

Cloud Security Posture Management in Resource-Constrained Organizations: A Review of Azure, AWS, and Hybrid Approaches

Kenneth Nnadi¹, Yaw Agyekumhene Okrah² and Jochebed Akoto Opoku³

¹University of Oregon, USA

²Taskimpetus Inc- New Orleans, LA, USA

³Department of Telecommunication Engineering, Kwame Nkrumah University of Science and Technology, Ghana

Abstract: Small and resource-constrained organizations increasingly adopt public cloud platforms such as Microsoft Azure and Amazon Web Services (AWS) to gain scalability and reduce infrastructure costs. However, these organizations face persistent security challenges due to limited budgets, skills shortages, and immature governance structures. Misconfigurations in cloud environments are now among the leading causes of data breaches, yet many small teams lack the expertise and tools to manage these risks effectively. Cloud Security Posture Management (CSPM) has emerged as a key approach to address this gap by continuously monitoring configurations, enforcing compliance, and automating remediation. This review examines how CSPM is implemented in Azure, AWS, and hybrid or multi-cloud environments, focusing on its applicability to resource-constrained organizations. It analyzes native CSPM capabilities such as Microsoft Defender for Cloud, Azure Policy, AWS Security Hub, and AWS Config, and compares their coverage, automation, compliance support, and cost models. Findings indicate that while Azure and AWS offer robust posture management features, their complexity, consumption-based pricing, and skills requirements limit adoption in smaller organizations. Hybrid CSPM platforms provide unified visibility and standardized compliance but introduce additional cost and integration challenges. The paper concludes with practical recommendations and a tiered roadmap for SMEs: start with built-in CSPM tools, enforce critical policies, and gradually integrate automation and compliance frameworks. Future research should focus on lightweight CSPM patterns and usability studies to ensure these solutions close, rather than widen, the security gap for small organizations.

Keywords: Cloud Security Posture Management, Azure, Amazon Web Services, Small and Medium-Sized Enterprises, Multi-Cloud Security, Misconfigurations.

INTRODUCTION

Small and resource-constrained organizations are moving to the cloud to gain flexibility, scale, and access to modern digital services without building their own data centers (Ahmet el, 2025 a,b). Studies on small and medium enterprises (SMEs) show that cloud services support digital transformation, operational efficiency, and competitiveness, especially when organizations cannot afford large capital investments in IT infrastructure. At the same time, the move to cloud platforms introduces new security responsibilities. Many SMEs lack mature governance, formal security processes, and dedicated security teams, making them vulnerable when adopting complex cloud platforms such as Microsoft Azure and Amazon Web Services (AWS) (Jain, 2024; Mohammad & Abbas, 2024).

Security concerns are among the most persistent barriers to cloud adoption in SMEs. Mixed-method studies report that data security and privacy are the highest-ranked obstacles, followed by limited technical expertise, integration challenges, and regulatory compliance pressures (Mohammad & Abbas, 2024). A recent scoping review on cybersecurity in SMEs finds that lack of awareness, unsuitable guidelines, limited

cybersecurity knowledge, and constrained financial resources are key reasons why these organizations struggle to build resilience against modern cyber threats (Awan *et al.*, 2025). These conditions create a structural “resource poverty”, a term used to describe the severe lack of financial, technical, and human resources that leaves SMEs exposed to the same threats as large enterprises but with far fewer means to respond (Panful *et al.*, 2025 a,b,c).

Cloud Security Posture Management (CSPM) has emerged as a central approach to addressing these risks. CSPM refers to tools and practices that continuously identify, assess, and remediate misconfigurations and security risks in cloud environments. It focuses on configuration baselines, compliance, and visibility rather than on network perimeter defense alone. CSPM tools automate the scanning of identity and access management settings, storage permissions, network rules, and other configuration elements that, if misconfigured, can expose sensitive data or critical workloads. Misconfigurations are now recognized as one of the leading causes of cloud data breaches, especially in multi-cloud and hybrid

deployments, making CSPM a foundational layer in modern cloud security strategies (Jimmy, 2023).

Major cloud providers have integrated CSPM capabilities into their native security services. In Azure, CSPM is a core function of Microsoft Defender for Cloud, which provides continuous visibility into the security state of resources, prioritized recommendations, and compliance assessments across Azure and connected AWS or Google Cloud environments. AWS offers similar capabilities through AWS Security Hub, which performs automated configuration checks, aggregates security findings, and maps controls to common frameworks such as CIS and PCI DSS. Industry-wide definitions from vendors and standards bodies emphasize the same core elements: continuous monitoring of cloud configurations, centralized visibility across accounts and regions, automated compliance checks, and remediation workflows integrated into DevOps pipelines (Jimmy, 2023).

Azure and AWS are particularly important in this discussion because they dominate the public cloud market that SMEs use. For resource-constrained organizations, this concentration means that security posture decisions are often framed directly in terms of Azure and AWS service offerings, pricing, and tooling. At the same time, many small organizations do not migrate everything to a single public cloud. They retain on-premises systems for regulatory or operational reasons and combine them with one or more public cloud providers. Hybrid cloud strategies are therefore common among SMEs, because they allow sensitive data or legacy applications to remain under direct control while less sensitive or more elastic workloads move to the public cloud (Jain, 2024).

Hybrid and multi-cloud architectures, however, significantly increase complexity. Organizations must manage identities, network segmentation, encryption, logging, and policies across multiple technical and administrative domains. Research on multi-cloud security shows that inconsistent policies and configuration drift between environments are major vulnerability sources, and that CSPM tools are one of the few practical ways to maintain a coherent security posture across providers (Jimmy, 2023). For SMEs, the challenge is more severe. They face multi-cloud-level complexity without the scale of security teams and automation that large enterprises can afford.

This context leads to a clear problem statement. Resource-constrained organizations increasingly depend on Azure, AWS, and hybrid cloud architectures, yet they operate with limited budgets, scarce security expertise, and fragmented or immature tooling. Empirical studies on SME cloud adoption emphasize that the lack of skilled staff, cost pressures, and difficulty understanding shared-responsibility models are persistent obstacles to secure cloud use (Awan *et al.*, 2025). Work on resource allocation in SMEs further shows that many firms struggle even to provision and manage basic cloud resources effectively, which amplifies the risk that security configurations will be poorly understood or neglected. In this setting, CSPM is conceptually attractive but may be difficult to adopt and operate in practice (Mohammad & Abbas, 2024).

The purpose of this review is to examine how CSPM is realized in Azure, AWS, and hybrid environments and to evaluate what this means for resource-constrained organizations. The paper synthesizes academic and practitioner literature on CSPM tools and techniques, cloud adoption in SMEs, and hybrid or multi-cloud security. It aims to clarify how CSPM capabilities differ between Azure and AWS, how these capabilities extend (or fail to extend) to hybrid architectures, and how they intersect with the realities of limited budget, staff, and skills. By bringing together technical CSPM research with SME-focused cloud adoption and cybersecurity studies, the review seeks to identify realistic strategies rather than idealized enterprise-scale solutions.

CLOUD SECURITY POSTURE MANAGEMENT (CSPM)

Cloud Security Posture Management (CSPM) refers to tools and processes that continuously assess cloud environments for misconfigurations, policy violations, and security risks, and then help remediate them. Vendor and research sources describe CSPM as automated technology that identifies and fixes misconfigurations, improves compliance, and provides unified visibility across cloud services (Ahmed, 2023). These services include infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). CSPM operates across single-cloud, hybrid, and multi-cloud environments. In contrast to traditional perimeter-focused security, CSPM focuses on configuration correctness and least-privilege access inside the cloud platform, where

most modern failures now occur (Torkura *et al.*, 2021).

CSPM has evolved alongside cloud adoption. Early tools focused on static rule-based checks against a single provider, often scanning for a short list of risky patterns such as open object storage buckets or publicly exposed virtual machines (Ahmed, 2023). Over time, providers and third-party vendors expanded CSPM to support multiple clouds, integrate with DevOps pipelines, and correlate misconfigurations with real threat intelligence. Recent work on continuous auditing and threat detection in multi-cloud environments emphasizes the need for constant, automated

checks rather than occasional manual audits, and positions CSPM-like capabilities as central to this approach. Modern CSPM is now often packaged within broader cloud-native application protection platforms (CNAPPs), where posture management, workload protection, and code scanning share a single data model (Torkura *et al.*, 2021; Talwar, 2024).

Although vendors describe CSPM in many ways, three core functions recur across definitions: misconfiguration detection, compliance monitoring, and threat visibility (Jimmy, 2023). These functions are summarized in Table 1.

Table 1: Core functions of Cloud Security Posture Management

Core function	Brief description	Typical examples
Misconfiguration detection	Identify insecure or non-recommended settings across cloud resources	Publicly exposed storage, weak IAM policies, open management ports
Compliance monitoring	Map configurations to standards and regulations and flag violations	CIS benchmarks, ISO 27001, PCI DSS, sector-specific regulatory checks
Threat visibility and risk	Correlate configuration weaknesses with assets, identities, and external signals	Risk scores, attack path analysis, prioritized findings across accounts/regions

In Azure, CSPM is implemented primarily through Microsoft Defender for Cloud, which constantly evaluates resources against security standards for Azure, AWS, and Google Cloud projects and issues recommendations to reduce misconfigurations. In AWS, security posture management is centered on AWS Security Hub, which aggregates findings from AWS Config and other services and evaluates them against selected security standards and best practices. These platform-native implementations show that CSPM is no longer an optional add-on but a built-in layer of cloud governance (AlRababah, 2023).

CSPM also plays an important role within the shared responsibility model. Both Azure and AWS emphasize that while providers secure the cloud infrastructure (data centers, physical hosts, and core services), customers remain responsible for securing configurations, identities, and data within their environments. Many security incidents arise not from provider failures, but from customer misconfigurations, such as overly permissive access policies or unencrypted storage (Talwar, 2024). CSPM tools address this gap by giving customers continuous insight into “security in the cloud” and by automating parts of their side of the shared responsibility model. For resource-constrained organizations that cannot maintain

large security teams, this automation is especially important (Calvo-Manzano *et al.*, 2025).

Cloud Adoption in Resource-Constrained Settings

Resource-constrained organizations, including small and medium enterprises (SMEs), non-profits, and many public bodies, adopt cloud services to gain flexibility, reduce capital expenditure, and improve access to digital infrastructure (AlRababah, 2023). However, empirical studies consistently show that these organizations face distinctive constraints. Common barriers include limited budgets, a shortage of skilled staff, dependency on a small number of generalist IT personnel, and immature governance structures for risk and compliance (Jain, 2024; Tetteh, 2024; Calvo-Manzano *et al.*, 2025).

These constraints shape how such organizations use cloud platforms. Many adopt cloud services gradually, often in an ad-hoc fashion, starting with email, file sharing, or a single line-of-business application. Integration, identity design, and network segmentation are therefore often an afterthought rather than part of a planned architecture (Tetteh, 2024). Governance maturity tends to lag behind technology adoption. Policies for access control, data classification, change management, and incident response may be absent or not enforced in practice, creating fragmented

environments where CSPM tools must compensate for inconsistent configurations and weak policy

enforcement. (AlRababah, 2023).

Table 2: Typical constraints in resource-constrained organizations and implications for CSPM

Constraint	Brief description	Implications for CSPM and security posture
Limited budget	Small operating and capital expenditure for IT	Preference for built-in tools and low-cost tiers; difficulty funding specialists
Skills and staffing gaps	Few in-house security experts; reliance on generalists	Misunderstanding of cloud security models; slow or incorrect remediation
Governance immaturity	Weak or informal policies and processes	Inconsistent configurations; poor change control; audit findings hard to resolve
Tooling fragmentation	Mix of legacy, on-premises, and cloud services	Limited visibility across environments; overlapping or unused security features

These structural limits translate into specific security risks. Studies of SME cloud adoption and cybersecurity report frequent issues such as weak authentication, absence of multi-factor authentication, poor backup practices, informal use of personal devices, and lack of systematic patching (Tetteh, 2024). In cloud settings, misconfigured access control policies, publicly exposed storage, and excessive permissions on service accounts appear as recurring patterns of weakness (Talwar, 2024). Because these organizations often serve as suppliers or partners to larger firms, their vulnerabilities also create systemic risk in supply chains (Calvo-Manzano *et al.*, 2025).

Given these challenges, automation and low-cost tooling are central to any realistic security posture strategy. Research on cloud security automation argues that automated controls are essential to keep pace with the rate of change in cloud environments and to reduce human error in routine tasks such as configuration checks and log analysis. Studies focused on CSPM specifically show that automated posture management can significantly reduce misconfigurations and improve compliance by continuously scanning configurations and proposing or executing remediations (van Ede *et al.*, 2022). For SMEs, structured frameworks such as CyberESP emphasize the need to prioritize scalable, affordable controls and to outsource or automate functions that cannot be staffed internally (Calvo-Manzano *et al.*, 2025).

Azure and AWS Security Foundations

Azure and AWS are the most widely used public cloud platforms and form the technical foundation for the CSPM capabilities examined in this review. Both platforms provide global infrastructures

composed of regions and availability zones. An Azure region is a set of data centers deployed within a defined geographic area, while availability zones are separate groups of data centers within a region, each with independent power, cooling, and networking to support high availability (Ali *et al.*, 2025). AWS uses a similar model, describing geographic regions made up of multiple isolated availability zones that host redundant data centers and support fault-tolerant deployment of workloads. This shared architectural pattern enables resilience but also multiplies the number of resources and configurations that must be governed by CSPM (van Ede *et al.*, 2022).

On top of these architectural and responsibility models, Azure and AWS provide native security tools that implement CSPM functions directly. In Azure, the main posture management service is Microsoft Defender for Cloud, which continually assesses resources against built-in and custom security standards, detects misconfigurations, and provides a consolidated security score with remediation recommendations (Haimed *et al.*, 2023). Defender for Cloud integrates with Azure Policy to enforce configuration baselines, with Azure Monitor for logging and alerting, and with Microsoft Entra ID for identity-centric risk insights. In AWS, Security Hub aggregates findings from AWS Config, Amazon GuardDuty, Amazon Inspector, and other services, and evaluates them against security controls aligned with standards such as CIS and PCI DSS. AWS Config records configuration changes and evaluates them against rules, while CloudTrail and CloudWatch provide audit logs and monitoring needed to investigate and respond to posture issues (Ali *et al.*, 2025).

Table 3: Native Azure and AWS security tools relevant to CSPM

Provider	Service	Primary CSPM-related role
Azure	Microsoft Defender for Cloud	Core CSPM: continuous assessment, security score, recommendations
Azure	Azure Policy	Defines and enforces configuration baselines and compliance requirements
Azure	Azure Monitor / Log Analytics	Collects and analyzes logs and metrics for posture and incident visibility
Azure	Microsoft Entra ID	Identity and access management; conditional access and risk-based controls
AWS	AWS Security Hub	Aggregates security findings; evaluates controls and compliance status
AWS	AWS Config	Records and evaluates resource configurations against rules and standards
AWS	AWS Identity and Access Management (IAM)	Central identity and access control for AWS resources
AWS	AWS CloudTrail and CloudWatch	Logging, monitoring, and alerting related to configuration and security

CSPM IN AZURE

Azure is one of the dominant public cloud platforms for small and medium-sized organizations. Security posture management in Azure is delivered mainly through Microsoft Defender for Cloud and a set of governance and monitoring services. These tools work together to detect misconfigurations, enforce policies, and surface security recommendations across Azure and connected multi-cloud or hybrid environments (Verdet, 2023).

Native CSPM Tools

Microsoft Defender for Cloud is the core CSPM service in Azure. It continuously assesses Azure subscriptions and connects AWS or Google Cloud accounts against built-in and custom security policies (Engström *et al.*, 2023). It provides a secure score, regulatory compliance views, and prioritized recommendations that help organizations reduce risk and track progress over time. Defender for Cloud now also includes AI-assisted posture analysis and threat protection, including for newer workloads such as generative-AI services (Thangaraj, 2024).

Azure Policy is the main governance engine behind Azure CSPM. It lets administrators define rules that describe allowed configurations. For example, “all storage accounts must use encryption” or “no public IPs on virtual machines”. Azure Policy continuously evaluates resources, marks non-compliant items, and can block non-compliant deployments. Research on Azure Policy shows that policy-as-code can automate security controls, reduce

misconfigurations, and improve encryption and monitoring compliance across subscriptions (Verdet, 2023).

Azure Advisor is a recommendation engine that analyzes deployed resources and suggests improvements in five areas: cost, security, reliability, performance, and operational excellence. For security, Advisor surfaces configuration issues and links them to Defender for Cloud and Azure Policy, enabling organizations to apply fixes and track their impact (Thangaraj, 2024).

Azure Monitor collects logs and metrics from Azure and on-premises resources and is the data backbone for security services. Microsoft Sentinel, built on Azure Monitor, is a cloud-native SIEM that correlates telemetry, alerts, and Defender for Cloud findings to support detection, investigation, and response. While Sentinel is not a CSPM tool in the narrow sense, it completes the posture picture by adding incident and threat-centric views on top of configuration data (Thangaraj, 2024).

Strengths

The main strength of Azure CSPM is its deep integration with the wider Microsoft ecosystem. Defender for Cloud ties directly into Azure Resource Manager, Azure Policy, Microsoft Entra ID, Microsoft Sentinel, and Microsoft 365 workloads. This integration allows posture data, identity telemetry, and incident information to be analyzed together. Studies on Azure Security Center (the earlier name for Defender for Cloud) show that this unified view supports more effective threat detection and proactive risk mitigation,

especially when combined with machine-learning-based analytics. For small organizations that already rely on Microsoft 365 and Entra ID, this tight coupling reduces the need to deploy and maintain separate security stacks (Verdet, 2023; Neicu *et al.*, 2020).

Azure CSPM also benefits from rich built-in compliance content. Defender for Cloud maps Azure Policy definitions to frameworks such as CIS, ISO 27001, PCI DSS, and regional regulations, and presents results in a regulatory compliance dashboard. Recent empirical work on cloud compliance automation notes that Azure Policy and similar tools enable continuous auditing and policy enforcement, which is essential for sectors facing strict regulatory demands. Additional studies on Azure Policy show significant gains in encryption and monitoring compliance once policies are systematically applied, indicating that the template-driven approach can reduce configuration drift (Neicu *et al.*, 2020).

Another strength is the level of automated guidance. Defender for Cloud produces prioritized recommendations linked to the secure score, highlighting actions that yield the largest posture improvement. Azure Advisor adds further suggestions spanning security, performance, and cost and presents them in a unified dashboard. Economic analyses of Defender for Cloud deployments report measurable reductions in security risk and operational effort when organizations act on these recommendations, even though the exact benefit depends on maturity and deployment size. For resource-constrained teams, this recommendation-driven model is valuable because it helps them focus on a small set of high-impact changes rather than trying to interpret raw findings (Engström *et al.*, 2023).

Limitations

Despite these advantages, Azure CSPM has several limitations that are important for small and resource-constrained organizations.

First, cost remains a non-trivial factor. Defender for Cloud pricing is based on the number and type of protected resources and on data volume, while Sentinel and Azure Monitor charge mainly for log ingestion and analysis. Forrester's Total Economic Impact study of Defender for Cloud shows a positive return for large enterprises but also notes that benefits depend strongly on the number of workloads, breach likelihood, and the

organization's security culture. For small organizations with tight budgets, these consumption-based costs can be hard to predict and may discourage full adoption, especially when combined with Microsoft 365, Entra ID, and other license fees. Studies on SME cloud security more generally confirm that tooling costs are a recurring barrier to implement advanced controls (Wen *et al.*, 2025).

Second, policy management is complex. Azure Policy allows very fine-grained control, but designing, testing, and maintaining a large policy set requires expertise and coordination between security and development teams. Azure Policy can work really well, but it can also be hard to manage. Using policy-as-code helped teams improve things like encryption and monitoring. But without clear governance and DevOps support, policies can grow too fast and start conflicting with each other. An empirical study of infrastructure-as-code security practices also finds that many projects only adopt a subset of recommended Azure policies in Terraform templates, suggesting that best practices are not consistently implemented in real deployments (Chandrima *et al.*, 2024).

Third, there is a significant learning curve for small teams. Azure RBAC, Policy, Defender for Cloud, Monitor, and Sentinel each introduce their own configuration models and terminology. Recent research on Azure infrastructure hardening notes that misconfigurations, over-permissive roles, and privilege escalation paths persist even in environments that use Microsoft's security features, largely because administrators misunderstand complex options. The Future Internet study on Azure Active Directory misconfigurations shows how subtle configuration mistakes in dynamic groups and managed identities can enable privilege escalation, despite the presence of security tooling. For small organizations with few specialists, acquiring and maintaining this expertise is challenging, which can limit the real-world effectiveness of CSPM capabilities (Neicu *et al.*, 2020; Tetteh-Kpakpah *et al.*, 2025).

CSPM in AWS

AWS offers a rich set of native services for cloud security posture management. Posture management in AWS is centered on AWS Security Hub (and its CSPM capabilities), together with AWS Config, IAM Access Analyzer, and threat-detection services such as Amazon GuardDuty. These services work together to check

configurations against best practices, detect dangerous identity and access patterns, and surface high-priority findings for remediation (Pitkar, 2025).

Native CSPM Tools

AWS Security Hub CSPM is the primary posture-management service. It runs continuous security best-practice checks against AWS resources, ingests findings from other AWS security services and partners, and evaluates the environment against industry standards and internal baselines. The new Security Hub CSPM component focuses on misconfigurations and compliance posture, while Security Hub itself aggregates and correlates findings (including CSPM findings) and helps teams prioritize and respond at scale (Wen & Ping, 2025).

IAM Access Analyzer complements these services by focusing on identity and access. It uses automated reasoning to identify resources that are accessible from outside the account or organization and to detect unused or overly broad permissions. It can also generate least-privilege policies based on observed access patterns and validate policies against best practices. Findings from IAM Access Analyzer can be sent directly into Security Hub, where they become part of the overall posture picture (Engström *et al.*, 2023). Amazon GuardDuty is a managed threat-detection service that continuously analyzes CloudTrail logs, VPC flow logs, DNS logs, and other telemetry for signs of account or workload compromise. GuardDuty findings are ingested into Security Hub and provide the threat-centric side of posture, complementing configuration-centric CSPM (Pitkar, 2025).

Table 4: Key AWS services relevant to CSPM

Service	Primary CSPM-related role
AWS Security Hub + CSPM	Core posture layer: runs best-practice checks, aggregates, and prioritizes findings
AWS Config	Records configurations; evaluates them against rules and conformance packs
IAM Access Analyzer	Analyses IAM and resource policies for external and unused access; supports least privilege
Amazon GuardDuty	Detects threats and anomalous behavior from logs and telemetry

Strengths

A central strength of CSPM in AWS is strong identity and configuration monitoring. IAM is the core of AWS security, and both IAM Access Analyzer and several AWS Config rules are designed specifically to help achieve least privilege and to catch dangerous cross-account or public access. Research on IAM misconfigurations confirms that identity policies are a major source of risk, but also shows that they can be systematically analyzed and improved when good telemetry and tooling are available (Wen & Ping, 2025).

Another strength is flexible automation. Security Hub CSPM runs best-practice checks automatically and converts them into findings that can trigger workflows through Event Bridge, Lambda, and Systems Manager Automation. AWS Config can invoke Lambda functions for automatic remediation, creating self-healing patterns such as automatically closing public S3 buckets or enabling encryption. This automation capability is important for small teams that cannot manually review every configuration change (Continella *et al.*, 2018; Najana & Ranjan, 2024).

Limitations

However, AWS CSPM also has important limitations, especially for small teams. First, service sprawl can make setup and ongoing management complex. Security Hub, Config, IAM, GuardDuty, Macie, and Inspector each have their own concepts, configuration pages, and pricing models. AWS documentation itself presents Security Hub CSPM and Security Hub as separate but complementary services, and recommends that customers also enable GuardDuty, Macie, and Inspector for full coverage. This layered design is powerful but can be confusing for small organizations that lack specialist staff. Because the setup is complex, many organizations only use some of the tools. This creates an incomplete security setup and leaves important areas unprotected. Academic work on IAM policy analysis also notes that the sheer number of policy objects and relationships in real AWS environments creates cognitive overload for administrators (Chandrima *et al.*, 2024).

Second, cost can be hard to predict. Security Hub CSPM is priced per best-practice check and per integrated finding, while Config charges per configuration item recorded and per rule

evaluation; GuardDuty and other services also use usage-based models. For large enterprises, the cost is often justified by regulatory and risk-reduction needs, but for small organizations the combined consumption from multiple services and high-volume logs may exceed expectations. Empirical work on cloud misconfiguration and compliance under DORA shows that continuous scanning and auditing are essential, *yet also* points out that the tool stack and its operating cost must be carefully scoped to remain sustainable (Wen & Ping, 2025; Najana & Ranjan, 2024).

Third, AWS CSPM assumes a certain level of skill. Designing Config rules and conformance packs, tuning Security Hub standards, interpreting IAM Access Analyzer findings, and correlating GuardDuty alerts all require an understanding of AWS services, IAM semantics, and threat models (Paul, 2023). A CCS 2022 study on anomalous IAM misconfigurations (van Ede *et al.*, 2022) shows that even experienced organizations struggle to understand complex real-world policies, and that data-driven anomaly detection can find 3.7 to 6.4 times more misconfigurations than rule-based approaches. This suggests that many dangerous configurations remain undetected in typical deployments, particularly in small teams that cannot invest in advanced analysis.

HYBRID AND MULTI-CLOUD CSPM APPROACHES

Hybrid and multi-cloud environments are now common even in small and resource-constrained organizations. Many starts with on-premises or single-cloud deployments and then add public cloud services for specific workloads, often without a single, coherent security strategy. Over time, this creates a mix of legacy systems, Azure, AWS, and sometimes other providers, which increases configuration complexity and the risk of inconsistent controls. Research on multi-cloud posture management shows that maintaining a consistent security baseline across providers is difficult without automation and centralized governance. In this context, hybrid and multi-cloud CSPM tools can help small teams obtain a unified view of risk and compliance across their entire estate (Julakanti *et al.*, 2022). A hybrid cloud combines private or on-premises infrastructure with public cloud services. Multi-cloud refers to the use of two or more public cloud providers, such as Azure and AWS, often alongside on-premises systems. For many SMEs and NGOs, this is not a deliberate “multi-cloud

strategy” but the result of incremental decisions, vendor lock-in concerns, and piecemeal migrations constrained by budget and staff (Awagu, 2025).

Empirical work on SMEs shows that hybrid models are valued because they balance economic, technical, and security considerations. Sensitive data or core business systems often remain on-premises or in a private cloud, while non-critical or compute-intensive workloads move to the public cloud to reduce costs. Studies on hybrid strategies for SMEs highlight that hybrid cloud helps these organizations gain scalability and resilience without fully abandoning existing infrastructure but also introduces governance and skills challenges. At the same time, industry surveys report that most enterprises now use several cloud providers, with multi-cloud strategies driven by cost optimization, avoidance of vendor lock-in, and resilience (Najana & Ranjan, 2024). For resource-constrained organizations, this trend often appears in smaller form: one primary cloud plus a second provider used for specific services (for example, identity, analytics, or backup). In such settings, CSPM must work across heterogeneous platforms, identity models, and policy languages, which is where hybrid and multi-cloud-aware tools become relevant (Julakanti *et al.*, 2022).

Strengths of Hybrid and Multi-Cloud CSPM

A key strength of hybrid and multi-cloud CSPM is unified visibility. Studies of multi-cloud security posture management emphasize that configuration drift and inconsistent policies are major risks when workloads span providers with different security models. Centralized CSPM platforms reduce this risk by aggregating asset inventories, misconfiguration findings, and compliance status into a single view, making it easier for small teams to understand their overall posture (Wen *et al.*, 2025; Julakanti *et al.*, 2022).

Second, these tools support standardized compliance monitoring. Gandhi’s evaluation of CSPM tools in multi-cloud environments shows that one of their main benefits is the ability to map provider-specific controls to common frameworks (such as CIS, NIST, PCI-DSS, or ISO 27001) and to apply standardized policies across clouds. Paul (2023) discusses tools such as Cloud Guardian, which enforces consistent policies and automatically checks compliance across multiple clouds and container platforms, significantly improving the security posture and reducing operational disruptions in the reported case studies.

Third, hybrid CSPM can lower operational overhead. Instead of each administrator manually checking Azure, AWS, and on-premises dashboards, CSPM tools consolidate alerts and provide prioritized remediation recommendations. Lopez's work on security posture management for dynamic multi-cloud configurations argues that unified posture management is essential for continuous monitoring and automated enforcement in environments where manual oversight cannot keep up with change. For small organizations with limited staff, this consolidation can translate into fewer missed misconfigurations and more efficient use of specialist time (Nainar, 2025).

LIMITATIONS

Despite these benefits, hybrid and multi-cloud CSPM also present notable limitations for resource-constrained organizations.

Subscription cost barriers
Commercial CSPM and CNAPP platforms are typically priced per asset, account, or workload. For SMEs, these recurring costs sit on top of cloud consumption charges and may be hard to justify, especially when their environments are relatively small. Gandhi's review notes that advanced CSPM deployments often involve additional expenditure for integrations, data retention, and professional services. A recent study on the hidden financial implications of cloud security shows that advanced security tools, compliance audits, and incident management can contribute significantly to the total cost of ownership of cloud services, and these costs are not always visible at the planning stage (Kopparthi, 2025).

Integration challenges
Hybrid and multi-cloud CSPM solutions must interface with different APIs, identity systems, and logging formats. Lopez highlights that configuration drift and inconsistent policies are common in dynamic multi-cloud environments because each provider exposes distinct controls and semantics. Case studies of Cloud Guardian also show that integrating agents, data pipelines, and policy engines across multiple platforms require careful engineering and tuning. Open-source tools such as Cloud Custodian or Prowler, commonly used in practitioner settings, reduce licensing costs but shift the integration burden to internal teams, who must maintain scripts, CI/CD integration, and reporting workflows.

Need for Multi-Platform Skills
Human factors remain a critical weakness. Nobles' investigation of cloud misconfiguration errors shows that human error, lack of training, and organizational factors are central causes of misconfigurations, with one vendor study reporting a 424% increase in misconfigurations and an estimate that 95% of breaches involve human error. In a hybrid or multi-cloud scenario, administrators must understand security models, IAM concepts, and network constructs in at least two major cloud providers, plus on-premises systems. European agency guidance on SME cloud security stresses that small organizations often lack in-house expertise to correctly configure cloud security and to ask the right questions of providers. For resource-constrained organizations, this skills requirement can limit the effectiveness of CSPM. Tools may be purchased or deployed, but policies, baselines, and remediation workflows are not fully tuned, which can lead to alert fatigue or false confidence (Kamaluddin, 2023; Wen *et al.*, 2025).

ORGANIZATIONAL CHALLENGES

Skills shortage
Skills shortages are a persistent problem. A 2025 study on cybersecurity talent in SMEs finds that small firms struggle to attract and keep skilled staff, and that many rely on one or two generalists who must cover many roles, including security (Awan *et al.*, 2025). Nagahawatta *et al.* (2021) show, in their review of SME cybersecurity, that the lack of specialized staff is one of the most consistent barriers to resilience. Industry reports echo this, highlighting a global shortage of cyber skills that hit SMEs hardest. CSPM tools are meant to offset this by automating checks. Yet they still require people who can design policies, interpret findings, and prioritize remediation. Studies of IAM misconfigurations in AWS and identity issues in Azure show that even experienced teams struggle with complex policies and that many high-risk paths are only found by advanced analysis (Van Ede *et al.*, 2022; Haimed *et al.*, 2023; Ejaz & Gimah, 2024).

Weak Governance Structures
Many SMEs lack formal security governance. Rahman *et al.* (2023) examine SME governance in the context of Industry 5.0 and report resistance to structured security measures, limited policy implementation, and weak management involvement. A qualitative study on SME cloud adoption finds that organizations often lack a clear IT policy, have difficulty integrating cloud

services with existing systems, and struggle to enforce rules consistently (Nagahawatta *et al.*, 2021). Without governance, CSPM findings may not lead to real change. Misconfigurations get flagged but remain unresolved. Ferzali *et al.* (2025) show that even in regulated financial environments, posture improvements depend on linking CSPM outputs into formal risk and change processes; otherwise, issues recur.

Limited Security Culture

Security culture is often weak in small organizations. Nagahawatta *et al.* (2021) report that many SMEs see cybersecurity as a technical cost rather than as part of business risk management. A cross-country study by Rahman *et al.* (2023) also finds resistance to security controls among staff and managers, who fear disruption or extra work. This low security culture affects CSPM. Administrators may treat recommendations as optional. Business owners may reject necessary configuration changes because they appear to slow down development or operations. Awagu (2025) argues that compliance and security can support SME performance, but only when leaders see them as enablers rather than burdens.

LEGAL AND COMPLIANCE CHALLENGES

Multi-Region Laws

Many SMEs serve customers in more than one country, even if they are physically small. This exposes them to a mix of laws such as the EU General Data Protection Regulation (GDPR), sectoral rules, and national cyber regulations. A recent study on security, compliance, and risk in SME cloud adoption shows that GDPR, PCI DSS, data sovereignty, and auditing are seen as the most critical compliance concerns (Cambronerio *et al.*, 2022). Research on compliance in cloud computing stresses that organizations need an enterprise-wide compliance strategy for cloud, with continuous monitoring and specialist advice (Ahmad & Aujla, 2023). For SMEs, this level of planning is hard to achieve. They often rely on provider defaults and high-level guidance, which may not cover all legal obligations.

Data Residency and Sovereignty

Data residency refers to where data is stored and processed. Data sovereignty concerns which laws apply to that data. Both matter for cloud. Industry overviews on data residency note that GDPR and similar laws require some data to stay in defined regions and that organizations must be able to prove where data lives. Cambronerio *et al.* (2022)

show that SMEs struggle with these issues and propose GDPR Validator, a tool to help small firms that move to the cloud check their compliance posture. Multi-cloud strategies make these questions harder. Ahmad & Aujla (2023) point out that GDPR compliance becomes more complex when data is spread across several providers, each with its own contracts and transfer mechanisms. Recent discussion of the interplay between GDPR and the US CLOUD Act also highlights conflicts when non-EU authorities can request data from EU data centers via providers, which raises governance and trust questions for SMEs that depend on global platforms.

Certification Pressures

Certification and audit expectations are rising. Many customers now expect even small suppliers to follow standards such as ISO 27001, ISO 27018, or SOC 2 (Nnadi & Opoku, 2025). Industry reports notes that European SMEs use certifications and “trusted cloud” labels to signal compliance and win contracts. Awagu (2025) finds that security compliance can improve SME performance and trust, but it requires sustained investment. Thangaraj (2024) shows that security posture management tools are important for compliance but also adds significant direct and indirect costs, which are often overlooked in budgeting. For many SMEs, CSPM may be needed to support certification, yet its licensing and operational costs can be a barrier.

BEST PRACTICES FOR CSPM IN SMALL AND RESOURCE-CONSTRAINED ORGANIZATIONS

Small organizations with limited money and staff should aim for “good enough and consistent” security, not perfection. Pick one person who is responsible for cloud security (even part-time). Write a few simple rules on who can access what, how changes are made, how data is classified, and what to do in an incident. Keep a short list of your biggest cloud risks (like public storage, missing backups) and what you are doing about them.

Also, small organizations should use built-in cloud tools like Azure Policy or AWS Config to check and enforce rules automatically, starting in “audit only” mode, then slowly move a few critical checks to “block” or “auto-fix.” They should manage these rules as code so you can track changes and roll back if needed. Again, they must keep costs low by turning on free security features first, using open-source scanners from time to time, sending logs only from the most important

systems, and preferring managed cloud services instead of running their own security tools (Thangaraj, 2024).

Resource-constrained organizations should focus first on the most dangerous mistakes: wide-open permissions, no multi-factor login, public storage or open management ports without a strong reason, no encryption, and no activity logging. They should make sure everyone understands shared responsibility: the cloud provider secures the platform, but you still own things like user accounts, configuration, backups, and incident response.

Finally, resource-constrained organizations should follow a simple three-step roadmap: Tier 1 is “do not be wide open” (turn on native CSPM, enforce MFA, block public storage). Tier 2 is “protect key services” (policy as code, some auto-fixing, regular scans, simple incident steps) and Tier 3 is “ready for audits and growth” (align with standards like ISO/NIST, integrate with SIEM, do periodic tests and formal risk reviews), and only move up a tier when your business needs it and your team can handle the extra complexity (Kopparthi, 2025).

CONCLUSION

This review has shown that CSPM is now a core part of secure cloud use, but that its benefits are unevenly realized in small and resource-constrained organizations. Azure and AWS both offer broad native coverage across identities, networks, storage, virtual machines, and containers, with built-in compliance mappings and increasing levels of automation. Yet misconfiguration complexity, fragmented tools, and demanding cost and skill profiles limit what small teams can achieve in practice. Hybrid and multi-cloud CSPM platforms can improve visibility and standardize controls, but their subscription costs, integration demands, and multi-platform skill requirements often exceed SME capacity.

The analysis points to several practical priorities. Small organizations need a minimum viable governance model, focused automated policy enforcement, low-cost monitoring, and clear attention to a small set of high-impact misconfigurations. CSPM must be framed within the shared responsibility model and embedded in simple processes for triage and remediation, rather than treated as a stand-alone tool purchase. At the same time, the literature reveals major gaps: little

empirical evidence on CSPM adoption in SMEs, limited cost-benefit data, and almost no usability studies. Future research should develop standard evaluation benchmarks, lightweight CSPM patterns for nonprofits and small businesses, and AI-assisted posture scoring that adds value without overwhelming constrained teams. Addressing these gaps is essential if CSPM is to support, rather than widen, existing security inequalities.

REFERENCES

1. Ahmad, H., & Aujla, G. S. "GDPR compliance verification through a user-centric blockchain approach in multi-cloud environment." *Computers and Electrical Engineering* 109 (2023): 108747.
2. Ahmed, Z., Filani, A., Osifowokan, A. S., & Hutchful, N. "The Impact of Data Breaches in US Healthcare: A Cost-Benefit Analysis of Prevention vs. Recovery." (2025).
3. Ahmed, Z., Osifowokan, A. S., Filani, A., & Donkor, A. A. "Comprehensive analysis of cyber attacks and data breaches in the US health sector: Identifying vulnerabilities and developing proactive defense strategies."
4. Ali, S., Talpur, D. B., Abro, A., Alshudukhi, K. S. S., Alwakid, G. N., Humayun, M. & Shah, A. "Security and privacy in multi-cloud and hybrid cloud environments: Challenges, strategies, and future directions." *Computers & Security* (2025): 104599.
5. Alrababah, Z. A. K. A. R. I. A. "Barriers to cloud computing adoption among SMEs in the middle east: a systematic review." *Journal of Theoretical and Applied Information Technology* 101.17 (2023): 6853-6865.
6. Awagu, K. K. "Analyzing the Effectiveness of Information Security Compliance on Cloud Based Small and Medium Enterprises (SMEs)." (2025).
7. Mujtaba, A., Alam, A., & Kamran, M. "Cybersecurity challenges in small and medium enterprises: A scoping review." *Journal of Cyber Security and Risk* 2025.3 (2025): 89-102.
8. Calvo-Manzano, J. A., San Feliu, T., Herranz, Á., Mariño, J., Fredlund, L. Å., & Moreno, A. M. "CyberESP: An Integrated Cybersecurity Framework for SMEs." *Journal of Software: Evolution and Process* 37.9 (2025): e70050.
9. Cambroner, M. E., Martínez, M. A., de la Vara, J. L., Cebrián, D., & Valero, V. (2022). GDPRValidator: a tool to enable companies using cloud services to be GDPR compliant. *PeerJ Computer Science*, 8, e1171.

10. Chandrima, N., Bhatnagar, M., & Nigam, R. K. "Azure Cloud Infrastructure Hardening: A Survey." *International Journal of Advanced Computer Technology* 13.6 (2024): 01-08.
11. Continella, A., Polino, M., Pogliani, M., & Zanero, S. "There's a hole in that bucket! a large-scale analysis of misconfigured s3 buckets." *Proceedings of the 34th Annual Computer Security Applications Conference*. (2018).
12. Ejaz, U., & Gimah, M. "Cybersecurity Talent Shortage in SMEs: Innovative Approaches to Recruitment and Retention." (2024).
13. Engström, V., Johnson, P., Lagerström, R., Ringdahl, E., & Wällstedt, M. "Automated security assessments of amazon web services environments." *ACM Transactions on Privacy and Security* 26.2 (2023): 1-31.
14. Ferzali, A., Mengistu, N., Seid, E., & Blix, F.. "Cloud Security Misconfigurations and Compliance: An Empirical Model for DORA Readiness in Financial Environments." *management* 24.38 (2025): 40.
15. Forrester Consulting. "The Total Economic Impact™ of Microsoft Defender for Cloud." *Forrester Research*. (2025).
16. Haimed, I. B., Albahar, M., & Alzubaidi, A. "Exploiting misconfiguration vulnerabilities in microsoft's azure active directory for privilege escalation attacks." *Future Internet* 15.7 (2023): 226.
17. Jain, P. "Cloud adoption strategies for small and medium enterprises (SMEs): A comprehensive guide to overcoming challenges and maximizing benefits." *Sch J Eng Tech* 1.1 (2024): 28-30.
18. Jimmy, F. N. U. "Cloud security posture management: tools and techniques." *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)* 2.3 (2023).
19. Julakanti, S. R., Sattiraju, N. S. K., & Julakanti, R. "Multi-cloud security: strategies for managing hybrid environments." *NeuroQuantology* 20.11 (2022): 10063-10074.
20. Kamaluddin, K. "Network isolation for cloud native applications in multitenant Architectures." (2023).
21. Kopparthi, G. S. "Cost Optimization in Azure and AWS Cloud." *Journal of Marketing & Social Research* 2 (2025): 177-182.
22. Mohammad, A., & Abbas, Y. "Key challenges of cloud computing resource allocation in small and medium enterprises." *Digital* 4.2 (2024): 372-388.
23. Nagahawatta, R., Warren, M., Lokuge, S., & Salzman, S. "Security concerns influencing the adoption of cloud computing of SMEs: a literature review." (2021).
24. Nainar Balasubramanian, P. "ML-Driven Threat Detection with Azure Security Center." *Available at SSRN 5393916* (2025).
25. Seth, D., Najana, M., & Ranjan, P. "Compliance and regulatory challenges in cloud computing: a sector-wise analysis." *International Journal of Global Innovations and Solutions (IJGIS)* (2024).
26. Neicu, A. I., Radu, A. C., Zaman, G., Stoica, I., & Răpan, F. "Cloud computing usage in SMEs. An empirical study based on SMEs employees perceptions." *Sustainability* 12.12 (2020): 4960
27. Nnadi, K., & Opoku, J. A. "Cybersecurity curriculum alignment with industry needs: A literature review of educational models integrating labs, certifications, and research." *Sarcouncil Journal of Engineering and Computer Sciences*, 4.12 (2025): 1–20.
28. Nobles, C. "Investigating cloud computing misconfiguration errors using the human factors analysis and classification system." *Scientific Bulletin* 27.1 (2022): 59-66.
29. Panful, B., Apaflo, B., & Hutchful, N. "Cyber-Physical Systems Under Threat: A Case-Study Review of Recent SCADA Attacks in the US Utility Sector." *Journal Of Engineering And Computer Sciences* 4.12 (2025): 104-117.
30. Panful, B., Apaflo, B., & Hutchful, N. "From compliance to culture: Assessing organizational cybersecurity readiness in public vs. private U.S. utility companies." *EPRA International Journal of Research & Development (IJRD)*, 11.1 (2026).
31. Panful, B., Apaflo, B., Filani, A., Nnadi, K., & Hutchful, N. "Human factor vulnerabilities in energy industry cybersecurity: Assessing employee awareness and behavior in breach prevention." *International Journal for Multidisciplinary Research (IJFMR)*, 7.6 (2025): 1–18.
32. Paul, F. "AI-Powered Threat Detection in Hybrid and Multi-Cloud Environments: Overcoming Security Challenges." (2023).
33. Pitkar, H. "Cloud Security Automation Through Symmetry: Threat Detection and Response." *Symmetry* 17.6 (2025): 859.
34. Rahman, A., Shamim, S. I., Bose, D. B., & Pandita, R. "Security misconfigurations in open source kubernetes manifests: An empirical study." *ACM Transactions on*

- Software Engineering and Methodology* 32.4 (2023): 1-36.
35. Talwar, S. "Unified Framework for Securing Cloud-Native Storage: Approach for Detecting and Mitigating Multi-Cloud Bucket Misconfigurations." (2024).
 36. Tetteh, A. K. "Cybersecurity needs for SMEs." *Issues in Information Systems* 25.1 (2024).
 37. Tetteh-Kpakpah, C., Adjaottor, S., & Donkor, A. A. "MITIGATING CYBER THREATS THROUGH CYBERSECURITY AUDITS AND ADAPTIVE DEFENSE: A CASE STUDY ON FINANCIAL INSTITUTIONS." *Chief Editor*.
 38. Thangaraj, P. "The Hidden Costs of Cloud Security Based on Understanding Financial Implications for Businesses." *J Contemp Edu Theo Artific Intel: JCETAI-114* (2024).
 39. Torkura, K. A., Sukmana, M. I., Cheng, F., & Meinel, C. "Continuous auditing and threat detection in multi-cloud infrastructure." *Computers & Security* 102 (2021): 102124.
 40. van Ede, T., Khasuntsev, N., Steen, B., & Continella, A. "Detecting anomalous misconfigurations in AWS identity and access management policies." *Proceedings of the 2022 on Cloud Computing Security Workshop*. (2022).
 41. Verdet, A. "Exploring security practices in infrastructure as code: An empirical study." *Ecole Polytechnique, Montreal (Canada)*, (2023).
 42. Wen, J., & Ping, H. "PHOENIX: Misconfiguration detection for AWS serverless computing." *IEEE Transactions on Cloud Computing* (2025).
 43. Wen, J., Chen, Z., Zhu, Z., Sarro, F., Liu, Y., Ping, H., & Wang, S. "LLM-Based Misconfiguration Detection for AWS Serverless Computing." *ACM Transactions on Software Engineering and Methodology* (2025).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:

Nnadi, K., Okrah, Y. A. & Opoku, J. A. "Cloud Security Posture Management in Resource-Constrained Organizations: A Review of Azure, AWS, and Hybrid Approaches." *Sarcouncil Journal of Applied Sciences* 6.1 (2026): pp 9-21.