White Paper

by Gregory Krisberg, Senior Associate

Untangling the evolving landscape of Workforce Identity and Access Management

New York - London - Paris

www.axavp.com

Untangling the evolving landscape of Workforce Identity and Access Management

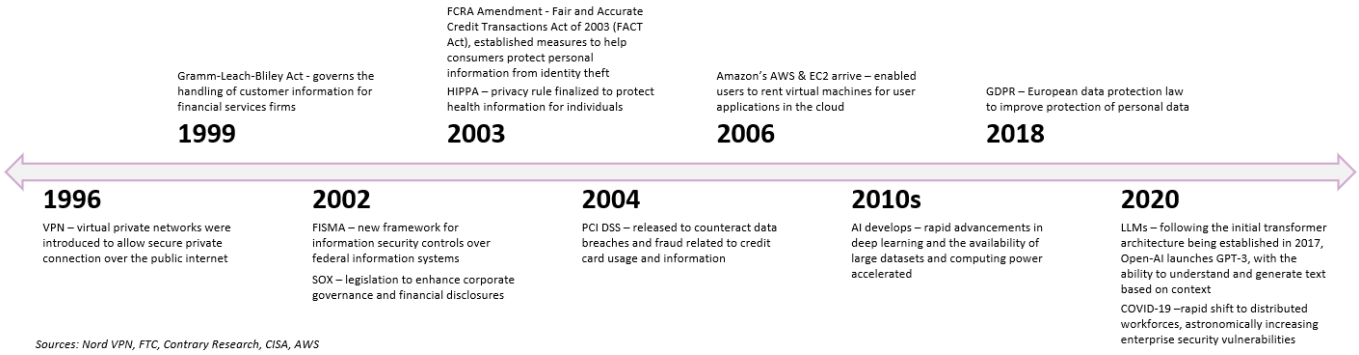
Identity sits at the core of every organization today. Businesses of all sizes are searching for the appropriate balance between security and modernization, aiming to empower employees for optimal productivity. While the foundation of modern workforce Identity and Access Management originated in the 1980s with the advent of the modern computer, still today, 80% of breaches are identity driven.[1]

Beginning with Novell, a pioneer in identity-based security, introduced NetWare, a technology designed to enable multiple PCs to share files and printers in business environments. NetWare leveraged Bindery, an authentication and resource management system, which later evolved into the Novell Directory Services (NDS) in 1993. The first iteration of the offering had a flat structure, as opposed to a directory tree, where administrative rights were all or nothing, with limited ability to adapt to new standards. These scalability issues opened the door for new entrants, most notably Microsoft, looking to serve companies globally. A primary driver of innovation came in the form of the LDAP, or Lightweight Directory Access Protocol, an open standard protocol making it easier for applications to integrate with directory services.[2]

LDAP was the first in a lineage of identity-based security protocols that proliferated into the Identity and Access Management (IAM) software ecosystem that exists today. As our economy and workforce become increasingly digitized, an ever-expanding list of digital identity issues arise. Therefore, business' new identity-based needs have been driven by two main categories:

1. New technologies creating monumental shifts in how businesses conduct work.
2. Stringent regulations concerning the management of key information.

See below for representative examples:



Sources: Nord VPN, FTC, Contrary Research, CISA, AWS

[1] Shastri, Venu. "Identity Protection: What It Is and Why You Need It - Crowdstrike." Crowdstrike.Com, 11 July 2023, www.crowdstrike.com/cybersecurity-101/identity-protection/.

[2] "What Is LDAP? All You Need to Know." OneLogin, www.onelogin.com/learn/what-is-ldap#:~:text=The%20Lightweight%20Directory%20Access%20Protocol,printers%2C%20LDAP%20is%20the%20answer. Accessed 31 July 2024.

When you combine these proceedings, with the extreme scale that identity platforms needed to cover, two additional categories of IAM formed at roughly the turn of the century. While the early players of IAM remained to form what we call Access Management, we gained two addition sub-segments, IGA, or Identity Governance and Administration, and PAM, or Privileged Access Management adding a full set of complementary tools for access governance and management of accounts with the most influential access.

What questions are IGA software companies answering?

1. How do individuals gain access to certain resources?
2. Do we have the right processes around granting access?
3. Can we map out the relationships between accounts and software?
4. Can we provide evidence of access controls that follow regulations and standards?

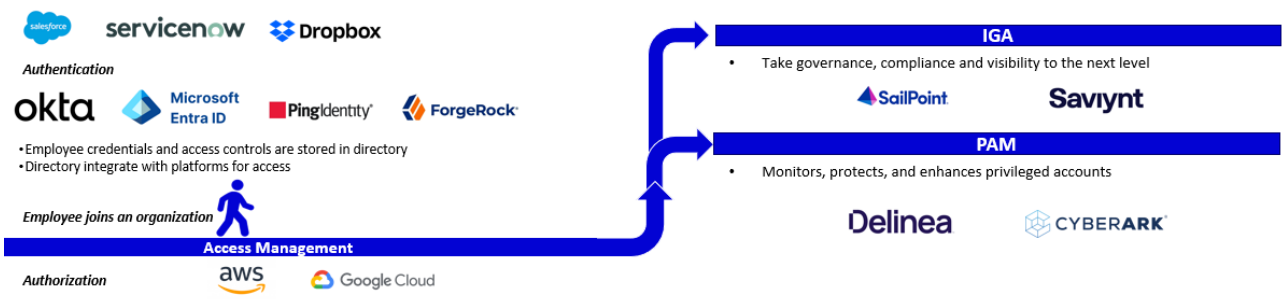
As these solutions have expanded, we have since seen improved details around access visibility, streamlined processes, provisioning, and expanded regulatory oversight. Simultaneously, Privileged Access Management technology materialized to offer increased security for privileged accounts or those with entry to the most critical systems, controls and, or information. These solutions often specialize in more technical resources such as cloud environments, infrastructure, and IT software.

What questions are PAM software companies answering?

1. Who has accounts with access to our foundational systems?
2. How can we monitor those critical accounts?
3. Can we elevate certain employees' accounts to those levels, even for just a brief period?
4. How secure are those specific accounts?

As these two segments took force, the strengthening of Access Management capabilities coincided. The most prominent advancements observed were Single Sign-On (SSO) and Multi-Factor Authentication (MFA). SSO, or federated access, enables users to maintain a single set of trusted credentials from an identity provider across various applications. This capability hinges on the support of authentication protocols for integrations. Additionally, MFA enhances security by requiring multiple verification factors, including one-time passcodes, phone calls, texts, push notifications, security keys, and biometric verification.

As outlined above, and illustrated below, the resulting landscape was a complete identity offering so organizations could address any identity related challenges they faced. By combining a precise access management platform with governance and privileged access tools, enterprises were well-equipped for success.



Moreover, identity platforms have become integral to workflows across various business units. While executives, managers, and other individuals may engage with these platforms periodically, the following teams leverage systems for core activities:

- Access Management
    - HR teams for onboarding and offboarding employees as well as ensuring individuals have the appropriate access.
    - IT administrators monitor user access and manage applications.
- Identity Governance and Administration
    - IT and Security Teams provision and de-provision users.
    - IT and Security Teams enforce policies and procedures.
    - Legal / Compliance teams execute access reviews and other compliance workflows.
- Privileged Access Management
    - IT and Security teams manage and monitor privileged accounts.
    - Developers and Product Managers are granted privileged access or receive brief elevated access for tasks or projects.
    - HR teams often require privileged access given connection to sensitive information.

Due to over 40 years of technological advancements and increased corporate recognition of access management's importance, we now have a continuously evolving landscape ripe with opportunities for innovation. At AVP, we believe that each facet of IAM deserves careful review due to its impact on organizational security, compliance, and efficiency. As outlined below by Gartner, each subsegment of IAM has continued to advance.

Comparison of IAM Suites
Via Gartner

As the digital landscape progresses, there is an ongoing demand for diverse, resilient identity security solutions. Of late we have observed growing attack surfaces, advancements in fraud capabilities, the establishment of remote work, and the exponential rise in AI and computing capabilities.

Starting with Access Management:

In our evaluation of Access Management, we explored two of the most identifiable incumbents, Microsoft and Okta. We have pinpointed the specific areas where these companies thrive, in addition to where there are opportunities to augment or replace solutions based on needs, trends, and use cases.

- Joining the identity market in 1999, Microsoft launched with its Active Directory, focusing on serving as a workforce system of record across networks. What multiplied the effectiveness of this solution was its correspondence with the debut of the Windows 2000 Server, representing significant progress in network scalability and performance.[3] Today Microsoft has maintained this stance as it offers Entra ID, a cloud based IAM solution to help support users with seamless access to its broader set of solutions and external providers. The platform offers multiple authentication methods (password-based, multi-factor, smart card, and certificate-based authentication), SSO, User Management, and developer features to enhance Azure capabilities.[4]
- Next comes Okta, founded in 2009, born out of the recognition that businesses were prepared to move to the cloud. When Microsoft struggled out of the gate to migrate its systems, Okta took advantage. Today, Okta thrives in its core offering, which includes an employee directory, SSO and MFA. They have also added controls around privileged access, supplementary workflows, and Customer Identity and Access Management (CIAM).[5]

Our findings suggest that these two players prioritize being the central store of employee credentials enabling SSO, MFA and scalability across organizations. That being said, many startups have identified areas of opportunity to complement Microsoft and Okta, or target organizations with unique needs.

- Extended Identity / Account Management – while Okta and Microsoft do a very good job at managing core applications like a CRM or ERP system, an enterprise workforce typically leverages hundreds of other applications. Managing integrations, account hierarchies, and relationships across these disparate applications can be complex. Companies like Grip, Silverfort, Cerby, Zluri, and Strata offer solutions like visibility, discovery, SSO, and MFA for incremental applications not integrated with your core identity provider. The lack of connectivity is typically due to cost, legacy technology, or business preferences. This need extends beyond software to physical identity and access, with companies like Oloid providing security solutions for physical access points.

---

[3] "Active Directory Extranet Adoption Fueled by Internet Scalability and Rapid Return on Investment." Stories, 8 May 2002, news.microsoft.com/2002/05/08/active-directory-extranet-adoption-fueled-by-internet-scalability-and-rapid-return-on-investment/.

[4] "Microsoft Entra - Secure Identities and Access: Microsoft Security." Microsoft Entra - Secure Identities and Access | Microsoft Security, www.microsoft.com/en-us/security/business/microsoft-entra. Accessed 29 July 2024.

[5] "Employee and Customer Identity Solutions." Okta, www.okta.com/. Accessed 29 July 2024.

Next is IGA

SailPoint and Saviynt are examples of two first movers in the enterprise market by focusing on comprehensive identity governance solutions tailored to the needs of large organizations. Growth has been driven by the ability to address intricate access management challenges, deliver robust compliance and security features, and most importantly scale effectively to support vast environments.

- SailPoint, founded in 2005, set out on a mission to "connect individuals with the resources and information they need to be productive and secure — enabling a trusted, frictionless user experience, regardless of device or location".[6] Over the years, SailPoint has both refined and expanded its focus to provide robust governance tools, evolving into a comprehensive identity security platform. The company began its journey by focusing primarily on provisioning, ensuring companies could address user lifecycle management. Today, SailPoint offers an all-encompassing suite of solutions across provisioning, governance, and identity, looking to support expansive organizations and cross functional purposes.
- Saviynt, established in 2010, emerged five years after SailPoint, at the outset of the cloud era. It has emphasized cloud, multi-cloud, and hybrid settings, for enterprises. Unlike SailPoint, which began with a strong emphasis on provisioning, Saviynt took the reverse approach initially prioritizing governance solutions, then significantly invested its provisioning capabilities.

IGA solutions offered by companies like SailPoint and Saviynt are often effective for enterprises due to their plentiful features and scalability. However, these solutions can be costly and often require collaboration with consulting firms to manage complex requirements and compliance intricacies. Core hurdles to value include intensive processes related to integrating with on-prem environments and legacy servers. As a result, there remain opportunities for start-ups, the mid-market, and more technologically advanced enterprises where businesses are cloud focused, API-based, and increasingly seeking automation and AI-driven capabilities. Moreover, the segment is ripe for solutions that offer advanced technology at a more accessible price point.

- Implementation / Automation – SailPoint and Saviynt's focus on enterprise solutions tend to result in lengthy implementation. A new crop of dynamic IGA companies has emerged such as ConductorOne, Lumos, Zilla, Securends, and ClearSkye who offer accelerated time to value through API-based integrations, out of the box capabilities, and workflow automation. In addition, these businesses differentiate themselves by branching outside of IGA to offer adjunct features like ConductorOne who has ventured in PAM, Lumos into SaaS management and Zilla into security posture management.
- SaaS-focused companies – Primarily focusing on SaaS businesses, this sub-sector of IGA also expands to IaaS (Infrastructure as a Service), PaaS (Platform as a Service), and AI. These organizations address unique challenges of managing identify across all cloud and SaaS assets without having to individually analyze and evaluate all changes in a dynamic environment. Companies like Oleria, who specializes in providing real time, adaptive access, creates an organizational graph to consolidate data across a company. Companies like Savvy, Obsidian, Valence, and Nudge are often classified as SSPM solutions (SaaS Security Posture Management) but offer user lifecycle controls and SaaS sprawl management features to limit the rampant dispersion of SaaS solutions within an organization.

---

[6] "Sailpoint." The Global Business Directory, 5 June 2024, businessabc.net/wiki/sailpoint-technologies#:~:text=History,in%20more%20than%2050%20countries.

Lastly, PAM

PAM is typically the most technical and granular part of IAM because it requires both administration and governance to monitor and protect prominent accounts. Even more than that, privileged accounts are spread across an organization ranging from IT accounts to administrative accounts to cloud service accounts to emergency accounts and many more.[7] CyberArk and Delinea are two tenured providers of PAM today, who have each taken distinct paths to reach their current positions.

- CyberArk, founded in 1999, initially aimed to secure a company's most sensitive data using its digital vault technology. The company has since expanded to cover privileged session management and monitoring and later cloud and DevOps tools to secure the most technologically advanced, critical environments. The latest progress has been in zero trust, the idea that regardless of network location or prior authentication, no devices, users, or applications should be trusted by default.[8]
- Delinea was officially formed in April 2021 through the merger of Thycotic and Centrify. Thycotic, founded in 1996, started as a consulting firm focused on improving IT departments. The business later developed its own software solutions focusing on automating discovery and management of privileged accounts.[9] Centrify, founded in 2004, focused on bridging management of Linux Environments with Microsoft Active Directory. The company later continued to supplement its offering with additional tools. In April 2021, the companies merged to form a comprehensive PAM platform and have pushed to take market share from CyberArk. The platform is a bit lighter weight focusing on securing credentials, remote access, entitlement elevation, and identity threat protection.

While CyberArk and Delinea have done well in capturing market share, many alternatives have emerged that are more commonly targeting startups, mid-market, and upper mid-market businesses looking to offer more specific PAM capabilities at relatively affordable prices. We have seen startups who have truly prioritized and embraced automation looking to enable seamless security experiences, along with startups focused on deepening integrations of PAM into a business' core identity stack with powerful governance features.

- Modern PAM – While CyberArk has excelled in offering a truly comprehensive platform for large global enterprises, the startup community recognized the opportunity in PAM to build a modern, cloud-native offering, prioritizing key PAM functions along with automation, integrations, and governance. Companies like Opal, Britive, Trustle, Axiom, and Ubyon have focused on improving automation around Just-in-Time Access Management and enhancing abilities for modern access controls. New entrants lean towards Just-in-Time access so privileged credentials are granted on demand and do not remain outstanding.
- Governance - There are also cloud-focused competitors prioritizing governance, compliance, and reporting. While companies like Teleport, and StrongDM have functionality that can apply to all different organizations, they have succeeded with sensitive industries like healthcare and financial services given their ability to support regulatory needs.

---

[7] Carson, Joseph. "Privileged Access Management Best Practices." Delinea, delinea.com/blog/privileged-access-management-best-practices. Accessed 30 July 2024.

[8] "Advancing Zero Trust with Privileged Access Management." BeyondTrust, www.beyondtrust.com/resources/whitepapers/advancing-zero-trust-with-pam. Accessed 30 July 2024.

[9] Netsurion. "Thycotic Secret Server Integration." Netsurion, 29 Mar. 2024, www.netsurion.com/data-source-integrations/thycotic-secret-server#:~:text=Thycotic%20Secret%20Server%20(SS)%20is,malicious%20activity%2C%20across%20the%20enterprise.

Conclusion

Ultimately, while the above outlines an in-depth look at the Identity and Access Management market, if there is anything that we've learned, it's that this market is perpetually evolving. The initial paradigm of IAM started with directories and improving connectivity for individuals and software. As technology advanced and regulations emerged, needs grew, leading to new market participants.

Startups have since developed, offering more targeted and modern products at accessible price points, reflecting the reality of today's diverse needs.

1. In Access Management, startups have found ways to augment incumbents' offerings.
2. In IGA and PAM, startups have prioritized cloud-focused customers of all sizes, looking for specific, advanced capabilities.

Despite this, the bulk of identity spend remains concentrated among enterprise players. Therefore, new entrants are betting on two key trends: the growth of modern, cloud-focused companies and the ongoing shift of enterprises to the cloud, prioritizing modernization, and efficiency, which will inevitably alter their requirements. In the end, as the IAM market continues its prominence, adaptability remains key for established and emerging organizations. Ongoing innovation highlights the importance of staying ahead of technological advancements and regulatory changes to meet the ever-changing needs of identity-based security.

We invest in great entrepreneurs.

We support outstanding companies.

New York - London - Paris

www.axavp.com