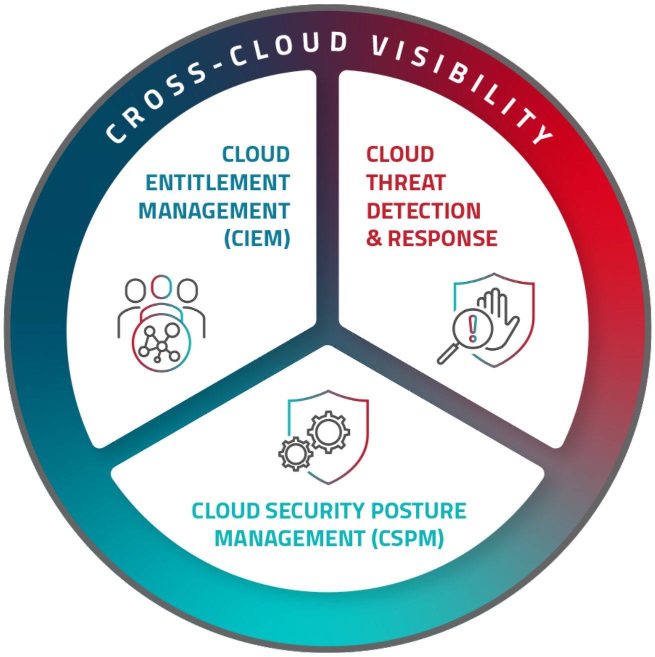
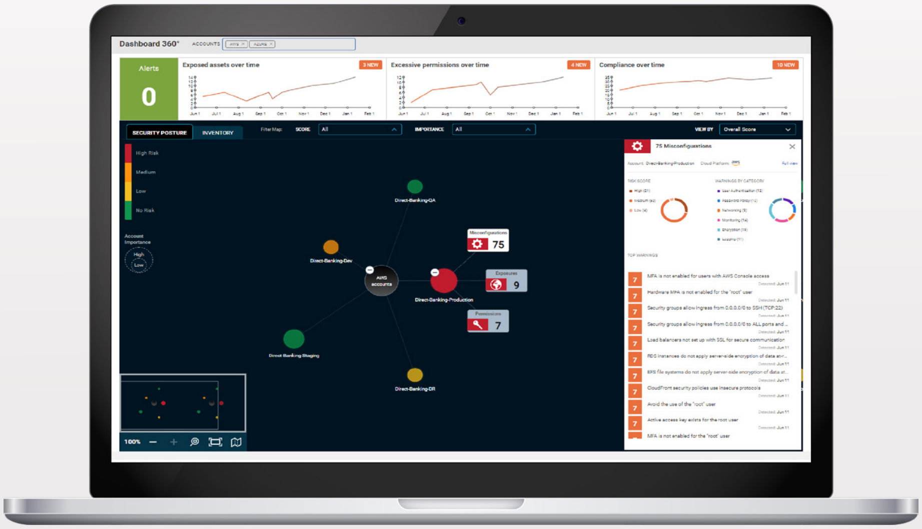
Comprehensive Protection for the Public Cloud

Managing workloads in the cloud frequently means losing visibility and control over cloud-hosted assets. Cloud environments are managed remotely and change rapidly, making it difficult for security teams to keep track of assets, supervise access to sensitive resources or manage security across multiple clouds. As a result, many organizations fail to detect and prevent cloud-based cyberattacks.

Radware provides an agentless, easy to deploy, cloud-native solution for applications, workloads and infrastructure hosted on Amazon Web Services (AWS) and Microsoft Azure. Radware's Cloud Native Protector offers multi-layered protection to reduce risk by continuously verifying compliance against multiple security standards, identifying publicly exposed assets, keeping track of asset inventory with prioritized cross-cloud visibility, fortifying the cloud threat surface with context-aware smart hardening, and providing advanced attack detection and remediation capabilities to stop data theft attempts.


CROSS-CLOUD VISIBILITY
CLOUD ENTITLEMENT MANAGEMENT (CIEM)
CLOUD THREAT DETECTION & RESPONSE
CLOUD SECURITY POSTURE MANAGEMENT (CSPM)



7 MFA is not enabled for users with AWS Console access — Detected: Jun 11

7 Hardware MFA is not enabled for the "root" user — Detected: Jun 11

7 Security groups allow ingress from 0.0.0.0/0 to SSH (TCP:22) — Detected: Jun 11

7 Security groups allow ingress from 0.0.0.0/0 to ALL ports and ... — Detected: Jun 11

7 Load balancers not set up with SSL for secure communication — Detected: Jun 11

7 RDS instances do not apply server-side encryption of data at-r... — Detected: Jun 11

7 EFS file systems do not apply server-side encryption of data at... — Detected: Jun 11

7 CloudFront security policies use insecure protocols — Detected: Jun 11

7 Avoid the use of the "root" user — Detected: Jun 11

7 Active access key exists for the root user — Detected: Jun 11

MFA is not enabled for the "root" user

Cross-Cloud, Actionable Visibility & Control

Radware provides centralized workload security management with single-pane-of-glass controls and multi-cloud support for AWS and Azure workloads. Automated discovery of cloud asset inventory and a unified view of assets across multiple accounts, regions, and environments within a single dashboard is also provided.

Separating Insight From Noise

ALERT

Identify suspicious activities using a wide range of Malicious Behavior Indicators (MBIs)

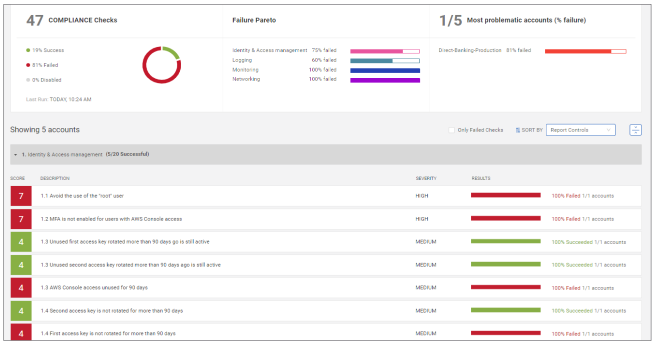
CORRELATE

Create a unified attack sequence with a correlated, step-by-step breakdown of the attack kill chain

REMEDIATE

Block threats before they evolve to breach with a risk-based view and alerts

Advanced Threat Detection & Risk Prioritization



47 COMPLIANCE Checks

● 19% Success
● 81% Failed
● 0% Disabled

Last Run: TODAY, 10:24 AM

Failure Pareto

Identity & Access management	75% failed
Logging	60% failed
Monitoring	100% failed
Networking	100% failed

1/5 Most problematic accounts (% failure)

Direct-Banking-Production 81% failed

Showing 5 accounts

☐ Only Failed Checks SORT BY Report Controls

1. Identity & Access management (5/20 Successful)

SCORE	DESCRIPTION	SEVERITY	RESULTS
7	1.1 Avoid the use of the "root" user	HIGH	100% Failed 1/1 accounts
7	1.2 MFA is not enabled for users with AWS Console access	HIGH	100% Failed 1/1 accounts
4	1.3 Unused first access key rotated more than 90 days go is still active	MEDIUM	100% Succeeded 1/1 accounts
4	1.3 Unused second access key rotated more than 90 days ago is still active	MEDIUM	100% Succeeded 1/1 accounts
4	1.3 AWS Console access unused for 90 days	MEDIUM	100% Failed 1/1 accounts
4	1.4 Second access key is not rotated for more than 90 days	MEDIUM	100% Succeeded 1/1 accounts
4	1.4 First access key is not rotated for more than 90 days	MEDIUM	100% Failed 1/1 accounts

1-Click Compliance Reporting

Comprehensive compliance reporting with out-of-the-box reports for multiple compliance standards.

Prioritized, Risk-Based Visibility

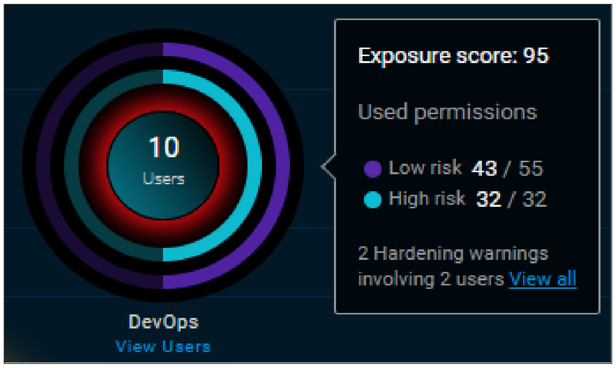
Unified view across multiple cloud environments and accounts, with built-in alert scoring for efficient prioritization.

Continuous Misconfiguration Detection

Detects misconfigurations and publicly exposed assets to fortify the cloud security posture and reduce attack threat surface.

Smart Hardening Recommendations

Provides prioritized risk recommendations with plain explanations of risk and suggested remediation.



10 Users

DevOps

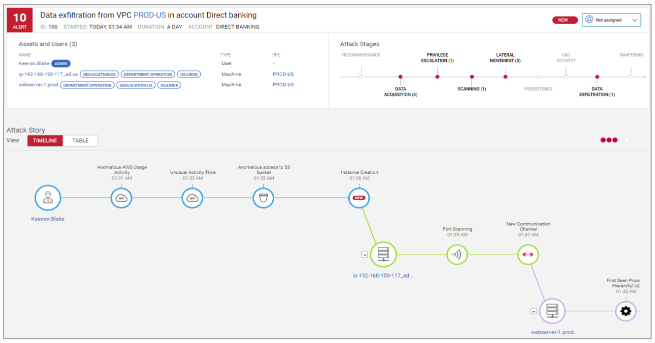
View Users

Exposure score: 95

Used permissions

● Low risk 43 / 55
● High risk 32 / 32

2 Hardening warnings involving 2 users View all



10 ALERT

Data exfiltration from VPC PROD-US in account Direct banking

ID: 100 STARTED: TODAY, 01:34 AM DURATION: A DAY ACCOUNT: DIRECT BANKING

NEW Not assigned

Assets and Users (3)

NAME	TYPE	VPC
Keenan.Blake ADMIN	User	-
ip-192-168-100-117_ad.us GEOLOCATION:US DEPARTMENT:OPERATION OS:LINUX	Machine	PROD-US
webserver-1.prod DEPARTMENT:OPERATION GEOLOCATION:US OS:LINUX	Machine	PROD-US

Attack Stages

Attack Story

View TIMELINE TABLE

Keenan.Blake
Anomalous AWS Usage Activity 01:31 AM
Unusual Activity Time 01:33 AM
Anomalous access to S3 bucket 01:33 AM
Instance Creation 01:36 AM
NEW
ip-192-168-100-117_ad...
Port Scanning 01:39 AM
New Communication Channel 01:42 AM
webserver-1.prod
First Seen Proce Hierarchyl (4) 01:43 AM

Advanced Detection of Malicious Behavior

Uses 70+ MBIs to identify suspicious behaviors such as anomalous storage access, network activity or data exfiltration.

Intelligent Correlation of Attacks

Correlates individual suspicious events into streamlined attack storylines which show step-by-step progression of the attack kill chain.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.