Securing Containers for GDPR Compliance.

THALES

March 1, 2018

Juan C. Asenjo | Thales eSecurity Global Partner Marketing

Around the world, enterprises are anxious about May 25, 2018, the day enforcement begins for the European Union's General Data Protection Regulation (GDPR).

They have good reason.

Perhaps the most comprehensive data privacy standard to date, the GDPR presents a significant challenge for organizations that process the personal data of EU citizens – *regardless of where the organization is headquartered or processes the data*. And, with potential fines of up to four percent of global revenues or 20 million EUR (whichever is higher), the GDPR has the attention of CEOs and Boards of Directors. No matter where your organization is located, if it processes or controls the personal data of EU residents, it must be in compliance with GDPR, or it will be liable to significant fines and the requirement to inform affected parties of data breaches.

We at Thales have blogged about the GDPR, its global impact, reach, and penalties. My purpose here is to provide guidance on how enterprises that are using, or are planning to deploy, container technology can ensure these are secured for compliance.

Container Adoption and Security Concerns

Nearly one-quarter (24%) of the respondents to the 2018 Thales Data Threat Report (DTR) survey[1] indicate they already are using containers in production. This shows a rapid adoption of an only recently commercialized technology.

Also according to the 2018 DTR, the top security concern globally for container environments is the "security of data stored in containers." And, close behind that, in third place is "unauthorized access to containers."

It is no surprise that the container security concerns of the senior security executives surveyed, and what the GDPR requires for compliance, seem to be walking hand in hand.

recently commercialized technology.

Also according to the 2018 DTR, the top security concern globally for container environments is the "security of data stored in containers." And, close behind that, in third place is "unauthorized access to containers."

It is no surprise that the container security concerns of the senior security executives surveyed, and what the GDPR requires for compliance, seem to be walking hand in hand.

GDPR Data Security Requirements

The GDPR calls for a layered or "Defense in Depth" security approach to protect sensitive data from compromise. Layers should include not only perimeter security, but also, among others as prescribed by GDPR Article 32:

1. Limiting access to data
2. Encrypting or pseudonymization of sensitive data
3. Monitoring and reporting user access patterns

recently commercialized technology.

Also according to the 2018 DTR, the top security concern globally for container environments is the “security of data stored in containers.” And, close behind that, in third place is “unauthorized access to containers.”

It is no surprise that the container security concerns of the senior security executives surveyed, and what the GDPR requires for compliance, seem to be walking hand in hand.

GDPR Data Security Requirements

The GDPR calls for a layered or “Defense in Depth” security approach to protect sensitive data from compromise. Layers should include not only perimeter security, but also, among others as prescribed by GDPR Article 32:

1. Limiting access to data
2. Encrypting or pseudonymization of sensitive data
3. Monitoring and reporting user access patterns

[1]The 2018 DTR surveyed more than 1,200 senior security executives from around the world.