Comprehensive Protection for the Public Cloud

Transitioning to the cloud means losing visibility and control over computing assets. Cloud-hosted workloads are managed remotely, making it difficult for security teams to supervise access to sensitive cloud resources. As a result, many organizations are unable to prevent cloud misconfigurations, identify cyberattacks as they are happening and respond in time.

Radware provides an agentless, cloud-native solution for the comprehensive protection of Amazon Web Services (AWS) environments against cloud threats and attacks. Radware's Cloud Workload Protection Service fortifies an organization's security posture by detecting and eliminating excessive permissions to workloads, detects malicious activity in a cloud environment, correlates individual events into orchestrated attack storylines and provides automated response mechanisms to block attacks as soon as they are detected.

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

AUTOMATIC RESPONSE

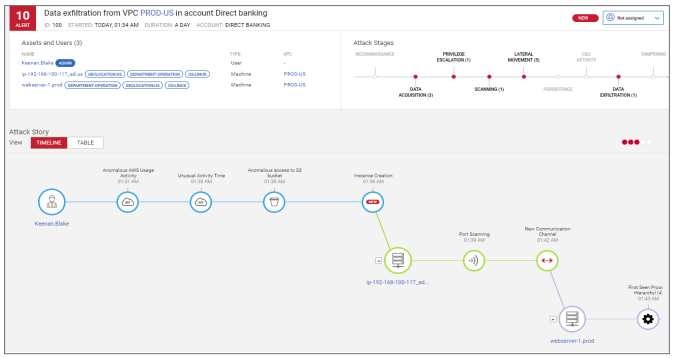
Cloud Workload Protection Service automatically blocks attacks against your cloud workloads before they turn into breaches

How Radware Keeps Your Workloads and Data Secure

Key Benefits of Radware's Solution:

- Detects publicly exposed assets
- Identifies excessive and unused permissions
- Hardens security configurations
- Uncovers data theft attempts
- Correlates events into orchestrated storylines
- Automatically responds to threats

Secure Your Workloads With Cloud Workload Protection Service



Context-Aware Smart Hardening

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

Orchestrated Attack Storylines

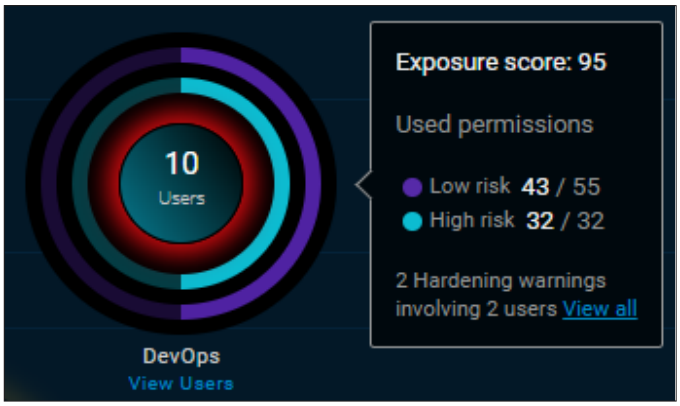
Radware correlates individual events using advanced machine learning algorithms and places them in contextual attack storylines to detect potential data theft attempts and block them as they evolve.

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.

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.



Agentless, Nonintrusive Deployment