FROST & SULLIVAN

Frost Radar™: Digital Trust and eSignature Ecosystem, 2026

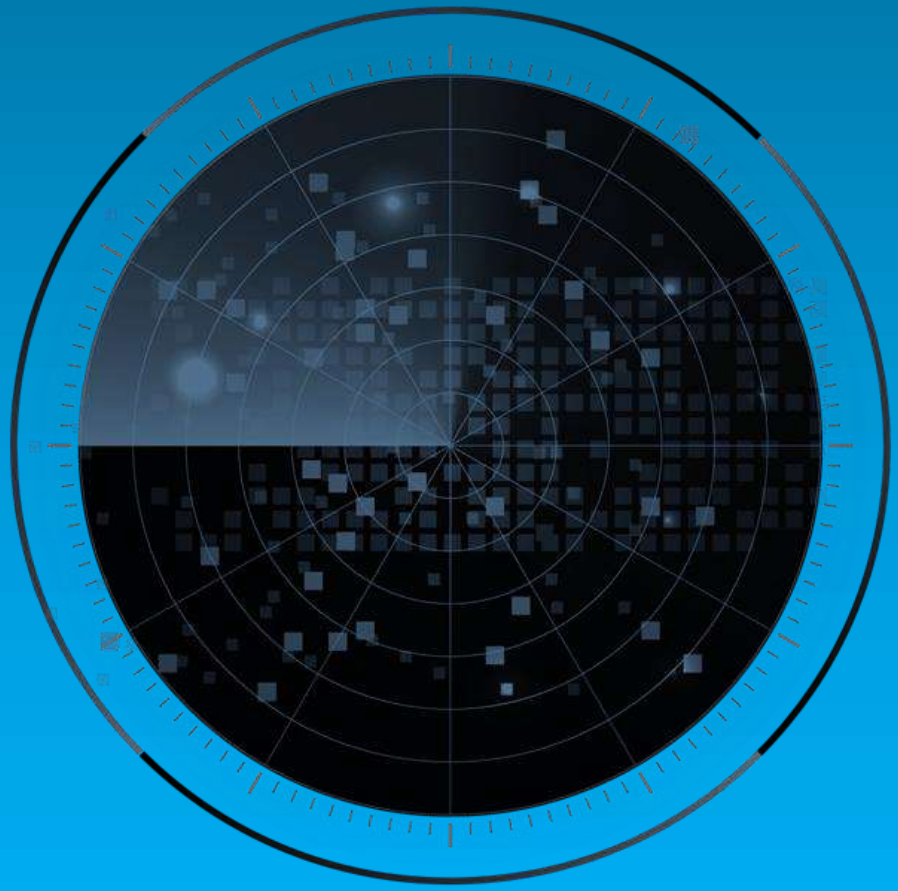
A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines

Authored by: Riana Barnard
Contributor: Alaa Saayed

KC63-70
May 2026

FROST & SULLIVAN

Strategic Imperative and Growth Environment



Strategic Imperative

- The most pressing challenge facing the digital trust and electronic signature (eSignature) ecosystem in 2026 is the fragmentation of trust across digital transactions. While eSignatures have achieved broad adoption, enterprises and public sector organizations struggle to scale trust beyond the act of signing. They must consistently verify who signs, what is being signed, when the transaction occurs, and whether it will remain legally defensible over time and across jurisdictions.
- As regulatory scrutiny intensifies, cyber threats grow more sophisticated, and artificial intelligence (AI)-generated content blurs the distinction between authentic and manipulated information, organizations must focus as much on risk mitigation as on digital transformation. Point solutions no longer suffice in an environment where repudiation risk, regulatory exposure, and AI-enabled fraud carry material financial and legal consequences.
- Market leaders navigate this inflection point by redefining their value propositions from transactional signing tools to end-to-end trust service platforms that unify signature, identity, and integrity layers into a single, compliant, and future-ready architecture. Their goal is to enable scalable, interoperable digital trust across industries and borders while embedding cryptographic assurance as a foundational control against escalating digital risk.
- The introduction of Electronic Identification, Authentication and Trust Services (eIDAS 2.0) and the European Digital Identity (EUDI) Wallet framework has significantly raised expectations around assurance levels, interoperability, and cross-border recognition. Global enterprises must reconcile European trust requirements with the Electronic Signatures in Global and National Commerce Act (ESIGN), the Uniform Electronic Transactions Act (UETA), and other regional frameworks, driving demand for solutions that can abstract regulatory complexity while maintaining legal certainty.

Strategic Imperative (continued)

- The identity layer has become the fastest-evolving component of the ecosystem. Certificate-based trust models are increasingly complemented by AI-enabled identity verification, biometric authentication, and reusable digital identity credentials. In parallel, the integrity layer has regained strategic importance as organizations focus on long-term validation and cryptographic resilience. In 2026, post-quantum cryptography (PQC) considerations are no longer confined to research roadmaps; “harvest now, decrypt later” threat models have moved from government advisories into enterprise procurement requirements for records that must remain verifiable for decades.
- As digital transactions become more automated, trust requirements are extending beyond human signers to encompass applications, devices, and software-driven processes. Machine identity, code signing, and software integrity are important complements to human-centric trust, ensuring that the systems executing and enforcing digital agreements can also be authenticated and protected against tampering across their lifecycle.
- Recent disruptive forces, including the proliferation of generative AI-driven fraud and synthetic identities, have exposed weaknesses in traditional verification and elevated the economic cost of mistrust. Consequently, competitive differentiation now depends on responsible and explainable AI deployment governed by robust controls and privacy safeguards to ensure that automation strengthens, rather than undermines, evidentiary trust. The developments have reshaped buyer priorities, shifting demand from usability alone toward assurance, resilience, and defensible trust at scale.
- The market will favor providers serving as trust anchors in complex digital ecosystems. Solutions must be modular and interoperable, supporting integration with enterprise systems and digital identity wallets. A secondary imperative is the productization of compliance: translating complex public key infrastructure (PKI) and regulatory requirements into API-driven services that let non-technical business units deploy high-assurance trust services without friction.

Strategic Imperative (continued)

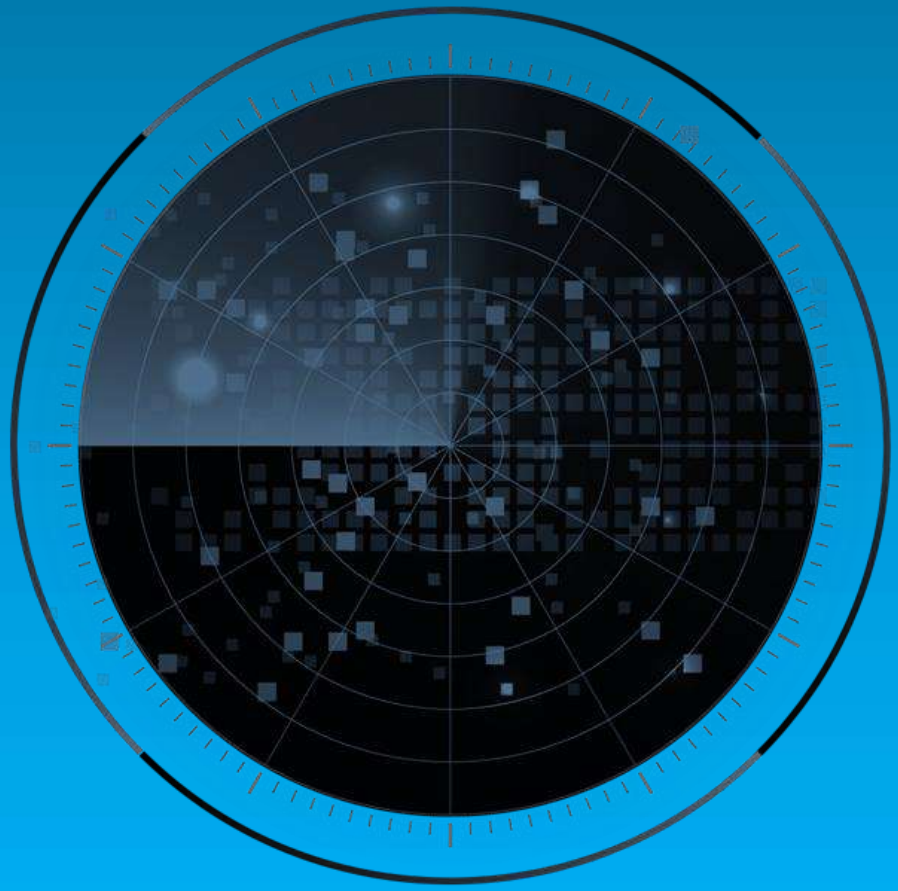
- Across the ecosystem, successful companies are distinguished by their ability to execute across technology, services, and governance simultaneously.
  - Technology leadership is defined by the integration of the three foundational trust layers into a resilient architecture that includes machine identity and operationalized PQC migration strategies.
  - From a services perspective, market leaders provide deep regulatory expertise and compliance assurance across multiple jurisdictions, lifecycle trust services spanning onboarding through long-term preservation, and enterprise-grade deployment flexibility across cloud, hybrid, and sovereign environments.
  - Governance leadership is distinguished by active participation in standards development and a transparent AI framework that prioritizes ecosystem-oriented interoperability over closed platforms.
- Ultimately, the strategic imperative is not incremental enhancement, but platform-level transformation. Providers that evolve into orchestrators of digital trust—balancing assurance, usability, and future-proof cryptographic resilience—will shape the next phase of the market and enable secure, compliant digital economies.

Growth Environment

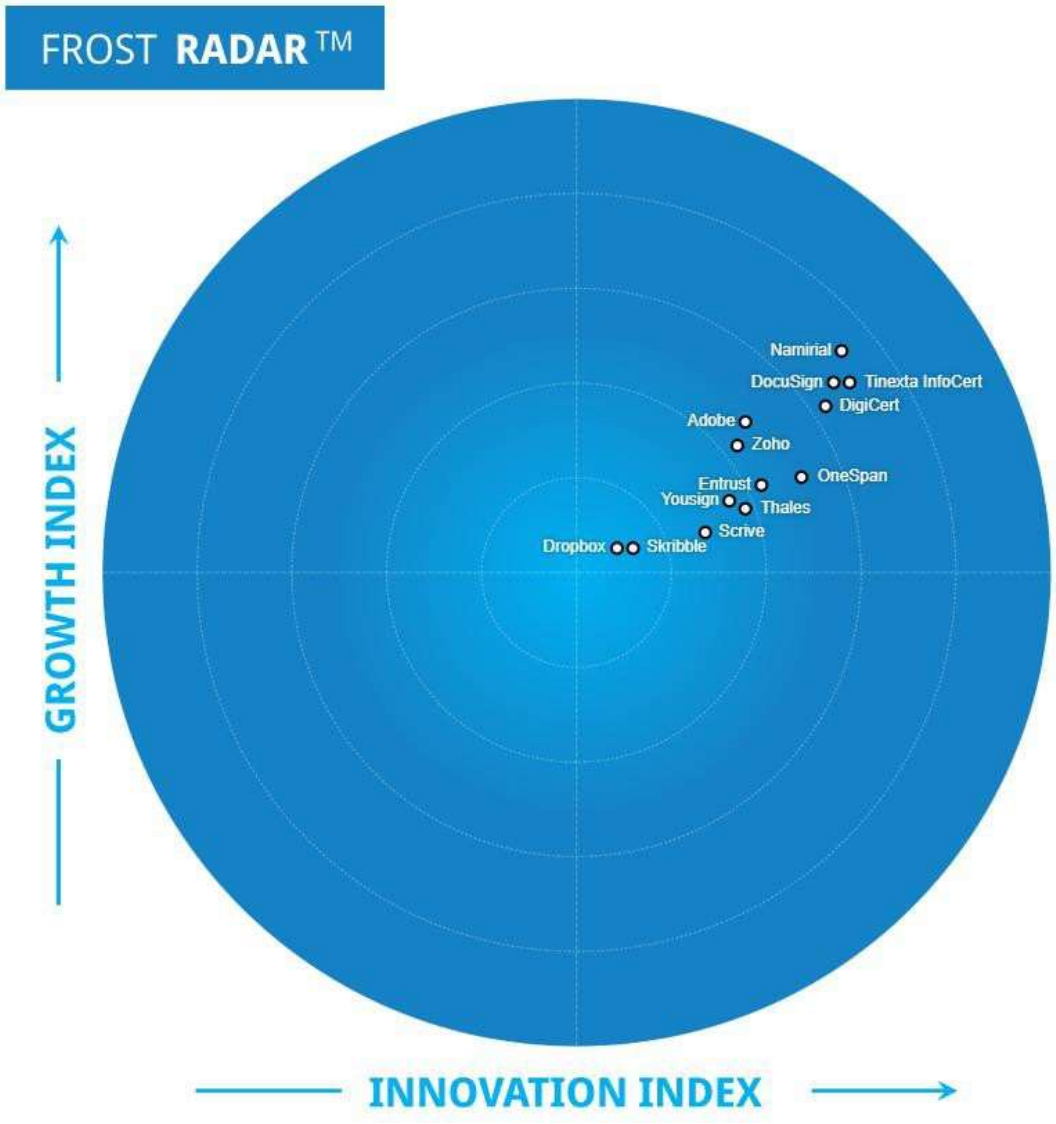
- The digital trust and eSignature ecosystem is expanding as digital transactions scale across enterprise and public sector workflows. Buyers increasingly standardize on platforms that deliver repeatable, defensible digital execution across processes, driven by pressure to increase efficiency, reduce waste, and replace paper-based handling.
- Frost & Sullivan estimates that the market will generate approximately $13.48 billion in 2026 and reach about $20.84 billion by 2031 at a compound annual growth rate of 9.1%. As eSignature becomes embedded infrastructure and competition shifts to platform depth rather than signature volume, growth is expected to moderate.
- Growth is increasingly captured through value-added trust services surrounding the signature event, including identity layer services (know your customer [KYC], biometrics, risk-based authentication, wallet credentials, and identity verification), fraud controls, and integrity/evidence services (timestamps, seals, tamper evidence, evidence packaging, long-term preservation, retention, and archiving).
- Adoption is being pulled forward by higher-assurance and regulated workflows where buyers prioritize solutions that can enforce differentiated assurance levels based on transaction risk and generate dispute-ready evidence, making premium trust layers the main lever for growth outperformance.
- Growth is tempered by commoditization pressure in low-assurance use cases, procurement-driven price scrutiny, and the friction of large-scale integrations. Persistent misconceptions about cross-jurisdiction eSignature legality increase the importance of time to value, deployment simplicity, and operational reliability.
- A Frost & Sullivan study related to this independent analysis:
  - Frost Radar™: Electronic Signature Software, 2024

FROST & SULLIVAN

Frost Radar™: Digital Trust and eSignature Ecosystem



Frost Radar™: Digital Trust and eSignature Ecosystem



Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- The digital trust and eSignature market comprises a focused subset of a broader, fragmented ecosystem. Frost & Sullivan tracks approximately 80–100 active vendors globally, including global eSignature platforms, European Qualified Trust Service Providers (QTSPs), identity-first specialists, PKI-centric security vendors, and regional or vertical-focused providers.
- Frost & Sullivan selected 13 vendors for inclusion in this Frost Radar™ analysis based on validated market traction and differentiated innovation. Selection criteria include measurable revenue growth, expanding deployments, regulatory depth, and execution against emerging requirements such as eIDAS 2.0, digital identity wallets, AI-enabled fraud mitigation, and long-term cryptographic resilience.
- The Frost Radar™ reveals distinct vendor clusters shaped by scale, regulatory exposure, and architectural ambition.
- A leadership cluster at the upper end of the Innovation and Growth indices includes vendors that align platform breadth, regulatory credibility, and commercial execution. They set the competitive benchmark, demonstrating that leadership requires architectural completeness and sustained market execution.
  - DocuSign (4.60 Innovation, 4.20 Growth) anchors this group, turning large-scale adoption into sustained growth and advancing toward Intelligent Agreement Management with analytics, AI, and agreement lifecycle orchestration.
  - DigiCert (4.55 Innovation, 4.05 Growth) drives innovation in PKI, mass-signing automation, and PQC readiness, with growth propelled by enterprise demand for cryptographic trust at scale.
  - Tinexta InfoCert (4.70 Innovation, 4.20 Growth) reinforces leadership with innovation across signature, identity, and integrity layers, backed by qualified trust infrastructure and strong execution against eIDAS-driven demand.

Frost Radar™ Competitive Environment (continued)

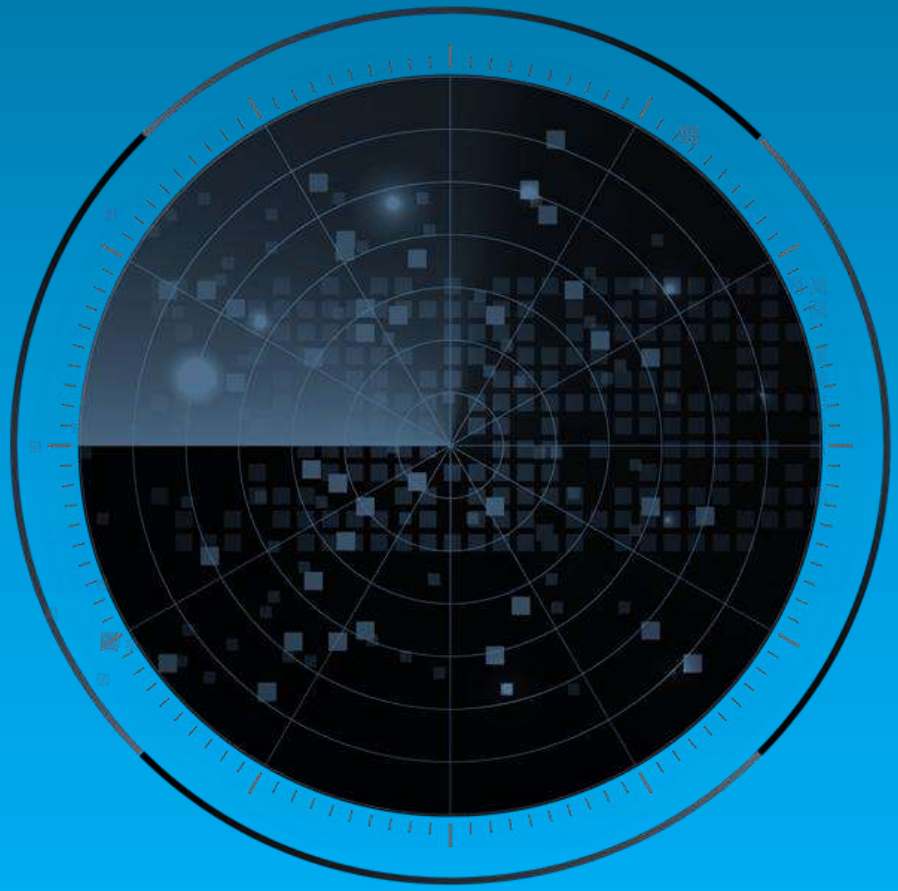
  - Namirial (4.65 Innovation, 4.40 Growth) is distinguished by robust growth as qualified and regulated digital transactions increase across European markets.
- A group of innovation-forward vendors reflects the dynamics of regulated and security-driven trust markets and demonstrates how high-assurance, cryptography-intensive trust solutions prioritize robustness, longevity, and regulatory alignment over rapid transaction volume growth.
  - Entrust (4.15 Innovation, 3.55 Growth) leverages vertically integrated PKI, hardware security models (HSMs), identity verification, and qualified signing to support complex, regulated use cases across government and large enterprises.
  - OneSpan (4.40 Innovation, 3.60 Growth) stands out with an identity-first approach, FIDO-based authentication, and immutable transaction assurance, positioning trust as an authentication-driven process.
  - Thales (4.05 Innovation, 3.40 Growth) applies cryptographic and security expertise to digital trust use cases, with growth shaped by its wider security portfolio rather than pure-play eSignature expansion.
- Two vendors demonstrate that ecosystem reach supports meaningful growth and innovation in digital trust, even without a comprehensive trust infrastructure. Adobe (4.05 Innovation, 3.95 Growth) and Zoho (4.00 Innovation, 3.80 Growth) embed signing and trust capabilities in broader application platforms. Adobe's growth stems from its document-centric installed base and investments in identity binding, document intelligence, and AI-assisted workflows, though it falls short of high-assurance or identity-centric trust leadership. Zoho follows a similar model in Zoho’s business software suite, leveraging platform integration to drive adoption and innovation without full ownership of the trust stack.

Frost Radar™ Competitive Environment (continued)

- European digital trust specialists form another cluster, translating strong regional positions into broader relevance. These vendors address a shared requirement: simplifying regulatory complexity while maintaining evidentiary strength, but without the scale or breadth of global platforms.
  - Scrive (3.80 Innovation, 3.25 Growth) stands out for innovation in cross-border qualified signatures and consolidated access to national eID schemes, with growth linked to expansion beyond its Nordic base into regulated enterprise environments.
  - Yousign (3.95 Innovation, 3.45 Growth) follows a similar path, combining steady growth with innovation focused on usability and compliance for European SMEs and mid-market organizations.
- Vendors closer to the center of the Frost Radar™ reflect focused execution models and ecosystem-driven differentiation.
  - Dropbox (3.25 Innovation, 3.15 Growth) occupies a central position, with growth and innovation driven by embedded adoption across the broader enterprise and a focus on low-friction, accessible trust.
  - Skribble (3.35 Innovation, 3.15 Growth) stands out for qualified signatures and compliance-driven use cases, though its geographic reach remains limited.
- The Frost Radar™ Innovation and Growth Index scores reinforce a central conclusion: sustainable advantage in digital trust goes to vendors that orchestrate identity, signature, and integrity as a coherent system and consistently convert that capability into measurable market growth.

FROST & SULLIVAN

Frost Radar™: Companies to Action



Adobe

INNOVATION

- Adobe addresses the digital trust and eSignature market through Acrobat Sign, delivered as part of Adobe Document Cloud. The platform enables individuals, teams, and enterprises to execute eSignatures across commercial and regulated use cases, supporting simple, advanced, and qualified eSignatures aligned with frameworks such as eIDAS and ESIGN. Acrobat Sign is embedded in Adobe's PDF-centric document environment, enabling document creation, review, signing, and management in a single lifecycle across web, desktop, and mobile platforms, with deep integration into enterprise productivity environments, such as Microsoft 365 and Teams.
- A core innovation underpinning Adobe's position in this market is its three-layer digital trust architecture, which balances signature execution, identity assurance, and document integrity. Trust controls are embedded directly into the PDF file format through Adobe's native rendering engine rather than applied externally at the workflow level. This enables cryptographic sealing, tamper detection, trusted timestamping, and long-term validation to persist in the document itself, preserving evidentiary value beyond the signing event and over extended retention periods. Identity assurance is implemented as a configurable layer, allowing Acrobat Sign to integrate with government-backed and third-party identity schemes while remaining adaptable to jurisdiction-specific requirements.
- During the past 18–24 months, Adobe expanded innovation through AI-driven document intelligence that reshapes how documents are prepared and consumed before signing. New capabilities across Document Cloud include AI-assisted document understanding and summarization; generative creation of derivative content, such as presentations; and audio-based document outputs that convert documents into personalized podcasts. Voice-based document interaction on mobile devices further reduces participation friction.

Adobe (continued)

INNOVATION

- These innovations increase document velocity and complexity upstream of signing, reinforcing the importance of embedded integrity and verifiable provenance at the document level. As documents become more dynamic, multimodal, and AI-generated, Adobe's document-centric trust model becomes more relevant.
- Adobe has invested in future-oriented trust capabilities, including exploration of post-quantum signature approaches and the introduction of richer verified identity data concepts in signing workflows. Alongside these initiatives, Adobe has delivered incremental enhancements, such as UI modernization, expanded PDF/A enforcement, improved mobile participation, and deeper collaboration integrations.

Adobe (continued)

GROWTH

- Adobe holds a solid position in the digital trust and eSignature market, underpinned by its scale in digital documents and deep enterprise penetration. Acrobat Sign sits in Adobe's Digital Media segment, which generates tens of billions of dollars in annual revenue and continues to deliver low double-digit growth, providing a stable financial foundation for continued investment in digital trust capabilities.
- Acrobat Sign benefits from Adobe's extensive installed base across commercial and regulated organizations, including broad adoption among large enterprises and public sector institutions. Adobe's document technologies are used by the vast majority of global enterprises, creating a large addressable base for incremental adoption of signing and trust services. Geographic reach is strongest in North America and Europe, with European growth increasingly influenced by regulatory momentum around eIDAS 2.0 and cross-border trust requirements.
- Growth in this market is primarily driven through Adobe's integrated go-to-market model, which combines direct enterprise sales, channel partners, and bundling in Document Cloud subscriptions targeted at business professionals and consumers. Acrobat Sign is commonly adopted as part of broader document modernization initiatives rather than as a stand-alone purchase, supporting steady expansion in existing accounts. The embedded distribution model supports durable, repeatable growth and reduces reliance on transactional deal cycles typical of point solution vendors.

Adobe (continued)

FROST PERSPECTIVE

- Adobe should keep leveraging its native PDF architecture and three-layer trust model as a key differentiator. Embedding signature, identity, and integrity controls at the document level ensures long-term evidentiary value and strengthens Adobe's position for regulated and archival use. Frost & Sullivan advises Adobe to emphasize integrity and long-term validation in its messaging, especially to drive adoption in industries with strict retention and compliance needs, such as the public sector, life sciences, and financial services.
- With eIDAS 2.0, Adobe should clarify its position against identity-first and wallet-centric providers. Its flexible identity layer is an asset, but clearer messaging on Acrobat Sign's alignment with wallet frameworks and member-state implementations would reduce buyer uncertainty. Adobe should offer explicit reference architectures and participation models to reinforce relevance in cross-border and high-assurance European use cases.
- Adobe's expanding AI in Document Cloud is a chance to further differentiate Acrobat Sign by linking document intelligence to trust and compliance. Summarization, content generation, and multimodal interaction accelerate workflows, but their impact on risk reduction and auditability should be clearer. Frost & Sullivan encourages Adobe to connect these AI features to measurable gains in accuracy, governance, and signing integrity to reinforce its innovation message.
- Adobe can extend its leadership by systematizing customer-centric innovation in regulated segments. Its scale enables co-creation around regulatory change, cryptographic resilience, and industry-specific workflows. Formalizing with clearer vertical templates, compliance blueprints, or roadmap transparency would support retention, adoption, and reinforce Adobe as a long-term digital trust partner.

DigiCert

INNOVATION

- DigiCert is a cryptographic trust infrastructure provider that serves organizations requiring legally enforceable, high-assurance digital transactions across jurisdictions, particularly in regulated sectors. DigiCert's solutions cover signature, identity, and integrity layers, binding verified identities to eSignatures and preserving long-term evidentiary integrity under frameworks such as eIDAS, ZertES, ESIGN, and UETA. Its services are embedded into enterprise environments, supporting human and automated transactions at scale.
- DigiCert ONE, a container-based, globally distributed PKI platform secured by HSMs, delivers DigiCert's core solutions. For signature, DigiCert provides certificate-backed simple, advanced, and qualified eSignatures and seals via CertCentral and Document Trust Manager. Identity is managed through centralized PKI lifecycle, credential management, and remote identity verification, using document checks, biometrics, and support for digital identity wallets aligned with European initiatives. Integrity services include timestamping, validation, electronic seals, and long-term archival that preserves cryptographic proof. Open APIs and SDKs enable integration with existing document management, transaction, and enterprise applications.
- DigiCert's PKI-native model unifies identity, signing credentials, and integrity services under a single root of trust operated by a global certificate authority. Unlike vendors focused on end-user interfaces, DigiCert prioritizes verifiability, compliance, and cryptographic assurance. Its QTSP status in multiple European jurisdictions and global infrastructure enables consistent trust policy enforcement and data residency. The integration-first design—aligned with Adobe, DocuSign, Ascertia, and the Cloud Signature Consortium—lets organizations enhance workflows with high-assurance trust services without replacement.

DigiCert (continued)

INNOVATION

- Recent innovation includes expanding enterprise-scale automation for the signature and integrity layers. DigiCert rolled out mass-signing server tools and SDKs, enabling automated electronic sealing of large document volumes via folder monitoring or application integrations. This serves high-throughput needs, such as regulated reporting and invoicing, where manual signing is impractical. Policy-driven, auditable mass signing with qualified certificates strengthens integrity and enterprise automation.
- Another innovation is enhanced identity verification and credential lifecycle visibility. DigiCert now offers browser-based identity verification, reducing reliance on mobile apps and lowering friction for users and admins. These workflows tightly integrate with certificate issuance and lifecycle management, providing real-time visibility into identity status, issuance, revocation, and renewal. This improves governance and compliance, especially for organizations under multiple regulatory regimes.
- DigiCert is investing in cryptographic agility and readiness for new trust frameworks. The roadmap includes PQC, expanded support for European Digital Identity wallets, and interoperability with evolving ecosystems. By advancing governance for cryptographic assets and aligning signing and identity services with future requirements, DigiCert enables customers to adopt new standards without rearchitecting infrastructure.
- DigiCert also delivers steady incremental enhancements: counter-signing workflows for sequential approvals, desktop signing clients for macOS and Windows (including offline use), XML signing for high-volume machine-to-machine transactions, improved audit reporting, and enhanced long-term validation. These updates broaden functionality and compliance support while keeping the core platform unified.

DigiCert (continued)

GROWTH

- DigiCert occupies a distinct position as a provider of foundational trust infrastructure rather than a mass-market, workflow-centric eSignature vendor. Its scale in this market reflects a focused concentration on regulated and high-assurance use cases.
- Adoption is strongest in Europe, where regulatory frameworks mandate qualified signatures, seals, and strong identity verification, and where DigiCert operates as a QTSP for financial institutions, government bodies, and other compliance-driven organizations. The customer base extends into North America and Asia-Pacific, supported by a geo-distributed PKI footprint that addresses data sovereignty and cross-border trust requirements.
- Go-to-market execution combines direct enterprise sales with ecosystem-driven distribution through technology alliances and platform integrations. DigiCert's services are embedded into widely used document and signing environments through partnerships with Adobe, DocuSign, and members of the Cloud Signature Consortium, while also supporting hybrid and on-premises deployments for customers with specific regulatory or operational constraints.
- Growth is increasingly driven by customers moving beyond basic eSignatures to integrated digital trust architectures that combine identity verification, signing, and integrity controls. Regulatory pressure, heightened awareness of AI-enabled fraud, and early planning for PQC are contributing to greater demand across existing accounts and new locations, positioning DigiCert for continued momentum.

DigiCert (continued)

FROST PERSPECTIVE

- DigiCert's PKI-native trust platform stands out as enterprises shift to unified digital trust architectures, moving beyond e-signature tools. Customers increasingly require a single, auditable trust backbone across identity, signing, and integrity. Frost & Sullivan notes that DigiCert has an opportunity to further support adoption by packaging its trust capabilities in ways that simplify deployment and scaling for large organizations.
- Early alignment with eIDAS 2.0, qualified trust services, EU Digital Identity wallets, and post-quantum cryptography positions DigiCert as a long-term partner. To translate this readiness into near-term impact, DigiCert can further operationalize its roadmap through concrete deliverables, including phased post-quantum migration tooling, wallet-enabled signing patterns, and clearer transition timelines to support adoption.
- While DigiCert's integration-first approach reduces friction in established ecosystems, adoption outside its regulated core has historically been perceived as more complex, reflecting the inherent demands of PKI-centric trust architectures. Recent automation improvements, including web-based enrolment, faster issuance for nonregulated use cases, and simplified signing experiences, help lower entry barriers; however, translating cryptographic assurance into measurable business value remains an opportunity. Frost & Sullivan encourages continued focus on articulating use-case-driven value and quantifiable outcomes to support expansion beyond Europe and highly regulated segments, while preserving the assurance and governance that differentiate DigiCert.

DocuSign

INNOVATION

- DocuSign delivers a full-stack digital trust and agreement platform that unifies its core eSignature service with adjacent modules across the agreement lifecycle. Its platform features eSignature for individuals and teams, Agreement Preparation and Agreement Desk for document configuration, Navigator for visibility and lifecycle control, Maestro for automation of multiparty workflows, and robust contract analytics and lifecycle management, enhanced by DocuSign's May 2024 acquisition of Lexion. The DocuSign App Center extends the platform with prebuilt integrations into enterprise and line-of-business applications, such as Salesforce, HubSpot, and ServiceNow, reinforcing its role as an extensible platform beyond stand-alone signing.
- Trust services include DocuSign Identify, supporting assurance from email/SMS access codes to government-issued ID and biometric liveness checks, plus integrity controls, such as PKI-based seals, qualified timestamping, and archiving. DocuSign Notary delivers remote notarization for US RON jurisdictions, while high-assurance European needs use Qualified Electronic Signatures (QES) under eIDAS. The API-first, embeddable stack supports Simple Electronic Signatures (SES), Advanced Electronic Signatures (AES), and QES across web/mobile, and is designed for cross-jurisdictional compliance in regulated verticals.
- Differentiation flows from integrated signature, identity, and integrity layers, not separate trust components. The architecture is identity-aware and automation-ready, enabling programmatic trust controls throughout the agreement lifecycle while preserving evidentiary consistency and auditability.
- Embedded AI automates tagging, data extraction, and summarization, and enables natural language queries of agreement repositories. With Lexion, users identify contract terms conversationally, shifting value from execution to agreement intelligence.

DocuSign (continued)

INNOVATION

- Alignment with global legal frameworks (eIDAS, ESIGN, and UETA), adherence to security and trust standards, and a focus on crypto-agility reinforce DocuSign as digital trust infrastructure rather than just an eSignature utility.
- Since 2024, DocuSign has executed on this platform vision. Intelligent Agreement Management formalized the shift from signature-centric to agreement orchestration, while the Lexion acquisition deepened contract analytics and AI insights.
- Identity innovation introduced the DocuSign Identity Wallet, letting repeat signers reuse verified attributes to reduce friction while maintaining assurance, supported by risk-based verification via partners. Integrity advanced with Notary On-Demand for US notarizations and ongoing QES investment for European needs.
- DocuSign has rolled out AI enhancements—summarization, clause extraction, intelligent assistance, and conversational Q&A—supported by partnerships to incorporate advanced generative models into workflows. Preparatory work for European Digital Identity Wallet alignment, plus continued advances in performance, scalability, governance, accessibility, auditability, and cryptographic readiness, shows a focus on enterprise operability and long-term trust resilience.

DocuSign (continued)

GROWTH

- DocuSign is achieving steady, durable growth while shifting from an eSignature utility to an Intelligent Agreement Management (IAM) platform. In fiscal year 2026, the company delivered high-single-digit revenue growth while maintaining strong profitability and cost discipline. Quarterly billings exceeded $1 billion for the first time in Q4, supported by bookings momentum, renewal timing, and foreign exchange benefits, while continued enterprise traction underscored its position in a maturing market.
- IAM now drives growth, accounting for a larger percentage of annual recurring revenue, with higher retention in early cohorts. Customers are increasingly adopting agreement orchestration, analytics, and reusable trust services. Navigator, having ingested hundreds of millions of private agreements, creates a proprietary data asset that enhances AI precision and long-term differentiation.
- DocuSign maintains a strong enterprise position, with traction among large customers and regulated sectors, such as financial services and healthcare. International revenue is rising faster than US revenue, gradually improving geographic balance. Despite competition, DocuSign's audit-grade evidence, ESIGN and UETA-aligned legal framework, and broader agreement platform capabilities support its enterprise leadership.
- Go-to-market now focuses on expanding in the installed base, guiding customers from eSignature to broader IAM through maturity-based selling, direct sales, partner channels, and integrations. The App Center and API strategy embed DocuSign in core business systems, reinforcing long-term account value and enabling sustained, platform-led growth over transactional spikes.

DocuSign (continued)

FROST PERSPECTIVE

- DocuSign should leverage its scale, brand trust, and unified agreement-centric platform to reinforce its position as foundational digital trust infrastructure. The integration of signature, identity, integrity, and agreement management within IAM differentiates DocuSign from point solutions and supports enterprise standardization on fewer platforms. Regulated organizations increasingly seek consistency, auditability, and global coverage across digital transactions. To sustain its advantage, DocuSign should prioritize platform coherence, ensuring that innovations in AI, identity, and orchestration are integrated capabilities.
- DocuSign can further differentiate by deepening agreement intelligence. Ingesting hundreds of millions of agreements into Navigator and leveraging Lexion's natural language Q&A creates a proprietary data asset, sharpening AI precision and customer insight. This shifts DocuSign's value from execution enablement to decision support, risk awareness, and compliance insight—areas where competitors lack comparable datasets. DocuSign should expand these capabilities into prescriptive use cases, including obligation tracking, renewal risk, and compliance monitoring for regulated industries.
- DocuSign has an opportunity to accelerate adoption by sharpening clarity around trust models and ecosystem usage across regions. While the portfolio spans Remote Online Notarization, QES, and emerging digital identity use cases, customer understanding of when and how to deploy each assurance level can vary. DocuSign should further clarify regional workflows, packaging, and guidance, while continuing to promote the App Center and partner ecosystem to embed IAM more deeply into adjacent enterprise systems and drive expansion-led growth.

Dropbox

INNOVATION

- Dropbox Sign is a digital trust and eSignature platform enabling secure, compliant agreements for SME, mid-market, and enterprise customers across legal, financial, healthcare, real estate, and business sectors. The platform unifies signature, identity, and integrity in a single transaction flow embedded in Dropbox. It supports SES, AES, and QES, combining authentication, identity verification, auditability, cryptographic sealing, and long-term evidence retention. Its API-first, modular design lets organizations embed signing and trust services into document-centric workflows, removing the need for a stand-alone system.
- Dropbox Sign combines high usability with increasingly advanced trust controls, leveraging Dropbox's scale alongside HelloSign's legacy simplicity. Signing is positioned as a secure transaction anchored in verified identity and document integrity, while rapid deployment, minimal configuration, and intuitive UX continue to drive adoption. Support for SES, AES, and QES under ESIGN, UETA, and eIDAS is complemented by partnerships with QTSPs, enabling regional compliance without complex, bespoke implementations. This balance allows Dropbox Sign to serve low-friction SMB use cases and higher-assurance regulated workflows on a common platform.
- A key innovation is Dropbox eID, which extends the identity layer beyond basic authentication to reusable, regionally aligned electronic identification. Dropbox eID integrates identity verification, document checks, and liveness detection directly into the signing flow, addressing regulatory and fraud prevention requirements without introducing separate identity silos. This approach enhances assurance for regulated transactions, reduces repeated identity friction for end users, and aligns the platform with emerging wallet-based and reusable identity models, particularly in jurisdictions preparing for EUDI-driven frameworks.

Dropbox (continued)

INNOVATION

- Another advancement is AI-assisted agreement workflows, enabled by deeper integration with Dropbox Dash and AI-native services. AI supports contract search, content discovery, data extraction, and early fraud signal detection across the agreement lifecycle. AI improves speed, accuracy, and visibility in high-volume environments, reducing manual effort while maintaining trust and auditability. This aligns AI adoption with efficiency and compliance, not just automation.
- Crypto-agility and long-term integrity readiness address regulatory durability and future cryptographic risk. Dropbox Sign has invested in algorithm flexibility, enhanced key management, and integrity controls to preserve evidentiary value over extended retention periods. These measures support cross-jurisdictional compliance and prepare for PQC, strengthening credibility for agreements that must remain verifiable in the long term.
- Dropbox Sign has also delivered incremental enhancements, including a mobile-first Form View experience, an expanded template gallery for HR and legal workflows, multidomain API support for large enterprises, hybrid fax integration for legacy-dependent industries, improved notifications and analytics, and the inclusion of Advanced Signature Details across paid plans. The updates demonstrate sustained product investment while reinforcing accessibility and speed.
- Innovation at Dropbox Sign includes strategic pricing, such as adding advanced compliance details to standard plans, to lower barriers to higher-assurance use. Coupled with a “Virtual First” model and strong customer feedback loops, this aligns product evolution with real-world usage, expanding trust capabilities without sacrificing simplicity.

Dropbox (continued)

GROWTH

- Dropbox Sign demonstrates steady, ecosystem-driven growth in the digital trust and eSignature market, supported by broad adoption and expansion into higher-assurance use cases. Growth is fueled by deeper penetration of trust capabilities in the Dropbox installed base, not by aggressive displacement of incumbent enterprise vendors.
- The customer base is strongest in North America, with traction in Europe as regulatory frameworks, such as eIDAS, elevate demand for identity-bound, auditable signatures. Growth in international markets is reinforced by local compliance enablement, including support for regional regimes, such as Mexico's NOM-151. SMB and mid-market organizations account for most users, while enterprise adoption is rising through API-led implementations in legal, financial services, healthcare, and real estate, where customers consolidate signature, identity, and integrity services in existing document environments.
- Go-to-market execution blends product-led adoption, developer-centric engagement, and ecosystem partnerships. Embedding Dropbox Sign in the Dropbox platform supports a land-and-expand motion, enabling customers to start with low-friction signing and scale to higher-assurance workflows without rearchitecting processes. Packaging and pricing decisions, including adding advanced signature and compliance details to standard plans, have lowered barriers to higher trust and supported retention. Growth reflects disciplined expansion aligned with regulatory and security expectations rather than short-term volume capture.

Dropbox (continued)

FROST PERSPECTIVE

- Frost & Sullivan suggests that Dropbox Sign leverage its core strength in digital trust through low-friction document workflows. Combining SES, AES, and QES with embedded identity verification and integrity controls inside Dropbox would reduce adoption barriers while meeting regulatory and audit demands. As trust becomes a baseline industry requirement, Dropbox Sign must extend higher-assurance features into default workflows so that stronger identity and integrity controls scale without sacrificing usability.
- Dropbox Sign can strengthen its position by sharpening its enterprise and regulated use case messaging. Despite expanded support for higher-assurance transactions, market perception is still shaped by its SMB heritage, while enterprise buyers now seek consolidated trust platforms. Dropbox Sign should more explicitly link investments in identity, AI, and crypto-agility to compliance durability, fraud reduction, and resilience in finance, healthcare, and legal sectors.
- The vendor should systematize its AI investments around trust and governance, not just productivity. AI-driven document search, data extraction, and fraud signal detection address complex agreement lifecycles at scale. The company should package these tools into trust-centric use cases, showing how AI strengthens assurance, oversight, and decision-making in regulated environments.
- Dropbox Sign should deepen customer alignment by formalizing how feedback and usage insights drive product evolution. Including advanced signature and compliance features in standard plans shows responsiveness and eases adoption of higher trust levels. Extending this through clearer roadmap communication, co-creation with regulated customers, and vertical templates would boost retention and strengthen Dropbox Sign's position as an accessible, credible digital trust provider.

Entrust

INNOVATION

- Entrust acts as an end-to-end provider across signature, identity, and integrity layers, focusing on regulated transactions. The company serves governments, financial institutions, and large enterprises needing legally enforceable signatures, high-assurance identity, and long-term cryptographic integrity in a single auditable framework. Entrust consolidates trust services; prioritizes architectural depth, regulatory alignment, and operational scale; and treats signing as an identity-driven workflow.
- Its portfolio provides SES, AES, QES, and (Qualified) eSeals via Signhost and its Digital Signing Infrastructure, supporting eIDAS 2.0, ESIGN, UETA, electronic seals, and long-term validation. Workflow Studio tightly unifies these functions, enabling identity-verified signing in a seamless flow and reducing the need for custom integrations in regulated scenarios. The identity layer delivers remote proofing, biometric and liveness checks, and lifecycle management, all orchestrated by the no-code Workflow Studio, now supporting advanced orchestration, testing, and configuration across onboarding and signing journeys. The integrity layer leverages Entrust's PKI, certificate authorities, nShield HSMs, timestamping, and key management. Signhost and Entrust's identity verification capabilities are cloud-delivered, while the broader portfolio supports cloud, hybrid, and on-premises deployment patterns.
- Entrust's ownership of the cryptographic roots of trust differentiates its platform. By developing and operating its own PKI engines and certified HSMs, Entrust controls key lifecycles, assurance, and compliance. Vertical integration enables high-assurance use cases and scales from enterprise to national programs. Advances in crypto-agile PKI and PQC-ready nShield HSMs allow cryptographic modernization in existing infrastructures. Entrust's standards participation and ecosystem integration reinforce its platform approach.

Entrust (continued)

INNOVATION

- Entrust features Onfido's AI-based identity verification, using machine learning models trained on millions of checks, to enhance proofing with advanced document verification, facial biometrics, and liveness detection. These features embed into signing workflows, strengthening fraud detection in high-risk scenarios and removing the need to combine separate identity vendors with signing platforms.
- The Document Fraud Engine addresses generative AI, deepfakes, and synthetic identities by ingesting global fraud signals and adapting detection models. The engine embeds fraud intelligence into identity verification and signing, enabling Entrust to counter emerging manipulation in live workflows rather than treating fraud prevention as a downstream control.
- Entrust also improves usability and workflow completeness in regulated signing scenarios. Recent enhancements include signer delegation, contact management, drag-and-drop form fields, expanded API and SDK features, and a redesigned mobile signing experience. These upgrades reduce friction for users and integrators while preserving assurance for AES and QES.
- Entrust's innovation includes deployment flexibility and regulatory readiness. New cloud regions and alignment with regional hosting support data residency and sovereignty. The platform prepares for the European Digital Identity Wallet across signing, identity verification, and IAM integration. Modular packaging lets customers adopt identity, signing, and integrity services incrementally, expanding assurance as regulatory needs evolve.
- Entrust's innovation aligns with market shifts toward AI-driven fraud, continuous identity assurance, PQC, and wallet-based digital identity. Recent product execution operationalizes these trends in production-grade, regulated trust infrastructures.

Entrust (continued)

GROWTH

- Entrust employs approximately 3,100–3,200 people and serves customers in more than 150 countries, reflecting the organizational depth and global reach required to support large enterprise and regulated market deployments. The company serves a global customer base across North America, Europe, Asia-Pacific, and other regions, with strong penetration in regulated sectors, such as government, financial services, healthcare, and critical infrastructure.
- Its ability to combine signature, identity, and integrity capabilities into a single portfolio differentiates it from vendors focused on narrower segments. Recent growth has been supported by demand for high-assurance identity verification and compliance-driven digital transactions, with the identity verification business emerging as one of the fastest-growing contributors following the Onfido integration.
- Entrust's go-to-market strategy blends direct enterprise sales with a broad ecosystem of channel partners, system integrators, and technology alliances, enabling access to complex, compliance-heavy buying environments. The company increasingly emphasizes platform embedding through APIs and OEM relationships, supporting use cases in digital government, financial services, and emerging digital ecosystems.
- Geographic expansion through new cloud regions and localized deployments has supported customer acquisition in markets with stringent sovereignty requirements. Diversified regional and vertical exposure allows Entrust to balance growth across mature and emerging markets.

Entrust (continued)

FROST PERSPECTIVE

- Frost & Sullivan recommends that Entrust leverage its end-to-end control of the digital trust stack—PKI, HSMs, identity verification, qualified signing—as a core differentiator for regulated markets. As regulatory scrutiny and liability increase, buyers want to consolidate trust services and avoid loosely integrated solutions. To maximize this advantage, Entrust should craft outcome-driven narratives that clearly demonstrate how unified control reduces operational risk, streamlines audits, and cuts compliance costs across complex, multijurisdictional environments.
- Entrust's early lead in AI-driven fraud detection and PQC aligns with evolving threat models and regulatory demands. Customers need assurance that today's digital agreements will remain verifiable amid AI attacks and cryptographic shifts. Frost & Sullivan suggests that Entrust visibly productize these strengths—offering packaged assurances, readiness assessments, and roadmap-linked services—to help clients demonstrate proactive risk management.
- To boost adoption beyond large, regulated customers, Entrust should reduce perceived complexity at entry. The platform's breadth is a strength, but it can slow engagement if buyers lack clear starting points. Simplifying onboarding via clear entry use cases, default workflows, and modular packaging would guide customers from initial deployment to advanced scenarios, accelerating time to value without weakening enterprise positioning.
- Entrust should systematically leverage customer co-creation and ecosystem partnerships for growth and innovation. Formalizing collaborations with governments, financial institutions, and platform partners into repeatable programs would further strengthen differentiation and retention. Scaling co-innovation, deepening alliances, and integrating customer insights into roadmap priorities would reinforce the company's relevance as digital trust expands into new sectors and regions.

Namirial

INNOVATION

- Namirial operates a full-stack digital trust platform unifying eSignAnyWhere for signature orchestration, Namirial Sign for teams and individuals, Namirial Onboarding for regulated remote identity proofing, and integrity services (certificate lifecycle, qualified timestamping, certified communication via Namirial Certified Delivery Service, and SERCQ) as well as long-term preservation. The stack supports SES, AES, and QES to PAdES, XAdES, and CAdES standards, is API-first for embedded experiences, and is built for cross-jurisdictional compliance in regulated workflows.
- Differentiation comes from the vertical integration of signature, identity, and integrity to produce end-to-end evidence chains, with emphasis on eIDAS-aligned QTSP operations, multi-country delivery, and resilience constructs that harden availability. The architecture is identity-first and automation-ready, so trust controls are consumed programmatically while preserving auditability.
- Since 2025/26, Namirial has been integrating and harmonizing acquired capabilities toward a unified platform layer, reinforcing an infrastructure-grade posture. It advanced an EUDI-aligned Wallet Platform and, in October 2025, opened a Global Sandbox. Namirial frames it around Wallet Gateway, Wallet App, and Wallet Studio to support relying-party verification, credential issuance, and wallet provider enablement. The design targets relying-party needs in the transition to wallet-based journeys and supports hybrid flows combining wallets with national eIDs and other identity sources for multiyear coexistence. In April 2024, eSignAnyWhere introduced generative AI features (summarization and an intelligent assistant). In December 2025, Namirial announced an AI-first transformation and introduced Agentic AI Trust Services to automate high-assurance steps—fraud prediction, biometric checks, document validation, and compliance monitoring—while preserving auditability.

Namirial (continued)

INNOVATION

- A post-quantum readiness program complements the platform strategy. Namirial reports benchmarking PQC algorithms in the context of NIST standardization and describes an integration model between PQC and quantum networks for key distribution to support crypto-agility across signatures, timestamps, and archival.
- A delivery cadence focused on enterprise operability, evidence quality, and developer control strengthens large-scale programs: API lifecycle governance removed legacy REST routes (v3/v4) from feature stream releases while maintaining continuity for current enterprise integrations and recommending newer API versions for new builds and migrations. Recent enhancements include improved traceability for SigString-generated signature fields, controls to prevent actions on signed PDFs, PDF/A-2b audit-trail generation, and accessibility aligned with WCAG 2.2 AA and PDF/UA. Operability upgrades—performance for large documents, batch/group signing, higher per-envelope limits, multipart ZIP backups across storage options, and instance-wide OAuth configuration—address procurement and production requirements at scale and reduce integration overhead.
- Wallet-readiness (Gateway + Sandbox), AI-first automation in high-assurance steps, PQC preparation, and steady enterprise-grade improvements position Namirial as a pan-European, infrastructure-grade provider for organizations that prioritize legally defensible evidence chains over basic document execution.

Namirial (continued)

GROWTH

- Since 2020, Namirial has tripled revenue and more than quadrupled profitability, supported by a buy-and-build program including seven add-on acquisitions, reflecting persistent structural demand for digital trust infrastructure and the company's ability to translate regulatory developments into scalable services. Growth is recurring and programmatic, not project-based, with adoption expanding across identity verification, signature execution, and document integrity workflows, underpinned by eIDAS-aligned trust services and QES capabilities.
- As of March 2025, the company served more than 3 million users and 150,000 clients globally. Adoption spans compliance-critical sectors—financial services, healthcare, embedded finance, occupational health, and hybrid retail banking—indicating broad applicability and stable retention where evidentiary/audit requirements drive purchasing.
- Namirial operates in 92 countries and supports 27 languages, with 32 offices across Europe, Latin America, Southeast Asia, the Middle East, and Asia. Over the past decade, the company has processed more than 1 billion digital transaction workflows.
- Inorganic expansion has been selective and complementary, broadening capabilities and reach; momentum remains primarily organic. A structured growth-pipeline—systematic signal capture, prioritization, validation, and cross-functional delivery—converts demand into scaled offerings. As adoption deepens across regulated workflows and multijurisdiction enterprises, Namirial's pan-European position in high-assurance digital trust and eSignature services strengthens.

Namirial (continued)

FROST PERSPECTIVE

- Namirial's evolution into an infrastructure-grade digital trust service provider is clear. The company can keep leveraging eIDAS-aligned QTSP operations, identity-first architecture, and multicountry delivery to anchor high-assurance workflows. The Wallet Platform's public components, plus the Global Sandbox launched in October 2025, position Namirial to support wallet-based and hybrid journeys across jurisdictions as the EUDI ecosystem matures. eSignAnyWhere added generative AI in April 2024, and the AI-First Agentic AI Trust Services announced in December 2025 target automation of high-assurance steps (fraud prediction, biometrics, document validation, and compliance monitoring) while preserving auditability. Continued evidence engineering (traceability, archival, and accessibility) remains a pragmatic differentiator in regulated procurement.
- Sovereignty alone is becoming less differentiating as vendors adopt EU-hosted, localized operating models; Namirial could deepen integration gravity—out-of-the-box embeddings and low-overhead APIs. Publishing outcome metrics for agentic and wallet-enabled journeys (completion rate lift, time-to-QES reduction) would quantify high-assurance advantages. Outside Europe, certifications indicate a measured export path; prioritizing jurisdictions with compatible frameworks and accessible attribute sources could improve efficiency.
- Looking ahead, Namirial can translate post-quantum readiness into concrete crypto-agility policies—re-timestamping/re-signing playbooks, lifecycle triggers, and guidance for long-lived evidence—while maintaining disciplined integration and service continuity SLOs across geographies. Sustaining API-lifecycle clarity, migration tooling, and telemetry would reduce change management overhead and support enterprise adoption at scale.

OneSpan

INNOVATION

- OneSpan positions itself in the digital trust and eSignature market as a provider of high-assurance digital transaction infrastructure. The company focuses on regulated and risk-sensitive environments—particularly financial services, insurance, government, and large enterprises—where digital agreements must withstand regulatory scrutiny, fraud attempts, and long-term evidentiary requirements. This positioning reflects a deliberate emphasis on transactions where identity assurance, cryptographic integrity, and non-repudiation are as important as usability.
- The company's core portfolio centers on OneSpan Sign, supported by modular services for identity verification, strong authentication, transaction signing, and long-term document integrity. These capabilities span the full spectrum of eSignatures, from SES through AES and QES, and integrate identity assurance, consent capture, and auditability into a single transaction flow. OneSpan delivers these services through an API-first, low-code integration platform that enables enterprises to embed digital trust directly into core business applications while maintaining white-label control and sovereign data residency.
- Over the past two years, OneSpan's most significant innovation has been its shift to an identity-first, transaction-centric architecture. The integration of Nok Nok has embedded phishing-resistant, passwordless authentication based on FIDO2 standards directly into digital agreement workflows, reducing credential-based fraud and reliance on legacy authentication. This approach supports customer demand for stronger identity assurance without added friction, particularly as enterprises prepare for a post-passwordless era and confront increasingly sophisticated AI-driven attacks.

OneSpan (continued)

INNOVATION

- A second major innovation is the expansion of end-to-end transaction integrity and cryptographic durability through Trust Vault, underpinned by ProvenDB technology. This creates immutable, tamper-evident records that bind document content, signer identity, and transaction metadata into a single evidentiary chain. For regulated customers with long retention and audit requirements, this strengthens non-repudiation and long-term trust. OneSpan has complemented this with a roadmap focused on crypto-agility and post-quantum readiness, enabling customers to transition cryptographic algorithms as quantum-safe standards mature. This forward-looking posture differentiates OneSpan from lighter eSignature vendors and reinforces its positioning for environments where failure is not an option.
- OneSpan extended innovation to the mobile transaction layer through its acquisition of Build38 in February 2026, adding mobile application security and runtime protection to its trust stack. This expands assurance beyond the signature itself to include the device and application environment, improving outcomes for mobile-first use cases, such as digital banking, remote onboarding, and government services.
- OneSpan continues to deliver incremental enhancements across its platform, including low-code integration improvements, expanded API coverage, enhanced analytics and risk visibility, and tighter integration between authentication, signing, and audit workflows. Innovation extends beyond product features, with the roadmap aligned to regulatory and ecosystem shifts, such as eIDAS 2.0 and EUDI wallet readiness, supported by sustained R&D investment and close alignment with customer deployment patterns.

OneSpan (continued)

GROWTH

- OneSpan's growth reflects its focus on high-assurance, regulated use cases rather than volume-driven eSignature adoption. The company maintains a strong presence among global banks, insurers, wealth management firms, and government agencies, with many large financial institutions relying on its technology for transaction signing and approval workflows. The customer base reinforces OneSpan's positioning around mission-critical digital transactions rather than transactional document volume.
- The company continues to shift to a software- and subscription-led model, supported by a land-and-expand strategy enabled by low-code tooling. In practice, this expansion is often anchored in high-volume authentication deployments—particularly in retail and commercial banking—where Nok Nok-based passwordless authentication serves as the initial entry point. From there, deployments typically expand into transaction signing, approval workflows, and long-term integrity services across the same customer footprint.
- Europe remains a key growth region, driven by eIDAS 2.0, digital identity initiatives, and demand for qualified trust services. North America continues to generate demand for phishing-resistant authentication, mobile transaction security, and fraud reduction, particularly as financial institutions modernize legacy authentication and approval processes.

OneSpan (continued)

FROST PERSPECTIVE

- OneSpan's cryptographic rigor and transaction-centric architecture are clear strengths in high-assurance digital trust environments as regulated buyers prioritize measurable business outcomes, such as reduced fraud exposure, regulatory resilience, and long-term evidentiary trust, over technical sophistication alone. To accelerate adoption and strengthen positioning, OneSpan should more explicitly link its cryptographic capabilities to quantified outcomes by publishing impact metrics, compliance benchmarks, and customer-validated ROI narratives, particularly across banking, insurance, and public sector markets.
- OneSpan has assembled a differentiated digital trust stack through acquisitions and sustained R&D investment, but the overall platform story risks appearing complex to non-security-led buyers. Narrative fragmentation can slow decision-making and limit expansion beyond core accounts. To broaden appeal, OneSpan should further unify its acquired capabilities—including Nok Nok, Build38, ProvenDB, and AI-driven identity risk detection—under a cohesive digital trust narrative that bridges security and business stakeholders. In particular, the company must demonstrate that high-assurance trust does not imply high friction for line-of-business leaders responsible for customer and employee experience.
- OneSpan's identity-first security model, white-label flexibility, and API-first integration extend beyond traditional financial services workflows. As adjacent sectors, such as government services, healthcare enrollment, and complex B2B transactions, demand seamless digital experiences and strong assurance, these strengths create expansion opportunities. To sustain growth, OneSpan should leverage them to deliver vertical-specific solutions that combine signature, identity, and integrity services aligned to the trust requirements of these markets.

Scrive

INNOVATION

- Scrive is a European digital trust specialist for high-assurance, compliant digital transactions in regulated, document-intensive sectors. Its platform supports the entire trust lifecycle under frameworks such as eIDAS 2.0, unifying eSignatures, identity verification, and document integrity in one architecture. Scrive serves enterprises and software providers needing legally robust, cross-border digital agreements, while also supporting smaller organizations with managed workflows and browser-based signing.
- Scrive's modular product portfolio spans signature, identity, and integrity layers. It offers SES, AES, and QES via eSign Online, eSign GO, and eSign API, supporting both stand-alone and integrated use. Identity features include the eID Hub, connecting to multiple European national eID schemes, and ID Check, which handles document verification, biometric matching, and liveness detection for onboarding and authentication. Integrity is ensured through PKI-based mechanisms: PAdES-compliant signatures, embedded long-term validation, and qualified electronic seals, all backed by Scrive's QTSP status.
- A major recent innovation is Scrive's expansion of qualified signature capabilities into a cross-border model via QES Global. This allows high-assurance transactions in more than 60 countries without extra software or manual video identification. QES Global abstracts local qualification requirements, removing a core barrier to international digital contracting and differentiating Scrive from providers limited to single jurisdictions.

Scrive (continued)

INNOVATION

- Scrive evolved its identity layer into a centralized, scalable access point for European digital identities. The eID Hub consolidates multiple national eID schemes into one API, letting customers expand geographically without repeated integration. Recent enhancements include more schemes and biometric flows, such as BankID-based biometric checkout in Norway. This integration aligns identity verification with signature workflows, improving completion rates and readiness for European Digital Identity Wallet use cases.
- Scrive is also shifting to end-to-end agreement management by integrating Contractbook and workflow automation. The platform now supports pre- and post-signature processes: template generation, automated data extraction, lifecycle tracking, and offboarding. AI capabilities enable metadata and clause extraction from signed documents and natural language queries for agreement repositories, boosting visibility and operational follow-through for legal, HR, and commercial teams.
- Alongside major initiatives, Scrive delivers incremental innovation, including eSign API extensions, broader document coverage, faster ID Check processing, more enterprise integrations, and workflow usability improvements. The eIDAS 2.0 Milestone Tracker and enhanced compliance offerings help customers translate regulatory change into operational readiness without bespoke consulting.
- Modular packaging and transparent pricing, with “no-integration” options to lower adoption barriers, give customers control over cost and complexity. Scrive has expanded its partner ecosystem, embedding its capabilities in industry-specific platforms in real estate, automotive, and financial services. The go-to-market and packaging advances extend Scrive’s reach and enable the delivery of digital trust solutions aligned with how customers buy and operationalize compliance-driven technology.

Scrive (continued)

GROWTH

- Scrive serves more than 12,000 organizations and processes over 100 million transactions annually. The company holds a leadership position in the Nordic region and is increasingly visible in Western Europe, particularly in regulated and high-volume transaction environments.
- Recent growth has been driven primarily by enterprise customers, with strong momentum in banking, financial services, real estate, and automotive, where high-assurance identity and qualified signatures are core requirements rather than optional features. While Scrive does not match the global footprint of the largest multinational eSignature providers, it has established itself as a fast-growing regional challenger with depth in compliance-driven use cases.
- Scrive's customer base spans more than 60 countries, with core strength in the Nordics and expanding traction in Germany, the Netherlands, and adjacent European markets. Growth outside the home region has been supported by local commercial teams and by a partner ecosystem that includes software vendors, system integrators, and industry specialists embedding Scrive's capabilities into their own solutions.
- Go-to-market execution combines direct enterprise sales with partner-led and embedded distribution models, reinforced by integrations with platforms such as Salesforce, Microsoft Dynamics, and Workday. This mix allows Scrive to address large, complex deployments and lower-friction SMB use cases, supporting steady expansion without diluting its compliance-led positioning.

Scrive (continued)

FROST PERSPECTIVE

- Scrive's key asset is its high-assurance European positioning, anchored in QTSP status and tightly integrated signature, identity, and integrity services. As buyers assess digital trust platforms holistically—especially under eIDAS 2.0 and rising regulation—Scrive should emphasize identity verification, document integrity, and evidentiary value as core to its value proposition. Using specific customer outcomes would reinforce its end-to-end agreement lifecycle narrative.
- The company's Europe-first focus and deep connectivity into national eID schemes provide clear differentiation in core markets, but they also create a natural boundary to growth outside the European Union. As global digital identity regimes evolve, Scrive could extend its relevance by articulating how its architecture can accommodate non-European trust frameworks and identity sources. This would allow the company to participate more actively in cross-border and multinational use cases where European firms transact beyond the eIDAS sphere, supporting expansion without competing head-on with low-assurance global tools.
- As Scrive expands agreement management, AI automation, and compliance tools, complexity management is crucial. Broad modules and APIs attract enterprises but can create friction for SMBs and new buyers. Scrive should simplify packaging, clarify adoption paths by use case or industry, and tighten workflows to ensure that innovation delivers faster time to value.
- Contractbook adds a robust AI contract assistant, enabling agreement queries, insights, automation, and workflow triggers—signaling a shift to strategic agreement intelligence. Scrive should systematize customer feedback and co-creation to deliver advisor-class, vertical-specific features, such as contract analytics and compliance monitoring, and communicate this roadmap externally to reinforce its evolution from digital signing to intelligent agreement management.

Skribble

INNOVATION

- Skribble's innovation strategy is anchored in its three-layer digital trust stack spanning Signature, Identity, and Integrity, designed to support legally binding, high-assurance digital transactions in regulated environments. The Signature layer supports SES, AES, and QES, enabling organizations to align legal weight with transaction risk. A core technical differentiator is Skribble's native, end-to-end implementation of QES, which integrates identification, certificate issuance, and signing in a single workflow. By eliminating reliance on external trust service providers and associated surcharges, the platform significantly reduces operational complexity, with documented performance improvements showing signing processes up to 10 times faster than traditional methods and average execution times reduced from approximately 30 minutes to three minutes.
- The Identity layer integrates multiple verification methods, including video and in-person checks, and is architected to support European Digital Identity Wallets under eIDAS 2.0. This roadmap enables future signing from self-sovereign mobile identities while maintaining crypto-agility to address long-term post-quantum security risks.
- The Integrity layer ensures long-term document authenticity through per-document encryption and insert-only audit logs, with all data hosted in geo-redundant Tier IV data centers in Switzerland. This hosting model, positioned outside the scope of the US CLOUD Act, strengthens trust among organizations with stringent confidentiality and regulatory requirements.

Skribble (continued)

INNOVATION

- Recent innovations include the June 2024 release of API v2, introducing the SignatureRequest object for granular, programmatic control over multiparty workflows, automated reminders, and status callbacks, as well as the integration of AI-driven trust services for automated identity verification, anomaly detection, and fraud prevention. These capabilities contribute to significant cost efficiencies, including a documented reduction of signing-related costs by up to 90%, equating to savings of approximately CHF 34 per document. Innovation is reinforced through usability-driven design and a partner-centric model that enables ISVs to embed Skribble directly into vertical software environments.

Skribble (continued)

GROWTH

- Skribble demonstrates strong momentum in the European digital trust segment, driven by adoption in regulated and high-stakes use cases where trust, compliance, and evidentiary value outweigh price competition. As of early 2026, the company supported more than 4,000 organizations across at least 30 countries, with growth concentrated in Switzerland, Germany, and France. With a specialized workforce and total funding of $14.5 million, including a Series A round focused on strengthening its DACH and French presence, Skribble has prioritized depth of penetration over broad geographic expansion. The company competes effectively against larger, US-centric vendors in scenarios where QES and data sovereignty are decisive purchasing criteria.
- Growth is supported by a hybrid go-to-market model combining direct enterprise sales with an expanding ecosystem of resellers and software partners. Native integrations with platforms such as SAP, Salesforce, and Guidewire enable land-and-expand dynamics, allowing departments to standardize on Skribble once high-assurance signing is operationally validated. The partner-led approach has driven vertical expansion in insurance, legal, real estate, and HR.
- A notable example is the deployment at Swiss Federal Railways, which reached approximately 3,000 employees and exceeded 20,000 executed signatures, illustrating Skribble's ability to scale in complex, regulated organizations. Localized support and consistent regulatory alignment underpin a sustainable, trust-driven growth profile.

Skribble (continued)

FROST PERSPECTIVE

- Skribble should continue to leverage its native QES stack and Swiss-based hosting model as core competitive anchors—capabilities that directly address compliance, sovereignty, and trust requirements in regulated European markets. Full-stack control over identification and signing provides a more defensible value proposition than third-party-dependent alternatives, particularly as EUDI Wallets expand access to high-assurance digital identity. Frost & Sullivan encourages the company to consistently extend this integrated trust model across new workflows and partner-embedded use cases to sustain differentiation as regulatory complexity increases.
- To support longer-term growth, Skribble could address gaps across the broader document lifecycle, particularly in post-signature management and long-term archiving. Extending capabilities or partnerships into these adjacent stages would increase enterprise stickiness and reduce fragmentation for customers in legal, insurance, and public-adjacent sectors that require multiyear auditability.
- As mobile identity adoption accelerates, the company could strengthen its position by deepening its mobile experience beyond browser optimization, enabling more seamless wallet-initiated signing, and improving adoption among distributed workforces. Frost & Sullivan suggests that Skribble systematize its vertical and partner-embedded go-to-market playbooks, and formalize repeatable approaches to ISV integration and customer co-creation to accelerate expansion while reinforcing its positioning as a specialist digital trust provider.

Thales

INNOVATION

- Thales operates as a foundational digital trust infrastructure provider, positioned beneath the application layer to focus on identity and integrity rather than end-user document workflows. The infrastructure-first strategy delivers the cryptographic foundation for advanced and qualified eSignatures under eIDAS 2.0, ESIGN, and UETA. By avoiding application-level orchestration, Thales functions as a neutral trust authority underpinning application providers and QTSPs without direct competitive overlap.
- In the identity layer, the OneWelcome Identity Platform manages complex lifecycles across B2C, B2B, gig worker, and internal employee segments. It supports strong authentication and regulatory compliance while integrating with external signing workflows.
- In the integrity layer, Thales provides globally deployed PKI, HSMs, and trust services infrastructure used to secure signing keys, issue digital certificates, apply electronic seals, generate qualified timestamps, and ensure long-term non-repudiation and validation of signed transactions.
- Thales differentiates itself through a hardware-rooted assurance model, prioritizing PQC resilience and digital sovereignty. While the market is increasingly software-centric, Thales anchors trust in hardware, utilizing FIPS 140-3 and Common Criteria EAL4+ certified Luna HSMs. This creates an immutable root of trust decoupled from hyperscale cloud vulnerabilities, preserving cryptographic control across multicloud environments and limiting exposure to extraterritorial access mandates.

Thales (continued)

INNOVATION

- Innovation in 2025 and 2026 focused on future-proofing digital trust. In June 2025, Thales introduced PQC-ready HSMs supporting hybrid models, followed in October by CC-certified PQC smart cards for long-lived identities and qualified signature tokens. It also launched post-quantum secure elements protecting firmware updates and IoT device identities at scale.
- To counter systemic risks from generative AI, Thales deployed the AI Security Fabric in early 2026. This enterprise-grade runtime layer acts as an AI firewall for retrieval-augmented generation (RAG) systems, classifying sensitive data before vector database ingestion and blocking threats including prompt injection and data poisoning. To address autonomous, non-human agentic workflows, Thales launched the Authenticator Lifecycle Manager, automating passwordless credential enforcement and identity policy orchestration.
- Strategic partnerships refine the ecosystem. In October 2025, a partnership with Badge integrated biometric cryptography into OneWelcome, enabling Identity without Secrets for authentication and account recovery without stored passwords or exposed private keys. In early 2026, Thales partnered with Ubiqu to deliver certified infrastructure for the eIDAS 2.0 European Digital Identity Wallet, combining remote secure element technology with Luna HSMs to host unlimited verifiable credentials under sovereign control. This culminated in March 2026 with the launch of SafeNet Trusted Access on the Google Cloud Marketplace, accelerating the deployment of high-assurance access management globally.

Thales (continued)

GROWTH

- Thales maintains a well-established position in the digital trust ecosystem as an infrastructure provider supporting high-assurance digital transactions. With a global workforce of approximately 85,000 and more than 30,000 enterprise customers, Thales operates at substantial scale relative to infrastructure-centric peers. Growth is supported by the company's long-standing role in hardware-rooted trust, with Luna and payShield hardware security modules securing an estimated 80% of global point-of-sale transactions and protecting approximately $150 trillion in annual interbank transfers. These assets position Thales as a critical cryptographic layer underlying regulated digital trust services, including advanced and qualified eSignatures.
- The 2024 acquisition of Imperva expanded the company's data security portfolio, enhancing its ability to mitigate more than 113 billion application-layer attacks per month and reinforcing the operational resilience required for legally enforceable digital trust services.
- Geographic growth is diversified across Europe, North America, and Asia-Pacific, with expansion closely aligned to regulatory emphasis on data residency, privacy, and digital sovereignty. Frameworks such as eIDAS 2.0, NIS2, and GDPR, together with regional cloud sovereignty initiatives, continue to generate localized demand for infrastructure-level trust controls. Thales supports this expansion through a partner-led go-to-market model encompassing approximately 6,700 global partners. Overall, Thales' growth profile reflects sustained demand visibility for compliance-driven trust infrastructure, supported by regulatory complexity, high switching costs, and long infrastructure replacement cycles.

Thales (continued)

FROST PERSPECTIVE

- Thales benefits from a structural architectural advantage driven by its early deployment of PQC and remote secure element technologies, which are increasingly relevant as regulatory frameworks, such as the European Digital Identity Wallet, impose higher assurance requirements. These capabilities position Thales favorably relative to software-centric competitors that may face challenges meeting qualified trust and sovereignty expectations at scale.
- Thales' positioning as an infrastructure provider introduces a visibility constraint among non-technical line-of-business stakeholders, where application-layer vendors often retain the primary customer relationship. This dynamic may limit Thales' influence over purchasing decisions despite its central role in trust enablement. Addressing this imbalance could require tighter packaging and clearer articulation of value at the integration layer, particularly where access management and eSignature platforms converge.
- Portfolio coherence represents another consideration following the Imperva acquisition. As enterprise buyers prioritize vendor consolidation, greater convergence between the CipherTrust Data Security Platform and the OneWelcome Identity Platform could improve administrative simplicity and reinforce Thales' positioning as a unified trust infrastructure provider.
- The accelerating adoption of generative AI introduces new identity and access risks, particularly from autonomous, non-human agents. Thales' investments in AI-driven security and biometric identity technologies provide a foundation for more automated threat detection and response. The degree to which these capabilities can be operationalized and integrated across the broader portfolio will influence Thales' ability to sustain relevance as identity assurance requirements evolve.

Tinexta InfoCert

INNOVATION

- Tinexta InfoCert delivers an integrated digital trust portfolio spanning the signature, identity, and integrity layers, operating as a leading European QTSP with services deployed through cloud, on-premises, and hybrid models across Europe and selected international markets.
- At the signature layer, the company supports SES, AES, and QES through platforms including InfoCertSign, SigningHub, Proxysign, and API-based signing services, while operating as a QTSP and Certification Authority responsible for qualified certificate issuance and PKI lifecycle management. At the identity layer, digital identity and onboarding capabilities are delivered through the TOP platform, combining identity verification, KYC, biometric checks, and unattended identification to support enterprise onboarding and embedded, high-volume transactional scenarios. At the integrity layer, qualified timestamping, electronic seals, and long-term archiving preserve document integrity, authenticity, and evidentiary validity over time for enterprises, public sector organizations, regulated industries, SMEs, and individual professionals.
- Differentiation is driven by the depth of qualified infrastructure and a modular, interoperable architecture controlled end-to-end. By managing core trust primitives in-house, including qualified certificate issuance, PKI, secure devices, and compliance operations, product design remains tightly aligned with evolving regulatory frameworks, such as eIDAS 2.0. Interoperability with third-party PKI and signature providers and compliance with open standards, including Cloud Signature Consortium specifications, reduce lock-in across heterogeneous enterprise environments. This foundation is reinforced through systematic AI integration across identity verification, fraud detection, document intelligence, and user guidance, alongside support for multiple identity schemes and assurance levels in parallel.

Tinexta InfoCert (continued)

INNOVATION

- Structured R&D programs and participation in European pilot initiatives focused on digital identity wallets and trustworthy AI anchor innovation in long-term platform evolution rather than isolated feature delivery. Over the past 18–24 months, the innovation trajectory has shifted from regulatory reinforcement to automation, intelligence, and ecosystem readiness. In early 2024, compliance and usability baselines were strengthened through formal accessibility certification for signature platforms. By mid-2024, the focus moved to interoperability, with InfoCertSign updated to support Cloud Signature Consortium standards and more flexible API-based embedding using external qualified certificates.
- In the second half of 2024, identity-led innovation accelerated through the integration of European Digital Identity schemas and unattended identification workflows, culminating in real-time issuance of QES without human intervention for high-volume and embedded use cases. In 2025, innovation efforts concentrated on intelligence, convergence, and future-proofing. AI-driven assistance was embedded into signing and onboarding journeys to guide users through complex processes, improve completion rates, and reduce operational friction, while document intelligence and anti-fraud modules were enhanced with biometric analysis and deepfake detection. In parallel, a platform convergence initiative unified previously distinct signature solutions into a single ecosystem with a more consistent user experience and improved scalability.
- Workflow automation features, such as automated signature placement, were introduced and execution of the eIDAS 2.0 compliance program began, aligning identity proofing, wallet readiness, and qualified trust services with the forthcoming regulatory framework. The initiatives define an innovation roadmap in which compliance, identity, AI, and usability evolve as interdependent elements of the digital trust value proposition.

Tinexta InfoCert (continued)

GROWTH

- Tinexta InfoCert is a notable player in the European digital trust and eSignature market, holding a leadership position in Italy and steadily expanding across Europe. The company stands out for its expertise in qualified trust services. It serves more than 6,000 enterprise and public sector clients in highly regulated sectors, including financial services, healthcare, utilities, telecommunications, insurance, and government, alongside a wide base of SMEs and professionals. Its trust services reach more than 12 million users worldwide, highlighting strong enterprise adoption and substantial transactional volume.
- Beyond its Italian base, Tinexta InfoCert operates in Spain, France, the United Kingdom, and other European markets through subsidiaries and acquisitions in the Tinexta Group. Leveraging a blend of direct operations, partnerships, and international entities, it is active in at least 85 countries and continues to expand into the DACH region, Eastern Europe, Latin America, and parts of the Middle East and North Africa.
- Tinexta InfoCert's growth is driven by a hybrid go-to-market approach: direct enterprise sales for complex, regulated deployments; an eCommerce channel for SMEs and professionals; and a partner ecosystem that supports localization and industry specialization. Over the last three years, the digital trust business maintained double-digit growth, fueled by regulatory momentum from eIDAS 2.0, greater alignment between identity and anti-fraud applications, and disciplined acquisitions. The market now recognizes Tinexta InfoCert as a rapidly growing and credible alternative in regulated environments, with its prospects strengthened by ongoing international investment and portfolio expansion.

Tinexta InfoCert (continued)

FROST PERSPECTIVE

- Tinexta InfoCert leverages structural advantages—qualified trust infrastructure, regulatory expertise, and integrated signature, identity, and integrity services—to enable compliant, high-assurance transactions where evidentiary strength is paramount. Its open, standards-based architecture provides flexibility for evolving wallet models, while early execution against eIDAS 2.0 positions the company to capture regulatory-driven demand. Strategic AI investments in identity verification and fraud prevention mitigate the complexity inherent in qualified processes.
- Frost & Sullivan recommends that Tinexta InfoCert sharpen its global value proposition by harmonizing brand architecture and portfolio clarity across subsidiaries to reduce perceived complexity for multinational buyers. As AI scales, articulating clear governance, compliance, and measurable outcomes will help convert technical capability into demonstrable customer impact.
- The company must maintain focus on executing its platform convergence initiative to unify the user experience and sustain innovation credibility without disrupting existing deployments.
- Defining clear monetization models for emerging areas, including digital identity wallets and AI-enabled services, would further differentiate Tinexta InfoCert from UX-led incumbents and security-centric competitors.
- Addressing these priorities would support the company's transition from a best-in-class qualified trust provider to a next-generation digital trust platform with broader relevance globally.

Yousign

INNOVATION

- Yousign is a sovereign European digital trust platform for SMBs navigating regulatory and fraud pressures. Founded in 2013 and transitioning to the Youtrust brand in 2026, it has evolved from eSignature to a broader trust platform aligned with eIDAS 2.0, the EU AI Act, and GDPR. The platform is built on three trust layers: signature, identity, and integrity, with all customer data hosted in the European Union.
- The solution portfolio mirrors this layered architecture. The signature layer offers SES, AES, and QES, compliant with eIDAS, plus electronic seals for the origin and integrity of documents. The Verify platform delivers the identity layer, consolidating static ID capture, video verification, biometric matching, certified hybrid verification, and Know-Your-Business checks. The integrity layer uses OCR, large language model analysis, and tiered IBAN/bank account verification via document checks, SEPAmail, and Open Banking. All features are accessible via a single REST API for rapid CRM and workflow integration.
- A key differentiator is Yousign's sovereign-first architecture and unified platform. EU-only hosting mitigates compliance risks, while consolidating services behind one API simplifies integration and operations versus multivendor solutions. Ergonomics, transparent pricing, and fast onboarding support adoption in regulated, compliance-sensitive segments.
- The Verify platform recently expanded into a risk-segmented identity framework with four assurance modes, from low-risk static capture to certified verification combining automated and human review. This allows tailored identity assurance per transaction, accelerating onboarding for low-risk workflows while meeting high standards in banking, legal, and notarial sectors—and removing dependence on external KYC solutions.

Yousign (continued)

INNOVATION

- AI and machine learning are deeply embedded across the trust stack. Autonomous contract agents extract and structure terms, reducing contract cycle times by up to 60% while improving compliance consistency. AI risk scoring prioritizes legal review, while ML models detect suspicious signing, synthetic identities, and deepfakes via real-time liveness analysis. Large language models enhance integrity by assessing ancillary document authenticity, strengthening auditability and dispute resolution.
- Yousign is advancing regulatory innovation for eIDAS 2.0 and the European Digital Identity Wallet, building infrastructure for wallet-based attestations and near-instant qualified certificate issuance. The roadmap also focuses on long-term cryptographic resilience, with active monitoring of post-quantum standards and guidance on quantum readiness as document retention extends.
- Additional enhancements include electronic seals for organizations, deeper IBAN verification via SEPAmail and Open Banking, expanded registry and sector support, workflow and UI refinements, and continued CRM and productivity platform integrations.
- Innovation at Yousign extends beyond technology. The transition to the Youtrust brand supports suite-based packaging and cross-selling across signature, identity, and integrity services. Transparent pricing, extensive implementation guidance, and a strong content and education strategy address regulatory complexity and digital skills gaps, contributing to high customer satisfaction and sustained adoption.

Yousign (continued)

GROWTH

- Yousign is a European specialist propelled by evolving regulations, rising fraud risks, and surging demand for EU-hosted trust services. As a sovereign provider, Yousign captures market share in compliance-driven sectors while avoiding direct competition on a global scale.
- The platform serves more than 30,000 organizations across Europe, with customers spanning regulated and semi-regulated industries, such as financial services, legal and notarial services, professional services, and telecommunications. Expansion beyond core eSignature into identity verification and integrity services has increased share of wallet and broadened the company's addressable opportunity.
- Yousign's growth is anchored in France, with more traction across the DACH region, Spain, and Italy. The company is targeting further expansion into additional EU markets as eIDAS 2.0 adoption progresses and is selectively evaluating opportunities in the United Kingdom aligned with the Digital Identity Trust Framework. Its go-to-market approach emphasizes direct sales, ecosystem integrations with CRM and workflow platforms, and content-driven education, supported by high customer satisfaction and strong renewal dynamics.

Yousign (continued)

FROST PERSPECTIVE

- Yousign should continue to lean into its sovereign-first positioning and EU-only data hosting as regulatory complexity increases under eIDAS 2.0, the EU AI Act, and related frameworks. This architectural choice directly addresses buyer concerns around jurisdictional exposure and compliance risk, particularly for SMEs and mid-market organizations that lack the resources to manage overlapping regulatory regimes. By emphasizing this positioning in regulated and compliance-sensitive use cases, the company can strengthen differentiation and accelerate adoption where sovereignty is becoming a baseline requirement.
- The company should further systematize the adoption of its unified platform by encouraging customers to use multiple trust layers rather than isolated capabilities. Yousign's consolidation of signature, identity, and integrity services behind a single API is a clear structural advantage, but its strategic value depends on customers realizing cross-layer benefits in real workflows. Clearer packaging, use-case-driven reference architectures, and workflow templates that demonstrate how Verify, eSeals, and integrity checks work together would increase share of wallet, improve retention, and reinforce positioning as a digital trust platform rather than an eSignature provider.
- With the mandatory rollout of European Digital Identity Wallets by December 2026, Yousign should sharpen its positioning as a key enabler of wallet-based trust. While progress on eIDAS 2.0 and wallet integration is evident, customers still question how wallet attestations will map to real-world signing and onboarding, especially for QES. Offering practical implementation guidance, reference flows, and validating wallet-centric use cases early can reduce uncertainty, accelerate adoption, and establish Yousign as a trusted intermediary between regulation and execution.

Zoho

INNOVATION

- Zoho Sign serves as both a stand-alone eSignature solution and an embedded agreement execution layer in Zoho's broader business software ecosystem. It supports SMB and enterprise customers in regulated, document-intensive industries, such as financial services, healthcare, insurance, legal, and real estate.
- In the past two years, Zoho Sign expanded its layered digital trust architecture to separate signature execution, identity assurance, and document integrity. The platform now supports SES, AES, and QES, integrates with QTSPs and national eID schemes, and lets customers select assurance levels for each transaction. This approach enables cross-border and high-assurance workflows while ensuring compliance with frameworks such as eIDAS, UK regulations, FDA 21 CFR Part 11, and EU GMP Annex 11 without imposing a single trust model for all use cases.
- Zoho Sign embeds AI-driven agreement intelligence directly into the agreement workflow. The platform summarizes documents, extracts clauses, generates first-draft agreements, and enables natural language queries of executed agreements. Customers access these functions across all pricing tiers, making AI a baseline productivity layer instead of a premium feature and helping them reduce review time and manual effort in high-volume agreement environments.
- Zoho Sign now connects tightly with more than 40 Zoho applications and expands its API and SDK support to enable embedded and white-label signing in CRM, HR, finance, CLM, and vertical software platforms.

Zoho (continued)

INNOVATION

- Zoho Sign has recently focused its innovation on strengthening evidentiary value and long-term trust resilience. The platform now captures audio and video evidence during signing, applies liveness detection to mitigate impersonation and deepfake risks, and builds crypto-agility to support future algorithm changes for long-lived documents. Its roadmap aligns with emerging digital identity models, including eIDAS 2.0 and EUDI wallets, to support selective disclosure and changing regulatory requirements.
- Zoho Sign delivers a steady stream of incremental enhancements that broaden usability and deployment flexibility. The team has expanded recipient roles, enabled parallel and in-person signing, added delivery channels including SMS and messaging platforms, deepened enterprise system integrations, and continually improves document creation, collaboration, storage, and retention management. These changes boost operational efficiency without altering the core platform architecture.
- Zoho Sign also innovates beyond technology. Usage-based pricing supports high-volume and embedded scenarios. Bundled AI capabilities, free migration assistance, and self-service evaluation resources lower adoption friction for organizations transitioning from incumbent eSignature platforms. This blend of technical and commercial innovation reinforces Zoho Sign’s value-oriented positioning and drives broader adoption across diverse customer segments.

Zoho (continued)

GROWTH

- Zoho Sign continues to grow steadily as part of Zoho Corporation's broader business software portfolio, gaining from stand-alone adoption and expansion in existing Zoho customer accounts. It serves SMBs through large enterprises and consistently attracts document-intensive and regulated industries, such as financial services, insurance, healthcare and life sciences, legal, real estate, and professional services.
- Adoption first accelerated in North America and India, then spread to Europe and other Asia-Pacific and EMEA markets. Zoho's global infrastructure and regional data hosting strategy support this expansion, enabling Zoho Sign to meet local compliance and data residency requirements while supporting cross-border agreement workflows.
- Competitive displacement increasingly drives customer acquisition. Many new customers switch to Zoho Sign for cost predictability, unlimited or high-volume signature models, and advanced AI capabilities without extra fees. Most organizations first adopt Zoho Sign as a point solution, then expand its use as they integrate adjacent Zoho applications into sales, HR, finance, and operational workflows.
- The go-to-market strategy combines digital-led acquisition with direct enterprise engagement and partner-supported deployments. Migration assistance, onboarding support, and a centralized evaluation center reduce switching friction and speed up time to value. Recently, usage-based pricing and API-driven deployment options have fueled growth in embedded and automated signing scenarios, positioning Zoho Sign for continued expansion beyond traditional seat-based models.

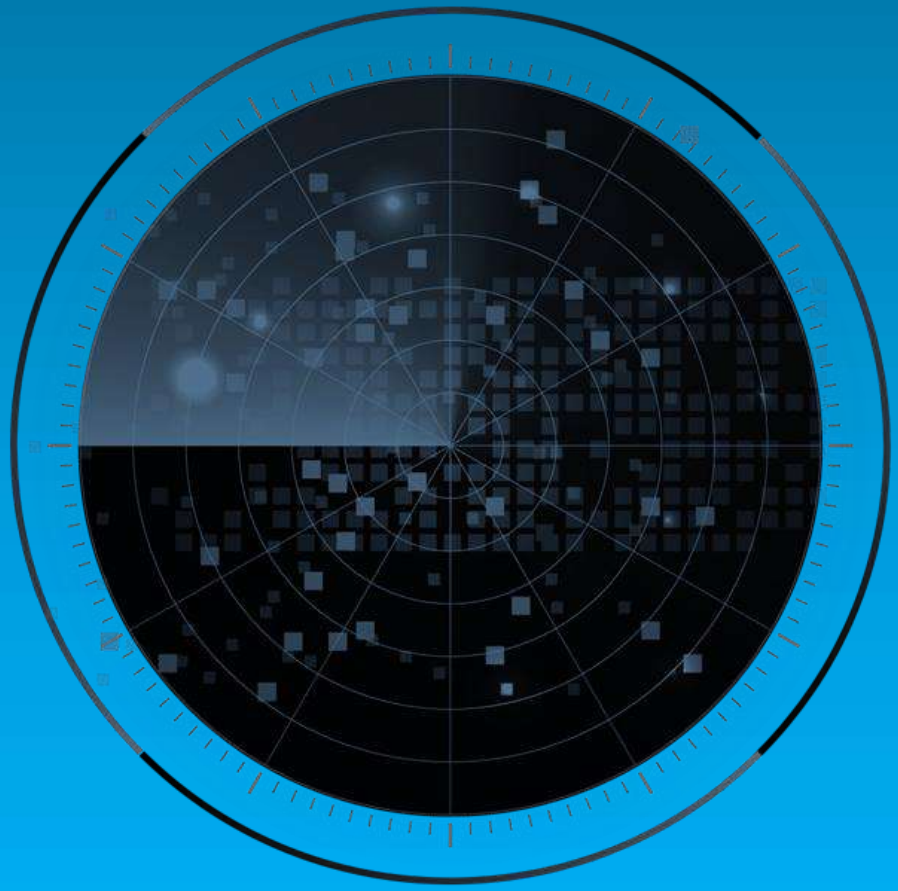
Zoho (continued)

FROST PERSPECTIVE

- Zoho Sign's layered digital trust architecture delivers flexibility for low- and high-assurance use cases and drives adoption in regulated, cross-border environments. To build on this strength, Zoho Sign can actively translate its architectural depth into prescriptive, vertical-specific trust configurations and guided setup paths, enabling customers to quickly align assurance levels with regulatory and business needs.
- Broadly available AI-driven agreement intelligence enhances Zoho Sign's value proposition by embedding productivity directly into agreement workflows. To maximize impact, Zoho Sign should package these capabilities into clear, outcome-oriented use cases, such as role-based workflows or preconfigured agreement templates, that make AI benefits tangible and easy to scale.
- Zoho Sign's ecosystem-led integration strategy positions the platform for embedded and platform-driven growth beyond traditional seat-based deployments. As this channel matures, Zoho Sign should prioritize developer enablement by offering standardized embedding frameworks, partner certification, and clear reference architectures to accelerate adoption in CLM platforms and vertical software ecosystems.
- Zoho's value-oriented commercial model and focus on customer enablement drive strong competitive displacement and long-term retention. To sustain this advantage, Zoho Sign should systematize customer feedback and co-creation practices, using insights from enterprise and regulated customers to validate roadmap priorities and reinforce its position as a long-term digital trust partner.

FROST & SULLIVAN

Best Practices & Growth Opportunities



Best Practices

1. Embed digital signing into identity and risk. Integrate biometrics, risk-based authentication, fraud detection, and auditability into workflows. Prioritize usability, strong cryptography, and future-proofing against AI fraud and synthetic identities.

2. Unify technology, services, and governance. Align resilient architecture, automation, and responsible AI to scale across regulated and global use cases.

3. Eliminate friction to accelerate adoption. Simplify deployment, clarify legal defensibility, and boost time to value for broader digital trust adoption.

Source: Frost & Sullivan

Growth Opportunities

1. Extend trust beyond the signature. Growth is shifting from transaction volume to identity, fraud mitigation, and evidence services. Vendors that embed KYC, biometrics, reusable credentials, timestamps, seals, and long-term preservation into standard workflows will outperform as enterprises standardize on dispute-ready, high-assurance digital execution.

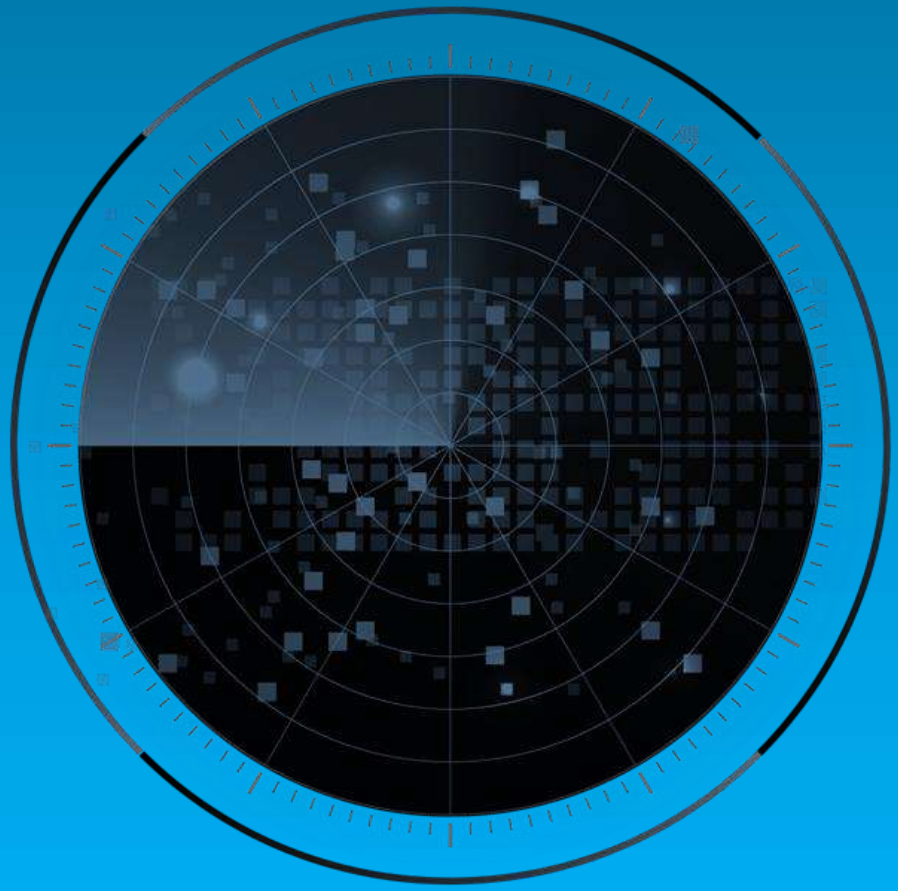
2. Operationalize regulation at scale. eIDAS 2.0, the EUDI Wallet, and evolving global regimes favor platforms that codify multijurisdiction rules into products. Wallet-ready architectures, sandboxed environments, and pre-integrated compliance services enable faster adoption and turn regulatory complexity into a durable growth advantage.

3. Lead with AI, crypto agility, and machine trust. AI-driven automation, fraud detection, and document intelligence are becoming baseline capabilities, while post-quantum readiness is emerging as a procurement criterion. Expanding trust to machines through code signing and device identity extends the market beyond human signers and creates new leadership pathways.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™ Analytics



Frost Radar™: Benchmarking Future Growth Potential
2 Major Indices, 10 Analytical Ingredients, 1 Platform

Growth Index

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a robust growth pipeline system; and effective market, competitor, and end-user focused sales and marketing strategies.

GI1

MARKET SHARE (PREVIOUS 3 YEARS)
This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.

GI2

REVENUE GROWTH (PREVIOUS 3 YEARS)
This is a look at a company's revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar™.

GI3

GROWTH PIPELINE
This is an evaluation of the strength and leverage of a company's growth pipeline system to continuously capture, analyze, and prioritize its universe of growth opportunities.

GI4

VISION AND STRATEGY
This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?

GI5

SALES AND MARKETING
This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Frost Radar™: Benchmarking Future Growth Potential
2 Major Indices, 10 Analytical Ingredients, 1 Platform (continued)

Innovation Index

Innovation Index (II) is a measure of a company's ability to develop products/ services/ solutions (with a clear understanding of disruptive megatrends) that are globally applicable, are able to evolve and expand to serve multiple markets and are aligned to customers' changing needs.

II1

INNOVATION SCALABILITY
This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.

II2

RESEARCH AND DEVELOPMENT
This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.

II3

PRODUCT PORTFOLIO
This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.

II4

MEGATRENDS LEVERAGE
This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of megatrends can be found here.

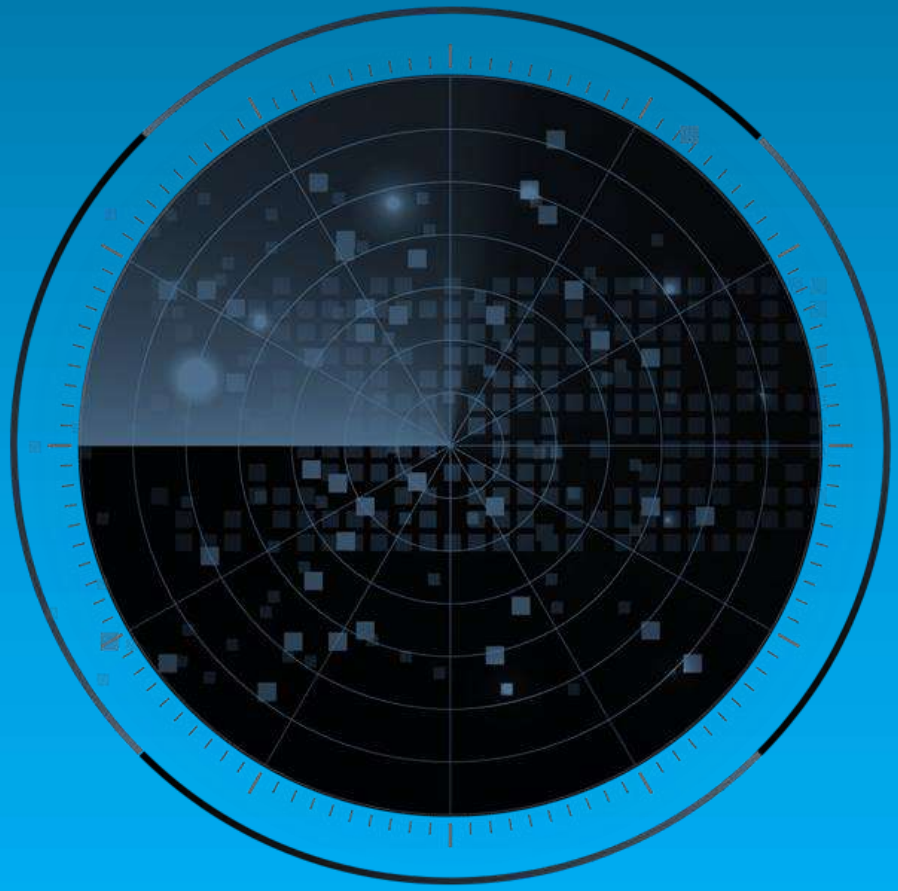
II5

CUSTOMER ALIGNMENT
This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Source: Frost & Sullivan

FROST & SULLIVAN

Next Steps: Leveraging the Frost Radar™ to Empower Key Stakeholders



Significance of Being on the Frost Radar™

Companies plotted on the Frost Radar™ are the leaders in the industry for growth, innovation, or both. They are instrumental in advancing the industry into the future.

GROWTH POTENTIAL

Your organization has significant future growth potential, which makes it a Company to Action.

BEST PRACTICES

Your organization is well positioned to shape Growth Pipeline™ best practices in your industry.

COMPETITIVE INTENSITY

Your organization is one of the key drivers of competitive intensity in the growth environment.

CUSTOMER VALUE

Your organization has demonstrated the ability to significantly enhance its customer value proposition.

PARTNER POTENTIAL

Your organization is top of mind for customers, investors, value chain partners, and future talent as a significant value provider.

Frost Radar™ Empowers the CEO's Growth Team

STRATEGIC IMPERATIVE

- Growth is increasingly difficult to achieve.
- Competitive intensity is high.
- More collaboration, teamwork, and focus are needed.
- The growth environment is complex.

LEVERAGING THE FROST RADAR™

- The Growth Team has the tools needed to foster a collaborative environment among the entire management team to drive best practices.
- The Growth Team has a measurement platform to assess future growth potential.
- The Growth Team has the ability to support the CEO with a powerful Growth Pipeline™.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**
- **Growth Pipeline™ Dialogue with Team Frost**

Source: Frost & Sullivan

Frost Radar™ Empowers Investors

STRATEGIC IMPERATIVE

- Deal flow is low and competition is high.
- Due diligence is hampered by industry complexity.
- Portfolio management is not effective.

LEVERAGING THE FROST RADAR™

- Investors can focus on future growth potential by creating a powerful pipeline of Companies to Action for high-potential investments.
- Investors can perform due diligence that improves accuracy and accelerates the deal process.
- Investors can realize the maximum internal rate of return and ensure long-term success for shareholders
- Investors can continually benchmark performance with best practices for optimal portfolio management.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Opportunity Universe Workshop**
- **Growth Pipeline Audit™ as Mandated Due Diligence**

Source: Frost & Sullivan

Frost Radar™ Empowers Customers

STRATEGIC IMPERATIVE

- Solutions are increasingly complex and have long-term implications.
- Vendor solutions can be confusing.
- Vendor volatility adds to the uncertainty.

LEVERAGING THE FROST RADAR™

- Customers have an analytical framework to benchmark potential vendors and identify partners that will provide powerful, long-term solutions.
- Customers can evaluate the most innovative solutions and understand how different solutions would meet their needs.
- Customers gain a long-term perspective on vendor partnerships.

NEXT STEPS

- **Growth Pipeline™ Dialogue**
- **Growth Pipeline™ Diagnostic**
- **Frost Radar™ Benchmarking System**

Frost Radar™ Empowers the Board of Directors

STRATEGIC IMPERATIVE

- Growth is increasingly difficult; CEOs require guidance.
- The Growth Environment requires complex navigational skills.
- The customer value chain is changing.

LEVERAGING THE FROST RADAR™

- The Board of Directors has a unique measurement system to ensure oversight of the company's long-term success.
- The Board of Directors has a discussion platform that centers on the driving issues, benchmarks, and best practices that will protect shareholder investment.
- The Board of Directors can ensure skillful mentoring, support, and governance of the CEO to maximize future growth potential.

NEXT STEPS

- **Growth Pipeline Audit™**
- **Growth Pipeline as a Service™**

Source: Frost & Sullivan

Next Steps

JOIN:
Growth Council

APPLY:
Companies to Action

ENGAGE:
Growth Dialog

PARTICIPATE:
Growth Council Think Tank

Does your current system support rapid adaptation to emerging opportunities?

Source: Frost & Sullivan

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com