SOLUTION BRIEF

Address GDPR Compliance with Pervasive Data Protection

McAfee helps you discover and protect sensitive personal data

General Data Protection Regulation (GDPR) becomes enforceable on May 25, 2018. This regulation replaces Data Protection Directive 95/46/EC. The GDPR's goal is to enforce a single set of data protection rules across the European Union (EU) and to give citizens better control over their personal data. If your organization does business in Europe or collects personal data from or processes personal data of EU citizens, GDPR compliance requirements will apply to your data protection strategy going forward. Now is a good time to work with all your business units to integrate data protection into the fabric of your organization as you strive to achieve GDPR compliance. While no single vendor or solution can guarantee full compliance with GDPR, McAfee® data protection solutions are uniquely positioned to help your organization in two critical areas: discovery and classification of personal data and protection of this vital information wherever it resides.

Prevalence of Data Loss

- Compromised customer records top the list of security incidents, and employees are the number one source of security incidents.[1]
- 40% of companies with more than 5,000 employees experienced between 21 and 75 data loss incidents per day.[2]

Connect With Us

Relevant GDPR Articles

Article 5: Delineates principles for processing data:

- Security of personal data, including protection against unauthorized or unlawful use and against accidental loss, destruction or damage

Articles 25 and 32: Recommend data protection by design and security of processing by:

- Integrating data privacy into an information security policy
- Encrypting personal data
- Maintaining security measures
- Regularly testing security posture

Challenge #1: Discover and Classify Personal Data

The type of personal data regulated by GDPR covers a much wider range than the current EU Data Protection Directive. Aside from basic personally identifiable information (PII)—such as name, address, phone number, and national identification numbers—it also encompasses genetic, medical, economic, cultural, and social data, as well as online identifiers. Because of the proliferation of data in this digital world, this data can reside on individual devices, network file servers, databases, applications, and in cloud storage.

The problem is it's impossible to protect the data you don't know about. The recent McAfee Data Residency survey reveals that more than half of organizations surveyed don't have a clear idea as to where their data is located. The first step toward better data protection is to gain an understanding of what to protect through data discovery and classification.

The McAfee Advantage: Comprehensive Data Discovery and Classification

McAfee can provide you with full visibility to sensitive content, such as personal data, through our comprehensive yet flexible discovery and classification solution, which locates and protects sensitive content on your network, endpoints, databases, and in the cloud.

Here's how our technology can help you implement a program to discover, classify, and inventory personal data:

- **Network inventory and categorization:** McAfee® Data Loss Prevention (McAfee DLP) Discover scans and identifies sensitive data stored on file shares, network data repositories, and databases, providing data classification and analysis for more than 300 types of content.
- **Endpoint discovery and classification:** McAfee DLP Endpoint scans for personal data on local drives, such as laptops and desktops, and includes a self-remediation discovery scan option. Through manual classification, users are empowered with the ability to classify a file at creation. User classification is further enhanced through integrations with McAfee Security Innovation Alliance partner solutions from TITUS and Boldon James.

- **Cloud storage inventory and discovery:** McAfee DLP Discover provides scheduled scans and identifies personal data stored in cloud repositories, such as Box, and creates an inventory list for personal data. McAfee Skyhigh Security Cloud detects and categorizes a wide range of personal data based on keywords, standard data patterns (example: credit card numbers), custom data patterns (example: part numbers), document fingerprints, database fingerprints, and more.

Challenge #2: Protect Data Wherever It Resides

Once you know what data to protect and know where it is, how do you go about protecting it? A truly comprehensive data protection program defends data-at-rest, data-in-motion, and data-in-use. But there are some challenges to overcome. Technology trends, like cloud adoption and and Bring-Your-Own-Device (BYOD), are blurring traditional corporate perimeters, making it difficult to detect inappropriate use, sharing, or transmission of confidential and personal data. Moreover, few organizations have implemented a unified approach to protecting data across endpoints, the network, and the cloud. Fewer than one in five organizations are using all available data loss prevention technologies, according to the Ponemon Institute's *2016 Data Protection Benchmark* study.[3] Some companies have confined themselves to just device control or email protection, and others only turn on blocking and monitoring when deploying their data loss prevention (DLP) solution, but rarely do they activate enforcement mode. Protecting personal data requires more than basic blocking and monitoring.

The McAfee Advantage: Unified Data Protection

McAfee provides a unified data protection solution that integrates endpoint and network DLP, encryption, and security information and event management (SIEM) to proactively identify and prevent malicious data theft and loss caused by external bad actors, malicious internal ones, or careless but well-meaning employees. Our technologies help curb data loss attempts by rogue applications or attackers, whether the data is at rest, in motion, or in use. This applies to data in the cloud as well—whether it is being uploaded to the cloud, residing in the cloud, or being downloaded from the cloud. These robust, full-spectrum controls help you build a stronger security culture and achieve data protection maturity.

Advanced data protection technologies from the McAfee product and solution portfolio that support GDPR compliance include:

- **Protecting data-at-rest:** McAfee Endpoint Encryption protects against intentional data theft and accidental loss on Macs, PCs, and removable media, such as USB devices. McAfee DLP Discover also protects data residing on network repositories through issuance of alerts, encryption, and blocking and/or removal of sensitive data.
- **Protecting data-in-motion:** McAfee Network DLP safeguards personal data in motion across multiple channels—email, web, text messaging, and FTP—and prevents it from leaving the network.
- **Protecting data-in-use:** McAfee DLP Endpoint and McAfee Device Control protect personal data from employee actions such as clipboard copying, printing,

Do You Know Where Your Data Is?

According to the latest 2017 McAfee Data Residency report, only 47% of organizations are completely confident that they know where their data is physically located—and only 44% have a thorough understanding of the GDPR regulation and how it impacts them.

emailing, social media, and downloading to removable media devices. In addition, McAfee Enterprise Security Manager monitors both user activities and file activities. When an event has a high-risk score, this information is passed over to McAfee DLP, which, in turn, swiftly enforces data protection policies to prevent theft attempts.

- **Protecting data in the cloud:** McAfee Skyhigh Security Cloud can automatically quarantine or remove files that contain personal data from cloud services. The solution can also enforce sharing controls across pre-existing data already stored in the cloud. In addition, McAfee Skyhigh Security Cloud can enforce controls that allow users to view and collaborate on data within cloud applications but prevent them from downloading data when they access it from an unmanaged device. Device management status can be defined using your existing endpoint security solution or a device certificate.

Conclusion

McAfee provides a unified, integrated approach to data protection that will not only support your GDPR compliance efforts but also evolve and mature both your security infrastructure and your business culture. Our pervasive data protection solutions and other integrations help you quickly and accurately discover and classify the sensitive personal data of EU citizens and protect it whenever it is stored, wherever it is used, and wherever it travels—across endpoints, the network, and the cloud.

Learn More

Find out how McAfee data protection technologies and related solutions can help you become GDPR ready: **www.mcafee.com/gdpr**.

1. 2018 IDB Global Information Security Survey: https://www.pwc.com/us/en/cybersecurity/information-security-survey.html
2. Ponemon Institute 2016 Data Protection Benchmark study: https://virtualizationreview.com/whitepapers/2017/04/intel-2016-data-protection-benchmark-study.aspx?tc=page0
3. Ibid

McAfee™
Together is power.

2821 Mission College Blvd.
Santa Clara, CA 95054
888.847.8766
www.mcafee.com