

Cloud Threat Detection & Response (CTDR)

Running workloads in the public cloud opens them to unique, cloud-native threats, which are different than the threats facing on-premise environments. Radware provides comprehensive Cloud Threat Detection and Response (CTDR) capabilities to help organizations both detect suspicious activities in their cloud environments, but also correlate them into streamlined attack storylines to display step-by-step progression of attack activities so they can be stopped before they develop into a data breach.



Detect suspicious activity in your cloud



Risk-based prioritization of suspicious events



Correlate individual events into unified attack storylines



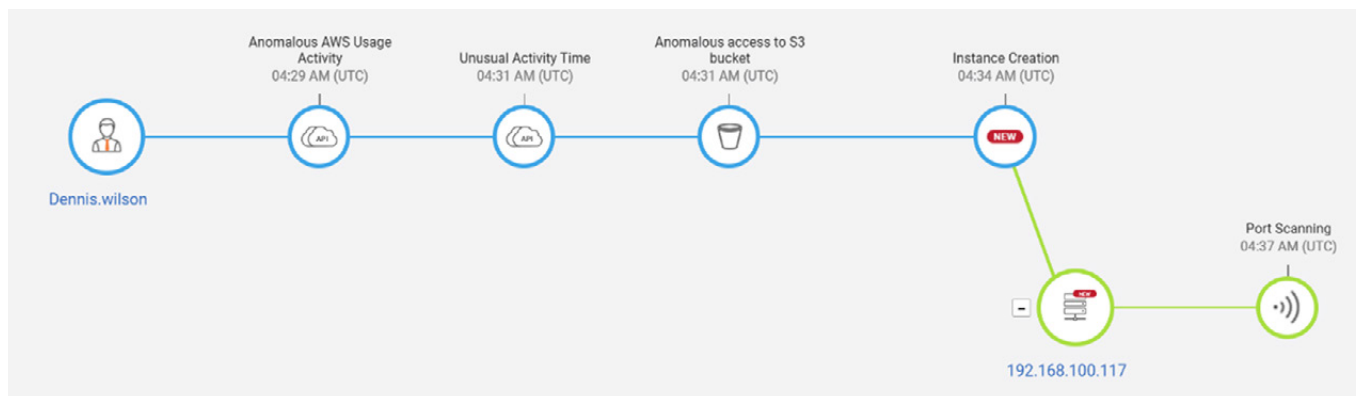
Automated response against malicious activity

Avoid Log Overload

Radware detects suspicious activity in your cloud environment using dedicated Malicious Behavior Indicators (MBIs) that are custom-tailored to the threats facing cloud environments. Moreover, Radware not only detects, but correlates individual events across time, threat surfaces and resources into unified attack storylines to show the step-by-step progression of attacks.

Don't Just Detect... Correlate

Radware's Cloud Native Protector detects malicious activity in your cloud environments using advanced AI algorithms that both detect malicious activities and correlate individual events into streamlined attack storylines. This allows you to keep track of event across long time spans, automatically identify relevant events in the stream of log alerts, and see visually how seemingly independent, low-priority alerts combine into a high-risk breach.



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 Alerting

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.

7	Anomalous user activity and Port scanning in account Direct-Banking-Production	aws	Direct-Banking-Production	Public-US	TODAY, 04:41 AM	200	New
10	Data exfiltration from VPC Public-US in account Direct-Banking-Production	aws	Direct-Banking-Production	Public-US	TODAY, 04:26 AM	100	New
10	Communication to crypto-mining IP	Azure	Online-Shopping-Production	-	TODAY, 04:13 AM	300	New
7	Credentials exfiltration of EC2 role Web-WAF-Role	aws	Direct-Banking-Production	Public-US	TODAY, 04:13 AM	215	New
7	Anomalous Outbound Communication DEPARTMENT:OPERATION GEOLOCATION:US	aws	Direct-Banking-Production	PROD-US	TODAY, 04:46 AM	110	-
5	New connection to database	aws	Direct-Banking-Production	-	TODAY, 04:46 AM	209	-
2	New Communication Channel DEPARTMENT:OPERATION GEOLOCATION:US	aws	Direct-Banking-Production	PROD-US	TODAY, 04:40 AM	104	-

Radware's Cloud Native Protector provides detailed, risk-prioritized threat alerts



“Radware’s Cloud Native Protector has helped Perion to identify threats in real time without the noise of false alerts. It has been excellent in exposing misconfigurations and potential risks and thus very helpful in both detection and prevention.”

— Amir Arama, Sr. Director of Engineering Operations at Perion