Schedule A

Data Processing Profile

Radware's Cloud Native Protector Service

This Data Processing Profile is supplemental to a Global Data Processing Agreement ("**DPA**") between Radware Ltd./Inc. ("**Radware**" or "**Processor**") and the entity that has executed or accepted the DPA ("**Customer**" or "**Customer**"). This Data Processing Profile describes the processing of personal data (or personal identifiable information) by Radware in connection with Radware's **Cloud Native Protector Service** (the "**Service**"). Capitalized terms used in this Data Processing Profile but not defined herein shall have the meanings ascribed to them in the DPA.

Service Overview

Radware's Cloud Native Protector Service detects excessive permissions in cloud workloads, hardens security configurations and detects data theft using advanced machine-learning algorithms.

It is an agentless, cloud-native solution for comprehensive protection of AWS and Azure assets, to protect both the overall security posture of cloud environments, as well as protect individual cloud workloads against cloud-native attack vectors.

The Cloud Native Protector Service provides centralized visibility and control over large numbers of cloud-hosted workloads and helps security administrators quickly understand where the attack is taking place and what assets are under threat.

Data Privacy Profile

The Service does not store any information that can directly identify a natural person.

Data Privacy Topic	Description
Description of Data Processing	1) The Customer provides the Radware with METADATA and logs including configuration data, CloudTrail/Activity logs and network flow logs. Radware is given read only permissions to the Customer's cloud accounts. These permissions allow Radware to download CloudTrail/Activity Logs/Flow Logs from the locations in which they are stored. It also triggers specific Cloud API calls, which return the cloud account configuration and the Customer's cloud compute inventory. 2) Behavioral and attack surface analysis designed to detect excessive permissions.

	3) Machine learning algorithms are designed and applied to detect abnormal user/entity behavior, malicious communication, anomalous access to data and more suspicious activities. 4) Configuration scanning to detect publicly exposed assets and cloud misconfigurations. 5) Storage and management of Customer supplied information logs, findings and alerts controlled by the Service are stored and encrypted under the AWS Cloud platform.
Purpose of the Processing	Processing is performed to protect the assets of the Customer that are covered by the Service (the "Protected Assets") from cyber-threats leveraging vulnerabilities caused by misconfiguration, excessive or unnecessary privileges, unintentionally publicly exposed assets and malicious activity; all pursuant to and for the limited purpose of performing Radware's obligations set out in the Principal Agreement.
Categories of Data	Data processed is limited to configuration data, external IP addresses of the Customer and network metadata. Organizational user IDs may be included in the logs supplied by the Customer.
Data Subjects	The Customer's internal cloud and/or infrastructure/application administrators and users.
Duration of the Processing	The duration of the processing is determined by the Principal Agreement (as defined in the DPA) or until the deletion of all of Customer's Personal Data in accordance with the DPA and the "Data Retention and Deletion" details set forth below.
Data Retention and Deletion	The retention period for logs is determined by the Customer. The default is 6 months unless an extended period of time is requested by the Customer. Findings are retained until they are deleted by the Customer. When no longer required by the Customer or after a certain period determined by the Customer following Service termination, this information is cryptographically deleted.

Processing Locations

Approved Sub-Processor/Affiliate (Company Name)	Company address	Approved scope of work	Approved Service Locations	Service Location address
Amazon Web Services	USA	Hosting for CNP Processing and Portal	us-east-1, cn-northwest-1	USA, north-Virginia China, Ningxia

Industry Standard Certificates

Radware's Cloud Native Protector Service complies with the following standards for cybersecurity and privacy:

- *ISO 27001 Information Security Management Systems*
- *ISO 27032 Security Techniques -- Guidelines for Cybersecurity*
- *ISO 27017 Information Security for Cloud Services*
- *ISO 27018 Information Security Protection of Personally identifiable information (PII) in public clouds*
- *HIPAA Health Insurance Portability and Accountability Act*

Compliance with these standards is audited annually by third party auditors.

Customer may find Radware's latest cybersecurity and privacy certifications and attestations in https://www.radware.com/newsroom/certificationsindustry/.

An annual SOC2 type II report is being prepared for Radware's Cloud Services.