

Data Loss Prevention – On-Premise

This Notice describes how the above designated Product processes Personal Data. It provides the information relevant to assess and document privacy relevant aspects of the use of this Product. This Notice and the relevant terms of the [Broadcom Privacy Policy](#) are the authoritative statements relating to the Personal Data processing activities and privacy regulatory compliance aspects associated with the use of this Product.

About this Notice

Product version(s) covered by this Notice:	v16 and earlier
Last revision of this Notice:	September 21, 2022

Prior versions of this Notice as applicable to earlier releases of the Product may be available in the Archives. Where this Notice references other Products marked with an asterisk (*), please refer to the separate Notices of such Products.

About the Product

For information on the purpose, features and technical characteristics of the Product, please refer to the documentation at <https://www.broadcom.com/products/cyber-security/information-protection/data-loss-prevention>.

Product type:	<input type="checkbox"/> Hardware	<input checked="" type="checkbox"/> Software	<input type="checkbox"/> Service	<input type="checkbox"/> Other
Deployment model(s):	<input checked="" type="checkbox"/> On-premise	<input type="checkbox"/> Cloud-based	<input type="checkbox"/> Hybrid	<input type="checkbox"/> Other

About the Processing Operation(s) performed by / for the purpose(s) of the Product

This Product:	<input checked="" type="checkbox"/> Must process Personal Data to deliver its core feature(s)	<input type="checkbox"/> Does not require processing any Personal Data to deliver its core feature(s)
This Product:	<input checked="" type="checkbox"/> Has optional features that may process Personal Data	<input type="checkbox"/> Such optional features are active by default <input checked="" type="checkbox"/> Such optional features are inactive by default
This Product processes:	<input checked="" type="checkbox"/> Non-sensitive Personal Data	<input checked="" type="checkbox"/> Sensitive Personal Data <input type="checkbox"/> Not applicable
The Product involves:	<input type="checkbox"/> Profiling of individuals based on personal characteristics	<input checked="" type="checkbox"/> Automated decision making that produces legal or other significant impacts on individuals

The Product is designed to protect confidential information. Such confidential information typically includes Personal Data, and especially sensitive Personal Data. In order to be able to protect such Personal Data, it is essential for the Product to detect, identify and index it, which is why using the Product will involve processing the data to be protected.

The Product has capabilities to enforce automatic decisions based on Customer-defined policies, such as preventively blocking outbound network traffic containing confidential information. Such automated decisions solely serve to enforce the information protection policies defined by the Customer. For the unlikely event of such decisions producing legal or other significant impacts on individuals, the Product enables the Customer to manually override automatic decisions.

The Product includes pre-defined policy templates designed to help Customers configure the Product in consideration of typical compliance objectives under major privacy laws and regulations such as the EU GDPR. Such templates should not be considered as authoritative legal guidance or interpretation. Customers should seek qualified legal advice tailored to their specific requirements when deploying, configuring and using the Product in their environment.

About the Personal Data processed by / for the purpose(s) of the Product

Categories of Personal Data	Categories of Data Subjects	Purpose(s) of Processing	Categories of Data Recipients	Needed for core features (Yes/No)	Processing location(s)	CA Inc. acts as Processor (Yes/No)
Identifiers and contact details in the Customer's Active Directory; online identifiers and trackers; network activity data; electronic	Customers' end-users	Detection, logging and reporting of confidential information mishandling, and of other violations of Customer-defined data	Customer admins	Yes	Customer premises	No

communications data		protection policies				
Personal Data as configured in Customer-defined policies	Customer's end-users	Protection of confidential information from exposure	Customer's authorized personnel	Yes	Customer premises	No

About managing the Personal Data processed by / for the purpose(s) of the Product

Privacy Enhancing Technologies

Subject to more detailed information provided in the Product description and other customer literature e.g. on optional Product settings and configurations available, the Product has the following technical and organizational capabilities to enhance and protect the privacy of the Personal Data it processes:

Privacy Objective	Privacy Enhancing Technologies / Measures	Data at rest	Data in transit ^a
Data confidentiality	Access control measures Encryption	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/>
Data integrity	Anti-tampering technology Change logging	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
Data availability	Business continuity measures (e.g. failover) Disaster recovery measures (e.g. backups)	<input type="checkbox"/> <input type="checkbox"/>	NA NA
Data incident	Detection and flagging of incidents Response mechanisms to incidents	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
Current certification(s):	FIPS 140-2: Secure Software Development Life Cycle		

^aData in transit encompasses traffic between client systems and SaaS endpoints.

Data Subject Rights

The Customer has full control and sole responsibility for servicing Data Subject Rights applicable to Personal Data collected through the use of the Product and processed on Customer premises.

Personal Data Retention Schedule

The Customer has full control and sole responsibility for defining and enforcing retention policies for the Personal Data collected through the use of the Product and processed on Customer premises.

About Regulatory Compliance Matters

Data Processing Addendum

Where your use of the Product or of related services involves CA Inc., its parent and/or affiliates acting as a Data Processor on your behalf, the rights and obligations of both parties with respect to such Personal Data processing, including as regards disclosures and cross-border transfers of Personal Data to and/or by CA Inc., its parents and/or affiliates and any of their sub-processors, are defined in the applicable Data Processing Addendum available at <https://www.broadcom.com/company/legal/ca/data-transfers>.

CCPA Compliance

If you are subject to the California Consumer Privacy Act and require CA Inc., its parent and/or affiliates to enter into CCPA-based service provider terms with you, please use our CCPA Customer Agreement Supplement available at <https://www.broadcom.com/company/legal/ca/data-transfers>.

Sub-Processing

Not applicable