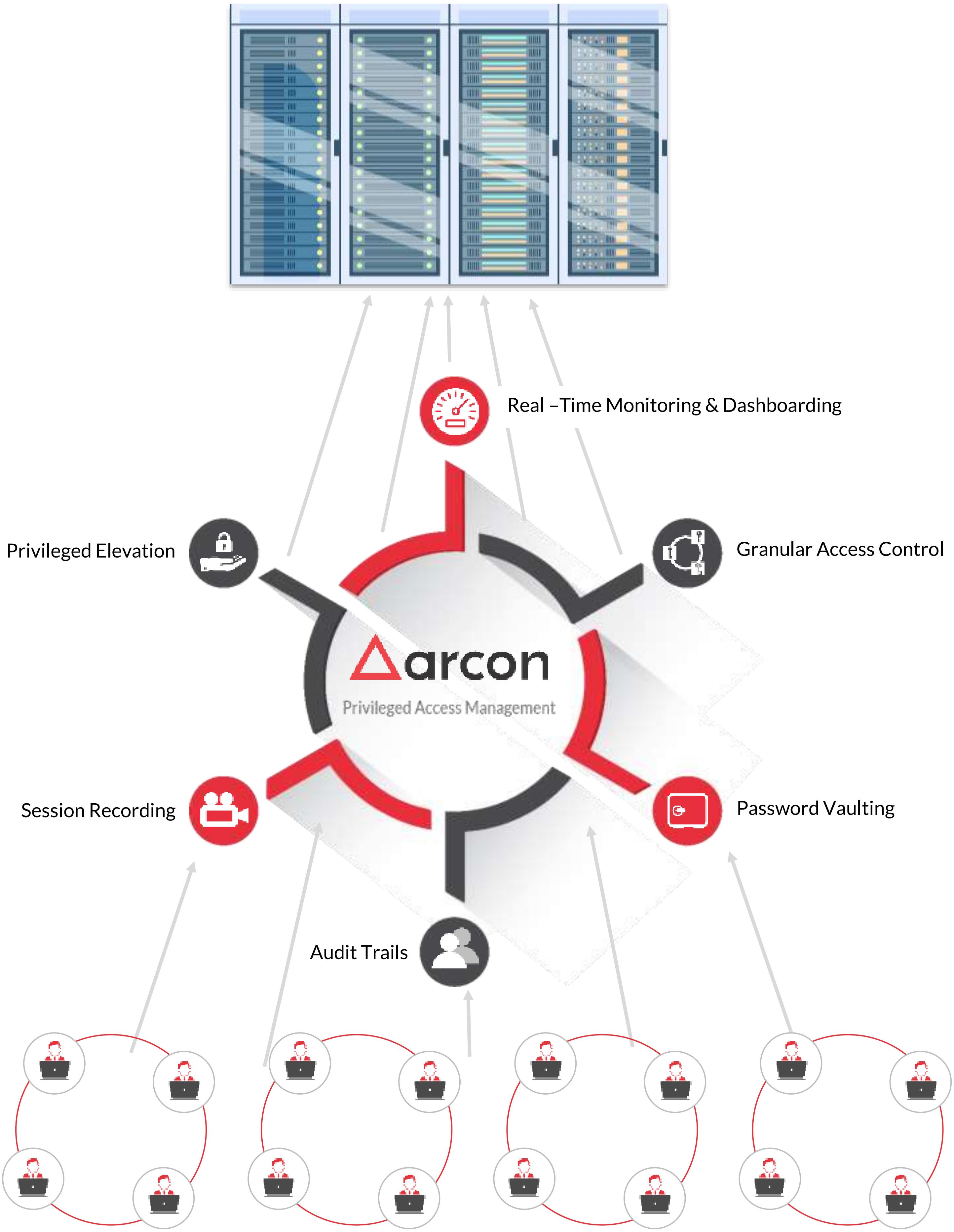
Predict | Protect | Prevent

The General Data Protection Regulation

Protect your Critical Information with ARCON | PAM



The General Data Protection Regulation (GDPR): An Overview

The EU General Data Protection Regulation (GDPR) is a global compliance standard that mandates protecting and securely processing the personal identifiable information (PII) of European Union (EU) citizens. The regulation states that an organization cannot process the PII of data subjects without their consent.
The GDPR is applicable to every EU-based organization (of all shapes and sizes) that stores and processes personal information of EU data subjects. **In addition, a non-EU organization is required to comply with the regulation if it does business with an EU based organization or stores and process PII of EU citizens.**

Moreover, a data controller and data processor is equally liable to protect the PII if it has an existing contracts with third parties such as Managed Service Providers (MSP) and Cloud Service Providers. The cost is huge for failing to comply with the GDPR. Organizations can be fined up to 4% of annual global turnover or €20 million (whichever is higher) in case of noncompliance with the regulation.

What the EU GDPR expects from organizations?

To ensure a successful implementation of the GDPR, organizations will need to reinforce their information security framework. Every layer of the IT infrastructure through which data flows will have to be identified and risk points mitigated. Accordingly, the Data Protection Officer (DPO), as mandated by the GDPR for organizations controlling and processing PII in a large scale will need to ensure appropriate safeguards to protect sensitive information.

The GDPR effective from May 25, 2018 is broad in its scope addressing various security concerns and gaps (99 articles). However, from a secure data processing standpoint (in the context of privileged access management) proactively implementing the following articles are very important:

GDPR: Article 25

Implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

GDPR: Article 32

A data Controller and data processor must take steps that ensures any natural person with access to personal data does not process the data except on instruction of the controller, processor, European Union law or member state law.

GDPR: Article 33

a) In the case of a personal data breach, the controller shall without any undue delay and wherever feasible, not later than 72 hours, after becoming aware of it, notify the personal data breach to the supervisory authority

b) the processor shall notify without undue delay after becoming aware of personal data breach

These articles imply that organizations will have to:

- Formulate a centralized policy engine to authorize end-users access to database and applications
- Apply the principle of least privilege to protect & securely process confidential data
- Segregate end-users and user group's access to databases and applications according to their job functionalities and privileges
- Apply granular level access control over end-users
- Secure third-party access to IT systems
- Ensure third-parties (MSPs and Cloud Service Providers) are GDPR compliant
- Control and monitor every activity around critical database and applications
- Ensure access credentials to critical systems are securely managed and frequently rotated
- Ensure access to any underlying target systems is only after a thorough authentication process
- Possess real-time threat analytics capabilities
- Record sessions of all critical/privileged activities in an IT environment
- Capture audit logs of every critical sessions to identify anomalies

The challenge

While information technology has allowed global organizations to streamline business operations, securely managing and processing data remains a challenge. The digital workspace is expanding. Within an organization, confidential information is stored in multiple layers of IT infrastructure.

It becomes a daunting task to keep a check on hundreds or thousands of end users that have access to this critical information. Accidental or intentional data breach threats always linger. Also, a highly distributed and shared IT environment makes even more difficult for the security and risk management group to keep a control over confidential information. A growing number of organizations are migrating data centers to public cloud service providers and outsourcing key IT processes to manage service providers (MSPs). This transition is giving rise to shared vulnerabilities. It expands the attack surface.

Protecting data at the core of your enterprise

The GDPR requires an organization to reinforce privileged identity access controls and monitor end-Users

The essence of the GDPR is to securely process the confidential information of EU citizens, conditionally upon their consent. To comply with, the first step for an organization will be to do a comprehensive mapping of the IT ecosystem. It will have to identify all the databases and applications that store the PII and other mission critical information.

Secondly, the Identity and Access control Management especially the Privileged Access Management will require a closer look. Organizations will need to be vigilant about who is accessing what from where and when. With typical mid-scale organization managing 500-1000 privileged accounts, controlling and monitoring end user activity becomes an uphill task. Typically, confidential information such as PII is accessed through privileged accounts. Misuse of privileged accounts is one of the biggest sources of confidential data breach.

Therefore, it is extremely crucial to protect the privileged accounts. Privileged Access Management builds a foundation for best practices in identity and access control management. In addition, it provides a single window for all administration activities improving efficiency and productivity.

The GDPR compliance is incomplete without ARCON | Privileged Access Management solution

The GDPR is the biggest push towards data privacy by default and design. Essentially the regulation mandates that every layer of IT infrastructure (database, application) and business process is embedded with a well-defined data security policy framework which includes identity and access control measures.

ARCON | Privileged Access Management (PAM) suite enables an organization to overcome identity & access control challenges faced by an organization.. Trusted by 250+ enterprise customers across the globe, this highly scalable solution helps in integrating all the IT elements under a single centralized IT policy framework. The solution reinforces an organization's access & control mechanism through real-time monitoring and controlling of end user activities around privileged accounts.

1. Regulate end user activities and secure IT ecosystem through centralized access control policy

ARCON | PAM suite enables an organization to build a robust governance framework. Typically, privileged users have access to sensitive data such as payroll, HR records among many other forms of confidential information. It is imperative to ensure that only authorized end users have access to these database.

ARCON's secure gateway server serves as a centralized policy engine to restrict, control, and monitor privileged users. It allows an organization to assign and segregate end-users with access to target systems based on duties. Thus, it mitigates the chances of illegitimate data processing or data breach as all end-users are granted access to any database only on centralized governing policy. All administrators, IT operators and other privilege users are allowed to login to any target systems only on 'need -to-know' and 'need- to- do' basis.

2. Restrict control and secure IT environment through granular level control and multi factor authentication

ARCON | PAM enables an organization to restrict, control and temporary elevate IT admin / privileged user access to critical database through robust access control mechanism.

The solution minimizes the risk surface by providing deepest levels of granular control over data controllers and data processors.
Granular level control restricts and controls privileged user commands to control critical activities on target devices. Privileged Elevation and Delegation Management (PEDM) enables to control and monitor non – admin users having temporary elevated rights to systems. The solution enforces the principle of least privilege.

There is an always a risk of compromising systems in environments where 'privileged passwords' are manually managed. A security layer of ARCON Password Vaulting provides a resilience against data theft and unlawful data processing. It enables the security staff to generate and change passwords in a highly secure manner.

Managing multiple 'privileged passwords' is a daunting task. ARCON | PAM includes a highly advanced Password Vault which generates strong and dynamic passwords according to the frequency requirements for several devices and systems. This feature will assuage security concerns for the DPO as ARCON Password Vaulting ensures no misuse of privileged credentials.

In addition, ARCON's multi-factor authentication mechanism will make your IT environment impregnable to possible unauthorized access to critical systems. The solution has an inbuilt dual factor authentication feature, but it also easily integrates with other authentication devices such as Access Cards, Biometrics, RSA Tokens and Vasco Tokens.

3. Monitor end user activities through dashboarding, real-time alerts, session recordings and audit trails

Notifying the supervisory authority in the case of data breach is also a prerequisite to implement GDPR. ARCON | PAM reinforces enterprise security with real-time threat analytics to spot anomalous activity and prevent data breach in real-time. Through audit trails and session recording all privileged user activities are centrally monitored.

It enables the security and risk management team to capture all logs performed by every end-user in a video and text format. It proactively secures all databases and applications as every command or query executed by the end users are captured.

In addition, it allows the security team to set real-time alerts for any critical command/query executed by an end user on the target device. This feature also equips the security team to suspend activities in case of anomalous privileged activities are found.

Advanced capabilities such as customized reporting, dashboarding, real-time alerts and priviledged user analytics enables IT security team to improve upon privilege actions and decision making.

But that's not all....

A close collaboration among all business functions to maintain data privacy is also important. A successful implementation of the GDPR does not start and end with the Security and Risk Management Group. Although the DPO is mandated to map an Information Security policy, the responsibility to implement it is not restricted solely to one authority.

Data controller and data processor from all business departments will have to be extremely vigilant. For a successful implementation, a data controller (be it in marketing, procurement, operations, HR) will need to be vigilant in protecting PII records of the data subjects.

The GDPR mandates that a data controller cannot process PII unless the data subject has provided an explicit consent. Therefore, every bit of data collected in the CRMs, applications and databases will require appropriate safeguards. Likewise, securing personal information stored in on-premises IT systems (applications and databases) does not make an organization GDPR compliant if its contracts fail to comply with the guidelines.

From CEO to Digital Marketing Team and from HR department to Business Manager, it is essential for business function to be familiar with the GDPR and comply with the regulation.

Conclusion

The GDPR is designed to standardize data privacy laws across Europe. It mandates organizations to reshape the way it approaches data security. The regulation's primary requirement for an organization is to identify all the PII stored in every database and applications before processing it, subject to the consent of data subjects. However, for a successful implementation of the GDPR, a data controller and data processor is required to have adequate information security controls to mitigate threats of PII misuse. Organizations will have to reinforce Privileged Access Control to strengthen data security.

GDPR compliance: Benefits of deploying ARCON | Privileged Access Management

- Ensures PII is not compromised or illegitimately and accidentally processed
- Protects highly sensitive documents and critical corporate information
- Ensures secure third-party access to confidential data
- Keeps the brand equity intact. Legal implications are costly in case of data breach
- Assists implementing data privacy by design, wherein every technology platform, application and process functions under a well-defined security framework and robust control mechanism
- Helps winning the digital trust of customers and all business stakeholders, which will result in stronger business relationship

arcon

About ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us