comforte

SOLUTION BRIEF

COMFORTE DATA PROTECTION

PROTECT ALL YOUR SENSITIVE DATA

All companies retain highly sensitive information about their own employees, intellectual property, and business strategies, but many of them also collect, handle, process, and store highly sensitive information about prospects and customers. This data includes personally identifiable information (PII), payment details, and depending on the industry even health and personal records.

All of this information requires very careful handling and processing, mostly by regulatory mandate but also by the ethics of good business. Keeping customer data safe ultimately means building and maintaining their trust in your organization. How you decide to protect it cuts to the core of your ongoing reputation with your customers.

> Data protection is the most important part of a cybersecurity and compliance strategy

DIGITAL INNOVATION AND HYPER-AGILITY

The enterprise that fully embraces digital innovation gains a distinct competitive advantage.

Trends like digital commerce, digital transformation, and SaaS & cloud services are significant, but they are just milestones in the march to achieve real digital innovation as an aspect of the company's operational strategy.

Digital innovation is multi-dimensional: at the intersection of strategy, technology, process, and invention.

As such, digital innovation as an enabler of business is incredibly powerful—but when the organization makes shortcuts and sacrifices with data protection in order to drive the digital innovation engine, security or compliance become imposing roadblocks.

Don't let data protection pains take away your cloud gains.

68% of industry influencers cited data security as the biggest challenge in moving to the public cloud

THE OLD CONTROLS AREN'T GOOD ENOUGH

Applications and data are so transient now, changing and moving rapidly, one moment in the cloud and the other in the data center.

Traditional controls that come with modern cloud platforms tend to be from a prior generation of data-at-rest and data-in-motion access controls and perimeter-based protections. Unfortunately, these models have proven time and again to be incompatible with the new types of threats that we see.

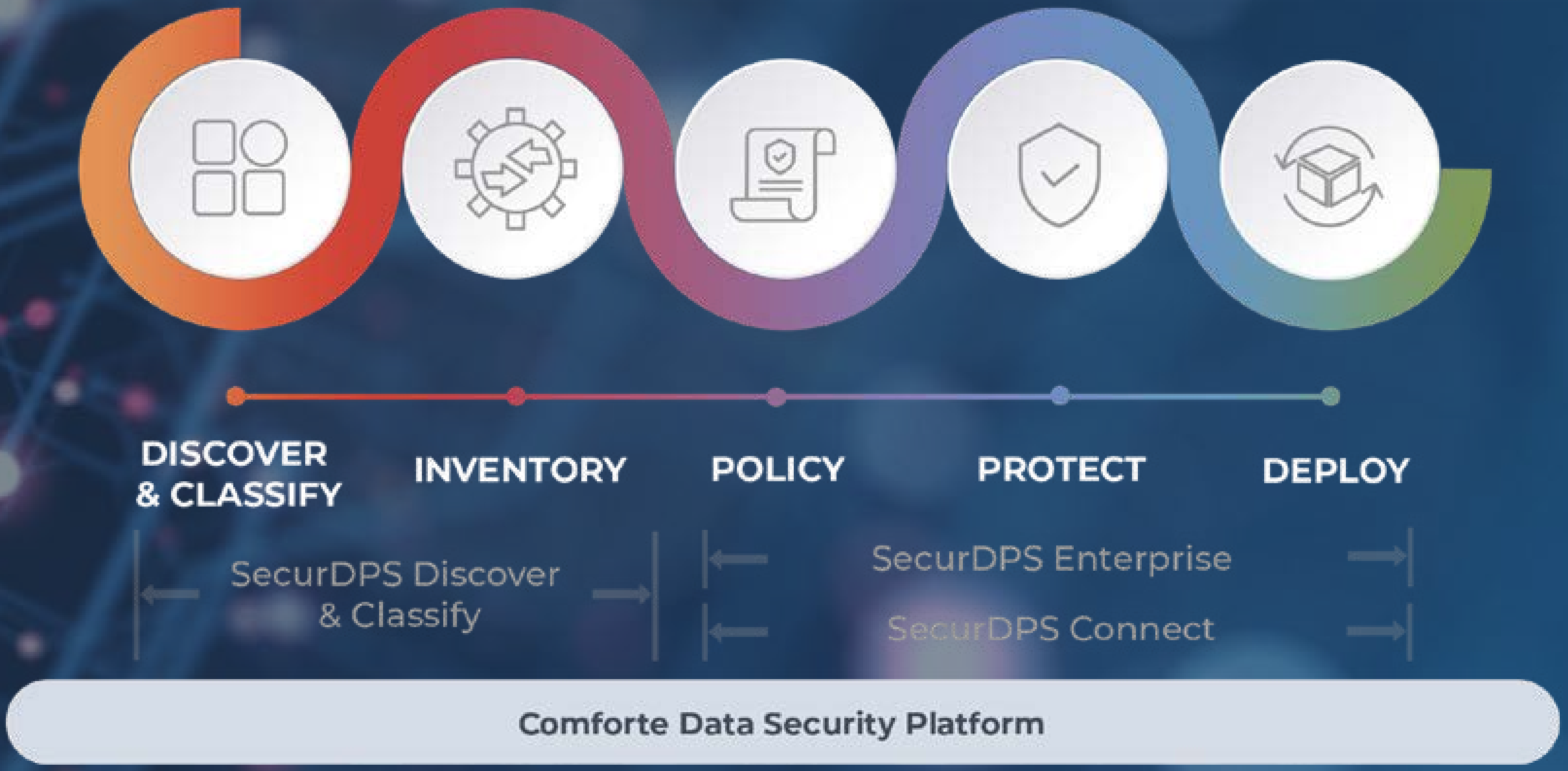
When you combine the adoption of new technologies, hyper-agile processes, and increased volumes of data, these more traditional controls fail utterly—like using a tractor from the 1930s as the centerpiece of 21st century digital-driven farm. It just won't work.

YOU NEED AN END-TO-END SOLUTION

Protecting sensitive data at its earliest point of entry into your systems, and reducing the need to expose the data afterwards, facilitates your business operating within and complying with regulations, all while effectively managing risks.

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, assess, and classify data-sets and perform data analytics across all of them. A data-centric solution must enable you to integrate into your enterprise applications and existing data security infrastructure.

Comforte's data security platform comprises three integrated packages to enable a comprehensive data security strategy: SecurDPS Discover & Classify, SecurDPS Enterprise for data protection, integration and monitoring, and SecurDPS Connect for protecting data in cloudbased services and applications.



DISCOVER & CLASSIFY

INVENTORY

POLICY

PROTECT

DEPLOY

SecurDPS Discover & Classify

SecurDPS Enterprise

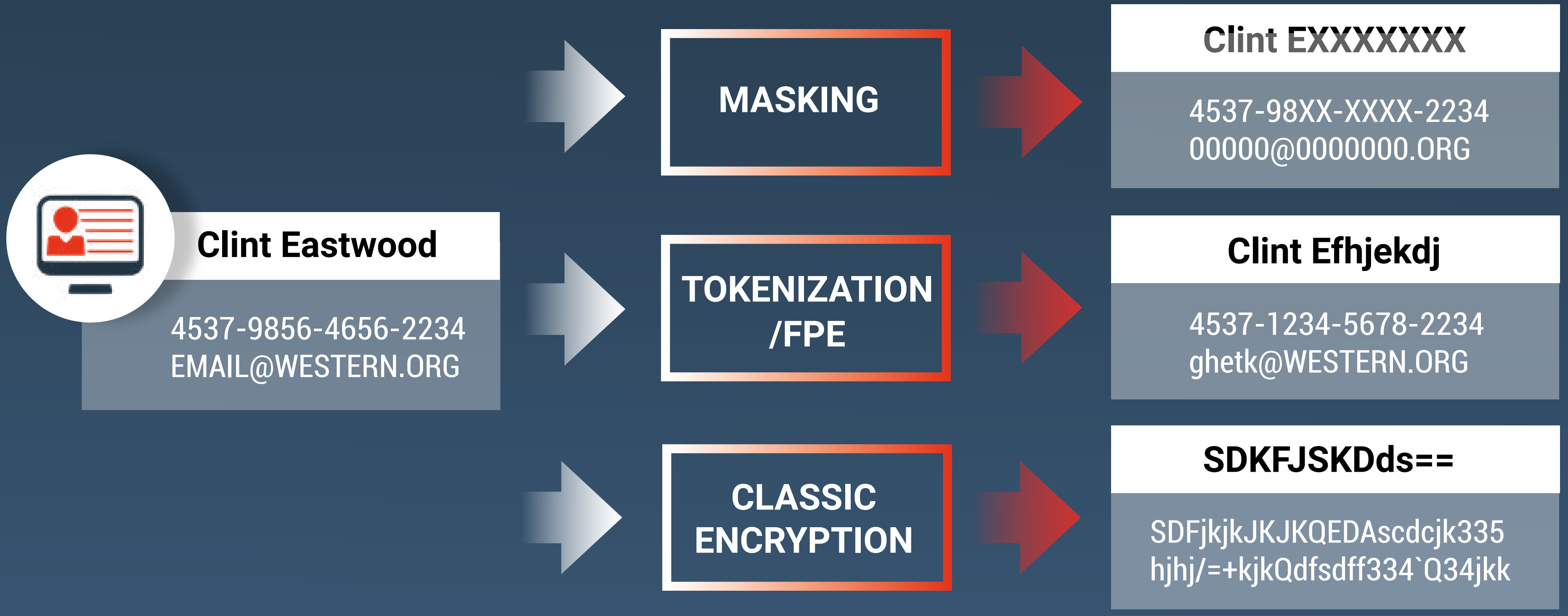
SecurDPS Connect

Comforte Data Security Platform

A BETTER WAY TO PROTECT SENSITIVE INFORMATION

Comforte's data protection suite is a scalable and fault-tolerant enterprise tokenization and encryption solution enabling robust protection of sensitive data with minimal effort and with little to no impact on existing applications. It helps organizations achieve end-to-end data protection, lower compliance costs, and a significantly reduced impact of and liability for data breaches.

> Data-centric security is not only the most important part of a cybersecurity and compliance strategy – it literally changes everything



Clint Eastwood
4537-9856-4656-2234
EMAIL@WESTERN.ORG

MASKING

Clint EXXXXXXX
4537-98XX-XXXX-2234
00000@0000000.ORG

TOKENIZATION /FPE

Clint Efhjekdj
4537-1234-5678-2234
ghetk@WESTERN.ORG

CLASSIC ENCRYPTION

SDKFJSKDds==
SDFjkjkJKJKQEDAscdcjk335
hjhj/=+kjkQdfsdff334`Q34jkk

Comforte was a pioneer in data-centric security methods such as tokenization. As a matter of fact, the industry-accepted tokenization standard—ANSI X9.119-2—is the first security standard for this method and is one which comforte helped to develop. Our data protection capabilities provide security layers ranging from fully protecting sensitive elements or files using various data protection methods to auditing user access of a specific database record.

Comforte offers a variety of data protection methods, including industry-standard-based data tokenization, encryption, next-generation format-preserving encryption, data masking, and hashing.

>> 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 exposed.

>> Achieve true compliance and reduce dependency on compensating controls as a temporary measure to pass security audits.

>> Leverage 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.

THE BENEFITS OF FORMAT PRESERVATION

Creating a balance between utility and security

Due to format preservation and referential integrity capabilities, a business can operate on protected data instead of clear text data for many use cases and operational workflows. Remember, reducing the need to expose data allows your business to operate efficiently, comply with regulations, and mitigate risk.

Our stateless protection eliminates the limitations and complexities of traditional stateful tokenization solutions, which often require synchronization between instances, and which perform much more slowly. They're also more difficult to integrate, adding weeks or months of costly integration activities.

Protection methods by comforte can secure any sensitive structured data while preserving the meaning, utility, and value of live data in your environment. For many applications — including data analytics, AI/ML, and also development & testing — data processing can run on protected sensitive fields without requiring live, clear data. Doing so reduces risk and compliance scope across a large number of workflow scenarios.

Leading enterprises across many industries leverage comforte's data protection solution to secure all kinds of structured sensitive information such as payment data, healthcare records PHI, personally identifiable information (PII), and other sensitive data elements.

GET BACK CONTROL - STOP SHARING KEYS

Typical implementations of classic encryption require protection secrets to be shared among all entities that need access to clear text elements. This results in complex key management and integration and increases encrypt/decrypt cycles. It's tough to manage and even more difficult to audit.

With comforte's data protection solution, the protection system and the underlying protection secrets are only resident in a central system that can consist of multiple distributed instances. With this model, key management complexities are eliminated, and you can easily enforce access control and auditing tasks. Comforte's security-hardened central access system, deployed in a clustered fashion, yields the optimal combination of security, availability, scalability, and reliability.

What makes our solution unique is the utility and control of protection and de-protection operations.

Click to learn more about protection methods

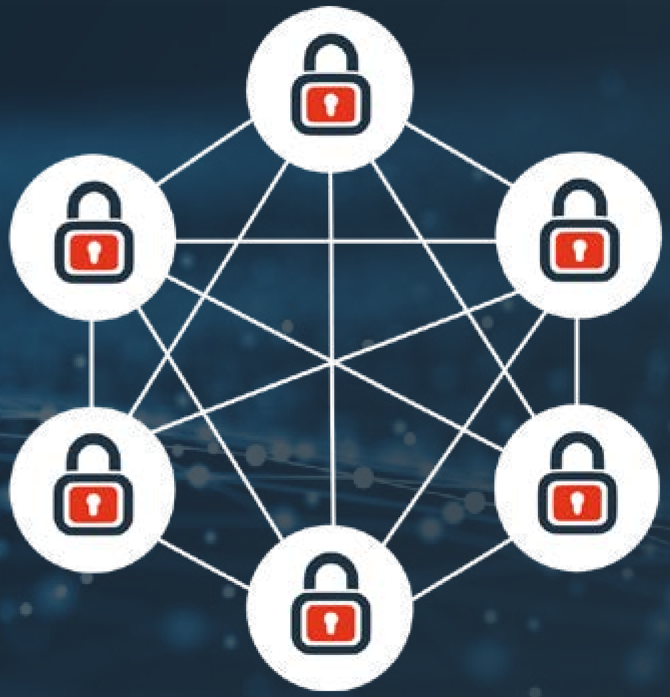
BUILT FOR CLOUD AND AGILITY

Holistic data protection with linear scalability and fault tolerance

Our protection solution is both scalable and fault-tolerant, 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, and ensuring business service levels are where they need to be.

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.



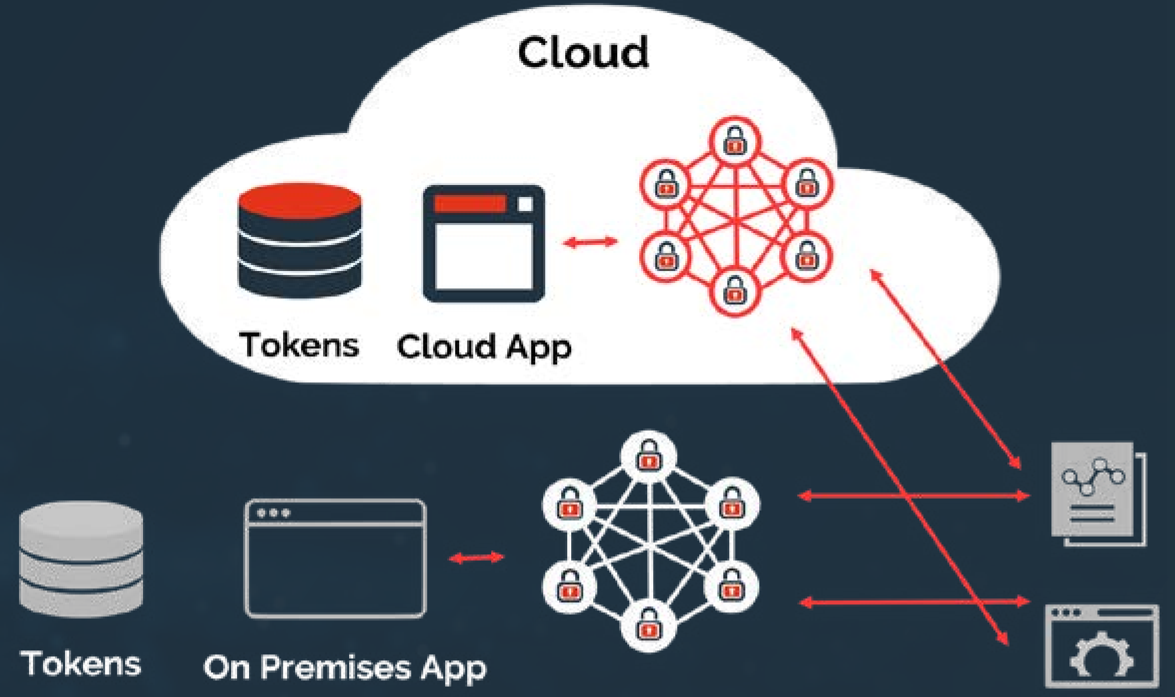
Using a micro-services approach, the system is designed for scalability, fault tolerance, and high performance. It handles any outage transparently to the applications that are utilizing protection services.

FLEXIBILITY AND ELASTICITY

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.



Key differentiator: It's built for the cloud to enable your organization's agility and cloud native focus.

PAY ATTENTION TO INTEGRATION DEMANDS

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

Our entire solution 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.

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.

> A good solution only makes sense when it can also be easily integrated – and that's where we differentiate

Web, Cloud, and SaaS Applications

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.

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.

Apache Kafka

Apache Kafka is an open-source distributed event streaming platform 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.

The protection mechanisms provided by SecurDPS Enterprise can be easily integrated into Apache Kafka and the platforms based upon it (e.g. the Confluent Platform). With Kafka as the enterprise's "central nervous system", data should always be stored and processed in its protected form, and only be revealed on an as needed basis using one of the available integration options.

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 integration options (i.e., Apache Kafka). This allows sensitive data to be effectively secured on the fly at capture and therefore over its entire lifecycle.

For IT security & operations teams

Ease of implementation

Transparent integration capabilities reduce implementation efforts and costs to a minimum. SecurDPS Enterprise enables implementation of data protection in months rather than years and at a fraction of the cost compared to other approaches. It allows integration without changing the record format of the original data. Designed for infrastructure as code (IaC) and a continuous adaptive risk and trust assessment (CARTA) approach, SecurDPS Enterprise can be programmatically controlled via its Management API.

Ease of operations & high availability

SecurDPS Enterprise minimally impacts the applications whose data it protects. The suite makes integration and operations as easy as possible and thus results in a negligible financial impact on cost per transaction. As tokenization touches the heart of your data, SecurDPS Enterprise was designed with maximum scalability and high-availability. You can rest assured that it is a reliable component to protect your mission-critical data.

Your future secured – Providing flexibility and elasticity to ensure business agility

SecurDPS Enterprise 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 be confident that your core will remain secure.

For line of business and risk & compliance teams

Don't let an incident become a data breach

SecurDPS Enterprise tokenization enables comprehensive data protection across the enterprise. Files and databases containing tokenized sensitive data are of no use to an attacker. SecurDPS Enterprise achieves a significant reduction of the impact in the case of a data breach by providing protection without any sensitive data in the clear.

Get it out of the way – Achieving compliance

Reduce dependency on compensating controls as a temporary measure to pass security audits and achieve true compliance (PCI, HIPAA, GDPR, CCPA etc.) by meeting the requirement for no sensitive data on your core enterprise systems and thus reducing compliance scope.

Innovate, differentiate & grow

Leverage data protection as a competitive differentiator against other players in your industry or use it as a value-added service to drive additional revenues. Safeguard innovative developments in your organization and enable a secure basis for company growth.

Our data security platform 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. Today it is protecting hundreds of millions of payment transactions, healthcare records, insurance records, and other personally identifiable information (PII), reliably running in business-critical environments.

At comforte, we understand the importance and value of data protection. For 20 years, we have helped leading organizations worldwide to protect their most mission-critical assets, and we have built long-term customer relationships based on professionalism and trust.

Your next steps

We would love to show you our data security capabilities in action. Contact us to get a demo.

www.comforte.com