.

The flexible deployment models allow Daon to support customers that are subject to data residency regulations, with data retention policies definable per customer and per jurisdiction including GDPR and CCPA. Daon takes a data protection by design approach.

KYC/AML screening can be initiated via integrated third-party services for politically exposed persons (PEP), ultimate beneficiary owners (UBO), blacklists, sanctions, and adverse media.

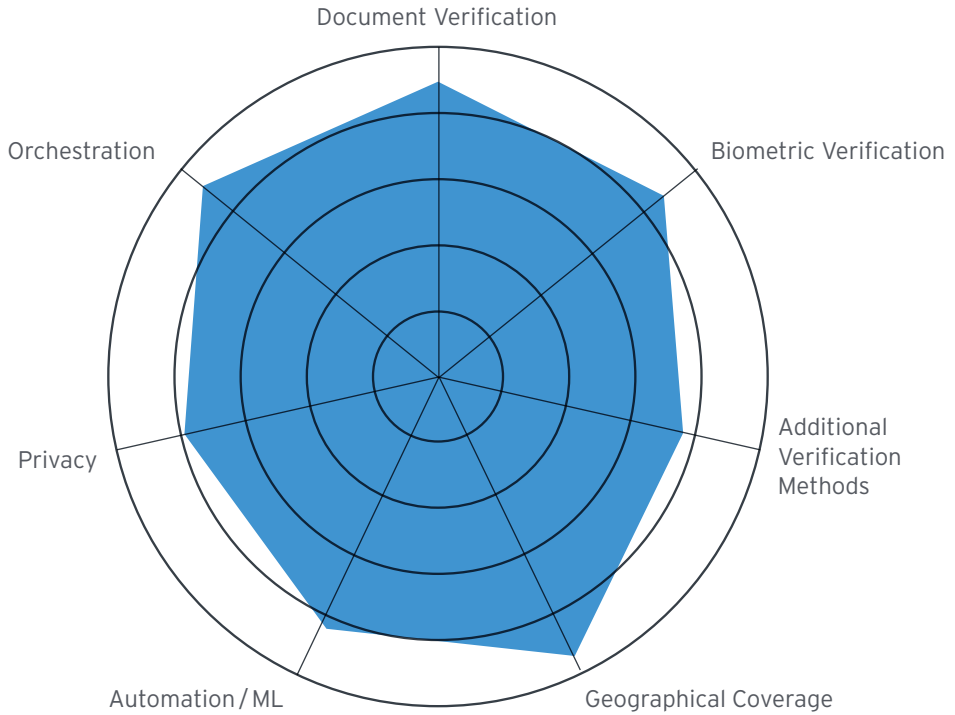
Daon provides a comprehensive workflow and orchestration as part of xProof, which enables organizations to build their own identity verification steps coordinating between product functionalities, partner and external services, and the customer's own functionalities. Functionalities are exposed via REST APIs and webhooks. Processes and activities are mapped using low-code and a graphical interface, with versioning at an activity level for each step in process and A/B testing available. Fitting with Daon's identity continuity concept, information collected during identity verification may be used to support authentication and for trust-elevation activities.

Daon's products have privileged access management control in place, API access is authenticated with support for SAML, OpenID Connect, JWT and key exchange. Multifactor authentication for administrators is required, and available with DuoSecurity mobile app, Google authenticator, Microsoft authenticator, username/password, or SSO. Federation via SAML, OIDC, and JWT is supported. Audit trails for administrative activities are kept. Daon is audited for ISO 27001 compliance and AICPA SOC 2 Type 2, HIPAA/HITECH, and WCAG 2.1 AA for accessibility.

Daon has in-house specialist customer success teams in multiple locations around the world. This is a particularly important service for customers who need the reassurance of continuing support from their vendor. Daon doesn't bring a system integrator into the project, which can add complexity and cost. Daon also has in-house research scientists, for constant improvement, adaptation, and testing of all components (algorithms and AI systems) according to standards. This knowledge is used to recommend default settings and to provide expert advice and guidance to customers for best-practice usage and to address new threats like deepfakes.

xProof is a robust identity verification solution suitable for global organizations with users being verified, onboarded, and authenticated from around the world. Its proactive stance on AI governance accompanied by early support for mDL demonstrate a commitment to innovation. The ability to use already verified data to support additional use cases such as authentication help organizations increase the value of properly implemented identity verification.

Overview of Daon xProof Capabilities



Chapter 6

Considerations

Architectural Considerations

Deployment
Identity verification solutions are generally delivered as SaaS, but some are offered as on-premises deployments. Some vendors can offer additional flexibility in deployment options, supporting running in the customer's private cloud or as a managed service.

Potential customers should consider the vendor's ability to support data residency regulations, the location of data centers used, and other aspects related to data privacy.

Integrations and interoperability
APIs are the primary means by which customer Line of Business applications, customer security infrastructure, CIAM, and third-party product or service integrations are achieved. Interoperability should be in place with international travel document regulation, eID and mDL standards, flexibility towards reusability and thus support for digital wallets and Verifiable Credentials.

Where relevant, potential customers should consider the vendor's ability to integrate across channels, such as for mobile, web kiosks and in-store devices.

Pre-deployment Considerations

Does the identity verification service enhance both the security and user experience of the transaction?
Adding an identity verification process to the onboarding process or during a transaction does not have to add much time or effort on the part of the user. But if there is a mismatch in the value of the transaction and the level of effort a user must go through to verify themselves, the user experience will suffer.

Will the identity verification service under consideration meet your expectations and/or the Service Level Agreements (SLAs) you have?
Inquire about how much latency adding callouts to the identity verification service will add. The identity verification solution being considered must be able to meet your SLAs and regulatory requirements around IT resilience, infosec and compliance with AI regulations.

What integrations are needed within the identity verification solution?
Understand what the integration model is and if you must accept the vendor's existing integrated systems/partners. It is important to know if the vendor is flexible enough to integrate with your preferred systems instead. This would allow you to leverage an existing relationship a third-party vendor that can provide value in the identity verification process.

How will you handle biometric and document algorithms?
Establish transparent communication from the get-go by clarifying that the vendor willingly shares the accuracy and performance rates of algorithms, and has the in-house expertise to explain the verification checks and settings.

Will you get independent testing of the critical components of an IDV system by a 3rd party tester?
Know what proactive steps the vendor is taking to ensure hardness and robustness of the solution, and if it is in line with your own requirements.

Chapter 6

Questions to Ask Vendors during RFPs

Do you specialize in serving specific industries?
Some vendors focus on the finance industry and/or KYC/AML compliance. Others bring KYC capabilities to other industries such as ecommerce, gaming, travel, telecommunications, and hospitality. Some provide services that work across multiple industries.

What regional coverage do you have?
Identity verification solutions often scan and compare the government-issued identity document of an individual against government repositories, supported by proprietary matching algorithms. The matching accuracy, relationship and access to government sources, access to and robustness of fraudulent document checks, and ability of the solution to match against a variety of different types of identity documents is necessary for coverage of a particular region. Biometric regional coverage includes the accuracy of facial matching across gender, ethnicity, and age, especially as they pertain to regional majorities and minorities. The solution's regional coverage must match your use case requirements.

Does your solution help achieve regulatory compliance? If so, which ones and how?
Depending on geography, authentication providers need to enable compliance with EMV 3DS2, and EU PSD2. Organizations that hold consumer or citizen personal information may be subject to various privacy regulations such as EU GDPR, Canada's PIPEDA, California's CCPA, etc. Financial institutions need to comply with AML and KYC. Health care providers are subject to HIPAA in the US. Identity verification solutions can aid their customers in complying with different regulatory frameworks.

What are the emerging user experience preference trends that you are seeing?
In most cases, identity verification is an active part of the user journey to access a service. The addition of identity verification to an onboarding or transaction flow must improve the user experience, leverage existing user habits (such as a tendency to use mobile devices, online banking, etc.), and become an intuitive but trustworthy part of the relationship between enterprise and customer. The solution must be able to accommodate the user journey that best fits your customers.

Can you use the identity verification platform to establish a trusted customer identity record that can easily be verified (authenticated) later whenever necessary?
A full-service identity verification solution enables organizations to support multiple use cases, such as reusing the verification for higher-assurance authentication. Establish with the vendor that this is possible, and that the vendor has the appropriate orchestration capabilities to make this as smooth as possible.

How easy is it to maintain multiple identity verification processes?
Identity verification should not detract from the user experience, and maintaining unique processes for globally spread customers, returning customers, and other situations to best meet the customer's needs is an important aspect to consider.

What is the scope for human adjudication of exceptions?
Understand what the implications on business processes are, such as manual review of exceptions. Clarify what ability there is to adjust thresholds by user group or use case in live environments.

How will you monitor insights in operational environments?
Understand how you can leverage insights on changes in completion rates and what variables this can be measured by, such as rates by process step or by browser type for different user types.

Recommendations

Identity verification is an important addition to onboarding, authentication and many transactions while fulfilling regulatory compliance. For many industries and for regulated goods, identity verification is key to providing digital and remote flows. And identity verification remains a key piece to reducing fraud. Identity verification provides a unique combination of enabling digital interaction with higher security.

Related Research

Leadership Compass

- Providers of Verified Identity - 80919
- Reusable Verified Identity - 80803
- Fraud Reduction Intelligence Platforms - 80488

Market Compass

- Providers of Verified Identity - 80521
- Decentralized Identity - 80064

Buyer´s Compass
Providers of Verified Identity - 80792

Executive View

- 1Kosmos - 79064
- HID Global Fraud Prevention Offering - 81104
- Signicat - 72537

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

For further information, please contact clients@kuppingercole.com.

KUPPINGERCOLE ANALYSTS AG
Wilhelmstraße 20 – 22
65185 Wiesbaden | GERMANY
P: +49 | 211 - 23 70 77 - 0
F: +49 | 211 - 23 70 77 - 11
E: clients@kuppingercole.com.
KUPPINGERCOLE.COM