SOLUTION BRIEF

GDPR: An Opportunity to Transform Your Security Operations

McAfee SIEM solutions improve breach detection and response

Is your security operations GDPR ready? General Data Protection Regulation (GDPR) becomes enforceable on May 25, 2018. This regulation replaces Data Protection Directive 95/46/EC and provides consistent data privacy protections to all European Union (EU) citizens. If you have offices in the European Union (EU) or doing business with countries in the EU, GDPR compliance is top of mind. It's also a great opportunity to transform the way your security operation detects and responds to breaches. No single vendor or solution can guarantee full compliance with GDPR, but advanced McAfee® security information and event management (SIEM) solutions and complementary integrated products can help you achieve two positive outcomes. First, these technologies can enhance and bolster your GDPR compliance efforts. Second, they can improve security operation performance overall to support the growth and security maturity of your organization.

Connect With Us

GDPR Compliance: Addressing Breach Detection and Response

A successful and comprehensive GDPR compliance strategy 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.

McAfee Enterprise Security Manager (SIEM), related solutions, and the integrated products that support it all enable risk-based decisions and address the breach detection and response phase of your threat defense lifecycle, which has direct relevance to GDPR requirements. When it comes to GDPR compliance, the value of McAfee SIEM solutions is twofold:

- It augments and accelerates data breach detection to ensure compliance.
- It adds intelligence to your existing data protection strategy by correlating threat information with vulnerabilities and with the countermeasures you are currently deploying. This enables your security staff to gain a broader and deeper understanding of your data exfiltration risk posture and guides you on where you need to focus your remediation efforts.

Before diving deeper into the McAfee capabilities for breach detection and notification, let's look at two critical GDPR requirements:

- Article 30: Maintain strict records of data processing activity:
  - Inventory and classify data
  - Track how data is processed and for what purpose
  - Disclose entities with whom data is shared or transferred
- Article 33: Timely breach notification:
  - Notify an authority within 72 hours of a breach
  - Communicate the breach to individuals affected by it

These two requirements should give you pause to evaluate the current state of your security operations and to consider this fundamental question: Do you have the right processes in place to detect, investigate, and remediate breaches in a timely manner?

GDPR Breach Notification

According to GDPR Article 32, organizations are required to report a breach to authorities and affected individuals within 72 hours. A recent study commissioned with Vanson Bourne, surveying 800 senior business professionals across eight countries, reveals that it takes most organizations 11 days on average to report a breach.

Time Is of the Essence

Can you say with confidence that your security operations can identify and investigate data breaches within the 72-hour GDPR timeframe?[1] If not, the problem usually boils down to three things: visibility gaps that impede investigations, inconsistent processes, and/or lack of effective analytics to identify anomalies.

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 is an important first step.
- **Incident investigation:** Once a potential incident is identified or reported, it's important to validate the issue, understand the full scope of the problem, and discover the root cause.
- **Incident containment:** Once an incident is identified and validated, containment is 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 SIEM and related solutions can help security operations with GDPR readiness by enabling or providing:

- **Centralized data collection and search:** Getting the right visibility into the users, data, and application logs on your network is vital 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. McAfee Enterprise Log Manager solution automates log management, storage, and analysis for all log types; stores them in their original format; and validates them. All of this is necessary for compliance. This log data enriches McAfee Enterprise Security Manager with additional valuable threat intelligence.
- **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, the User Behavior Analytics Content Pack can identify activity anomalies and provide associated indicators of attack. Integration with McAfee Behavioral Analytics, a dedicated UEBA solution, enables advanced behavior detection capabilities.
- **Rapid incident containment:** OpenDXL is a messaging fabric that enables security automation and provides a simplified integration point for control technologies to ingest orchestrated actions.

Is Your Security Operations GDPR Ready?

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?

Example Use Case: McAfee Enterprise Security Manager Exfiltration Content Pack

Let's take a look at a specific use case to see how the prebuilt Exfiltration Content Pack, available at no charge for McAfee Enterprise Security Manager users, can be leveraged by your security operations in a data loss prevention (DLP) use case. This powerful content pack is a valuable addition to your GDPR compliance toolbox. It is designed for:

- Detection and monitoring of all communications protocols commonly used for data exfiltration, such as BitTorrent, command-and-control (C&C) channels, Gnutella, and others.
- Identification and investigation of users who are violating corporate data policies and possibly engaged in insider data exfiltration by looking at who is viewing sensitive data, the type of data being viewed, and where the data is being sent. This provides rapid insight into specific users and activity from possible insider threats to help immediately stop data exfiltration.

In addition to these detection and monitoring capabilities, the Exfiltration Content Pack also sends notifications that trigger automated action when data exfiltration is detected. You can configure trigger parameters that correspond with your organization's data policies and use static watch lists fine-tuned to specific data-handling scenarios within your organization. The content pack also enables you to create compliance reports that you can email to specific recipients and to remote locations, which can help you prepare for GDPR audits.

Collaborative Support for Data Breach Investigations

The McAfee Database Event Monitor for SIEM solution facilitates in-depth investigations and provides detailed data tracking and reporting to enable fast, accurate, and comprehensive response to compliance audits.

Support for data breach investigations:

- Faster and broader data breach investigation, compared to a siloed approach consisting of individual devices, systems, and application logs
- To help you ensure compliance, McAfee Database Event Monitor for SIEM can discover sensitive 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
- Provides reliable centralized log management
- Enables secure access restrictions to log data via McAfee Enterprise Security Manager role-based access

McAfee SIEM and other integrated solutions can add value to even the most complex, multivendor security infrastructures. McAfee Enterprise Security Manager, for example, consumes feeds and inputs from both McAfee and non-McAfee sources specifically to help in this type of scenario in several ways. It helps to identify,

understand, and respond to stealthy threats that aim to exfiltrate personal data. McAfee Enterprise Security Manager also provides heightened visibility to user, network, and system activities. Finally, it significantly reduces the time and skills required to run investigations of data breaches and accidental data leakage, which lightens the load on your security team and addresses the security resource shortage. Given the GDPR requirements to report data breaches, these capabilities will be vital in the near future and in general for the health and prosperity of your organization.

Conclusion

As your trusted security advisor, McAfee provides a unified, integrated approach to data security that will support your GDPR compliance efforts and help you evolve your security maturity. McAfee Enterprise Security Manager and complementary solutions help accelerate detection and response so that your security operations 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—a basic GDPR requirement.

Learn More

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

1. The GDPR requires breach notification to an appropriate authority within 72 hours of becoming aware of the breach.

McAfee™
Together is power.

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