Support GDPR with Endpoint and Data Management

Simplify GDPR compliance for your on-premises, cloud or hybrid environments

The General Data Protection Regulation (GDPR) comes at a transformative time for IT administrators and controllers. Any IT appliances, processors and networks that are involved in data-processing activities relating to citizens from the European Union (EU) must add GDPR readiness to their seemingly endless list of strategic business initiatives.

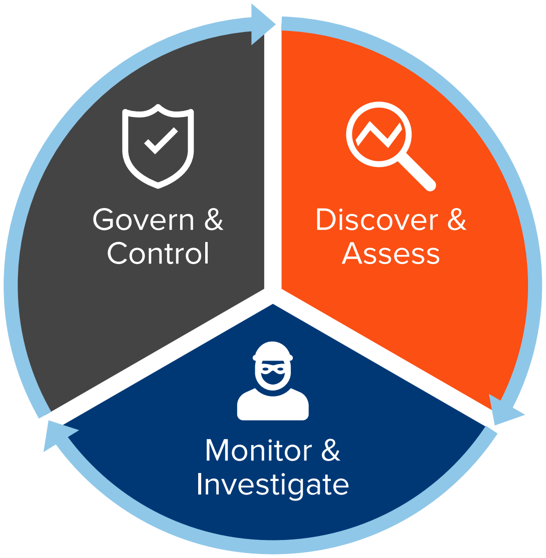
GDPR will require organizations — both the data controllers and the data processors — to strengthen data protection and security measures to protect the personally identifiable information (PII) of EU citizens, and to demonstrate compliance at any time. More specifically, organizations must ensure the correct people have access to PII. Additionally, reasonable measures must be in place to protect data from unauthorized access, as well as prove accountability of those accessing it. And, in the event of a breach, accurate understanding of the scope of the breach must be provided in a timely manner. Effective May 25, 2018, steep penalties will apply for failure to comply with GDPR provisions.

GDPR impacts all organizations, in all industries and in all regions — even those outside the EU that control or process personal information of EU citizens. However, most organizations are unclear on the extent of change required to achieve GDPR compliance, the severity of penalties for non-compliance and how changes will affect the business. In fact, according to a July 2017 Osterman Research study, 61 percent of respondents aren't very familiar with the key provisions of GDPR, and 64 percent aren't ready to comply with GDPR compliance requirements. Organizations must become experts quickly, as key GDPR provisions will present major challenges for IT, including:

- **The need for continuous compliance and auditing —** Organizations must be able to demonstrate compliance at any time, not just monthly or annually.

BENEFITS:

- Gain visibility across your data systems, whether on premises or in the cloud
- Evaluate and report on existing security policies, system configuration settings and privileged access rights
- Support GDPR compliance reporting with tools that provide sub-reporting with a benchmark
- Help mitigate the risk of personal data breaches
- Detect suspicious activity
- Protect data against physical loss and carry out restores of lost data
- Get real-time physical data protection
- Gain optimum protection against data breaches with information on patch and software releases



- **Mandatory data breach notifications —** When a sensitive data breach occurs, organizations must notify the data protection authority (DPA) and all affected customers within 72 hours. GDPR compliance violations can result in heavy fines of up to 4 percent of global revenue or €20 million (whichever is higher), job loss from the C-level on down and public embarrassment for the organization.

If your organization handles any personal data about EU citizens — whether they're customers, vendors, partners or employees — it's critical to start on GDPR compliance now so you can meet the deadline and avoid all the consequences of non-compliance.

But without the right tools, achieving and maintaining GDPR compliance for the complete IT infrastructure, from server to endpoint, is time-consuming and costly, and diverts resources away from improving operational efficiency, meeting SLAs and innovating the business.

Quest® solutions can help make it easier to ensure your on-premises, cloud or hybrid environment meets GDPR requirements. Your organization can start preparing for GDPR now by improving your security posture and strengthening data protection safeguards across your environment. Doing so can help you achieve and maintain GDPR compliance, and avoid costly fines and damage to your reputation. With Quest solutions, you'll be in a better position to assess, monitor and control your environment to help you meet your GDPR compliance requirements and stay more productive and secure.

CAPABILITIES

Discover and assess

Quest solutions scan your entire network to identify connected devices, and provide you with detailed hardware and software inventory, allowing a comprehensive assessment of the environment. The network discovery and asset inventory functions enable you to obtain actionable information even about connected, non-computer devices, such as networking gear, printers and IP telephony. With this information, you are able to evaluate and report on the data helping you demonstrate compliance within your organization.

Monitor and investigate

Quest solutions provide end-to-end monitoring and reporting of your physical and virtual environments. Using one client interface for end user, infrastructure and application performance monitoring allows you to gauge the interdependencies between all three to quickly target problem resolution. For GDPR and data protection, this provides deep insight into available resources, maximum application uptime, data availability and helps to avoid bottlenecks.

Our solutions allow you to perform system checks and end-user checks each day, and alert users when the need arises to resolve an incident before it impacts end-user productivity. This leads to a deeper understanding of exactly what requires protection and resolves problems earlier before having to rely on restores. Thus, allowing for a better understanding of what data is required for backup purposes, for optimization of the physical and virtual estate, and to return wasted resources to resource pools.

Govern and control

Strengthen internal security and governance by implementing measures to help mitigate risks, such as accidental or unlawful destruction, loss, and alteration such as encryption. Up-to-date security patches and software releases on servers and endpoints, and streamlining configuration and policy enforcement processes will lower these risks with the ability to report on all activity that has taken place and is due to take place. In combination with high-frequency backups and very fast restores in case of unforeseen breaches, Quest solutions enhance your ability to stay GDPR compliant.

ABOUT QUEST

At Quest, our purpose is to solve complex problems with simple solutions. We accomplish this with a philosophy focused on great products, great service and an overall goal of being simple to do business with. Our vision is to deliver technology that eliminates the need to choose between efficiency and effectiveness, which means you and your organization can spend less time on IT administration and more time on business innovation.

QUEST GDPR COMPLIANCE SOLUTIONS

DISCOVER AND ASSESS

KACE® Systems Management Appliance (SMA)

MONITOR AND INVESTIGATE

Quest VROOM

Foglight®

Foglight for Virtualization

GOVERN AND CONTROL

Quest VROOM

Rapid Recovery

KACE SMA

FOR MORE INFORMATION

Visit www.quest.com/solutions/gdpr-compliance/

Quest
4 Polaris Way, Aliso Viejo, CA 92656 | www.quest.com
If you are located outside North America, you can find local office information on our Web site.

Quest, Foglight, KACE and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit www.quest.com/legal/trademark-information.aspx. All other trademarks are property of their respective owners.