comforte Data Security Platform - Solution Brief

Digital Complexity Requires Data Protection

Growing complexity of digital business ecosystems. Ever-present data exposure risks. Increased pressure to be in compliance with evolving regulations. These conditions are forcing businesses to find and adopt new data security and privacy standards. Unfortunately, most solutions are proving to be incomplete, overly difficult to use, and incompatible with modern DevOps practices.

At comforte, we take a different approach. With powerful structured data privacy, data security, and automation technology, organizations can be more agile and meet their compliance needs, secure their own applications and products, and embrace SaaS, cloud, and cloud-native strategies.

Agile Data-Centric Security

Even though boundary defenses and access control methods can reduce the vulnerability of businesses to malicious attacks, threat actors are still successfully bypassing these controls. The adoption of cloud services even further deters effective control of the boundaries around their data. One overlooked security hole or vulnerability, and suddenly attackers can find a way through. And this doesn't even account for inside jobs, which are becoming more prevalent too.

Many traditional data security solutions are actually pre-cloud and pre-regulation, with lengthy and complex deployments and only minimal risk mitigation value. Clearly another approach is necessary. We built our data security platform precisely so that businesses have another, and better, way to secure their data.

> *Using comforte's platform we can balance data use, privacy, customer data value, and security under a single integrated and intelligent platform.*

> A reputational event like a data breach can cost your company **billions** of dollars in shareholder value which directly hits your **bottom line**.

comforte delivers a powerful data security platform with integrated security policy management for protecting and governing access to discovered sensitive structured data.

Organizations Need an End-to-End Solution

Power through regulatory roadblocks with measurably reduced risk

1) Protect sensitive data at its earliest point of entry into your systems

2) Reduce the need to expose the data over the entire data lifecycle

These two measures are critical to success with data security and point to the need for end-to-end solutions. Implementing data-centric security requires a platform that not only offers protection methods fitting your specific use cases, but that also allows you to identify and classify data-sets and perform data analytics across all of them. Protecting data requires knowing where data is, and knowing what it is. A data-centric solution must be comprehensive and enable you to integrate these capabilities easily into your enterprise applications and existing cyber security infrastructure.

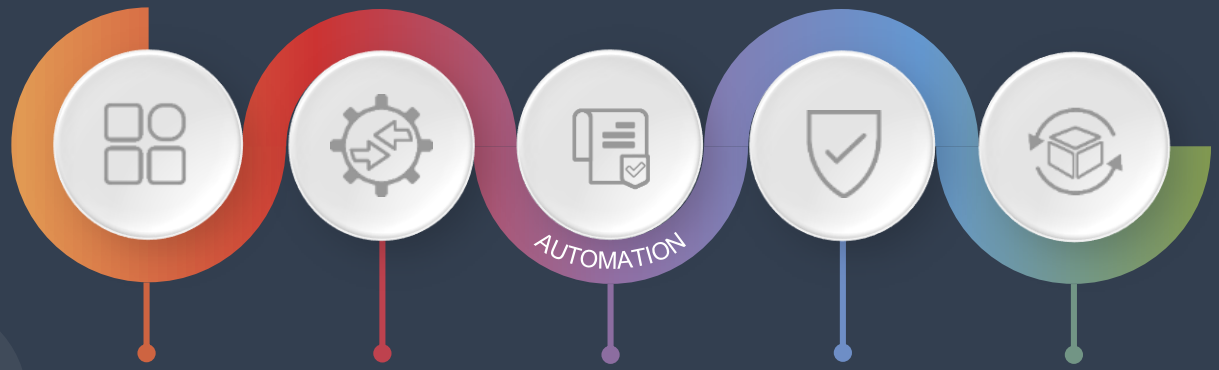
Designed for IaC and CARTA

Full automation for operation, data protection, audit, and logging

Comforte's data security platform is built on an Infrastructure as Code model, enabling automated data security provisioning and delivery with orchestration systems like Kubernetes. APIs enable secure control over system management, operations, and audit streams. In addition to machine interfaces, GUI editors and audit consoles provide simple interfaces for operations.

Our data security platform comprises three integrated services to enable a comprehensive end-to-end data security strategy: SecurDPS Discovery & Classification, SecurDPS Enterprise for data protection integration and monitoring, and SecurDPS Connect.

Today, comforte's data security platform is protecting hundreds of millions of payment transactions, healthcare records, insurance records, and more, reliably running in business-critical environments.



DISCOVER & CLASSIFY
Instrument Sensitive Data Discovery as a Continuous Process

INVENTORY
Identify Data, Ownership, Lineage & Flows

POLICY
Enable Data Security as a Service from the CI/CD

PROTECT
Instrument Data Security in applications.

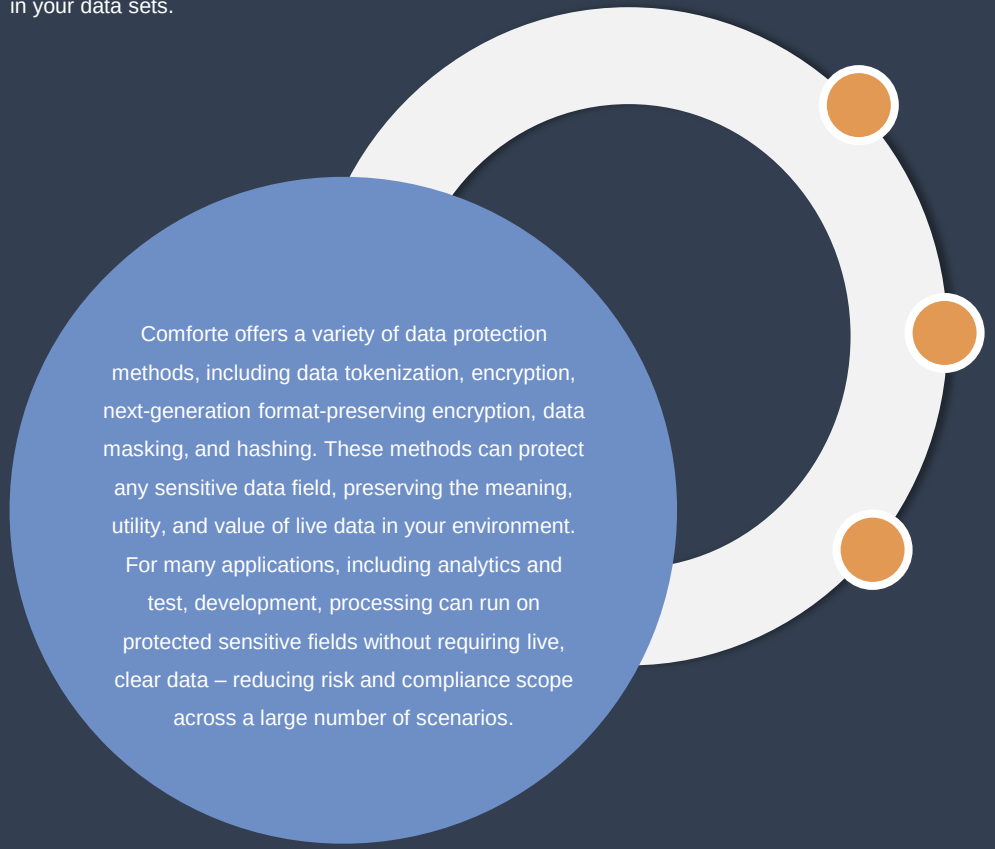
DEPLOY
Reduce implementation costs and effort. No code to low-code.

comforte Data Security Platform

Discovery and Classification

Intelligent and automated data discovery and privacy management for compliance

This AI-driven and policy-based solution can understand the contextual nature of sensitive data and drive ongoing automated discovery. It can learn patterns of identity, scan and sample data to rapidly map where data resides, and help determine which data is regulated and exposed across structured, semi-structured, and unstructured data sets. More importantly, the solution can quickly associate data sets with data lineage and then identify data movement in live applications and workflows, building an up-to-date catalog. This is not only beneficial for compliance but also allows you to manage risk by knowing where potential dangers actually are in your data sets.



Data Protection

Holistic data protection with linear scalability and fault tolerance

comforte's data security platform uses the results of discovery to determine data protection policies. It is a scalable and fault-tolerant solution enabling successful protection of sensitive data with minimal effort and with little to no impact on existing applications. With built-in automatic failover, scaling, and load handling, we've taken care of the complexity so you don't have to—speeding up deployment, avoiding even more complexity, and ensuring business service levels are where they need to be.

Tokenization is provided according to ANSI X9.119-2 standards that comforte helped pioneer, the world's first security standard for such technology, and is now widely accepted in many industries.

Using a micro-services approach, the system is designed for scalability, fault tolerance, and high performance. It handles any outage transparently to the applications that are utilizing protection services.

The protection system that handles the conversion from live to sensitive data enables granular control, visibility, audit, and reporting over all sensitive data access. For policy management and enforcement for sensitive data companies can leverage standard IAM infrastructure. The platform also creates a solid audit trail and allows stakeholders to gain real-time insights around data protection in the enterprise.

Flexibility and Elasticity

From Hybrid to Multi-Cloud to Cloud Native

Comforte's data security platform offers multiple deployment options. The elements of our platform can run fully distributed across your environment including on-premise, cloud-based, or hybrid deployment options. It is already cloud native, with full integration into auto-scaling, self-healing, metrics, logging, operation, and control via APIs in modern stacks and CI/CD pipelines.
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.

Deployment

SecurDPS Enterprise reduces implementation costs and effort to a minimum in order to shorten project time and avoid service interruptions. The basis for our platform is the flexible and sophisticated integration framework, which allows multiple layers of data protection for new and existing applications.

A complete platform *for Data lineage detection across a scaled enterprise, combined with data protection* ***to reduce discovered data risks****.*

Designed *to be operated within* ***modern DevOps*** *processes, integrated into the* ***CI/CD*** *and robotic processes, and taking full advantage of modern* ***application orchestration*** *systems including Kubernetes for* ***automated scale, operation and management****.*

Transparent integration

Comforte's data security platform allows "snap-in" integration to processes identified as high risk during data discovery. In many cases, data protection can be achieved without having to change the respective application. Transparent integration is also available for files, streams, databases and pipes ranging from JDBC intercepts to native Apache Kafka integration. This allows sensitive data to be effectively secured on the fly at capture and therefore over its entire lifecycle.

APIs

Enterprise applications can also utilize powerful APIs including Java, .NET, REST, and modern lean RESP (Reddis standard) for integration in any language or script.

Web, Cloud, and SaaS Applications - rapidly reducing potential exposure

Comforte's data security platform secures data in systems not controlled or managed by your organization. It accelerates protection of structured, semi structured, and unstructured data in modern web, cloud, SaaS, COTS apps, and database-driven applications without coding. It can learn patterns of data use in applications, then instrument data protection automatically.

A modern, reliable data-security architecture

Comforte's data security platform seamlessly integrates with other enterprise data protection solutions and provides a comprehensive and mature set of capabilities that enable data-related risk reduction. The result is a reduced time to success with a more streamlined transition.

Solution Summary

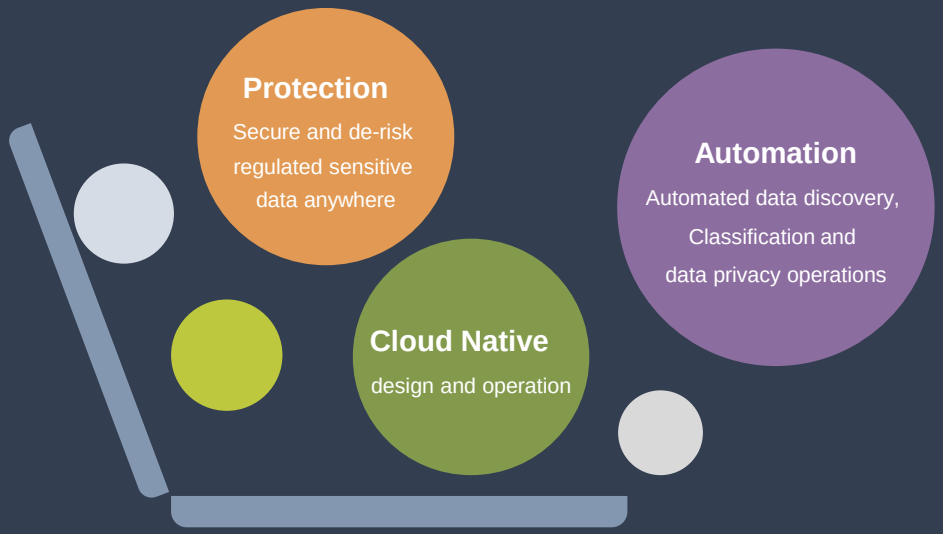
When used together, the full SecurDPS platform can enable organizations to understand all of their sensitive data assets. With powerful levels of visibility—including a better and more rapid understanding of data privacy risks as well as visibility into lineage and use of data—your organization can gain a unique and powerful perspective for planning privacy compliance, implementing cloud migrations, and then measuring your breach risks in a quantitative manner.

Besides discovery, the ability to instrument data protection over sensitive data in a consistent and intuitive manner at scale provides total control over sensitive data, wherever it goes. This facilitates cloud migration, SaaS adoption, deeper data science, and other high-value activities involving sensitive data without data-leakage exposure.

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.



comforte

www.comforte.com