WHITE PAPER

COMFORTE SECURDPS

ENTERPRISE SOLUTION FOR GDPR

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 European Union (EU) General Data Protection Regulation (GDPR).

Organizations doing business with subjects of the EU may require additional organizational and technical safeguards to satisfy the requirements of GDPR. Selected organizational and technical safeguards should align with data privacy requirements and outcomes specified by GDPR, including data minimization, storage limitation, purpose limitation, accuracy, integrity, confidentiality, availability, accountability, lawfulness, fairness, and transparency. It is necessary to discover and identify the processing of protected data as defined by GDPR and understand the risks associated with such processing to appropriately apply safeguards.

This paper primarily focuses on possible available technical safeguards SecurDPS can provide and determine the effectiveness of SecurDPS to support an organization's environment, principally for data protection. The solution submitted for review is positioned to enable visibility, insight, and control capabilities for GDPR-regulated 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 overall GDPR 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 GDPR requirements.

GENERAL DATA PROTECTION REGULATION (GDPR)

The EU GDPR replaces the Data Protection Directive, officially known as Directive 95/46/EC, and is designed to harmonize data privacy laws across Europe to protect and empower all EU citizens' data privacy and reshape the way organizations across the region approach data privacy.

GDPR was approved and adopted by the EU Parliament in April 2016. The regulation had a two-year transition period and became enforceable on May 25, 2018.

GDPR not only applies to organizations located within the EU, but also to organizations located outside of the EU if they offer goods or services to or monitor the behavior of EU data subjects. It also applies to all companies processing and holding the personal data of data subjects residing in the EU, regardless of the company's location.

Organizations can be fined up to 4% of their annual global turnover for breaching GDPR or €20 million, depending on which is greater. This is the maximum fine that can be imposed for the most serious infringements, including insufficient customer consent to process data or violation of the core of Privacy by Design concepts. There is a tiered approach to fines: a company can be fined only 2% for not having their records in order (Article 28), not notifying the supervising authority and data subject about a breach (Article 33), or not conducting an impact assessment (Article 35). It is important to note that these rules apply to both controllers and processors; therefore, cloud environments are not exempt from GDPR enforcement.

GDPR is categorized in various Chapters, Articles, and Recitals formats. Articles and Recitals are essential to understanding GDPR. Supervisory authorities have implemented several Recitals that set precedents for enforcement of GDPR and provide unambiguous instructions on the applicability of the Articles.

The GDPR includes any data elements that can be traced to a specific person, including Global Positioning System (GPS) data, genetic and biometric data, browser cookies, mobile identification identifiers (e.g., Unique Device Identifier [UDID], International Mobile Equipment Identity [IMEI]), Internet Protocol (IP) addresses, MAC addresses, and application user IDs.

PROTECTING DATA WITH SECURDPS

SecurDPS offers a data-centric security approach for the protection of sensitive data to help organizations comply with privacy regulations. 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.

[1] SB_Enterprise_Tokenization_with_SecurDPS_201911.pdf

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 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. 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 Social Security Numbers [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:** The 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.

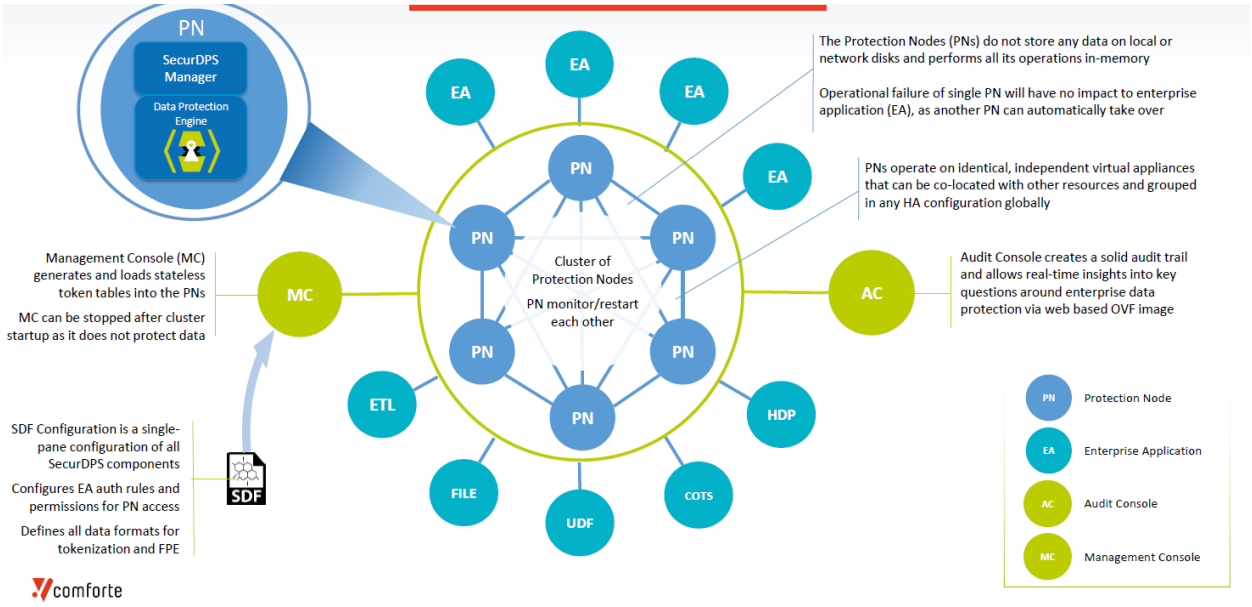

Figure 1: SecurDPS High-Level Architecture and Components

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.

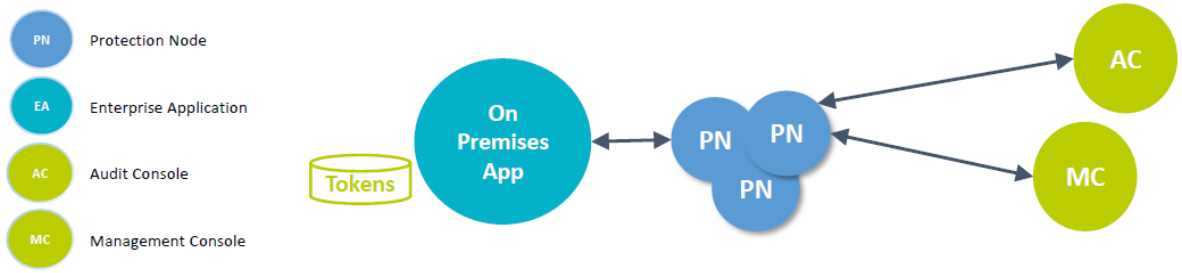

Figure 2: SecurDPS Deployment Model On-Premises

Option 2: Hybrid Deployment

In this deployment option, the Management Console and the 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.

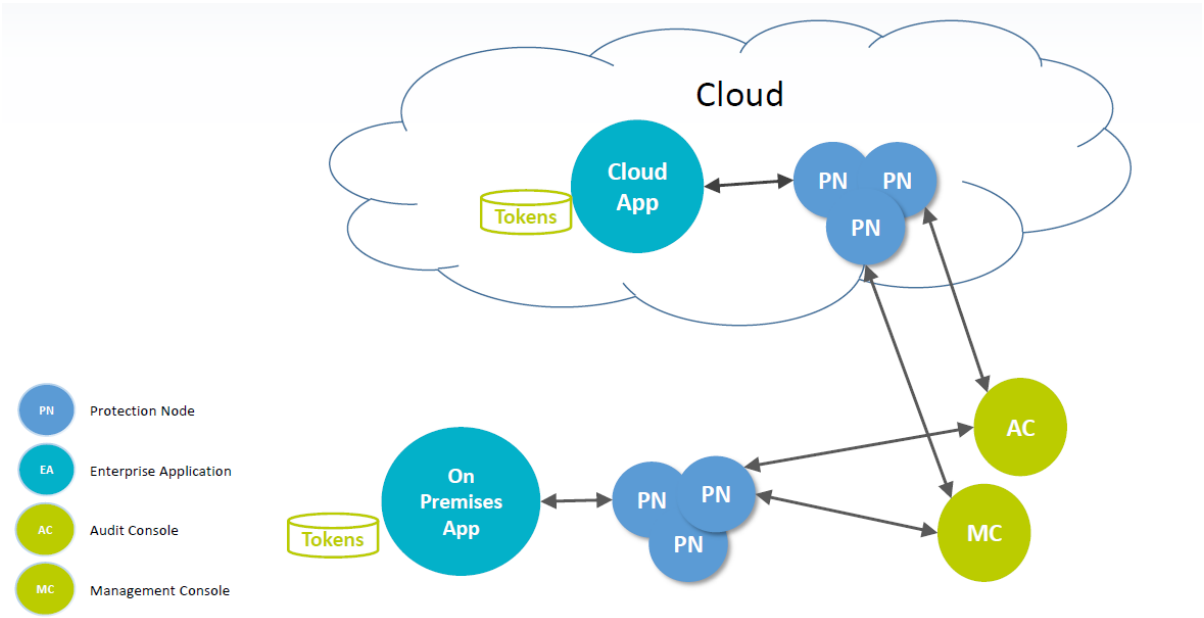

Figure 3: SecurDPS Deployment Model Hybrid

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.

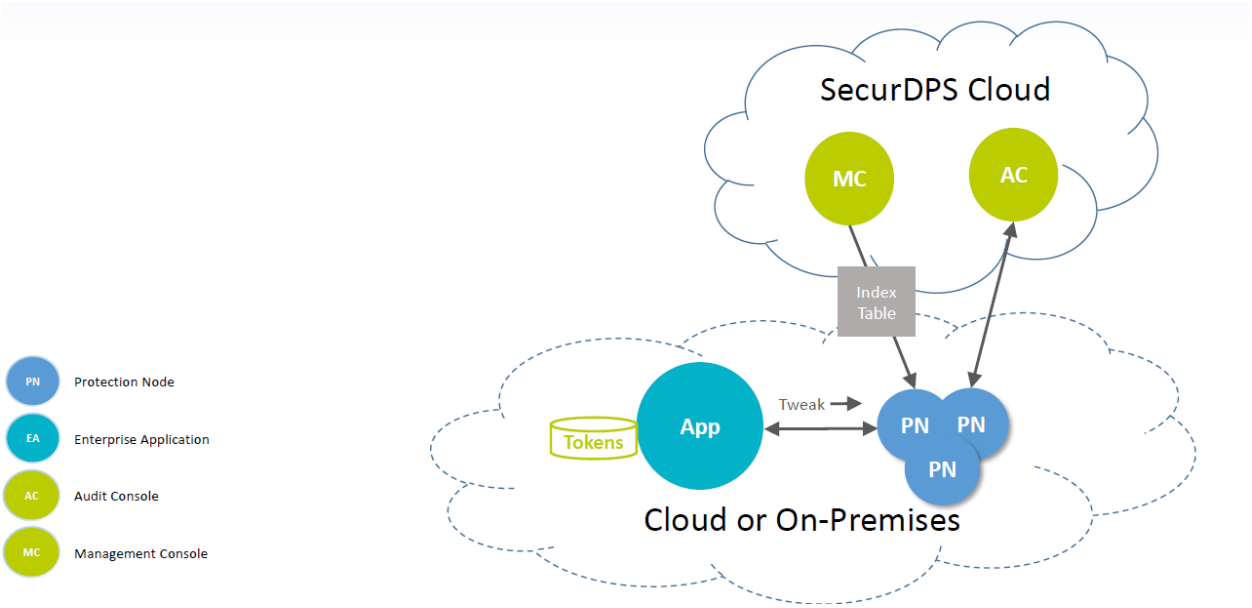

Figure 4: SecurDPS Deployment Model - Hybrid Client Cloud Deployment

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 GDPR-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 GDPR requirements:

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.

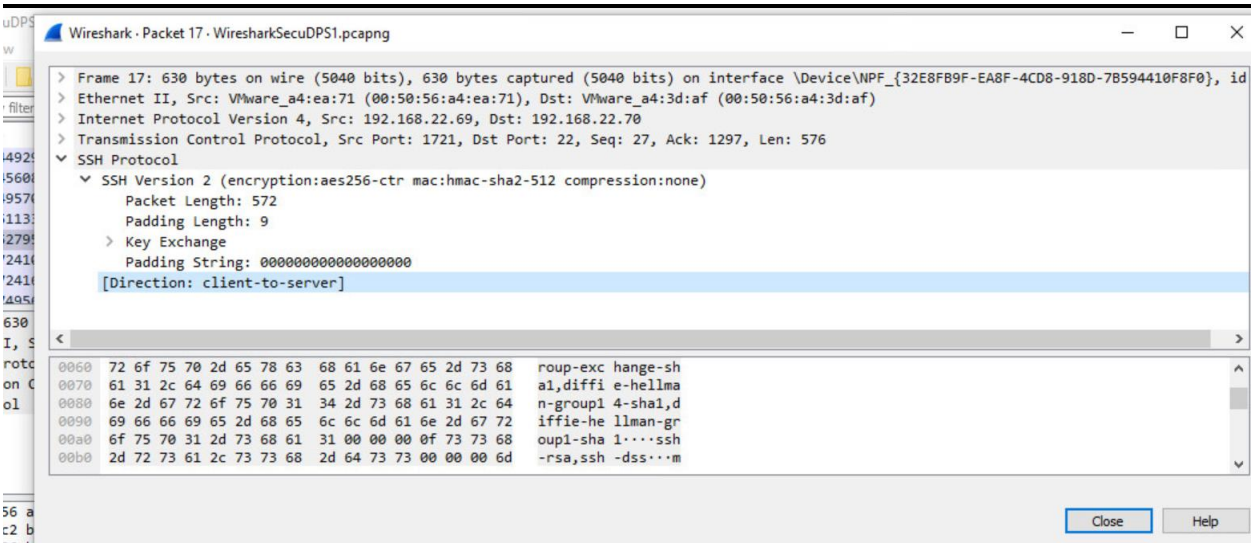

Figure 5: SecurDPS Public/Private Key Pair Authorization

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
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

Vault Type	SecurDPS Strategy (Supplied YAML Configurations)	Input Data	Output Results
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 solution 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 were able to display 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 based on the configurations performed by the implementing organization.

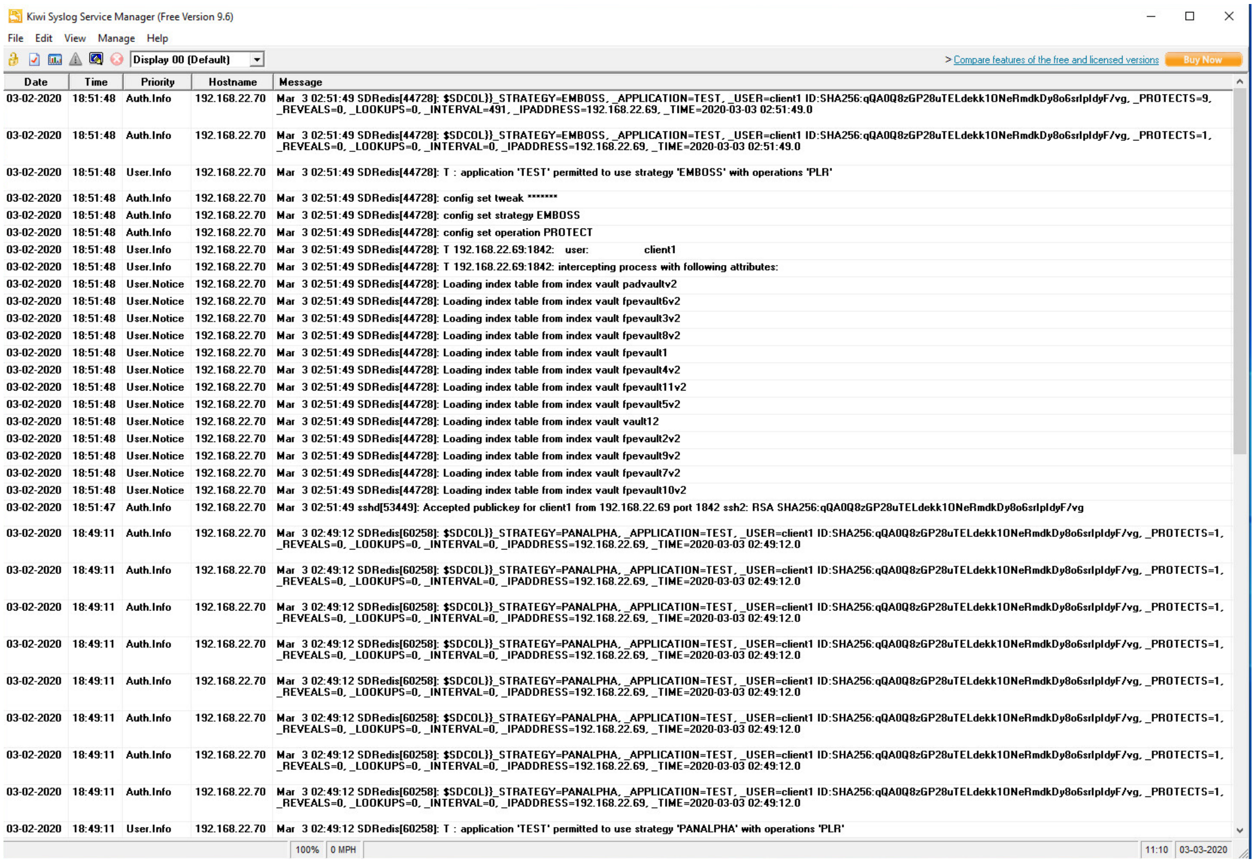

Figure 6: Syslog Messages from SecurDPS

SecurDPS Audit Console

The Audit Console dashboard can display log messages retrieved from the PNs and Management Console as seen 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.

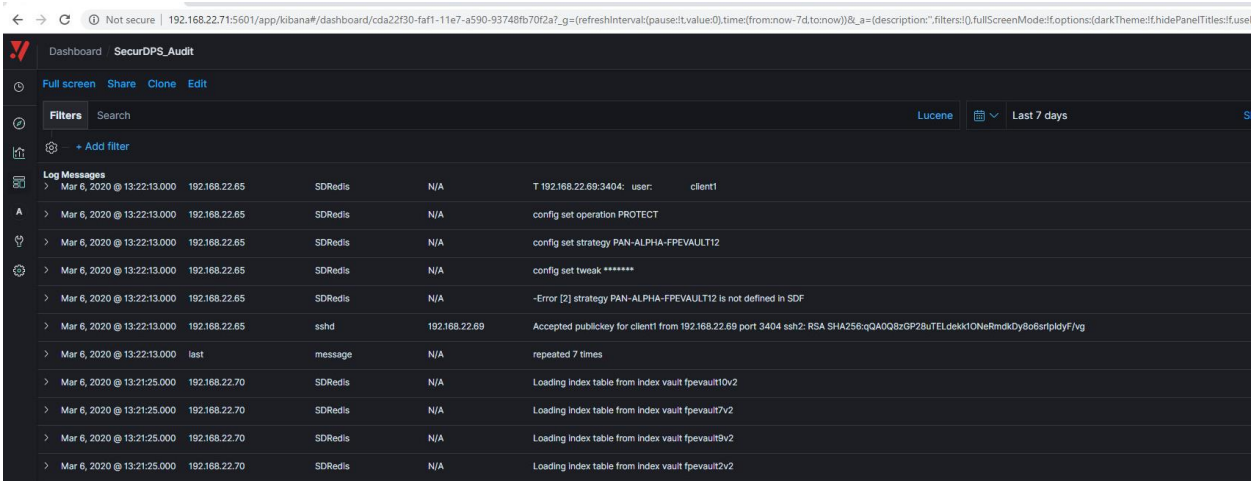

Figure 7: Aggregated Log Messages from SecurDPS Nodes

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 GDPR 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 GDPR articles focuses on specific data protection, data de-identification and pseudonymization use cases, SecurDPS could help address several common threats associated with data privacy if an organization's systems are compromised.

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

- Article 5, *Principles Relating to Processing of Personal Data*
- Article 6, *Lawfulness of Processing in Relation to Retention/Minimization and Territoriality*
- Article 24, *Responsibility of the Controller*
- Article 25, *Data Protection by Design and by Default*
- Article 30, *Records of Processing Activities*
- Article 32, *Security of Processing*
- Article 33, *Notification of a Personal Data Breach to the Supervisory Authority*
- Article 34, *Communication of a Personal Data Breach to the Data Subject*

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

The following table provides more detail of the alignment and capabilities of SecurDPS to support the GDPR outcomes for data privacy.

GDPR – REGULATION (EU) 2016/679			
ARTICLE NUMER AND HEADING		**SUBSECTION**	**SECURDPS SUPPORT DETAILS**
5	Principles Relating to Processing of Personal Data	5-1.(f). *1. Personal data shall be:* *(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').*[2]	• SecurDPS offers various options such as classic encryption, format preserving encryption, tokenization, format preserving hashing, and masking methods for protection of sensitive data. • Restricted (service) accounts with limited functions and hardened OSes can be configured as part of SecurDPS. • SecurDPS can constrain where sensitive data may be decrypted, minimizing the risk to data stores. • Additional controls will likely be required pursuant to the controller's or processor's assessment of risk and determination of appropriate technical and organizational safeguards to reduce or eliminate risk in alignment with GDPR.

[2] https://gdpr-info.eu/

GDPR – REGULATION (EU) 2016/679			
ARTICLE NUMER AND HEADING		**SUBSECTION**	**SECURDPS SUPPORT DETAILS**
6	Lawfulness of Processing	6-4.(e) *4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:* *(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.*[2]	• SecurDPS capability includes accepted tokenization standard (ANSI X9.119-2) for data pseudonymization. • Controllers contemplating processing without the consent of the individual or beyond purpose specification may consider encryption as one possible factor for assessing the risk of continued processing. SecurDPS provides the means to encrypt the data. • Controllers may also consider other options to reduce the risk to data privacy, such as data anonymization to enable lawful processing in ways that exceed the original collection purpose. • The concepts in Article 6 mostly pertain to data privacy protections at the record level. This is typically achieved through the application's design, including data privacy as an integrated function. • SecurDPS can supply the necessary encryption, tokenization and masking to support the encryption process or pseudonymization as a factor for continued processing.
24	Responsibility of the Controller	24-1. *Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.*[2]	• Security measures include the hardening of OSs and governance over privileged accounts for data protection processing. • Protection of data in storage via encryption or tokenization of GDPR data at rest can be achieved via SecurDPS. • SecurDPS offers the flexibility to limit where GDPR-sensitive workloads may run to trust-attested OSs and where data may be decrypted to support workload execution and data access. • Other considerations for additional technical and organizational safeguards may be warranted based on findings associated with the controller's or processor's risk and privacy impact assessments.

GDPR – REGULATION (EU) 2016/679			
ARTICLE NUMER AND HEADING		**SUBSECTION**	**SECURDPS SUPPORT DETAILS**
25	Data Protection by Design and by Default	25-1., 25-2. *Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.* *The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*[2]	• Organizations can use encryption, tokenization or masking to limit access to GDPR data, where that data 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 could utilize SecurDPS to monitor files containing GDPR data and their activity to help identify files no longer used and candidates for decommissioning. • Data protection by design and by default 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, 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.

GDPR – REGULATION (EU) 2016/679			
ARTICLE NUMER AND HEADING		**SUBSECTION**	**SECURDPS SUPPORT DETAILS**
30	Records of Processing Activities	30-1.(f) *Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:* *(c) a description of the categories of data subjects and of the categories of personal data;* *(f) where possible, the envisaged time limits for erasure of the different categories of data;*[2]	• Organizations could utilize SecurDPS to categorize the GDPR data to facilitate encryption, tokenization, governance, and timely erasure and records retention of these protections.
32	Security of Processing	32-1 (a,b) *Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:* *(a) the pseudonymisation and encryption of personal data;* *(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*[2]	• Organizations could implement policies to ensure ongoing confidentiality of GDPR data-at-rest with use of SecurDPS encryption, tokenization, hashing feature. • The solution may be a part of a controls framework for enforcing compliance. The organization must have a comprehensive program of security utilizing a broader security control framework that is inclusive of both technical and organizational safeguards. For pseudonymization, format preserving protection, tokenization can reduce some risk for unauthorized disclosure and can support actions necessary requiring breach notification where data is exposed without the decryption key. Masking can be used to pseudonymize (when masking identifiers) or anonymize (when masking all fields that hold sensitive information). 32.1(a), *Use of Pseudonymization*, is more specific to the function of the business application that handles personal data and the prevention of unauthorized access through programmatic means to obtain such access.

GDPR – REGULATION (EU) 2016/679			
ARTICLE NUMER AND HEADING		**SUBSECTION**	**SECURDPS SUPPORT DETAILS**
33	Notification of a Personal Data Breach to the Supervisory Authority	33-1. *In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay*[2]	• Breach notifications do not need to be made to the supervisory authority where the data in question was protected. The organization will be required to prove that keys were not also compromised in the breach. • SecurDPS can be used to mitigate much of the risk of a breach by actively scanning for GDPR data and encrypting it at rest. • SecurDPS audit logging and console features can retrieve the necessary information for investigation of data breach for notification purposes.
34	Communication of a Personal Data Breach to the Data Subject	34-3.(a) *The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:* *(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*[2]	• Breach notifications do not need to be made to the data subjects where the data in question was protected using SecurDPS. • In the event of a data breach, characterize the data in question to ascertain the scope of GDPR data potentially exposed. • The organization must consider that there may be other cause for breach notification where data was exposed in other ways for which the encryption or tokenization solution provided by SecurDPS was not able to protect.

Table 2: SecurDPS Enterprise Solution GDPR Applicability

The most important applicability of the SecurDPS is for protection of sensitive data, identification and increased awareness for location of sensitive data. This solution best applies to the GDPR when it is applied in alignment with the 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

GDPR has the potential to enforce penalties on organizations that are unable to demonstrate they are taking appropriate technical and organizational measures to protect the privacy and security of EU citizens' data. GDPR places the emphasis on organizations architecting solutions that are considerate of the jurisdiction of data subjects, yet flexible enough to meet the needs of modern enterprise. The features or capabilities offered by SecurDPS such as tokenization, encryption, masking, format preserving hashing, audit logging and monitoring features can be used towards implementing strong technical safeguards to support GDPR compliance environment. Features within SecurDPS can help enterprises with comprehensive data protection across the enterprise, which could reduce the impact of data breaches and better prepare 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

Nick Trenc | Director

Nick Trenc is the Director of the Solution Validation team at Coalfire. Nick has several years of experience working in information security and has an in-depth understanding of application, network, and system security architectures. He holds CISA, CISSP, QSA and PA-QSA certifications.

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.