Enterprise Tokenization with SecurDPS

Core Concepts & Architecture

CONTENTS

Introduction **2**

Core Concepts **4**

> Data Protection Methods 4

> Classic Encryption 4

> Secure High-Performance Tokenization 5

> Format-Preserving Hashing 6

> Masking 6

> IT Automation: Designed for IaC and CARTA 7

> Access Control and Policy Management 7

> Analysis & Audit 8

> Application Integration 9

> Out-of-the-box Integration 9

> Use of APIs 9

> Apache Kafka 10

Architecture Overview **11**

> Protection Cluster 12

> Deployment Options 13

> On-Premises deployment 13

> Cloud deployment 14

Summary & Conclusion **15**

> Benefits 15

> For IT security & operations teams 15

> For line of business and risk & compliance teams 15

> For your customers – It is all about trust 15

> Conclusion 16

Introduction

The growing complexity of digital business ecosystems and the increasing pressure to be in compliance has led to new levels of awareness and a new sense of urgency in the areas of risk management & data protection. Organizations are investing more than ever in security, to meet compliance demands and to manage risk associated with cyberattacks.

Classic perimeter defence, anti-virus solutions and access control are reducing the vulnerability of your business to malicious attacks. However, threat actors have been successful in bypassing those controls. Recent examples show that the costs of a successful data breach can become astronomical due to the effects on stock price, customer retention, brand reputation, not to mention regulatory fines.

SecurDPS 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.

Introduction

comforte's data protection suite is a scalable and fault-tolerant enterprise tokenization and encryption solution enabling successful 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 significantly reduce the impact and liability of data breaches.

The basis for SecurDPS 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.

SecurDPS 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. Additionally, key protection in Hardware Security Modules (HSMs) and dual custodian mechanisms further secure the data.

SecurDPS 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. This document aims at providing a detailed view of the core concepts and the architecture behind SecurDPS and why it is the best possible choice for your Enterprise-wide data-protection needs.

Core Concepts

Data Protection Methods

Based on your business and regulatory needs, SecurDPS offers various options including classic encryption, tokenization, format preserving hashing, and masking. SecurDPS allows the configuration of any number of protection strategies. A strategy controls how a sensitive data element is protected. Properties of a strategy include the protection method, algorithm attributes, the format (e.g. how many leading and trailing characters are left in the clear), a distinguishing method (i.e. how plain values can be distinguished from tokens), and more.

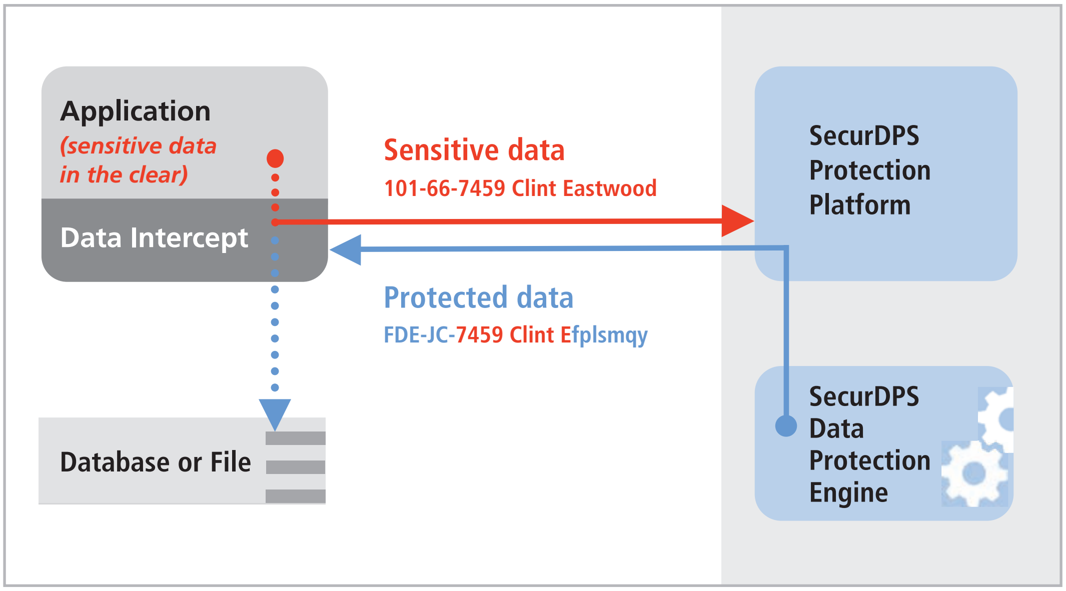

Application
(sensitive data in the clear)
Data Intercept
Sensitive data
101-66-7459 Clint Eastwood
SecurDPS Protection Platform
Protected data
FDE-JC-7459 Clint Efplsmqy
Database or File
SecurDPS Data Protection Engine

Figure 1: Tokenization concept

Classic Encryption

With classic encryption, the protected data element has completely different format properties from those of the underlying sensitive value. In particular, classic encryption schemes (both symmetric and asymmetric) map values to a protected element which has a different length and typically contains values of a completely different alphabet. Especially the change of the length of the value has a huge impact when it comes to the need to implement data protection - existing databases, message formats and applications typically built in a way that the maximum space and format of each data element is predefined.

While this usually results in the need to deprotect sensitive data for application usage and processing, classic encryption has its use cases. Examples are Data-in-Transit Protection for complete streams and Fullfile/device encryption for unstructured data or exchange of sensitive files between systems.

SecurDPS comes with the ability to translate between protection methods (e.g. encrypted to tokenized data) in a secure fashion, reducing the exposure of clear text data in the data life cycle to an absolute minimum and eliminating any intermediate storage on the server.

Core Concepts

Secure High-Performance Tokenization

Tokenization is the protection of data elements in a reversible and format preserving way. Tokenization techniques allow not only underlying data format preservation, but also "prescription" of the appearance of the protected element. This includes, for example, preserving the length of the underlying data or padding it to a desired length. Other options include staying within the same alphabet or transforming the data to a different one, etc.

Format-preserving tokens can be generated for structured data such as credit card numbers, social security numbers, as well as other personally identifiable information such as names or Email addresses.

In particular, the capability of tokenization to preserve the length of the underlying sensitive value provides a huge benefit, as existing applications and message structures don't have to be changed when migrating to using tokenization. This is often a large cost-saver for the implementer.

In contrast, the lack of this format-preserving property in classic encryption prevents its use, especially when dealing with existing systems. Tokenization can be implemented in various ways and with the help of different approaches. The main approaches are: On Demand Random Assignment-based Tokenization (ODRA), Static Table based Tokenization and Encryption based Tokenization (often called Format Preserving Encryption).

SecurDPS offers a set of finely-tuned algorithms that can be chosen to fit perfectly to each sensitive data element that needs to be protected. It provides linearly scalable, high performance tokenization while operating stateless, vaultless and collision-free. Because all tokenization operations happen purely in memory and in CPU, without any disk IO, the comforte solution is more secure. SecurDPS also provides the flexibility to choose the most performant algorithm, while always being 100% secure.

The comforte tokenization approach & algorithm have been vetted by an independent cryptologist and also constitute one of the reference schemes for static table driven tokenization in the ANSI X9.119-2 tokenization standard (C.3.3.2).

Core Concepts

Format-Preserving Hashing

Classic hashes (e.g. SHA256), similarly to classic encryption operations, do not preserve the format of the underlying sensitive values. This can be a problem again, for example, when the size of the field the original sensitive value was stored in is restricted to the format properties (such as length). To address this, SecurDPS Format-Preserving Hashing algorithms can be used to preserve the irreversible protection with deterministic results, but in a way that maintains format properties.

Masking

A typical example of irreversible protection is masking. Masking basically replaces a given number of characters of a value with a set of masking characters. Masking can be helpful to simply hide sensitive values (e.g. replacing all characters with X's), or, to provide sufficient amount of information to identify the data associated with the underlying sensitive value.

Core Concepts

IT Automation: Designed for IaC and CARTA

Two main design goals of SecurDPS are to allow for easy deployment and automation following Infrastructure as Code (IaC) principles, and to allow for easy integration into modern security approaches like CARTA (Continuous Adaptive Risk and Trust Assessment). For this purpose SecurDPS provides a Management API allowing programmatic control of various operations. Beneficially, the need for interactive management access is kept to a minimum.

Access Control and Policy Management

SecurDPS allows enterprises to leverage their standard Identity and Access Management (IAM) infrastructure for policy management and enforcement for sensitive data. Authentication & authorization for users and services is supported through Kerberos, which allows for seamless integration with standard IAM solutions. This also allows for role-based access control to sensitive data elements. Highly granular data protection policies can be tailored to sensitive data elements, defining the protection format and what operations (e.g. protecting or revealing the underlying plain value) are allowed for any given business user.

In combination with an isolation of the protection secret and the use of a central access model, the right to access a sensitive data element can be changed in real time. This allows organizations to take complete control of their sensitive data.

In contrast to other solutions in the market, the Kerberos-based access control with SecurDPS is not limited to authenticating and authorizing the application service from which a user initiates the protection operations. Instead, the authentication and authorization will be performed on both the application that is requesting protection services, as well as the user who performs the request.

Secret Isolation – the Key to Secure Data

When utilizing any form of protection, it is required to not just look at the protection method, but the isolation of the protection system and its secrets. The level of isolation defines how hard it is to obtain unauthorized access to the underlying secrets. There are two isolation models: a) the central access model and b) the shared access model. In a central access model, the protection system and the underlying protection secrets are only resident in a central system that could consist of multiple distributed instances. In contrast in a shared access model the protection technique and protection secret are shared among multiple, different entities.
Compared to the central access model, the shared access model is much harder to secure and audit access for. While with the central access model, access control and auditing can be easily enforced there is risk that the central access becomes a single point of failure. However, a security hardened system deployed in a clustered fashion yields the optimal combination of security, availability, scalability and reliability.

Core Concepts

Analysis & Audit

SecurDPS has built-in audit and analysis capabilities to help different IT or security stakeholders to make the right decisions. The captured meta data creates a solid audit trail and allows stakeholders to gain real-time insights into key questions around data protection in the enterprise. Some of the most common and most important areas would include the following:

> What is the status of the data protection system?

> How many unique/distinct data elements are being protected vs. how many data elements are being protected in total?

> How many sensitive data elements were accessed today? (e.g. how many Social Security Numbers were accessed today/this week/this month/etc.?)

> Am I seeing any peaks in terms of data access to sensitive data elements? By whom? Which application or service? Which data elements?

> Is someone accessing sensitive data elements right now?

> What is the status of the data protection system? Where are the different components running?

> How has my protection system behaved in the past? A historical and current behavior comparison can indicate unusual system behavior.

> Who logged on to the management console? How often and when? What actions have been performed?

Besides providing data & insights to these questions, the visualization & presentation is not limited to what is provided out-of-the-box by SecurDPS, but can be easily integrated into existing security information and event management (SIEM) frameworks.

Core Concepts

Application Integration

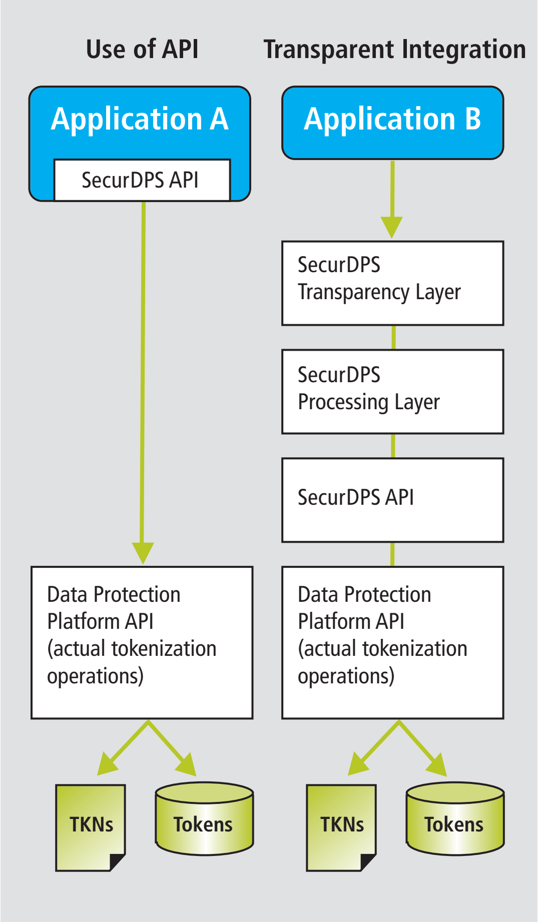
comforte has designed its data centric security platform to reduce implementation costs and effort to a minimum, shorten project time and avoid service interruptions. SecurDPS offers sophisticated out-of-the-box integration capabilities, enabling implementation without any changes to applications. It also provides easy-to-use APIs and allows integration without changing the record format of the original data. Once an organization starts implementing data protection measures, the actual protection of sensitive data is pretty straight forward. The complexity related to integrating data protection services into other applications is the real key in determining the cost and risk associated with any data protection project.

Out-of-the-box Integration

Applications seldom have to be modified to integrate a data protection layer. This simple integration is made possible because SecurDPS provides operating system specific integration capabilities, based on interpose /intercept or virtual file system technology. The underlying data processing layer locates and extracts the sensitive information from the surrounding structures (e.g. ISO8583). The sensitive data elements are passed to the protection engine as outlined in Figure 2. Application-transparent capabilities are available for sequential file processing (e.g. typical payment settlement operations or file transfers) on Windows, Linux, Unix and HPE NonStop (supporting Enscribe, SQL/MP and SQL/MX).

Use of 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.



Use of API
Transparent Integration
Application A
SecurDPS API
Application B
SecurDPS Transparency Layer
SecurDPS Processing Layer
SecurDPS API
Data Protection Platform API (actual tokenization operations)
Data Protection Platform API (actual tokenization operations)
TKNs
Tokens
TKNs
Tokens

Figure 2: Integration options

Core Concepts

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.

The protection mechanisms provided by SecurDPS 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 in its protected form, and only be revealed on an as needed basis using one of the available Integration Options.

For Kafka Producers and Consumers, SecurDPS integration can be performed using the SmartAPI. For Kafka Streams, SecurDPS provides a dedicated passive integration module out-of-the-box to make integration as easy as possible. This transparent integration option does not preclude the alternative of using the Smart API for integration of SecurDPS into Kafka Streams. To integrate data protection into Kafka Connectors, SecurDPS provides dedicated, transparent integration for Kafka Connect, allowing integration of data protection without the need to change the Kafka Connectors.

As a general rule with data-centric protection as performed by SecurDPS, the actual sensitive data should be protected as close as possible to the point of ingestion and only be revealed at the fewest necessary locations throughout the enterprise.

Architecture Overview

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

Protection Cluster

The heart of SecurDPS is the Protection Cluster, a centrally managed, scalable and fault-tolerant cluster of virtual appliances performing the actual protection operations on behalf of the enterprise applications. The Protection Cluster delivers virtually unlimited scalability of the core components through a unique architecture.

The Protection Cluster (PC) consists of multiple clustered soft appliances operating as Protection Nodes (PN's). Enterprise applications (EA's) connect to the PC to protect or reveal sensitive data elements using SecurDPS APIs or the transparent protection layer (Figure 3).

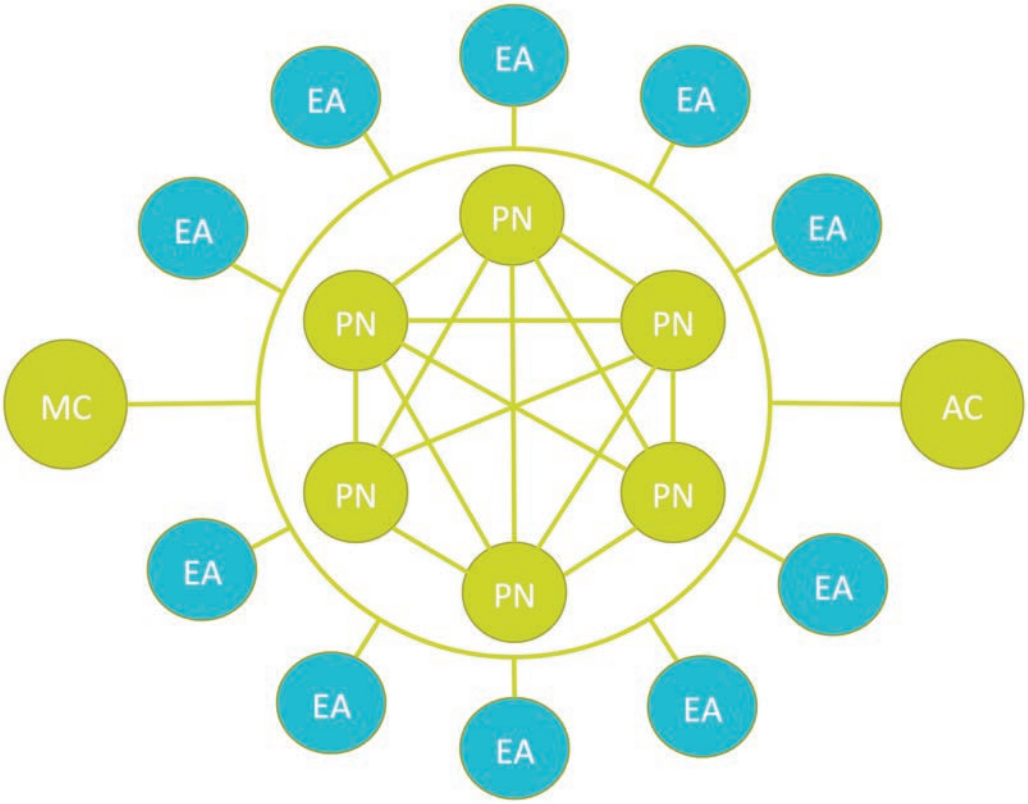


Figure 3: Protection cluster architecture

Architecture Overview

The appliances are based on a highly secure, hardened SecurDPS Operating System (SecurDPS OS). SecurDPS OS provides the absolute minimal functionality required for its purpose. For example, it does not provide any shell or root access. The applications utilizing the SecurDPS client components are granted access via interfaces using strong authentication mechanisms including public key and/or Kerberos authentication.

Any number of PNs can form a PC, distributed across multiple physical servers or datacentres. PNs can be co-located with the servers hosting enterprise applications within the same rack providing optimal performance and minimal latency. The PN does not store any data on a local or network disk and performs all its operations, very securely, in-memory. Data protection is performed using comforte's patented, highly efficient, stateless (aka.vault- less) tokenization algorithm.

The PC is centrally administered through a Management Console (MC). The MC is another hardened appliance which securely stores all configuration data, keys and secrets required for the cluster operation. For the initialization of the PC, the MC loads all required information into the PNs RAM. Therefore, once a PN is powered off, all sensitive data previously loaded from the MC is lost. The PN's in a cluster monitor each other. In the event of a failure of a PN, the remaining PNs will not only take over protection operations on behalf of the EA but will also re-initialize the rebooted PN without involvement of the MC.

Additionally, SecurDPS handles any outage of one or even multiple PNs transparently to the applications that are utilizing protection services. In the unlikely event of a failed PN, processing will automatically switch to other PNs without any interruption of the service for the application. comforte has leveraged its high availability heritage to architect true fault tolerance into SecurDPS.

PN's also send audit information to an Audit Console (AC). The AC collects and displays metrics about usage of protection services by the EA, including the number of distinct sensitive data elements accessed by users in plain text, the number of protection operations per time interval, the number of failed authentications, etc.

Stateless Protection Nodes

The SecurDPS Protection Nodes operate purely in memory and CPU, i.e. without the need to have any access to permanent storage. All context (configuration, keys, etc.) that is needed is injected centrally via the MC. This architecture not only allows for virtually unlimited scalability as no synchronization is required, but also further reduces the potential attack surface. The only place where the sensitive data (e.g. tokenization secrets) is being permanently stored is the MC. The PNs only hold it in memory once they are seeded. Once the PN is shut down, all secrets are gone from the PN.

Architecture Overview

Deployment Options

The following section gives an overview of the deployment options for the elements of SecurDPS: Protection cluster architecture consisting of protection nodes (PN), management console (MC) and audit console (AC). 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 fashion. Following are some of the most common deployment scenarios.

On-premises Deployment

With this deployment option, the management console and the audit console are deployed on-premises and they can either be used in conjunction with a protection node cluster deployed on-premises or in the cloud. Even with a model where protection nodes are deployed in the cloud, security-relevant information is never stored in the cloud and only resides in the memory of the protection nodes.

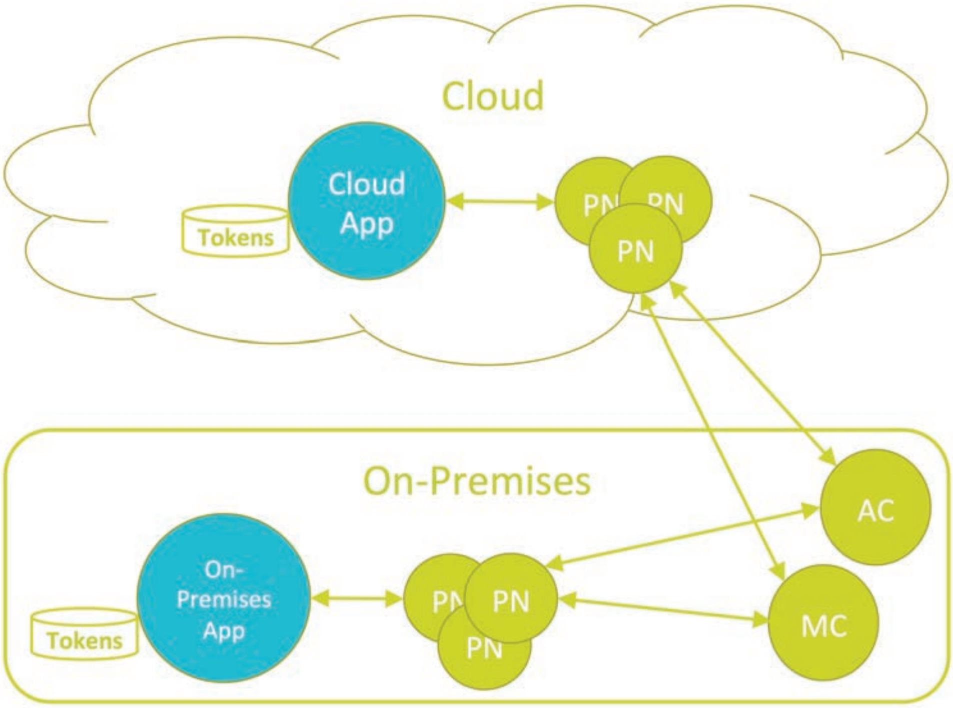


Figure 4: On-premises deployment with protection nodes on-premises or in the cloud

Architecture Overview

Cloud Deployment

With this deployment option, all elements of SecurDPS are deployed on a client's cloud infrastructure and the protection nodes either connect to applications running in a cloud environment or on-premises.

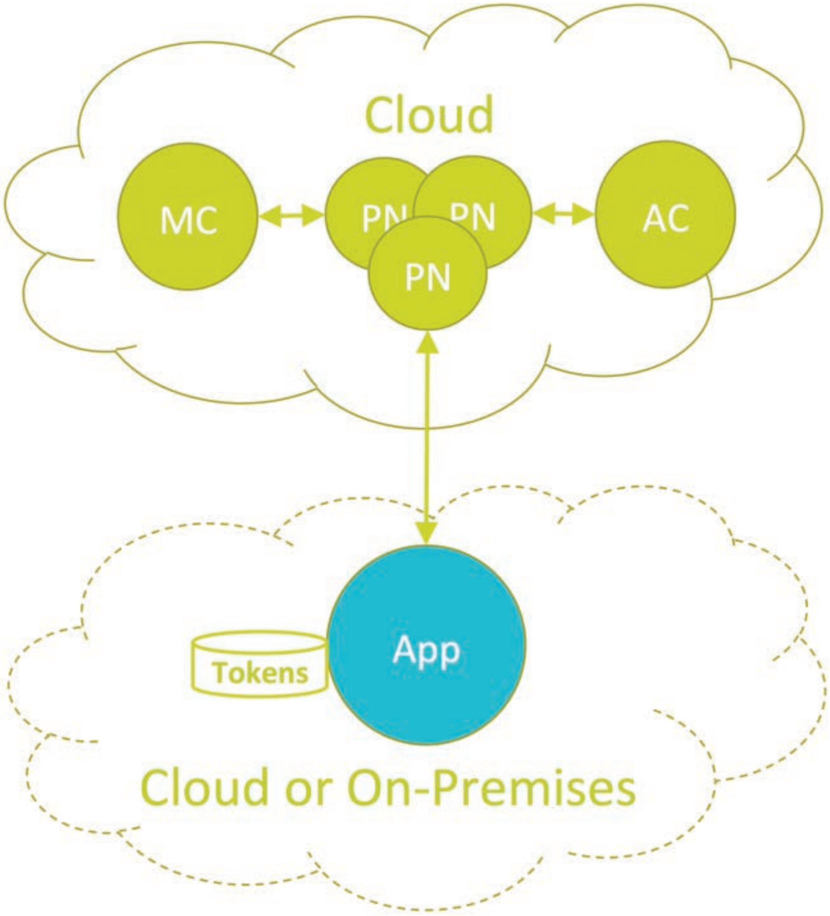


Figure 5: Full cloud deployment protecting applications on-premises or in the cloud

Summary & Conclusion

Benefits

For IT security & operations teams

Ease of implementation

Transparent integration capabilities reduce implementation efforts and costs to a minimum. SecurDPS 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 IaC and CARTA, SecurDPS can be programmatically controlled via its Management API.

Ease of operations & high availability

SecurDPS 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 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 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

Your mind at ease – Reducing the impact of data breaches

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 achieves a significant reduction of the impact in the case of a data breach by providing protection without any intermediate files 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.

For your customers – It is all about trust

In an age where choice has never been broader and where it has never been easier to simply switch to a different product or service, customers are looking for business partners they can trust. Data protection is the foundation to demonstrate to your customers that you care about their data, their privacy and their business.

Summary & Conclusion

Conclusion

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.

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

We are here to enable your success by providing expertise, an innovative technology suite and local support. To learn more, please talk to your comforte representative today and visit www.comforte.com.