Enterprise Identity

Product Innovation and Managed Service Opportunities

Executive Summary

The enterprise identity market, encompassing identity and access management (IAM), privileged access management (PAM), identity governance and administration (IGA), and related security solutions, is experiencing robust growth due to the increasing complexity of digital ecosystems, rising cyber threats, and regulatory compliance requirements.

Valued at approximately $13.5 billion in 2024, the global IAM market is projected to grow at a CAGR of 15.6%, reaching $25.6 billion by 2029. Key drivers include the shift to cloud-based infrastructure, the proliferation of remote work, and the adoption of zero trust security models.

However, challenges such as integration complexities, skill shortages, and evolving threat landscapes pose significant hurdles. This report analyzes market trends, drivers, challenges, competitive landscapes, and future opportunities to provide actionable insights for channel partners.

Executive Summary

The enterprise identity market, vital for securing the digital enterprise, is witnessing robust growth as organizations grapple with escalating cyber threats, cloud adoption, and stringent regulatory demands.

Valued at approximately $13.5 billion in 2024, the global identity and access management (IAM) market is projected to reach $25.6 billion by 2029, growing at a compound annual growth rate of 15.6%.

Drivers

This expansion is fueled by the increasing complexity of digital ecosystems, where securing both human and machine identities is critical to safeguarding sensitive data and ensuring operational continuity. The rise of remote work, bring-your-own-device policies, and hybrid IT environments has amplified the need for scalable, cloud-native solutions that seamlessly integrate with legacy systems.

Key drivers of this market include the surge in cyberattacks, with over 80% of 2024 data breaches involving compromised credentials, pushing enterprises to prioritize robust authentication and privileged access management.

The shift to cloud infrastructure, coupled with the adoption of zero trust security models, underscores the demand for adaptive IAM platforms that support continuous verification.

Regulatory frameworks like GDPR and CCPA further compel organizations to invest in identity governance to ensure compliance, with non-compliance penalties reaching €1.7 billion in 2024. However, challenges persist, including integration complexities across heterogeneous IT environments and a 25% shortage of skilled cybersecurity professionals, which hinders effective implementation.

Market Opportunities

The competitive landscape is dynamic, with leaders like Okta and Microsoft (via Entra ID) dominating cloud-based IAM, while SailPoint and CyberArk excel in governance and privileged access management, respectively.

Emerging trends include AI-driven analytics for anomaly detection, passwordless authentication using biometrics, and decentralized identity solutions leveraging blockchain, particularly in finance and healthcare.

The market also presents opportunities for growth in small and medium-sized enterprises, which seek affordable, user-friendly solutions, and in securing machine identities, driven by the proliferation of APIs and IoT devices.

Looking ahead, the enterprise identity market is poised for transformation, with zero trust and passwordless authentication becoming standard by 2027, and decentralized identity gaining traction by 2030.

Enterprises must invest in AI-enhanced, cloud-native platforms, prioritize compliance, and address skill gaps through training to stay resilient. Vendors innovating in automation and industry-specific solutions will lead the charge, enabling organizations to secure the digital enterprise against an evolving threat landscape.

IDaaS and MSP Solutions

Delivered through Managed Service Providers, IDaaS (Identity as a Service) enables businesses of all sizes—especially small and medium-sized enterprises to leverage enterprise-grade security without the burden of managing complex infrastructure.

IDaaS is a cloud-delivered model that centralizes identity management, offering tools like single sign-on (SSO), multi-factor authentication (MFA), and identity governance to secure access to applications and data.

Unlike traditional on-premises IAM systems, IDaaS eliminates the need for costly hardware, extensive IT expertise, and lengthy deployments, making it ideal for organizations with limited resources.

For SMEs, which often lack dedicated cybersecurity teams, IDaaS provides a cost-effective way to protect against rising cyber threats, such as phishing and credential theft, which accounted for over 80% of data breaches in 2024.

By integrating with cloud platforms like AWS, Microsoft Azure, and Google Cloud, IDaaS supports hybrid and multi-cloud environments, aligning with the digital transformation strategies of modern enterprises.

MSPs play a critical role in delivering IDaaS, acting as trusted partners that manage and maintain identity solutions for their clients.

Okta

Through platforms like Okta, MSPs can offer comprehensive IAM services, including passwordless authentication and zero trust security models, which verify users continuously to minimize risks.

Okta’s platform offers robust features like single sign-on (SSO), multi-factor authentication (MFA), and lifecycle management, addressing modern cybersecurity challenges such as credential theft and unauthorized access.

A key focus for Okta is passwordless authentication, which enhances security and user experience by replacing traditional passwords with methods like FIDO2 WebAuthn for biometric logins, device-based authentication (e.g., YubiKey), and push notifications via Okta FastPass.

Okta’s cloud-native platform, with its extensive app integrations and features like Okta FastPass, enables MSPs to provide seamless, secure access to applications while ensuring compliance with regulations like GDPR and CCPA.

ZeroTek

However, the complexity of managing multiple clients with diverse needs can challenge MSPs, particularly in terms of scalability and cost.

This is where partners like ZeroTek enhance the IDaaS ecosystem. ZeroTek’s multitenant, pay-as-you-go SaaS platform simplifies the deployment, management, and reselling of Okta’s IAM solutions for MSPs.

ZeroTek’s multitenant SaaS platform simplifies Okta’s deployment for MSPs, offering a single dashboard to manage multiple SME clients, automate policy enforcement, and streamline auditing.

By providing pay-as-you-go pricing, integration with Okta FastPass and rapid provisioning, ZeroTek enables MSPs to deliver Okta’s advanced features—like biometric authentication, device-trust-based logins and role-based access control—without upfront costs or technical barriers. This partnership empowers MSPs to secure their clients’ digital enterprises efficiently, addressing the growing demand for flexible, scalable identity solutions.

ZeroTek enhances Okta’s offerings with MSP-centric features, such as granular policy configuration, auditing for compliance, and rapid deployment capabilities, enabling MSPs to deliver passwordless authentication and zero trust security without upfront costs or complex procurement.

Solution Synthesis

Digital Workplace

The synergy between Identity as a Service (IDaaS) technologies, such as those offered by Okta and ZeroTek, and digital workplace solutions like virtual desktops and endpoint security creates a comprehensive framework for securing and optimizing the modern enterprise.

IDaaS platforms like Okta provide centralized identity management through single sign-on (SSO), multi-factor authentication (MFA), and passwordless authentication, ensuring secure access to applications and data.

Virtual desktops, such as those from Citrix, VMware Horizon, or Microsoft Windows 365, deliver standardized, cloud-hosted desktop environments, allowing employees to access work resources from any device. Endpoint security solutions, like those from CrowdStrike or Microsoft Defender, protect devices against malware, ransomware, and other threats.

Together, these technologies create a cohesive ecosystem.

For example, Okta's SSO and FastPass integrate with virtual desktops to provide seamless, biometric-based access to virtualized applications, while endpoint security ensures devices meet compliance standards before granting access. Furthermore Okta's adaptive MFA can trigger additional verification if endpoint security detects anomalies, such as an unpatched device.

ZeroTek's multitenant platform enhances this for MSPs by enabling scalable deployment of these policies across SMB clients, simplifying management and reducing costs.

Enterprise Browsers

The synergy between Identity as a Service (IDaaS) technologies, such as those provided by Okta and ZeroTek, and enterprise browsers creates a powerful framework for securing the digital enterprise.

Enterprise browsers are built for zero trust environments, enforcing strict access controls and monitoring user behavior in real time. They integrate with IDaaS solutions to verify identities continuously, ensuring that only authorized users and devices access sensitive resources.

When combined with IDaaS, they enhance access control, streamline user experiences, and fortify security in cloud-centric, remote, and hybrid work settings. Enterprise browsers, such as Island, Talon, or Google Chrome Enterprise, extend these capabilities by embedding identity-aware access controls directly into the browser.

For instance, Okta's FastPass, which uses biometrics and device trust, can be enforced through an enterprise browser's security layer, validating user sessions before granting access to web applications. ZeroTek's platform complements this by allowing MSPs to deploy these policies across multiple clients, ensuring consistent zero trust enforcement.

This combination mitigates risks from phishing and insider threats by aligning browser-level security with IDaaS-driven identity verification.

Vendor Directory

These capabilities collectively reduce IT overhead, enhance security, and support digital transformation by providing a unified, efficient approach to identity management.

Below is a table analyzing key vendors providing IDaaS solutions.

--

Vendor	Key Technologies	Functionality Highlights	Strengths	Potential Weaknesses
1Password	SSO, MFA, Password Management, SCIM Integration, Passkeys	Secure credential management, passwordless login with passkeys, SSO for business users	Strong password management, user-friendly, integrates with major IdPs (e.g., Okta, JumpCloud)	Limited focus beyond credential management, not a full IAM suite
OneLogin	SSO, MFA, LDAP/AD Integration, User Provisioning, Machine Learning	Centralized access management, real-time anomaly detection, affordable for SMEs	User-friendly, cost-effective, good for mid-sized businesses	Fewer advanced features compared to larger competitors, less scalability for enterprises
JumpCloud	SSO, MFA, Cloud Directory, Device Management, LDAP/RADIUS	Unified directory for identity and device management, zero-trust policies, extensive integrations	Comprehensive cloud-native solution, SME-friendly, cross-platform support (Windows, Mac, Linux)	Complexity in setup for advanced features, higher cost for full suite
Okta	SSO, MFA, Universal Directory, Adaptive Authentication, API Integration	Workforce and customer identity management, real-time threat detection, SSO for 5000+ apps. Read more in their guide.	Market leader, extensive app integrations, AI-powered threat response.	Higher cost for premium features, complexity for smaller organizations
Microsoft (Entra ID)	SSO, MFA, Conditional Access, AD Integration, AI-driven analytics	Extends Azure AD to cloud, hybrid identity management, seamless Microsoft ecosystem integration	Broad adoption, cost-effective within Microsoft stack, strong compliance tools	Less flexibility outside Microsoft ecosystem, steep learning curve for non-MS users

Ping Identity	SSO, MFA, Identity Governance, Directory Services, OIDC/SAML	PingOne Cloud Platform, customer identity solutions, hybrid deployment support	Flexible deployment (cloud/hybrid), strong customer IAM focus, robust MFA options	Smaller market share compared to Okta/Microsoft, limited visibility in some regions
SailPoint	Identity Governance, SSO, MFA, AI/ML Analytics, Provisioning	Focus on identity governance and compliance, predictive analytics for risk management	Strong governance and compliance tools, enterprise-grade scalability	Less emphasis on consumer IAM, higher complexity for setup
IBM (Cloud Identity)	SSO, MFA, Identity Governance, Hybrid Integration, Behavioral Analytics	Bridges on-premises IAM to cloud, risk-based authentication, extensive reporting	Robust hybrid support, trusted brand, good for regulated industries	Higher cost, slower innovation pace compared to newer vendors
CyberArk	Privileged Access Management (PAM), SSO, MFA, Identity Security, API Integration	Focus on securing privileged identities, zero-standing privileges, integration with cloud services	Leader in PAM, strong security focus, good for high-risk environments	Niche focus on privileged access may limit broader IAM appeal, premium pricing
ForgeRock	SSO, MFA, Identity Governance, OpenID Connect, Autonomous Identity (AI-driven)	Full lifecycle identity management, strong customer and workforce IAM, open-source roots	Highly customizable, strong in complex deployments, innovative AI features	Smaller market presence, steeper learning curve for customization

Notes on Analysis

- **1Password:** Primarily a password manager with IDaaS features like SSO and MFA, it excels in credential security but lacks the breadth of full IAM solutions.
- **OneLogin:** Offers a solid, affordable IDaaS option with enterprise-grade features, though it’s less robust for large-scale or highly complex deployments.
- **JumpCloud:** Stands out as a comprehensive cloud directory platform, blending identity and device management, making it ideal for modern, diverse IT environments.

- **Market Trends:** As of 2025, vendors are increasingly integrating AI/ML for threat detection and adopting passwordless authentication (e.g., passkeys, FIDO2). The shift to hybrid and remote work continues to drive demand for scalable, cloud-native solutions.
- **Vendor Selection:** Choice depends on needs—Okta and Microsoft lead for broad ecosystems, JumpCloud and OneLogin appeal to flexibility-focused firms, while SailPoint and CyberArk excel in governance and security.
- **Limitations:** Pricing, feature depth, and regional availability evolve rapidly; organizations should verify current offerings directly with vendors.