Comprehensive Protection for the Public Cloud

Promiscuous permissions are the #1 threat to computing workloads hosted on the public cloud. Public cloud environments make it very easy to grant extensive permissions and very difficult to keep track of them. As a result, cloud workloads are vulnerable to data breaches, account compromise and resource exploitation. Radware provides an agentless, cloud-native solution for comprehensive protection of AWS assets to protect the overall security posture of cloud environments as well as the individual cloud workloads against cloud-native attack vectors. Cloud Workload Protection Service detects promiscuous permissions to your workloads, hardens security configurations before data exposure occurs and detects data theft using advanced machine learning algorithms.

REDUCE CLOUD EXPOSURE

Radware helps organizations reduce their attack surface by detecting promiscuous permissions and providing smart hardening recommendations

DETECT DATA THEFT ACTIVITY

Radware uses advanced machine learning algorithms to identify anomalous activity within your cloud account and alert against data theft activity

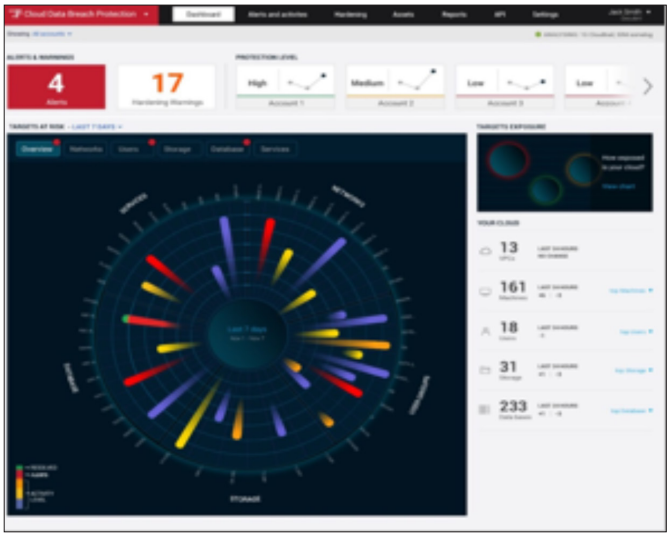
COMPREHENSIVE PROTECTION

Cloud Workload Protection Service protects the overall security posture of the cloud environment as well as the individual workloads running inside them

CLOUD-NATIVE SOLUTION

Cloud Workload Protection Service is an agentless cloud-native solution, providing low-touch, unobtrusive and easy deployment

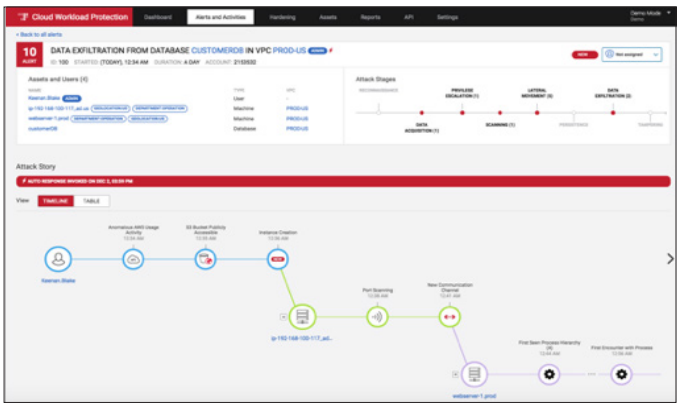
How Radware Keeps Your Workloads and Data Secure



Key Benefits of Radware's Solution:

- Detect publicly exposed assets
- Identify excessive and unused permissions
- Harden security configurations
- Uncover data theft attempts
- Automate cloud security function
- Meet compliance requirements

Secure Your Workloads With Cloud Workload Protection Service



Orchestrated Attack Storylines

Radware correlates individual events using advanced machine learning algorithms and places them in contextual attack storylines to detect potential data theft attempts and block them as they evolve.

Centralized Security Management

Radware provides centralized visibility and control over large numbers of cloud-hosted workloads and helps administrators understand where the attack is taking place and what assets are under threat.

Context-Aware Smart Hardening

Radware detects excessive permissions by analyzing the gap between granted and used permissions and provides smart hardening recommendations to fortify security posture and reduce attack surfaces.

Automated Response Mechanisms

Radware provides built-in measures to automatically remediate suspicious behavior when it is detected, so you don't lose time once a breach is detected.

Agentless, Nonintrusive Deployment