COALFIRE

WHITE PAPER

COMFORTE AG SECURDPS PLATFORM

PCI DSS v4.0 TECHNICAL ASSESSMENT

VIKRAM DHABAL DEB, SENIOR CONSULTANT | CISA, CISSP, QSA, PCI SSCLA

comforte

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 Payment Card Industry Data Security Standard (PCI DSS). Organizations accepting payment cards for purchases are subject to the requirements of PCI DSS.

Selected organizational and technical safeguards should align with the requirements and outcomes specified by PCI DSS including, among other things, data minimization, storage limitation, purpose limitation, accuracy, integrity, confidentiality, availability, and accountability. It is necessary to discover and identify the processing of cardholder data (CHD) to appropriately apply safeguards. The primary account number (PAN) is the defining factor for cardholder data. Organizations storing such data should understand the risks associated with such storage and processing.

This paper primarily focuses on possible available technical safeguards provided by SecurDPS that can be useful for the protection of PAN data in customer environments. Comforte requested that Coalfire determine the effectiveness of SecurDPS to support PCI DSS, principally for data protection. The solution submitted for review is positioned to enable visibility, insight, and control capabilities for the organizations subject to PCI DSS to help reduce risk and improve data security.

ABOUT SECURDPS ENTERPRISE

SecurDPS is a scalable and fault-tolerant enterprise tokenization and encryption solution. It enables 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. Additionally, key protection in Hardware Security Modules (HSMs) and dual custodian mechanisms further secure the data when configured. 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.

SecurDPS also provides a Discovery & Classification tool which allows users to query structured and unstructured data sources based on classified sensitive data. Searches utilize a wide range of attributes, as well as identifying the storage of specific data types to ensure focus on sensitive information. Discovery & Classification works with sensitive data elements (payment, personal, etc...) and provides valuable information pertaining to data protection activities.

ASSESSMENT SCOPE

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

- Confirm that SecurDPS can support a consumer-facing enterprise's overall PCI DSS compliance efforts.
- Determine how SecurDPS can reduce the risk and the scope of data stores in the merchant's or enterprise's network PCI DSS compliance responsibilities and efforts.

In this report, Coalfire will explain SecurDPS architecture at a high level, delving into the technical aspects of the solution that are applicable to the compliance. The report will also assess the expected impact of the technology on audit scope using PCI DSS version 4.0.

PAYMENT CARD INDUSTRY DATA SECURTY STANDARD (PCI DSS)

PCI DSS is an information security standard for organizations that handle branded credit cards from Visa, Master Card, Discover, American Express, and JCB. The PCI standard is mandated by the card brands but administered by the PCI Security Standards Council (PCI SSC). Version 1.0 of PCI DSS was published in 2004. This standard has undergone several updates; the current version is 4.0 and was released in March 2022.

PCI DSS applies to all entities involved in payment card processing, including merchants, processors, acquirers, issuers, and service providers. PCI DSS also applies to all other entities that store, process, or transmit CHD or sensitive authentication data (SAD).

Compliance with PCI DSS for the above-named entities is mandatory. Organizations found to be out of compliance with PCI DSS may be subject to fines as assessed by the individual card brands.

PCI DSS is made up of 12 requirements, which can be grouped into six major control objectives:

OBJECTIVES	REQUIREMENTS
Build and Maintain a Secure Network and Systems	**1.** Install and Maintain Network Security Controls. **2.** Apply Secure Configurations to All System Components.
Protect Account Data	**3.** Protect Stored Account Data. **4.** Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	**5.** Protect All Systems and Networks from Malicious Software **6.** Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	**7.** Restrict Access to System Components and Cardholder Data by Business Need to Know. **8.** Identify Users and Authenticate Access to System Components. **9.** Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	**10.** Log and Monitor All Access to System Components and Cardholder Data. **11.** Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	**12.** Support Information Security with Organizational Policies and Programs.

Table 1: PCI DSS High Level Requirement

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 Payment Card Industry Data Security Standard (PCI DSS). 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 the input of a protection method, algorithm attributes, the format of the data, and a distinguishing method.

- **Tokenization**: SecurDPS offers a set of 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 the central processing unit (CPU) without any disk input or output operations, the SecurDPS solution offers a secure approach for the protection of sensitive data.

  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, helping to reduce the exposure of clear text data in the data life cycle to an absolute minimum and eliminating any intermediate storage on the server.

- **Format Preserving Encryption (FPE)**: SecurDPS supports tokenization using Format Preserving Encryption (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 that meet 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****: SecurDPS supports SHA-1, SHA-256, SHA-384, and SHA-512. The SecurDPS format-preserving hashing algorithm can be used to preserve irreversible protection with deterministic results in a way that maintains format properties.

****SecurDPS currently supports the use of SHA-1 hashes. At this time, the PCI SSC accepts the use of cryptographic controls which support a minimum key length of 112-bits key length but strongly recommends the use of cryptographic controls which support a minimum key length of 128-bits in favor of insecure cryptographic protocols, including SHA-1.**

INTEGRATING ENTERPRISE SOLUTIONS

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) environments.

AUDITING AND ANALZYING

SecurDPS has built-in audit and analysis capabilities to help different IT or security stakeholders. SecurDPS provides integration with 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 cardholder numbers 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 include the data elements.
- Sensitive data elements being currently accessed by any users.
- 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

The 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. The Protection Cluster consists of the following sub-components:

- **Management Console (MC):** The protection cluster is centrally administered through an MC. The MC 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 (EAs) connect to the PN to protect or reveal sensitive data elements using SecurDPS APIs or the transparent protection layer. PNs do not store any data on a local or network disk and perform all operations in memory.

- **Audit Console (AC):** AC collects and displays metrics about usage of protection services by an EA, 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 AC can be run standalone or as a cluster on its own. The AC consists of multiple subcomponents and services as shown in Figure 1. Key components of the AC 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 (Dashboard).
    - **Logstash**: Logstash is a data processing pipeline. It is used to ingest data from Kafka into Elasticsearch.
    - **Kibana**: Kibana provides visualization in 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 MC to Kafka.

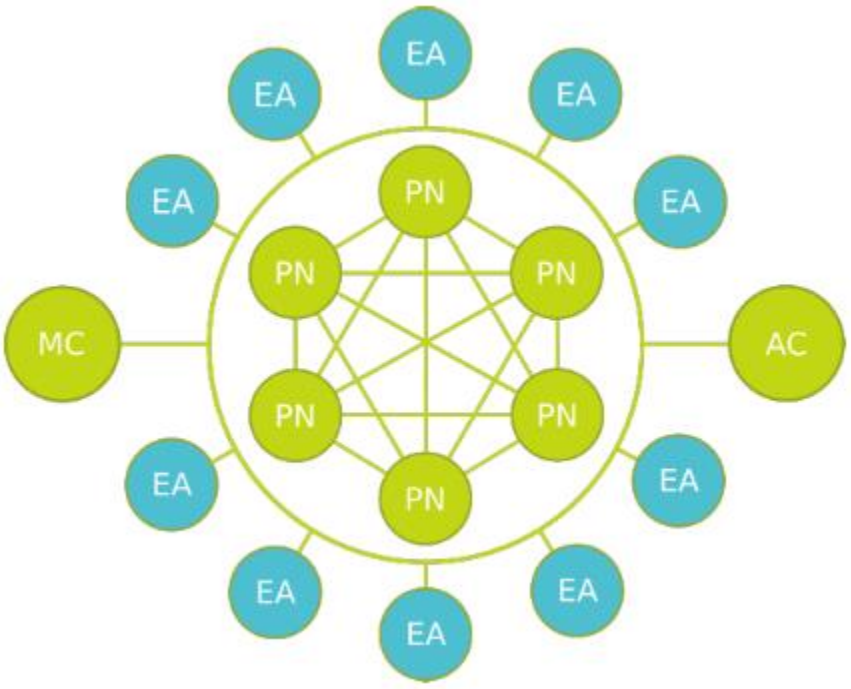


FIGURE 1: SECURDPS PROTECTION CLUSTER HIGH-LEVEL ARCHITECTURE AND COMPONENTS

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 virtual appliances are based on the specialized and highly secure SecurDPS Operating System (SecurDPS OS), which 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 instant messaging (IM) 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 fault tolerance and performance features.

- **Stateless protection nodes** – The PN operates purely in memory and CPU and does not require permanent storage. The configurations are managed centrally via the MC, 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 MC and PNs hold it in memory once seeded. Once a PN is shut down, the secrets do not exist in the PN.

In addition to the data protection features provided by SecurDPS, the Discover & Classify module queries structured and unstructured data sources to identify sensitive information and sensitive personal data via the following components:

- **Analytic Engine** – The analytic engine can be configured for data-in-motion discovery, including network and interfaces, DNS, domains, subnets and IP ranges.

- **Data Source Catalog** – The data source catalog application stores data source entries regarding how to connect to each data source and when to analyze it. Data source analysis discovers and retrieves locations of all instances of sensitive data-at-rest. Analysis of data-at-rest is executed by seven analyzing plugins:

    - Database Analyzer (DB Analyzer): Analyzes SQL databases aiming at discovering and retrieving the sensitive data instances from the database tables.

    - NoSQL Service (NoSQL): Analyzes the NoSQL databases, discovering and retrieving the sensitive data instances from the database tables.

    - File System Analyzer (FS Analyzer): Analyses files in the local and cloud storage, discovering and retrieving sensitive data instances. The FS analyzer supports the commonly used file formats, both structured and unstructured.

    - Google Analyzer: Analyzes Google products, discovering and retrieving sensitive data instances. Google analyzer supports both structured and unstructured file formats.

    - MS365 Analyzer: Analyzes Microsoft data sources, discovering and retrieving sensitive data instances in files, emails, notes, etc.

    - Salesforce Analyzer: Analyzes files in Salesforce accounts.

    - BigQuery Analyzer: Analyzes Google BigQuery data lakes.

- **Master Catalog** – This is a baseline catalog created by the end user from the entire contents of the data source. The master catalog consists of personal data, which integrates all data relevant to a specific data subject, including links to all copies of personal data, data sources and metadata on the sources, and data assets.

- **Data Asset** – This is the set of organization data that brings value to the business. Within Discover & Classify, data assets are manually configured virtual catalogs of data subjects, grouped by business purpose or the reasons for processing. Data assets can be associated with the following business purposes:
    - Geographic location of individuals for compliance with local privacy regulations like GDPR, CCPA.
    - Grouping individuals for compliance with security regulations for different types of data like PCI security policy for credit card data or HIPPA for medical data.
    - Grouping individuals by role, e.g. customers, employees, consultants.
    - Grouping individuals by business unit or business needs, e.g. marketing, service, IT.

DEPLOYMENT SCENARIOS

OPTION 1: KUBERNETES DEPLOYMENT VIA HELM CHART

With this deployment option, the SecurDPS protection cluster can be deployed into Kubernetes environments using the corresponding Helm Chart. The installation and management of SecurDPS in this deployment model is mainly performed using Helm commands, with Kubernetes providing the overall orchestration.

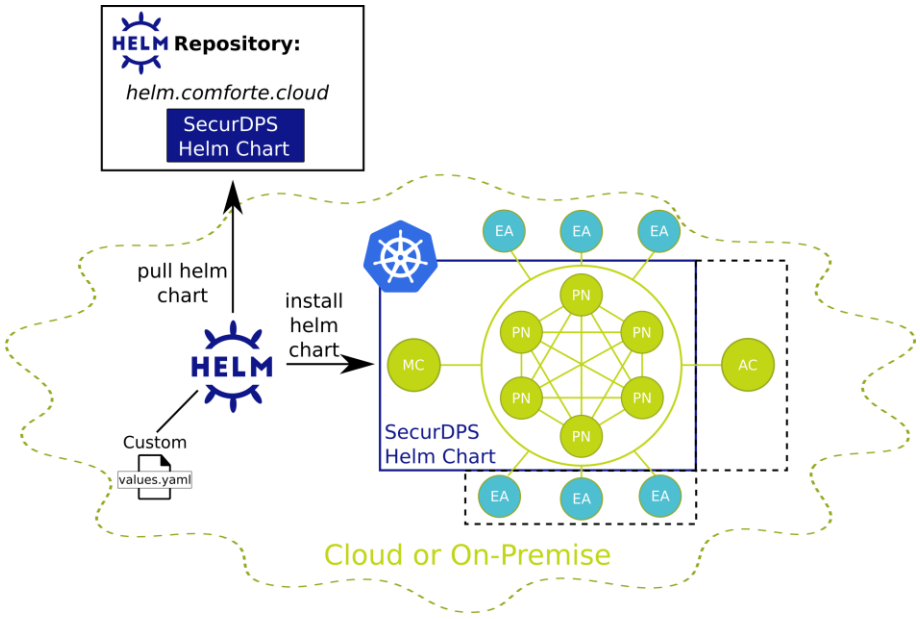


FIGURE 2: SECURDPS KUBERNETES DEPLOYMENT VIA HELM CHART

OPTION 2: MC/AC ON-PREMISES AND HYBRID PN CLUSTER DEPLOYMENT

With this deployment option, the Management Console and Audit console are deployed on-premises, and they can either be used in conjunction with a Protection Node cluster deployment on-premises or in the cloud. Even with this model where the Protection Nodes are deployed in the cloud, security relevant information is never stored in the cloud and only resides in-memory of the Protection Nodes.

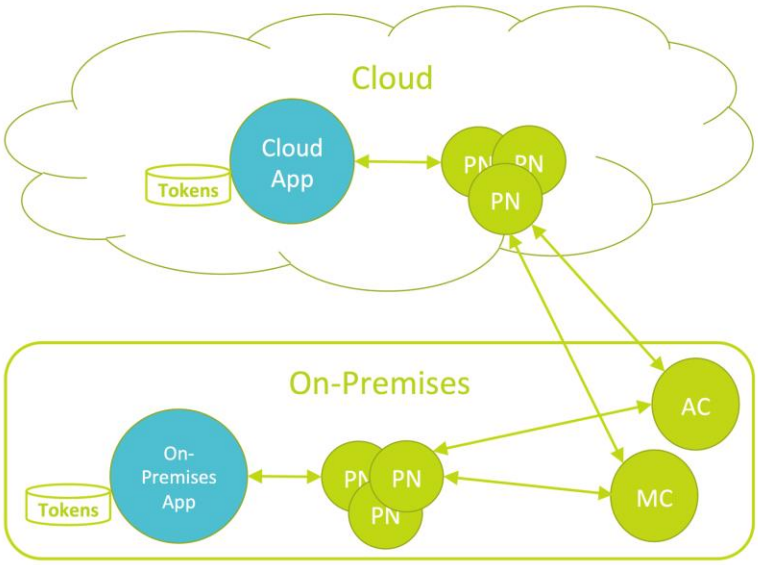


FIGURE 3: SECURDPS ON-PREMISES AND HYBRID CLOUD DEPLOYMENT

OPTION 3: CLOUD DEPLOYMENT

With is deployment option, the overall SecurDPS Protection Cluster, including the Management Console, Protection Nodes and Audit Console are deployed in a cloud infrastructure. Enterprise applications utilizing the services of the Protection Nodes can run either in the cloud environment or in an on-premises deployment.

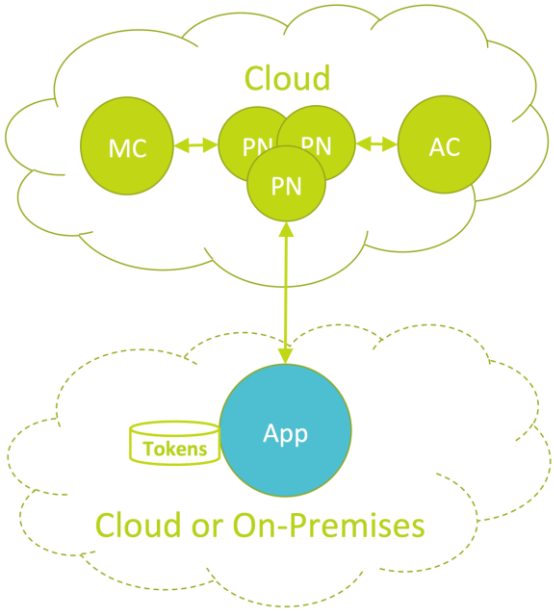


FIGURE 4: SECURDPS CLOUD DEPLOYMENT

ASSESSMENT METHODOLOGY

SecurDPS protects sensitive data stored on systems components via tokenization, masking and/or hashing mechanisms. Data protection mechanisms provided by SecurDPS are secured within the SecurDPS Virtual Appliance

with AES-256-bit encryption. Additionally, use of the Discovery & Classification component within SecurDPS assists in the identification of unprotected sensitive data.

Coalfire validated the sensitive data protection and identification mechanisms provided by SecurDPS solution in support of applicable PCI DSS v4.0 controls.

ASSESSMENT METHODS

Coalfire performed technical testing of the SecurDPS components (Data Protection and Discovery & Classification) in a cloud environment built to ComforteAG's specifications. Deployment architecture included the use of the Management console and Protection Nodes. All components supporting SecurDPS were deployed within an Amazon Web Services Kubernetes environment.

Test data for filesystems with environment was provided by Comforte to demonstrate the functionality and effectiveness of the SecurDPS solution.

Testing and administration of the SecurDPS solution in Coalfire's AWS environment was done using SSH v2 with strong cryptographic ciphers.

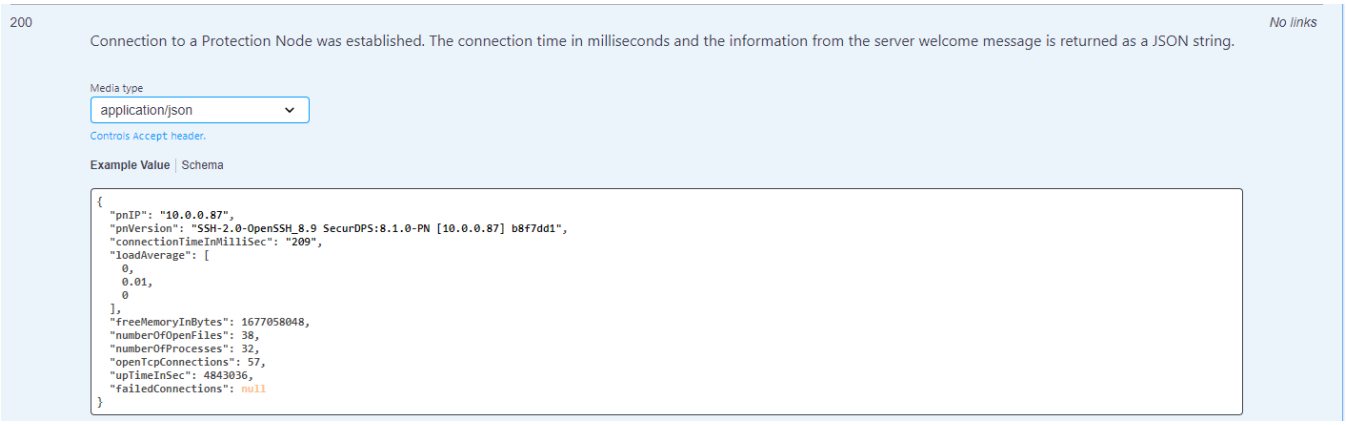


FIGURE 5: CONNECTION TO PROTECTION NODE VIA SSH

```
Include /etc/ssh/ssh_config.d/*.conf

Host *
#   ForwardAgent no
#   ForwardX11 no
#   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
#   IdentityFile ~/.ssh/id_dsa
#   IdentityFile ~/.ssh/id_ecdsa
#   IdentityFile ~/.ssh/id_ed25519
#   Port 22
#   Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
#   MACs hmac-md5,hmac-sha1,umac-64@openssh.com
#   EscapeChar ~
#   Tunnel no
#   TunnelDevice any:any
#   PermitLocalCommand no
#   VisualHostKey no
#   ProxyCommand ssh -q -W %h:%p gateway.example.com
#   RekeyLimit 1G 1h
#   UserKnownHostsFile ~/.ssh/known_hosts.d/%k
    SendEnv LANG LC_*
    HashKnownHosts yes
    GSSAPIAuthentication yes
```

FIGURE 6: PROTECTION NODE SSH CONFIGURATION

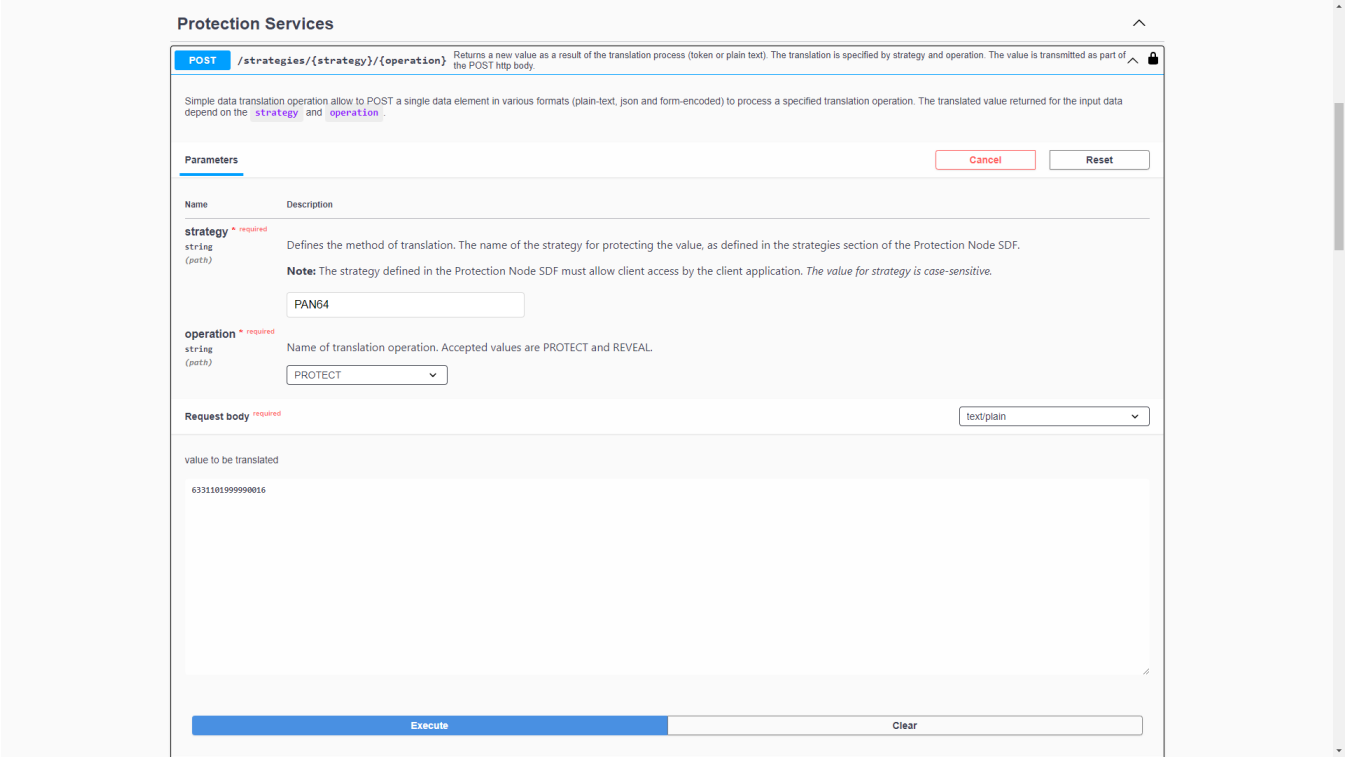
VAULTS AND STRATEGIES

Coalfire tested the SecurDPS Data Protection solution with the base configuration, including the security vaults used to protect data. Coalfire observed that cardholder data was tokenized using the protection schemes defined in the Security Definition File (SDF). Cardholder data processed by REST API yielded a token which only exposed the first six and last four digits of the card number, replacing the middle 4-6 digits of the specific card number with a random numeric string dependent upon the card brand's number scheme. Additionally, it was observed that ACLs for data access (Protect and Reveal) could also be set within the data protection strategy in an effort to further limit access already granted to users with access to the REST API.

```
ACCNR:
  vault: ACCNR-VAULT
  distinguish-method: NONE
  format: NUMERIC
  audit-collector: TEST-AUDIT
  audit-interval: 30
  preserve-first: 1
  preserve-last: 3
  use-preserved-data-as-salt: true
  direct-interface: "#ACCNR"
  acl:
    TEST: PLR # P=Protect, L=Lookup, R=Reveal
  unique-index: true
  preserve-length: true

CARDNR:
  vault: CARDNR-VAULT
  distinguish-method: NONE
  format: NUMERIC
  audit-collector: TEST-AUDIT
  audit-interval: 30
  preserve-first: 6
  preserve-last: 4
  use-preserved-data-as-salt: true
  direct-interface: "#CARDNR"
  acl:
    TEST: PLR # P=Protect, L=Lookup, R=Reveal
  unique-index: true
  preserve-length: true


PAN64:
  vault: CARDNR-VAULT
  distinguish-method: NONE
  format: NUMERIC
  audit-collector: TEST-AUDIT
  audit-interval: 30
  preserve-first: 6
  preserve-last: 4
  use-preserved-data-as-salt: true
  direct-interface: "#PAN64"
  acl:
    TEST: PLR # P=Protect, L=Lookup, R=Reveal
  unique-index: true
  preserve-length: true
```

```
ACCNR-VAULT:
  type: swift3
  store: ACCNR
  prf: siphash-128
  alphabet: NUMERIC
  ignore-unsupported-chars: true

CARDNR-VAULT:
  type: swift3
  store: CARDNR
  prf: siphash-128
  alphabet: NUMERIC
  ignore-unsupported-chars: true
```

FIGURE 7: SECURITY VAULTS AND STRATEGIES



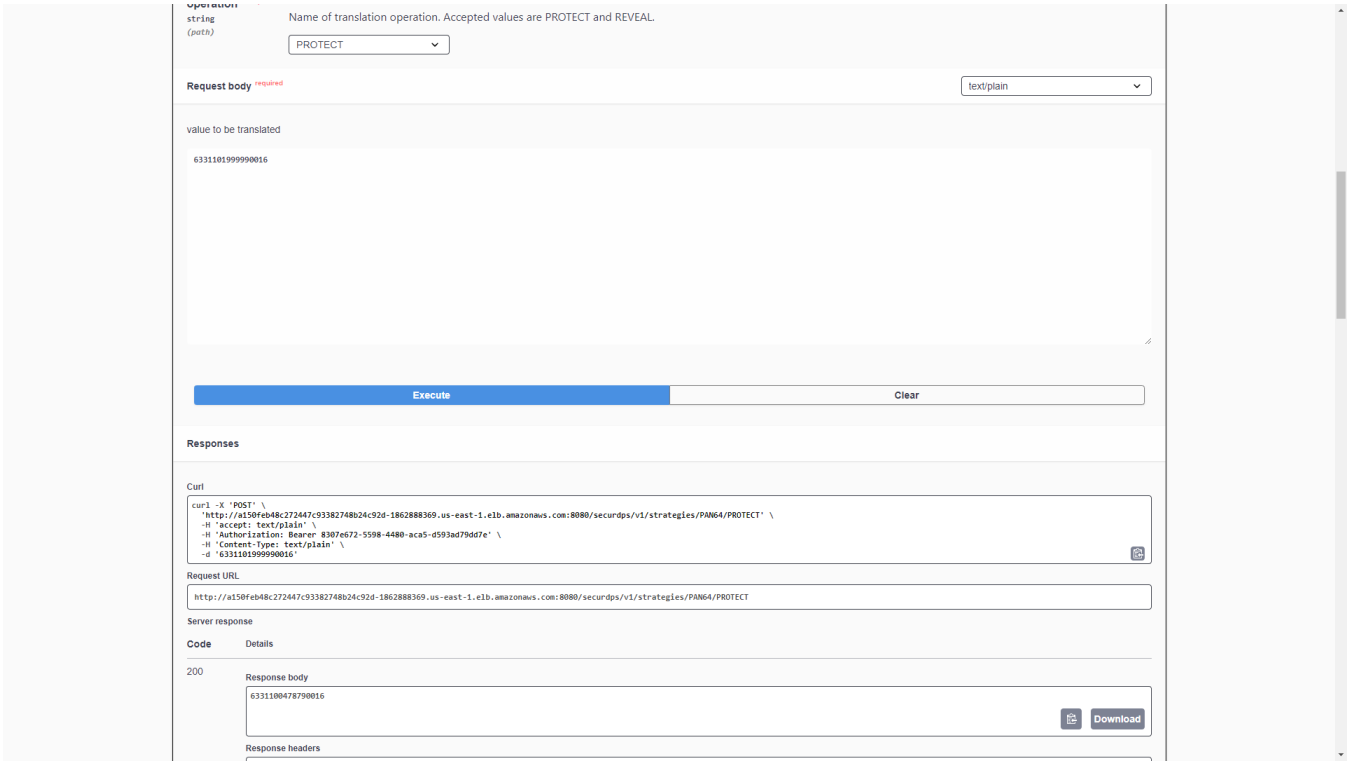
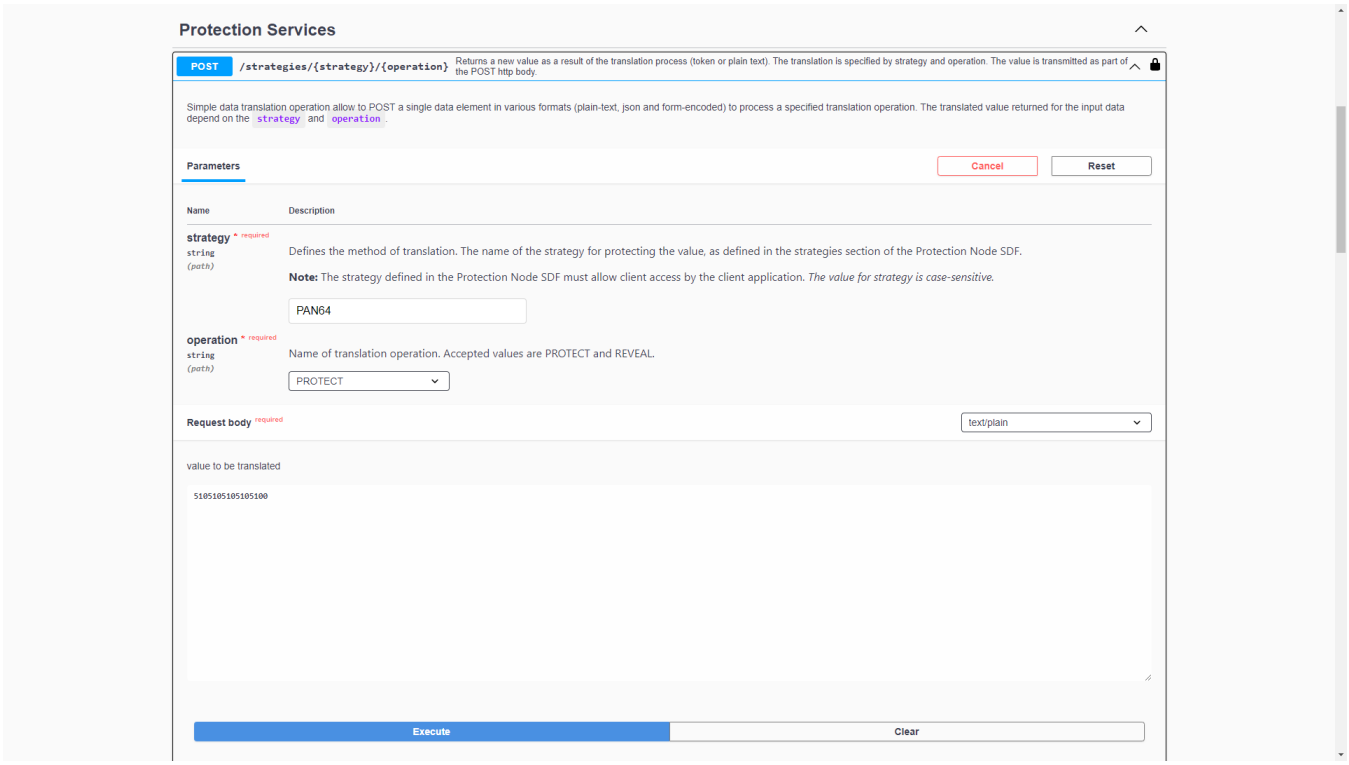


FIGURE 8: PRIVATE CARD TOKENIZATION



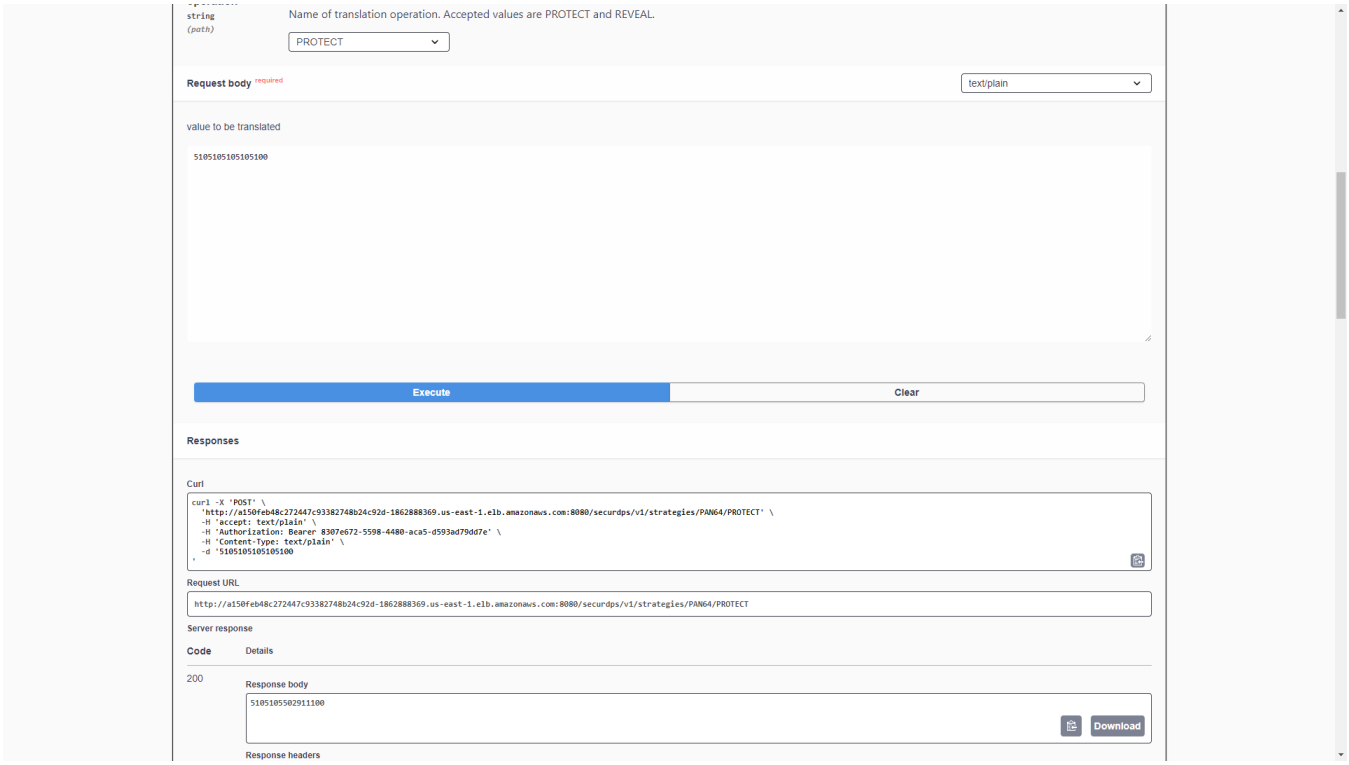
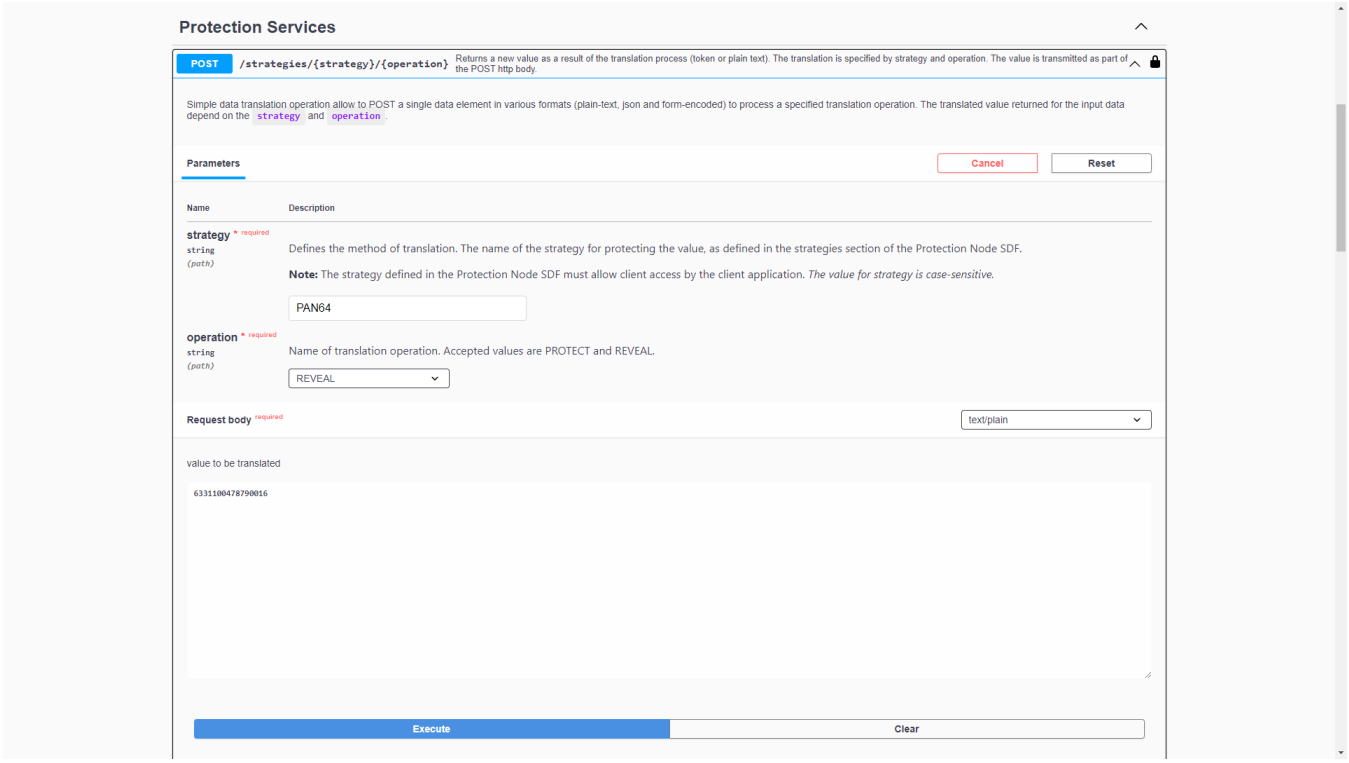


FIGURE 9: BRANDED CARD TOKENIZATION



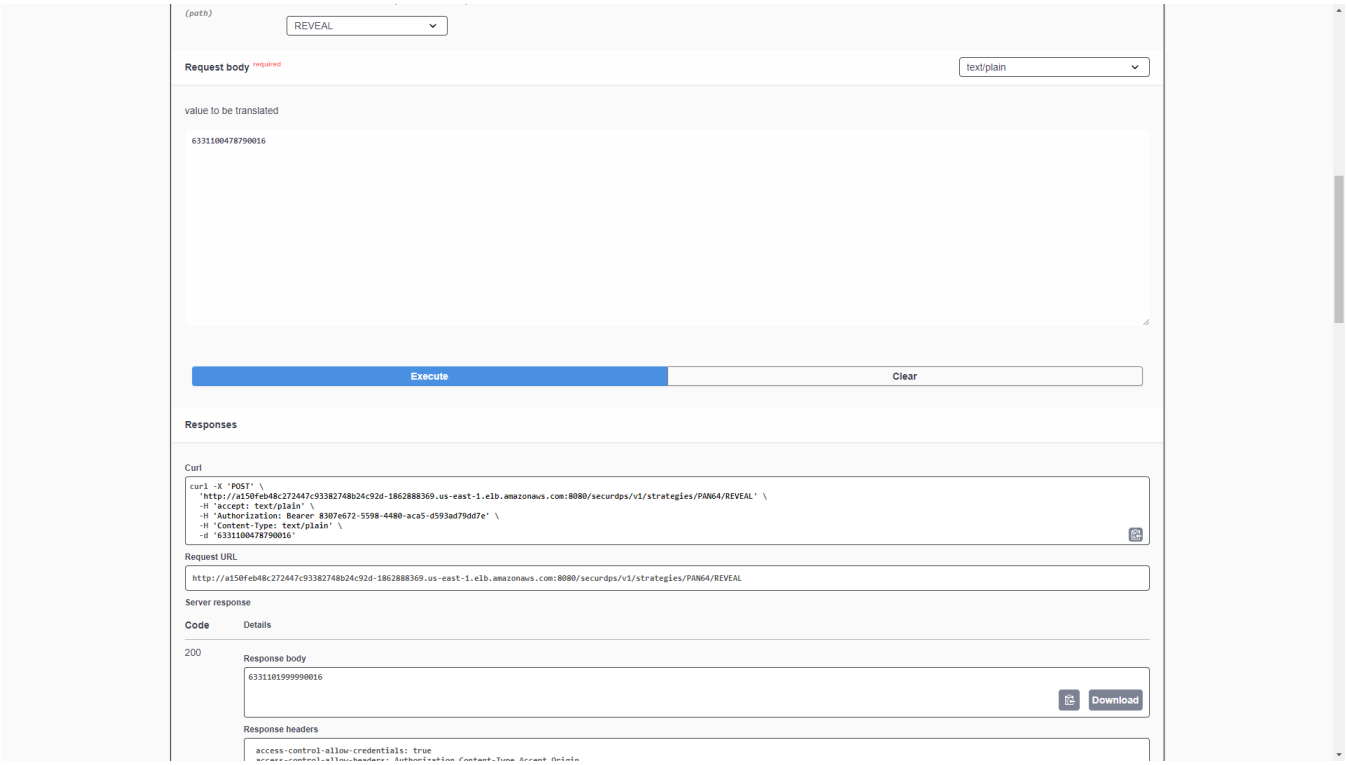
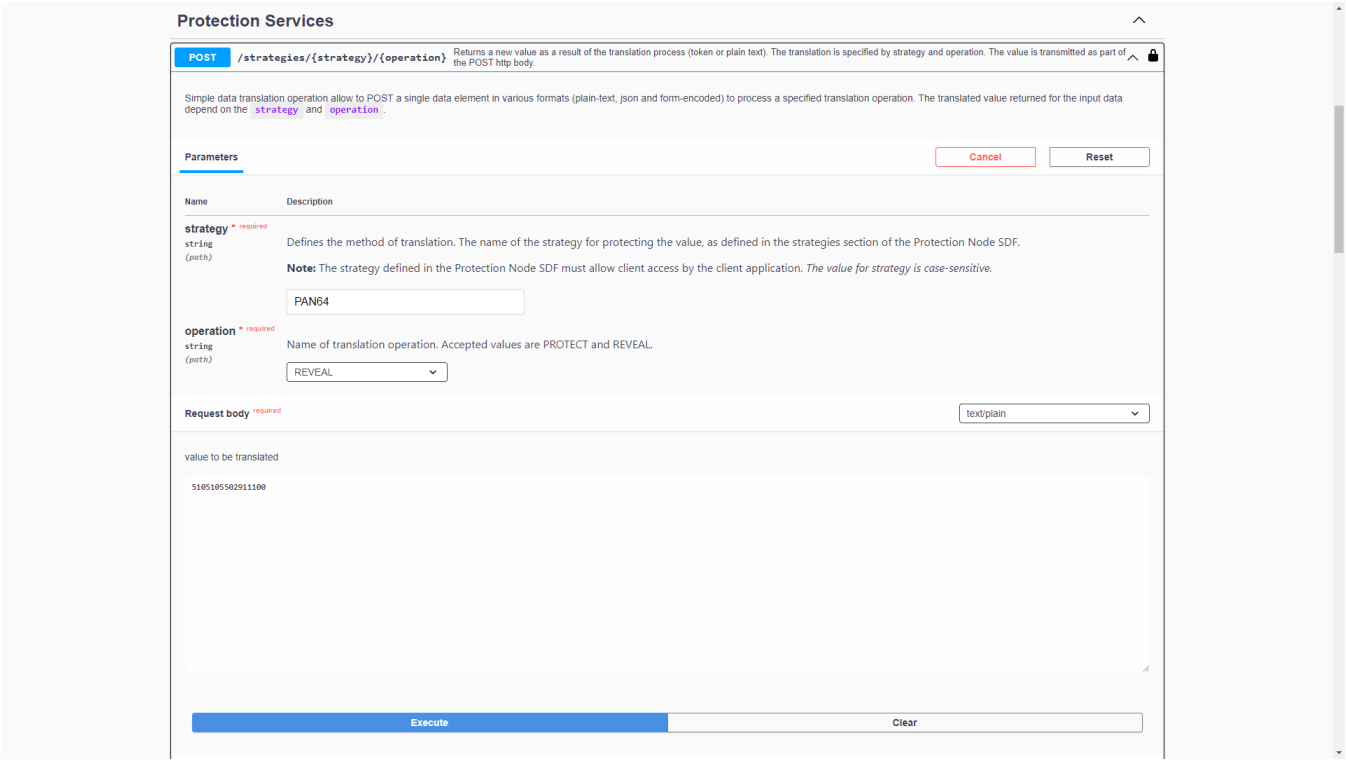


FIGURE 10: PRIVATE CARD TOKEN REVERSAL



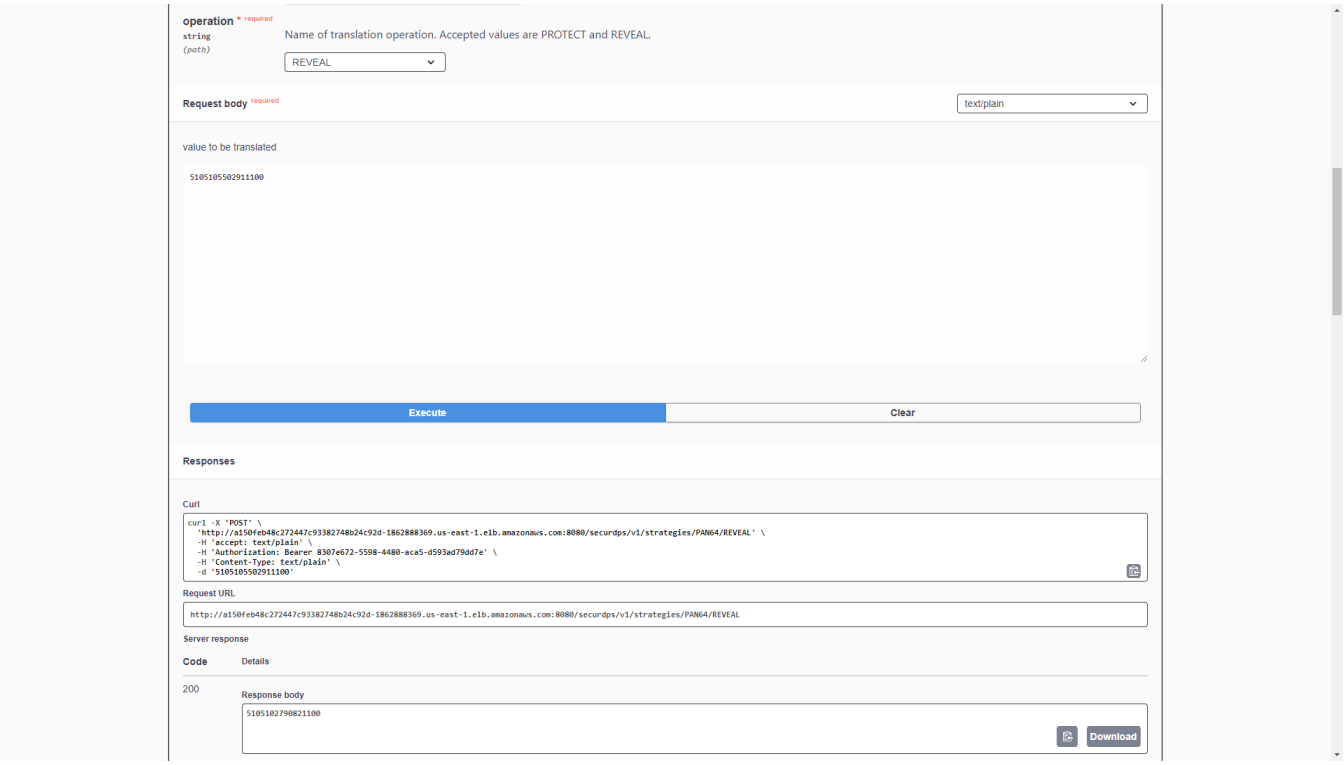


FIGURE 11: BRANDED CARD TOKEN REVERSAL

AUDIT LOGGING

Coalfire was able to view activity logs from the SecurDPS protection cluster via a dedicated syslog server. Observable events from the protection cluster included authentication events via SSH, and protection node events including data protection or reveal activities.

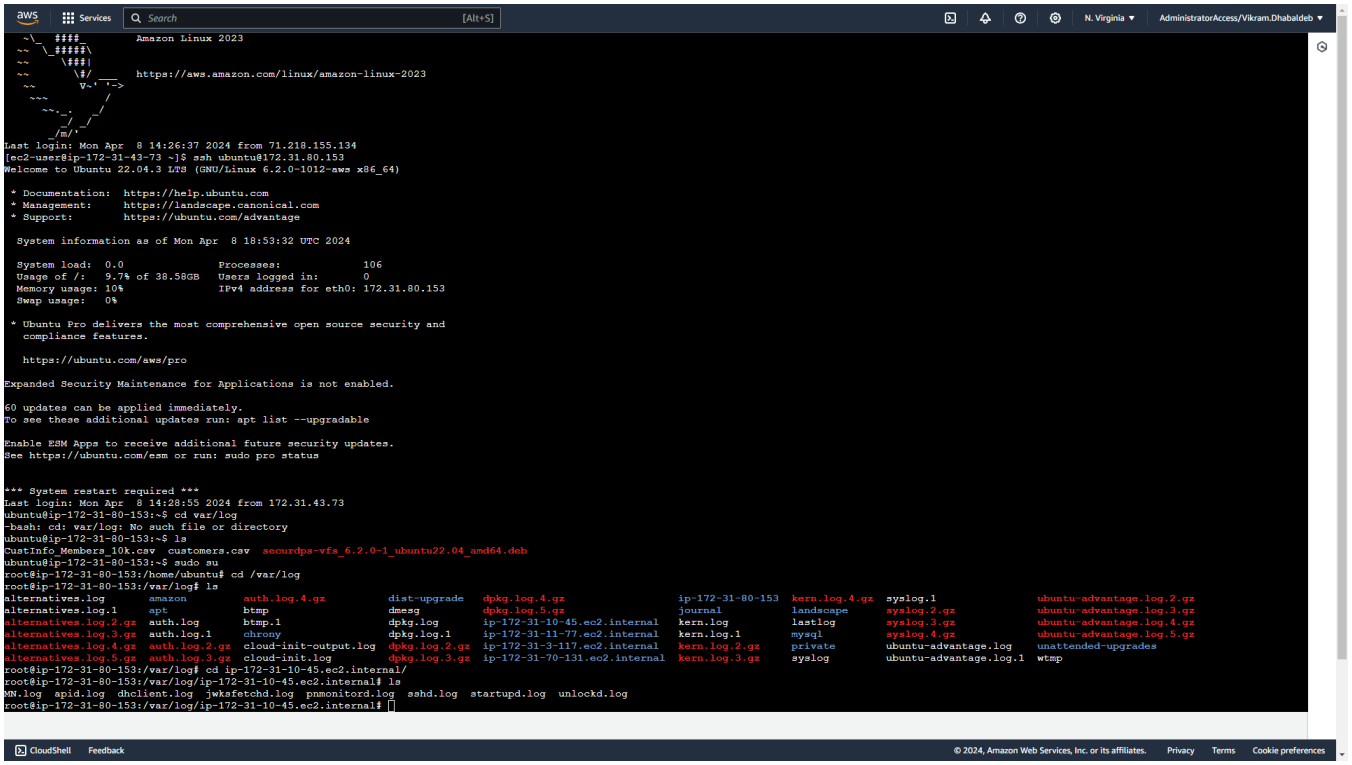


FIGURE 12: SYSLOG SERVER RECORDS

SECURDPS AUDIT CONSOLE

Coalfire tested the Audit Console component which supports Comforte SecurDPS via the browser-based user interface. Coalfire was able to observe data “protect” and “reveal” activities executed in SecurDPS via the REST API, as well as unauthorized/unauthenticated attempts to view data. Additionally, Coalfire observed “trigger” events could be configured to generate and send alerts, and data/metrics monitors could be setup based on customer needs.

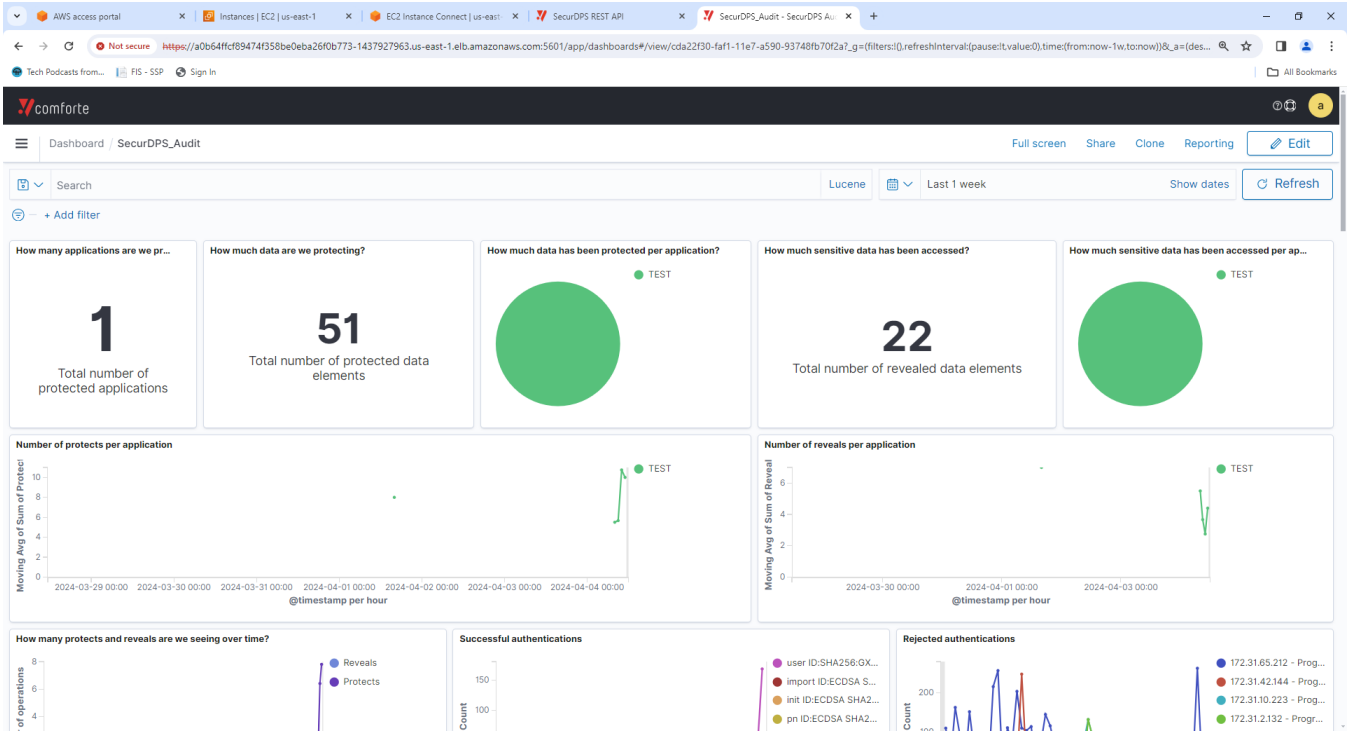


FIGURE 13: AUDIT CONSOLE DASHBOARD

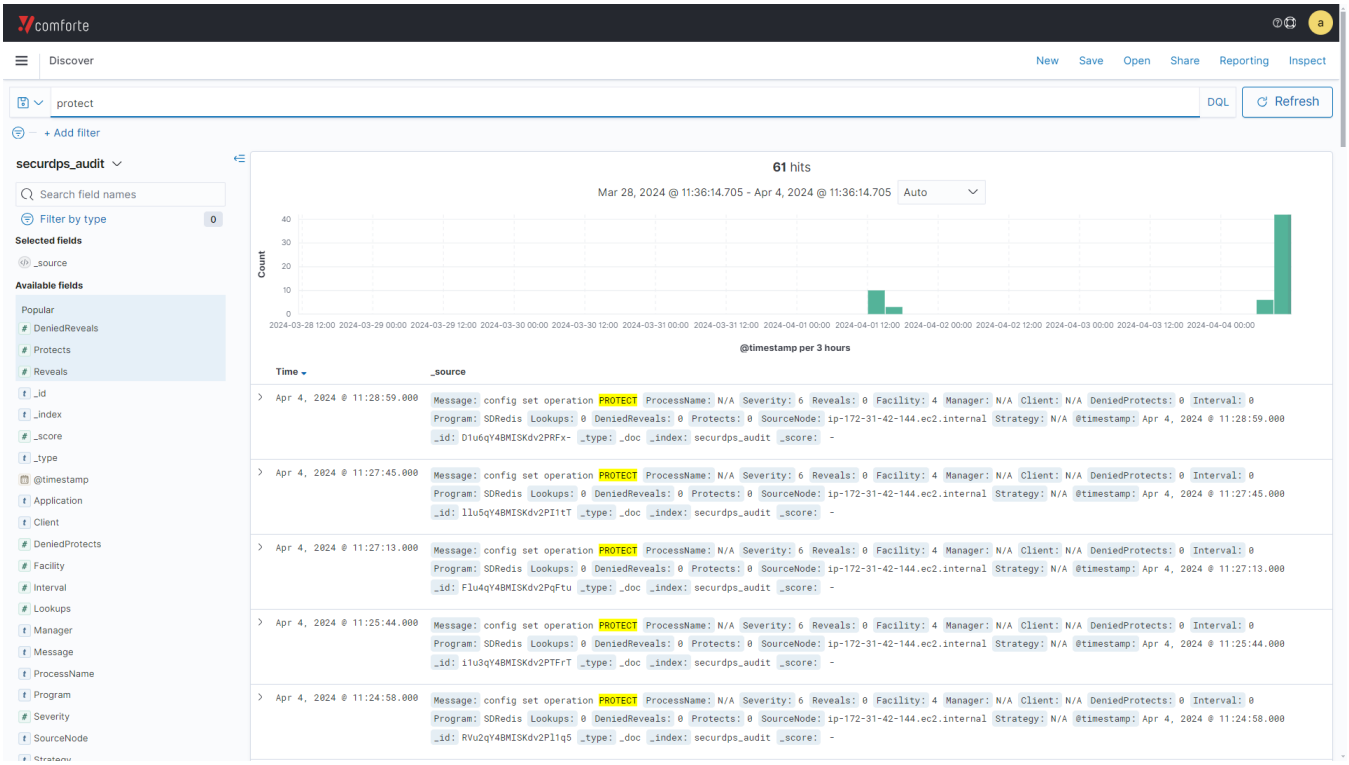


FIGURE 14: DATA PROTECTION LOGS

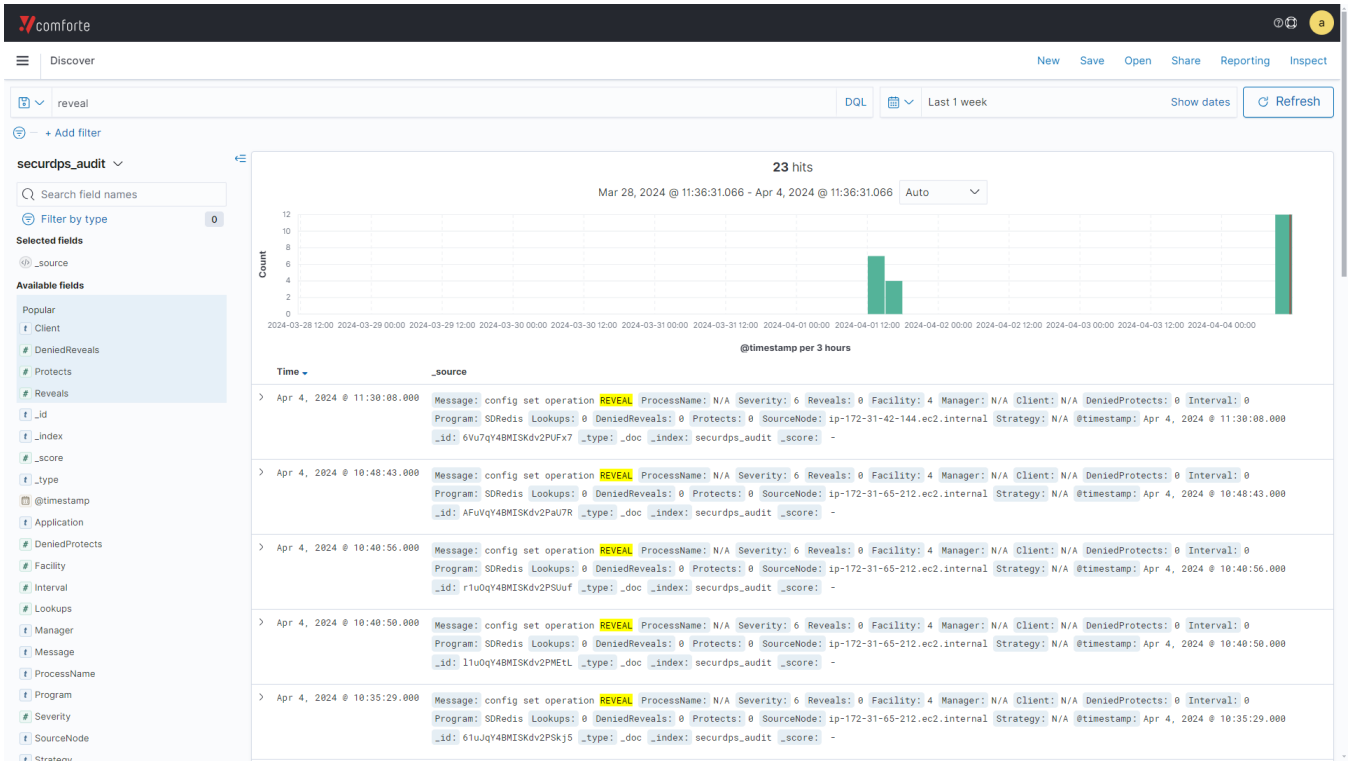
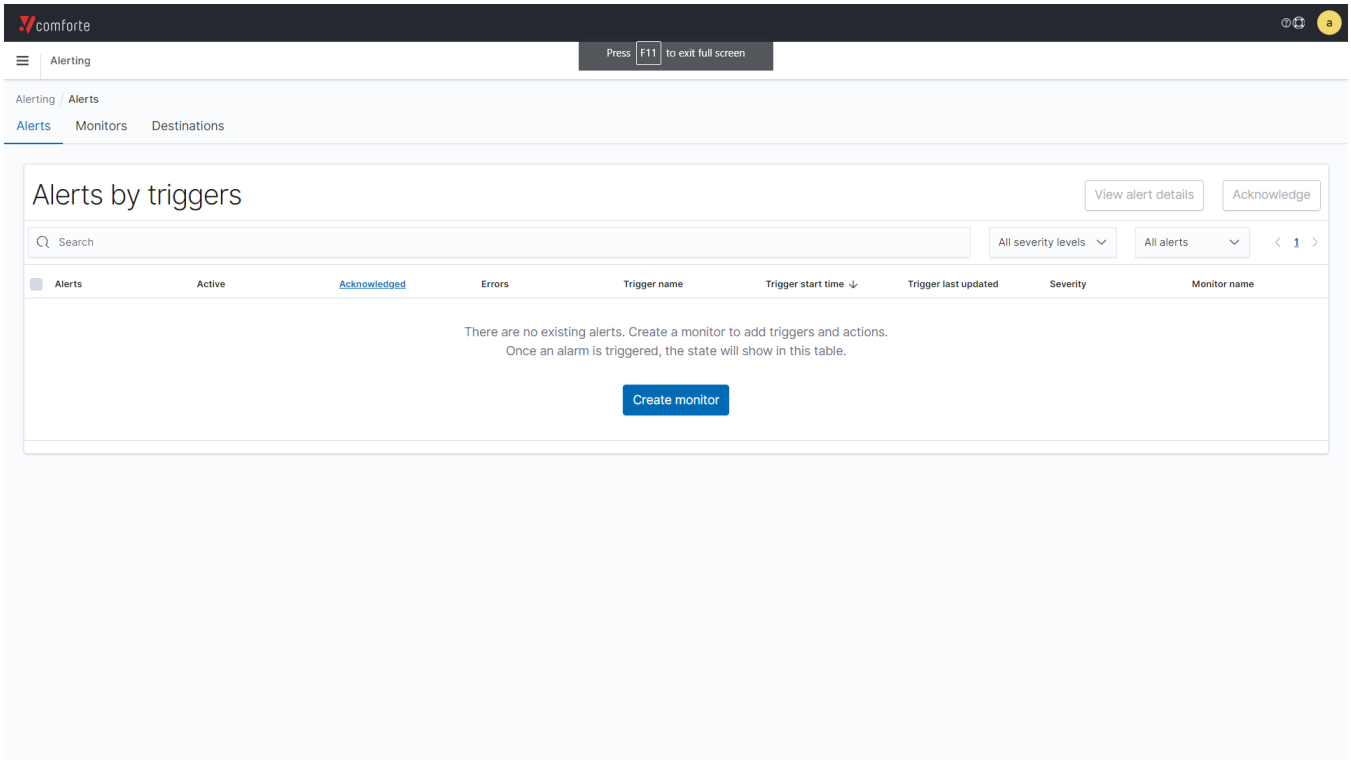
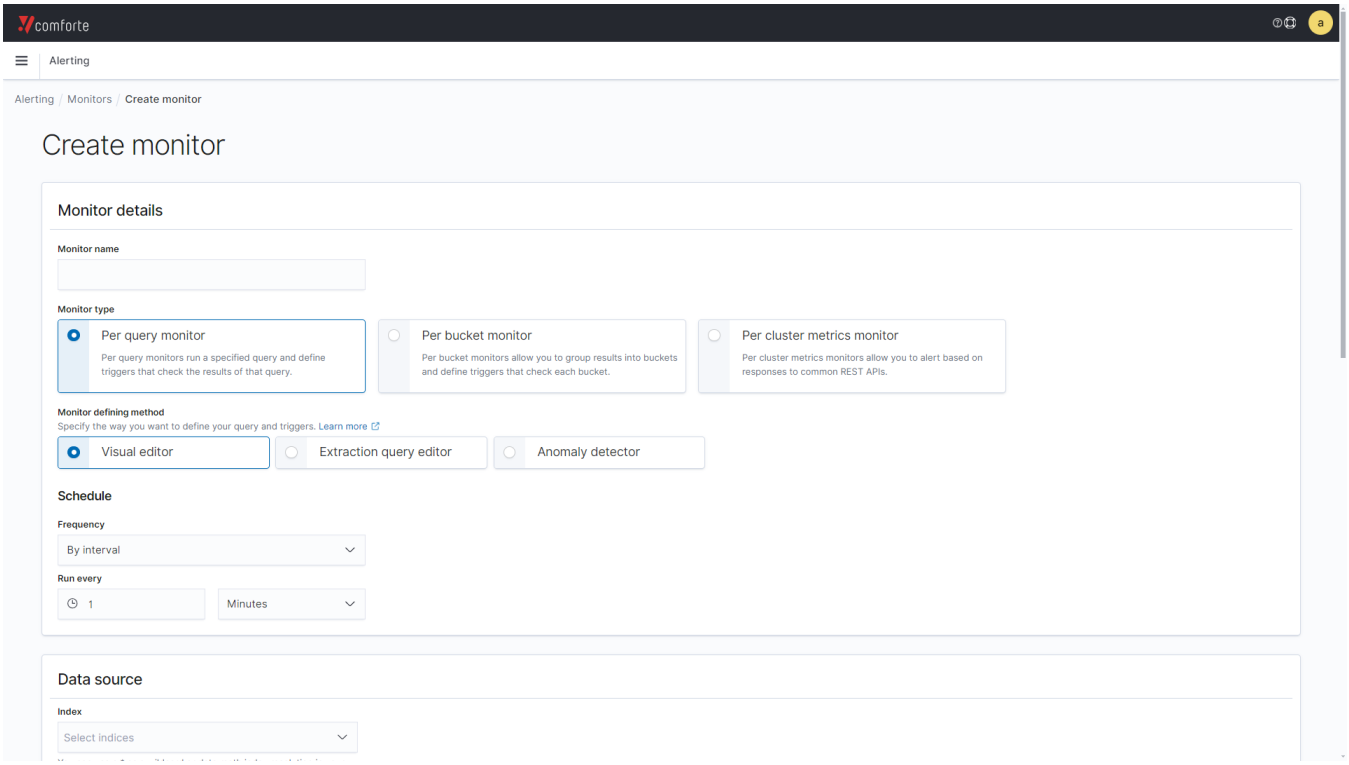


FIGURE 15: DATA REVEAL LOGS





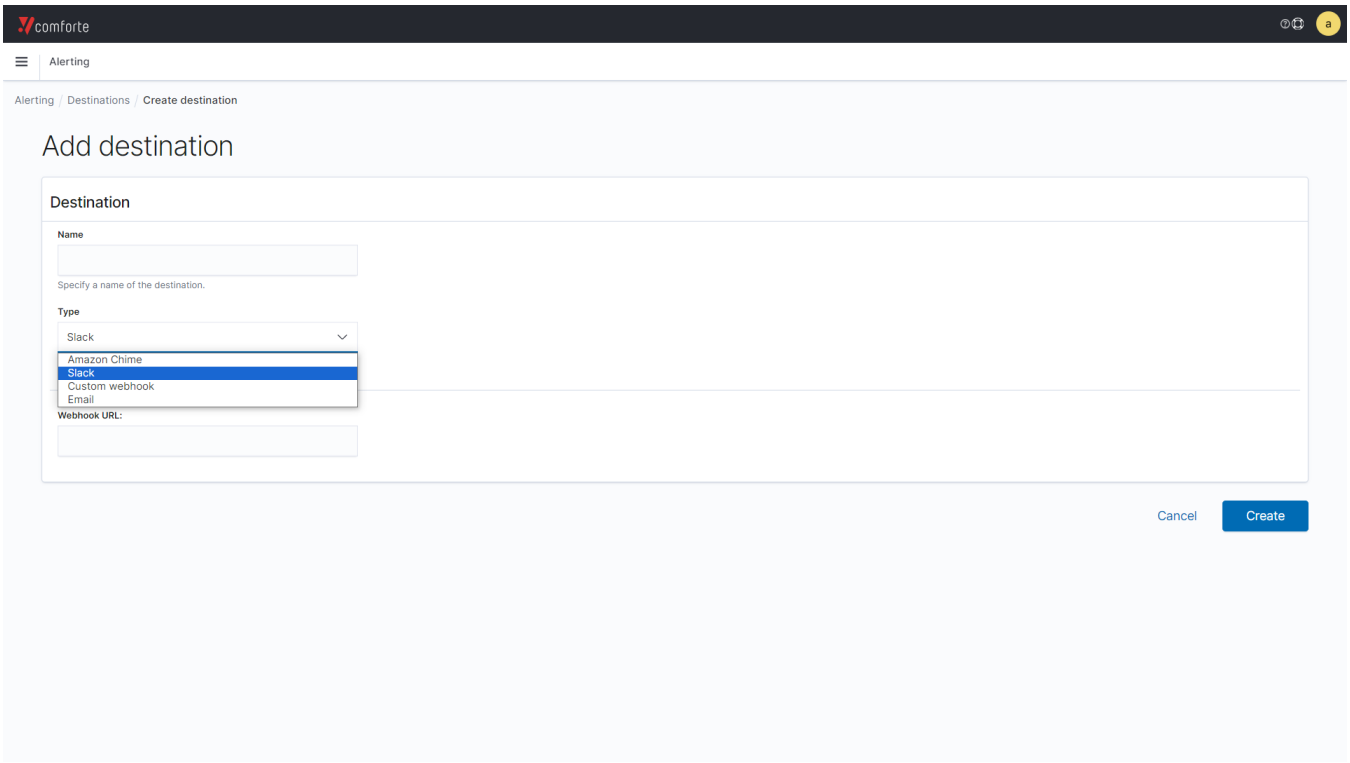


FIGURE 16: EVENT ALERTING TRIGGER, CUSTOM MONITORING AND EVENT FORWARDING CONFIGURATIONS

DISCOVERY & CLASSIFICATION

Coalfire tested the Discovery & Classification solution via the browser-based application which reported in on data within the AWS test environment setup for this engagement.

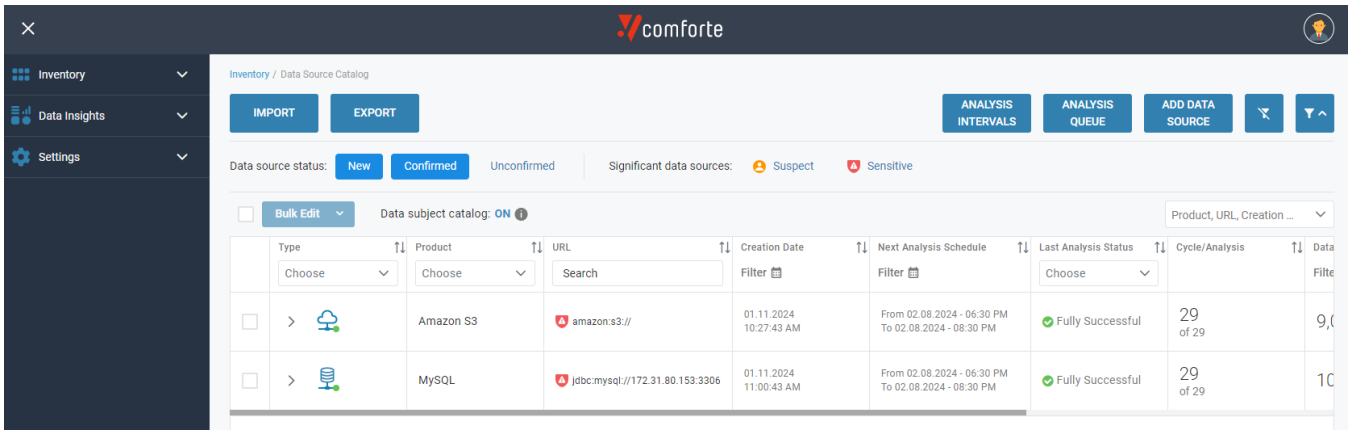


FIGURE 17: DISCOVERY & CLASSIFICATION MONITORED DATA SOURCES

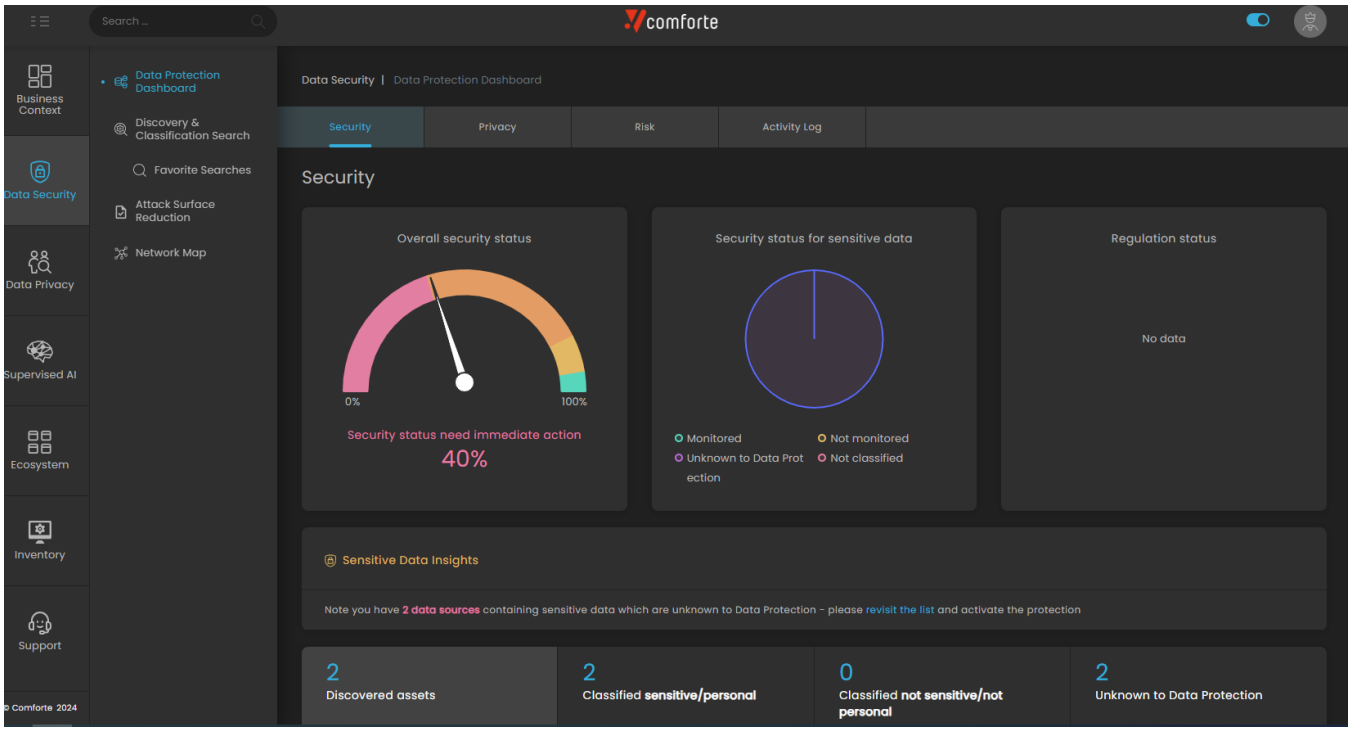


FIGURE 18: DISCOVERY & CLASSIFICATION DASHBOARD

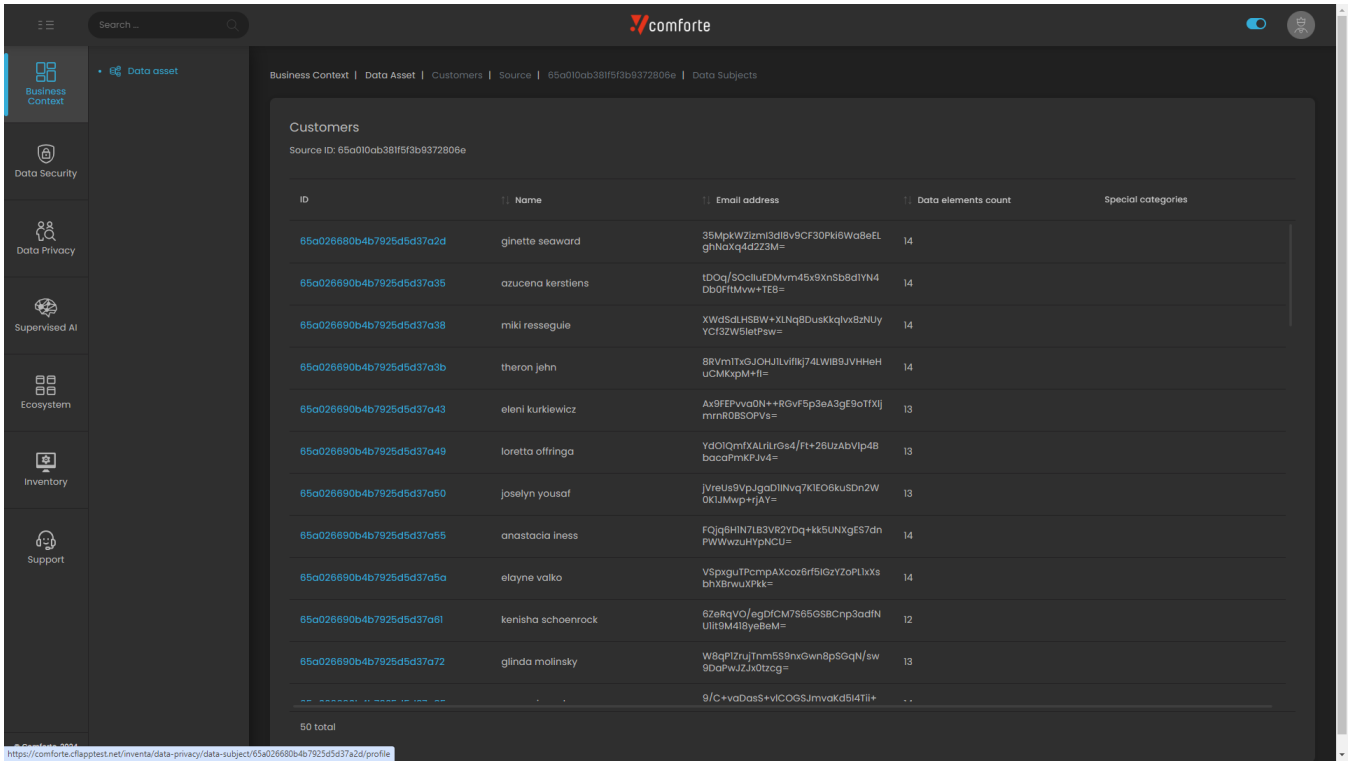
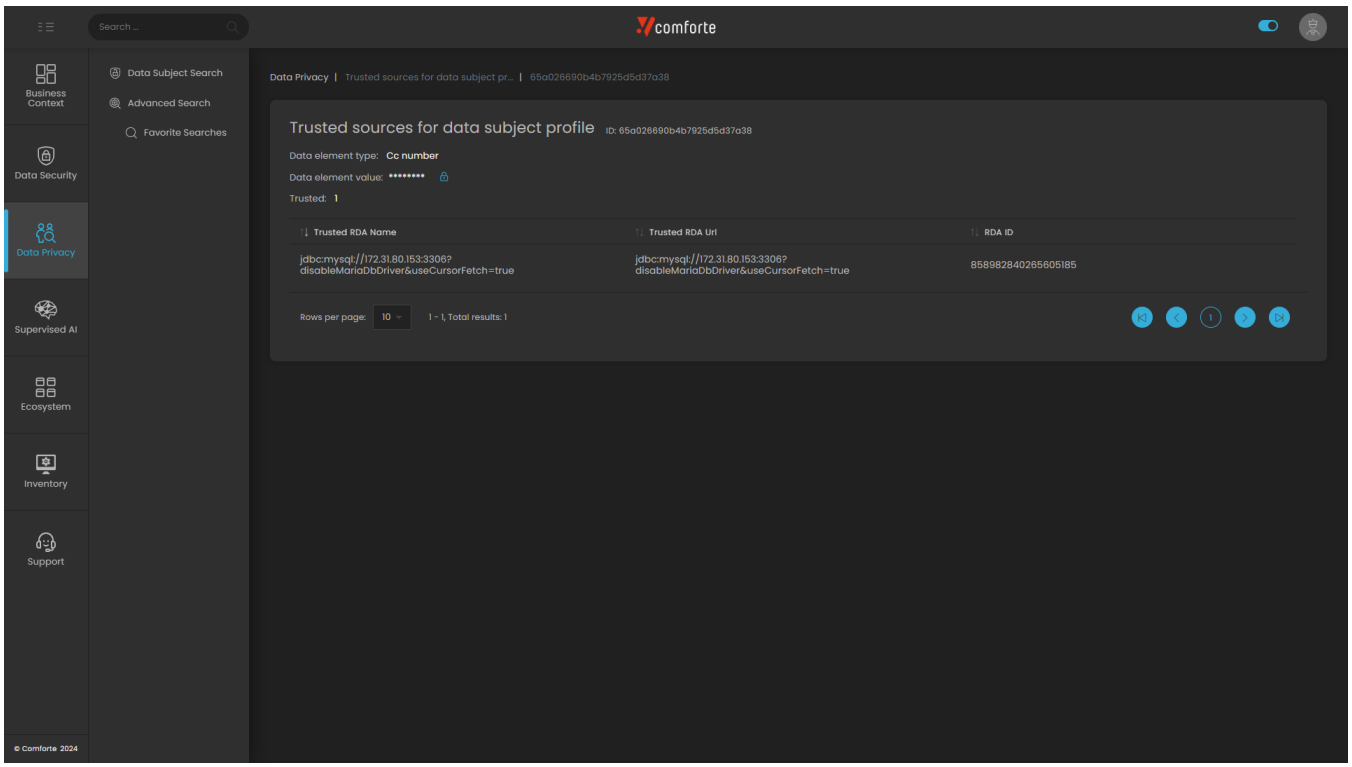


FIGURE 19: DISCOVERY & CLASSIFICATION DATA ASSETS



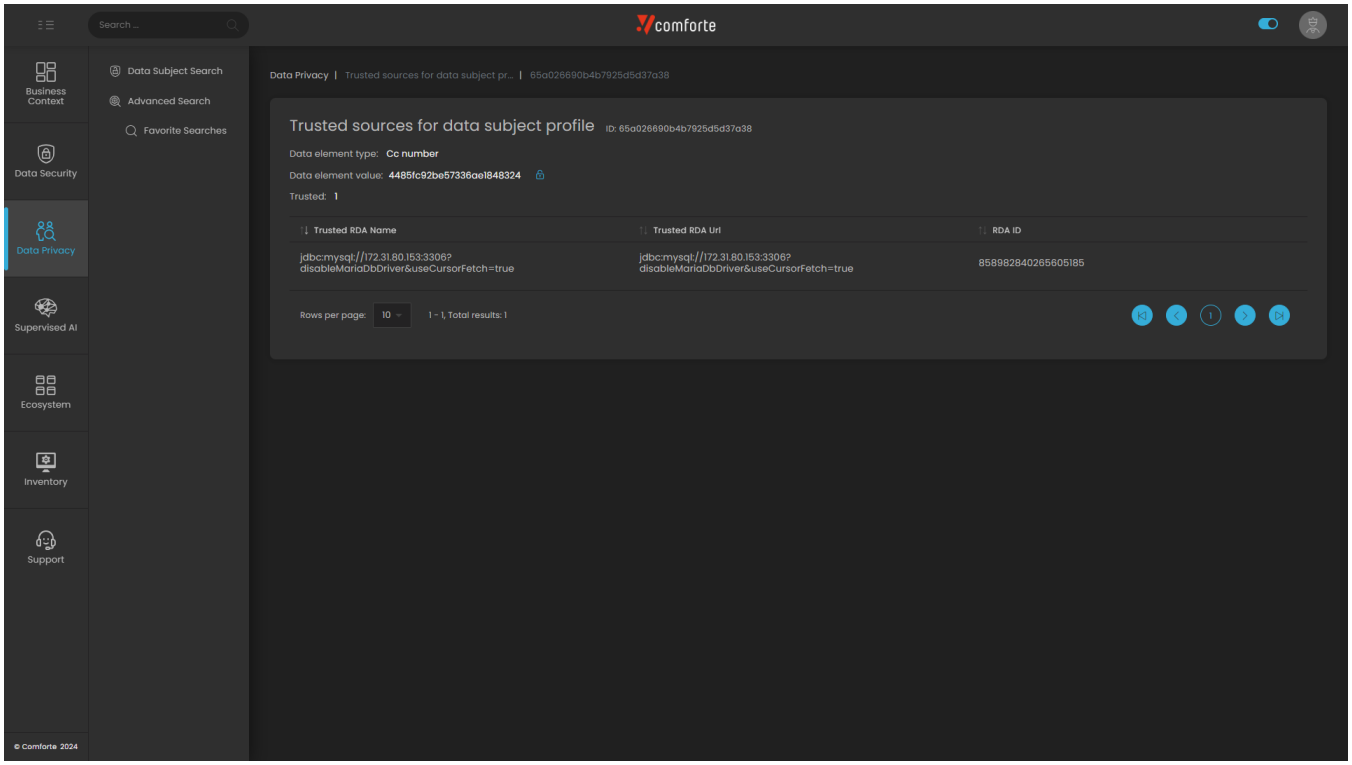


FIGURE 20: DISCOVERY & CLASSIFICATION DATA SUBJECT HIDE AND REVEAL

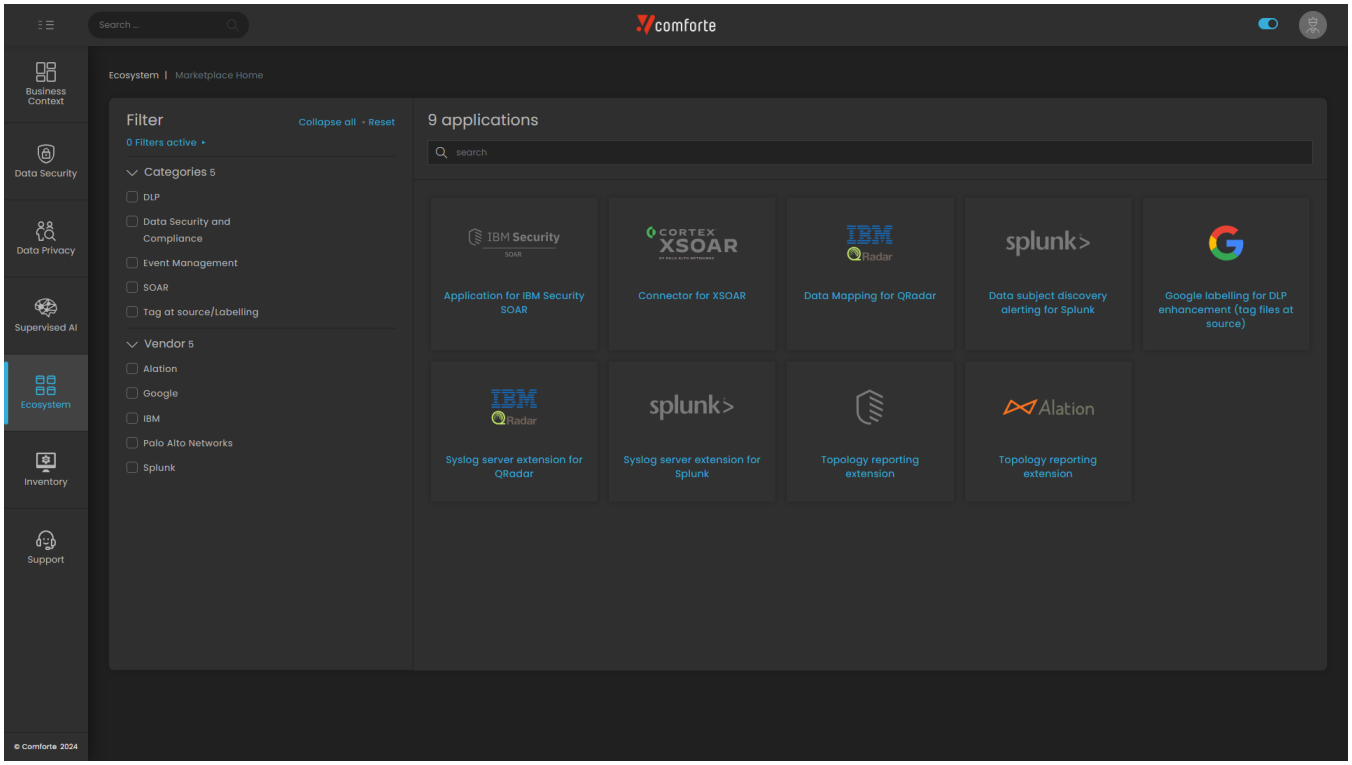


FIGURE 21: DISCOVERY & CLASSIFICATION THIRD-PARTY INTEGRATION OPTIONS

COALFIRE FINDINGS

Coalfire found that SecurDPS solution protected sensitive data using appropriate tokenization, masking and/or hashing strategies. SecurDPS relied on a tokenization mechanism which resided within the SecurDPS Virtual Appliance. Users could tokenize sensitive data or access tokenized data and view the full contents (i.e. Primary Account Number(PAN)) via the REST API. Coalfire observed that the tokenization algorithm used by SecurDPS generated a random output to ensure unique tokens for each instance of sensitive data protected by the solution.

Additionally, Coalfire found that the discovery and classification solution appropriately identified unprotected sensitive data using both vendor and user defined search parameters. Discovery & Classification provided a centralized view of all sensitive data identified by data asset type, data source and/or data subject which resided within environment in plain text format. Viewing access to data within the discovery and classification solution could be controlled by Role Based Access Controls (RBAC) at the application and/or entity level.

POTENTIAL IMPACT ON PCI DSS 4.0 APPLICABLE CONTROLS TABLE

In this section, the SecureDPS solution is evaluated against the PCI DSS v4.0 requirements at a granular level. Any requirements not identified in the table below are fully the responsibility of the customer implementing the solution within their environment. Requirements identified in the table below are categorized as “supports” or “meets” to identify which security controls SecurDPS provides support to meet and which security controls SecurDPS can meet for the entity implementing the solution.

KEY TO POTENTIAL IMPACT ON APPLICABLE CONTROLS TABLE

PCI DSS 4.0 REQUIREMENT	SecurDPS supports this requirement	SecurDPS meets this requirement	SecurDPS support details
Requirement 2: Apply Secure Configurations to All System Components			
2.2 System components are configured and managed securely.			
2.2.2 Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.	**Yes**		SecurDPS comes with single purpose service user accounts which are disabled by default. Functionality for each account is specific to the activities required for their purpose and based on least privileges. Single purpose service user accounts enabled by SecurDPS users can be accessed using SSH public keys and/or Enterprise IAM based authentication with Kerberos combined with LDAP based group/role based access controls.
2.2.7 All non-console administrative access is encrypted using strong cryptography. **Applicability Notes** This includes administrative access via browser-based interfaces and		**Yes**	SecurDPS uses SSH v2 for non-console administrative access to its components.

PCI DSS 4.0 REQUIREMENT	SecurDPS supports this requirement	SecurDPS meets this requirement	SecurDPS support details
application programming interfaces (APIs).			
Requirement 3: Protect Stored Account Data			
3.4 Access to displays of full PAN and ability to copy account data is restricted.			
3.4.1 PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.		**Yes**	SecurDPS can be configured to protect cardholder data via tokenization, masking or hashing.
3.5 PAN is secured wherever it is stored.			
3.5.1 PAN is rendered unreadable anywhere it is stored by using any of the following approaches: • One-way hashes based on strong cryptography of the entire PAN. • Truncation (hashing cannot be used to replace the truncated segment of PAN). • Index tokens. • Strong cryptography with associated key-management processes and procedures. • Where hashed and truncated versions of the same PAN, or different truncation formats of the same PAN, are present in an environment, additional controls are in place to ensure that the different versions cannot be correlated to reconstruct the original PAN.		**Yes**	SecurDPS can be configured to protect cardholder data via tokenization, masking or hashing.
3.5.1.1 Hashes used to render PAN unreadable (per the first bullet of Requirement 3.5.1), are keyed cryptographic hashes of the entire PAN, with associated key-management processes and procedures in accordance with Requirements 3.6 and 3.7. *This requirement is considered a best practice until 31 March 2025, after which it will be required and must be*		**Yes**	SecurDPS can be configured to protect cardholder data via tokenization, encryption, masking or hashing. SecurDPS configuration data, data protection keys and secrets are securely stored on the SecurDPS Virtual Appliance, which supports the Management Console and Protection Cluster.

PCI DSS 4.0 REQUIREMENT	SecurDPS supports this requirement	SecurDPS meets this requirement	SecurDPS support details
fully considered during a PCI DSS assessment.			
3.6 Cryptographic keys used to protect stored account data are secured.			
3.6.1.2 Secret and private keys used to encrypt/decrypt stored account data are stored in one (or more) of the following forms at all times: • Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key. • Within a secure cryptographic device (SCD), such as a hardware security module (HSM) or PTS-approved point-of-interaction device. • As at least two full-length key components or key shares, in accordance with an industry-accepted method.		**Yes**	SecurDPS securely stores all data protection keys and secrets on the SecurDPS Virtual Appliance, which is similar to a Secure Cryptographic Device (SCD)/Hardware Security Module (HSM). SecurDPS can also be configured to leverage a dedicated HSM to provide an additional layer of protection.
3.6.1.3 Access to cleartext cryptographic key components is restricted to the fewest number of custodians necessary.		**Yes**	SecurDPS allows customers to create “unlock custodians” and an “unlock administrator” at the time of setup. The custodians together hold the public keys required to access the administrator account, following the principle of split knowledge and dual control.
3.6.1.4 Cryptographic keys are stored in the fewest possible locations.		**Yes**	SecurDPS securely stores all data protection keys and secrets on the SecurDPS Virtual Appliance, which is similar to a Secure Cryptographic Device (SCD)/Hardware Security Module (HSM). SecurDPS can also be configured to leverage a dedicated HSM to provide an additional layer of protection.
3.7 Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.			
3.7.1 Key-management policies and procedures are implemented to include generation of strong cryptographic keys used to protect stored account data.	**Yes**		SecurDPS generates Format Preserving Encryption keys and tokenization keys during the product initialization process. Data encryption keys generated by SecurDPS utilize AES-256-bit encryption and tokenization keys

PCI DSS 4.0 REQUIREMENT	SecurDPS supports this requirement	SecurDPS meets this requirement	SecurDPS support details
			are based on Comforte's proprietary algorithm, which is one of the reference schemes in the ANSI X9.119-2 tokenization standard.
3.7.3 Key-management policies and procedures are implemented to include secure storage of cryptographic keys used to protect stored account data.	**Yes**		SecurDPS securely stores all data protection keys and secrets on the SecurDPS Virtual Appliance, which is similar to a Secure Cryptographic Device (SCD)/Hardware Security Module (HSM). SecurDPS can also be configured to leverage a dedicated HSM to provide an additional layer of protection.
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know			
7. 2 Access to system components and data is appropriately defined and assigned.			
7.2.1 An access control model is defined and includes granting access as follows: • Appropriate access depending on the entity's business and access needs. • Access to system components and data resources that is based on users' job classification and functions. • The least privileges required (for example, user, administrator) to perform a job function.	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC). Access to sensitive data is determined and set by entities deploying the solution.
7.3 Logical access to system components and data is managed via an access control system(s).			
7.3.1 An access control system(s) is in place that restricts access based on a user's need to know and covers all system components.	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC). Access to sensitive data is determined and set by entities deploying the solution based and the users need to know.
7.3.2 The access control system(s) is configured to enforce privileges assigned to individuals, applications, and systems based on job classification and function.	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing

PCI DSS 4.0 REQUIREMENT	SecurDPS supports this requirement	SecurDPS meets this requirement	SecurDPS support details
			granular Role Based Access Controls (RBAC). Access to sensitive data is determined and set by entities deploying the solution based and the user job function(s) and classification.
7.3.3 The access control system(s) is set to “deny all” by default.	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC). Access to sensitive data is defined by the entities deploying the solution and set to “deny all” access by default.
Requirement 8: Identify Users and Authenticate Access to System Components			
8.2 User identification and related accounts for users and administrators are strictly managed throughout an account’s lifecycle.			
8.2.1 All users are assigned a unique ID before access to system components or cardholder data is allowed.	**Yes**		SecurDPS by default requires the use of unique user ID to access system components. SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC).
8.2.2 Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows: • Account use is prevented unless needed for an exceptional circumstance. • Use is limited to the time needed for the exceptional circumstance. • Business justification for use is documented. • Use is explicitly approved by management. • Individual user identity is confirmed before access to an account is granted.	**Yes**		SecurDPS comes with built in service users accounts for a designated purpose within the solution. Each service user account is locked down to only perform the specific activities required for its purpose and is only granted the minimum privileges possible for doing it.

PCI DSS 4.0 REQUIREMENT	SecurDPS supports this requirement	SecurDPS meets this requirement	SecurDPS support details
• Every action taken is attributable to an individual user.			
8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified on the documented approval.	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC). Access to sensitive data or the application can be accomplished outside of SecurDPS.
8.2.6 Inactive user accounts are removed or disabled within 90 days of inactivity.	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC). Revocation or deactivation of credentials should be implemented and enforced by the deploying entity.
8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session. **Applicability Notes** This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals). This requirement is not meant to prevent legitimate activities from being performed while the console/PC is unattended.	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC). Access to systems, including inactivity timeout thresholds should be implemented and enforced by the deploying entity.

PCI DSS 4.0 REQUIREMENT	SecurDPS supports this requirement	SecurDPS meets this requirement	SecurDPS support details
8.3 Strong authentication for users and administrators is established and managed.			
8.3.1 All user access to system components for users and administrators is authenticated via at least one of the following authentication factors: • Something you know, such as a password or passphrase. • Something you have, such as a token device or smart card. • Something you are, such as a biometric element.	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC) to enforce the use of unique usernames and passwords for all users.
8.3.2 Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.	**Yes**		SecurDPS uses SSH v2 for non-console administrative access and transmission of authentication credentials.
8.3.4 Invalid authentication attempts are limited by: • Locking out the user ID after not more than 10 attempts. • Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed. **Applicability Notes** This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC). Access to systems, including lockout thresholds should be implemented and enforced by the deploying entity.
8.3.5 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows: • Set to a unique value for first-time use and upon reset. • Forced to be changed immediately after the first use.	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC).
8.3.6 If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters). • Contain both numeric and alphabetic	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC). Access controls such as password

PCI DSS 4.0 REQUIREMENT	SecurDPS supports this requirement	SecurDPS meets this requirement	SecurDPS support details
characters. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.* Until 31 March 2025, passwords must be a minimum length of seven characters in accordance with PCI DSS v3.2.1 Requirement 8.2.3.			length should be enforced by the deploying entity.
8.3.7 Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used. **Applicability Notes** This requirement is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction (such as IDs used by cashiers on point-of-sale terminals).	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC). Access to controls, including password history should be implemented and enforced by the deploying entity.
8.3.9 If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either: • Passwords/passphrases are changed at least once every 90 days, **OR** • The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC). Access controls, including password rotations should be implemented and enforced by the deploying entity.
8.3.11 Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used: • Factors are assigned to an individual user and not shared among multiple users. • Physical and/or logical controls ensure only the intended user can use that factor to gain access.	**Yes**		SecurDPS can be integrated with Enterprise Identity and Access Management (IAM) systems for streamlined user management and implementing granular Role Based Access Controls (RBAC). Access controls, including credentials are unique to each user and not intended to be shared.
8.6 Use of application and system accounts and associated authentication factors are strictly managed.			

PCI DSS 4.0 REQUIREMENT	SecurDPS supports this requirement	SecurDPS meets this requirement	SecurDPS support details
8.6.1 If accounts used by systems or applications can be used for interactive login, they are managed as follows: • Interactive use is prevented unless needed for an exceptional circumstance. • Interactive use is limited to the time needed for the exceptional circumstance. • Business justification for interactive use is documented. • Interactive use is explicitly approved by management. • Individual user identity is confirmed before access to account is granted. • Every action taken is attributable to an individual user. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		**Yes**	SecurDPS does not utilize system or application accounts by default.
8.6.2 Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code. Note: stored passwords/ passphrases are required to be encrypted in accordance with PCI DSS Requirement 8.3.2. *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*		**Yes**	SecurDPS does not utilize system or application accounts by default.
8.6.3 Passwords/passphrases for any application and system accounts are protected against misuse as follows: • Passwords/passphrases are changed periodically (at the frequency defined in the entity's targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise.		**Yes**	SecurDPS does not utilize system of application accounts by default.

PCI DSS 4.0 REQUIREMENT	SecurDPS supports this requirement	SecurDPS meets this requirement	SecurDPS support details
• Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases. **Applicability Notes** *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*			
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data			
10.2 Audit logs are implemented to support the detection of anomalies and suspicious activity, and the forensic analysis of events.			
10.2.1 Audit logs are enabled and active for all system components and cardholder data.	**Yes**		SecurDPS can be configured to log access to cardholder data.
10.2.1.1 Audit logs capture all individual user access to cardholder data.	**Yes**		SecurDPS can be configured to log individual access to cardholder data.
10.2.1.2 Audit logs capture all actions taken by any individual with administrative access, including any interactive use of application or system accounts.	**Yes**		SecurDPS can be configured to log actions taken by users with administrative access.
10.2.1.3 Audit logs capture all access to audit logs.	**Yes**		SecurDPS can be configured to log access to audit logs.
10.2.1.4 Audit logs capture all invalid logical access attempts.	**Yes**		SecurDPS can be configured to log invalid logical access attempts.
10.2.1.5 Audit logs capture all changes to identification and authentication credentials including, but not limited to: • Creation of new accounts. • Elevation of privileges. • All changes, additions, or deletions to accounts with administrative access.	**Yes**		SecurDPS can be configured to log the creation of new accounts, escalations in privileges and changes to user accounts be users with administrative privileges.
10.2.1.6 Audit logs capture the following: • All initialization of new audit logs, and • All starting, stopping, or pausing of the existing audit logs.	**Yes**		SecurDPS can be configured to log the initialization, pausing and stopping of the audit log service.

PCI DSS 4.0 REQUIREMENT	SecurDPS supports this requirement	SecurDPS meets this requirement	SecurDPS support details
10.2.1.7 Audit logs capture all creation and deletion of system-level objects.	**Yes**		SecurDPS can be configured to log the creation and deletion of system level objects.
10.2.2 Audit logs record the following details for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure indication. • Origination of event. • Identity or name of affected data, system component, resource, or service (for example, name and protocol).	**Yes**		SecurDPS can be configured to log event details, including user identification, event type, date and time, success and failure indicators, originating point, affected data, systems, resources or services.
10.3 Audit logs are protected from destruction and unauthorized modifications.			
10.3.1 Read access to audit logs files is limited to those with a job-related need.	**Yes**		SecurDPS only permits authorized users with a job-related function to access audit log files.
10.3.2 Audit log files are protected to prevent modifications by individuals.	**Yes**		SecurDPS audit log files cannot be modified.
10.3.3 Audit log files, including those for external-facing technologies, are promptly backed up to a secure, central, internal log server(s) or other media that is difficult to modify.	**Yes**		SecurDPS can send logs to dedicated logging servers via <connection>. SecurDPS can also be integrated with enterprise logging solutions/Security Incident and Event Management (SIEM) tools.
10.3.4 File integrity monitoring or change-detection mechanisms is used on audit logs to ensure that existing log data cannot be changed without generating alerts.	**Yes**		SecurDPS only permits authorized users with a job-related function to access audit log files. SecurDPS audit log files cannot be modified.
10.5 Audit log history is retained and available for analysis.			
10.5.1 Retain audit log history for at least 12 months, with at least the most recent three months immediately available for analysis.	**Yes**		SecurDPS can send logs to dedicated logging servers via rsyslog, or be integrated with enterprise logging solutions/Security Incident and Event Management (SIEM) tools to meet audit log file retention requirements.

Requirement 12: Support information security with organizational policies and programs			
12.3 Targeted risks to the cardholder data environment are formally identified, evaluated, and managed.			
12.3.1 Each PCI DSS requirement that provides flexibility for how frequently it is performed (for example, requirements to be performed periodically) is supported by a targeted risk analysis that is documented and includes: • Identification of the assets being protected. • Identification of the threat(s) that the requirement is protecting against. • Identification of factors that contribute to the likelihood and/or impact of a threat being realized. • Resulting analysis that determines, and includes justification for, how frequently the requirement must be performed to minimize the likelihood of the threat being realized. • Review of each targeted risk analysis at least once every 12 months to determine whether the results are still valid or if an updated risk analysis is needed. • Performance of updated risk analyses when needed, as determined by the annual review. Applicability Notes *This requirement is a best practice until 31 March 2025, after which it will be required and must be fully considered during a PCI DSS assessment.*	**Yes**		SecurDPS can assist in the process of identifying assets in which sensitive data, such as cardholder data, are subject to periodic targeted risk analysis activities.
12.5 PCI DSS scope is documented and validated.			
12.5.2 PCI DSS scope is documented and confirmed by the entity at least once every 12 months and upon significant change to the in-scope environment.	**Yes**		SecurDPS can assist in the required annual scoping process by identifying both known and unknown instances of cardholder data within an entity environment.
12.10.7 Incident response procedures are in place, to be initiated upon the detection of stored PAN anywhere it is not expected, and include: • Determining what to do if PAN is discovered outside the CDE, including its retrieval, secure deletion, and/or migration into the currently defined CDE, as applicable.	**Yes**		SecurDPS offers monitoring and alerting capabilities for known and newly identified instances of cardholder data within an entity environment. Additionally, integration with enterprise logging/SIEM solutions offers entities a greater level of visibility into their environment.

• Identifying whether sensitive authentication data is stored with PAN. • Determining where the account data came from and how it ended up where it was not expected. • Remediating data leaks or process gaps that resulted in the account data being where it was not expected.			

CONCLUSION

Data protection capabilities provided by SecurDPS, including tokenization, masking and/or hashing can support entities in fulfilling their data security obligations identified PCI DSS v4.0 when implemented in a manner consistent with Comforte's implementation guidance. Additionally, the Discovery & Classification component of SecurDPS can support entities in the scope validation processes defined in PCI DSS v4.0 by identifying both known and unknown data stores and/or instances of sensitive data such as cardholder data when configured in accordance with Comforte's guidance and recommendations.

REFERENCES

- SDPS-DC_3-5_Analytic_Engine_and_Console_Management_Administrator_Guide.pdf
- SDPS-DC_3-5_Data_Asset_Management_User_Guide.pdf
- SDPS-DC_3-5_Data_Recognition_Accuracy_User_Guide.pdf
- SDPS-DC_3-5_Data_Security_Dashboards_for_DC_GDP.pdf
- SDPS-DC_3-5_Data_Source_Catalog_User_Guide.pdf
- SDPS-DC_3-5_Data_Subject_Search_User_Gude.pdf
- SDPS-DC_3-5_Discovery_Classification_Search_User_Guide.pdf
- SecurDPS_Enterprise_Audit_Console (2).pdf
- SecurDPS_Enterprise_Protection_Cluster (3).pdf
- SecurDPS_Enterprise_REST_API (3).pdf

Legal disclaimer

this white paper has been taken from sources that Coalfire believes to be reliable, but its accuracy, completeness, or interpretation cannot be guaranteed. Information is current as of the date of this white paper only and is subject to change without notice. This white paper is provided “as-is” with no warranties, including any warranty of merchantability, fitness for a particular purpose, and non-infringement. Coalfire expressly disclaims all liability arising from or relating to the use of any information or material included in this white paper for any purpose, including any actions taken or not taken based on the contents of this white paper. You are solely responsible for making your own independent assessment of the information in this white paper and for the development, implementation, and execution of your information security program. For questions regarding any legal or compliance matters referenced in this white paper, you should consult your legal counsel, security advisor, or the relevant standard authority.

About the Author

Vikram Dhabaldeb, Senior Consultant

Vikram is a payments security consultant on the Industry Solutions team at Coalfire. Vikram has seven years of experience as a PCI Qualified Security Assessor (QSA), supporting merchants and service providers with their PCI DSS compliance programs. Along with his PCI QSA certification, he holds a PCI Secure Software Lifecycle (SSLC) assessor certification, supporting software vendors in validating their software development processes. In addition to his PCI Security Standards Council issued certification, Vikram holds a Certified Information Systems Auditor (CISA) certification issued by ISACA, and a Certified Information Systems Security Professional (CISSP) certification issued by ISC2.

About the Reviewer

Bhavna Sondhi | *Director, Technical Solutions*

Bhavna Sondhi is the Director of Industry Solution Validation team at Coalfire managing PCI SSF, PCI 3DS, PCI PIN, PCI P2PE frameworks. Bhavna joined Coalfire in 2013 and brings over 14 years of software engineering and information security experience to the team. Her software engineering experience plays a vital part in ensuring that teams recognize the importance of secure code development and information security within their operational practices. Bhavna has performed advisory work and assessments for various payment card industry compliance frameworks and authored technical white papers.

WP_Comforte SecurDPS Whitepaper April 17, 2024