KuppingerCole Report

EXECUTIVE VIEW

by Alexei Balaganski | January 2019

comforte AG SecurDPS Enterprise

comforte AG SecurDPS Enterprise is a highly scalable data protection platform that combines stateless tokenization technology and hardened fault-tolerant architecture to ensure security and compliance of sensitive data in mission-critical business applications.

by **Alexei Balaganski**
ab@kuppingercole.com
January 2019

Content

Related Research

Advisory Note: Database Governance – 70102

Leadership Compass: Database Security – 70970

Leadership Brief: Six Key Actions to Prepare for GDPR – 70340

Advisory Note: Maturity Level Matrix for GDPR Readiness – 72557

Survey: The Future of Banking – 74002

1 Introduction

comforte AG is a privately held software company specializing in data protection and digital payments solutions based in Wiesbaden, Germany. The company's roots can be traced back to 1998 when its founders came to the market with a connectivity solution for HPE NonStop systems – a fault-tolerant self-healing server platform for critical business applications, which is still widely used in banking and financial services, as well as in manufacturing, retail, and healthcare industries.

Soon, the solution for secure communications between mission-critical systems was adopted by a number of large banking and retail organizations. During later years, comforte AG's offering has evolved into a comprehensive solution for protecting sensitive business data with encryption and tokenization, tailored specifically for critical use cases that do not allow even minimal downtime. With wholly owned subsidiaries in key geographies beyond Europe – USA, Australia, and Singapore – the company has a strong global presence, currently serving over 500 customers around the world, with more than forty large Fortune 500 enterprises among them, still primarily from the banking and financial sectors.

However, as modern businesses across all verticals continue their rapid digitalization, the need to store, process and exchange data securely is becoming an essential business continuity factor for any company. Although some industries have experienced strong compliance regulations for specific types of information like financial transactions or healthcare records for decades, the introduction of much broader data protection regulations like GDPR has put massive pressure on just about any organization that has to store and process personal data.

On the other hand, as the growing number of high-profile data breaches indicates, even the largest businesses are still struggling with implementing consistent enterprise-wide information security measures. Setting up various security tools for numerous different applications, services, and heterogeneous systems and then making them work together efficiently is such a massive challenge that even the prospect of paying huge fines for compliance violations apparently does not motivate these companies enough.

There is however an alternative approach that has been gaining traction recently – data-centric security. While simple in theory – just protect the data at its source instead of securing each piece of infrastructure separately – its successful deployment depends critically on the solution's capability to enforce the same security and compliance policies consistently across all systems (be it on-premises servers, cloud services, databases, mainframes or anything else) and the effort needed to integrate it with existing modern and legacy applications.

A few years ago, comforte AG has entered the data-centric security market with their SecurDPS Enterprise solution that combines the company's patented stateless tokenization algorithm, proven highly scalable and fault-tolerant architecture, flexible access control and policy management, augmented by a broad range of transparent integration options, which allow various existing applications to be quickly included into the enterprise-wide deployment without any changes in infrastructure or code. With SecurDPS Enterprise, any organization can thus join the data-centric revolution relatively quickly and enjoy the same level of enterprise-grade data protection and compliance as the world's biggest financial institutions.

2 Product Description

comforte AG SecurDPS (Secure Data Protection Suite) Enterprise is a highly scalable and fault-tolerant data protection platform that utilizes tokenization technology to replace sensitive information in various data sources with non-sensitive equivalents, which have no exploitable value. By ensuring that existing business applications are operating on tokenized data instead of original information, businesses can successfully reduce risks of data breaches or unlawful exposure as well as ensure regulatory compliance. Together with encryption, data tokenization has long been one of the recommended data protection technologies under such frameworks as PCI DSS.

As opposed to traditional encryption, however, tokenization methods are format-preserving (thus not breaking the functionality of legacy applications), can be flexibly configured to support partial anonymization, and require substantially less computational resources. These properties have made tokenization solutions very popular for high-performance but highly regulated environments where sensitive data like financial transactions, criminal records or stock trades are processed. What makes SecurDPS stand out among many other similar solutions available on the market is a combination of three major differentiating factors.

First of all, comforte AG's platform utilizes the company's patented stateless tokenization algorithm. As opposed to many earlier-generation methods which rely on a centralized database (token vault) to maintain the mapping between original data elements and their corresponding replacement tokens, a stateless method requires just a small randomly generated table unique for each client system. This does not merely eliminate a single point of failure in the overall architecture but ensures that the attack surface of the tokenization system is made significantly smaller and much easier to protect. Additionally, it allows the solution to scale freely as needed just by adding more instances of the tokenization engine.

Each customer has the ability to configure the algorithm to their specific needs – out-of-the-box token formats for various sensitive data types can be customized, for example, to only mask a part of the value or otherwise conform to specific application requirements.

comforte AG's tokenization algorithm has been validated by several independent security researchers who were unable to identify any design weaknesses or vulnerabilities in the implementation. In fact, the ANSI X9.119-2 standard for protecting sensitive payment card data lists this algorithm as one of the reference tokenization methods.

Second, from the ground up, the architecture of the solution has been designed to be highly scalable and fault-tolerant – the requirement stemming from the company's decade-long experience in supporting critical business applications. Every SecurDPS deployment is a cluster comprising multiple virtual appliances called Protection Nodes. These appliances are running a specially hardened SecurDPS operating system that does not expose any unprotected interfaces and do not use any persistent storage, performing all operations in-memory. All protection nodes form a self-healing cluster system that ensures uninterrupted processing even when individual nodes fail.

A separate Management Console node is used to configure and initialize a protection cluster. This is the only node that keeps configuration files and secret keys, which are securely transmitted to the protection nodes during the initialization process; after that, it is no longer needed for the cluster to

operate. The only other stateful node is the Audit Console, which collects all the performance metrics and other audit information and provides reporting functionality. Of course, access to both consoles is strictly governed by fine-grained access policies.

Needless to say, all communications between the nodes are encrypted, thus giving customers the freedom of deploying them anywhere – on premises, in the cloud or in a hybrid fashion – enabling support for protecting both local and cloud-based applications in a transparent and uniform way. By running the protection nodes close to applications and centralizing the management of multiple clusters in the cloud, a multitenant "tokenization as a service" model can be implemented. By adding additional unique parameters to each customer's deployment, a provider of such a service can effectively guarantee full tenant isolation comparable to the Bring Your Own Key approach in encryption solutions.

Finally, SecurDPS is notable for a rich set of out-of-the-box application integration options. Of course, the platform provides its own Software Development Kit and the SmartAPI that powers it. This is perhaps the most natural choice for developers to integrate into their new applications, since the SmartAPI offers built-in support for automated failover, scaling and load balancing for mission-critical scenarios.

However, for existing applications, legacy systems, Big Data frameworks and other data sources which cannot be natively integrated with comforte AG's data protection solution, the company offers several methods of transparent integration to ensure that sensitive data is being secured as close to the source as possible:

- for batch operations, unstructured data transfers and similar use cases, a Virtual File System layer is provided, which intercepts all access to specific directories and files and transparently applies tokenization to the data contained within them. Both Windows and Linux file systems are supported;
- for data stream processing, common within Big Data frameworks like Hadoop and streaming platforms like Apache Kafka, a custom file/stream filter is implemented that can run on any platform that supports Java;
- For Linux/Unix and HPE NonStop systems, the third available option is the Interpose/Intercept technology, which enables on-the-fly data transformation on physical file systems by intercepting the system I/O.

For all these use cases, the company provides both general guidance and specific integration samples for common use cases. The company is also constantly working to add new integration capabilities, such as JSON/REST interception or support for popular object-relational mapping tools. Even more popular Apache Kafka integration is implemented through a technology partnership.

The most recent version of SecurDPS has introduced a number of important additions to the platform, including support for data masking in addition to tokenization, as well as supporting hardware security modules for secure key management. The company's roadmap for future releases clearly indicates that comforte AG is fully committed to making SecurDPS a general-purpose tokenization platform suitable for almost any type of business application while retaining its proven scalable and fault-tolerant architecture suitable even for the most highly regulated industries.

3 Strengths and Challenges

With the first release of SecurDPS Enterprise in early 2018, comforte AG has begun its expansion from their traditional, if a somewhat narrow market segment of highly scalable, fault-tolerant tokenization solutions for banks and financial institutions into the much larger general data protection market.

By combining their decade-long experience in catering towards truly non-stop mission-critical transactional systems and a broad range of transparent integration capabilities with modern and legacy applications, the company has successfully managed to transform their solution into a general-purpose data-centric security product. Yes, technically speaking, SecurDPS is lacking many of the features more traditional database security products are expected to contain. Yet, the one thing the platform does (replacing sensitive data with non-sensitive substitutes without any exploitative value), it does exceptionally well – offering a flexible and scalable solution to address modern compliance requirements, including PCI DSS, HIPAA or GDPR.

The company's roadmap reveals that comforte AG is committed to transforming their product into a general-purpose data protection platform not limited to tokenization only. We also expect to see more features to support modern agile development methodologies like DevOps and DevSecOps in the future releases.

Strengths	Challenges
• Unique scalable and fault-tolerant architecture for mission-critical use cases • Hardened platform, end-to-end data protection at rest and in transit • Deployment flexibility, hybrid cloud, and as-a-Service scenarios are supported • Broad range of transparent application integration options, support for Big Data and stream processing frameworks • Strong focus on regulatory compliance, directly addresses PCI DSS and GDPR requirements	• Current functionality limited to tokenization and masking (other data protection technologies planned for future) • Somewhat limited market visibility outside of the financial industry

4 Copyright

The Future of Information Security – Today

KuppingerCole supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact **clients@kuppingercole.com**

KuppingerCole Analysts AG
Wilhelmstraße 20-22
65185 Wiesbaden | Germany

Phone +49 (211) 23 70 77 – 0
Fax +49 (211) 23 70 77 – 11
www.kuppingercole.com