Author: Alejandro Leal

kuppingercole ANALYSTS

Buyer's Compass

Passwordless Authentication B2C

AIRLOCK®

Chapter 1 The Challenge
Chapter 2 The Solution
Chapter 3 Top Use Cases
Chapter 4 Top Functional Selection Criteria
Chapter 5 Considerations
Chapter 6 Vendor Spotlight

Chapter 1

The Challenge

Consumer authentication remains one of the most persistent pain points in digital security. Traditional password-based login systems have become a liability for both organizations and users, leading to widespread fraud, account takeover, and abandonment of online transactions. The introduction of passwordless authentication aims to eliminate these weaknesses, but adoption remains uneven across sectors.

The most common types of challenges that organizations face are:

Account Takeover (ATO)

ATO continues to be one of the highest-impact threats to consumer digital services. Attackers exploit weak or reused passwords through credential stuffing, phishing, and malware-based interception. Once in control of an account, they can commit financial theft, identity fraud, or exploit loyalty programs. Even when MFA is deployed, poorly implemented step-up mechanisms or SMS OTPs are easily bypassed.

Friction and Abandonment

Consumers expect frictionless experiences. Password resets, forgotten credentials, and failed login attempts create frustration and drive users to competitors. High abandonment rates during registration or login directly affect revenue in retail, media, and financial services. Balancing security and convenience remains a key challenge.

Fragmented Device Ecosystems

Consumers access services from multiple devices, including smartphones, tablets, browsers, and smart TVs. Implementing consistent passwordless login across all these environments requires support for diverse platforms and secure synchronization mechanisms. The lack of interoperability and standardization in some ecosystems slows down deployment.

Privacy and Data Protection

Storing biometric templates or personal identifiers centrally raises privacy concerns. Regulatory frameworks such as GDPR, CCPA, and others mandate data minimization and consent-based processing. Many organizations struggle to ensure that passwordless technologies align with privacy-by-design principles and maintain transparent data flows.

Chapter 2

The Solution

Overview

Passwordless authentication for consumers replaces passwords with cryptographic credentials or biometrics bound to user devices, offering stronger security and a smoother experience. The technology leverages standards such as FIDO2, WebAuthn, and passkeys, integrating with Customer Identity and Access Management (CIAM) systems to deliver secure and convenient authentication flows.

How the solution works

Passwordless authentication establishes trust by linking a user identity to a verified device or authenticator. Public-key cryptography ensures that private keys remain securely on the device, while only non-reusable public keys are shared with the service provider. Authentication events are typically validated through device biometrics (fingerprint, face, or PIN) or system-level confirmation

Passkeys and FIDO

Passkeys are FIDO authentication credentials based on the FIDO2 and WebAuthn standards that allow users to sign in to apps and websites using the same method they use to unlock their devices, such as biometrics, a PIN, or a pattern. Each passkey is a cryptographic key pair tied to a specific user account on a website or application, removing the need for usernames, passwords, or additional authentication factors. The private key remains securely stored on the device or within a trusted cloud keychain, while the public key is shared with the service. When supported by secure cross-device synchronization, passkeys enable phishing-resistant authentication with a fast, low-friction sign-in experience.

Biometric Authentication

Many consumer applications embed native biometrics such as facial recognition, fingerprint matching, or Windows Hello, which remove the need for password entry and deliver high assurance when combined with device-bound cryptographic keys. These methods store biometric templates locally, preserving user privacy. In addition to physiological biometrics, some vendors also employ behavioral biometrics. For instance, patterns such as typing cadence, gesture dynamics, or device interaction. Unlike static biometrics, behavioral signals are continuous and passive, providing an additional layer of risk assessment or step-up evaluation.

Device Binding and Cloud Synchronization

Passwordless systems increasingly rely on secure enclave technologies and encrypted synchronization across ecosystems such as Apple iCloud Keychain or Google Password Manager. This allows consumers to use passkeys across multiple devices without re-enrollment, improving usability while maintaining security.

Integration with CIAM

Modern CIAM platforms provide the orchestration, analytics, and policy frameworks needed to deliver passwordless journeys. They handle registration, consent, risk assessment, and recovery processes, ensuring compliance and consistent experience across multiple channels.

Chapter 3

Top Use Cases

Seamless Account Login and Registration

Consumers can register and sign in with passkeys or device biometrics instead of passwords. This improves conversion rates, reduces login failures, and minimizes password reset costs.

Reducing ATO Fraud

By replacing reusable credentials with cryptographic keys, passwordless solutions close the door on phishing and credential stuffing, dramatically reducing ATO incidents.

Regulatory and Privacy Compliance

Passwordless solutions help organizations meet privacy-by-design requirements by storing biometric data locally and limiting exposure of personal identifiers, supporting compliance with GDPR, CCPA, and PSD2 strong customer authentication (SCA) mandates.

Multi-Device Continuity

Consumers often move between phone, tablet, and desktop. Passwordless systems supporting synchronized passkeys and device binding provide continuity without compromising security.

Brand Trust and User Retention

A smooth, secure login experience strengthens consumer confidence, reinforcing brand trust and reducing churn across digital channels.

Chapter 4

Top Functional Selection Criteria

Authenticators

This covers the breadth, flexibility, and interoperability of authentication options supported by the passwordless authentication solution. It examines whether traditional credentials are still supported alongside modern passwordless methods, including passkeys, mobile-based verification, and biometric authentication

Device Management

Device management capabilities are critical aspects of maintaining secure passwordless authentication. It examines capabilities provided for a device registration workflow and how this process can be customized to meet organizational or regulatory requirements.

Provisioning

This covers the user provisioning and lifecycle management capabilities of the passwordless authentication solution, assessing how it can onboard and manage users at scale.

Adaptive Risk Factors

Adaptive risk and contextual intelligence capabilities that enable dynamic, risk-based authentication decisions. It also evaluates IP reputation, geolocation, device identifiers, and behavioral signals to step up authentication when anomalies are detected.

Risk Policy

This covers the risk policy management and orchestration capabilities of the passwordless authentication solution, focusing on how administrators define, manage, and enforce adaptive access rules.

Account Recovery

Secure mechanisms to restore access when a device is lost or replaced, using secondary authenticators or verified identities without reintroducing passwords. By offering strong yet user-friendly recovery mechanisms, vendors can preserve a seamless experience while ensuring that device loss does not compromise account security.

Performance and Scalability

Evaluating performance, scalability, and reliability involves reviewing metrics like the largest customer's transaction volume, average daily login throughput, and peak authentication rates (logins per second) to understand how the platform behaves under steady load and stress scenarios.

Use Case / Capabilities Mapping

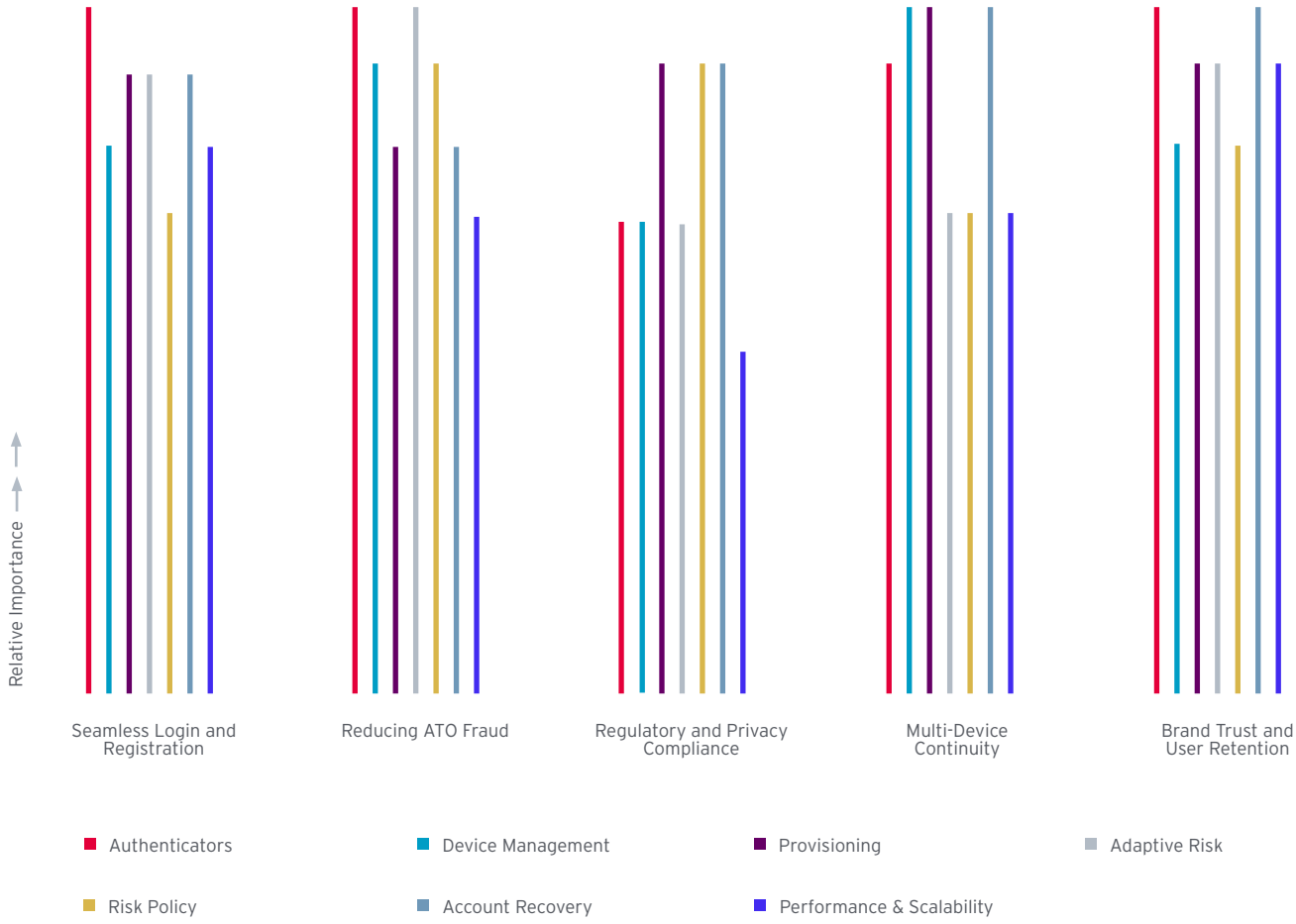


Figure 1: Use Case / Capability Mapping for Password-less Authentication B2C

Chapter 5

Considerations

Architectural considerations

Deployment

Passwordless authentication solutions are primarily delivered as cloud-hosted SaaS offerings, with most vendors emphasizing rapid deployment and scalability. Many also support hybrid or fully on-premises environments to accommodate regulated industries or legacy requirements. As organizations move toward more agile multi-cloud and hybrid strategies, vendors must provide flexible deployment models that enable gradual cloud migration while maintaining interoperability across environments. Regional hosting options, support for major IaaS providers, and transparent information about data center locations and certifications are increasingly essential to meet data sovereignty, residency, and compliance requirements across global markets.

Integrations and interoperability

APIs are the primary means by which passwordless authentication solutions interoperate with customer line of business applications, customer security infrastructure, CIAM, and third-party products or services. REST APIs are nearly ubiquitous. Other communications standards supported may include syslog and CEF for SIEM interoperability and GraphQL for contemporary applications.

Pre-deployment considerations

Organizations must evaluate their current identity stack and customer data flows. If legacy systems rely on password-centric logic, orchestration or gradual migration strategies will be required. Customer education and UX design play a major role in successful adoption.

Which applications in our portfolio still depend on password-based logic, and what level of refactoring or orchestration is required to enable passkey support?

This helps assess the scope of technical debt, identify blockers, and determine whether a phased or full migration is realistic.

How well does the passwordless solution interoperate with our existing IAM stack, including CIAM platforms, directories, risk engines, and fraud tools?

Evaluates integration complexity, ensures consistent policy enforcement, and reduces the risk of creating parallel identity silos.

What customer or user education, UX adjustments, and communication strategies are required to ensure a smooth transition to passwordless authentication?

Highlights the importance of adoption readiness, minimizing friction, and aligning the rollout with user expectations.

Questions to Ask Vendors during RFPs

Is your solution FIDO Certified, and do you also hold FIDO Biometric Certification for your authentication methods?

Certification validates that the vendor's implementation meets industry security and interoperability standards. FIDO Biometric Certification is especially important for ensuring biometric matchers meet strict anti-spoofing and liveness requirements.

How do you synchronize passkeys across user devices while maintaining privacy and security?

Passkey portability is essential for usability, but poorly designed sync introduces privacy and security risks. Understanding the mechanism helps assess whether private keys remain protected and whether the vendor relies on secure, standards-aligned OS-level infrastructure.

Where are user credentials and metadata stored, and how do you ensure compliance with GDPR or other data protection laws?

Data residency, minimization, and lawful processing are critical for regulatory compliance. Compliance is also an opportunity to build customer trust and gain a competitive advantage in the global market. This is relevant for many European-based organizations.

What recovery mechanisms are available for lost or replaced devices?

Account recovery is a major usability and security challenge in passwordless systems. Some vendors still allow username and password recovery as an optional fallback. Therefore, evaluating recovery options ensures continuity without reintroducing weak fallback methods that compromise security.

How do you mitigate phishing, replay, or man-in-the-browser attacks?

Understanding threat-mitigation techniques shows whether the authentication model is truly phishing-resistant and resilient against modern attack vectors, not just passwordless in name.

Can your solution integrate natively with our existing CIAM or CRM platform?

Smooth integration reduces deployment effort and ensures the passwordless experience extends consistently across all digital touchpoints. Native support also minimizes custom code and accelerates time to value.

What analytics and reporting capabilities are available to monitor authentication success and fraud events?

Visibility into authentication behavior and anomalies is essential for detecting fraud, optimizing user experience, and meeting audit or compliance requirements. Strong analytics differentiate mature platforms from basic toolkits.

How do you price the solution — per user, per transaction, or via API calls?

Pricing models significantly affect scalability and TCO. Understanding the model helps anticipate cost growth and align it with expected usage patterns.

What roadmap developments are planned regarding passkey interoperability or wallet integration?

Future readiness matters. Roadmap transparency shows whether the vendor is aligned with emerging standards, digital identity wallets, and cross-platform interoperability that will shape next-generation authentication.

Recommendations

Passwordless authentication has matured into a viable mainstream approach for consumer digital access. KuppingerCole Analysts recommends that organizations handling consumer identities, including banks, retailers, telecoms, and media providers, adopt passwordless technologies to improve both security and experience. A phased rollout beginning with high-risk or high-value users can reduce risk while validating usability. Integration with CIAM and fraud detection systems ensures contextual risk evaluation and compliance with regional privacy regulations. Passwordless solutions should be treated as strategic enablers of trust, customer retention, and digital resilience, not merely as technical replacements for passwords.

Chapter 6

Vendor Spotlight

Airlock

Ergon Informatik AG was founded in 1984 in Zurich, Switzerland, where it remains headquartered today. The company is a Swiss software house specializing in digitalization, security, and bespoke enterprise solutions. Its security product line, Airlock, was launched in 2002 and has since evolved into a closely integrated platform combining identity and access management (IAM) with web application and API protection (WAAP). Airlock IAM is the identity-facing component. It is positioned primarily as a Customer IAM (CIAM) platform, designed to scale to large consumer-facing populations. Airlock Gateway and Airlock Microgateway - a cloudnative WAAP - cover application and API security. Both product lines are sold independently, but their combination creates a particularly strong position for identity-based end-to-end API.

Airlock IAM delivers authentication, Single Sign-On (SSO), federation via OAuth 2.0, OpenID Connect (OIDC), Security Assertion Markup Language (SAML), adaptive authentication, transaction approval, user self-services, multifactor authentication (MFA) and passwordless authentication. FIDO2 support is mature and broad. Airlock IAM acts as the FIDO relying party, communicates with authenticators via WebAuthn and Client to Authenticator Protocol versions 1 and 2 (CTAP1/CTAP2), and supports Universal Serial Bus (USB) security keys, Near-Field Communication (NFC) tokens, and platform authenticators including Windows Hello and mobile Operating System (OS) implementations. Passwordless and usernameless flows are available natively and can be delivered either through the standard Loginapp User Interface (UI) or via representational state transfer (REST)-based flows for native apps and single-page applications.

The company supports passkeys broadly and has customers using them at scale, including for transaction approval scenarios with hardware passkeys. However, Ergon's position is to maintain passkeys as a supported authentication tier while combining them with its own step-up two-factor authentication (2FA) offering built for high-compliance scenarios. The near-term roadmap focuses on combining the strengths of both approaches rather than treating passkeys as the terminal destination. Account recovery in passwordless deployments is handled through configurable workflow-based processes. Ergon supports high-assurance re-enrollment through integrations with identity verification providers, including document and video verification solutions. For regulated customers in Switzerland and in the European Union (EU), physical letter-based recovery mechanisms remain common, and Airlock IAM continues to support those channels.

The Airlock IAM solution offers customizable device registration workflows and supports a wide variety of devices including mobile, smartwatches, FIDO keys, and more. The focus is centered on authenticator and token management rather than deep endpoint posture assessment. The company is actively tracking the European Union (EU) Digital Identity Wallet (EUDI) initiative and views it as a potentially important mechanism for identity verification, enrollment, and account recovery. If EUDI adoption evolves as anticipated, it could provide a trusted independent authentication channel for European consumers. Ergon emphasized that Airlock IAM's workflow-based architecture allows new identity and authentication channels, including EUDI-based mechanisms, to be integrated into existing processes without requiring replacement of the underlying IAM deployment. Risk evaluation and adaptive authentication are central to the platform's security posture.

Airlock IAM acts as a policy enforcement point for customer access by combining authentication flows, authorization policies, adaptive rules, and transaction approval. Risk policy authoring supports multiple import methods including YAML Ain't Markup Language (YAML) and Graphical User Interfaces (GUI) with flow chart models. Administrators can create granular access controls using rules and logical operators, Role-Based and Attribute-Based Access Controls (RBAC/ABAC), re-authentication/timeouts by role, and workflow-based policies built in the config UI (no-code/low-code) with flow-chart visualization. Policies can be enforced across federated apps and APIs, with SSO and token translation ensuring consistent application of conditional/step-up requirements.

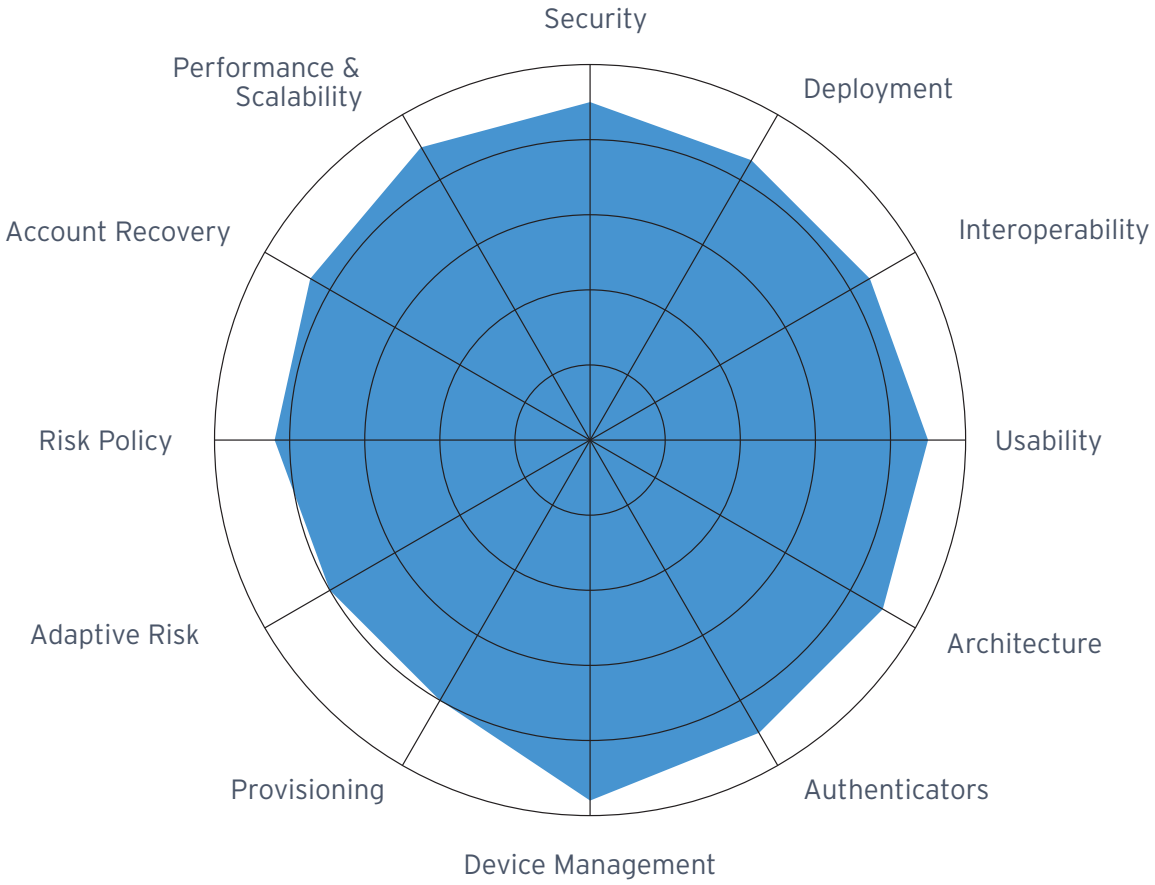
Airlock IAM evaluates Internet Protocol (IP) reputation, geolocation, velocity, time of day, device ID, device type, device fingerprint, software signature, device posture, device reputation, and session anomalies. Risk factors produce tags rather than simple scores, enabling multi-dimensional risk evaluation and step-up authentication triggers addressable via Application Programming Interfaces (APIs). The platform can incorporate external threat and contextual signals to authentication requirements based on evaluated threat context. A developing area on Ergon's roadmap is endpoint risk signals, specifically signals pulled directly from mobile app Software Development Kits (SDKs) and browser environments. The goal is to extend the context available for authentication decisions, particularly in passwordless flows where traditional password-based signals are absent.

When Airlock Gateway is deployed alongside Airlock IAM, the combined product set creates a larger signal surface, as the gateway can capture additional behavioral signals that can feed into risk-based authentication decisions. Today, IAM and Gateway are sold independently, with integration treated as an optional value-add rather than a prerequisite.

A significant recent addition is Airlock IAM as a Service (SaaS), now in productive use with live customers. The SaaS offering is hosted in Swiss datacenters, a deliberate positioning for customers with data privacy concerns tied to Swiss or EU data privacy requirements. The onboarding model has been refined to the point where a tenant can be spun up, configured with corporate branding, and made operationally ready within minutes from initial registration. Full production configuration requiring project-level effort is still available for complex deployments, but the time-to-value bar has been lowered substantially. Pricing is based on monthly active users, with scalability cost aligned to actual growth rather than projected peak load.

Ergon's partner model reflects its view of CIAM as a long-term operational relationship rather than a point-in-time deployment. A security engineering and consulting team supports partners with complex integration work, custom plugin development, and training through an Ergon Security Engineering and Consulting team (SEC). For buyers evaluating Airlock IAM, the relevant question is whether their identity requirements are complex enough to justify the depth of the platform, and whether Swiss-hosted data sovereignty, Payment Services Directive (PSD2/PSD3) compliance depth, and the ability to precisely model non-standard authentication journeys are factors that matter to their deployment context. Organizations with strong security and compliance needs such as financial institutions, insurers, and government agencies should consider Ergon Airlock. Its Swiss development and data sovereignty position resonate strongly with customers seeking stronger sovereignty assurances and regional data residency controls.

Overview of Airlock Capabilities



Related Research

- Leadership Compass: Passwordless Authentication B2C
- Buyer's Compass: Passwordless Authentication for Consumers
- Leadership Compass: Customer Identity and Access Management
- Leadership Compass: Fraud Reduction Intelligence Platforms - Finance
- Leadership Compass: Fraud Reduction Intelligence Platforms - eCommerce
- Leadership Compass: Passwordless Authentication for Enterprises

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

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