SOLUTION BRIEF

# GDPR and Your Data Protection Transformation

## McAfee technologies and services advance your data security lifecycle

Enforcement of the General Data Protection Regulation (GDPR) is less than a year away—May 25, 2018, to be exact. Approved by the European Union (EU) Parliament on April 14, 2016, this regulation replaces Data Protection Directive 95/46/EC and provides consistent data privacy protections to all EU citizens. It also broadens the type of data that is regulated to include genetic, medical, economic, cultural, and social data. Whether your organization has offices in the European Union (EU) or does business with countries in the EU, you can view the GDPR as an opportunity to not only comply with the articles of the regulation, but also to profoundly transform how you protect your data, ensure personal privacy, and make your business more secure overall. While no single vendor or solution can guarantee full compliance with GDPR, McAfee can assist you in this transformation through its technology solutions and services across these areas of the data security lifecycle: data discovery, data and privacy protection, application security, cloud data protection, and breach detection and response in the security operations (SOC) environment.

Connect With Us

## Change the Way You Secure Data

Data protection has always been an object of serious attention by enterprise security executives and compliance officers, but GDPR will undoubtedly elevate data protection to the boardroom due to the potentially serious consequences of noncompliance. GDPR presents an excellent opportunity for your C-level executives to engage with a trusted advisor like McAfee to discuss impact to current business initiatives and to strategize your GDPR security transformation. GDPR compliance requires more than basic data loss prevention (DLP). It demands a risk-based approach to data protection that will define the appropriate controls needed to secure the vital information of European citizens, streamline compliance processes, and achieve positive outcomes.

### Key GDPR challenges

Complying with stringent GDPR requirements is by no means a simple proposition. Some of the main challenges associated with the new regulation are as follows:

- **Complexity:** The regulation is complicated, with close to 500 requirements that will affect governance, cybersecurity, and IT.
- **Breach notification:** Under GDPR, organizations are required to inform a supervisory authority in the event of a personal data breach notification within 72 hours of becoming aware of the breach. This calls for better data breach detection and response capabilities in enterprise SOCs.
- **Proliferation of data devices:** Mobility, bring-your-own-device (BYOD), and the Internet of Things (IoT) have resulted in an explosion of connected devices that are handling anywhere from petabytes to zettabytes of data—and some of this data may be pertinent to GDPR regulations.
- **Cloud data security:** With the dissolution of the corporate network perimeter, gaining visibility and control over the cloud is on everyone's mind today. Securing data that traverses the cloud is a major concern in light of "Shadow IT" (use of unauthorized applications by employees), storing data without encryption, and lack of multifactor authentication to access cloud services.
- **DevOps:** Exploitation of application vulnerabilities could lead to accidental or intentional data loss. Application developers need to take into account risk and privacy during the design process, and security professionals need to find better ways to protect applications in use today. Application security is top of mind for most security and IT executives. A recent IDG study reveals that 83% of enterprise IT executives believe it should be an integral part of their security strategy.[1] Rather than bolting on security at the deployment phase, DevOps can benefit from best practices, such as performing penetration testing and using code analysis tools earlier in the application development process, to identify and minimize security issues.

**GDPR Awareness**

We recently commissioned Vanson Bourne to survey 800 senior business professionals from a range of industry sectors across eight countries around the world about their current approach to data protection, management, and residency.[2] Here are some of our findings:

- **Where's the data?** 47% of organizations are completely confident that they know where their data is physically located.
- **How well do you understand GDPR?** 44% have a thorough understanding of the regulation and what it means to them.
- **How long does it take to report a breach?** It takes most organization 11 days on average to report a breach. (The GDPR reporting deadline is 72 hours from becoming aware of the breach.)

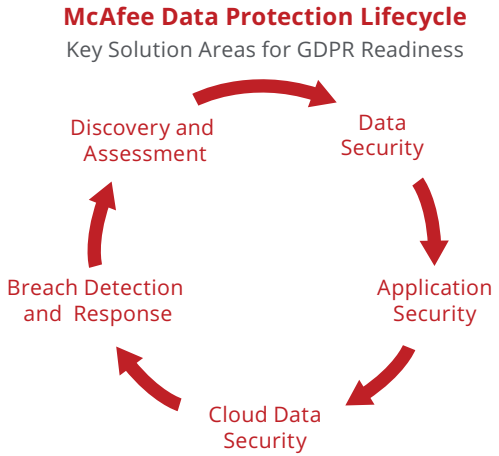


Figure 1. McAfee can help make your organization GDPR-ready across the entire data protection lifecycle.

**Step 1: Continuous Discovery and Assessment**
Discover, classify, and inventory personal data.

**Step 2: Data Security**
Protect personal data at rest and in motion on endpoints and in the cloud.

**Step 3: Application Security**
Defend critical applications in the data center and cloud.

**Step 4: Cloud Data Security**
Safeguard personal data that is uploaded to the cloud, residing in the cloud, and downloaded from the cloud.

**Step 5: Breach and Detection Response**
Ensure that critical processes are in place to detect, investigate, and remediate breaches in a timely manner.

## How McAfee Addresses Your Data Protection Priorities

Delivering personal data protection to EU residents continues to be a challenge and a priority as the business, technology, and threat landscapes evolve and become more complex. Where do you begin? As a first step, assess your data loss risks. Next, take an inventory of your attack surfaces and look at how you can better protect them. Finally, you'll want to think about how your technology transformation plans could be integrated with a GDPR security investment to deliver personal data security.

In response to GDPR, McAfee supports and accelerates security transformation across your entire data protection lifecycle in an automated and integrated manner that reduces the skills and complexity burden. We can help create positive outcomes, not only relative to ongoing GDPR compliance but also over the long term for the benefit and growth of your business. As your trusted partner, McAfee can assist you with building a stronger security culture and achieving advanced security maturity.

**40% of companies with more than 5,000 employees experienced between 21 and 75 data loss incidents (requiring security staff to investigate and analyze) per day.[3]**

**Questions to Ask Yourself When Planning and Prioritizing Your Data Protection Transformation**

- Is there a culture of data security and awareness in your organization?
- Do you know where your sensitive data or privacy-related data is stored?
- Do you employ encryption for data protection?
- Is there a current data loss prevention project in place or planned for this year?
- Do you have an existing in-house application security program?
- Do you know where all of your databases are located and the types of data stored?
- How do you account for cloud Software-as-a-Service (SaaS) applications that house private data?
- How are you controlling privileges and privileged user activity, particularly with cloud services?
- What is the status of your advanced malware protection plans?
- Does your SOC have pre-planned data breach detection use cases?


Figure 2. McAfee Data Security Capabilities

## Mapping McAfee Solutions to GDPR Articles

The chart below summarizes how McAfee technology can support GDPR readiness requirements by Article.

| GDPR Articles | Requirements | Data Protection Lifecycle Phase | McAfee Technologies and Services |
|---|---|---|---|
| **Article 5** | Principles for processing data:<br>▪ Transparent, fair, and lawful<br>▪ Data collection for explicit and legitimate purposes<br>▪ Accuracy of data<br>▪ Data minimization<br>▪ Limitations on storage of data<br>▪ Security of personal data, including protection against unauthorized or unlawful use and against accidental loss, destruction, or damage | Discovery and assessment | ▪ McAfee DLP Endpoint<br>▪ McAfee DLP Discover<br>▪ McAfee DLP Monitor<br>▪ McAfee Database Vulnerability Manager<br>▪ TITUS<br>▪ Boldon James<br>▪ Foundstone Services |
| **Articles 25, 32** | Data protection by design and security of processing:<br>▪ Put measures in place to ensure that data is not accessible without the individual's intervention<br>▪ Integrate data privacy into an information security policy<br>▪ Encrypt personal data<br>▪ Maintain security measures<br>▪ Regularly test security posture | ▪ Data protection<br>▪ Application security<br>▪ Cloud data protection | ▪ McAfee Endpoint Encryption<br>▪ McAfee DLP Prevent<br>▪ McAfee Web Protection<br>▪ McAfee DLP Endpoint<br>▪ McAfee Network DLP<br>▪ McAfee Device Control<br>▪ McAfee Application Control<br>▪ McAfee Database Activity Monitor<br>▪ McAfee Cloud Workload Discovery |
| **Article 30** | Records of processing activity:<br>▪ Inventory and classify data<br>▪ Track how data is processed and for what purpose<br>▪ Disclosure of entities with whom the data is shared or transferred | SOC breach detection | ▪ McAfee ePO software reports<br>▪ McAfee Enterprise Security Manager reports<br>▪ McAfee Enterprise Log Manager reports<br>▪ McAfee DLP Monitor and McAfee DLP Discover reports and data |
| **Article 33** | Breach notification:<br>▪ Notify an authority within 72 hours of becoming aware of a breach<br>▪ Communicate the breach to the individuals affected by it | SOC breach detection | ▪ McAfee Enterprise Log Manager<br>▪ McAfee Enterprise Security Manager<br>▪ Interset<br>▪ OpenDXL<br>▪ Foundstone Services |

## Discovery and assessment

As you evaluate your data protection and overall security maturity level, you'll need to determine whether your organization is affected by the GDPR regulation. If your business involves processing, storing, or transmitting personal data of EU citizens, then you are obliged to comply. One of the first things you'll want to find out is whether you have full visibility over the personally identifiable data you possess and where it resides and travels.

Here's how McAfee can help you implement a program to discover, classify, and inventory sensitive data:

- **Network inventory and categorization:** McAfee® DLP Discover scans and identifies sensitive content, such as personal data stored on file shares and other network data repositories. It provides classification and analysis for data in more than 300 content types.
- **Endpoint discovery and classification:** McAfee DLP Endpoint scans for personal data on local drives, such as laptops and desktops, and offers a self-remediation discovery scan option. The manual classification feature empowers users with the capability to classify a file at creation. It can be further enhanced through integrations with McAfee Security Innovation Alliance partner solutions from organizations like TITUS and Boldon James.
- **Database discovery:** McAfee Database Vulnerability Manager discovers databases and identifies sensitive content, including data specific to GDPR readiness. It tests databases for vulnerabilities and patching status with preconfigured compliance reporting templates.
- **Cloud storage inventory and discovery:** McAfee DLP Discover provides scheduled scans and identifies personal data stored on cloud repositories, such as Box, and creates an inventory list for such sensitive content.
- **Security assessment:** Foundstone® Data Security Program helps organization transition to a mature data protection program by defining data lifecycle elements that are critical to the organization, developing a governance framework for the program, and assisting with technology implementation activities.

## Data protection

Now that you know the whereabouts of the personally identifiable information you have access to, you must evaluate whether the right technologies and processes are in place to help you prevent malicious data theft attempts—whether caused by external bad actors or internal ones—and accidental data loss caused by careless, but well-meaning, employees. You can start by looking at various ways to protect personal data at rest and in motion on endpoints and in the cloud.

Consider some of these advanced data protection technologies from the McAfee product and solution portfolio:

- **Protect data-at-rest:** McAfee Endpoint Encryption protects against intentional data theft and accidental loss on Macs, PCs, and removable media like USB devices. McAfee DLP Discover further protects data residing on network repositories with remediation actions such as alerts, encryption, and blocking and/or removal of sensitive content such as personal data.

- **Protect 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. McAfee Web Gateway provides added visibility by leveraging an integrated DLP library to do DLP-aware decryption and re-encryption of content on the fly.
- **Protect data-in-use:** McAfee DLP Endpoint and McAfee Device Control are effective tools against insider threats. They protect sensitive content against day-to-day employee actions such as clipboard copying, printing, emailing, social media, and downloading to removable media devices.

## Cloud data protection

For most forward-thinking enterprises, using cloud services are a given, but the security of data as it traverses the cloud is not. If you are among the many that are using cloud services on a daily basis, it's time to consider GDPR compliance from several perspectives:

- Is your data protected as you adopt cloud services like Microsoft Office 365?
- Are your cloud service providers or cloud platform providers aware of GDPR requirements? What steps have they taken to ensure protection of personally identifiable information?
- What technologies does your organization have in place to discover and protect data in the cloud?

Again, McAfee can be of assistance with several solutions:

- **Protect data being uploaded to the cloud:** McAfee DLP Endpoint offers cloud protection rules and web protection rules to monitor and block unauthorized sensitive content such as personal data being uploaded into cloud storage destinations like Box, Dropbox, Google Drive, and Microsoft OneDrive. It also intercepts uploads of files containing sensitive personal across all vectors—Microsoft Office Suite, OneDrive sync applications, and OneDrive for business and SharePoint Online web access.
- **Protect data residing in the cloud:** McAfee DLP Discover provides automated and scheduled scans for data residing in Box. McAfee Cloud Workload Discovery provides automated discovery of workloads in Amazon Web Service (AWS), Microsoft Azure, and VMware platforms.
- **Protect data being downloaded from the cloud:** McAfee DLP Endpoint and McAfee Endpoint Encryption work closely together to tag protected files being downloaded from a secure cloud location to the local endpoint. They can encrypt and decrypt files on the fly, if required. Additionally, McAfee DLP Endpoint fingerprints content that is download from Office 365, preventing data leakage across endpoint channels such as removable storage media, social media, printing, and others.
- **Skyhigh Cloud Security:** Skyhigh identifies sensitive information using keywords, data patterns, fingerprints, metadata, and file types and analyzes behavior across cloud services, users, and devices.

### McAfee Database Security Suite Capabilities that Support GDPR Compliance

**Database discovery and data classification:**
- Database discovery
- Sensitive data discovery
- User rights management
- GDPR, BSI, CIS-specific

**Protection and virtual patching:**
- Identification and prevention of exploitation attempts
- Protection against known attacks
- Generic pattern
- Abnormal activity

**Security Assessment**
- Vulnerabilities
- Misconfiguration
- Missing patches
- Vulnerable code
- More than 6,000 checks

**Activity Monitoring**
- Real-time monitoring
- Policy enforcement
- Audit, alert, or block activity

Skyhigh helps control sensitive information either moved to or originating in the cloud utilizing cloud context. It also enforces sharing permissions within applications to ensure unauthorized access doesn't occur. In addition, administrators can manage access controls across multiple environments to restrict downloading of sensitive data to unmanaged devices, controlling the potential for oversharing information. Skyhigh protects both structured and unstructured data with information rights management and encryption.

## Application security

Application exploits like SQL Injection are among the most prevalent ways that organizations lose data. Protecting critical applications in the data center or cloud should be an important aspect of your data protection and GDPR readiness program. Some key questions you should ask in relation to GDPR readiness and application security are:

- What applications are processing sensitive or GDPR-related information?
- Is your in-house development team trained in secure coding practices?
- Do you monitor access and application logs for signs of suspicious activity?

Again, McAfee helps protect your critical applications by:

- **Application security program development:** Foundstone Services provides training in secure coding practices and penetration testing to help you assess application vulnerabilities.
- **Preventing vulnerability exploitations over the network:** McAfee Network Security Platform positioned at the data center perimeter can identify and prevent application or operating system vulnerability exploitation. Additionally, McAfee Network Security Platform Virtual Network Security Platform can be deployed to monitor east-west traffic between server workloads in a virtualized or cloud data center.
- **Hardening server infrastructure:** McAfee Endpoint Security and McAfee Application Control whitelists critical application servers, preventing unauthorized software installation, changes, or malware from being loaded onto systems.
- **Protecting databases:** McAfee Database Activity Monitor provides an additional layer of protection against application exploits and a critical visibility into user and administrator activity. This gives security operations the ability to identify and investigate suspicious user activity.

## Security operations

GDPR requires breach notification within 72 hours of becoming aware of the breach to an appropriate authority. Unfortunately, many SOCs currently struggle to identify and investigate data breaches in a timely manner. Usually this comes down to visibility gaps that impede investigations, inconsistent processes, or lack of effective analytics to identify anomalies.

Some key questions you should ask in relation to GDPR readiness and security operations are:

- How do you go about identifying unauthorized user behavior or detecting data exfiltration?
- What operational insights do you require to identify and validate a data breach?
- Do you have the right data to support detection and investigation?
- If you detect a possible incident, how fast can you respond?

Some critical processes in security operations relative to GDPR are:

- **Incident detection:** The ability to analyze security events, application logs, or network data to identify user or data activity anomalies. This is a critical first step.
- **Incident investigations:** Once a potential incident is identified or reported, it's important to validate, understand the full scope of the problem, and discover the root cause.
- **Incident containment**: Once an incident is identified and validated, containment becomes the final phase. In addition to traditional response actions, like blocking IP or host access, containing a data breach could involve blocking access to data resources or closing a user account to prevent further data loss.

McAfee can help security operations with GDPR readiness by enabling or providing:

- **Efficient processes and procedures:** Foundstone Services offers engagements that help organizations build proactive incident response processes.
- **Endpoint detection and response:** McAfee Active Response combines behavior-based protection with continuous insights to rapidly detect, contain, investigate, and eliminate advanced threats at patient-zero.
- **Centralized data collection and search:** Getting the right visibility into the users, data, and application logs on your network is critical for data breach detection and investigations. McAfee Enterprise Security Manager provides a central data management platform for aggregating events and raw log collection and identifying and prioritizing potential threats.
- **Analytics to identify a data breach:** With McAfee Enterprise Security Manager's content packs, consisting of use-case specific correlations, rules, and dashboards, analysts can quickly and confidently deploy advanced security use cases, including indicators of suspicious activity. Additionally, McAfee Behavioral Analytics content pack, as well as integrations with leading UEBA vendors, such as Interset, can identify activity anomalies and provide high-confidence indicators of attack.
- **Rapid incident containment:** OpenDXL is a messaging fabric enabling security automation and providing a simplified integration point for control technologies to ingest orchestrated actions.

## Conclusion

As you embark on your journey to data protection transformation in alignment with GDPR requirements, you can count on McAfee as your trusted advisor and partner. We provide a truly integrated security system that delivers interoperable data protection across

### Content Packs Enable Faster and More Accurate Detection and Investigation via McAfee Enterprise Security Manager and McAfee Database Activity Monitor

- Faster and broader data breach investigation, compared to a siloed approach consisting of individual devices, systems, and application logs
- To help ensure compliance, McAfee Database Event Monitor for SIEM discovers personal data in use. You can monitor these databases and establish an audit trail for protected data access, user account activity, and changes.
- Retains details of all database transactions from login to logoff to support auditing
- Simplifies analysis with "one click" reconstruction of sessions
- Reliable centralized log management
- Secure access restrictions to log data via McAfee Enterprise Security Manager role-based access

endpoints, the network, and the cloud. Orchestrated management provides centralized visibility of all data storage locations, policy controls for sensitive content such as personal data, and simplified reporting.

Our unified approach to data security helps you achieve data protection by design in three fundamental ways:

- **Increased visibility through data discovery and classification:** A necessary first step toward reducing risk is understanding where all your personal data resides and what type of data it is.
- **Data protection technologies to prevent exfiltration of personal data and safeguard privacy:** McAfee solutions help prevent accidental and malicious data theft by insiders and cybercriminals with the help of unified data protection policies that are effective and easy to manage.
- **Accelerated detection and response:** SOCs can quickly identify, analyze, and validate key indicators of a data breach, understand the full scope of a breach, and report these incidents within 72 hours of becoming aware of the breach, which is a GDPR requirement.

Our comprehensive portfolio of technologies and services supports both continued compliance and accountability and your evolution into a stronger, more secure enterprise that can confidently grow its global presence.

## Learn More

Find out how McAfee can help you become GDPR ready:

- Read our white paper: **"From Endpoint to Network to Cloud: Optimized Data Lifecycle Security In an Era of Pervasive Threats."**
- Visit: **www.mcafee.com/gdpr**.

**Detection of unauthorized accesses:**

- Misconfigured access protection (example: detection of unauthorized protocols, successful use of accounts that are not in a watch list for critical assets)
- Privilege access abuses (example: use of accounts not in a watch list for critical assets)

**Detection of data exfiltration:**

- Metrics for a status check of sensitive content locations and identification of possible data exfiltration
- Workflow for reviewing user interactions with sensitive information
- Insights into specific users and activity from possible insider threats in order to help stop data exfiltration

1. https://www.csoonline.com/article/3206270/security/it-s-time-to-get-serious-about-web-application-security.html
2. https://www.mcafee.com/us/resources/reports/restricted/rp-beyond-gdpr.pdf
3. Ponemon Institute's 2016 Data Protection Benchmark Study




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


3712_0218
FEBRUARY 2018