Secure your Business with Data Protection

Your customers demand data privacy and expect that you conduct business with their data in a secure manner. As evident with the alarming rate of data breaches reported worldwide, perimeter defenses and intrusion detection are not enough to prevent data exposure.

Whether implementing a layered security methodology, or taking a data-centric approach, securing your sensitive data is a key component – and this is where SecurDPS Enterprise fits with your Business.

Data breaches can cause severe damages to businesses processing sensitive data. Compliance rules and regulations require organizations to develop sound security strategies in order to protect their valuable data assets. For example, PCI-DSS demands Primary Account Numbers (PAN) on payment cards to be rendered unreadable whenever stored, and HIPAA provides data privacy and security provisions for safeguarding medical information. Additionally, GDPR, which goes into effect May 2018, provides international rules and requirements around data protection laws and rights that are crucial to businesses and individuals.

Reducing compliance burden is just one driver – minimizing risk, or at least lowering the impact of risk, is another one. It is an understood fact that attackers are constantly seeking ways to circumvent data security to gain access inside organizations. However, as many industry reports have shown, when it comes to a data breach, the costs can become astronomical due to the effects on the stock price, customer retention, and brand reputation.

Another driver motivating companies to protect sensitive data is to stay competitive, and to gain new business. Some organizations will only work with companies who have the ability to share data that is already protected, rather than having to carry the responsibility of protecting the data themselves. Companies who have the ability to protect data in this aspect will be in a better position to attract new customers.

Instrumenting existing applications with a compliant data-at-rest protection mechanism, however, can be a daunting task. SecurDPS Enterprise provides the technology to successfully protect any sensitive data at rest with minimal efforts and without changing existing applications. SecurDPS Enterprise allows organizations to take complete control of their sensitive data, lowering compliance costs and significantly reduce the risk of data breaches.

Using SecurDPS Enterprise your business can

> Reduce business liability as SecurDPS replaces in-the-clear sensitive data with a token value that is meaningless if it is exposed

> Achieve true compliance (PCI, HIPAA, GDPR) as SecurDPS reduces compliance scope by meeting the requirement for no sensitive data on your core enterprise components

> Avoid accidental exposure by insiders or 3rd party vendors since sensitive data will no longer be in-the-clear, and will require proper authorization to expose the original data

> Continue to grow and land new business as you exchange data with other companies in a manner that does not expose sensitive data

> Reduce dependency on compensating controls as a temporary measure to pass Security Audits

How does it work?

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

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: data.

SecurDPS has been built from the ground up to best address data security in a world that is driven by digital business innovations, empowered customers and continuous technology disruptions.

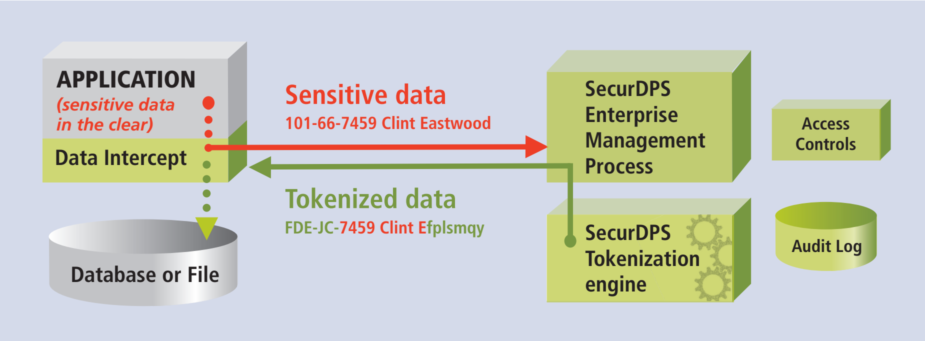
We are here to enable your success by providing expertise, an innovative technology suite and local support.

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

SecurDPS Enterprise runs directly on your existing hardware or virtualization environment, and takes the responsibility of securing sensitive data and meeting key compliance and regulation requirements.

SecurDPS Enterprise uses the well-established data-intercept approach to insert a protection layer into your business applications. Combined with advanced mechanisms for locating sensitive data, SecurDPS Enterprise operates transparently from your application – meaning your Development team does not need to make source code changes to your business applications in order to secure the data.

Without changing the record format of the original data, the patented tokenization capability of SecurDPS Enterprise replaces sensitive data elements with tokens (surrogate values) and ensures optimal performance and minimal impact to your transaction volume or data exchange. Access is allowed to authorized application processes only when needed.


APPLICATION
(sensitive data in the clear)
Data Intercept
Database or File
Sensitive data
101-66-7459 Clint Eastwood
Tokenized data
FDE-JC-7459 Clint Efplsmqy
SecurDPS Enterprise Management Process
SecurDPS Tokenization engine
Access Controls
Audit Log

Besides providing protection for data at rest, SecurDPS also comes with built-in capabilities for protecting data in motion designed for exchange of sensitive files between systems. These files can be protected via encryption or your application can be instrumented to work directly with files on your partner systems via secure SFTP/SSH file transfer, eliminating any intermediate storage on the server.

CAPABILITY	VALUE
Patented powerful security tokenization	Completely remove confidential data from your internal systems by replacing it with random-generated data of no exploitable value to criminals.
Out-of-the-box integration	Spend less DevOps time and costs in order to get to a "protected state" since you won't have to make code changes to your applications.
Granular access control and auditing	Meet compliance requirements by only allowing authorized users and programs access to tokenization, and, by auditing access attempts to your sensitive data.
Elastic and fault-tolerant deployment	Establish a data protection layer that is future proof due to the unique and highly scalable architecture. Different deployment options for on-premises, cloud or hybrid ensure that you stay aligned with your IT strategy. Unexpected failures get resolved automatically without interruption of service or impact to customers.