+44 20 8123 2220
info@marketpublishers.com

Advanced Authentication Market – Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented by Authentication Method (Smart Cards, Biometrics, Mobile Smart Credentials, Tokens, User-based Public Key Infrastructure), End-user Industry (BFSI, Healthcare, Government, Defense, IT, and Telecom), By Region, Competition 2018-2028

https://marketpublishers.com/r/AA017CE2C922EN.html
Date: November 2023
Pages: 185
Price: US$ 4,900.00 (Single User License)
ID: AA017CE2C922EN

Abstracts

Global Advanced Authentication Market was valued at USD 14.02 Billion in 2022 and is anticipated to project robust growth in the forecast period with a CAGR of 12.83% through 2028, Factors driving the Advanced Authentication Market include increased adoption of mobility, and enterprises are feeling pressure to enable employees, partners, and other stakeholders to access more sensitive information. Security threats have been increasing continuously. Hackers are finding new ways to steal data, while new viruses are being developed to steal sensitive information from enterprises and individual users. With most users now preferring to perform transactions online, it becomes imperative for the organization to deploy authentication solutions that help ensure convenient and secure access.

Key Market Drivers

Increasing Cybersecurity Threats

The persistent and ever-evolving landscape of cybersecurity threats is a primary driving force behind the growth of the global advanced authentication market. As cybercriminals become more sophisticated and relentless in their attacks, organizations are increasingly recognizing the critical importance of deploying advanced

+44 20 8123 2220
info@marketpublishers.com

authentication solutions to protect their sensitive data and digital assets. One of the key drivers is the escalating frequency and severity of cyberattacks. From ransomware and phishing attacks to data breaches and identity theft, organizations of all sizes and industries are facing a barrage of threats. Advanced authentication, particularly multifactor authentication (MFA) and biometric recognition, provides an extra layer of defense against these attacks. MFA, which requires users to provide multiple forms of verification, such as a password and a fingerprint scan, significantly reduces the risk of unauthorized access, even if one authentication factor is compromised.

Another driver is the increasing sophistication of cyber threats. Attackers are employing advanced tactics, techniques, and technologies to breach security systems and exploit vulnerabilities. Traditional password-based authentication methods are proving inadequate against these advanced threats. Advanced authentication solutions offer more robust protection by utilizing cutting-edge technologies like facial recognition, voice recognition, and behavioral analytics, making it significantly more challenging for cybercriminals to gain unauthorized access. Remote work and the expansion of digital services have also amplified the attack surface for cyber threats. With employees accessing company networks and data from various locations and devices, the need for secure authentication has become paramount. Advanced authentication methods can be seamlessly integrated into remote work environments, ensuring that only authorized individuals can access critical resources.

Furthermore, compliance with data protection regulations, such as GDPR and HIPAA, is driving the adoption of advanced authentication. Organizations must implement strong security measures to safeguard sensitive customer and employee data or face substantial fines and legal consequences for non-compliance. In conclusion, the relentless growth in cybersecurity threats is a powerful catalyst for the global advanced authentication market. Organizations across industries are investing heavily in advanced authentication solutions to fortify their security defenses, protect against data breaches, and ensure regulatory compliance. As cyber threats continue to evolve, advanced authentication will remain an essential component of any comprehensive cybersecurity strategy, driving the market's expansion in the years to come.

Regulatory Compliance

Regulatory compliance plays a pivotal role in driving the growth of the global advanced authentication market. As governments and regulatory bodies worldwide introduce increasingly stringent data protection and cybersecurity regulations, organizations are compelled to invest in advanced authentication solutions to achieve and maintain

compliance. One of the most significant regulatory frameworks influencing this market is the European Union's General Data Protection Regulation (GDPR). GDPR imposes strict requirements on how organizations collect, process, and protect personal data. It mandates the implementation of robust security measures to safeguard the privacy of individuals. Advanced authentication, particularly multifactor authentication (MFA) and strong access controls, is essential for complying with GDPR's security provisions. Organizations handling EU citizens' data must ensure that only authorized personnel have access to sensitive information, and advanced authentication methods are a key tool in achieving this goal.

In addition to GDPR, various regional and industry-specific regulations also mandate advanced authentication. For example, the Health Insurance Portability and Accountability Act (HIPAA) in the United States requires healthcare organizations to secure patient data. Similarly, the Payment Card Industry Data Security Standard (PCI DSS) demands stringent authentication and access controls to protect credit cardholder data. Financial institutions are another sector heavily impacted by regulatory compliance. Regulations like the New York Department of Financial Services' (NYDFS) Cybersecurity Regulation and the Basel III framework for banking impose strict cybersecurity requirements, including advanced authentication, to protect financial systems and customer data.

Furthermore, as organizations expand their global reach, they must navigate a complex web of international data protection laws, such as the California Consumer Privacy Act (CCPA) and Brazil's Lei Geral de Prote??o de Dados (LGPD). Advanced authentication solutions that can be tailored to meet the specific requirements of different jurisdictions and industries are in high demand. The consequences of non-compliance with these regulations can be severe, including substantial fines, legal liabilities, and reputational damage. Consequently, organizations are increasingly recognizing that advanced authentication is not only a security necessity but also a legal and regulatory imperative. This awareness is driving substantial investments in advanced authentication technologies and services, propelling the global advanced authentication market to continued growth as organizations strive to ensure compliance with evolving regulatory landscapes.

Bring Your Own Device (BYOD) and Remote Work

The adoption of Bring Your Own Device (BYOD) policies and the prevalence of remote work have emerged as major drivers propelling the growth of the global advanced authentication market. These trends have fundamentally transformed the way

+44 20 8123 2220
info@marketpublishers.com

organizations operate, making security a paramount concern. Advanced authentication solutions have become indispensable in addressing the unique security challenges posed by BYOD and remote work environments. BYOD, which allows employees to use their personal devices for work-related tasks, offers numerous benefits, including increased productivity and flexibility. However, it also introduces significant security risks. With a diverse range of devices accessing corporate networks and data, organizations are vulnerable to unauthorized access, data breaches, and other cybersecurity threats. Advanced authentication solutions provide a robust defense against these risks by ensuring that only authorized users gain access to sensitive resources.

Remote work, accelerated by the COVID-19 pandemic, has become a permanent fixture in the modern work landscape. This shift has further underscored the importance of advanced authentication. Remote employees accessing corporate networks and cloud-based applications require secure and convenient authentication methods. Advanced authentication methods, such as multifactor authentication (MFA), biometrics, and token-based systems, offer enhanced security while accommodating the needs of remote workers. MFA, for instance, combines multiple authentication factors, such as something the user knows (password), something the user has (smartphone or token), and something the user is (biometric data like fingerprints or facial recognition). This multi-layered approach significantly reduces the risk of unauthorized access, even in remote work scenarios.

Moreover, the growth of cloud-based services and applications further necessitates advanced authentication. Cloud adoption allows employees to access corporate data and applications from anywhere, but this convenience must be balanced with robust security measures. Advanced authentication seamlessly integrates with cloud services, adding an additional layer of security to protect sensitive data stored in the cloud. As BYOD and remote work continue to shape the modern workplace, organizations are recognizing the imperative need for advanced authentication solutions. They understand that safeguarding their digital assets and sensitive information requires not only flexibility but also uncompromising security. Consequently, the global advanced authentication market is poised for sustained growth, driven by the ever-evolving demands of a mobile, remote, and digitally connected workforce.

Key Market Challenges

User Resistance

+44 20 8123 2220
info@marketpublishers.com

User resistance represents a significant challenge that has the potential to impede the growth of the global advanced authentication market. This resistance arises from various factors, including user preferences, perceptions, and concerns about the usability and security of advanced authentication methods. One of the key reasons for user resistance is the perceived inconvenience of advanced authentication. Many advanced authentication methods, such as biometric recognition (e.g., fingerprint or facial recognition) and token-based systems, introduce additional steps or requirements for users during the login process. Users may find these methods more time-consuming or complex than traditional password-based authentication. This perception of inconvenience can lead to frustration and resistance, as users are often resistant to change that disrupts their established routines and workflows.

Privacy concerns also contribute to user resistance. Biometric authentication methods, in particular, require the collection and storage of sensitive personal data, such as fingerprints or facial scans. Users may be apprehensive about how their biometric data is handled, stored, and potentially shared. Privacy breaches or data misuse incidents can further erode trust in these systems, leading to reluctance to adopt advanced authentication methods. Moreover, some users express concerns about the security of advanced authentication technologies. While these methods are generally more secure than traditional passwords, they are not immune to vulnerabilities and attacks. Users may worry about the possibility of biometric data theft or replication, which could potentially compromise their security. This fear can deter users from embracing advanced authentication methods.

False Positives and Negatives

False positives and false negatives are significant challenges that have the potential to hamper the global advanced authentication market. These errors can undermine the effectiveness and user trust in advanced authentication methods, creating barriers to adoption and hindering the market's growth. False positives occur when an advanced authentication system incorrectly authenticates an unauthorized user as an authorized one. In other words, the system incorrectly accepts access to an application or system. This can result from various factors, such as inaccurate biometric readings or issues with token-based authentication. When users experience false positives, they may become frustrated and lose trust in the authentication system's reliability, which can lead to reluctance in adopting or continuing to use such methods.

On the flip side, false negatives happen when an authentication system incorrectly rejects an authorized user. This can occur when biometric data is not recognized

+44 20 8123 2220
info@marketpublishers.com

correctly, or tokens fail to authenticate the user due to issues like low battery or technical glitches. False negatives can cause user inconvenience and delay access to critical systems, impacting productivity and user satisfaction. Several factors contribute to false positives and false negatives in advanced authentication systems: Biometric Variability: Biometric authentication, such as fingerprint or facial recognition, can be affected by factors like lighting conditions, injuries, or changes in appearance, leading to errors. Environmental Factors: Token-based authentication methods, like smartcards or tokens, can be affected by environmental factors, such as damage or electromagnetic interference, leading to authentication failures.

Algorithm Accuracy: The accuracy of the algorithms used in authentication systems plays a crucial role in minimizing false positives and negatives. Less accurate algorithms can result in more errors. User Training: Users may not be adequately trained on how to use certain authentication methods correctly, leading to errors in the authentication process. System Updates and Maintenance: Lack of regular updates and maintenance of authentication systems can introduce vulnerabilities and increase the likelihood of errors. To mitigate the impact of false positives and negatives on the global advanced authentication market, several measures can be taken: Continuous Improvement: Vendors should invest in research and development to improve the accuracy and reliability of authentication methods.

User Education: Users should receive training and guidance on how to use advanced authentication methods effectively. Redundancy: Implementing backup authentication methods can help users gain access in case of false negatives. Regular Maintenance: Organizations should ensure that authentication systems are regularly updated and maintained to minimize errors. Adaptive Authentication: Systems that learn from user behavior over time can reduce the occurrence of false positives and negatives. Addressing false positives and negatives is crucial for the continued growth and success of the advanced authentication market. Users and organizations need to have confidence in the reliability and accuracy of these authentication methods to fully embrace their potential for enhanced security.

Privacy Concerns

Privacy concerns represent a significant obstacle to the growth and widespread adoption of advanced authentication technologies, which may ultimately hamper the global advanced authentication market. As organizations and individuals increasingly turn to advanced authentication methods for enhanced security, they are met with valid apprehensions regarding the collection, storage, and potential misuse of sensitive

+44 20 8123 2220
info@marketpublishers.com

personal information, particularly in the context of biometric authentication.

One of the primary privacy concerns surrounding advanced authentication is the storage and protection of biometric data. Biometric authentication methods, such as fingerprint recognition, facial recognition, and iris scans, require the capture and storage of unique physical or behavioral characteristics of individuals. Users worry that if this biometric data is not adequately protected, it could be vulnerable to theft or misuse by malicious actors. High-profile data breaches have demonstrated that even large organizations can fall victim to cyberattacks, raising valid questions about the security of stored biometric data.

Additionally, there are concerns related to the long-term implications of using biometric authentication. Once biometric data is compromised, it cannot be easily changed or reset, unlike passwords or tokens. This makes individuals hesitant to entrust their biometric information to systems that may not be foolproof or adequately safeguarded. Furthermore, the fear of surveillance and tracking through biometric data usage can lead to resistance among users. Concerns about how and where biometric data is used, including potential government surveillance and tracking by private companies, contribute to apprehension and mistrust.

To address these privacy concerns and foster greater trust in advanced authentication technologies, several steps can be taken, Transparency: Organizations should be transparent about how biometric data is collected, stored, and used. Clear and concise privacy policies should be communicated to users. Data Encryption: Employ robust encryption methods to protect stored biometric data. Encryption helps ensure that even if data is breached, it remains unreadable to unauthorized parties. User Consent: Obtain informed consent from users before collecting and using their biometric data. Users should have the choice to opt-in or opt-out of biometric authentication. Regulatory Compliance: Adhere to relevant data protection regulations, such as GDPR or HIPAA, to demonstrate a commitment to safeguarding user privacy. User Control: Provide users with control over their biometric data, allowing them to delete or modify stored data as needed. Security Measures: Continuously invest in cybersecurity measures to protect biometric data against unauthorized access or breaches. While privacy concerns undoubtedly pose challenges, they also present an opportunity for organizations to differentiate themselves by prioritizing user privacy and data security. By addressing these concerns proactively and transparently, the advanced authentication market can mitigate potential setbacks and continue to thrive as a vital component of modern cybersecurity.

+44 20 8123 2220
info@marketpublishers.com

Key Market Trends

Biometric Authentication Dominance

The dominance of biometric authentication is serving as a major catalyst driving the growth of the global advanced authentication market. Biometric authentication methods, which leverage unique physiological or behavioral traits like fingerprints, facial features, or iris patterns, are emerging as the frontrunners in identity verification for both consumers and enterprises. The key driver of biometric authentication's dominance is its unparalleled combination of security and user convenience. Biometrics offer an extremely high level of accuracy in verifying individuals' identities, making it exceedingly difficult for unauthorized access to occur. This accuracy minimizes the risks associated with traditional password-based systems, which are vulnerable to theft, hacking, or human error.

Moreover, biometric authentication methods are user-friendly and seamless. They eliminate the need to remember and frequently change passwords, which can be a hassle and a source of security weaknesses. With biometrics, users can simply use their physical or behavioral traits for effortless and fast authentication, enhancing the overall user experience. The widespread integration of biometric authentication in smartphones, laptops, and other devices has further boosted its adoption. Mobile devices, in particular, have played a pivotal role in popularizing biometric methods like fingerprint recognition and facial scanning, making them easily accessible and widely accepted.

As the demand for robust yet user-friendly security solutions continue to rise, biometric authentication is well-positioned to dominate the global advanced authentication market. Its ability to deliver unmatched security and convenience is driving organizations across industries to invest in and adopt advanced authentication solutions that incorporate biometrics, ensuring a secure and user-friendly digital experience for consumers and employees alike.

Multi-Factor Authentication (MFA) Adoption

Multi-Factor Authentication (MFA) adoption is a powerful driver propelling the growth of the global advanced authentication market. MFA has emerged as a critical cybersecurity practice, and its implementation is rapidly expanding across various industries and sectors.

+44 20 8123 2220
info@marketpublishers.com

One of the primary reasons for the increasing adoption of MFA is its unparalleled ability to enhance security. By requiring users to provide two or more authentication factors before granting access, MFA significantly reduces the risk of unauthorized entry and data breaches. This added layer of protection is particularly crucial in an era where cyber threats are becoming more sophisticated and prevalent. Furthermore, regulatory requirements, such as GDPR in Europe and HIPAA in the United States, mandate the implementation of strong security measures to protect sensitive data. MFA helps organizations meet these compliance standards by providing robust authentication and access control.

The proliferation of remote work and the prevalence of BYOD (Bring Your Own Device) policies have further accelerated MFA adoption. With employees accessing corporate networks and data from various locations and devices, the need for secure authentication has become paramount. MFA offers a flexible and effective solution for verifying user identities in remote and mobile scenarios. As organizations recognize the critical role MFA plays in securing their digital assets, they are increasingly investing in advanced authentication solutions that incorporate MFA. This trend is expected to drive sustained growth in the global advanced authentication market as organizations prioritize cybersecurity and data protection in an evolving threat landscape.

Segmental Insights

Authentication Method Insights

The Biometrics segment holds a significant market share in the Global Advanced Authentication Market. Biometrics analyzes and authenticates individuals based on human physical characteristics, such as fingerprint, retina, iris, palm, speech, and voice, among others. This authentication method has been widely adopted, owing to its key advantages, namely its non-repudiation, non-transferable, and non-identifiable nature, thus providing a high level of protection against fraud.

The technology has found successful implementation across various end-users, such as forensics, governments, banking and financial institutions, and enterprise identity management, among others. Moreover, the widespread availability of fingerprint sensors in affordable mobile devices and the government's national ID programs have increased awareness and adoption of this technology.

In September 2022, The Ministry of Road Transport and Highways (MoRTH) issued a notification allowing citizens to access several transport-related services online with

+44 20 8123 2220
info@marketpublishers.com

their Aadhaar digital ID. Providing such services in a contactless and faceless manner will go a long way in saving time for citizens while easing their compliance burden.

Regional Insights

North America plays a significant role in the global Advanced Authentication market; Organizations across the United States are increasingly dependent on computer networks and electronic data to conduct their daily operations, and growing pools of personal and financial information are also transferred and stored online. People are more likely to use online services for day-to-day transactions. This has made it more important for the country to have advanced authentication services.

Moreover, the sophistication level of professional identity thieves involved in organized crime in the country continues to grow, creating a need for countermeasures to be used by companies in the country. Also, the BYOD trend is getting bigger and bigger, which makes it easier for advanced authentication methods like smart cards, physical tokens, and key performance indicators (KPIs) to be used to access sensitive information or log in to client servers.

Key Market Players

Fujitsu Ltd.

Thales Group (Gemalto NV)

NEC Corp.

Broadcom Inc. (CA Technologies)

Dell Technologies Inc.

Safran Identity and Security SAS

Lumidigm Inc.

Validsoft

Pistolstar

+44 20 8123 2220
info@marketpublishers.com

Securenvoy

Report Scope:

In this report, the Global Advanced Authentication Market has been segmented into the following categories, in addition to the industry trends which have also been detailed below:

Global Advanced Authentication Market, By Authentication Methods:

Smart Cards

Biometrics

Mobile Smart Credentials

Tokens

User-based Public Key Infrastructure

Other

Global Advanced Authentication Market, By End-user Industry:

BFSI

Healthcare

Government

Defense

IT and Telecom

Other

Global Advanced Authentication Market, By Region:

North America

+44 20 8123 2220
info@marketpublishers.com

United States

Canada

Mexico

Asia-Pacific

China

India

Japan

South Korea

Indonesia

Europe

Germany

United Kingdom

France

Russia

Spain

South America

Brazil

Argentina

Middle East & Africa

+44 20 8123 2220
info@marketpublishers.com

Saudi Arabia

South Africa

Egypt

UAE

Israel

Competitive Landscape

Company Profiles: Detailed analysis of the major companies presents in the Global Advanced Authentication Market.

Available Customizations:

Global Advanced Authentication Market report with the given market data, Tech Sci Research offers customizations according to a company's specific needs. The following customization options are available for the report:

Company Information

Detailed analysis and profiling of additional market players (up to five).

+44 20 8123 2220
info@marketpublishers.com

Contents

1. PRODUCT OVERVIEW

1.1. Market Definition
1.2. Scope of the Market
1.3. Markets Covered
1.4. Years Considered for Study
1.5. Key Market Segmentations

2. RESEARCH METHODOLOGY

2.1. Objective of the Study
2.2. Baseline Methodology
2.3. Key Industry Partners
2.4. Major Association and Secondary Sources
2.5. Forecasting Methodology
2.6. Data Triangulation & Validation
2.7. Assumptions and Limitations

3. EXECUTIVE SUMMARY

4. VOICE OF CUSTOMERS

5. GLOBAL ADVANCED AUTHENTICATION MARKET OUTLOOK

5.1. Market Size & Forecast
  5.1.1. By Value
5.2. Market Share & Forecast
  5.2.1. By Authentication Method (Smart Cards, Biometrics, Mobile Smart Credentials, Tokens, User-based Public Key Infrastructure)
  5.2.2. By End-user Industry (BFSI, Healthcare, Government, Defense, IT, and Telecom)
  5.2.3. By Region
5.3. By Company (2022)
5.4. Market Map

+44 20 8123 2220
info@marketpublishers.com

6. NORTH AMERICA ADVANCED AUTHENTICATION MARKET OUTLOOK

6.1. Market Size & Forecast
6.1.1. By Value
6.2. Market Share & Forecast
6.2.1. By Authentication Method
6.2.2. By End-user Industry
6.2.3. By Country
6.3. North America: Country Analysis
6.3.1. United States Advanced Authentication Market Outlook
6.3.1.1. Market Size & Forecast
6.3.1.1.1. By Value
6.3.1.2. Market Share & Forecast
6.3.1.2.1. By Authentication Method
6.3.1.2.2. By End-user Industry
6.3.2. Canada Advanced Authentication Market Outlook
6.3.2.1. Market Size & Forecast
6.3.2.1.1. By Value
6.3.2.2. Market Share & Forecast
6.3.2.2.1. By Authentication Method
6.3.2.2.2. By End-user Industry
6.3.3. Mexico Advanced Authentication Market Outlook
6.3.3.1. Market Size & Forecast
6.3.3.1.1. By Value
6.3.3.2. Market Share & Forecast
6.3.3.2.1. By Authentication Method
6.3.3.2.2. By End-user Industry

7. ASIA-PACIFIC ADVANCED AUTHENTICATION MARKET OUTLOOK

7.1. Market Size & Forecast
7.1.1. By Value
7.2. Market Share & Forecast
7.2.1. By Authentication Method
7.2.2. By End-user Industry
7.2.3. By Country
7.3. Asia-Pacific: Country Analysis
7.3.1. China Advanced Authentication Market Outlook
7.3.1.1. Market Size & Forecast

+44 20 8123 2220
info@marketpublishers.com

7.3.1.1.1. By Value
7.3.1.2. Market Share & Forecast
7.3.1.2.1. By Authentication Method
7.3.1.2.2. By End-user Industry
7.3.2. India Advanced Authentication Market Outlook
7.3.2.1. Market Size & Forecast
7.3.2.1.1. By Value
7.3.2.2. Market Share & Forecast
7.3.2.2.1. By Authentication Method
7.3.2.2.2. By End-user Industry
7.3.3. Japan Advanced Authentication Market Outlook
7.3.3.1. Market Size & Forecast
7.3.3.1.1. By Value
7.3.3.2. Market Share & Forecast
7.3.3.2.1. By Authentication Method
7.3.3.2.2. By End-user Industry
7.3.4. South Korea Advanced Authentication Market Outlook
7.3.4.1. Market Size & Forecast
7.3.4.1.1. By Value
7.3.4.2. Market Share & Forecast
7.3.4.2.1. By Authentication Method
7.3.4.2.2. By End-user Industry
7.3.5. Indonesia Advanced Authentication Market Outlook
7.3.5.1. Market Size & Forecast
7.3.5.1.1. By Value
7.3.5.2. Market Share & Forecast
7.3.5.2.1. By Authentication Method
7.3.5.2.2. By End-user Industry

8. EUROPE ADVANCED AUTHENTICATION MARKET OUTLOOK

8.1. Market Size & Forecast
8.1.1. By Value
8.2. Market Share & Forecast
8.2.1. By Authentication Method
8.2.2. By End-user Industry
8.2.3. By Country
8.3. Europe: Country Analysis
8.3.1. Germany Advanced Authentication Market Outlook

+44 20 8123 2220
info@marketpublishers.com

8.3.1.1. Market Size & Forecast
8.3.1.1.1. By Value
8.3.1.2. Market Share & Forecast
8.3.1.2.1. By Authentication Method
8.3.1.2.2. By End-user Industry
8.3.2. United Kingdom Advanced Authentication Market Outlook
8.3.2.1. Market Size & Forecast
8.3.2.1.1. By Value
8.3.2.2. Market Share & Forecast
8.3.2.2.1. By Authentication Method
8.3.2.2.2. By End-user Industry
8.3.3. France Advanced Authentication Market Outlook
8.3.3.1. Market Size & Forecast
8.3.3.1.1. By Value
8.3.3.2. Market Share & Forecast
8.3.3.2.1. By Authentication Method
8.3.3.2.2. By End-user Industry
8.3.4. Russia Advanced Authentication Market Outlook
8.3.4.1. Market Size & Forecast
8.3.4.1.1. By Value
8.3.4.2. Market Share & Forecast
8.3.4.2.1. By Authentication Method
8.3.4.2.2. By End-user Industry
8.3.5. Spain Advanced Authentication Market Outlook
8.3.5.1. Market Size & Forecast
8.3.5.1.1. By Value
8.3.5.2. Market Share & Forecast
8.3.5.2.1. By Authentication Method
8.3.5.2.2. By End-user Industry

9. SOUTH AMERICA ADVANCED AUTHENTICATION MARKET OUTLOOK

9.1. Market Size & Forecast
9.1.1. By Value
9.2. Market Share & Forecast
9.2.1. By Authentication Method
9.2.2. By End-user Industry
9.2.3. By Country
9.3. South America: Country Analysis

+44 20 8123 2220
info@marketpublishers.com

9.3.1. Brazil Advanced Authentication Market Outlook
9.3.1.1. Market Size & Forecast
9.3.1.1.1. By Value
9.3.1.2. Market Share & Forecast
9.3.1.2.1. By Authentication Method
9.3.1.2.2. By End-user Industry
9.3.2. Argentina Advanced Authentication Market Outlook
9.3.2.1. Market Size & Forecast
9.3.2.1.1. By Value
9.3.2.2. Market Share & Forecast
9.3.2.2.1. By Authentication Method
9.3.2.2.2. By End-user Industry

10. MIDDLE EAST & AFRICA ADVANCED AUTHENTICATION MARKET OUTLOOK

10.1. Market Size & Forecast
10.1.1. By Value
10.2. Market Share & Forecast
10.2.1. By Authentication Method
10.2.2. By End-user Industry
10.2.3. By Country
10.3. Middle East & Africa: Country Analysis
10.3.1. Saudi Arabia Advanced Authentication Market Outlook
10.3.1.1. Market Size & Forecast
10.3.1.1.1. By Value
10.3.1.2. Market Share & Forecast
10.3.1.2.1. By Authentication Method
10.3.1.2.2. By End-user Industry
10.3.2. South Africa Advanced Authentication Market Outlook
10.3.2.1. Market Size & Forecast
10.3.2.1.1. By Value
10.3.2.2. Market Share & Forecast
10.3.2.2.1. By Authentication Method
10.3.2.2.2. By End-user Industry
10.3.3. UAE Advanced Authentication Market Outlook
10.3.3.1. Market Size & Forecast
10.3.3.1.1. By Value
10.3.3.2. Market Share & Forecast
10.3.3.2.1. By Authentication Method

+44 20 8123 2220
info@marketpublishers.com

10.3.3.2.2. By End-user Industry
10.3.4. Israel Advanced Authentication Market Outlook
10.3.4.1. Market Size & Forecast
10.3.4.1.1. By Value
10.3.4.2. Market Share & Forecast
10.3.4.2.1. By Authentication Method
10.3.4.2.2. By End-user Industry
10.3.5. Egypt Advanced Authentication Market Outlook
10.3.5.1. Market Size & Forecast
10.3.5.1.1. By Value
10.3.5.2. Market Share & Forecast
10.3.5.2.1. By Authentication Method
10.3.5.2.2. By End-user Industry

11. MARKET DYNAMICS

11.1. Drivers
11.2. Challenge

12. MARKET TRENDS & DEVELOPMENTS

13. COMPANY PROFILES

13.1. Fujitsu Ltd.
13.1.1. Business Overview
13.1.2. Key Revenue and Financials
13.1.3. Recent Developments
13.1.4. Key Personnel
13.1.5. Key Product/Services
13.2. Thales Group (Gemalto NV)
13.2.1. Business Overview
13.2.2. Key Revenue and Financials
13.2.3. Recent Developments
13.2.4. Key Personnel
13.2.5. Key Product/Services
13.3. NEC Corp.
13.3.1. Business Overview
13.3.2. Key Revenue and Financials

+44 20 8123 2220
info@marketpublishers.com

13.3.3. Recent Developments
13.3.4. Key Personnel
13.3.5. Key Product/Services
13.4. Broadcom Inc. (CA Technologies)
13.4.1. Business Overview
13.4.2. Key Revenue and Financials
13.4.3. Recent Developments
13.4.4. Key Personnel
13.4.5. Key Product/Services
13.5. Dell Technologies Inc.
13.5.1. Business Overview
13.5.2. Key Revenue and Financials
13.5.3. Recent Developments
13.5.4. Key Personnel
13.5.5. Key Product/Services
13.6. Safran Identity and Security SAS
13.6.1. Business Overview
13.6.2. Key Revenue and Financials
13.6.3. Recent Developments
13.6.4. Key Personnel
13.6.5. Key Product/Services
13.7. Lumidigm Inc.
13.7.1. Business Overview
13.7.2. Key Revenue and Financials
13.7.3. Recent Developments
13.7.4. Key Personnel
13.7.5. Key Product/Services
13.8. Validsoft
13.8.1. Business Overview
13.8.2. Key Revenue and Financials
13.8.3. Recent Developments
13.8.4. Key Personnel
13.8.5. Key Product/Services
13.9. Pistolstar
13.9.1. Business Overview
13.9.2. Key Revenue and Financials
13.9.3. Recent Developments
13.9.4. Key Personnel
13.9.5. Key Product/Services

+44 20 8123 2220
info@marketpublishers.com

13.10. Securenvoy
13.10.1. Business Overview
13.10.2. Key Revenue and Financials
13.10.3. Recent Developments
13.10.4. Key Personnel
13.10.5. Key Product/Services

14. STRATEGIC RECOMMENDATIONS

15. ABOUT US & DISCLAIMER

+44 20 8123 2220
info@marketpublishers.com

I would like to order

Product name: Advanced Authentication Market – Global Industry Size, Share, Trends, Opportunity, and Forecast Segmented by Authentication Method (Smart Cards, Biometrics, Mobile Smart Credentials, Tokens, User-based Public Key Infrastructure), End-user Industry (BFSI, Healthcare, Government, Defense, IT, and Telecom), By Region, Competition 2018-2028

Product link: https://marketpublishers.com/r/AA017CE2C922EN.html

Price: US$ 4,900.00 (Single User License / Electronic Delivery)

If you want to order Corporate License or Hard Copy, please, contact our Customer Service:
info@marketpublishers.com

Payment

To pay by Credit Card (Visa, MasterCard, American Express, PayPal), please, click button on product page https://marketpublishers.com/r/AA017CE2C922EN.html

To pay by Wire Transfer, please, fill in your contact details in the form below:

First name:
Last name:
Email:
Company:
Address:
City:
Zip code:
Country:
Tel:
Fax:
Your message:

**All fields are required

Custumer signature _____

Please, note that by ordering from marketpublishers.com you are agreeing to our Terms & Conditions at https://marketpublishers.com/docs/terms.html

+44 20 8123 2220
info@marketpublishers.com

To place an order via fax simply print this form, fill in the information below and fax the completed form to +44 20 7900 3970