Mobile Encryption - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 132 pages | Mordor Intelligence

AVAILABLE LICENSES:

- Single User License $4750.00
- Team License (1-7 Users) $5250.00
- Site License $6500.00
- Corporate License $8750.00

Report description:

The Mobile Encryption Market size is estimated at USD 4.43 billion in 2024, and is expected to reach USD 15.20 billion by 2029, growing at a CAGR of 27.98% during the forecast period (2024-2029).

As organizations have adapted to increasingly pervasive regulatory and compliance mandates and more stringent internal policies, encryption deployments have increased in number and scope in significant enterprises.

Key Highlights
-Mobile encryption is the process of encoding data in a language or code only authorized individuals with the right decryption key can decipher. Due to increased worries about data security and privacy, the market is expanding quickly. The demand for mobile encryption solutions is becoming increasingly critical as most people utilize mobile devices to store sensitive information like financial data, personal information, and confidential corporate information.
-Increasing and evolving advanced threats, the enhanced adoption of cloud services, mobile device proliferation, and virtualization are the major factors creating disruptive changes in the mobile encryption market. The need for stringent compliance and regulatory requirements and increasing concern for the security and privacy of intellectual property are the major factors driving the market. Also, the rising trend of the Internet of Things among various end-user verticals is a crucial factor facilitating the expansion of the mobile encryption market.
-Mobile encryption safeguards customer data by making it unintelligible to outsiders, ensuring it remains private and secure. The number of digital payments has increased dramatically as a result of the rise in smartphone payment usage. To improve the present payment system, businesses are integrating blockchain with mobile payment. The most important feature of blockchain is its effectiveness, which establishes a benchmark for safe and secure transactions.
-The "bring your own device" (BYOD) phenomenon and its incredibly fast and pervasive adoption by almost every organization

necessitated a fundamental rethinking of security approaches, and it has been found that organizations are deploying many disparate encryption platforms. As a result, managing policies and keys efficiently and securely is an increasingly troublesome challenge.
-The demand for mobile encryption has grown dramatically over the years as organizations increasingly deploy a mobile workforce. A mobile workforce has many advantages, including increased productivity, lower expenses, and more flexibility. As more businesses continue to employ a mobile workforce, the market has consequently experienced considerable expansion over the past few years, and this trend is projected to continue in the years to come.
-The comprehensive use of encryption varies considerably by industry segment. Specifically, heavily regulated and mobile-dependent industries, such as financial services and IT services, have the highest use rate, and less regulated industries, such as manufacturing and consumer products, have the lowest use rate.
-Additionally, one major barrier is that organizations do not recognize the importance of mobile encryption solutions. Concerns regarding the complexity of encryption solutions, the absence of industry standards for encryption technology, and the possible effects of encryption on device performance are some further limitations.
-COVID Lockdowns and limitations increased mobile technology use more than usual. As the need for security device interoperability grows and becomes the new standard, there will be a significant rise in demand for mobile encryption.

Mobile Encryption Market Trends

BFSI is Expected to Hold a Major Market Share

- For the security of their mobile apps, banks employ a number of encryption techniques. For data in transit, common techniques include Transport Layer Security (TLS) and Secure Sockets Layer (SSL), whereas for data at rest, common techniques include Advanced Encryption Standard (AES) or RSA. To further safeguard customer information, banks may additionally employ extra security measures like multi-factor authentication and device fingerprinting. The banking industry's expanding requirement for payment security solutions to offer its consumers a more secure service is what is causing the growth.
- Among the current identified trends influencing this segment of the market, the usage of encrypted OTP SMS is one of them, along with a PIN to avoid any possible attacks like phishing, man-in-the-middle attacks, and malware Trojans. As more of the bank account information and passwords of customers come on mobile devices, even personal pictures (while applying for loans online) have become a major security concern. SSL/TLS enables secure transmissions of private data over the internet, including credit card details, passwords, and sensitive personal information.
- Banks and financial institutions use SSL/TLS to encrypt their traffic to address these multiple issues, including controlling access, protecting confidentiality, and reducing exposure to protocol-specific attacks. With the increased sophistication of online transactions, payment providers are catching up with the technologies to provide better security. The majority of online payments are now mobile or in-app payments; the traditional PCI-DSS standards have to be suitably upgraded.
- Moreover, it is projected that the efficiency and effectiveness of financial encryption software would grow with the addition of artificial intelligence (AI). At the same time, it helps organisations and customers meet the growing demand for data protection. As a result, it is anticipated that encryption software powered by artificial intelligence would be quickly adopted by the banking and finance sector.
- The integrity of the data must be maintained by the banks throughout the life of the data. As a result, it is essential for banks to put in place the appropriate threat detection and response procedures in accordance with their needs. Thus, by imposing various security standards, such as data masking and encryption software by banks, the data integrity can be preserved. As a result, it is anticipated that the banking, finance, and insurance (BFSI) industry will see an increase in demand for financial encryption software.
- The outdated SSL standards prevent the use of new initiatives like EMV Three-Domain Secure (3DS), a messaging mechanism that enables customers to authenticate themselves with their card issuer when making card-not-present online purchases..

Communication that uses two algorithms for encryption that work side-by-side is currently considered the strongest encryption, with cryptologists predicting double-cell encryption to remain so over the forecast period.

North America is Expected to Hold a Major Market Share

- In the North American region, the United States business sector increasingly depends on computer networks and electronic data to conduct its daily operations, and growing pools of personal and financial information are also transferred and stored in the cloud using phones. Furthermore, a significant increase in the BYOD trend is also favoring the conditions for advanced authentication methods, such as smart cards, physical tokens, and KPIs, to access sensitive information or log in to client servers.
- The dominance can be attributed to the more stringent regulatory standards in nations like Canada and the United States, which oblige banks to increase data privacy. In order to protect privacy, both public and private banks have increased their demand for cryptographic software. Additionally, the regional market expansion is anticipated to be fueled by the surge in cyberattacks and the threat to business-critical information.
- It is estimated that around 51% of mobile devices in the United States have full disk encryption, which is expected to increase in the coming years. However, with the growth in the adoption of full disk encryption, almost all these devices could become inaccessible to law enforcement. As a result, the government is regulating the encryption market. Companies like Google and other tech giants are facing restrictions and obstacles.
- AAG IT Services estimates that in 2021, 1 in 2 American internet users had their accounts breached. One in ten US businesses do not have any protection against cyberattacks. In addition, cybercrime had an impact on 53.35 million US individuals in the first half of 2022. Therefore, rising privacy laws and mobile payment technology are anticipated to open up new industry prospects in the area.
- Apple is the largest provider of mobile full-disk encryption, and around 55% of the mobile devices in the United States run on iOS. With increased malicious data breaches occurring in the North American region, it has become the largest market for encryption services.

Mobile Encryption Industry Overview

The Global Mobile Encryption Market is fragmented, as the mobile encryption ecosystem comprises various mobile encryption solutions and service providers. The major players deploy various strategies, such as new product launches and clinical trials, and are also taking market initiatives and innovations through high expenditure on research and development, joint ventures, partnerships, acquisitions, and others to increase their footprints in this market. Some of the major players in the market are IBM Corporation, HP Enterprises, Dell, Symantec, and Checkpoint Software, among others.

- October 2022 - Check Point Software Technologies Ltd., a top global provider of cyber security solutions, acquired Spectral, an Israeli startup that was a key innovator in developer-first security tools created by developers for developers. With this purchase, Check Point was expected to increase the developer-first security capabilities of its cloud solution, Check Point CloudGuard, and offer the broadest range of cloud application security use cases, including infrastructure as code (IaC) scanning and hardcoded secret detection.
- December 2022 - RingCentral, Inc. announced that it is extending End-to-End Encryption (E2EE) capabilities in its flagship RingCentral MVP product to encompass both phone and messaging in addition to video. E2EE technology shields users' communication content from being accessed by unauthorised parties. This offers protection against infiltration and attacks from outside parties as well as privacy for privileged discussions for security-conscious organisations.

Additional Benefits:

- The market estimate (ME) sheet in Excel format
- 3 months of analyst support

Table of Contents:

Mobile Encryption - Market Share Analysis, Industry Trends & Statistics, Growth Forecasts 2019 - 2029

Market Report | 2024-02-17 | 132 pages | Mordor Intelligence

To place an Order with Scotts International:

- - Print this form
- - Complete the relevant blank fields and sign
- - Send as a scanned email to support@scotts-international.com

ORDER FORM:

Select license	License	Price
	Single User License	$4750.00
	Team License (1-7 Users)	$5250.00
	Site License	$6500.00
	Corporate License	$8750.00
	VAT	
	Total	

*Please circle the relevant license option. For any questions please contact support@scotts-international.com or 0048 603 394 346.

** VAT will be added at 23% for Polish based companies, individuals and EU based companies who are unable to provide a valid EU Vat Numbers.

Email*		Phone*	
First Name*		Last Name*	
Job title*			
Company Name*		EU Vat / Tax ID / NIP number*	
Address*		City*	
Zip Code*		Country*	
		Date	2025-05-08
		Signature