WHITE PAPER

COMFORTE SECURDPS

ENTERPRISE SOLUTION FOR CCPA

BHAVNA SONDHI | CISA, QSA (P2PE), PA-QSA (P2PE), ISO/IEC 27001 LEAD IMPLEMENTER, SECURE SOFTWARE & SECURE SLC ASSESSOR

COALFIRE

North America | Europe
877.224.8077 | info@coalfire.com | Coalfire.com

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Comforte AG (Comforte) engaged Coalfire Systems, Inc. (Coalfire), a leading independent industry provider of information technology (IT) security, governance, and regulatory compliance services, to conduct an independent technical assessment of their SecurDPS Enterprise Solution (SecurDPS) in support of the consumer privacy law, California Consumer Privacy Act (CCPA).

Companies that receive personal information from California residents and meet one of the three defined thresholds defined by the CCPA may require additional organizational and technical safeguards to satisfy the requirements of the CCPA. Selected organizational and technical safeguards should align with data privacy requirements and outcomes specified by the CCPA, including safeguards such as data minimization, storage limitation, purpose limitation, accuracy, integrity, confidentiality, availability, accountability, lawfulness, fairness, and transparency. It is necessary to identify the processing of protected data as defined by the CCPA and understand the risks associated with such processing to appropriately apply safeguards.

This paper primarily focuses on possible technical safeguards SecurDPS can provide and determine the effectiveness of SecurDPS to support an organization's environment, principally for data protection in customer environments. The solution submitted for review is positioned to enable visibility, insight, and control capabilities for organizations to help reduce risk and improve data security.

ABOUT SECURDPS ENTERPRISE SOLUTION

SecurDPS is a scalable and fault-tolerant enterprise tokenization and encryption solution. It is intended to help organizations to achieve end-to-end protection of sensitive data, lower compliance costs, and significantly reduce the impact and liability of data breaches. SecurDPS provides a flexible integration framework that allows for multiple layers of data protection for new and existing applications. Change in existing applications may not be necessary to achieve the protection of data using SecurDPS.

SecurDPS provides protection layers ranging from fully protecting sensitive elements or files using various data protection methods to auditing user access of a specific database record. SecurDPS in conjunction with Hardware Security Modules (HSMs) and dual custodian mechanisms for key protection can further secure data. SecurDPS can be integrated with other enterprise data protection solutions and provides a comprehensive and mature set of capabilities that enable data-related risk reduction.

ASSESSMENT SCOPE

The scope of this assessment was to conduct an independent review of SecurDPS. The goal of the technical whitepaper was to:

- Confirm that SecurDPS can support a consumer-facing enterprise's CCPA compliance efforts.
- Determine how SecurDPS can reduce the risk to data stores.

In this report, Coalfire will explain the architecture of SecurDPS at a high level, delving into the technical aspects of the solution that are applicable to compliance.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

The CCPA, which was enacted in 2018 but formally went into effect January 1, 2020, grants California residents' new rights to control their personal information that businesses gather and sell. The statute applies to certain businesses in California, as detailed below. The California Attorney General may fine businesses up to $7,500 per intentional CCPA law violation, or $2,500 for unintentional violations. Individual consumers also maintain the right to sue the company if that consumer's non-encrypted and non-redacted

data is accessed without authorization, exfiltrated, stolen, or disclosed as a result of the company's failure to maintain reasonable security procedures and practices.

Compliance

Companies are required to comply with the CCPA if they receive personal information from California consumers and meet one of the following three thresholds:

a. If the company generates an annual gross revenue of $25 million or more.
b. If the company retrieves and handles personal information of 50,000 or more California residents, households, or devices annually.
c. If the company obtains 50 percent or more of their annual revenue from selling California residents' personal information.

Personal Information

Per the CCPA, *"'Personal information' is information that 'identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.'* Personal information includes the consumer's real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol (IP) address, email address, account name, social security number (SSN), driver's license number, passport number, or other similar identifiers. Other categories included as "Personal Information" include, standard identifiers (e.g. date of birth, telephone number), biometric information (e.g. fingerprint, face recognition), geolocation data (e.g. mobile phone location, internet-connected computer terminal location), consumer commercial information (e.g. history of purchases, internet browsing history), and other inferences drawn about a consumer's preferences (e.g. characteristics, psychological trends, behavior, attitudes, intelligence, abilities, and aptitudes), are all categories of personal information under the CCPA. Personal information does not include information that has been deidentified.

Privacy Rights Under CCPA

The main goals of the CCPA are to provide consumers the following rights to consumers:

- To know what information is being collected and why. This will include the categories of information, sources of the information, specific pieces of information, and purpose for collection.
- To know whether their personal information is sold or disclosed and to whom it is provided.
- To say "no" to the sale of personal information and have an "opt-out" option.
- To access their personal information, have data portability, and request deletion of personal information.
- To be provided equal service and price, even if a consumer exercises their privacy rights (an anti-discrimination provision).

Although CCPA does not specifically state the reasonable security procedures and practices to be implemented, the California Civil Code Section 1798.81.5 does require companies to implement and maintain reasonable security procedures and practices appropriate to protect personal information.

PROTECTING DATA WITH SECURDPS

SecurDPS offers a data-centric security approach for the protection of sensitive data to help organizations meet reasonable data security protection measures to comply with privacy regulations including the CCPA. The solution allows for control over sensitive data and protection of data using tokenization and encryption methods without significantly affecting the existing applications.

SecurDPS offers various options such as encryption, tokenization, format-preserving hashing, and masking methods for protection of sensitive data. Strategy configurations and properties manage protection, which requires input of a protection method, algorithm attributes, format of the data, and a distinguishing method.

- **Tokenization**: SecurDPS offers a set of finely tuned algorithms and random mapping techniques that can be customized to each sensitive data element that needs to be protected. It provides linearly scalable, high-performance tokenization while operating without states or vaults and free of collisions. As the tokenization mapping operations occur purely in memory and central processing unit (CPU) without any disk input or output operations, the SecurDPS solution offers a secure approach for the protection of sensitive data.[1]

  The SecurDPS tokenization method is based on the static table-driven tokenization scheme described in the American National Standards Institute (ANSI) X9.119-2 tokenization standard.

- **Encryption**: In classic encryption, the protected data element has completely different format properties from those of the underlying sensitive value. Classic encryption schemes (both symmetric and asymmetric) map values to a protected element that has a different length and typically contains values of a completely different alphabet. The change of the length of the value has a significant impact when it comes to the need to implement data protection. While this usually results in the need to deprotect sensitive data for application usage and processing, classic encryption has its use cases. Examples include, Data-in-Transit Protection for complete streams and Full file or device encryption for unstructured data. SecurDPS has 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.[1]

- **Format Preserving Encryption (FPE)**: SecurDPS supports tokenization using FPE along with the static table-based tokenization. The FPE key is kept isolated within the protection node and is not shared with external entities meeting the criteria for encryption-based tokenization.

- **Masking**: SecurDPS performs masking operations by replacing the sensitive data element with a series of masking characters.

- **Format-Preserving Hashing**: Classic hashes (e.g., SHA256), like classic encryption operations, do not preserve the format of the underlying sensitive values; SecurDPS format-preserving hashing algorithm can be used to preserve irreversible protection with deterministic results in a way that maintains format properties.

INTEGRATING ENTERPRISE APPLICATIONS

SecurDPS offers two options for integrating existing and new enterprise applications with SecurDPS protection services, described below. Benefits of these options include shortened project time through integration capabilities and minimized service interruptions through development and deployment activities.

[1] SB_Enterprise_Tokenization_with_SecurDPS_201911.pdf

SecurDPS offers easy-to-use application programming interfaces (APIs) and integration without changing the record format of the original data:

- **SmartAPIs**: A comprehensive and easy-to-use software development kit (SDK) that consists of SmartAPIs for different programming languages.
- **Transparent Integration**: No application changes are required for this option. The transparency layers provided by SecurDPS inject the data protection options into the application. The underlying SecurDPS processing layer then identifies the sensitive data elements to be protected and performs a call out to the SmartAPI. This simplifies implementation to enterprise, hybrid and cloud applications including Software as a Service (SaaS) environment.

AUDITING AND ANALYZING

SecurDPS has built-in audit and analysis capabilities to help different IT or security stakeholders. SecurDPS provides integration into existing security information and event management (SIEM) frameworks. SecurDPS offers audit trail details for the following areas:

- Status of the data protection system.
- The unique or distinct data elements being protected.
- Sensitive data elements accessed (e.g., how many SSNs were accessed based on day or time frame selection).
- Specific sensitive data elements accessed and any peak in those activities.
- The application or services accessed including the data elements.
- Sensitive data elements being accessed by anyone currently.
- The status of data protection system and the different components.
- The protection system behavior for both past and current occurrences and a comparison offered to show any unusual system behavior.
- Management console access login and details on who accessed data, how often it was accessed, and when it was accessed.
- The actual actions performed by system or users.

SECURDPS ARCHITECTURE REVIEW

ARCHITECTURE COMPONENTS

Protection Cluster is the main component of SecurDPS and is a centrally managed, scalable, and fault-tolerant cluster of virtual appliances that performs the actual protection operations on behalf of the enterprise applications. Protection Cluster consists of the following sub-components:

- **Management Console:** Protection Cluster is centrally administered through the Management Console. The Management Console is a hardened appliance that securely stores all configuration data, keys, and secrets required for the cluster operation.
- **Protection Nodes (PNs):** Protection Cluster consists of multiple clustered soft appliances operating as PNs. Enterprise applications connect to the PNs to protect or reveal sensitive data elements using SecurDPS APIs or the transparent protection layer. The PNs do not store any data on a local or network disk and performs all operations in memory.
- **Audit Console:** The Audit Console collects and displays metrics about usage of protection services by an enterprise application, including the number of distinct sensitive data elements accessed by users in plain text, the number of protection operations per time interval, and the number of failed authentications. The Audit Console can be run standalone or as a cluster on its own. The Audit Console consists of multiple subcomponents and services as shown in Figure 1. Key components of the Audit Console are:
  - *Kafka*: Kafka is a distributed streaming platform. It is used as the message broker and landing platform (LP) for all information from the protection node cluster.
  - *Elasticsearch*: Elasticsearch provides the data storage and analytics engine for Kibana.
  - *Logstash*: Logstash is a data processing pipeline. It is used to ingest data from Kafka into Elasticsearch.
  - *Kibana*: Kibana provides visualization in the form of dashboards.
  - *Rsyslog*: Rsyslog is a log message forwarder that implements the syslog protocol. It is used to locally redirect the incoming log and audit stream from the PNs and the Management Console to Kafka.

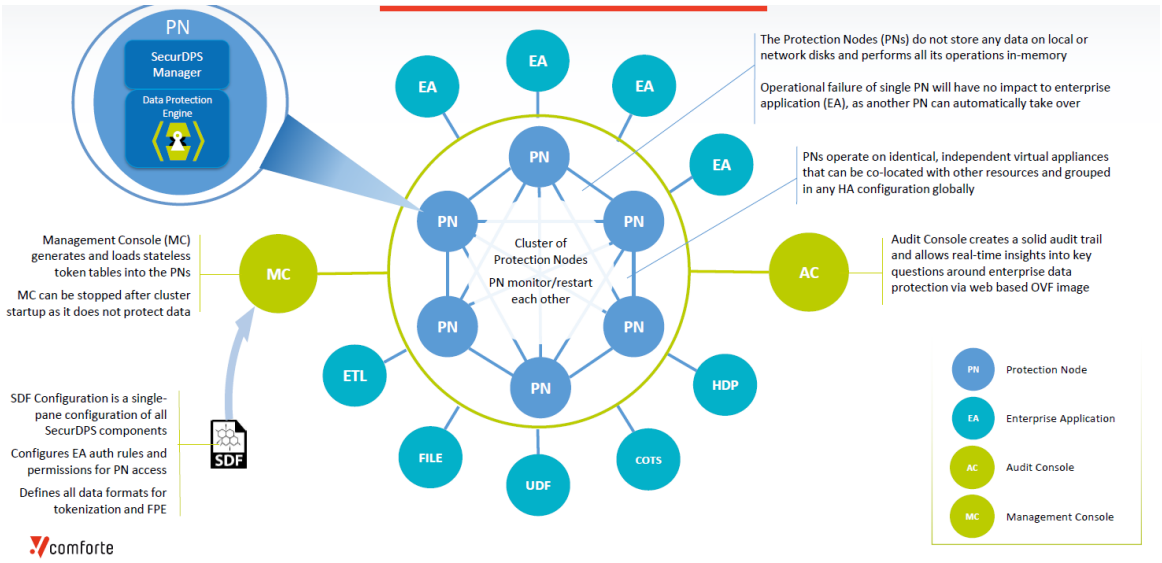

Figure 1: SecurDPS High-Level Architecture and Components

The goal of SecurDPS is to provide a secure architecture for management of the SecurDPS virtual appliance. However, the following aspects are also covered by the solution:

- Hardened operating system (OS) with restricted access – The SecurDPS OS is highly restricted and does not allow any shell or root access or for any software to be installed on the system. The sensitive data on the system is protected using the AES-256 encryption mechanism. Customers can optionally use either HSMs or secure cryptographic devices (SCDs) for the protection of keys if they require an additional layer of protection. The SecurDPS virtual appliance is considered a black box that operates securely by default.
- Single-purpose service user accounts – No user accounts exist for general use and service user accounts only provide the ability to perform activities needed for its purpose. SecurDPS provides strong authentication based on Secure Shell (SSH) public keys or enterprise identity access management (IAM) based authentication with Kerberos combined with Lightweight Directory Access Protocol (LDAP) based group or role-based access control.
- Minimal external attack surface – SecurDPS virtual appliances only allow SSH connections for incoming network interface connections. SecurDPS supports the use of other protocols via developed components that include proxy capabilities and provide the fault tolerance and performance features.
- Stateless PNs – The PN operates purely in memory and CPU and does not require permanent storage. The configurations are managed centrally via the Management Console, which allows for virtually unlimited scalability because no synchronization is needed. This reduces the potential attack surface. Sensitive data (e.g., tokenization secrets) is stored within the Management Console and PNs hold it in memory once seeded. Once a PN is shut down, the secrets no longer exist in the PN.

DEPLOYMENT SCENARIOS

SecurDPS can be implemented using various deployment models, these models provide flexibility for deployment due to use of stateless virtual PN. The PNs can be deployed everywhere and do not need to synchronize keys or tables. The PNs allow for protection and deprotection of data everywhere, independent of the location or environment. Common deployment models are discussed below:

Option 1: On-Premises Deployment

In this deployment option, the Management Console, Audit Console, and PNs are deployed on-premises. The applications can talk to PNs in the local network in this scenario.

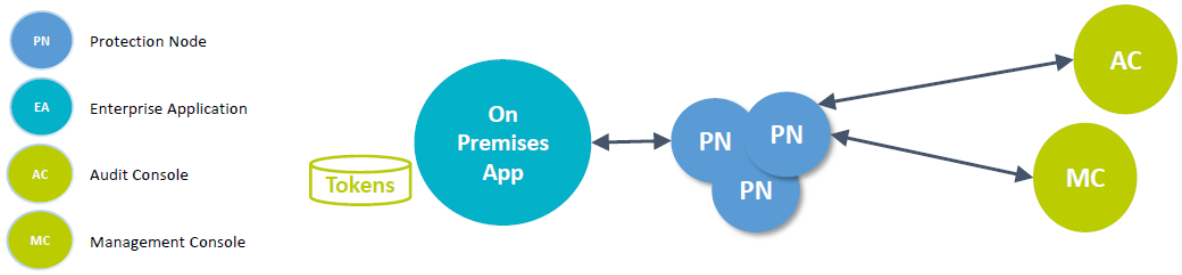

Figure 2: SecurDPS Deployment Model –On-Premises

Option 2: Hybrid Deployment

In this deployment option, the Management Console and Audit Console are deployed on-premises and can be used in conjunction with a PN cluster deployed on-premises or in the cloud. Even when PNs are deployed in the cloud, security-relevant information is never stored in the cloud and only resides in the memory of the PNs.

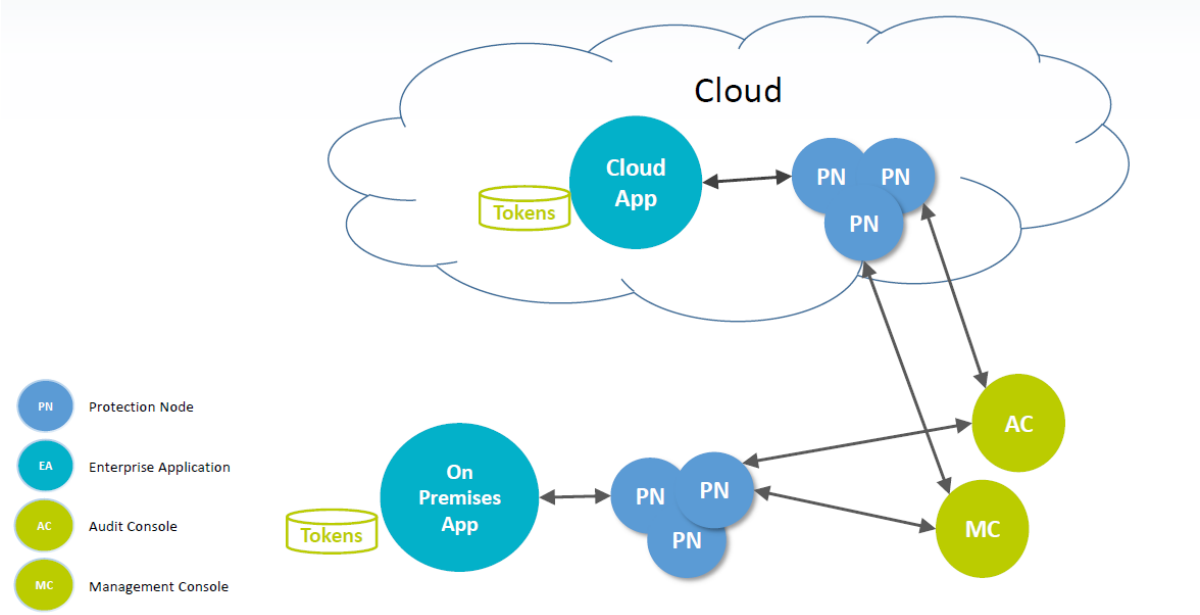

Figure 3: SecurDPS Deployment Model – Hybrid

Option 3: Hybrid Client Cloud Deployment

In this deployment option, all elements of SecurDPS are deployed on a client's cloud infrastructure. The PNs either connect to applications running in a cloud environment or on-premises.

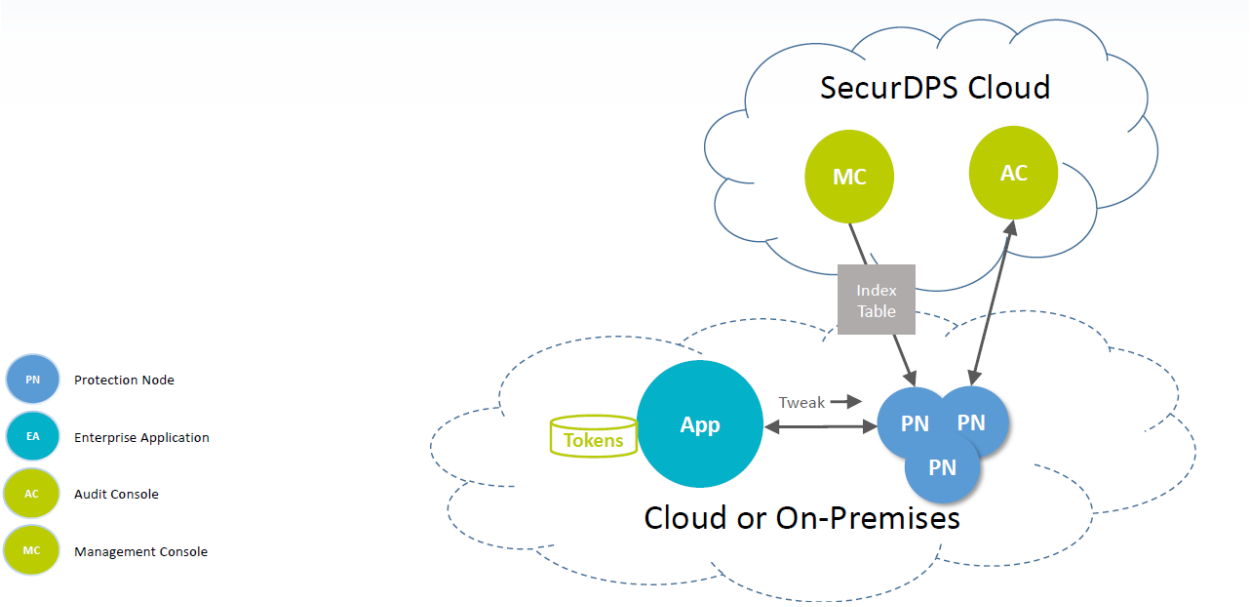

Figure 4: SecurDPS Deployment Model –Hybrid Client Cloud Deployment

ASSESSMENT METHODOLOGY

SecurDPS utilizes encryption, tokenization, and masking technologies for protecting data and requires the controllers to protect the encryption keys or tokenization secrets. SecurDPS can be implemented in the customer environment and secure implementation steps are outlined in guides and reference manuals provided by Comforte.

Coalfire validated the various protection strategies that can be configured for the protection of sensitive data elements. Strategies tested and their expected outcomes are displayed in Table 1 below.

Coalfire examined the impact of using SecurDPS within a CCPA-regulated environment. The applicable controls were analyzed, and the results were then summarized in the Coalfire Findings section.

ASSESSMENT METHODS

Coalfire conducted a technical analysis of SecurDPS by configuring the solution per the instructions outlined by Comforte. Deployment architecture using the Management Console or Audit Console On-Premises and Hybrid Protection Node Cluster Deployment (Hybrid Deployment) scenario was set up for testing. The SecurDPS Management Console, PN instances, Audit Console, and syslog server (Kiwi SIEM) were set up as virtual machines within the Coalfire lab.

A sample Java application to verify the file and stream filter integration provided by the vendor was tested on Windows platform with a Java runtime environment. The data was read from a source input stream, the data transformation actions (e.g., tokenization and encryption) were performed, and the modified data was written to a target output stream to a Windows file. The SecurDPS Virtual File System (SDFS) was mounted to a virtual folder to protect the sensitive data within the folder, and the file was available in tokenized format in the mapped folder.

Coalfire performed the following steps to confirm the functionalities offered to support CCPA compliance:

1. **Authorization**: The attributes were set with the Security Definition File (SDF) configuration file where the PNs authorized requests from enterprise applications based on the incoming SSH user ID. The users were authorized based on the public/private key pair. The use of strong authorization algorithms was observed, as shown in Figure 5.

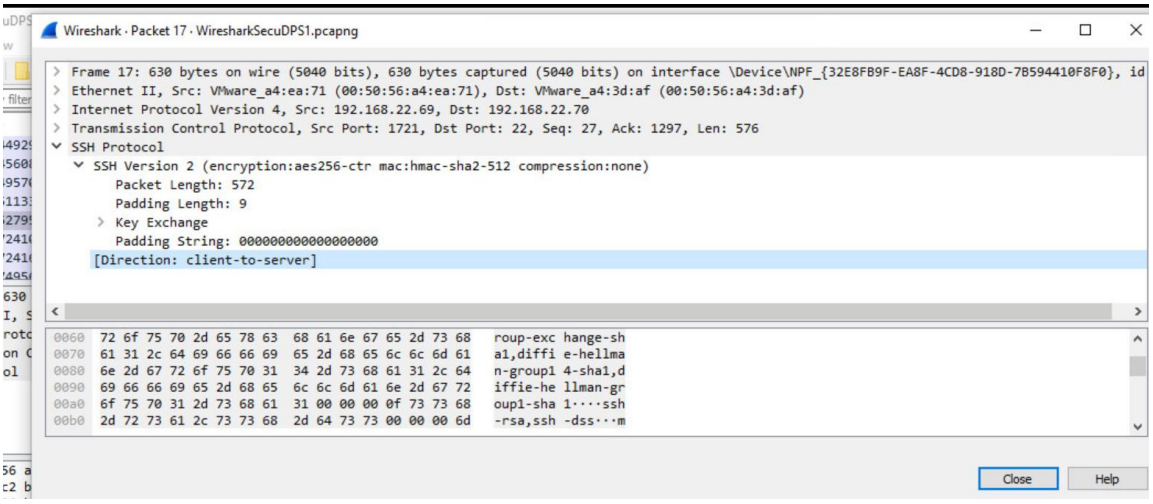

Figure 5: SecurDPS Public/Private Key Pair Authorization

2. **Vault Configurations**: Various mechanisms were configured to verify data protection using SecurDPS. The mechanisms configured for data protection were cryptographic algorithms, format-preserving encryption (FPE), and stateless tokenization.
3. **Strategy Configurations**: The "strategies" section of the SDF file specified how SecurDPS should perform the data protection operations associated with a distinct vault. Multiple strategies were tested with the supported vault type.
4. **Audit Logs**: The audit collector's format was configured to allow for information to be captured in specific audit log format. The log targets were configured to send logs to a syslog server.
5. **Audit Console**: The Audit Console virtual machine was configured to review the collected metric data about the usage of protection services by the applications.

Vaults and Strategies

In the context of SecurDPS, a vault is an object that manages the protection secret used to securely map between plain data strings and their protected equivalent, i.e. a token. The following combinations were validated with SecurDPS during the testing. The vault types supported with SecurDPS solution are:

- **Index Table Vault**: An index table is used by the SecurDPS internal tokenization engine to perform tokenization and detokenization. An index table vault will contain encoded random characters of the given alphabet, which are used to produce tokens with the secure tokenization mapping method developed by Comforte.
- **FPE Vault**: An FPE vault is used by SecurDPS to perform FPE or decryption with the FPE algorithm developed by Comforte. An FPE vault will contain the encryption key generated during the initialization step if it is detected that the file specified as vault store does not exist.
- **Basic Masking Vault**: A basic masking vault is used by SecurDPS to perform masking operations where some portion of a sensitive data element is replaced by a series of masking characters.

Vault Type	SecurDPS Strategy (Supplied YAML Configurations)	Input Data	Output Results
Tokenization	First Name Last Name: Preserve-first 2 Alphabet: A-Z and a-z	John Smith David Smith	Jozr bcSzT Daiuu XYxiF
FPE	Primary Account Number (PAN): Numeric, Preserve: First 6-Last 4 Alphabet: Distinguish (A-Z) Min-protection – 6 characters	5413330089020011	541333DHIDEB0011
Tokenization	Primary Account Number (PAN): Numeric, Preserve: First 6-Last 4 Alphabet: Distinguish (A-Z) Min-protection – 6 characters	5413330089020011 4761739001010267	541333DHIDEB0011 476173IEIAIA0267
Masking	Primary Account Number (PAN): Numeric, Preserve: First 6-Last 4 Alphabet: Masked character "X" Min-protection – 6 characters	5413330089020011 4761739001010267	541333XXXXXX0011 476173XXXXXX0267
FPE	ACCOUNT NUMBER: Alphabet: A-Z, a-z, 0-9	9001010267	mqoTYkeT0w

Vault Type	SecurDPS Strategy (Supplied YAML Configurations)	Input Data	Output Results
FPE	Government ID: Alphabet: A-Z, a-z, 0-9	M08833567	g3CG09Ep9 OR Vnn1oTKm4 OR KcaGwfPfz
FPE	PHONE: Alphabet: A-Z, a-z, 0-9	+44 20 7235 3457	+4U 1y yXC2 ksxZ
Tokenization	HOSTNAME: Alphabet: A-Z, a-z, 0-9	DESKTOP-PM76998	XKcCaYy-g6e4fgd
FPE	IPADDRESS: Alphabet: A-Z, a-z, 0-9	107.167.245.5	Uu7.TDC.VLd.w
FPE	Date of Birth: Numeric, Preserve: First 2 Alphabet: SQLDATE	3 June 2007	17 January 1975
FPE	EMAIL: Alphabet: A-Z, a-z, 0-9	joesmith@hotmail.com	1p6kz49f@8zAUFx5.aS3
Masking	Numeric, Preserve: First 6-Last 4 Alphabet: Masked characters “A-Z” Min-protection – 6 characters	joesmith@hotmail.com	joesmiABCDEFGHIJ.com
FPE	ADDRESS: Alphabet- ISO8859	550 Larimer St Ste 784, Denver, CO 80021	BsB ik7LtTI Ji 2CL kvo, 2MRFOG, g0 y1frH OR 550 qkvMmQs ZQ tKx 784, xlPWMB, iu 80021

Table 1: SecurDPS Enterprise Solution Testing Results

These examples illustrate the way SecurDPS protects data. These are a combination of just a few strategies tested; please refer to the SecurDPS guides provided by Comforte to retrieve details on configuration of strategies and the parameters for additional information. Properties of a strategy include the tokenization table, algorithm attributes, the token format (e.g., how many leading and trailing characters are left in the clear), and a distinguishing method (i.e., how plain values can be distinguished from tokens). Format-preserving tokens can be generated for credit card numbers, SSNs, and other personal information such as names or email addresses.

Audit Logging

The SDF attributes and cluster configurations displayed the log messages within the Kiwi Syslog SIEM, as shown in Figure 6. A separate syslog server was configured to receive the log data from the SecurDPS components.

Submitted sensitive data was not transmitted in clear text on the network. The SecurDPS architecture protects the sensitive data (personal information) based on the configurations performed by the implementing organization.

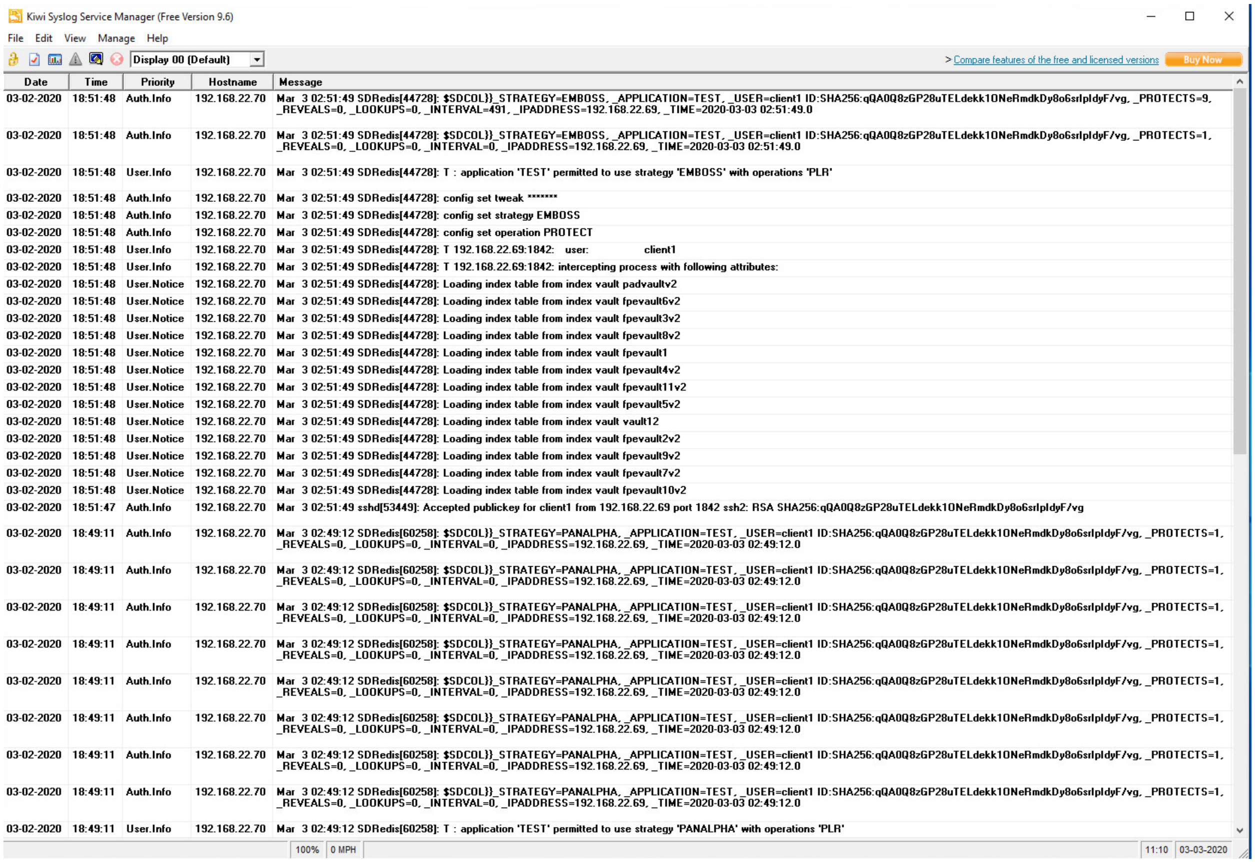

Figure 6: Syslog Messages from SecurDPS

SecurDPS Audit Console

The Audit Console dashboard can display log messages retrieved from the PNs and Management Console, as shown in Figure 7. The SecurDPS Audit Console dashboard, as shown in Figure 8, also provides statistical data represented in graph and pie chart format. The dashboard provides visibility into the data protection that would be useful for risk assessment or incident response management within an organization.

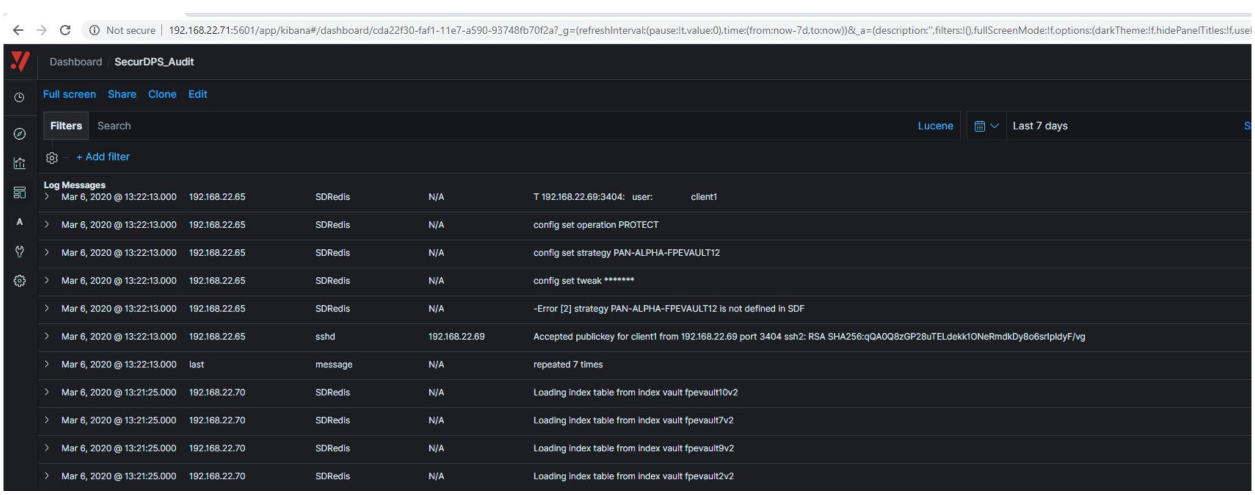

Figure 7: Aggregated Log Messages from SecurDPS Nodes

Figure 8: SecurDPS Audit Console Dashboard - DemoApp

COALFIRE FINDINGS

This paper's primary focus pertains to the use of SecurDPS for supplying technical safeguards that may be used to demonstrate reasonable security measures for data protection to support company's CCPA compliance efforts. Coalfire identified capabilities within SecurDPS would be suitable to be included in an organization's technical security measures to ensure a level of security in support of data privacy initiatives. Though applicability of the solution with CCPA focuses on specific data protection, data de-identification and pseudonymization use cases SecurDPS solution could help address several common threats associated with data privacy if an organization's systems are compromised.

Pertaining to applicability for CCPA outcomes, Coalfire has determined that focused applicability can be found with the following:

CCPA, Section 1798.140 – Personal information Deidentification

> *(o) (3) "Personal information" does not include consumer information that is deidentified or aggregate consumer information*
>
> *(h) "Deidentified" means information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:*
>
> *(1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.*
>
> *(2) Has implemented business processes that specifically prohibit reidentification of the information.*
>
> *(3) Has implemented business processes to prevent inadvertent release of the information.*
>
> *(4) Makes no attempt to reidentify the information.*

SecurDPS can help a company comply with deidentification measures through the following:

- SecurDPS offers various options such as classic encryption, FPE, tokenization, format-preserving hashing, and masking methods for protection of sensitive data. SecurDPS can be utilized to

implement the necessary technical safeguards within a company to help comply with required security measures.

- SecurDPS can limit where sensitive data may be decrypted, minimizing the need for access to live data in data stores, applications and processes that can operate on de-identified or tokenized data.

SecurDPS assists with very focused needs in CCPA related to data security redaction, one-way and reversible pseudonymization and de-identification. CCPA is broader than that process and people elements are required for complying with CCPA requirements.

Additional controls will likely be required pursuant to the company's assessment of risk and determination of appropriate technical and organizational safeguards to reduce or eliminate risk in alignment with CCPA.

CCPA, Section 1798.140 (r) – Pseudonymization

> *(r) "Pseudonymize" or "Pseudonymization" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.*[2]

Pseudonymization provides minimal benefit for CCPA purposes because any data that is identifiable must be protected in accordance with CCPA. Pseudonymization is a technique of deidentification that makes data indirectly but still identifiable to an individual. Only complete deidentification removes data from the CCPA requirements.

SecurDPS can help a company comply with data protection measures through the following:

- SecurDPS capability includes accepted tokenization standard (ANSI X9.119-2) for data pseudonymization.
- Encryption, tokenization, or masking of personal information using SecurDPS can help a company:

  (a) comply with the CCPA for the use of reasonable security procedures and practices.

  (b) limit liability exposure under CCPA because consumers only have a private right of action if the business is responsible for the loss nonencrypted or nonredacted personal information; encrypted or tokenized data do not allow a consumer to sue under the statute.
- Data privacy can be achieved for records through the other application's design integrated with SecurDPS.
- SecurDPS can supply the necessary data protection methods to support encryption, reversible and irreversible tokenization, and masking process for pseudonymization of personal information.

Principally, the concepts of application of security boundary protection mechanisms may be useful to limit exposure by minimizing accessibility to personal information through the cloud infrastructure or application platforms.

The following table provides details on the features offered by SecurDPS that can be used within an environment for improved security.

[2] *https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375*

REASONABLE SECURITY MEASURES SUPPORTED BY SECURDPS	
Security Features	**SecurDPS Support Details**
Data Protection by Design	• Organizations can use encryption, tokenization, or masking measures to limit access to personal information, where that information can be accessed, and for how long it can be made available. SecurDPS functionalities can be utilized to track the necessary activities to implement the necessary safeguards. • Organizations can use SecurDPS to monitor files containing personal information and their activity to help identify files no longer used and candidates for decommissioning. • Data protection by design is a higher-level organizational governance design consideration. This essentially requires that privacy and data protection be considered from the ground up when designing new products or services or implementing changes to existing items. The protection mechanisms offered by SecurDPS can be considered a means to comply with some aspects of organizational controls and considered as an element of a defense-in-depth strategy.
Records Retention	• Organizations can use SecurDPS to categorize the personal information to facilitate encryption or tokenization, governance, and develop policies and procedures for timely erasure and records retention of these protections.
Breach Investigations Support	• SecurDPS can be used to mitigate much of the risk of a breach by actively scanning for personal information and encrypting it at rest. • SecurDPS audit logging and console features can retrieve the necessary information for investigation of data breach for notification purposes.

Table 2: SecurDPS Enterprise Solution Security Measures

The key applicability of the SecurDPS is for protection of personal information, and the identification and increased awareness for the location of personal information. This solution best applies to the CCPA when it is applied in alignment with an organization's Governance, Risk and Compliance (GRC) program as part of its designed technical and organizational safeguards to address identified risks when performing a privacy impact assessment.

CONCLUSION

CCPA has the potential to enforce penalties on organizations that are unable to demonstrate they are taking appropriate technical and organizational measures to protect the personal information of California residents. The features or capabilities offered by SecurDPS such as tokenization, encryption, masking, format-preserving hashing, and audit logging can be used towards implementing strong technical safeguards to implement reasonable security measures for protection of personal information. SecurDPS can help companies with comprehensive data protection across the enterprise, which reduces the impact of data breaches and prepares them for CCPA compliance.

It is important to note that no one product, technology, or solution can address all security and compliance requirements. Security is a design principle that must be addressed through carefully planned and implemented strategies. Entities seeking compliance are best able to obtain it through its GRC program.

REFERENCES

- SB_Enterprise_Tokenization_with_SecurDPS_201911.pdf
- SecurDPS_Enterprise_Protection_Cluster.pdf

- SecurDPS_Enterprise_Integration_For_Windows_Manual.pdf
- SecurDPS_Enterprise_Virtual_File_System_for_Linux_Reference_Manual.pdf
- SecurDPS_Enterprise_REST_API.pdf
- SecurDPS_Enterprise_SmartAPI_for_Java_Reference_Manual.pdf
- SecurDPS Audit Console Reference Manual.pdf

ABOUT THE AUTHOR

Bhavna Sondhi | Principal Consultant

Bhavna Sondhi is the practice subject matter expert for the Solution Validation team at Coalfire. Bhavna performs advisory work and assessments for various payment card industry compliance frameworks and authors technical white papers. Bhavna joined Coalfire in 2013 and brings over 13 years of software engineering and information security experience to the team. Her software engineering experience plays a vital part in ensuring the teams recognize the importance of secure code development and information security within their operational practices.

ABOUT THE REVIEWER

Lisa Gumbs | Senior Consultant

Lisa Gumbs is a senior consultant in the GDPR and Privacy practice at Coalfire. Lisa has direct experience in the areas of IT governance, program development and deployment, risk management, assessment, and training. She has extensive experience advising on privacy including US and European privacy laws and policies, with a particular focus on GDPR readiness and compliance.

Published June 2020.

ABOUT COALFIRE

Coalfire is the trusted cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for nearly 20 years and has offices throughout the United States and Europe. For more information, visit Coalfire.com.