Information and Data Security

AN IDC CONTINUOUS INTELLIGENCE SERVICE

Information and Data Security is a recognition of the direct link between mastery of data and the ability to protect it. With data 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 using content as the control point for cybersecurity and data protection, including message security and sensitive data management technologies. Other topics 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 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 and privacy trends (containerization and enterprise rights management)
- Cryptography and data protection (file and whole disk encryption, key management, certificates, and tokenization)
- Data storage security (archive/backup, database, and obfuscation)
- Data intelligence solutions (messaging security, data loss prevention, data discovery and classification, data access governance)

Core Research

- Data Security Taxonomy
- Worldwide Message Security Market Shares
- Worldwide Message Security Forecast
- Worldwide Encryption and Key Management Infrastructure Market Forecast
- Insider Threat Forecast
- Insider Threat Market Shares
- IDC FutureScape
- Sensitive Data Management Market Shares
- Sensitive Data Management Forecast
- 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: Information and 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 the strategies, market positioning, and future direction of several providers in the *Information and Data Security* market including:

Amazon Web Services, Barracuda, Broadcom, Big ID, CA Technologies, Check Point, CipherCloud, Cisco, Collibra, Dataguise, Datto, Dell EMC–RSA, Digital.ai, Digital Arts, Digital Guardian, Entrust, ESET, Exostar, Fasoo,com, Forcepoint, Fortanix, Fortinet, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, IBM, Imperva, Informatica, Intel, McAfee, Microsoft, Mimecast, NEC, New H3C Group, NextLabs, Ns Focus, Opentext (Zix), Oracle, Protegrity, Qi An Xin Group, SAS, Securiti, Seclore, Securonix, Skyhigh Networks, SonicWALL, Sophos, Symantec, Thales (Gemalto), Titus, Trellix, Trend Micro, TrustARC, Trustwave, Utimaco, Varonis, Venafi, WinMagic, Zettaset, and Ziff Davis.