Privacy Data Sheet

We bring security to life.

Trellix Database Security (DBSec)

The purpose of this Privacy Data Sheet is to provide Customers of Database Security (DBSec) with details on how Trellix captures, processes, and stores[1] telemetry information, including personal data (or personally identifiable information), to help them understand and assess the impact of the telemetry capabilities on their overall privacy posture.

Trellix DBSec is a solution which protects servers, computer systems and networks against known and unknown threats like malware, suspicious communications, unsafe websites and files made available by Trellix to companies or persons who obtain a Trellix DBSec subscription.

Trellix will process personal data from DBSec in a manner that is consistent with this Privacy Data Sheet. In jurisdictions that distinguish between Data Controllers and Data Processors, Trellix is the Data Controller for the personal data processed to administer and manage the Customer relationship. Trellix is the Data Processor for the personal data processed by to provide its functionality.

Note: This Privacy Data Sheet is a supplement to the Trellix Website Privacy Notice.

Product Overview

Trellix Database Security is an easy-to-deploy and highly scalable software solution that monitors Customer Database Management Systems (DBMS) and protects it from internal and external threats, including intra database exploits and is ideal for servers operating within a Customer's on premise network infrastructure.

The DBSec solution delivers automated features for activities that Sec Ops teams previously managed manually. Trellix DBSec also provides discovery scanning of supported databases where the sensitive data they contain can be identified. In addition, Customers can apply access rights management to databases to ensure that only authorized employees have access to the information they contain.

[1] In this document, we adopt the broad definition of "processing" that appears at Article 4(2) of the GDPR: "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means …", which includes, but is not limited to the following non-exhaustive series of examples: "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction."

DBSec assists Customers to achieve regulatory compliance by blocking unauthorized access to sensitive data and by monitoring and responding to data events. Trellix DBSec enhances Trellix Customers' security posture by identifying known and unknown vulnerabilities, automating patching, and reinforcing security when patches are not available.

Trellix DBSec finds, classifies, and defends sensitive information in leading database types, keeping your databases secure, patched, and protected even when patches are not an option. With Trellix DBSec, Trellix Customers can easily conduct regular checks for issues with configuration and coding, as well as find performance problems. Trellix DBSec ensures your databases are up-to-date for specifically sensitive information.

Database Security provides full visibility into DBMS user activity and can issue alerts or terminate suspicious activities based on predefined vPatch rules and custom rules.

In line with a layered defense strategy employed by leading enterprises, Database Security complements other security measures offered by Trellix, such as encryption, network security, and other products, by providing a hardened security layer surrounding the DBMS itself.

Key advantages of Database Security include:

- Monitoring of all DBMS activities, including the activities of authorized and privileged users;
- Prevention of intrusion, data theft, and other attacks on the DBMS;
- Real SQL Injection Protection;
- Rule-based policies for users, queries, and DBMS objects;
- Quarantine rogue users;
- Enterprise level vulnerability assessment for DBMSs;
- Quick and easy deployment and configuration options.

Trellix DBSec integrates with supported databases including: Oracle, Microsoft SQL Server, MySQL, PostgreSQL, MariaDB, Sybase, DB2, SAP HANA, Percona, Teradata. Supported operating systems include: Windows, Linux, Solaris, AIX, and HPUX**.**

Trellix Database Security management console includes the following security features:

- **Database Activity Monitoring** — Protects data from all threats by monitoring local activity on each database server and by alerting or terminating malicious behavior in real time. **With Database Activity Monitoring, Customers can:**
  - Quickly build custom security policies to meet industry regulations or internal IT governance standards;
  - Log access to sensitive data for audit purposes, including complete transaction details;
  - Terminate sessions violating policies and quarantine suspicious users, preventing data from being compromised;
  - Maintain separation of duties as required by many regulations.
- **Vulnerability Manager for Databases** — Automatically discovers databases on the Customer network and determines if the latest patches have been applied to tests for vulnerabilities, such as weak passwords, default accounts, and other common threats. In addition, it allows for detailed data discovery scans, including Personally Identifiable Information (PII), Payment Card Industry Data Security Standard (PCI-DSS), Sarbanes-Oxley (SOX), and Health Insurance

Portability and Accountability Act (HIPPA). **With Vulnerability Manager for Databases, Customers can:**

  - Classify threats into distinct priority levels and provide fix scripts based upon recommendations from database security experts;
  - Improve visibility into database vulnerabilities— and provide expert recommendations for remediation, reducing the likelihood of a gravely damaging breach which saves money through better reparation for regulatory compliance audits;
  - Evaluate risk from virtually every threat vector by conducting more than 7800 vulnerability checks against leading database systems such as Oracle, Microsoft SQL Server, IBM DB2, and MySQL databases.

- **Virtual Patching** — Detects missing patches, applies vulnerability-specific countermeasures and fixes misconfigurations (via Database Security virtual patching technology) found by vulnerability scans to improve the security posture of databases immediately, without requiring any downtime.

The Trellix Database Security management console provides SecOps team with the following:

- **Alerts** — Lists the data activity monitoring alerts generated by the Trellix Database Security Server (Sensors).
- **Vulnerability Assessment (VA) Results** — Lists the results of Trellix Database Security Vulnerability Assessment scans.
- **Dashboard** — Displays a range of statistical data regarding the status of alerts, DBMS monitoring, security updates, and rules. For details, see Trellix Database Security Dashboard.
- **Rules** — Lists existing predefined (Vpatch) and custom rules and enables you to create rules and manage the rules that are enabled and applied on each DBMS.
- **VA Scans** — Enables the configuration of VA scans of the databases to identify a wide range of risks and problems. For details, see VA scans. VA Tests — Enables the configuration of customized VA tests.
- **Compliance** — Enables the configuration of Compliance rules based on established international standards and regulations.
- **Sensors** — Lists the installed Trellix Database Security Sensors and their approval status.
- **DBMSs** — Lists the DBMSs where Trellix Database Security Sensors have been installed, and databases that are available for security scans, and enables you to view the properties of each DBMS.
- **Permissions** — Lists the defined roles and authorized users in the system and enables you to add new roles/users and manage the permissions that apply to each role or user.
- **System** — Lists the history of actions performed by users in the graphical user interface and enables various system-wide configurations. Updates — Enables the configuration and execution of automatic and manual security and software updates.
- **Reports** — Provides detailed reporting for alerts, test results, and system history.

Trellix DBSec is offered as:

- **Standalone deployment:** In standalone deployments the DBSec solution reads data stored on the Customer’s enterprise endpoint system and no data is ever captured by Trellix.

Please see Trellix Database Security Security product sheet for additional information.

Personal Data Processing

Trellix Database Security is an on-premises solution for scanning Customers DB's for vulnerabilities whether they be known Common Vulnerabilities and Exposures (CVEs), insecure Database schemas, or user information. Customers create custom rules executed within their database environment, aimed at enforcing security and compliance.

The Trellix DBSec Sensor captures and transmits relevant information to a user-defined server for storage within the Customer's configurable database, facilitating comprehensive analysis of database activity and adherence to security protocols. The sensor is enabled in offline and online modes, and keeps all details cached locally until it connects to the management server. The local cache is encrypted where the location is configurable by the Customer. Trellix Database Security scans databases and presents and stores the results in the Customers Database Management Console.

As a result, Trellix DBSec may process a range of data potentially containing personal information. The table below shows the personal data processed by DBSec to provide its services and describes why the data is processed.

Table 1. Data Processed by Trellix Database Security

Personal Data Category*	Types of Personal Data Processed	Purpose of Processing
Administrative Data	Not applicable: no administrative data is captured or stored by Trellix.	Not Applicable.
Generated Data	Alerts: The alerts generated on DBSec sensor hits may have following personal data: ● Host Name	Used for database activity monitoring and troubleshooting purposes.

	- Host Machine - IP Address - Host Machine MAC Address - DB Instance Name - End User IP Address - Log On Time	
Collected Data	Configuration Information: - Custom vPatch Rules - Custom VA Test - System Configuration (e.g., SMTP, LDAP, Syslog, SNMP)	Used for vPatch Rules for activity monitoring and VA Test for vulnerability scanning.

Please note the Personal Data Categories explained below and used throughout Privacy Data Sheets for Trellix products and/or services:

Administrative Data: Information to enable the service and/or manage the Customer relationship.

Generated Data: Information generated by the product (events, evidence, logs).

Collected Data: Information generated by the Customer (policies and configurations).

Data Center Locations

For standalone implementation, the data center is located within the Customer's environment and no data is stored by Trellix.

Subprocessors

Trellix partners with service providers that act as subprocessors for the DBSec service and contracts to provide the same level of data protection and information security that you can expect from Trellix. A current list of subprocessors for the service is below:

Table 3. Subprocessors

Subprocessor	Personal Data Category	Service Type	Location of Data Center
Not Applicable	**Not Applicable**	**Not Applicable**	**Not Applicable**

Cross-Border Data Transfer

In the event of a need to share personal information with Trellix personnel in regions outside of those identified in the Data Center Locations section above, we will do so in compliance with applicable requirements for transfer of personal data, including those of the EU Standard Contractual Clauses as approved by the European Commission and/or other legal instruments recognized by EU data protection laws. For a more detailed assessment of our international data transfers, please refer to the Trellix Transfer Impact Assessment statement.

Access Control

Access to Customer information is subject to Trellix's Access Management Policy. Access is protected by multiple authentication and authorization mechanisms. Trellix has an account administration application that provides a central access point to request and perform administrative functions for account requests across multiple platforms. All resources have an owner who is responsible for deciding who will be granted access to that resource. Privileged access to resources is restricted to authorized users with a business need, consistent with the concepts of least privilege and segregation of duties based on roles and job functions. Shared accounts are prohibited. All usernames are traceable to a specific human user. User access credentials are promptly removed when user access is no longer authorized (e.g., Trellix employment terminates).

Remote user access by Trellix personnel is performed through a secure virtual private network (VPN) connection that requires multi-factor authentication (MFA). If remote access to production resources is required outside the VPN, then a TLS encrypted connection and MFA is required.

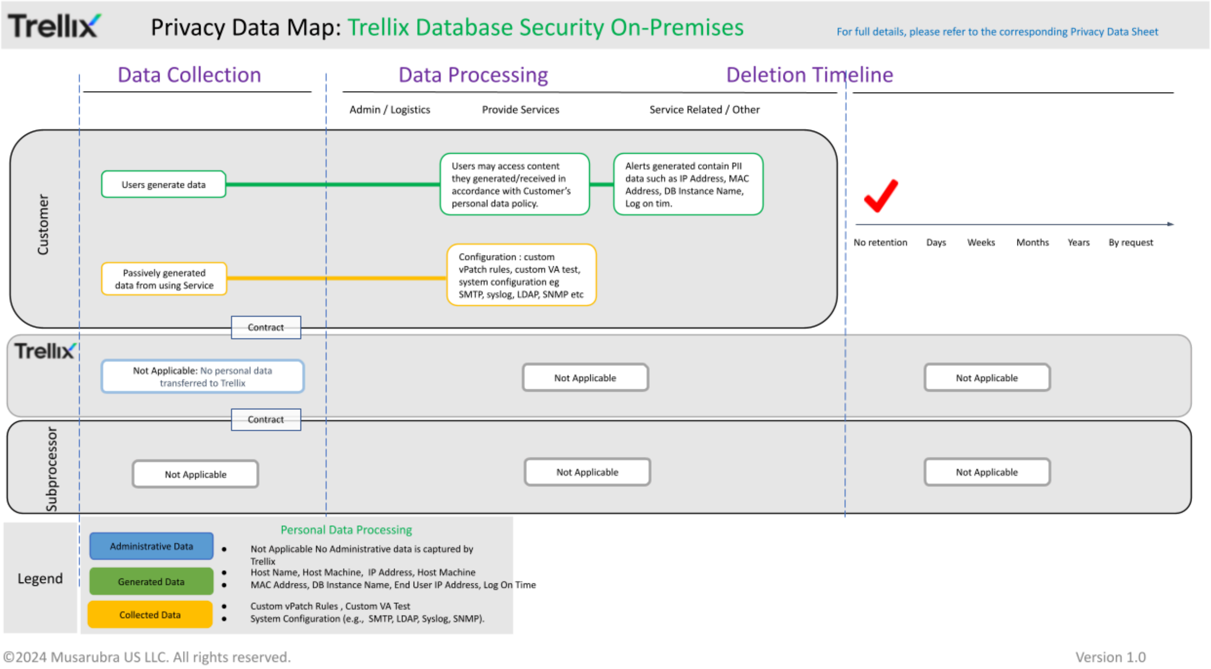
The table below lists the personal data used by Database Security to carry out the service, who can access that data, and why.

Table 4. Access Control

Personal Data Category	Who has access	Purpose of the access
Administrative Data	**Customer:** Not Applicable.	Not Applicable.
	Trellix: Not Applicable.	Not Applicable.
Generated Data: Alerts / Scan Results	**Customer:** Access is controlled by the Customer and no data is captured by Trellix.	To monitor databases for suspicious activity and scanning databases for vulnerability.
	Trellix: Not Applicable.	Not Applicable.
Collected Data: Configuration/Rules/Tests	**Customer:** Access is controlled by the Customer and no data is captured by Trellix.	To monitor databases for suspicious activity and scanning databases for vulnerability.
	Trellix: Not Applicable.	Not Applicable.

Database Security Data Flow Diagram

The key data flows associated with the information processing activities described in this document are shown below.



Trellix Privacy Data Map: Trellix Database Security On-Premises

For full details, please refer to the corresponding Privacy Data Sheet

Data Collection

Data Processing

Deletion Timeline

Admin / Logistics

Provide Services

Service Related / Other

Customer

Users generate data

Users may access content they generated/received in accordance with Customer's personal data policy.

Alerts generated contain PII data such as IP Address, MAC Address, DB Instance Name, Log on tim.

Passively generated data from using Service

Configuration : custom vPatch rules, custom VA test, system configuration eg SMTP, syslog, LDAP, SNMP etc

✓

No retention

Days

Weeks

Months

Years

By request

Contract

Trellix

Not Applicable: No personal data transferred to Trellix

Not Applicable

Not Applicable

Contract

Subprocessor

Not Applicable

Not Applicable

Not Applicable

Legend

Personal Data Processing

Administrative Data	• Not Applicable No Administrative data is captured by Trellix
Generated Data	• Host Name, Host Machine, IP Address, Host Machine • MAC Address, DB Instance Name, End User IP Address, Log On Time
Collected Data	• Custom vPatch Rules , Custom VA Test • System Configuration (e.g., SMTP, LDAP, Syslog, SNMP).

©2024 Musarubra US LLC. All rights reserved.

Version 1.0

Customer Privacy Options

Trellix designs its products to support our Customers' compliance with global data protection and compliance obligations. It does this by addressing threat intelligence and security challenges at the application, network, and endpoint levels, and in the cloud. In addition, Trellix offers product features that help our Customers meet their EU GDPR and other legal compliance goals. Such features include, but are not limited to data localization options, policy enforcement, access controls, logging capabilities, individual rights processing, and cross-border data transfer mechanisms.

Customers control whether the Database security service is enabled or disabled. When it is disabled, no data processed by the service is collected and sent to the Cloud and no data is downloaded by the service from the cloud data centers.

Data Portability

Except with respect to Registration Information, the Customer can forward the personal data processed by DBSec to a third-party data store. If applicable, to effectuate data portability, Customers may request assistance from Trellix Engineering for a large-scale movement of data (e.g., Customer does not renew subscription and asks for all data to be transferred to a third-party data store).

Data Deletion and Retention

The table below lists the personal data used by DBSec, the length of time that data needs to be retained and why we retain it.

A data subject may request deletion of his or her Personal Data by sending a data subject request as described below in this Privacy Data Sheet.

A Customer may request data deletion by submitting a ticket to Trellix support at support_reply@trellix.com. When a Customer makes a request for deletion, Trellix will purge the requested data from its systems to the extent required by applicable law and may retain administrative data required for legitimate business purposes (e.g., billing records).

Table 5. Data Retention

Personal Data Category	Retention Period	Reason for Retention
Administrative Data	Not Applicable.	Not Applicable.
Generated Data	Entirely configurable by the Customer.	Not Applicable.
Collected Data	Entirely configurable by the Customer.	Not Applicable.

*Customers apply their own retention period based on Customer configuration. No data is retained by Trellix.

Personal Data Security

Files stored on or processed by Trellix's systems are secured with state-of-the-art technologies, and Trellix implements rigorous technical and organizational security controls designed to secure personal data from accidental loss and unauthorized access, use, alteration, and disclosure.

Table 6. Personal Data Security

Personal Data Category	Type of Personal Data	Security Controls and Measures
Administrative Data	See Table 1.	No encryption provided by Trellix.
Generated Data	See Table 1.	No encryption provided by Trellix.
Collected Data	See Table 1.	No encryption provided by Trellix.

*Additional details for product certifications are available upon request. Note that Trellix does not provide encryption for this solution. Customers will need to integrate an independent encryption mechanism.

Compliance with Privacy Requirements

Trellix is committed to protecting personal data processed in the global and regional DBSec clouds. We will not access the content of files in a way in which we could learn meaningful information about natural persons, other than in exceptional cases where it is necessary for identifying security threats.

The Privacy Office and Trellix Legal provide risk and compliance management and consultation services to help drive security and regulatory compliance into the design of Trellix products and services. The Service is built with privacy in mind and is designed so that it can be used in a manner consistent with global privacy requirements.

Further, in addition to complying with our stringent internal standards, Trellix also maintains third-party validations to demonstrate our commitment to information security.

Exercising Data Subject Rights

Users whose personal data is processed by the Service have the right to request access, rectification, suspension of processing, or deletion of the personal data processed by the Service.

We will confirm identification (typically with the email address associated with a Trellix account) before responding to the request. If we cannot comply with the request, we will provide an explanation. Please note, users whose employer is the Customer/Controller may be redirected to their employer for a response.

Requests can be made by submitting a request via:

1) the Trellix Individual Data Request Form

2) by postal mail:

In the U.S. by registered mail:
Musarubra US LLC
Attn: Legal Department –Privacy
6000 Headquarters Drive, Suite 600

Plano, Texas, 75024

or call us at +1 (214) 494-9190

In the European Economic Area by registered post:
Musarubra Ireland Limited
Attn: Legal Department –Privacy
Building 2000, City Gate

Mahon, Cork, Ireland

or call us at +353 21 467 2000

In Japan by registered mail:
Musarubra Japan KK
Attn: Legal Department –Privacy
Shibuya Mark City West

1-12-1 Dogenzaka, Chibuyaku, Tokyo 150-0043

About This Data Sheet

Trellix Privacy Data Sheets are reviewed and updated on an annual, or as needed, basis.

Please note that the information provided with this document concerning technical or professional subject matter is for general awareness only, may be subject to change, and does not constitute legal or professional advice, warranty of fitness for a particular purpose, or compliance with applicable laws.