How Endpoint Central helps you achieve GDPR compliance?

Is GDPR your top concern?

GDPR (General Data Protection Regulation) furor has reached its peak and the top concern is to provide any individual the control over his/her personal data by enforcing strict commands over the parties accessing or processing the data across the world.

There is a lot of talk about the GDPR compliance, requirements and the penalties to be paid for non-compliance. This is just nothing! GDPR doesn't say that the enterprises should not acquire or process personal data. Whereas, they have a set of rules, guidelines and best operational practices for fair use of data. These regulations are set just to ensure end user's privacy.

Refer to the below mentioned articles on how to comply your user's device with Endpoint Central

1. How to configure GDPR related settings in Endpoint Central?
2. Endpoint Central DPO dashboard
3. How to become GDPR compliant with Endpoint Central?

How benefited are you?

The primary focus of GDPR is to provide end users the right to see through how, where and what amount of their personal data is stored, processed and used. Here the personal data refers to any information that directly or indirectly reveals the identity of a natural person. GDPR empowers an individual to -

1. Become aware on how their personal data is being used.
2. Obtain information on the data being used, processed or stored in any enterprise.
3. Demand any enterprise to completely remove their personal data.

Conceal Private Data while reporting

Generating or exporting reports for various purposes creates all the possible odds and puts user's private data at risk. With Endpoint Central **Report Settings**, you can choose to mask/hide all the personal data while generating reports. This way, even while sharing the generated reports, you can protect the end user's personal information from getting spilled over.

Role based access control

Do you have too many users working with Endpoint Central and you let them access every detail of your enterprise? With **User Management**, you can tailor roles or use the predefined roles to define scope for each user/technician and refine them from accessing information elevated to their privilege.

Breach Notification

With data security and user privacy being the prime focus area of Endpoint Central, whenever a vulnerability is detected it has a mechanism in place to notify the users about any possible threats immediately, along with its effects and relevant fixes.

Right to Erasure

User data is stored in the product database in the customer environment. Whenever a user is removed from the product, no personal information about the user is retained except the user name which is necessary for audit logging.

Right to Information

Endpoint Central users have complete visibility and control over the amount of data being obtained, processed, or stored as the data resides only in the customer environment.

Secure your communication

Endpoint Central processes personal information in an enterprise such as computer name, user name and IP address. There is always a constant flow of data as the agent communicates with the server, additionally, there is transfer of data between the central server and the integrated applications, hence emerging the need for secure communication.

Endpoint Central ensures secured communication through implementation of specific security strategies and configurations that aid in hardening the basic communication infrastructure.