



SecurDPS Enterprise Platform Overview

Felix Rosbach, Trevor J. Morgan



Contents

Introduction.....	2
Digital Complexity Requires Data Protection.....	2
Customer Pain Points	3
Organizational Growth Minus the Operational Roadblocks.....	3
Solution	4
Agile Data-Centric Security	4
SecurDPS Enterprise is an End-to-End Solution	5
Discovery and Classification	6
Protection	8
Protection Methods.....	8
Platform Architecture	10
Integration	11
Transparent Integration	11
SecurDPS Connect Supports Web, Cloud, and SaaS Applications.....	12
APIs.....	13
Apache Kafka.....	13
IT Automation: Designed for IaC and CARTA	13
Solution Summary	14
Main Features That Create Business Value	15
We're Here to Help	16

Introduction

Digital Complexity Requires Data Protection

The growing complexity of digital business ecosystems and the increasing pressure to be in compliance with regulations require new data security and data privacy strategies. comforte's data security platform allows organizations to take complete control of their sensitive data. Our vision, focused on data privacy and security automation, is to enable data digital freedom and simplicity without risk for leading enterprises faced with complex privacy and security regulatory requirements.

Compliance is essential regardless of what you do

And the challenge keeps getting bigger


GDPR

is the biggest thing in compliance yet; failure to comply can incur fines up to €20M or 4% of revenue. Yet, that's really just the start.

Other major regulations and standards include:

IFRS	UDI	KYC
ISO	IEEE	GS1
GDSN	COSHH	EU 1169/2011

The list grows daily, with a new regulatory alert in financial services alone² issued every

:07 
minutes



Customer Pain Points

Organizational Growth Minus the Operational Roadblocks

Today, modern enterprises are faced with a new array of privacy and security compliance risks, from internal concerns over data theft and attack to governmental regulations. Compliance has become both essential and mission-critical given the constant processing and handling of sensitive and regulated data. On top of that, sensitive data exposure from risk vectors including curious insiders, malicious and accidental data loss, and cyber-attack all increase the challenge and complexity. The fact is that these solutions usually necessitate new business processes, including data access and deletion requests, data discovery requests, and investigations.

Unfortunately, new processes can potentially disrupt growth strategies, add operational burdens, and increase operational risk and cost. An optimal solution must leverage automation and assistive technology for speed to compliance and the least amount of business disruption. It also needs to factor in the technology and cultural shift inside businesses to the extreme agility offered by powerful scaled orchestration platforms like Kubernetes, multi-clouds, and modern machine learning tools.

Many traditional privacy management and data security solutions are pre-cloud, and also pre-regulation, with long and complex deployments and only minimal risk mitigation value. The ideal solution needs to help enterprises balance growth objectives, data use, privacy, security, and customer data risk all in equal measures.



comforte's data security platform meets all these challenges. We designed our platform from the ground up specifically for modern, agile cloud-native delivery. This approach enables resilient data-first enterprises to deliver privacy by design in short order, which can also snap into applications, data processes, and workflows. Enterprises using comforte's platform can truly balance data use, privacy, customer data value, and security under a single integrated and intelligent platform. Our customers can make data privacy a business advantage to compete and grow successfully while building customer trust and loyalty.

Solution

Agile Data-Centric Security

Organizations are investing more than ever into data security. Even though classic perimeter defenses, anti-virus solutions, and access control methods are reducing the vulnerability of businesses to malicious attacks, malicious threat actors are still successfully bypassing these controls. Clearly another approach is necessary. Protecting sensitive data *at its earliest point of entry* into your systems and reducing the need to expose the data are best practices for all data protection. This approach allows your business to continue to operate and comply

with regulations, all while reducing risk, but only if you implement protection *across your entire data workflow* instead of just a part of it.

SecurDPS Enterprise is an End-to-End Solution

Protecting data transfer and use from initial data capture to its final destination limits exposure to attack, accidents, oversights, or unauthorized access. The goal in this is to provide these benefits over the entire data lifecycle, helping to meet compliance objectives more quickly.

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. The solution must be able to exceed minimum viable compliance and minimum viable security, while at the same time delivering maximum agility.

It must furthermore enable you to integrate these capabilities easily into your enterprise applications and existing cyber security infrastructure. Ease of integration often can be the deciding factor in determining the cost and risk associated with any data protection project.



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

comforte's data security platform comprises three integrated services to enable a comprehensive data security strategy: discovery & classification, data protection, and platform integration & monitoring.

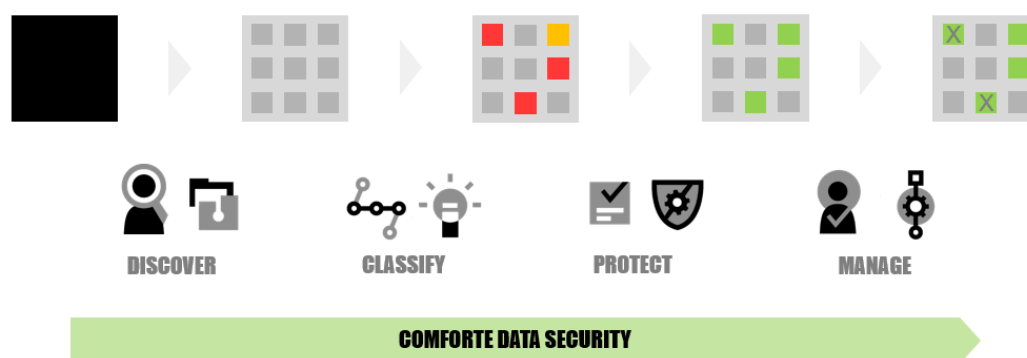


Figure 1. Data-centric security is an end-to-end, iterative process spanning the entire lifecycle of data.

Discovery and Classification

SecurDPS Discover and Classify delivers intelligent and automated data discovery and privacy management for compliance with GDPR, POPIA, CCPA, LGPD, and other regulations. This AI-driven and policy-based solution can understand the nature of sensitive data, learn patterns of identity, and then scan and sample data to rapidly map where data resides which is regulated and exposed across structured semi-structured and unstructured data sets. More importantly, the solution can quickly associate identity data sets with data lineage and then identify data movement in live applications and workflows, building an up-to-date catalog of PII for all unique data subjects.

All of these deliverables are achieved by monitoring network traffic (in specific segments) to analyze data movement, owners, applications, services, and repositories where data and patterns of data go. Our solution approach, as shown in Figure 2, uses a unique and proprietary passive network packet capture process to identify personal information flowing through the organization. This flow visibility enables it to identify repositories (databases, applications, file systems, log files, etc.) where this personal data resides. However, this is

not a one-time approach but rather an ongoing, iterative process of discovery and identification, as shown in the figure below.

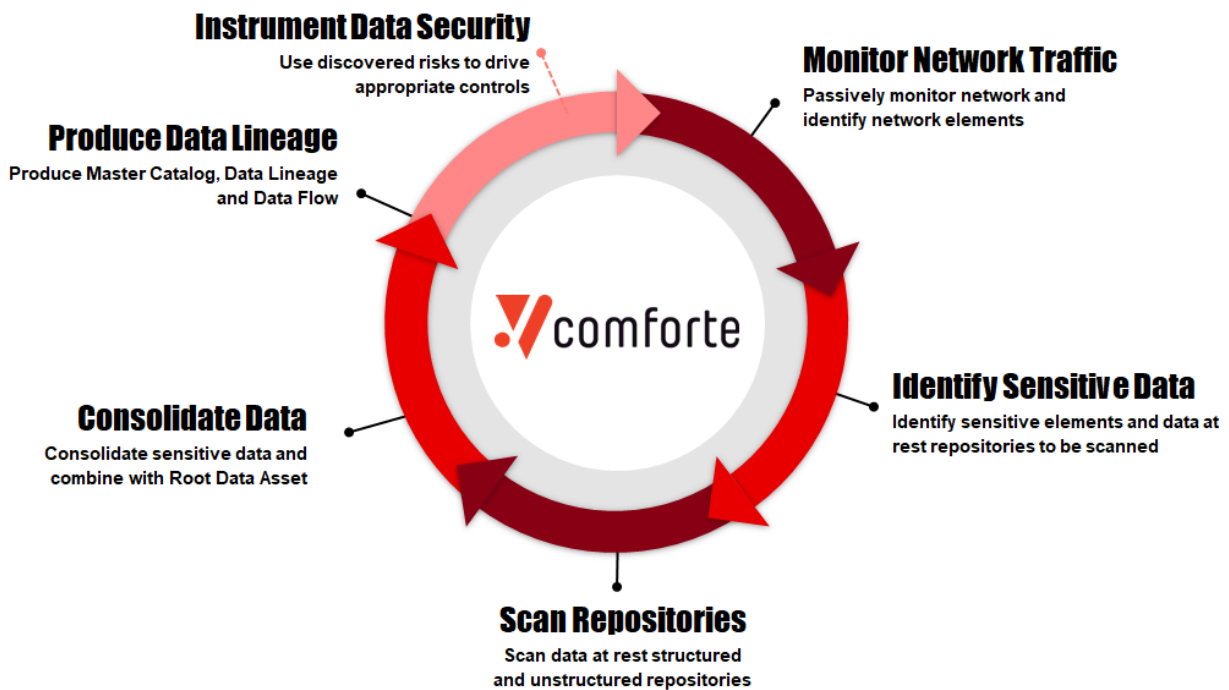


Figure 2. SecurDPS Discover and Classify process provides ongoing, iterative automated discovery, not just single scans.

Any downstream copies of data remain protected, maintaining compliance. Permitted applications and users can have controlled access to full clear data or partial data depending on policy.

Protection

comforte's data security platform uses the output of discovery to determine data protection policies. Our platform 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. It provides protection layers ranging from fully protecting sensitive elements or files using various different data protection methods to auditing user access of a specific database record.

Protection Methods

SecurDPS Enterprise offers a variety of data protection methods including data tokenization, encryption, next-generation format-preserving encryption, masking, and hashing. These methods can be applied to all personal data elements requiring privacy and security remediation and can protect any sensitive data field. Protecting data in our platform, though, preserves the meaning, utility, and value of live data in your environment.



Tokenization is provided to ANSI X9.119-2 standards that comforte helped pioneer, the world's first security standard for such technology, and is now widely accepted. SecurDPS includes automatic stateless key and secret management for tokenization and encryption. HSM support is optional. Full details of method and cryptanalysis are available for review for customers.

Data protection can be fully randomized, or preserve referential integrity across databases so that fields used in primary or foreign keys operate as they did in clear form. For many applications, including analytics, test, development, processing can run on the de-identified data of sensitive fields without requiring live data – vastly reducing risk across a large number of scenarios.

For example, a customer record containing personally identifying data elements can have each element secured such that the data format and structure is preserved. The fully flexible format policy also allows portions of live data to remain in the clear, such as the last 4 digits of a tax ID. A data element thus protected can still be utilized in a process whereby the last 4 digits are used, such as in a call center, yet the full tax ID is not accessible to the application user.



Figure 3. Example record converted into a protected record using one of the available data protection methods while preserving format, structure and referential integrity.

Platform Architecture

Our data security platform aims to provide the highest levels of security and availability. This approach applies not only to the protection services it provides to its users, but also to the overall design of the security-sensitive components and their interactions.

The protection system that handles the conversion from live to sensitive data enables granular control, visibility, audit, and reporting over all sensitive data access. 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.



Flexibility and elasticity:

SecurDPS is designed to adapt and adjust to any future changes or new business requirements in your environment. 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 in a hybrid combination. 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:** SecurDPS allows enterprises to leverage their standard IAM infrastructure for policy management and enforcement for sensitive data. For cases in which live data is required for authorized use, data access and protection occur in highly secure and high-performance Protection Nodes, ensuring data access operations are strictly governed.*

***Analysis & Audit:** SecurDPS Enterprise has built-in audit and analysis capabilities to help different IT or security stakeholders make informed decisions. The captured metadata creates a solid audit trail and allows stakeholders to gain real-time insights into key questions around data protection in the enterprise. The visualization & presentation is not limited by SecurDPS Enterprise to what is provided out-of-the-box, but can easily be integrated into existing security information and event management (SIEM) frameworks.*

Integration

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. In many cases, data protection can be achieved without having to change the respective application.

The solution enables snap-in integration to existing infrastructure to allow sensitive data to be effectively secured on the fly at capture and therefore over its entire lifecycle – from data sources like data streams, databases, web data or transactions, to structured and semi-structured data in files, data lakes, and database extracts, JSON, and XML structures.

Transparent Integration

Transparent integration, interception, and interceding technology enable comfote's data protection to be instrumented with configuration and without code changes. For example, comfote's unique Virtual Tokenizing File Systems enables rapid deployment to complex batch and file-based processes, and the SecurDPS Connect technology enables traditional database, cloud, SaaS, web or stream processes, and applications to be transparently secured with granular controls without code change.

Transparent integration for data protection is also available for files, streams, and pipes. comfote's unique transparent integration allows "snap-in" vs integration, to processes identified as high risk during data discovery, and enterprise applications can also utilize powerful REST and modern lean RESP (Redis standard) APIs for integration in any language or script. APIs also enable full automation for operation, data protection, audit, and logging.

SecurDPS Connect Supports Web, Cloud, and SaaS Applications

SecurDPS Connect accelerates protection of structured, semi structured, and unstructured data in modern application and processes, rapidly reducing potential exposure. SecurDPS Connect complements the built-in transparent integration in SecurDPS Enterprise for files and streaming processes, extending it for web, cloud, SaaS, COTS apps, and database-driven applications without coding.

Traditional data security and remediation approaches are either incomplete, such as data-at-rest encryption which exposes data to any and all processes on access, or complicated application integrations requiring substantial change effort and long projects. SecurDPS Connect enables data security and privacy for regulatory compliance, breach risk reduction, and for total control over data in systems not controlled or managed by ABSA. It can learn patterns of data use in applications, then instrument data protection automatically.

SecurDPS Connect integrates with SecurDPS Enterprise for centralized protection policy, audit, data access policy control, monitoring and reporting. Regulated data access is completely audited, allowing full visibility. Event data can be consumed by SIEM systems for irregular data access patterns detection, alerting, and action.

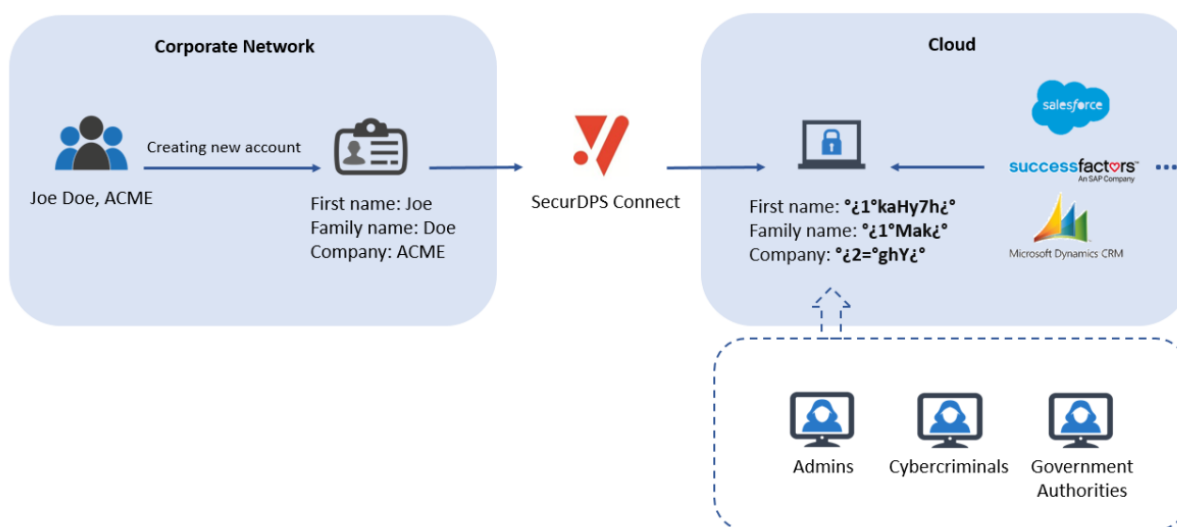


Figure 4. SecurDPS Connect sits between your protected data environment and your web & SaaS applications.

APIs

Applications can invoke APIs which are translated into calls for the respective protection engine. This design allows for modularity between the API and the protection engine underneath. With this approach, the protection engine can be changed at any point in time without any modification to the application.

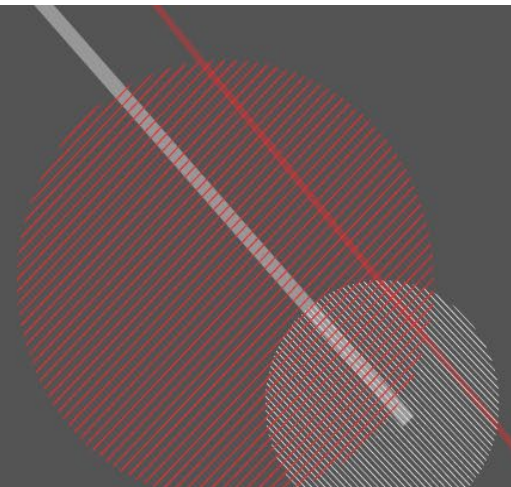
Apache Kafka

Apache Kafka is a distributed, partitioning, and replicating service that can be used for any form of "data stream." While Kafka has many advantages in terms of reliability, scalability and performance, it also requires strong data protection and security. comforte's data protection can be easily integrated into Apache Kafka and the platforms based upon it.

IT Automation: Designed for IaC and CARTA

Two main design goals of SecurDPS Enterprise are to allow for easy deployment and efficient automation. SecurDPS Enterprise is built on an Infrastructure as Code model, with API's for all management, operations, control and audit streams. In addition to machine interfaces, GUI editors, and audit consoles provide simple interfaces for operations.

SecurDPS Enterprise can be seamlessly integrated with other enterprise data protection solutions and provides a comprehensive and mature set of capabilities that enable data-related risk reduction. The result is rapid implementation, short time to success, and streamlines transition to a modern, reliable data-security architecture.



Solution Summary

When used together, the full SecurDPS platform can enable organizations seeking 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 fields 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. The following figure displays the entire scope of this data-centric process enabled by our platform:

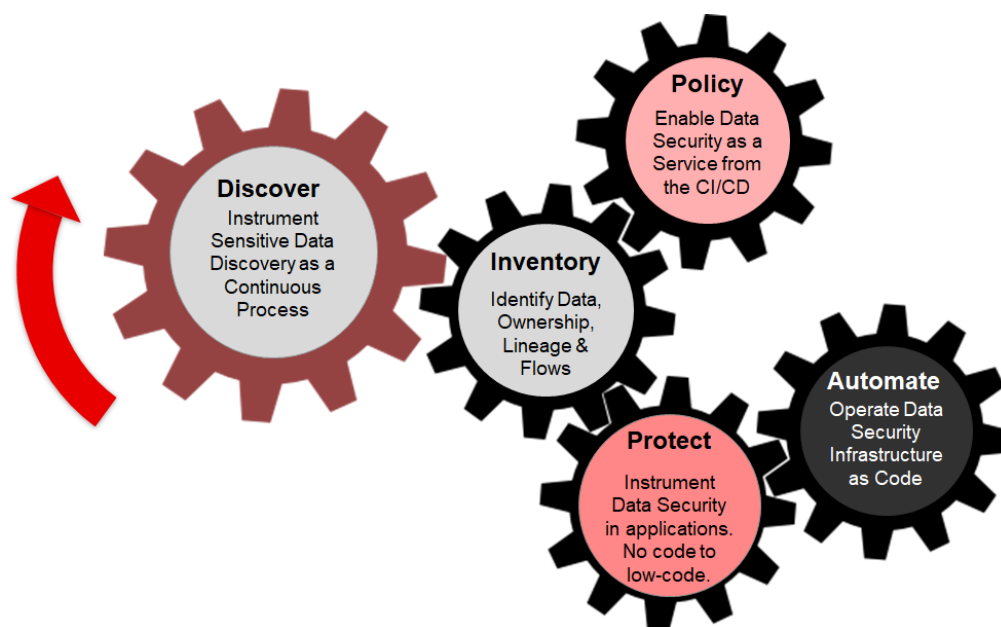


Figure 5. Data discovery drives our end-to-end protection solution.

Main Features That Create Business Value

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.



Automation

Automated data discovery, classification, and data privacy operations



Protection

Secure and de-risk personal data anywhere



Cloud Native

Cloud-native design and operation

We're Here to Help

Today, SecurDPS Enterprise is protecting hundreds of millions of payment transactions, healthcare records, insurance records, and more, reliably running in business-critical environments. comforte experts have implemented the SecurDPS platform for data security and privacy compliance solution in large enterprises and bring decades of experience to client projects for success on a global basis.

As a next step, why not reach out to us so that we can discuss your unique needs and requirements? Look us up at www.comforte.com.

