

Cloud Security Posture Management (CSPM)

Running workloads in public cloud environments opens them to new, cloud-native threats and vulnerabilities. Locking down your cloud security posture is paramount to guarantee the security and availability of user data. Radware provides comprehensive Cloud Security Posture Management (CSPM) capabilities, including compliance verification, detection of cloud misconfigurations, identifying publicly exposed assets and automatic governance enforcement to ensure your cloud environment is secure.



Detect suspicious activity in your cloud



Risk-based prioritization of suspicious events



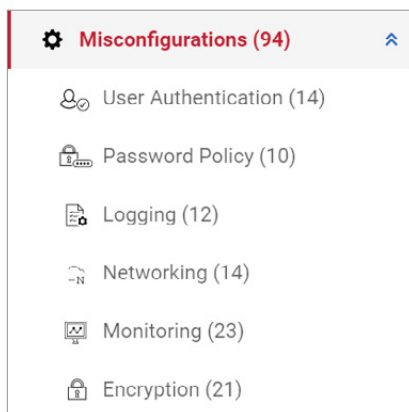
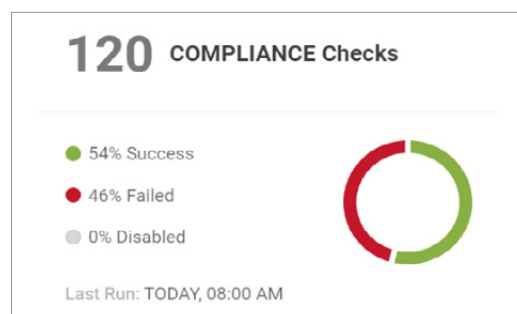
Correlate individual events into unified attack storylines



Automated response against malicious activity

One-Click Compliance Reporting

Radware's Cloud Native Protector provides detailed, one-click compliance reports for a wide range of industry and national compliance standards, including PCI DSS, SOC2, AWS CIS Foundations, NIST Cyber Security Framework, ISO 27001 and more, to provide both high-level verification of your compliance status and line-by-line assessment of each individual criterion in the standard. Radware also supports customized governance reports, tailored to your specific needs.



Comprehensive Misconfiguration Detection








Radware helps organizations detect cloud misconfigurations across a wide range of potential vulnerabilities, with detailed explanations of the error and its impact, and clear, actionable hardening recommendations. In addition, Radware provides a built-on query language for automatic remediation of misconfigurations and enforcement of governance policies to block vulnerabilities before they can get used.

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.

SCORE	DESCRIPTION	SEVERITY	RESULTS
7	Security groups allow ingress from 0.0.0.0/0 to ALL ports and protocols	HIGH	 100% Failed 1/1 accounts
4	Instances launched outside Virtual Private Cloud (VPC)	MEDIUM	 100% Succeeded 1/1 accounts
7	Security groups allow ingress from 0.0.0.0/0 to RDP (TCP:3389)	HIGH	 100% Failed 1/1 accounts
4	Security groups allow unrestricted outbound communication	MEDIUM	 100% Failed 1/1 accounts
7	Security groups allow unrestricted access from the internet to RDP port (TCP:3389)	HIGH	 100% Succeeded 1/1 accounts
7	Security groups allow ingress from 0.0.0.0/0 to SSH (TCP:22)	HIGH	 100% Failed 1/1 accounts
7	Default network access rule for Storage Accounts is not set to deny	HIGH	 100% Succeeded 1/1 accounts

Radware's Cloud Native Protector provides easy-to-understand, visual compliance reporting.



“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