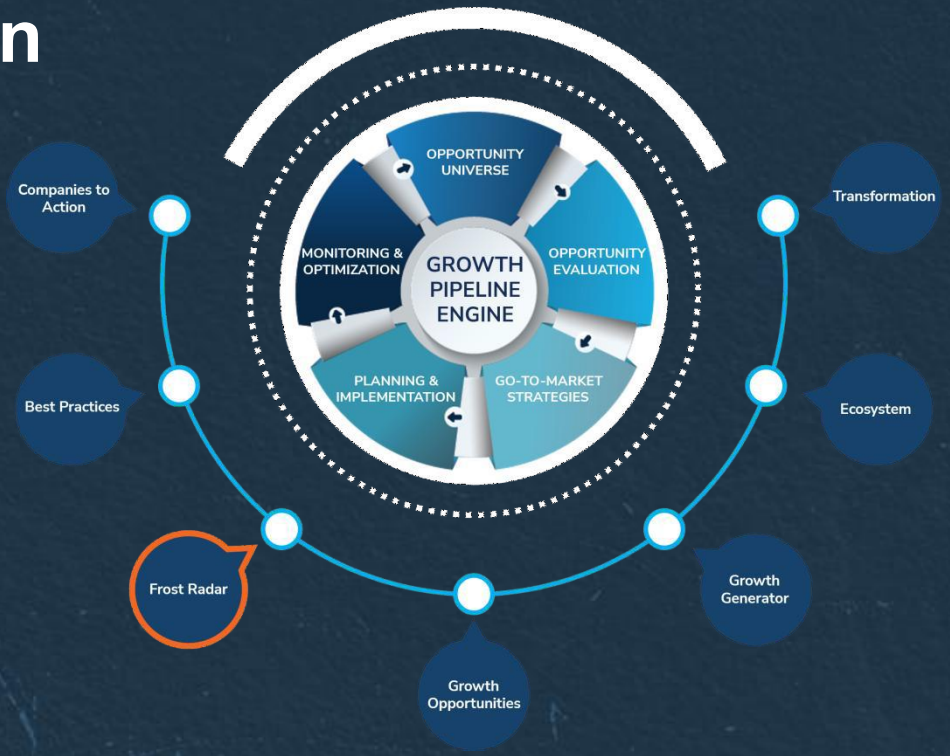
FROST & SULLIVAN

Frost Radar™: Non-human Identity Solutions, 2025



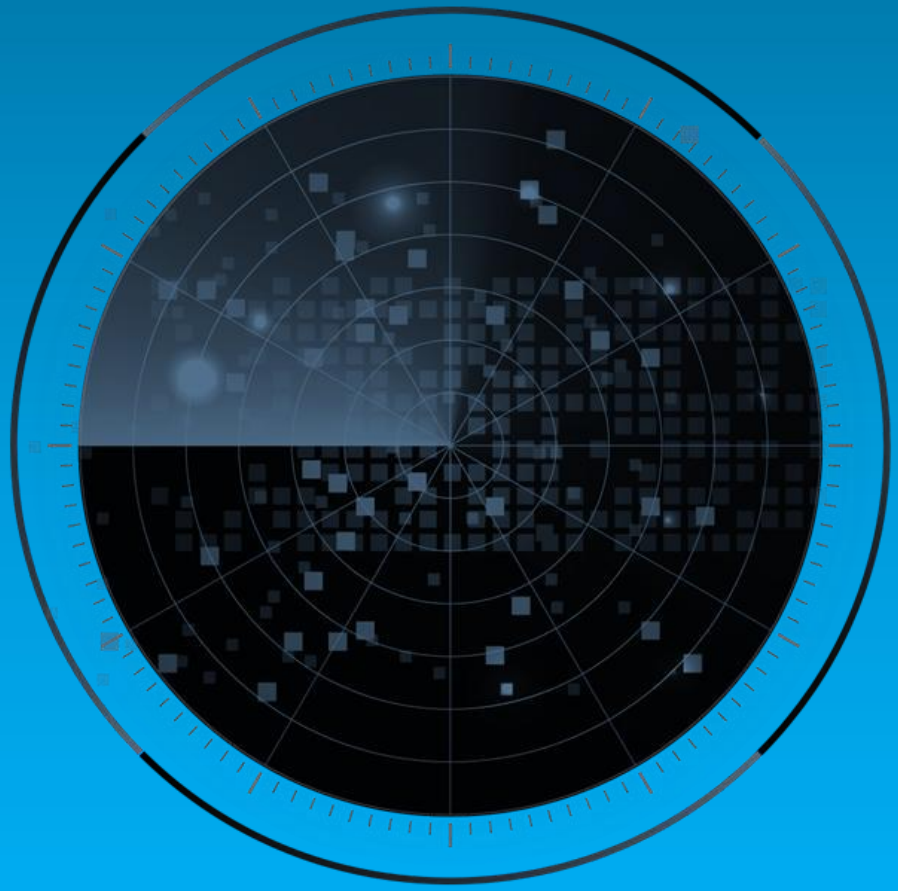
A Benchmarking System to Spark Companies to Action - Innovation That Fuels New Deal Flow and Growth Pipelines

Authored by: Dolores Aleman
Contributor: Danielle VanZandt

KC0C-23
November 2025

FROST & SULLIVAN

Strategic Imperative and Growth Environment



Strategic Imperative

- The non-human identity (NHI) solutions market is being shaped by a rapid expansion of machine identities that already outnumber human ones by more than 17 to 1 in large enterprises. This imbalance has been driven by the widespread adoption of cloud services, microservices, and automation pipelines, which are creating an exponential number of service accounts, tokens, API keys, and ephemeral workloads.
- As organizations scale DevOps and CI/CD pipelines, NHIs have become the connective tissue of automation, driving demand for governance, monitoring, and lifecycle enforcement tools that ensure least-privilege access. A further accelerator is the rise of agentic AI and large language model (LLM)-based copilots, which act autonomously with delegated access to data and systems. These AI-driven entities represent an entirely new class of NHIs, pushing enterprises to expand their identity strategies beyond human users.
- At the same time, regulators and boards are applying heightened scrutiny after high-profile breaches tied to unmanaged machine credentials, forcing organizations to treat NHI oversight with the same rigor as human identity and access management (IAM). This convergence with zero trust and identity security posture management (ISPM) strategies underscores why NHIs are now considered a pillar of modern security architectures.
- Despite the momentum, several restraints are slowing adoption across enterprises. Standards and frameworks for NHI governance remain immature; while human identity benefits from established protocols, such as SCIM or SAML, these frameworks are ill-suited for machine accounts, tokens, and AI agents, leaving interoperability gaps.

Source: Frost & Sullivan

Strategic Imperative (continued)

- Responsibility for NHIs is also fragmented, spread across DevOps, IT, and security teams, with no clear ownership leading to gaps in visibility and governance. Many enterprises still underestimate the risks, treating machine identities as “technical accounts” rather than high-value attack vectors, which has created awareness and skill gaps in organizations.
- The challenge is amplified by the sheer scale and velocity of modern environments, where millions of ephemeral workloads and multicloud deployments make even basic inventorying of NHIs a complex task without automation. Budget prioritization compounds the issue, as identity spending still tilts heavily toward human IAM solutions. such as identity governance and administration (IGA), multifactor authentication (MFA), and single sign-on (SSO), leaving NHI security often underfunded and underdeveloped.

Source: Frost & Sullivan

Growth Environment

- The global NHI solutions market is projected to expand from $5.0 billion in 2024 to $11.1 billion by 2030, registering a compound annual growth rate (CAGR) of 14.2%. This reflects the accelerating convergence of identity management, automation, and cybersecurity capabilities as enterprises seek to secure rapidly proliferating machine identities across hybrid and multicloud ecosystems.
- North America remains the largest and most mature market, underpinned by high enterprise adoption and stringent regulatory frameworks governing identity lifecycle management. Europe follows closely, driven by compliance mandates such as NIS2 and GDPR, which are reinforcing demand for governance and zero-trust identity assurance across human and non-human entities. Asia-Pacific stands out as the fastest-expanding region, with a projected 15.9% CAGR from 2024 to 2030, fueled by rapid digital transformation, AI-enabled automation, and large-scale investments in secure cloud infrastructures. Latin America and the region, including the Middle East and Africa, also record double-digit growth, reflecting increasing modernization of access infrastructures in sectors such as energy, banking, and public services.
- In addition to governance, NHI solutions must integrate with IAM, DevOps, and security frameworks to enforce policies such as least privilege, zero trust access, and real-time anomaly detection. This requires the ability to connect to a wide variety of platforms, from Kubernetes clusters to CI/CD pipelines, and to orchestrate identity workflows without slowing developer productivity. NHI platforms must also be capable of feeding telemetry into security information and event management (SIEM), security orchestration, automation, and response (SOAR), or identity threat detection and response (ITDR) systems, enabling organizations to identify misuse, privilege escalation, or compromised machine credentials before they can be exploited.

Source: Frost & Sullivan

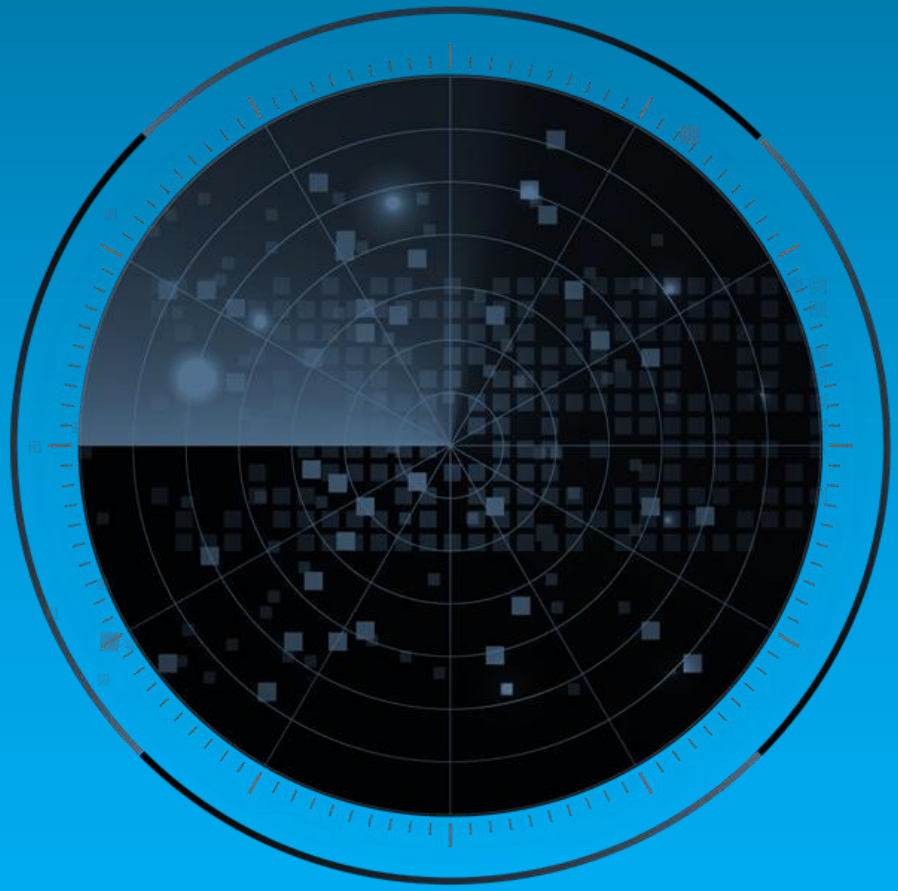
Growth Environment (continued)

- Four technology segments define how organizations discover, secure, and govern machine identities across digital ecosystems. Each addresses a distinct yet complementary layer of the NHI lifecycle.
  - **Discovery** covers tools that provide full visibility into all NHIs across multicloud, on-premises, and hybrid environments. Discovery solutions identify service accounts, API keys, secrets, and machine identities that are active, stale, or overprivileged. They generate risk scores and enable organizations to understand the blast radius of unmanaged identities. Discovery is often the entry point for organizations beginning their NHI security journey.
  - **Protocol access** technologies secure the channels through which NHIs communicate (e.g., TLS, SSH, Kerberos, OAuth, and SAML). While this area is more commoditized, it remains vital for interoperability and encrypted machine-to-machine (M2M) authentication. In Asia, for example, protocol access plays a larger role in enabling super-app ecosystems and cross-border platforms where APIs must seamlessly and securely interconnect across diverse services.
  - **Protection** solutions focus on defending NHIs from compromise and misuse. This includes continuous monitoring of NHI behavior, enforcing least privilege, rotating and vaulting secrets, and implementing ITDR for machine identities. Protection ensures that if a service account, certificate, or token is compromised, it can be quickly detected and contained. Regulatory frameworks, such as NIST Zero Trust, HIPAA, and PCI DSS, increasingly require this type of active protection.
  - **Management** solutions provide orchestration and lifecycle governance of NHIs. They automate provisioning and deprovisioning of machine identities, enforce policy-driven access, and integrate with DevOps pipelines (Kubernetes and CI/CD) to embed governance directly into workflows. They ensure scalability by controlling thousands or millions of NHIs without creating operational bottlenecks. This segment is growing quickly because lifecycle automation reduces risk and compliance burden.

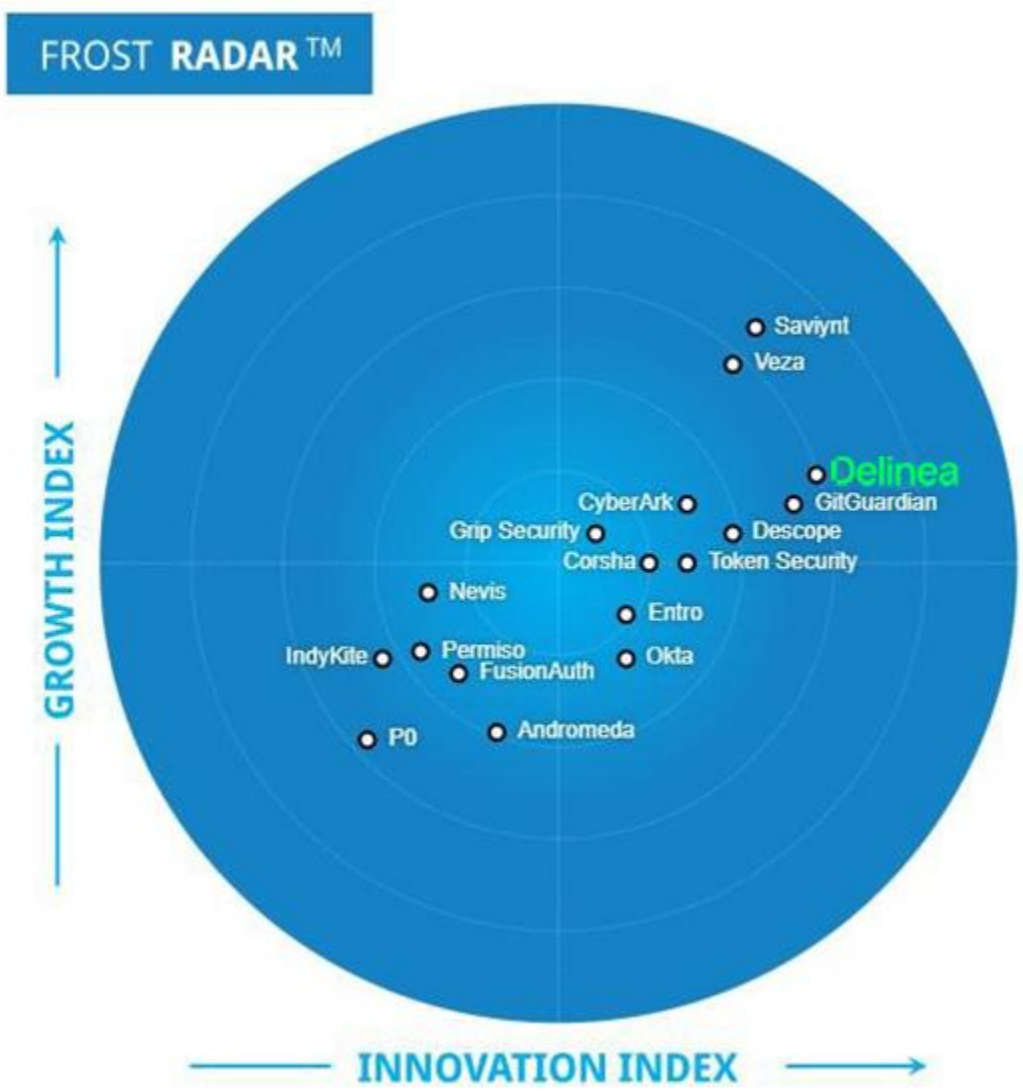
Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Non-human Identity Solutions



Frost Radar™: Non-human Identity Solutions



Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- When defining the scope of vendors for the Frost Radar™ NHI analysis, Frost & Sullivan selected companies that provide solutions designed to manage, secure, and monitor NHIs across digital ecosystems. At their core, NHI solutions must perform two critical functions: discovery of all machine identities in hybrid and multicloud environments, and lifecycle management to ensure that these identities are governed, rotated, and deprovisioned securely.
- Vendors were selected based on a combination of quantitative performance and qualitative innovation criteria that demonstrate their leadership and relevance in the evolving NHI ecosystem. Eligible companies must offer commercially available solutions that directly address machine identity discovery, protection, protocol access, and management, with proven deployments across multiple enterprise or institutional customers. Inclusion required a production-ready technology beyond pilot stage, supported by measurable adoption and customer references. Vendors also needed to exhibit innovation in automation, AI-driven analytics, or decentralized identity architectures, delivering differentiated capabilities that mitigate risks linked to identity sprawl and M2M communication.
- Additional selection factors included sustained revenue growth, an expanding customer base, or strategic partnerships in the past 24 to 36 months, as well as the ability to scale globally through cloud-native delivery or regional presence. Each vendor's strategic roadmap was assessed to ensure alignment with the market's shift toward autonomous, API-centric, and cross-platform identity governance, confirming their readiness to support secure digital transformation in complex, hybrid environments.
- Saviynt and Veza lead as benchmark innovators and growth drivers. Both have leveraged strong funding and enterprise traction to deliver advanced identity governance that now extends to machine and workload identities. They represent the convergence of traditional IGA and next-generation NHI governance.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Saviynt integrates zero trust and just-in-time (JIT) access into its privileged access and governance suite, enabling comprehensive control across human and non-human entities.
- Veza defines a new access intelligence model through its Access Graph™, mapping relationships among identities, data, and entitlements to deliver context-rich authorization and least-privilege enforcement.
- Delinea, GitGuardian, Descope, and Token Security combine strong product expansion with practical enterprise readiness. Delinea brings privileged access management (PAM) leadership into the machine identity space through AI-driven modules, such as Vault AI and Discover AI, reinforcing governance over secrets, credentials, and service accounts. GitGuardian complements this approach from a DevSecOps perspective, focusing on secrets detection, NHI visibility, and governance across code pipelines and cloud environments—a developer-first entry point into identity security. Descope differentiates itself with an Agentic Identity Control Plane built for AI agents and M2M environments, while Token Security focuses on AI and API identity protection, pioneering research on how agentic and LLM-driven identities challenge conventional IAM models. This group is driving innovation by addressing the operational and compliance challenges of NHI management in developer-centric and automation-heavy environments.
- CyberArk, Entro, Corsha, and Grip Security are bridging mature enterprise identity security with new forms of machine identity governance. CyberArk, long dominant in PAM, has evolved into a full Machine Identity Security platform, delivering lifecycle governance for secrets, certificates, and entitlements. Entro and Corsha bring complementary innovations—Entro with its secret-to-identity-to-entitlement chain for visibility and ownership of tokens, and Corsha with continuous authentication mechanisms for API and service-to-service communication. Grip Security manages SaaS-based NHI sprawl by unifying visibility and control across human and automated accounts in cloud environments. These companies exemplify how legacy IAM and PAM leaders are retooling to remain relevant in an ecosystem dominated by automation, APIs, and AI workloads.

Source: Frost & Sullivan

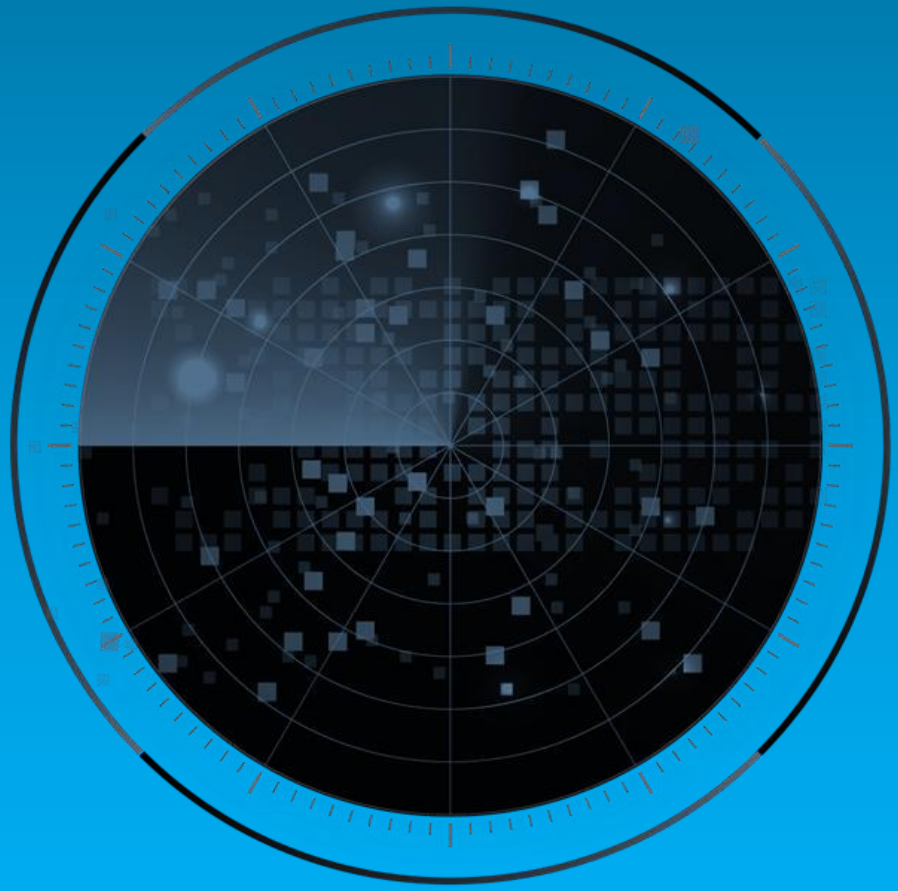
Frost Radar™ Competitive Environment (continued)

- Okta, FusionAuth, and Permiso are cultivating specialized capabilities to capture niche NHI opportunities. Okta leverages its identity cloud to integrate service-account management and workload identity protection, complementing its IAM dominance. FusionAuth and Permiso address developer-first identity orchestration and cloud identity detection, respectively.
- Emerging innovators Andromeda, Nevis, P0, and IndyKite each bring unique approaches to NHI control. Andromeda delivers lifecycle automation and hybrid visibility; Nevis extends its access management expertise into risk-based machine identity governance; P0 pioneers zero standing privilege (ZSP) enforcement for human and non-human users; and IndyKite applies graph-based, contextual authorization to AI and data-driven environments.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Companies to Action



Delinea

INNOVATION

- Delinea is advancing beyond its traditional PAM roots to become a cloud-native identity security platform capable of protecting human and non-human identities. The company's introduction of Iris AI marked a major innovation step, integrating machine learning, behavioral analytics, and adaptive policy enforcement into access control. It enables real-time, intelligence-driven decisions that reduce identity risk across hybrid and multicloud environments.
- Delinea's innovation roadmap—anchored in Vault AI, Discover AI, and Secure AI modules—reflects its strategy to govern machine identities, secrets, and AI workloads as enterprises adopt automation and generative AI technologies.
- The Delinea Platform unifies key security solutions, such as Secret Server, Cloud Suite, Privilege Manager, and Server Suite, providing centralized visibility and control over privileged access, credentials, and entitlements. Through identity threat protection and AI-driven authorization, Delinea enables context-aware access, dynamic privilege elevation, and continuous risk assessment across users, applications, APIs, and workloads.
- While Delinea's AI and NHI capabilities are still maturing, its enterprise-scale customer base, proven PAM expertise, and expanding cloud integrations give it a strong foundation for growth. The company is positioning itself as a transitional innovator, bridging legacy PAM leadership with next-generation identity security, AI governance, and machine identity management. Continued investment in AI-enhanced automation, ecosystem partnerships, and cross-platform integrations will solidify Delinea's role as a global leader in intelligent, adaptive identity security.

Source: Frost & Sullivan

Delinea (continued)

GROWTH

- Delinea maintains a robust partner ecosystem, including alliances with Microsoft Azure, Amazon Web Services, and Google Cloud, ensuring seamless deployment in hybrid and multicloud environments. Its listing on the Azure Marketplace has extended visibility among enterprise customers adopting cloud-based identity solutions.
- The company also collaborates with security integrators, managed service providers, and distributors such as QBS Software, which help expand its channel reach across North America, Europe, and Asia-Pacific. Delinea's partnerships with cybersecurity alliances, including MISA (Microsoft Intelligent Security Association) and CyberArk's extended ecosystem, have reinforced interoperability, helping customers embed Delinea's PAM and AI-driven identity controls into broader zero-trust architectures.
- Since the merger of independent PAM companies Thycotic and Centrify in April 2021, Delinea has sustained double-digit annual growth, driven by strong recurring revenue from subscription and SaaS offerings. Its customer base now exceeds 10,000 organizations worldwide, including large enterprises across financial services, government, healthcare, and critical infrastructure. The company has leveraged its legacy strengths to enter adjacent markets, such as ITDR, machine identity governance, and AI-based privilege management, positioning itself among the fastest-growing mid-tier identity security vendors.
- Backed by TPG Capital, Delinea continues to invest in global scaling, AI innovation, and channel partnerships, signaling a growth trajectory focused on expanding its enterprise footprint and cross-selling its expanding suite of identity security solutions.

Source: Frost & Sullivan

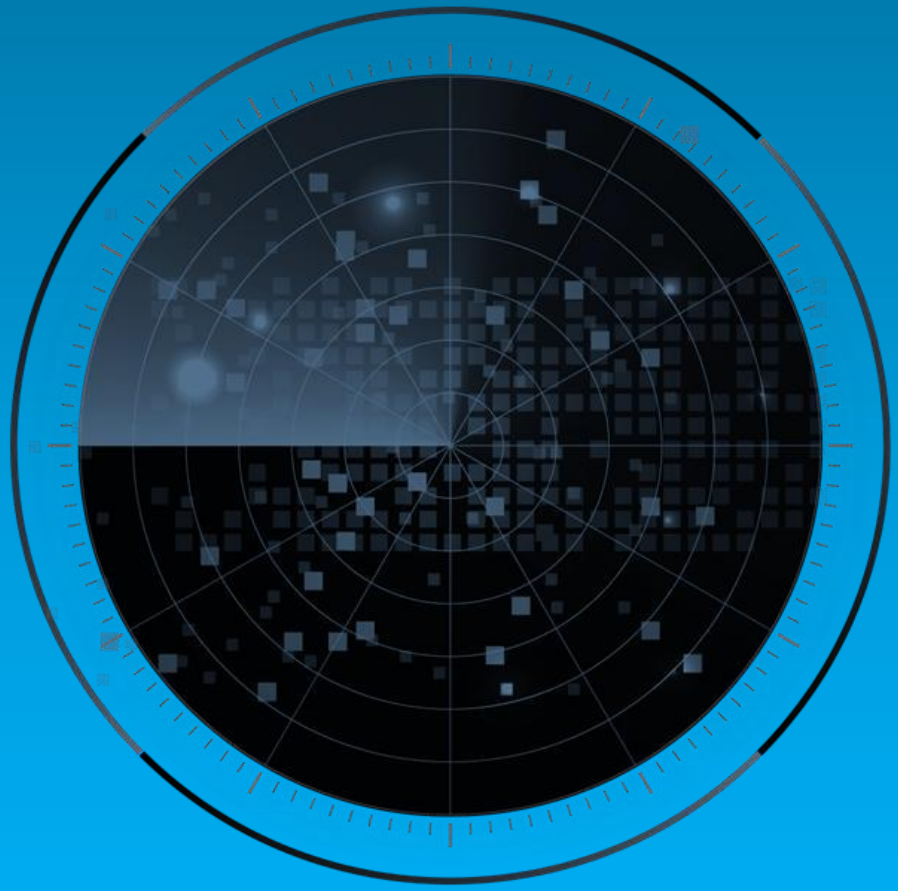
Delinea (continued)

FROST PERSPECTIVE

- While Delinea's heritage in PAM solutions provides credibility and market share, long-term growth depends on deepening its transition into ITDR, machine identity governance, and AI-driven access orchestration. Investing more in automation, continuous authentication, and agentic AI oversight would position Delinea as a unified identity security provider rather than a PAM specialist. Embedding these capabilities into its flagship solutions—Secret Server, Cloud Suite, and Identity Threat Protection—would unlock broader enterprise adoption across hybrid and cloud-native infrastructures.
- With Iris AI, Vault AI, and Discover AI, Delinea is positioned to lead in AI-governed access intelligence. To maximize growth, it should accelerate development of predictive analytics and autonomous remediation features that can detect, prioritize, and respond to identity-related risks—particularly for non-human entities, such as APIs, service accounts, and AI agents. Expanding AI explainability, compliance mapping, and governance reporting would appeal to customers in regulated sectors that require transparency in decision-making.
- Delinea's partnerships with Microsoft, AWS, and Google Cloud should be extended to include identity orchestration, secrets management, and AI governance vendors such as Saviynt, Veza, Descope, and Entro Security. Deep technology integrations and co-marketing efforts would improve cross-platform adoption and open new routes into DevOps, data security, and AI infrastructure domains. Collaborating with cyber insurance and compliance technology firms could highlight measurable risk-reduction benefits, reinforcing ROI for enterprise buyers.

Source: Frost & Sullivan

Best Practices & Growth Opportunities



Best Practices

1. Proper management of NHIs will require the adoption of the least privilege and ZSP models. Because machine identities often accumulate unchecked permissions across environments, continuously reducing entitlements and granting JIT access can minimize risk exposure. ZSP ensures that NHIs only operate with the permissions they need at the exact moment required, eliminating excessive or lingering privileges that attackers can exploit.

2. With thousands of tokens, certificates, service accounts, and API keys proliferating across hybrid and multicloud environments, manual oversight for NHIs is impractical and error-prone. Leveraging AI- and machine learning-driven tools to automate credential rotation, classification, and de-provisioning for NHIs will ensure that organizations maintain real-time visibility and consistent governance at scale, preventing orphaned or forgotten machine identities from becoming attack vectors.

3. NHIs are created and used in CI/CD pipelines, Kubernetes clusters, and automation frameworks, meaning that security policies must be embedded into these environments without disrupting speed or impacting availability. By aligning security controls with DevOps tooling, organizations can achieve operational agility and strong oversight over NHIs, ensuring that governance is seamless and part of the standard development lifecycle.

Source: Frost & Sullivan

Growth Opportunities

1. As enterprises increasingly deploy AI functionality, LLM-powered assistants, and autonomous agents, each becomes an NHI with access rights, credentials, and potential attack surfaces. Vendors that create frameworks to discover, monitor, and secure these identities can position themselves as pioneers in a rapidly expanding identity security frontier.

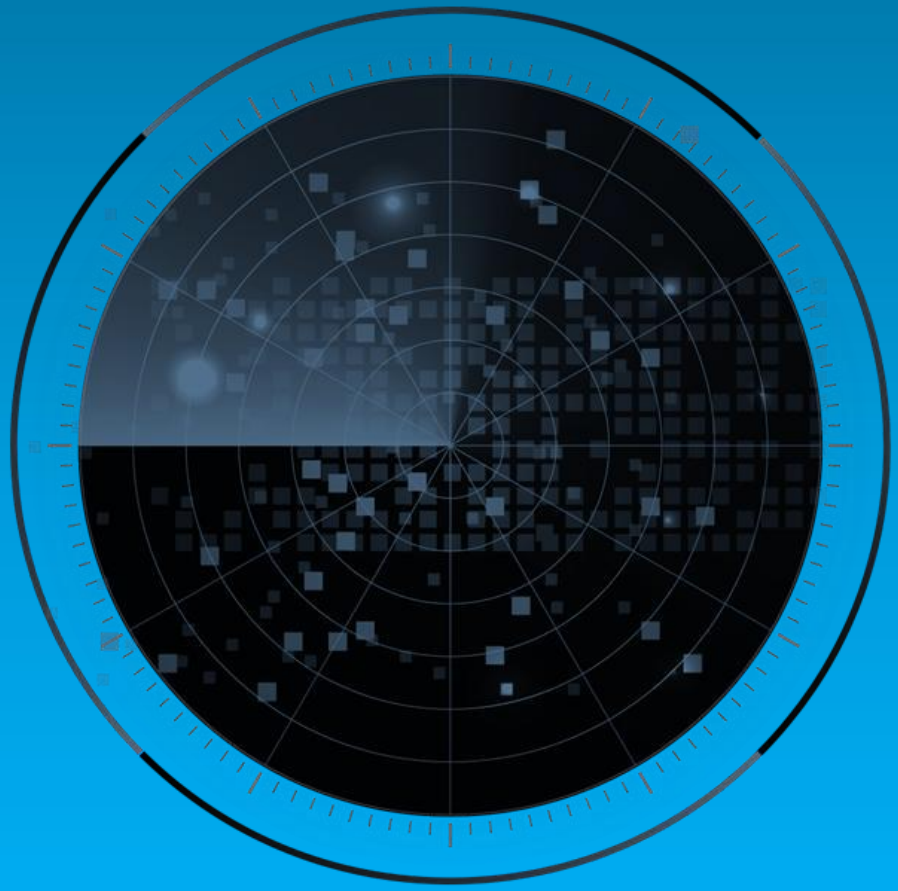
2. Enterprises adopting microservices, containerized workloads, and multicloud environments are experiencing a rapid expansion in machine identities. Solutions that integrate seamlessly with Kubernetes, Terraform, and CI/CD pipelines to automate discovery, credential rotation, and lifecycle management are becoming essential. Vendors that deliver such automation will be best positioned to satisfy the demand from organizations seeking to balance operational agility with strong security controls.

3. BFSI, healthcare, and government organizations face strict identity and data protection rules under GDPR, HIPAA, PCI, and NIS2 frameworks. Vendors that tailor NHI platforms to embed compliance accelerators, real-time auditing, and regulatory reporting will be able to command premium pricing and create sticky, long-term customer relationships.

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.

Source: Frost & Sullivan

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.

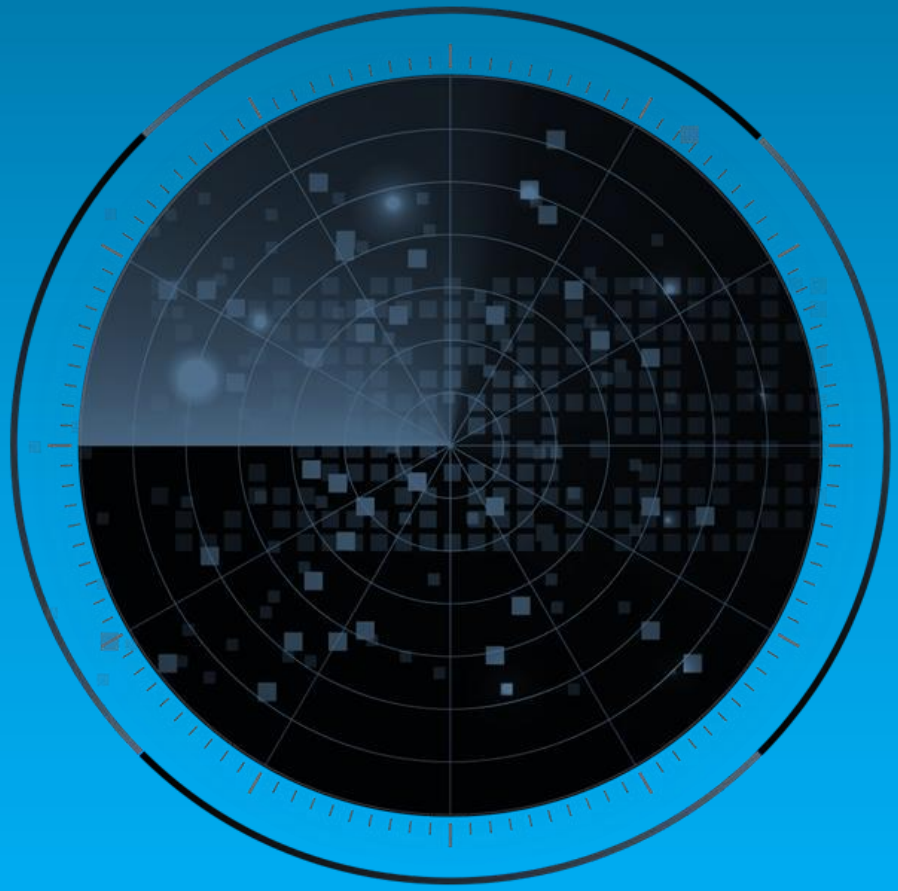
II5

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.

Source: Frost & Sullivan

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**

Source: Frost & Sullivan

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