3 Essential functions of GDPR and the cloud

By Doros Hadjizenonos

7 Jun 2019

New protections for consumers, such as the EU's General Data Protection Regulation (GDPR) - which is celebrating its first anniversary, and the new California Consumer Privacy Act (CCPA), provide consumers with added protection to ensure their privacy and prevent issues related to data theft or misuse.

Doros Hadjizenonos, Regional Director – SADC at Fortinet

They do this by defining what is meant by personally identifiable information (PII), establishing compliance standards for organisations to meet, and imposing severe penalties for organisations that fail to protect the PII of their customers.

Consumers in control

Some of the most important benefits of these regulations is their uniform definition of exactly what is meant by personal data; detail rules for how that data can and cannot be used by any organisation doing business within a specified region - or with any citizens that reside, work, or travel therein, even remotely; explicitly define what constitutes a breach of personal data along with standardised and consistent notification requirements; and give consumers complete control over the use and storage of their PII.

The GDPR established a common and broader definition of personal data than previous efforts, including things like IP addresses, biometric data, mobile device identifiers, and other types of data that could potentially be used to identify an individual, determine their location, or track their activities.

The CCPA extends that definition even further, adding such things as geolocation data and shopping, browsing, and search histories.

365 days of GDPR: Has the storm passed?
Johan Scheepers 29 May 2019

Further, organisations affected by these regulations not only need to obtain explicit approval from individuals to retain and use their personal data, but also honour their “right to be forgotten,” which enables individuals to demand that an organisation purge any personal data about them for any reason.

Data privacy and the cloud

The challenge is that with today’s highly distributed network, data could have been copied multiple times and distributed virtually anywhere. The recent and rapid transition to multi-cloud networks, platforms, and applications complicates this challenge. To meet data privacy requirements in such environments, organisations need to implement security solutions that span the entire distributed network in order to centralise visibility and control. This enables organisations to provide consistent data protections and policy enforcement, see and report on cyber incidents, and remove all instances of PII on demand.

Providing consistent data protection and policy enforcement

Achieving this requires three essential functions:

1. **Security needs to span multi-cloud environments**.
   Compliance standards need to be applied consistently across the entire distributed infrastructure. While privacy laws may belong to a specific region, the cloud makes it easy to cross these boundaries. Policies and protections established for data in a physical data centre under the control of local privacy laws need to follow data as it moves to the cloud or to other data centres as long as they are stored in the same geography.

   This creates two issues that need to addressed.

   - The first is that you need a mechanism in place to keep track of every instance of that data, especially as it moves into and across multiple applications and workflows. Data has a tendency to multiply and you need a way to manage that information.

   - The second is that you need to ensure consistent segmentation across the entire distributed infrastructure. This becomes a challenge when security policies are confined to specific physical and cloud environments, and security solutions deliver inconsistent enforcement and functionality due to the unique requirements of different cloud environments.

     Security tools need to natively integrate into cloud platforms in order to consistently segment the multi-cloud environment, and policies need to be translated on the fly to accommodate differences in cloud platforms as data moves. And data centres in other parts of the world need to support these new security requirements or they risk becoming the weak link in the security chain.

2. **Data loss prevention is essential**.

Tracking and managing PII requires the implementation of Data Loss Protection (DLP) technologies that can be applied inline as well as at the cloud API level. Such solutions need to be able to identify, seamlessly track, and maintain an inventory of all PII.

A few key principles when it comes to handling and exchanging PII:

- DLP monitoring needs to begin at the point of acquisition or creation of any PII data.
- Data containing PII that is in use by applications or users’ needs to be monitored to be sure it is being securely accessed and processed.
- Data in motion needs to be protected, especially when it is being transferred between different applications or cloud environments.
- Data at rest, whether in the cloud or in a physical location, needs to be monitored and secured.
- DLP also needs to track multiple versions of that data - or even pieces of that data - if they are copied, used by different applications, and stored in different locations.

3. **Compliance reporting requires centralised management**.
Compliance reporting needs to span the entire distributed infrastructure. As with other requirements, this also demands consistent integration throughout the cloud and with the on-premise security infrastructure.

   Achieving this requires the implementation of a central management and orchestration solution, such as a SIEM or other single-pane-of-glass management console which has visibility to the entire multi-cloud & security infrastructure.

   What you don’t want is having to hand-correlate data from multiple systems, because things get missed, and if they are found in an audit, the penalties can be severe.

Replace reactive solutions with integrated and proactive strategies

The best approach to security is to stop an attack before it even starts, and limit its scope once a breach occurs. This requires organisations to have technologies and policies in place, such as:

- Advanced prevention and detection tools, including live threat intelligence, hardened access controls, behavioural analytics, and ATP solutions that allow them to get out in front of breaches.
- Intent-based network segmentation, including both network and micro-segmentation, to limit the impact of a breach to a specific data set or network segment.
- Tightly integrated security solutions that talk to each other, share threat intelligence, and coordinate a threat response. These tools also need to be natively integrated into the API infrastructure of the various cloud environments being used, allowing you to enforce policies and respond to breaches consistently across the entire network.
- DLP solutions that allow you to track data and prevent its unauthorised access, use, or transfer regardless of where that data is used, travels, or resides. Important for these solutions to be sharing information across the various protected infrastructures.
- Centralised controls that provide a single point of visibility & control for all data, ensuring that policies and configurations are consistent, breaches are detected and reported, consumer requests are honoured, and compliance reporting is consistent and comprehensive.

When properly understood, privacy regulations not only ensure that the PII of consumers is protected, but they also raise the bar for security across the entire organisation.

It forces organisations to go back to the drawing board, rethink processes and policies, identify and close gaps, and centralise their visibility dashboard feeds and operational controls. Many of these security fundamentals have been lost in the rush of digital transformation, and this is a good excuse to regroup, rethink, and re-secure your infrastructure.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...