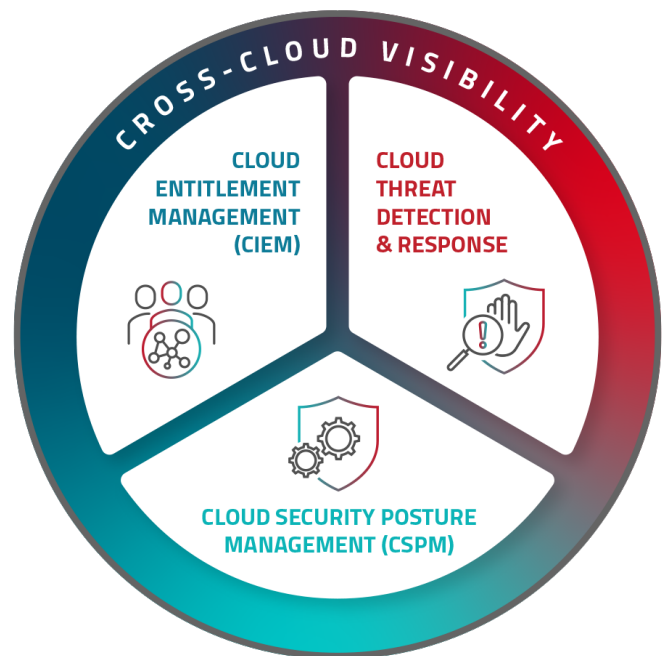


## Comprehensive Protection for the Public Cloud

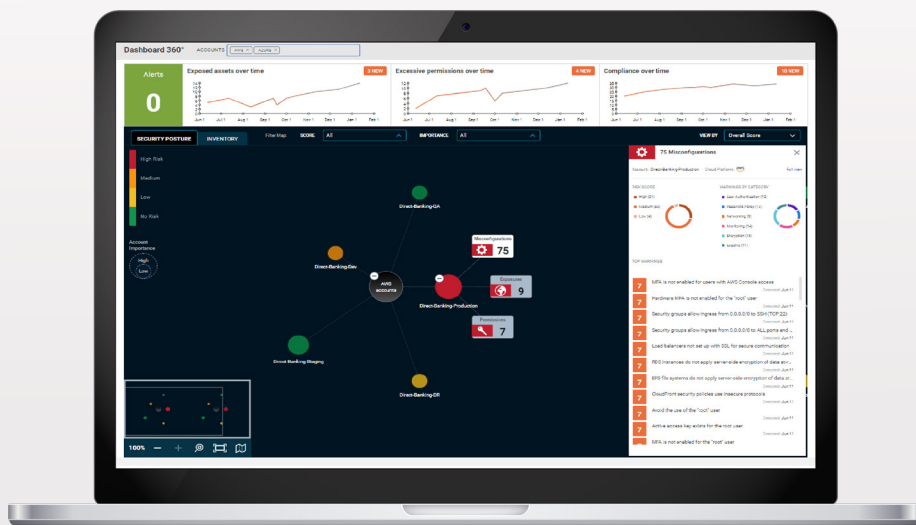
Managing workloads in the cloud frequently means losing visibility and control over cloud-hosted assets. Cloud environments are managed remotely and change rapidly, making it difficult for security teams to keep track of assets, supervise access to sensitive resources or manage security across multiple 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, 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

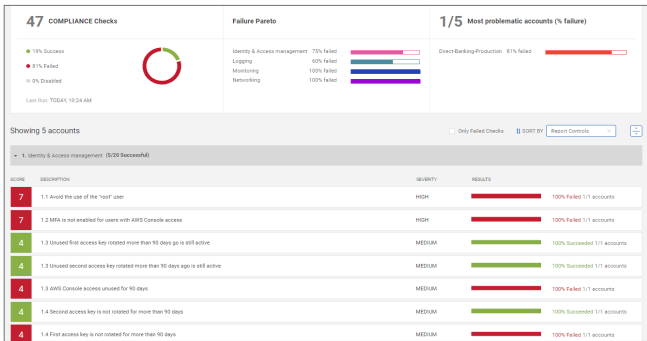
Create a unified attack sequence with a correlated, step-by-step breakdown of the attack kill chain



## REMEDiate

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

## Advanced Threat Detection & Risk Prioritization



### 1-Click Compliance Reporting

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

### Prioritized, Risk-Based Visibility

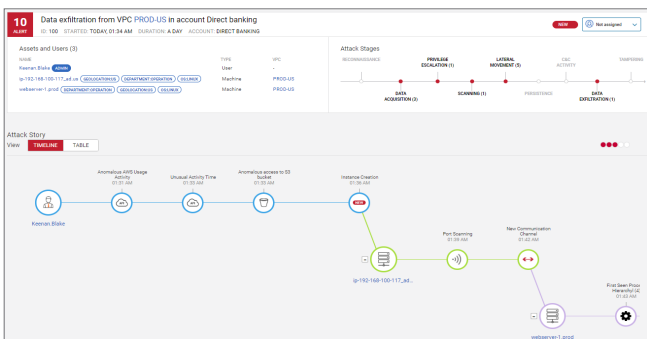
Unified view across multiple cloud environments and accounts, with built-in alert scoring for efficient prioritization.

### 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.



### 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.

© 2021 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details, please see: <https://www.radware.com/LegalNotice/>. All other trademarks and names are property of their respective owners.