Solution Brief

Why you need an Information Centric Security model for the GDPR

Introduction

The European Union's General Data Protection Regulation (GDPR) focuses attention on data security and privacy. Its reach spans beyond the EU border and applies globally. In fact, any organization that holds or processes personal data on individuals (or "data subjects") in the EU has to comply. The GDPR went into effect on 25 May 2018 influencing how organizations build, deploy and manage their information protection systems.

The GDPR is based on the concept that data privacy is a fundamental right and puts the onus on organizations to adopt data privacy, and by extension, data security by design. Symantec's view is that an information protection strategy that centers on the data—not the device, network or user—is one that meets the multiple data protection challenges facing organizations around the world, including many of the requirements of the GDPR.

How Ready Are You?

When the GDPR came into force in May 2018, research showed that many organizations were still developing plans and not confident that they would be fully compliant from the outset. In fact over 70% of them said that their lack of knowledge about GDPR was limiting their ability to establish compliance across their data management environment. Data protection is an important issue, one that organizations need to get right.

Implications of Non-compliance

Not only does failing to properly protect data undermine confidence in that organization, data breaches cause disruption, brand image and financial losses. In addition, organizations can be held to account by regulators and face significant fines (up to €20m or 4% of total worldwide annual turnover, whichever is higher).

Should a breach be discovered, organizations can be required to notify regulators and impacted individuals within 72 hours. Without a good handle on sensitive data (which includes risk management, visibility of data use and location, and a breach detection and reaction plan) this requirement will challenge organizations. Of course, if you can demonstrate that data is adequately protected (e.g. through encryption technology) then the breach notification requirements become significantly lighter.

How is Personal Data Defined?

Personal data is defined as "any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, medical information, posts on social networks, or a computer's IP address".

Key Provisions of GDPR

The GDPR is complex with many provisions that relate to not just technology, but an organizations' policies, systems and people behaviors. However, as the GDPR has a fundamental goal of ensuring that private data is kept secure, there are some key principles that will be common to any data protection plan with the goal of protecting data across the entire life cycle.

Key Provisions:

PREPARE

Know your personal data – Understand what personal data you collect and any retention rules you have to store personal data.

Assess your data security – Assess whether the level of security offered by current policies and procedures is adequate to offer protection against unauthorized processing and data loss.

PROTECT

Embed privacy – Ensure that the technologies embed privacy and the processes are built protecting the privacy of individuals.

Protect personal data – Ensure full risk management of personal data from who has access to it, where it is located, how it is used and that it is protected through strong information risk management and security.

DETECT

Control transfers of personal data – Transferring personal data out of the European Economic Area (e.g. in the cloud), will be subject to increased regulatory scrutiny.

RESPOND

Review any breach notification processes to ensure that your company has tools on hand to investigate the extent of any compromise within a 72-hour notification deadline.

Information Centric Security

Symantec's Information Centric Security has at its heart, the goal of protecting data. This is achieved by the innovative combination of key data protection technology and analytics to allow organizations to identify, monitor and protect sensitive data, including data that moves to the cloud and is used by third party organizations. And should you be concerned that data has fallen into the wrong hands, you have analytics data to highlight risky users and remotely triggered access controls to lock users out of a document, providing real time protection against a breach.

How Information Centric Security helps you with GDPR

Many organizations will use the GDPR as the impetus for reviewing and improving how they ensure personal data is kept both private and secure. Here is a logical, four-step process to follow:

1. **What are the top risks to my current data protection system?**
2. **How do I identify and monitor sensitive data, wherever it flows?**
3. **How do I protect the data, ensuring only intended users have access?**
4. **If I discover a breach, how do I respond?**

Within this section, we'll show how Symantec's Information Centric Security technologies assist you through this process.

1 What are the top risks to my current data protection system?

Symantec helps you to assess data exposure and associated risk within the organization. In fact Symantec offers customers several tools to prepare for GDPR.

First of all the Symantec Control Compliance Suite (CCS) GDPR readiness assessment helps evaluate an organization's current level of understanding and readiness on the path towards compliance. CCS can track all the organization's assets, especially those storing personal data, to ensure proper security configurations are always in place to address known vulnerabilities.

Symantec offers customers a Data Loss Prevention (DLP) risk assessment to help proactively identify threats to the organization's data before they become a major liability. The process consists of a passive DLP monitoring and discovery 'scan' on the production network and gives information about risk associated with broken business processes and potential malicious activity. It shows where sensitive data resides anywhere across the network, where it goes and how employees are using confidential data. For instance data aggregated from DLP risk assessments show that 1 in 50 network files is wrongly exposed and 1 in 400 email contains confidential information that may go out unprotected.

Symantec also provides a Cloud Access Security Broker (CASB) shadow data assessment. A CASB shadow data assessment gives visibility into shadow IT usage and identifies risky cloud applications by analyzing logs from proxies, firewalls, and endpoints.

Organizations can finally obtain cyber-risk visibility via Symantec Information Centric Analytics (ICA) powered by Bay Dynamics. By ingesting and correlating a large amount of information from deployed data protection sources and security systems Information Centric Analytics lets you

Recommendations:

- Use these last months wisely, implementation may take longer than you think
- Engage with your Board, report on progress in addressing data privacy through your security program
- Understand, and tackle your big data privacy and security risks
- Document what personal data you hold and ensure lawful use
- Identify where technology can help you achieve compliance:
  - **Prepare:** Understand IT (and data) environment and risks
  - **Protect:** Secure personal data everywhere
  - **Detect:** Breach monitoring and detection
  - **Respond:** Incident Response planning

identify risky users and behaviors that help to define new data protection strategies and fine tune policies. Risk scoring can be calculated based on past and present behavior and data incidents. This User and Entity Behavior Analytics can unveil insider risks that may lead to a data breach.

2 How do I identify and monitor sensitive data, wherever it flows?

To ensure that you are able to adequately protect sensitive data (including that defined under the GDPR) you need to be able to find it on the network (such as in file share, data bases, repositories and on endpoints) and inventory it. Symantec Data Loss Prevention includes the GDPR out-of-the-box and customizable detection policies to automatically look for specific data types that are subject to the Regulation and protect them with appropriate incident responses. DLP monitors data anywhere it is stored and anywhere it is transmitted via network protocols (such as via email or web) or even transferred from endpoints such as to removable storage or clipboard.

For situations where employees are generating data that they know is private, Symantec additionally allows users to simply classify data, as well as applying visual watermarks to inform other users about the sensitive nature of that data.

The integration of Symantec DLP and CloudSOC (a Cloud Access Security Broker) enables sensitive data, be it structured or unstructured, to be equally identified and monitored in the cloud.

DLP also reduces the likelihood of data loss by providing the ability to build automatic notification processes to educate users on behaviors that put personal data at risk.

A significant cause of data breaches is as a result of malicious insiders or unauthorized users having access to data and then exfiltrating it. Symantec Information Centric Analytics correlates user access records with sensitive data use, providing insight into usual, and importantly, unusual user behavior.

3 How do I protect the data, ensuring only intended users have access?

Symantec Information Centric Security (ICS) provides complete protection for personal data throughout its lifecycle with policy driven encryption and access management. It takes advantage of data loss prevention, cloud access security broker and data classification to discover sensitive data and protect it wherever it goes via Information Centric Encryption (ICE). Symantec Information Centric Encryption wraps automated protection around sensitive data when it is shared outside with vendors, partners, contractors and business affiliates. Encryption keys always remain under the organization's own control, maintaining a separation of duty from cloud providers or the security vendor.

Data access is limited to authorized viewers from any location and any device via Symantec VIP two-factor authentication (2FA). With DLP it is also possible to control data transfer to untrusted recipients and third party organizations who may be not GDPR ready yet, and apply geolocation restrictions for users trying to access data in the cloud via CASB Gateway. Finally, access to data can also be revoked at any time from a central location when digital shredding is required.

In addition, Symantec CCS helps ensure the permissions given to users on data subject to GDPR are in compliance with corporate policies and configured based on best practices.

Additional Symantec solutions:

GDPR requires a structured approach to managing private data, and Symantec offers a world class portfolio of products and services to do just this, delivering information security that supports an ongoing data governance process.

- **Technical Risk Assessments**
  Data Loss Prevention (DLP)
  Information Centric Tagging (ICT)
  CloudSOC Cloud Access Security Broker (CASB)
  Control Compliance Suite (CCS)
  Endpoint Management (EPM)
- **Personal Data Protection Everywhere**
  Data Loss Prevention (DLP)
  Information Centric Encryption (ICE)
  Multi-Factor Authentication (VIP)
  Information Centric Analytics (ICA)
- **Web and Cloud Application Security**
  CloudSOC Cloud Access Security Broker (CASB)
  Cloud Data Protection (CDP)
  Secure Web Gateway (SWG)
  Cloud Workload Protection (CWP)
- **Advanced Detection, Remediation and Notification**
  Data Loss Prevention (DLP)
  Complete Endpoint Security
  Email Security
  Data Center Security (DCS)
  Secure Web Gateway (SWG)
  CloudSOC Cloud Access Security Broker (CASB)
  Advanced Threat Protection (ATP)
  Information Centric Analytics (ICA)
  Security Analytics
  Cyber Security Services (CSS)

350 Ellis St., Mountain View, CA 94043 USA
+1 (650) 527 8000 | 1 (800) 721 3934
www.symantec.com

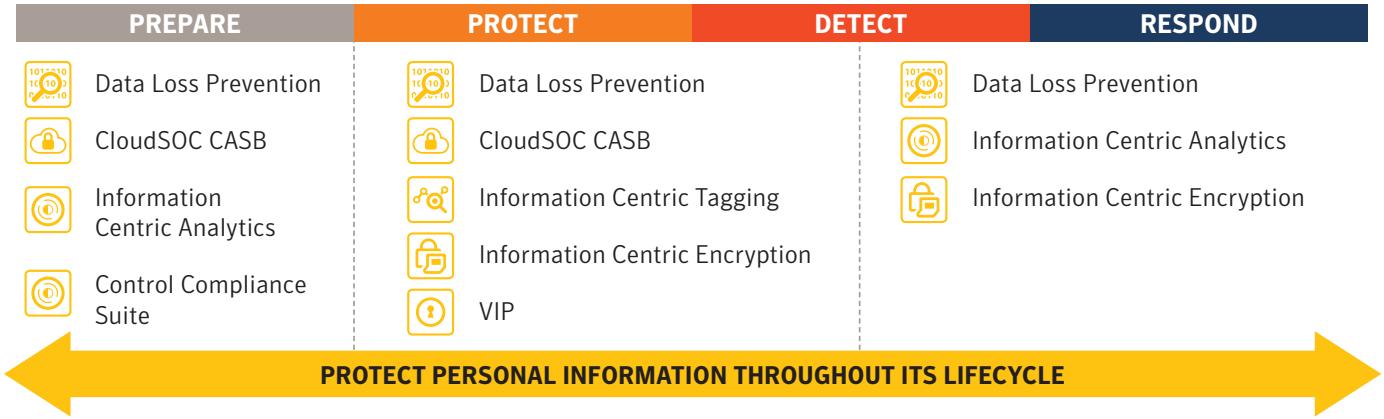
4 How do I discover a breach and how do I respond in 72 hours?

Discovering a breach could be a very challenging task and often organizations realize that they have been breached only a long time after the breach had occurred.

Indication of compromise could be obtained by a variety of data sources but the analysis of such a vast and diverse set of information is resource-intensive. Symantec Information Centric Security provides extensive data protection telemetry that is analyzed all together by Symantec Information Centric Analytics in conjunction with user access (identity telemetry), corporate asset data, and alerts from other security systems (threat telemetry). Information Centric Analytics helps identify an anomalous behavior of a specific user or a machine which can expose a malicious insider or an account-takeover. With drill down functions connecting the user to DLP incidents you gain visibility into the specific sensitive data that was exposed and why. Symantec also offers threat monitoring solutions such as Advanced Threat Protection and Cyber Security Services that are beyond the scope of this paper.

By running an encryption report, organizations can prove data was protected. Central monitoring of data access enables organizations to track sensitive data and to identify by whom, and from where sensitive data is accessed after the breach. Even if data was exposed by authorized users it is then possible to rapidly revoke access. Symantec Information Centric Security helps to investigate a data breach and respond fast.

Symantec Information Centric Security for Data Privacy and Security



Summary

Information Centric Security helps enabling compliance with the General Data Protection Regulation by delivering comprehensive data protection strategy that gives out-of-the-box GDPR policies, verifiable protection of sensitive data in managed and unmanaged environment and investigation analysis to respond to a data breach fast.

To learn more visit go.symantec.com/ICS

19B176377_SB_INFOCENTRICSECURITY_GDPR_EN