SPARK Matrix™: Identity Governance and Administration, Q4 2025

By Dhyey Sherasia, Sofia Ali

November 2025

Key Findings

Following are the key findings, insights, and trends in Identity Governance and Administration:

Key Findings

- The 2025 SPARK Matrix for Identity Governance and Administration (IGA) identify a strong set of vendors driving the market through governance automation, risk-based access decisioning, and enterprise adoption. Leaders such as Saviynt, One Identity, SailPoint, Omada, Ping Identity, Eviden, Netwrix, and Wallix distinguish themselves by delivering comprehensive IGA capabilities that scale across hybrid environments and align with enterprise Zero Trust and compliance modernization initiatives. Each vendor demonstrates unique differentiators: Saviynt with its cloud-native platform, advanced risk analytics, and convergence of human and machine identity governance; Omada with governance-first process frameworks, SoD enforcement, and lifecycle automation strength; One Identity with its highly customizable workflows, strong role management, and governance-privileged access convergence; SailPoint with market-leading access certification, role optimization, and AI-driven access insights; Ping Identity with convergence of access governance and identity orchestration across workforce and customer domains; Eviden with strong integration of risk-based access governance and enterprise-grade reporting; Netwrix with a focus on security analytics, access auditing, and compliance monitoring; and Wallix with governance tightly integrated with privileged account controls and a security-anchored approach to workforce identity.

- Omada is recognized as an Emerging Innovator for advancing identity governance through its cloud-native, event-driven architecture, AI assistant Javi, and unified governance of human and machine identities demonstrating forward-looking innovation in automation, contextual access control, and Zero Trust aligned lifecycle management.
- Contenders in the 2025 IGA SPARK Matrix include Microsoft, SAP, IBM, Oracle, Broadcom, RSA, OpenText, Bravura Security, and ManageEngine. These vendors demonstrate strengths in scalability, integration within large enterprise ecosystems, or specific vertical use cases. For instance, Microsoft extends Entra ID capabilities to governance but remains more access-centric than full IGA; SAP emphasizes governance in ERP and regulated industries; IBM and Oracle bring robust analytics and enterprise integrations; while Broadcom, RSA, and OpenText offer selective governance functions but often lack unified breadth compared to Leaders. Bravura Security and ManageEngine cater effectively to mid-market enterprises, offering essential lifecycle and certification features, yet further investment in advanced analytics, risk-aware access models, and flexible workflows is needed to match the Leaders.
- In the Aspirants category, Tools4ever is positioned as a niche provider. While recognized for accessible IGA solutions that simplify lifecycle management and workflows for small to mid-sized organizations, it has yet to demonstrate the depth of large-scale enterprise deployments or advanced risk analytics seen among stronger players. Tools4ever shows potential with user-friendly interfaces and cost-efficient governance solutions, but expansion in product scope, AI-driven automation, and ecosystem interoperability will be necessary to advance into higher tiers of the SPARK Matrix.

Trends

- IGA platforms are evolving beyond compliance checklists to become essential enablers of secure digital transformation. They integrate lifecycle governance, policy enforcement, and analytics into a unified framework that supports both human and non-human identities across cloud, hybrid, and on-prem environments. This positions IGA as foundational for operational resilience and regulatory readiness.
- A powerful shift is underway toward AI and ML driven automation, enabling dynamic role mining, behavioural anomaly detection, and risk-aware certification workflows, all designed to reduce human toil while elevating governance accuracy and responsiveness.
- Leading vendors are embedding Cloud Infrastructure Entitlement Management (CIEM) into broader identity frameworks, offering deep visibility into cloud permissions, policy automation, and risk remediation. This is evolving toward unified identity governance across SaaS, IaaS, and on-prem environments.

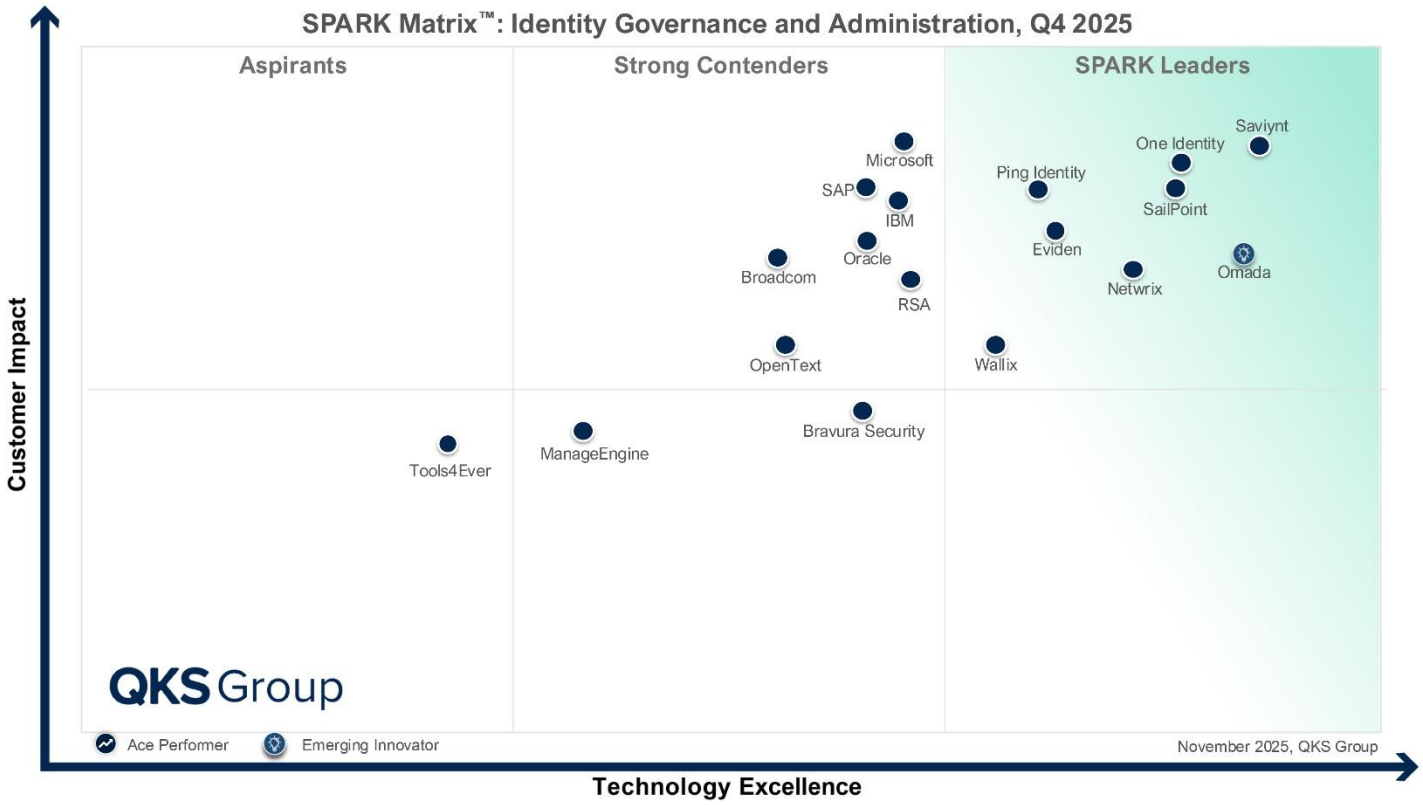
- Cloud-native delivery models, including SaaS and Identity as a Service (IDaaS), are becoming the norm, providing scalable, flexible, and accessible governance capabilities. This evolution supports rapid provisioning, seamless policy enforcement, and decentralized architectures.
- Non-human identities such as service accounts and AI agents are demanding new governance strategies. The blurring boundary between human and machine identity has triggered calls for unified, zero-trust–informed frameworks capable of treating all entities with consistent lifecycle and risk governance.

End users are increasingly focused on:

- Zero Trust Alignment: IGA is shifting from a compliance-centric view to a Zero Trust enabler. Continuous governance, least-privilege enforcement, and integration with policy engines are top priorities for modern enterprises.
- Cross-Platform Integration & Interoperability: Organizations require IGA platforms that integrate seamlessly with SaaS, on-premises, and multi-cloud ecosystems. Avoiding vendor lock-in and ensuring consistent governance across HR, ERP, IAM, and cloud apps is a rising focus.
- Governance of Non-Human Identities: End users are expanding governance expectations to machine identities, service accounts, and APIs. Visibility, ownership assignment, and lifecycle control for these non-human identities are becoming critical as automation and DevOps adoption increase.
- Integration with Privileged Access: End users want convergence between IGA and PAM (Privileged Access Management) to ensure governance extends to privileged and sensitive accounts. This reduces audit silos, strengthens risk oversight, and streamlines compliance.
- Risk-Based & AI-Driven Access Decisions: Enterprises are looking for governance systems that go beyond static roles and apply AI/ML-driven insights to recommend, approve, or revoke entitlements dynamically. Continuous risk scoring for access requests is becoming a differentiator.
- Identity Intelligence & Analytics: IGA buyers want advanced visibility into entitlements, access risks, and usage patterns. Analytics dashboards that highlight anomalies, dormant accounts, and excessive privileges are increasingly a baseline expectation.

SPARK Matrix™: Identity Governance and Administration, Q4 2025

Figure: 2025 SPARK Matrix™: (Strategic Performance Assessment and Ranking) Identity Governance and Administration



Vendor Profile

Following are the profiles of the Identity Governance and Administration vendors with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process. QKS Group research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technology capabilities. Users are advised to consult QKS Group before making any purchase decisions, regarding Identity Governance and Administration technology and vendor selection based on research findings included in this research service.

Omada

Founded in 2000 and headquartered in Copenhagen, Denmark, Omada offers Identity Governance & Administration focused solutions. Its product portfolio comprises Omada Identity Cloud (a cloud-native, SaaS IGA solution), Omada Identity (on-premises/hybrid IGA platform), and supporting components such as connector libraries, workflow engines, and analytics tools. Omada also publishes IdentityPROCESS+, a freely available, technology-agnostic framework for implementing IGA processes effectively. The IGA suite includes modules for identity lifecycle management (JML), access, role and entitlement management, certification and campaign-based access reviews, policy enforcement including separation of duties, compliance reporting, audit trails, and risk analytics. Omada has introduced the Cloud Application Gateway to facilitate secure connectivity between its cloud platform and on-premises or legacy systems using outbound-only links. It also launched Javi, a conversational AI assistant embedded in collaboration tools like Microsoft Teams to simplify IGA interactions. Omada is recognized for its configurability, hybrid deployment flexibility, and process-oriented implementation approach.

Strengths

- Omada Identity Cloud leverages a cloud-native, event-driven microservices architecture that processes incremental changes ("deltas") rather than re-importing full datasets. This enables near-real-time ingestion and reconciliation of identity and entitlement updates, which shrinks the blast window between HR or system changes and governance enforcement, and surfaces out-of-band entitlement changes sooner to create fewer privilege drift gaps, limiting shadow entitlements or toxic combinations. The platform supports both event-triggered and scheduled provisioning flows, with the flexibility to relay provisioning through intermediaries such as ServiceNow when direct integration is not feasible. Combined with Kubernetes-based autoscaling, built-in gateway failover, and lightweight deployment, Omada Identity Cloud ensures elastic performance and operational resilience at enterprise scale, maintaining SLAs even during bursts of joiner/mover/leaver activity or large-scale application onboarding.

- Omada's provisioning capabilities support both event-driven and scheduled provisioning flows. The system can generate assignment changes (via connectors like SCIM, LDAP, REST) and trigger tasks automatically when assignments change or on defined schedules. It also supports relayed or indirect provisioning through intermediaries (e.g. ServiceNow tickets) when direct provisioning is not possible. These provisioning options help reduce

orphan entitlements, support just-in-time access changes (after HR updates or role changes), and improve reconciliation accuracy.

- Omada's Cloud Application Gateway is a lightweight, customer-hosted component designed to provide secure outbound connections from on-prem systems to the Identity Cloud avoiding inbound firewall openings. It supports container or OS installations, automatic updates, and customer-controlled encryption keys to reduce operational attack surface while enabling governance over on-prem targets.

- Omada's Cloud Application Gateway (CAG) supports Bring Your Own Key (BYOK) functionality, allowing customers to use encryption keys stored in their own vaults (e.g., Azure Key Vault or HashiCorp Vault) for securing secrets exchanged through the gateway. This ensures that sensitive cryptographic material (secrets, credentials, tokens) is encrypted under keys the customer controls, minimizing exposure risk, and satisfying strict regulatory or compliance requirements around data sovereignty and auditability.

- Omada implements a continuous reconciliation/delta-calculation model. It ingests the actual state of identity/account/entitlement and computes a "delta" against the desired state, supporting near-real-time updates to the identity store and compliance dashboards. The platform exposes a rich compliance dashboard and "actionable" KPIs (orphaned accounts, risk items) driven by this always-fresh dataset. Such continuous reconciliation (vs. daily/weekly batches) shortens detection windows for orphan accounts, rogue entitlements, and reduces window for unauthorized access.

- Omada provides configurable pre-built templates and mapping tools for many protocols (SCIM 2.0, OData, REST, GraphQL, LDAP, PowerShell, .NET, CSV, SQL, SOAP). It also publishes connector packs for major enterprise targets (Microsoft AD / Microsoft Entra, SAP, ServiceNow, Salesforce, etc.) and offers a connector SDK and community templates to accelerate integration.

- Omada's IGA provides ML/AI-assisted role analysis (role-mining) and role recommendation capabilities intended to accelerate role modelling and reduce manual role maintenance. Role models are built from observed entitlement patterns and can feed into role design, hierarchical role structures and automated role lifecycle operations.

- Javi is Omada's AI Assistant that uses natural language to embed identity governance tasks directly into tools users already use. It is built on Microsoft Semantic Kernel, and offers a conversational interface embedded in Microsoft Teams that simplifies Identity

Governance and Administration tasks. Users can submit access requests, approve them, generate compliance reports, retrieve documentation, get role recommendations and receive contextual reminders or alerts, all via natural language commands. It respects enterprise policy by connecting actions to the user's identity, roles, and governance rules (e.g. separation-of-duty or least-privilege). Every operation is logged for auditability and for occasional users, Javi avoids dashboard fatigue; for power users, it accelerates repetitive workflows. Javi supports multilingual interaction and lowers friction in adoption by letting users work inside familiar tools.

- Omada's data model is the structural schema that represents identities, entitlements, and resource metadata across an organization. It defines how user objects, access rights, and resource classifications are stored, tagged, and correlated, providing a unified and consistent view of identity and access across diverse systems to enable meaningful governance, risk assessment, and compliance policies. The model also supports contextual identity governance, allowing access to be managed dynamically based on factors such as projects or other operational contexts rather than solely on static org charts. For example, users joining a project are automatically granted appropriate access, which is revoked when they leave, with these contexts treated as first-class elements within the security model. Additionally, the data model supports attribute extensions, custom fields, mapping and transformation, de-duplication, and master data source prioritization. These capabilities enable rapid onboarding of applications in cloud, on-premises, or hybrid environments, ensure frequent reconciliation, reduce custom coding, and support enforcement of security and compliance rules based on both identity and resource metadata.

- The Omada Cloud Management Portal provides users with autonomy over their Omada environment (cloud) without having to raise tickets with us as a vendor. Customers can clone, backup, restore, configure their Omada cloud environment themselves, without having to incur delays spending time raising and reading ticket responses.

- Omada Identity extends governance capabilities to machine identities such as service accounts and other non-human credentials. By extending Omada's IdentityPROCESS+ framework to machine accounts, organizations can systematically discover and classify these identities, ensuring they are inventoried and visible across hybrid environments. Each account is assigned an accountable owner, preventing "shared" or "orphaned" accounts from becoming invisible backdoors into critical systems. Governance controls,

including periodic reviews and attestations, help verify continued necessity, appropriate privilege levels, and alignment with regulatory requirements such as ISO 27001, NIS2, or SOX.

- Omada ships an API brief, documentation portal, connector templates, a Service Catalog integration for ServiceNow, and an Accelerator package (12-week implementation offer) plus IdentityPROCESS+ templates for business processes. These assets reduce delivery risk and speed up time-to-value for standard use cases.

Challenges

- Omada's Javi enables reading/viewing useful tasks such as submitting access requests, approving them, viewing notifications and reviews, retrieving documentation, and getting role insight recommendations. Its capabilities could be further strengthened by incorporating higher-privilege "write" or administrative functions such as modifying access, revoking permissions, or adjusting roles and policies via the conversational interface. Providing those actions with appropriate governance would help administrators bring more of the governance lifecycle directly into conversational IGA.

Appendix

Market Definition & Capabilities

QKS Group defines Identity Governance and Administration (IGA) as "a solution that empowers organizations to centrally govern, automate, and control user identities and their access rights across hybrid and multi-cloud enterprise environments. It supports end-to-end identity lifecycle management, role-based and policy-driven access provisioning, segregation of duties (SoD) enforcement, and dynamic access certifications."

The Identity Governance & Administration (IGA) market is undergoing rapid transformation, propelled by cloud adoption, hybrid-IT expansion, and the increasing necessity to enforce strong governance across human and non-human identities under Zero Trust mandates. Organizations are migrating from fragmented legacy access tools to converged IGA platforms that unify lifecycle governance, entitlement management, dynamic access certification, and policy enforcement across multi-cloud environments. This shift is fueled by growing regulatory scrutiny, complex IT estates, and the surge of machine identities, which demand consistent, auditable oversight. Vendors are differentiating themselves through AI-powered analytics, real-time risk scoring, behavior-based anomaly detection, and just-in-time access workflows positioning IGA as a cornerstone for compliance, scalable security, and intelligent governance.

To address these evolving challenges, IGA vendors are embedding AI and ML into governance workflows to automate access reviews, simplify entitlement descriptions, and prioritize risk-based certifications. Cloud-native and Identity-as-a-Service (IDaaS) delivery models are rising, offering scalable, subscription-based platforms that reduce deployment friction and support elastic governance. Additionally, decentralized identity architectures are beginning to emerge, enabling more user-centric control over identity data while preserving auditability. With organizations increasingly prioritizing operational resilience, regulatory compliance, and holistic identity oversight, the IGA market is poised for accelerated growth driven by demand for integrated, AI-augmented platforms that reinforce trust across complex identity ecosystems.

Following are the key capabilities of Identity Governance and Administration:

Role Management

Role Management automates the discovery, structuring, and lifecycle refinement of roles using behavior-based insights and access patterns. It ensures that roles correctly reflect evolving business responsibilities while preventing role explosion and enabling smooth decommissioning of outdated roles through staged deprecation workflows. By maintaining a clean, well-governed role model, organizations promote least-privilege access, reduce risk from excessive entitlements, and streamline change management, all while enhancing visibility, auditing, and governance.

Identity & Access Risk Management

Identity & Access Risk Management dynamically evaluates and scores user access and entitlements based on contextual risk factors such as sensitivity, frequency, and segregation-of-duties violations. By applying configurable risk models, it enables organizations to prioritize high-risk entitlements, mitigate access creep, and enforce policy-driven remediation. This proactive risk posture sharpens governance workflows, improves audit readiness, and ensures that users with unusual or risky access are identified and addressed promptly, enhancing overall identity security.

Workflow and Policy Management

Workflow and Policy Management orchestrate identity lifecycle events, access requests, and governance tasks via customizable, policy-driven workflows. It supports complex approval chains, exception handling, and automation of entitlement changes all through low-code, policy-inspired logic. By embedding governance into identity operations, organizations enforce consistent policy application, reduce manual bottlenecks, and ensure access changes happen reliably and transparently, leading to more agile, compliant, and auditable identity management.

Advanced Analytics

Advanced Analytics leverages AI, machine learning, and behavioral insights to surface anomalies, simulate risk, and drive intelligent decision-making via dashboards and visual reports. It enables

identity professionals to detect unusual access patterns, prioritize critical review tasks, and forecast governance needs. By transforming raw identity data into actionable, risk-aware insights, this capability empowers more proactive compliance validation, anomaly detection, and optimization of governance strategies.

Customization and Configuration

Customization and Configuration allow organizations to tailor workflows, policy definitions, UI components, and access logic via low-code or no-code tools. This adaptability ensures the platform aligns with business structure, compliance needs, and operational nuances, without requiring extensive development effort. As a result, IGA deployments remain flexible, resilient, and future proof, supporting rapid iteration, simplified administration, and reduced total cost of ownership in governance initiatives.

Access Governance and Lifecycle Automation

Access Governance and Lifecycle Automation, automates the entire journey of identity access from onboarding and provisioning to role changes and deprovisioning, ensuring access aligns with policy at every stage. By integrating policy enforcement with automation, it eliminates stale accounts, consolidates entitlement reviews, and accelerates access delivery. This streamlined lifecycle management enforces least-privilege, minimizes manual errors, reinforces compliance, and significantly enhances operational efficiency across hybrid and cloud environments.

Auditing and Reporting

Auditing and Reporting provides comprehensive logging and curated reports of access changes, certification outcomes, policy violations, and administrative actions. Offering both out-of-the-box templates and customizable views, it ensures traceability and transparency across identity governance activities. This capability simplifies compliance with regulatory standards such as SOX, GDPR, and HIPAA by delivering the necessary audit evidence while enabling real-time monitoring and forensic insights for security and governance teams.

Research Methodologies

Visit our website

Evaluation Criteria

QKS Group' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix provides a visual representation of market participants and provides strategic insights on how each supplier ranks related to their competitors, concerning various performance parameters based on the category of Technology excellence and customer impact. QKS's Competitive Landscape Analysis is a useful planning guide for strategic decision-making, such as finding M&A prospects, partnerships, geographical expansion, portfolio expansion, and similar others.

Technology Excellence	Weightage
Role Management	15%
Identity & Access Risk Management	15%
Workflow & Policy Management	10%
Advanced Analytics	10%
Customization & Configuration	10%
Access Governance & Lifecycle Automation	15%
Auditing & Reporting	10%
Scalability & Performance	5%
Competitive Differentiation Strategy	5%
Vision & Roadmap	5%

Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

Technology Excellence

- **Role Management**: Assesses the platform's ability to automatically discover and structure roles using behavior-based insights and access patterns. Includes support for continuous role refinement to align privileges with business responsibilities, thereby enhancing operational efficiency and promoting least-privilege access.
- **Identity & Access Risk Management**: Evaluates how user access and entitlements

are assessed through configurable risk models that assign dynamic scores based on contextual factors, entitlement sensitivity, access frequency, and segregation of duties (SoD) considerations. The focus is on enabling proactive mitigation of identity risks through intelligent enforcement and access recommendations.

- **Workflow and Policy Management**: Examines the orchestration of identity lifecycle events, access requests, and governance tasks using customizable, low-code workflows. Includes the ability to support complex approval chains, handle exceptions, and enforce policies for provisioning and deprovisioning in alignment with governance requirements.
- **Advanced Analytics**: Looks at the use of machine learning, AI, and behavioral analysis to monitor identity and access patterns, detect anomalies, and provide predictive insights. Encompasses reporting and visualization capabilities that strengthen auditing, compliance validation, and role/access governance optimization.
- **Customization and Configuration**: Considers the extent of low-code/no-code capabilities for customizing workflows, UI components, and access policies. The focus is on how quickly the platform can adapt to organizational structures, compliance mandates, and operational processes without requiring significant development resources.
- **Access Governance and Lifecycle Automation**: Evaluates automation across the identity lifecycle, from onboarding and role assignments to provisioning and deprovisioning. Highlights the integration of policy enforcement with workflow automation to ensure alignment with organizational policies, reduce manual overhead, and strengthen compliance across diverse environments.
- **Auditing and Reporting**: Assesses the ability to deliver comprehensive visibility into access events, entitlement changes, and administrative actions. Also considers the availability of both pre-built and custom reports to meet regulatory requirements such as SOX, GDPR, and HIPAA, while supporting forensic analysis and compliance assurance.
- **Scalability and Performance**: Focuses on the system's ability to govern identities and entitlements efficiently across expanding user bases and complex environments. Emphasis is placed on cloud-native and microservices-based architectures that enable horizontal scalability, consistent performance, low latency, and reliability in distributed and hybrid infrastructures.
- **Competitive Differentiation Strategy**: Examines the product's unique selling points (USPs) and competitive advantages that set it apart in the market.
- **Vision & Roadmap**: Evaluates the alignment of the product vision with customer needs in terms of acquisition, satisfaction, and retention. Also considers the clarity and

feasibility of the roadmap, the focus on customer experience, and the vendor's ability to execute planned improvements, innovations, and partnerships over the near to medium term.

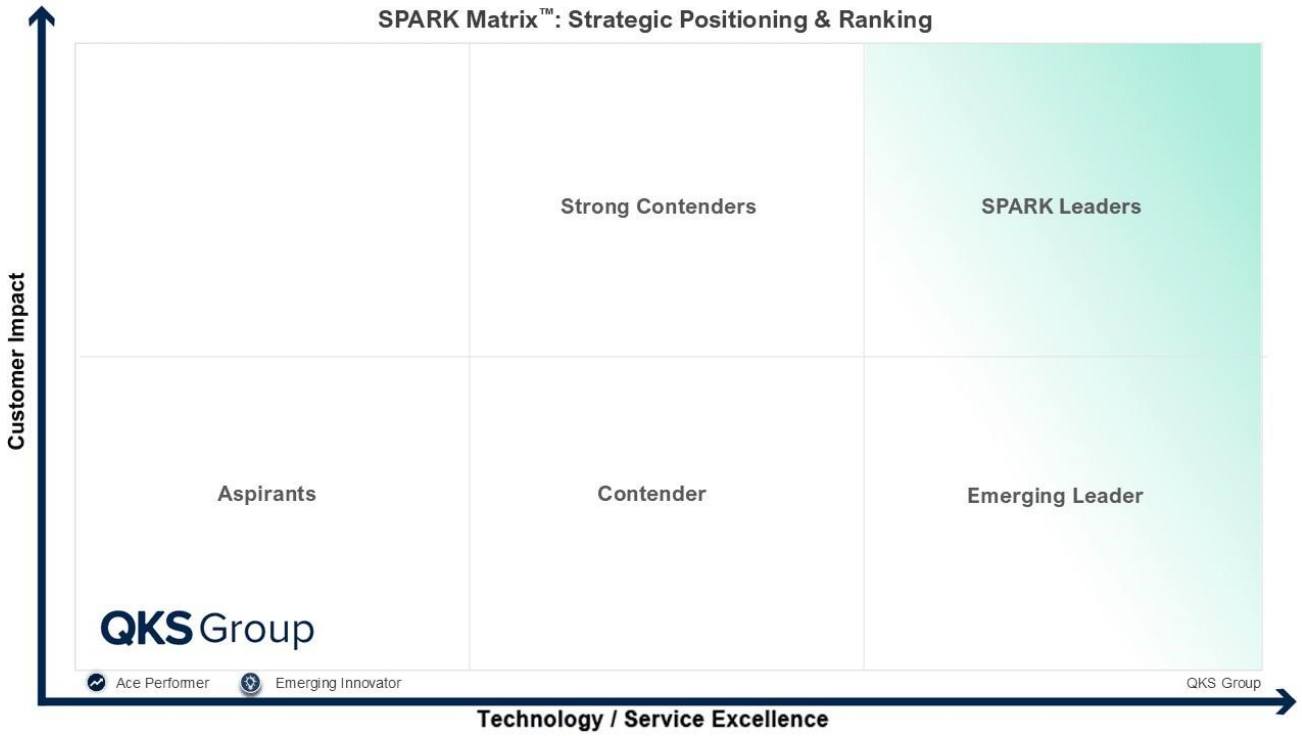
Customer Impact

- **Product Strategy & Performance**: Evaluation of multiple aspects of product strategy and performance in terms of product availability, price-to-performance ratio, excellence in GTM strategy, and other product-specific parameters.
- **Market Presence**: The ability to demonstrate revenue, client base, and market growth along with a presence in various geographical regions and industry verticals.
- **Proven Record**: Evaluation of the existing client base from SMB, mid-market, and large enterprise segments, growth rate, and analysis of the customer case studies.
- **Ease of Deployment & Use**: The ability to provide superior deployment experience to clients supporting flexible deployment or demonstrate superior purchase, implementation, and usage experience. Additionally, vendors' products are analyzed to offer a user-friendly UI and ownership experience.
- **Customer Service Excellence**: The ability to demonstrate vendors' capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.
- **Unique Value Proposition**: The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

How to read SPARK Matrix™

The **SPARK Matrix™** by QKS Group is a comprehensive evaluation framework that benchmarks vendors across key industries based on their **Technology Excellence** and **Customer Impact**. This proprietary analysis tool provides a detailed, comparative assessment of market players, enabling businesses to make informed decisions when selecting technology partners. The matrix highlights vendor strengths, growth trajectories, and market strategies, offering a dynamic visualization of their competitive positioning. Designed to cater to the needs of decision-makers, the SPARK Matrix serves as a trusted guide for navigating complex markets and identifying the vendors best suited to drive

organizational success and innovation.



- **Ace Performer:** Ace Performers are vendors that excel in operational performance based on their revenue growth potential, partnership strategy, and customer acquisition, all evaluated over the last one-year period or since the previous SPARK Matrix assessment.
- **Emerging Innovators:** Emerging Innovators are vendors recognized for their forward-thinking approach and disruptive innovations, even if they lack the scale or market penetration of more established players. This category highlights vendors with significant potential for long-term leadership in their domain, evaluated over the last one-year period or since the previous SPARK Matrix assessment.
- **Leader:** The Leader section of the SPARK Matrix represents organizations that set the gold standard in their respective industries. These vendors excel across both **Technology Excellence** and **Customer Impact** parameters, delivering best-of-breed solutions that are innovative, scalable, and future-ready. Leaders are recognized for their ability to anticipate market trends, address critical customer pain points, and deliver transformative outcomes. Their robust technological capabilities, combined with a deep customer-centric approach, position them as trusted partners for organizations seeking strategic growth and sustainable

competitive advantages.

- **Emerging Leader:** The Emerging Leader section highlights organizations that are rapidly closing the gap with established leaders. These vendors exhibit strong potential for future dominance, driven by significant advancements in **Technology Excellence** and increasing Customer Impact. Emerging Leaders often focus on niche markets or disruptive innovations, demonstrating a clear vision and execution capability. Their upward trajectory is marked by consistent enhancements to their offerings, growing market share, and an ability to deliver targeted solutions that cater to specific customer needs.

- **Strong Contender:** The Contenders section includes vendors that are establishing their footing in the market. These companies exhibit potential but may face limitations in terms of **Technology Excellence** or Customer Impact. Contenders often focus on addressing fundamental market needs and are actively investing in R&D and customer engagement strategies to strengthen their position. While they may not yet have the maturity or comprehensive offerings of higher-ranked categories, Contenders are key players to watch as they evolve and refine their strategies.

- **Aspirants:** The Aspirants section represents vendors that are in the early stages of development or are relatively new to the competitive landscape. These vendors have foundational offerings but lack the technological sophistication or customer-centric impact to compete at higher levels. Aspirants often serve niche markets or focus on incremental improvements, positioning themselves as future competitors in space. Their journey involves building credibility, enhancing solution capabilities, and developing customer relationships to rise through the SPARK Matrix rankings.

About the Authors

Dhyey Sherasia

Dhyey Sherasia is an Analyst at QKS Group specializing in the information security domain, with a focus on areas such as identity and access management (IAM), user authentication, and identity threat detection and protection. Through detailed market studies, vendor evaluations, and technology assessments, Dhyey provides clear, data-driven insights that help clients understand evolving cybersecurity trends and make informed decisions. Working closely with security vendors, product marketers, and technology buyers, Dhyey analyzes product capabilities, regulatory compliance considerations, and innovation roadmaps to evaluate how well solutions align with enterprise needs. His work supports strategic planning, product positioning, and investment decisions for stakeholders across the cybersecurity ecosystem. Grounded in thorough research and a strong understanding of both technical and market dynamics, Dhyey's knowledge delivers clarity in a complex, rapidly changing landscape.

Sofia Ali

Sofia Ali serves as an Associate Director - Research at QKS Group, where she oversees the information security global strategic market outlooks, market insight reports, technology and user-survey guides, SPARK Matrix Analysis, and consulting assignments. Her expertise primarily spans identity & access management, managed security services and related areas. Sofia leads both independent research and consulting projects while also collaborating closely with a team of analysts. She has partnered with clients across diverse industries and regions, contributing to consulting engagements in areas like technology architecture planning, cloud transformation, vendor selection strategies, and operational due diligence. Beyond her core responsibilities, Sofia is actively involved in industry events, conferences, webinars, and talk shows featured on various social media platforms, where she shares her insights and engages in thought leadership conversations with industry experts and peers.