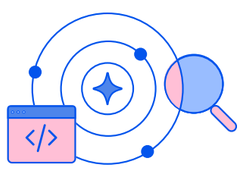
WIZ | DARKReading

TOP 10 TIPS

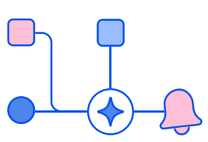
Securing Multi-Cloud With Modern CSPM

The cloud provides instant scalability and agility, enabling organizations to develop faster than ever. It's resulted in new security risks as cloud environments rapidly expand, making it harder to manage cloud configurations and compliance at scale. Cloud Security Posture Management (CSPM) tools help address these challenges by automating security and compliance on the cloud. In the current product offerings for CSPM, legacy CSPM lacks comprehensive risk coverage and context resulting in noisy alerts and lack of prioritization. In contrast, modern CSPM provides a holistic view of all risks across vulnerabilities, malware, network, data, identity, and secrets, and identifies toxic combinations that can result in critical risks. Modern CSPM provides the context around risks allowing organizations to prioritize and remediate critical issues faster. In this Top Tips, we offer expert advice on evaluating modern CSPM platforms and address key challenges that IT teams face securing today's multi-cloud deployments.



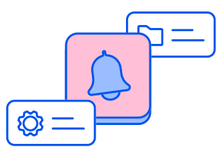
1. Identify Misconfigurations at Every Layer

Legacy CSPM tools rely on agents to detect misconfigurations, resulting in blind spots, performance impacts, and operational challenges. Modern CSPM tools are agentless and identify misconfigurations on every layer including, cloud, OS, and applications. Modern CSPM provides visibility across virtual machines, containers and serverless, and across all different CSPs



2. Deep Risk Assessment

Legacy CSPM tools only assess cloud misconfigurations, lacking full security context. Modern CSPM offers the full context of the security posture through deep risk assessment across vulnerabilities, network exposures, secrets, malware, identities, and sensitive data, enabling it to identify the toxic combinations in an environment that create a critical risk.



3. Understand Context to Identify Risk Criticality

Legacy CSPM lacks full context into risks, leaving organizations to correlate risks manually. Modern CSPM provides graph-based context into risks, correlating all risk factors, and enabling teams to remediate faster with actionable insights.

4. Establish Continuous and Comprehensive Governance

Modern CSPM tools monitor compliance on a continuous basis and support all major frameworks to help you meet regulatory requirements, including cloud frameworks such as PCI and NIST, and host level frameworks such as CIS benchmarks for Linux.

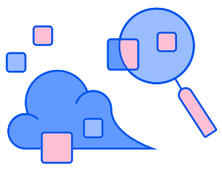
Wiz provides coverage for

5. Customize Controls to Meet Unique Security Requirements

Some organizations have unique compliance requirements. A modern CSPM offers flexibility to customize controls and frameworks to meet every regulatory standard, both across cloud and host controls and frameworks.

6. Prioritize Risks Through HighFidelity Alerts

Legacy CSPM tools create a lot of noise and result in alert fatigue. Modern CSPM uses context to surface only the most critical issues and prioritizes risks. Prioritization enables organizations to spend less time addressing distracting noise and more time on resolving critical risks.



7. Identify and Prevent Risks Early in the Development Cycle

Organizations are shifting left to identify risks early in the development cycle, empowering developers to fix misconfigurations before deployment. Modern CSPM integrates with development pipelines and scans IaC templates for misconfigurations, to detect and remediate issues before they reach production.

8. Employ Guidance to Remediate Faster

Modern CSPM gives you remediation guidance for any failed check in your environment so your team can respond faster. It enables you to set up automatic remediation workflows to reduce time on manual remediation.

9. Gain Consistent Visibility and Policy Enforcement

Single-point tools create segmented views of overall security posture, resulting in operational inefficiencies. Modern CSPM provides consistent visibility across all major CSPs and every cloud layer. It also provides consistent governance across all clouds, allowing one consistent policy across all environments.

10. Accelerate Your Cloud Journey

As cloud environments become more complex, modern CSPM automatically secures new technologies you adopt as you grow, for example Kubernetes. It provides additional security capabilities that allow you to expand from a CSPM to a CNAPP full set of features to support your cloud growth.

Wiz secures everything organizations build and run in the cloud. Founded in 2020, Wiz is the fastest-growing software company in the world, scaling from $1M to $100M ARR in 18 months. Wiz enables hundreds of organizations worldwide, including 35 percent of the Fortune 100, to rapidly identify and remove critical risks in cloud environments. Its customers include Salesforce, Slack, Mars, BMW, Avery Dennison, Priceline, Cushman & Wakefield, DocuSign, Plaid, and Agoda, among others. Wiz is backed by Sequoia, Index Ventures, Insight Partners, Salesforce, Blackstone, Advent, Greenoaks, Lightspeed and Aglaé. Visit https://www.wiz.io/ for more information.

WIZ