Data Security
AN IDC CONTINUOUS INTELLIGENCE SERVICE

Data Security is a recognition of the direct link between mastery of data and the ability to protect it. With fraud and identity/intellectual property theft impacting over 1 billion people and businesses, IDC identifies and quantifies solutions that can protect data against an evolving host of threats. Topic areas include the evolution of cryptography as we move toward cloud computing, Big Data and analytics, and the collection of massive amounts of machine and user-created content, which is increasingly turning many enterprises into data brokers. This service also includes coverage of the resurgence of masking and tokenization techniques as enterprise data stores grow with the promise of analytics, and the use of data to enable behavioral security solutions, cognitive analytics, and monitoring and supervision.

Markets and Subjects Analyzed
- Modern data security trends (containerization, behavioral analysis, cognitive analytics, data tracers, and enterprise rights management)
- Cryptography and data protection (file and whole disk encryption, key management, and tokenization)
- Data storage security (archive/backup, database, and obfuscation)
- Data intelligence solutions (data loss prevention, enterprise rights management, antifraud monitoring and remediation, and advanced threat detection and intelligence)

Core Research
- Data Security Taxonomy
- Worldwide Encryption and Key Management Infrastructure Market Forecast
- IDC MarketScape: Worldwide Key Management Solution Vendor Assessment
- IDC FutureScape: Worldwide Data Security Predictions
- IDC MaturityScape: Data Loss Prevention Solutions
- Vendor Profile, Analysis, and Case Studies

In addition to the insight provided in this service, IDC may conduct research on specific topics or emerging market segments via research offerings that require additional IDC funding and client investment. To learn more about the analysts and published research, please visit: Data Security.

Key Questions Answered
1. How can organizations better protect their sensitive data assets by understanding the motivations of hackers targeting their networks?
2. What steps can be taken to predict/combat emerging threats and improve data security?
3. What innovative data security products and approaches may have long-term efficacy?
4. How does continued cloud adoption, the growing nature of distributed corporate environments, and Big Data and analytics impact existing encryption mechanisms?
5. How do organizations address data security and rights management issues that could potentially expose sensitive data elements and cause data decentralization?

Companies Analyzed
This service reviews strategies, market positioning, and future direction of several providers in the Data Security market including: