# Information and Data Security

*AN IDC CONTINUOUS INTELLIGENCE SERVICE*

*Information and Data Security* recognizes the value that data brings to the enterprise and the criticality of protecting it without introducing delays or blocking essential operations. 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 information protection, security, privacy, and compliance with technologies such as discovery and classification, data loss prevention, messaging security, and data access governance. 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 (data discovery and classification)
- Cryptography and digital trust (file and whole disk encryption, key management, certificates, and tokenization)
- Data storage security (archive/backup, database, and obfuscation)
- Information protection solutions (messaging security, data loss prevention, data discovery and classification, and data access governance)

## Core Research

- Data Security Taxonomy
- Worldwide Digital Trust Market Shares
- Worldwide Digital Trust Market Forecast
- Insider Threat Market Glance
- IDC FutureScape
- Information Protection Market Shares
- Information Protection Market 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 attackers and/or malicious insiders?
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 data security markets?
5. How do organizations address data security 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, Cohesity, Dataguise, Datto, Dell EMC–RSA, Digicert, Digital.ai, Digital Arts, Egnyte, Entrust, ESET, Exostar, Faso.com, Forcepoint, Fortanix, Fortinet, Fortra, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, IBM, Imperva, Informatica, Intel, McAfee, Microsoft, Mimecast, NEC, NextLabs, Ns Focus, 1touch.io, Opentext (Zix), Oracle, Proofpoint, Protegrity, Qi An Xin Group, SAS, Securiti, Seclore, Securonix, Sectigo, Skyhigh Networks, SonicWALL, Sophos, Symantec, Thales (Gemalto), Trellix, Trend Micro, TrustARC, Trustwave, Utimaco, Varonis, Venafi, WinMagic, Zettaset, and Ziff Davis.