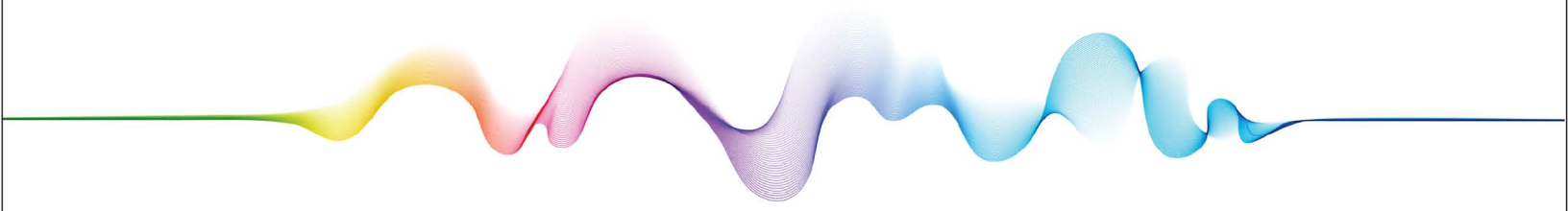
INSIGHT REPORT

OVERVIEW OF THE AUTHENTICATION COMMERCIAL MARKET



TAG CYBERSECURITY

TAG Insights Report: Overview of the Authentication Commercial Market

Prepared by
Dr. Edward Amoroso
Chief Executive Officer, TAG Infosphere
Research Professor, NYU
eamoroso@tag-cyber.com

Version 1.0
February 10, 2024

Introduction

This TAG Insights Report on *Authentication* is intended to help companies, managers, practitioners, researchers, investors, and commercial vendors better understand current trends, issues, and market opportunities in this area. A list of representative commercial vendors working in various areas of authentication is included. The five specific areas of covered in this report include:

1. Biometrics
2. Multifactor Authentication
3. Passwordless Authentication
4. Password Management
5. Single Sign-On

This report is intended for general and unrestricted use, but interested readers are encouraged to connect with the TAG research and advisory team for more information on the private TAG Research as a Service (RaaS) community that covers, discusses, and shares information on these topics in more depth and includes a wider range of startups, vendors, and companies.

TAG Taxonomy

We organize this TAG Insights Report as per our updated TAG Taxonomy which includes twenty categories of modern solution areas where stakeholders and buyers can find suitable commercial products and services for purchase and use. Each category has five subcategories

that correspond to the main areas in which practitioners can focus. These subcategories are discussed below.

1 Application Security 1.1 API Security 1.2 Application Security Testing 1.3 Application Security Posture Mgmt. 1.4 Runtime Application Security 1.5 SBOM/SCA	**6 Email Security** 6.1 Anti-Phishing Tools 6.2 DMARC 6.3 Email Encryption 6.4 Phish Testing and Training 6.5 Secure Email Gateway	**11 Identity and Access Management** 11.1 Authorization 11.2 IAM Platforms 11.3 identity, Anti-Fraud, and KYC 11.4 Identity Governance and Admin. 11.5 Privileged Access Management	**16 Operational Technology Security** 16.1 ICS/OT Device Security 16.2 ICS/OT Visibility 16.3 Unidirectional Gateway 16.4 Vehicle Security 16.5 Zero Trust OT
2 Attack Surface Management 2.1 Bug Bounty Services 2.2 External Attack Surface Management 2.3 Automated Pen Testing/Red Teams 2.4 Breach and Attack Simulation 2.5 Security Ratings Platforms	**7 Encryption and PKI** 7.1 Certification Authority (CA) 7.2 Data Encryption 7.3 Key and Secret Management 7.4 Key and Certificate Protection 7.5 Post-Quantum Cryptography	**12 Security Operations and Response** 12.1 Data Forensics and eDiscovery 12.2 Incident Response 12.3 SIEM Platforms 12.4 SOC/SOAR Support 12.5 Threat Hunting	**17 Security Professional Services** 17.1 Penetration Testing 17.2 Security Assessments 17.3 Security Research and Advisory 17.4 Security Training 17.5 Value Added Resellers
3 Authentication 3.1 Biometrics 3.2 Multifactor Authentication 3.3 Passwordless Authentication 3.4 Password Management 3.5 Single Sign-On	**8 Endpoint Protection** 8.1 Antivirus Software 8.2 Browser Isolation 8.3 Content Disarm and Reconstruction 8.4 Endpoint Detection and Response 8.5 Security Enhanced Browser	**13 Managed Security Services** 13.1 DDOS Security 13.2 Managed Detection and Response 13.3 Managed Security Services Platform 13.4 Network Detection and Response 13.5 XDR Services	**18 Software Lifecycle Security** 18.1 AI/MLOps Security 18.2 Container/Kubernetes Security 18.3 Container Scanning 18.4 DevSecOps Platforms 18.5 Infrastructure-as-Code Security
4 Cloud Security 4.1 Cloud Data Fragmentation 4.2 Cloud Infrastructure Entitlement Mgmt. 4.3 Cloud Security Posture Management 4.4 Cloud Workload Protection Platform 4.5 Microsegmentation	**9 Enterprise IT Infrastructure** 9.1 Asset Inventory 9.2 Backup Platform 9.3 Infrastructure Resilience 9.4 Physical Security 9.5 Secure Sharing and Collaboration	**14 Mobility Security** 14.1 IOT Security 14.2 Mobile App Security 14.3 Mobile Device Management 14.4 Mobile Device Security 14.5 Mobility Infrastructure Security	**19 Threat and Vulnerability Management** 19.1 Digital Risk Protection 19.2 Security Scanning 19.3 Third Party Risk Management 19.4 Threat and Vulnerability Platform 19.5 Threat Intelligence
5 Data Security 5.1 Cloud Data Security Posture Mgmt. 5.2 Data Access Governance 5.3 Data Discovery and Classification 5.4 Data Leakage Protection 5.5 Data Privacy Platform	**10 Governance, Risk, and Compliance** 10.1 Continuous Compliance 10.2 Cyber Insurance 10.3 Incident Reporting 10.4 GRC Platform 10.5 Risk Management Platform	**15 Network Security** 15.1 Network Access Control 15.2 Next Generation Firewalls 15.3 Secure Access Service Edge (SSE) 15.4 Virtual Private Networks 15.5 Zero Trust Network Access	**20 Web Security** 20.1 Bot Management 20.2 Content Security 20.3 Secure Web Gateway 20.4 Web Application Firewall 20.5 Website Scanning

Figure 1. TAG Taxonomy for Cybersecurity

Overview of Authentication Solutions

Modern authentication in the commercial market has seen significant advancements to address security concerns while prioritizing user convenience. These developments encompass various methods, including biometrics, multi-factor authentication (MFA), passwordless authentication, password management, and single sign-on (SSO). These techniques play a critical role in ensuring secure access to digital resources while simplifying the user experience.

- Biometric authentication leverages unique physical or behavioral traits, such as fingerprints, facial recognition, or iris scans, to verify a user's identity. Advancements in machine learning and image processing have improved accuracy and reliability in biometric authentication. During the authentication process, biometric data is securely stored and compared against templates, enhancing security.
- MFA enhances security by requiring users to provide multiple forms of identification. This typically involves something they know (like a password) and something they possess (like a smartphone or a hardware token). MFA solutions have become more user-friendly, offering options like mobile apps, SMS-based codes, or biometric verification as the second factor.
- Passwordless authentication eliminates the need for users to remember complex passwords. Instead, it relies on alternative methods, such as biometrics, hardware

tokens, or one-time codes sent via email or SMS. This approach enhances security by reducing password-related risks.

- Effective password management is crucial for security. Password managers enable users to generate, store, and autofill complex passwords for various accounts. These tools simplify the user experience while enhancing security by discouraging weak or reused passwords.
- SSO solutions enable users to access multiple applications and services with a single set of credentials. This reduces the need for users to manage multiple passwords, improving both security and convenience. SSO integrates with identity providers to streamline access control.

Focus Area: Biometrics

Biometrics in cybersecurity refers to the use of unique physical characteristics of individuals, such as fingerprints, facial recognition, iris patterns, and voice recognition, as security mechanisms to authenticate and authorize access to systems, devices, and data. This technology offers a higher level of security compared to traditional methods like passwords and PINs, which can be easily compromised. The focus on biometrics in cybersecurity is growing, as it provides a more user-friendly and secure method of authentication.

Biometric authentication systems function by capturing and storing an individual's biometric data, which is then used as a reference for future authentication attempts. When a user attempts to access a system or device, the biometric system compares the presented biometric data with the stored reference data. If the comparison is successful, access is granted; otherwise, it is denied.

Vendors in the biometric cybersecurity market provide various solutions and services. These range from hardware like fingerprint scanners and iris recognition cameras to software for processing and analyzing biometric data. These solutions often integrate with existing security systems to enhance authentication processes.

One of the critical aspects that vendors focus on is the accuracy and reliability of biometric systems. This involves ensuring a low false rejection rate (FRR), where legitimate users are incorrectly denied access, and a low false acceptance rate (FAR), where unauthorized users are incorrectly granted access. Advanced algorithms and machine learning techniques are employed to improve the accuracy of biometric systems.

Another crucial area is the protection of biometric data itself. Since biometric data is unique and permanent, its security and privacy are of utmost importance. Vendors implement robust encryption methods and secure storage solutions to protect biometric data from unauthorized access and breaches. They also comply with various data protection regulations to safeguard user privacy.

In addition, vendors are developing multimodal biometric systems that combine two or more biometric identifiers to enhance security and accuracy. For example, a system may require both fingerprint and facial recognition to authenticate a user, thereby reducing the chances of unauthorized access.

Integration and interoperability with other security systems are also a focus for vendors. They provide solutions that can easily integrate with a range of systems and platforms, ensuring that biometric security can be broadly applied across different applications and industries.

Focus Area: Multi-Factor Authentication (MFA)

Multifactor Authentication (MFA) is a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction. This approach to cybersecurity is designed to create a layered defense, making it more difficult for an unauthorized person to access a target, such as a physical location, computing device, network, or database. In essence, if one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

The three main categories of factors used in MFA are: something the user knows (knowledge), something the user has (possession), and something the user is (inherence). Knowledge factors include things like passwords and PINs, possession factors include things like mobile devices or smart cards, and inherence factors are biometrics, such as fingerprints or facial recognition.

Cybersecurity vendors play a crucial role in supporting MFA by providing a range of solutions and technologies. These include hardware tokens, which generate a one-time password (OTP); SMS-based verification codes sent to a user's mobile device; software tokens or apps that generate OTPs; and biometric systems, such as fingerprint or iris scanners.

One of the primary focuses for vendors in the MFA space is to balance security with user convenience. Overly complex MFA systems can lead to user frustration and resistance, which in turn can undermine security protocols. Therefore, vendors often emphasize the development of user-friendly MFA solutions that are easy to implement and use.

Vendors also concentrate on the integration capabilities of their MFA solutions, ensuring that they can be seamlessly integrated with a wide range of existing systems and platforms. This includes compatibility with various operating systems, cloud services, and enterprise applications. Such integration is crucial for businesses that need a flexible and scalable security solution that can be adapted to their specific needs.

Another critical aspect is the reliability and scalability of MFA solutions. Vendors must ensure that their systems are capable of handling a high volume of authentication requests without failures or significant delays, which is crucial in large organizations with many users.

Additionally, vendors are continuously working on advancing the security features of MFA solutions to stay ahead of evolving cyber threats. This involves implementing the latest encryption standards, continuously updating their algorithms, and conducting regular security audits. A major recent issue has been the implementation of phishing-resistant MFA, which is often accomplished in the context of passwordless authentication (see below).

Focus Area: Passwordless Authentication

Passwordless authentication, incorporating technologies such as FIDO (Fast Identity Online) protocols, is a progressive approach in cybersecurity. This methodology facilitates user access to systems and data without relying on traditional password-based logins. By leveraging FIDO standards, passwordless authentication systems enhance security and user experience by employing biometrics, security tokens, or SMS codes. Passwordless authentication is also generally a good foundation for reducing the risk of phishing.

FIDO protocols, developed by the FIDO Alliance, are key in driving the adoption of passwordless authentication. They provide a standardized framework for stronger authentication methods, such as public key cryptography, where a private key held by the user is paired with a public key stored on the server. This mechanism, utilized in FIDO2 – the latest set of specifications – allows for secure and convenient user authentication without transmitting sensitive information.

Biometric authentication is a widely used passwordless method, employing fingerprints, facial recognition, iris scans, or voice recognition. These biometric methods align well with FIDO standards, particularly in ensuring that biometric data remains localized on the user's device, enhancing privacy and security. However, deploying biometric systems requires careful consideration of privacy and data security, given the sensitive nature of biometric data.

Security tokens, including hardware and software-based varieties, are another avenue for passwordless authentication aligned with FIDO protocols. Hardware tokens, like USB keys or smart cards, offer physical devices for authentication, while software tokens generate a one-time code. These tokens, often used in conjunction with FIDO's multifactor authentication requirements, provide an added layer of security.

SMS and email-based authentication, sending a one-time passcode to a user's device, is simpler but potentially less secure. However, when combined with FIDO's framework, the security of these methods can be significantly enhanced, often being part of a multifactor authentication strategy.

Cybersecurity vendors play a crucial role in supporting FIDO-based passwordless authentication. They offer solutions incorporating user management and authentication software, along with necessary hardware for biometric or token-based systems. These vendors focus on compatibility across various devices and operating systems, ensuring seamless integration with existing IT infrastructures.

A critical challenge for these vendors is to balance security with usability. FIDO's passwordless systems aim to be user-friendly to encourage adoption, while providing robust security to prevent unauthorized access. This involves creating intuitive user interfaces and smooth experiences without compromising security features.

Vendors ensure their solutions comply with data protection regulations, a crucial aspect given the sensitive data involved in passwordless authentication. Implementing strong encryption and security measures to protect user data is a standard practice.

Focus Area: Password Management

Password management is a fundamental aspect of cybersecurity, focusing on the secure creation, storage, and management of passwords. In an era where digital security threats are rampant, efficient password management is essential for protecting user credentials and sensitive data. Vendors in the cybersecurity domain offer various password management solutions to address these needs, ensuring robust security and user convenience.

A primary function of password management systems is to facilitate the generation of strong, unique passwords. These systems use algorithms to create complex passwords that are difficult to guess or crack. This mitigates risks associated with common password-related vulnerabilities, such as weak, easily guessable, or reused passwords across multiple accounts.

Vendors provide password management tools that securely store and organize passwords. These tools typically use encrypted databases to keep password data safe. Users can access their passwords through a master password, which is the only password they need to remember. Advanced systems employ additional security measures such as two-factor authentication (2FA) for accessing the password vault, adding an extra layer of security.

Integration is a critical feature of password management solutions. Vendors ensure that their tools can integrate with various browsers and operating systems, allowing for seamless auto-fill capabilities for stored credentials. This not only improves security by reducing the likelihood of typing passwords into phishing sites but also enhances user convenience.

Security of stored data is paramount in password management. Vendors employ robust encryption standards, such as AES (Advanced Encryption Standard), to protect password databases. This encryption ensures that even if data is intercepted or the system is breached, the contents remain inaccessible without the decryption key.

In addition to secure storage, password management solutions often include features for monitoring and alerting users about potential security risks, such as breached or weak passwords. They can prompt users to change passwords regularly and alert them if their credentials have been compromised in a known security breach.

Scalability and user management are crucial for enterprise environments. Vendors offer password management solutions that cater to businesses, providing administrative controls for user and password policies, user group segmentation, and audit trails for compliance purposes. Vendors also focus on the user experience, ensuring that their password management solutions are intuitive and easy to use. A straightforward interface encourages adoption and consistent use, which is critical for maintaining security protocols.

Continuous support and updates are an integral part of the services provided by vendors. As cybersecurity threats evolve, vendors regularly update their password management solutions to address new vulnerabilities and enhance functionality.

Focus Area: Single Sign-On (SSO)

Single Sign-On (SSO) is a cybersecurity solution that allows users to access multiple applications or services with a single set of login credentials. This approach simplifies the user authentication process while enhancing security and reducing the risk of password-related breaches. SSO is increasingly vital for organizations managing numerous applications across various platforms.

SSO works by authenticating the user for all the applications they have been granted access to, eliminating the need to log in separately to each service. This process involves a central authentication server, which validates the user’s identity and provides tokens or assertions to the services, confirming the user's authentication. When a user attempts to access an application, the application requests authentication from the SSO server, which then responds based on the user's current authentication status.

Vendors in the field of cybersecurity provide SSO solutions to streamline access management across an organization. These solutions typically support various authentication protocols such as SAML (Security Assertion Markup Language), OAuth, and OpenID Connect, ensuring compatibility with a wide range of applications, including cloud-based and on-premise systems.

One of the main benefits of SSO from a security perspective is the reduction in the attack surface. By minimizing the number of credentials required, there is less risk of password theft or loss. Additionally, SSO solutions often integrate with other security mechanisms like multi-factor authentication (MFA) to enhance security. This integration allows organizations to implement a layered security approach, combining the convenience of SSO with the robustness of MFA.

Vendors also focus on the scalability and flexibility of their SSO solutions, ensuring they can accommodate the growing and changing needs of organizations. This includes supporting a diverse range of user roles and access levels, as well as the ability to easily add or remove applications from the SSO ecosystem.

Furthermore, compliance with data privacy and security regulations is a critical consideration. Vendors ensure that their SSO solutions comply with standards such as GDPR, HIPAA, and CCPA. They implement robust encryption for data in transit and at rest, along with audit trails and reporting features for compliance monitoring and management.

User experience is another key aspect of SSO solutions. Vendors strive to provide seamless and intuitive interfaces, minimizing login friction and enhancing productivity. By reducing the need for multiple passwords, SSO can significantly decrease the likelihood of password fatigue and the security risks associated with it.

Continuous support and updates are essential for maintaining the effectiveness of SSO solutions. Vendors provide regular updates to address emerging security threats and enhance functionality, along with support services to assist with implementation, troubleshooting, and optimization.

Companies and Contributions

The companies listed below emerged as part of our research at TAG. Our goal in listing these fine firms is to provide a starting point for buyers, advocates, stakeholders, and researchers trying to make sense of the commercial landscape for authentication as a means for driving toward a more secure global ecosystem.

Biometrics Vendors

1. 1Kosmos: 1Kosmos is an identity security and management company that provides digital identity proofing and biometrics in support of passwordless authentication.
2. Accops: Accops enables secure and instant remote access to business applications from any device and network.
3. BioCatch: BioCatch uses behavioral biometrics to detect fraudulent activities and enhance security.
4. BioConnect: BioConnect offers biometric solutions for physical and digital access control.
5. Daon: Daon provides advanced biometric authentication and identity assurance solutions.
6. FacePhi: FacePhi offers a range of facial recognition technologies for mobile and web authentication.
7. FaceTec: FaceTec provides advanced facial recognition software for secure user authentication.
8. Fulcrum Biometrics: Fulcrum Biometrics (A Fujitsu Company) offers a range of biometric solutions, including fingerprint and facial recognition.
9. HID Global: HID Global provides a range of identity and access solutions including smart cards, readers, RFID tags, and software.
10. Idemia: Idemia specializes in identity verification and offers biometric authentication solutions like facial recognition and fingerprint scanning.
11. ImageWare Systems: ImageWare Systems specializes in multi-modal biometric authentication solutions.

12. Innovatrics: Innovatrics provides fingerprint recognition and facial biometrics technology.
13. Iris ID: Iris ID offers advanced iris recognition technology for biometric authentication applications.
14. LexisNexis Risk Solutions: LexisNexis Behaviosec provides a biometric authentication solution based on behavioral attributes such as typing and clicking patterns.
15. NEC Corporation: NEC offers biometric solutions, including facial recognition and fingerprint authentication.
16. Neurotechnology: Neurotechnology specializes in biometric algorithms and software development.
17. SensibleVision: SensibleVision provides facial recognition technology for secure authentication.
18. Socure: Socure provides social biometric solutions for identity verification and on-line fraud detection.
19. TypingDNA: TypingDNA provides two factor authentication based on typing bio-metric analysis.
20. Veridium: Veridium offers biometric authentication solutions using face, fingerprint, and behavioral biometrics.
21. VU Security: VU Security provides two-factor authentication solutions with behavioral analysis for many different platforms.
22. ZKTeco: ZKTeco offers biometric hardware and software solutions, including fingerprint and facial recognition devices.

Multi-Factor Authentication (MFA) Vendors

1. Authy: Authy provides cloud-based MFA solutions and mobile application authentication.
2. CyberArk: CyberArk specializes in the provision of privileged access security and MFA solutions.
3. Duo Security: Duo Security offers MFA solutions, including two-factor authentication (2FA) and zero-trust security.
4. Entrust: Entrust offers secure identity and MFA solutions for enterprise.
5. JumpCloud: JumpCloud offers multi-factor authentication (MFA) with JumpCloud MFA and JumpCloud Protect.
6. ManageEngine: ManageEngine ADSelfService Plus is an identity security solution with MFA, single sign-on (SSO), and self-service password management capabilities.
7. NortonLifeLock: Symantec (Broadcom) offers a range of MFA and identity protection services.
8. Okta: Okta offers an industry-leading identity and access management platform which includes MFA.
9. OneLogin: OneLogin provides customers with identity and access management, including MFA.
10. Ping Identity: Ping Identity specializes in identity and access management solutions, including MFA.

11. RSA Security: RSA Security provides a range of advanced MFA and identity verification solutions.
12. SecureAuth: SecureAuth provides adaptive MFA and identity security solutions for enterprise.
13. Thales: Gemalto, part of Thales Group, offers MFA and secure access solutions.
14. Trusona: Trusona offers customers with passwordless MFA solutions for secure authentication.
15. WALLIX: WALLIX solutions offer identity, access, and data cyber security.

Passwordless Authentication Vendors

1. 1Kosmos: 1Kosmos provides digital identity proofing and biometrics in support of passwordless authentication.
2. Accops: Accops enables secure and instant remote access to business applications from any device and network.
3. Axiad: Axiad is a provider of cloud-based passwordless authentication and secure interactions for users and machines.
4. Banyan Security: Banyan Security offers passwordless access solutions and zero-trust network security.
5. Beyond Identity: Beyond Identity offers passwordless authentication solutions using cryptographic tokens and mobile device security.
6. HYPR: HYPR specializes in passwordless multi-factor authentication using biometrics and mobile device security.
7. ID R&D: ID R&D offers advanced biometric and voice recognition for passwordless authentication.
8. Jamf: Jamf provides ZTNA and mobile device management (MDM) solutions for Apple devices.
9. Keyless: Keyless offers passwordless biometric authentication with privacy-preserving technology.
10. LoginRadius: LoginRadius CIAM solution that provides a set of APIs to enable authentication, single sign-on, user management, data and account protection capabilities.
11. Microsoft: Microsoft provides its Windows Hello utility which is used for passwordless security by a wide range of users.
12. My1Login: My1Login provides identity and access management for enterprises.
13. Nok Nok Labs: Nok Nok Labs specializes in passwordless authentication and strong customer authentication.
14. Ping Identity: Ping Identity provides single sign-on and identity management solutions with emphasis on mobile access to the cloud.
15. Prove: Prove is a mobile and digital identity authentication solutions provider.
16. Secret Double Octopus: Secret Double Octopus offers passwordless multi-factor authentication solutions.
17. SecureAuth: specializes in continuous behavioral authentication and passwordless access contro.

18. Thales: Thales offers passwordless solutions with a comprehensive suite of tools to address security concerns.
19. Transmit Security: Transmit Security offers a platform that supports modern passwordless authentication solutions.
20. Trusona: Trusona offers passwordless MFA solutions, replacing traditional passwords with biometric authentication and secure tokens.
21. Typing DNA: TypingDNA provides two factor authentication based on typing bio-metric analysis.
22. Veridium: Veridium provides advanced passwordless authentication solutions using biometrics.
23. XTN Cognitive Security: XTN Cognitive Security provides behavioral biometrics for passwordless authentication.
24. Yubico: Yubico provides a hardware authentication solution that supports password-less multi-factor authentication.

Password Management Vendors

1. 1Password: 1Password offers secure password management and identity protection tools.
2. Avatier: Avatier Password Management is a self-service password reset based on Docker containers.
3. BeyondTrust: BeyondTrust Password Safe allows customers to discover, manage, audit, and monitor privileged accounts of all types.
4. Bitwarden: Bitwarden is a password manager that helps users store and manage your passwords securely
5. Cyclonis Password Manager: Cyclonis offers password management and encrypted vault solutions.
6. Dashlane: Dashlane's password manager allows users to pinpoint password hygiene problems, encourage action, and track changes over time.
7. F-Secure: F-Secure provides a range of anti-virus, Internet security, and password management products for companies and individuals.
8. KeePass: KeePass is a popular open-source password manager for individuals and small teams.
9. Keeper Security: Keeper secures business passwords to prevent data breaches, and meet compliance standards.
10. LastPass: LastPass (LogMeIn)Password Manager helps with creating, remembering and filling in passwords.
11. LogMeOnce: LogMeOnce provides password management, identity protection, and secure access solutions.
12. My1Login: My1Login provides identity and access management for enterprise.
13. One Identity: One Identity provides identity and access management.
14. Passbolt: Passbolt offers a range of open-source password management solutions for teams.

15. Click Studios: Click Studios offers Passwordstate an on-premise web based solution for Enterprise Password Management.
16. RoboForm: RoboForm stores all passwords and login information in an encrypted vault.
17. Sticky Password: Sticky Password is a password management solution designed to store and manage users' passwords and sensitive information.
18. TeamPassword: TeamPassword is a password management tool specifically designed for teams and businesses.
19. Delinea: Delinea offers privileged access management services and solutions for customers to discover, manage, and provision access to accounts and endpoints.
20. Zoho: Zoho's password management product, Zoho Vault, is a centralized solution designed to help businesses store, share, and manage their passwords and sensitive information.

Single Sign-On (SSO) Vendors

1. Accops: Accops HySecure is a Zero Trust-based Application Access Gateway that enables employees to connect into corporate apps and desktops as well as access private applications.
2. Arcon: ARCON SSO offers one-time administrative access to disparate technology platforms.
3. Authen2cate: Authen2cate's Single Sign-On (SSO) solution allows you to use one set of login credentials to access your custom portal.
4. Avatier: Identity Anywhere SSO is a Single-Sign On service based on Docker containers.
5. AuthO: Auth0, part of Okta, provides identity and access management, including SSO.
6. Duo Security: Duo Security, part of Cisco, offers multi-factor authentication and SSO.
7. F5 Networks: F5 Access Policy Manager offers SSO and secure access solutions.
8. Google: Google Cloud Identity offers SSO and identity management for enterprises.
9. IBM: IBM Security Verify provides SSO and identity management solutions.
10. JumpCloud: JumpCloud provides a cloud-based directory service and SSO solutions.
11. LastPass: LastPass (LogMeIn) provides popular password management and SSO solutions.
12. LoginRadius: LoginRadius SSO allows your customers to access any of your web properties, mobile apps, and third-party systems with a single identity.
13. Microsoft: Azure Active Directory offers cloud based SSO and identity services.
14. My1Login: My1Login SSO integrates with Active Directory to allow user access to their apps on their laptop, desktop or mobile phone.
15. Okta: Okta provides an identity and access management platform which includes SSO solutions.
16. One Identity: One Identity's (Quest Software) OneLogin provides SSO and identity management solutions.
17. Opentext: (formerly Micro Focus) offers identity governance and SSO solutions.
18. Optimal IdM: Optimal IdM is a provider of virtual cloud identity management solutions.
19. PingIdentity: PingIdentity specializes in identity and access management solutions, including SSO.

20. SailPoint: SailPoint specializes in the provision of identity governance and SSO solutions for enterprise.
21. SecureAuth: SecureAuth provides an identity management solution that supports enterprise requirements for single sign-on and two-factor authentication for mobile, web, and cloud applications.
22. Thales: Cloud single sign on (SSO) offers easy access to cloud applications by letting users log in to all their cloud apps with a single identity.

About TAG

TAG is a trusted next generation research and advisory company that utilizes an AI-powered SaaS platform to deliver on-demand insights, guidance, and recommendations in cybersecurity, artificial intelligence, and sustainability to enterprise teams, government agencies, and commercial vendors.