

Cloud Infrastructure Entitlement Management (CIEM)

Running in the cloud is all about agility, flexibility and moving fast. However, in the name of expediency, network administrators frequently grant wide-ranging and unnecessary permissions to cloud users. And should one of those users ever become compromised, then attackers will have wide-ranging access to your networks. Radware provides comprehensive Cloud Infrastructure Entitlement Management (CIEM) capabilities to help organizations secure cloud permissions without getting in the way of the business.



Remove inactive users



Eliminate excessive permissions



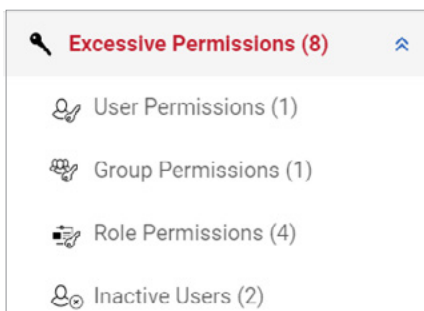
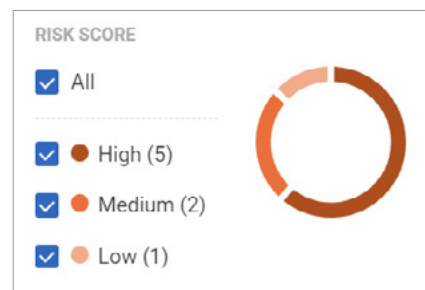
Curb cloud 'role' permissions



Cover all types of permissions

Your Permissions Equal Your Threat Surface

When you run workloads in the cloud, your resources and data are on the “outside.” Network administrators and hackers can access those workloads using the same methods, protocols and APIs. As a result, access to your sensitive data is defined by their access permissions. This means, in essence, that your permissions define the threat surface of your organization.



Complete Coverage for All Types of Permissions

Radware takes a unique approach to hardening permissions by analyzing the gap between defined and used permissions. This allows organizations to eliminate permissions for which there is no business need while keeping those which are being used. Radware also provides coverage for all permission types, including users, machines, roles, groups, cross-account and federated roles, making sure you are fully covered.

Easy to Use, Centralized Dashboard

Radware's [Cloud Native Protector](#) provides a centralized management dashboard for all your accounts across both Amazon AWS and Microsoft Azure. This allows you to get an immediate snapshot of your cloud security posture, for all your assets, regardless of where they are deployed.

Risk-Prioritized Permissions Management

To reduce log overload and help security managers focus on the most important alerts, Radware provides detailed, risk-prioritized alerting based on risk-assessment and severity to enable fast response and low false positives.

<input type="checkbox"/>	SCORE	DESCRIPTION	DETECTED	CLOUD PLATFORM	ACCOUNT	STATUS
<input type="checkbox"/>	8	User Catherine.brown is inactive ADMIN Inactive Users	TODAY, 07:46 AM	aws	Direct-Banking-Prod...	NEW
<input type="checkbox"/>	2	User Samantha.williams is inactive Inactive Users	TODAY, 07:46 AM	aws	Direct-Banking-Prod...	NEW
<input type="checkbox"/>	8	User group DataScientists has an unused inline polic... PRIVILEGED Group Permissions	TODAY, 07:46 AM	aws	Direct-Banking-Prod...	NEW
<input type="checkbox"/>	8	Federated role Okta-Developers has unused permissions in managed polic... Role Permissions	TODAY, 07:46 AM	aws	Direct-Banking-Prod...	NEW
<input type="checkbox"/>	8	Cross account role DevAccess has unused permissions in managed polic... Role Permissions	TODAY, 07:46 AM	aws	Direct-Banking-Prod...	NEW
<input type="checkbox"/>	8	User Larry.smith has unused permissions in managed poli... POWER User Permissions	TODAY, 07:45 AM	aws	Direct-Banking-Prod...	NEW
<input type="checkbox"/>	5	EC2 role Jenkins-masters has an unused managed... PRIVILEGED Role Permissions	TODAY, 05:45 AM	aws	Direct-Banking-Prod...	NEW
<input type="checkbox"/>	5	Lambda execution role LambdaUploaders has... PRIVILEGED Role Permissions	TODAY, 05:45 AM	aws	Direct-Banking-Prod...	NEW

Radware's Cloud Native Protector provide smart hardening recommendations for excessive permissions



Radware's Cloud Native Protector provides us with the single pane of glass to manage permissions and workloads that we were looking for. Being concerned about misconfigurations and potential risks associated with unaudited accounts has become a thing of the past. It's fortified our cloud-based network."

– Shay Reshef, Director of Security, SundaySky