SECURDPS

Implement a data-centric security ecosystem and protect sensitive data taking advantage of a broad range of integration options

What is it for?

SecurDPS Enterprise allows organizations to take complete control of their sensitive data. Protecting sensitive data with a data-centric security approach helps your organization to comply with privacy regulations, reduce the risk of breaches and monetize valuable data – while improving your competitive advantage.

Today SecurDPS Enterprise is protecting hundreds of millions of payment transactions, healthcare records, insurance records, and more, reliably running in business-critical environments.

Why should I care?

As your business grows, the last thing your organization needs is a data breach, data exposure incident, or a complex security audit to slow your progress. Classic approaches like perimeter defence, identity access management (IAM), and intrusion detection, reduce the vulnerability of your business to malicious attacks. However, attackers have been successful at bypassing those controls. Recent examples show that the costs can become astronomical due to the effects on stock price, customer retention, brand reputation, not to mention regulatory fines. Protecting data at its earliest point of entry into your systems, and reducing the need to expose the data allows your business to continue to operate and comply with regulations, while reducing risks.

How does it work?

Implementing data-centric security requires a platform that not only offers protection methods that fit your use cases – but also integrates easily into your enterprise applications and existing cyber security infrastructure. Ease of integration can be the deciding factor in determining the cost and risk associated with any data protection project.

Protection mechanisms:
Based on your business and regulatory needs, SecurDPS offers various options including tokenization, format preserving encryption, classic encryption, and masking.

With more than 20 years of experience, in data protection, on truly mission-critical systems, comforte is the perfect partner for organizations who want to protect their most valuable asset: their data.

We are here to enable your success by providing expertise, an innovative technology suite and local support.

Learn more

To learn more, talk to your comforte representative today and visit: www.comforte.com.

Follow us on social media:

Implementation:
comforte has designed its data centric security platform to reduce implementation costs and effort to a minimum, shorten project time and avoid service interruptions. SecurDPS offers sophisticated out-of-the-box integration capabilities, enabling implementation without any changes to applications. It provides easy-to-use APIs and allows integration without changing the record format of the original data. Designed for Infrastructure as Code (IaC) and Continuous Adaptive Risk and Trust Assessment (CARTA), SecurDPS Enterprise can be programmatically controlled via its ManagementAPI.

Deployment options:
SecurDPS offers an extremely flexible model that allows multiple deployment options, where the different elements of the solution can run fully distributed across your environment including on-premises, in the cloud or a hybrid combination.

Flexibility:
SecurDPS is built on a flexible, elastic & self-healing architecture that is designed to adapt and adjust to any future changes or new business requirements in your environment. No matter what kind of innovative solutions, new APIs, new business partners or new technologies you need to enable, you can rest assured that your core remains secure.

Access Control and Audit:
SecurDPS allows enterprises to leverage their standard IAM infrastructure for policy management and enforcement for sensitive data. It has built-in audit and analysis capabilities to help security stakeholders make the right decisions.

Which benefits does it provide?

Reduce business liability and avoid accidental exposure by insiders or 3rd party vendors as SecurDPS replaces in-the-clear sensitive data with token values that are meaningless if it is exposed.
Achieve true compliance and reduce dependency on compensating controls as a temporary measure to pass Security Audits.
Monetize data and continue to grow and land new business as you exchange data with other companies in a manner that does not expose sensitive data.