cloudaware

Cloudaware Data Privacy Statement

Cloudaware provides SaaS (Software as a Service) CMDB to [COMPANY NAME]. CMDB gathers Microsoft Azure infrastructure metadata that [COMPANY NAME] leverages. Cloudaware has recommended security policies for accessing resources in Azure. These cloud access policies are specifically designed to provide Cloudaware with access to describe [COMPANY NAME] cloud infrastructure without giving access to the business data.

Cloudaware operates as a container application inside Salesforce's app engine and is subject to all Salesforce security controls. The Cloudaware role is limited to updating, deleting and inserting new data into CMDB. There are no algorithms, automated batch export jobs that export [COMPANY NAME] data outside of the Salesforce instance where Cloudaware is hosted. In addition, the Cloudaware internal security policy explicitly forbids exporting customer data outside of the customer’s Salesforce instance.

In order to provide our customers with hands-on support, technical account managers associated with [COMPANY NAME] account have access to [COMPANY NAME]'s Cloudaware instance.

Cloudaware processes and stores [COMPANY NAME] data on Salesforce's app engine infrastructure. Many of Salesforce's SOC2 controls regarding data backup, DR, BCP, access control and auditing apply directly to Cloudaware. More information about compliance certifications are available here: https://compliance.salesforce.com/en

Salesforce performs its own security and audit process to vet vendors whose applications are offered via Salesforce's app store. More details about this process are available here: https://developer.salesforce.com/docs/atlas.en-us.packagingGuide.meta/packagingGuide/security_review_overview.htm

Additional helpful documentation: https://developer.salesforce.com/docs/atlas.en-us.securityImplGuide.meta/securityImplGuide/salesforce_security_guide.html