MARKET PERSPECTIVE

GDPR Compliance and Beyond: Veritas Enhances Data Protection Portfolio and Builds Personal Data Governance Framework

Carla Arend Archana Venkatraman

EXECUTIVE SNAPSHOT

FIGURE 1

Executive Snapshot: GDPR Compliance and Beyond: Veritas Enhances Data Protection Portfolio and Builds Personal Data Governance Framework

This IDC Market Perspective focuses on General Data Protection Regulation (GDPR) compliance and how Veritas' updated solutions and framework can help organizations achieve it and go beyond compliance. Enterprises need to invest in data management solutions that offer unified information management and data governance across multicloud infrastructures and provide the necessary foundations for GDPR compliance. A culture shift is also essential since the GDPR is about people, processes, and technology.

Key Takeaways

- Veritas understands that GDPR will fundamentally shake up the data protection landscape and has developed technologies, strategies, and features to ensure compliance and help enterprises yield the value from information governance strategies.
- Veritas has developed a GDPR-focused framework that maps how its solutions connect to the critical obligations around protecting and managing personal data on enterprises. It has simplified compliance strategies across key areas such as searching, locating, minimizing, protecting, and monitoring personal data.
- Moving forward, Veritas should educate its channel community and showcase the benefits of going

Recommended Actions

- End users need to think beyond minimum viable compliance. They need to know the benefits that good governance can bring such as establishing trust with customers, yielding more accurate insights from analytics, and meeting demanding obligations from GDPR such as right to be forgotten (RTBF) and subject access requests (SAR) efficiently and at scale.
- Enterprises should shift technology investments from patchy, point solutions to broader, holistic data protection strategies to have uniform information management across rapidly emerging multicloud architectures.
- C-suite, data stewards, and data protection officers must put personal data at the center of governance and ensure that there is a data protection framework that can help progress in digital transformation.

Source: IDC, 2018

May 2018, IDC #EMEA43811718

NEW MARKET DEVELOPMENTS AND DYNAMICS

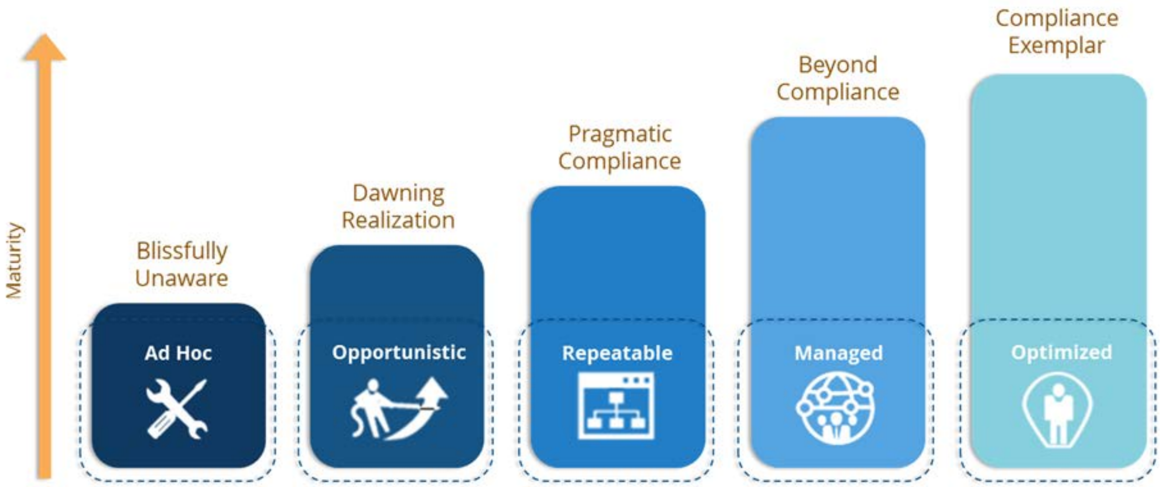
May 2018 is a critical time as the General Data Protection Regulation (GDPR) comes into effect in the EU and shakes up the data protection landscape. GDPR raises the bar on security, protection, and privacy of personal information of data subjects in the EU. Because of the significant impact of its extraterritoriality clause, GDPR applies to every organization globally that handles data of people in the EU; this is true irrespective of the location of data processing.

Ever since the regulation was ratified in 2016, GDPR has been a top-of-mind priority for organizations, especially European ones. However, this hasn't necessarily translated into action towards compliance.

In fact, IDC's *Enterprise Readiness for GDPR Research*, which maps organizations across five stages of maturity, found that about 40% of organizations were in Stage 2 (Dawning Realization), while 25% were in Stage 3 (Pragmatic Compliance) and less than 1% in Stage 5 (Compliance Exemplar). Much of the inertia is down to a debate on whether the supervisory authorities (regulators) have the resources and processes in place to enforce the hefty fines. Difficulty in changing people's behavior, culture, and engagement from all business stakeholders are other obstacles to enterprises becoming GDPR-compliant.

FIGURE 2

IDC's GDPR Compliance Readiness Model



Source: IDC, 2018

IDC believes that GDPR compliance is predominantly a business process and culture issue, rather than a technology one. We believe that organizations that see GDPR compliance as an opportunity to incorporate a robust data management hygiene, and to create a long-term solution and culture around individual data privacy and protection, will be the ones that can see their data as a value creator. Organizations that build a data protection framework and incorporate compliance and data privacy into their operational processes will be the ones that can transform from data laggards to data advocates.

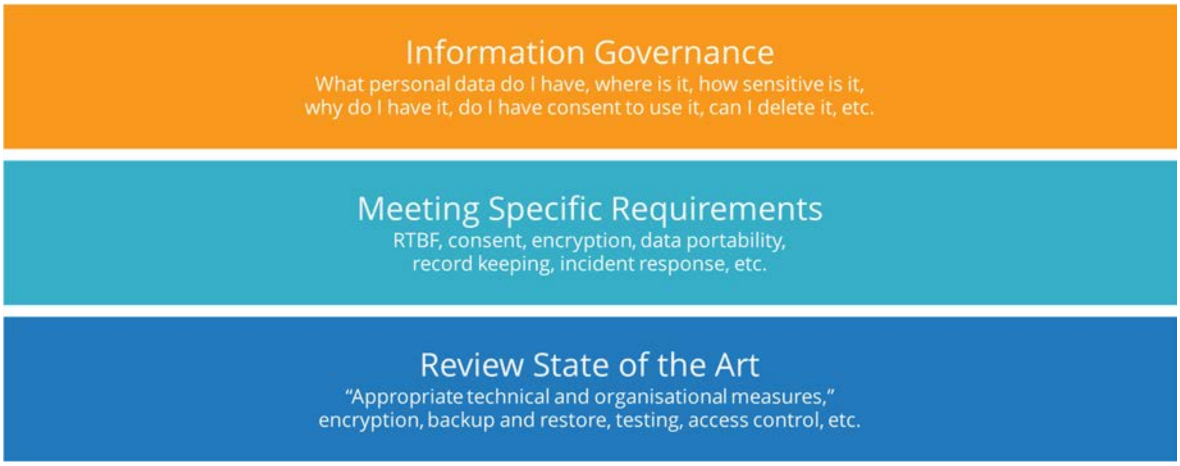
Hurried and patchy investments in point technologies to stitch together an uncoordinated data protection architecture and aim to attain a minimum viable compliance by May 25, 2018, is a very short-term approach.

In fact, May 25, 2018, should be seen as the starting point for a new era of data protection. GDPR compliance is not a one-press magic button but an ongoing and continuous effort that calls for a fresh new approach to data protection, especially when viewed in the context of emerging IT dynamics — multicloud, application heterogeneity, and growing volumes and variety of data. Developing a holistic and end-to-end data management strategy across multicloud and hybrid infrastructures and focusing on the potential benefits of good data governance is necessary. It can help organizations invest in technologies to embed privacy and compliance within product development, application development, operational processes, and third-party service discussions very early. A sound data privacy, protection and management program can ensure ongoing compliance as new products and services are introduced to the market.

It is going to take businesses time, investment, and effort to comply and maintain ongoing compliance with GDPR. To help organizations start their GDPR-readiness journey, IDC has developed a technology framework aimed at helping them strategize their GDPR compliance roadmaps on a step-by-step basis (given in Figure 3). Their approaches to GDPR compliance should start from identifying and knowing where personal data is, and then applying policies on a consistent and automated basis, an approach that IDC believes is essential for long-term compliance and for establishing a competent data foundation for business transformation.

FIGURE 3

Technology Framework for GDPR



Information Governance

What personal data do I have, where is it, how sensitive is it, why do I have it, do I have consent to use it, can I delete it, etc.

Meeting Specific Requirements

RTBF, consent, encryption, data portability, record keeping, incident response, etc.

Review State of the Art

"Appropriate technical and organisational measures," encryption, backup and restore, testing, access control, etc.

Source: IDC, 2018

When investing in technologies and vendors, organizations must assess the breadth of the solutions portfolio to make sure they have a unified, end-to-end data protection environment with common user experience for management across multiple platforms. They need to assess whether the vendor truly has a GDPR-ready portfolio — for instance, whether the engineering and innovation efforts in the past few cycles have been in line to plug gaps in solutions and products to enable compliance. Organizations should assess how the solutions map to the clauses and requirements in GDPR. Lastly, they need to understand the vendor's future roadmap and strategies to see how the solutions will be updated for ongoing compliance in the dynamically emerging multicloud and heterogeneous IT era.

How Veritas Updated its Data Protection Portfolio to Enable Broad GDPR Compliance and Go Beyond

Information management vendor Veritas started developing and outlining its solutions portfolio for GDPR in 2016. It expanded its data management portfolio with new products (such as Veritas InfoScale, Veritas Resiliency Platform, and Veritas Information Map) and launched copy data management solution Veritas Velocity to help businesses delve deep into their data stores to identify, prioritize, and manage information across their organizations. (see *Veritas Helps Organizations Become GDPR-Ready and Data-Driven with an Expanded Information Management Portfolio,* IDC #EMEA42178616, January 2017.)

2016-2018 Timeline: Feature Updates and GDPR Framework

Veritas started building its "360 Data Management" vision in 2016 and gave this vision substance by integrating newer solutions such as Velocity, Information Map, and Veritas Resiliency Platform with NetBackup 8.0.

Veritas' differentiated approach is to offer solutions that provide visibility and control of business data. IDC believes that by enabling IT teams to answer the "where," "who," and "what" of all their data, together with their ability to control data via policy in real time, is the first critical step to meeting regulatory requirements.

Veritas' solutions such as Data Insight, eDiscovery Platform, and Enterprise Vault, along with Information Map, specifically aim to help organizations meet GDPR's regulatory requirements. For example, Information Map and Data Insight help IT teams delve deep into their data stores to recognize, prioritize, and manage information across their organizations. Data Insight also delivers automated workflows for assessing and remediating access compliance. Enterprise Vault's auto-classification capabilities tag content for easier retention and faster search. Lastly, the eDiscovery Platform's predictive coding feature delivers machine learning to streamline compliance review. In IDC's opinion, these solutions and their capabilities directly contribute to helping organizations manage rapidly increasing volumes and varieties of data across heterogeneous platforms (physical and virtual infrastructure and cloud platforms) and meet regulatory compliance.

In the last 15 months, the company has continued to expand its GDPR-aligned data management portfolio. For one, it has created an enhanced classification engine that works consistently across all its information management products including its new Cloud Storage and CloudPoint solutions. One of the most significant classification hurdles organizations have struggled with in the past is trying to manage disparate classification rules and policies for different workloads. Understanding the value of classification as a critical capability, Veritas has extended its classification technology across its own solutions on premises and in the cloud to give a uniform and consistent approach to data classification. IDC believes that technologies that can help identify, classify, redact, and annotate personal data across structured and unstructured data formats can help operationalize compliance into business processes.

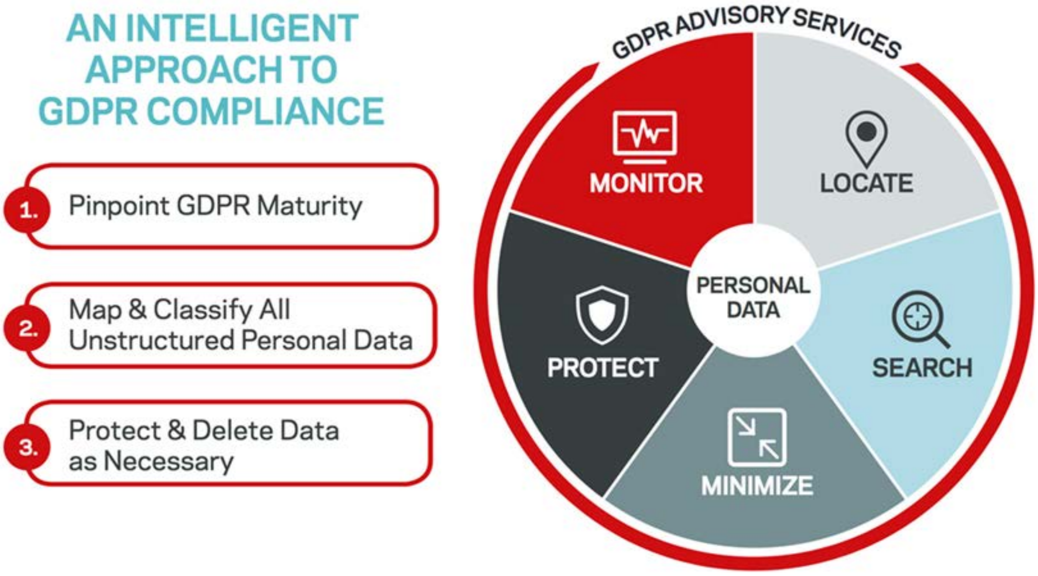
Veritas has also developed the Risk Analyzer, a free web tool where organizations can upload dummy data or real data sets to quickly scan, analyze, and classify personal data.

In addition to engineering compliance-driven features, Veritas has also invested in user experience. The classification engine and the Risk Analyzer have graphical dashboards that help quickly pinpoint which files contain sensitive data, as well as the nature and risk of that sensitive data (names, addresses, credit card details, dates of birth, etc.).

Further enhancing user experience around GDPR compliance, Veritas has also developed a "Focused GDPR Framework," as given in Figure 4.

FIGURE 4

Veritas' GDPR Compliance Framework


AN INTELLIGENT APPROACH TO GDPR COMPLIANCE
1. Pinpoint GDPR Maturity
2. Map & Classify All Unstructured Personal Data
3. Protect & Delete Data as Necessary
GDPR ADVISORY SERVICES
MONITOR
LOCATE
SEARCH
MINIMIZE
PROTECT
PERSONAL DATA

Source: Veritas

The framework can also help the vendor articulate the role of its solutions in the context of broader data management. Veritas' GDPR framework is also well-aligned with IDC's Technology Framework for GDPR (Figure 2) recommended for executing an ongoing compliance strategy.

In each segment within this framework, Veritas has updated its products with more compliance-oriented capabilities.

- For instance, within the Locate segment, it has added 23 new connectors to Information Map, providing on-premise and cloud ingest, taking the features beyond NetBackup. The connectors (third party tools from Box, NetApp, and Microsoft) can help organizations mitigate information risk regardless of where data is located. It also emphasizes the value of classification in Data Insight to articulate the Risk Analyzer engine. Version 6.1 of Data Insight allows admins to assign users specific role-based permissions that limit unnecessary exposure to sensitive information in the management console. IDC believes such information governance control is important in managing GDPR compliance.
- In the Search segment, Veritas has brought classification and a SAR workflow into the eDiscovery platform. eDiscovery 9.0 features automatic classification of sensitive data based on custom and built-in policies. it has also added bulk redaction capabilities, improving speed and efficiency to perform redactions and delete redactions at scale. More significantly, it also supports Integrated Windows Authentication Single Sign-On for Legal Hold authentication.
- In the Minimize segment, it is introducing privileged delete for Enterprise Vault. The latest version (12.3) of Enterprise Vault supports classification of all ingested content-email, files, Instant Messaging, and Social Media. It features customizable policies that automatically determine what to classify and retain or discard and whether to tag an item for faster

search, discovery or supervisory review. The vendor has added new support for Microsoft Azure, Amazon S3 Standard-Infrequent Access, Google Cloud Storage, and IBM Cloud Object Storage to improve archiving capabilities.

- Within the Protect segment, Veritas has engineered NetBackup application programming interface (API) additions. It is important to highlight how Veritas has released NetBackup REST APIs to allow developers or the channel community to natively integrate data protection at the application layer, to help overcome data security gaps at the application layer.
- As for innovation in the Monitor segment, Veritas has a built-in ransomware template for better predictive attack discovery (although not yet in the full cyberspace). The recent surge in high-profile ransomware attacks has made data protection and threat mitigation a boardroom and CIO priority for organizations of all sizes. It has also forced organizations to view storage and information management investment as closely tied to security priorities.

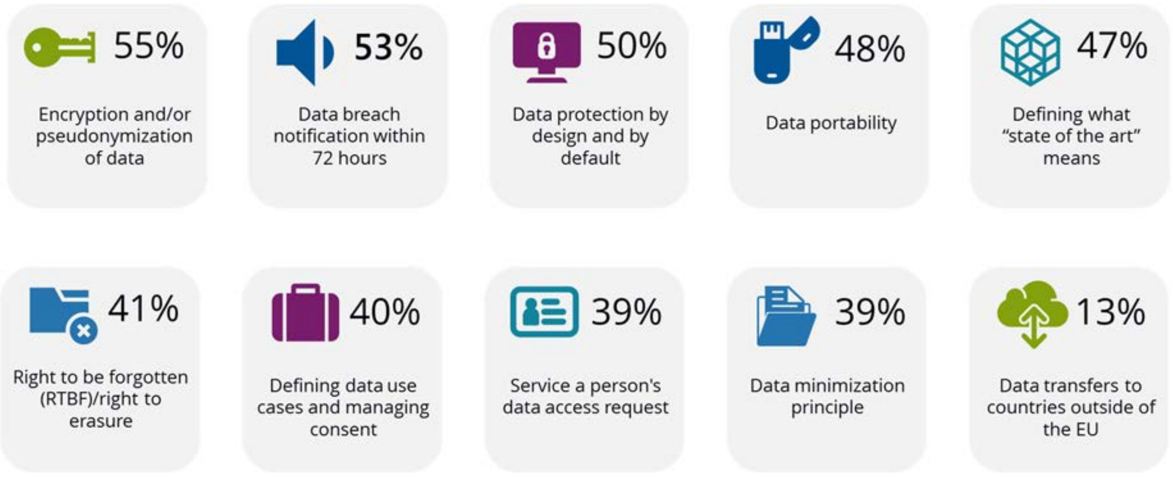
IDC's GDPR survey reveals how data assessment and classification (62%) is a key focus followed by improving documentation processes (60%) and improving identity and access management (59%). IDC notes how these key focus areas are ripe for innovation as enterprises accelerate their GDPR compliance strategies in the run-up to the deadline, making Veritas product upgrades timely and relevant.

Holistic Approach to Compliance

GDPR requirements are exhaustive and can overwhelm customers, especially non-European enterprises with significant personal data of subjects residing in the EU. Veritas' GDPR framework maps its offerings to the compliance requirements to guide enterprises on their compliance journeys. It can also help them identify areas that require investment and make progress on compliance in a methodical manner across five key areas (locate, search, minimize, protect, and monitor). In conversations with IDC, many enterprises admit that locating and minimizing personal data is one of the top challenges for them, as shown in Figure 5.

FIGURE 5

Which GDPR Requirement is the Most Challenging?



Source: IDC, 2018

In addition, Veritas has expanded its cloud and on-premises connectors for Data Insight and Information Map, resulting in much wider spread visibility. It has also beefed up the eDiscovery platform to facilitate repeatable and more efficient results for SARs. This scaling up of eDiscovery to help with the SAR clause of GDPR is important because the EU's end-user marketing campaign for GDPR in the coming months will raise awareness and there could be an increase in SARs or right to be forgotten (RTBF) requests. IDC's research reveals that 41% of organizations consider RTBF as one of the most challenging compliance requirements, as seen in Figure 4.

Going Beyond GDPR Compliance: Business Opportunities

With GDPR, data protection and management has become a boardroom issue, and data stewards should use this opportunity to secure investment and engagement in making data a business enabler. This can bring many benefits.

Building Trust with Customers

Demonstrating that GDPR compliance is taken seriously can help enterprises nurture a strong, transparent, and trusted relationship with their customers, both B2C and B2B. Savvy B2C customers are already asking questions on how their personal data is collected, stored, processed, secured, and managed. Having a confident conversation with customers will help them become more willing to share data, so that they have improved customer services. B2B customers are currently auditing their suppliers to make sure that they are GDPR compliant and will not introduce a compliance risk in the supply chain.

Improving Data Quality to Become Data-Driven and Future-Ready

Information is the most valuable intangible asset within an organization. An up-to-date data management framework will not only help organizations avoid hefty fines over non-compliance but also provide a springboard for the use of analytics, artificial intelligence (AI), and machine learning on useful and relevant data. It can also help streamline storage and infrastructure resource investment. Lastly, it will also help enterprises get ready to execute on new market dynamics; for example, financial services companies will be able to comply with Open APIs for banking regulations (Payment Services Directive 2 or PSD2) because they already have a data governance framework in place.

Achieving Security, Privacy, and Data Protection by Design and by Default (DPbDD)

A major element of the accountability termed in GDPR that affects data controllers is a new requirement: Data Protection by Design and by Default (DPbDD).

According to Paragraph 1 of Article 25 of the GDPR, "taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures designed to implement data-protection principles, such as data minimization, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects."

Paragraph 2 of the same article indicates that the controller "shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

The related recital (Recital 78) states: "… In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations..."

What this means in practical terms is that organizations must consider data protection at the innovation and design stage of any new business process ("at the time of the determination of the means for processing"), and that the onus is on the supply chain ("producers of the products, services and applications should be encouraged to take into account the right to data protection").

ADVICE FOR VERITAS

IDC believes that it is commendable to see Veritas' continued momentum of innovation because the data protection landscape is changing considerably as multicloud and application fragmentation become mainstream. Veritas is adding features and services and continuing to forge partnerships to enable GDPR compliance across multicloud infrastructures. This "omni data management" is platform, cloud and infrastructure agnostic and covers structured and unstructured data with a unified portfolio: this positions Veritas competitively for GDPR solutions.

Going forward, it needs to spread this vision to its channel community. One of the biggest challenges for Veritas is the customer attitude toward GDPR compliance; many customers approach it only with a view of minimum viable compliance. It needs to demonstrate through its work with large enterprises the benefits of putting personal data at the center of all business activities: don't just comply with GDPR but get deeper insight into the data and see how this data-driven decision making can boost business. Another challenge it faces is the cultural inertia and lack of engagement from key stakeholders in investing in GDPR compliance. IDC believes that steering conversations away from the doom and gloom of GDPR or the hefty fines to a conversation of opportunities of good data governance as highlighted in the above section can help overcome this barrier.

Veritas must also be aware of the significant efforts from its competitors on enabling GDPR compliance. From an engineering perspective, Veritas needs to further flesh out its multicloud data management strategy beyond classification to include data ingestion, data minimization, and location optimization services. Lastly, it must build a campaign around its own GDPR compliance journey and share best practices with customers to take the relationship to a more strategic level.

IDC believes that Veritas – with its rich, tightly integrated portfolio and 360 data vision – will play a key role in shaping GDPR strategies and subsequently enabling digital enterprises. IDC sees Veritas as one of the few tech providers that has shown ongoing commitment in fully understanding the potential impact of the GDPR and using it as a foundation to design and integrate solutions, including the release of representational state transfer (REST) APIs for its flagship data protection solution NetBackup.

IDC notes how in the last 12 to 18 months, the new features, capabilities, and upgrades to Veritas' existing products and the new solutions are all engineered with compliance as the fundamental objective. This commitment helps weave in security and compliance at the core product level and not just as an add-on feature.

Veritas' expertise, "compliance-driven" innovation, its own GDPR journey, and its full spectrum of data protection in the multicloud infrastructure gives it the opportunity to make its technology the underpinning foundation for making enterprises data-driven.

LEARN MORE

Related Research

- *What Data Services are Most Challenging for Large European Enterprises in Hybrid and Multicloud Environments?* (IDC #EMEA43762818, April 2018)
- *Top Datacenter Operations Priorities of European Organizations in 2018* (IDC #EMEA43763018, April 2018)
- *IDC Market Glance: Data Protection as a Service, 1Q18* (IDC #US43602418, March 2018)

Synopsis

This IDC Market Perspective focuses on GDPR compliance and how Veritas' updated solutions and framework can help organizations achieve it and go beyond compliance. It is essential for enterprises to take a long-term view of data protection and see GDPR as an opportunity to transform from data laggards to data advocates. "Enterprises need to invest in data management solutions that offer unified information management and data governance across multicloud infrastructures and provide the necessary foundation for GDPR compliance," says Archana Venkatraman, research manager, IDC European Storage Research. "A culture shift is also essential since the GDPR is about people, processes, and technology."

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC U.K.

IDC UK
5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.idc.com