National College of Ireland

Hybrid Cloud Security Auditing: Enhancing Posture Through Integrated Use of Native and Open-Source CSPM Tools

MSc Research Project
M.Sc. Cybersecurity

Jacklyne Mbuthia
Student ID: X23318104

School of Computing
National College of Ireland

Supervisor: Mark Monaghan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Jacklyne Mbuthia

Student ID: X23318104

Programme: M.Sc. Cybersecurity **Year:** 2024-2025

Module: Practicum Research

Supervisor: Mark Monaghan

Submission Due Date: 15-09-2025

Project Title: Practicum Part 2- Research Project

Word Count: 8500 **Page Count** 25 everything inclusive

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: 

Date: 08-08-2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Hybrid Cloud Security Auditing: Enhancing Posture Through Integrated Use of Native and Open-Source CSPM Tools

Jacklyne Mbuthia
X23318104

Abstract

As cloud adoption accelerates, organizations increasingly adopt multi-cloud models, facing pressure to maintain strong security postures under constrained budgets. Cloud Security Posture Management (CSPM) tools play a critical role in identifying missing configurations, misconfigurations and compliance violations. However, many security teams cannot afford premium commercial CSPM solutions or paid tiers of cloud-native tools. The potential of hybrid CSPM approaches strategically combining open-source tools like Prowler with free tier of Microsoft Defender for Cloud (MDC) remains largely unexplored.

This thesis investigates the feasibility, effectiveness and strategic implications of a unified hybrid CSPM framework integrating Prowler with MDC's free tier. A Python-based deployment framework was developed to enable deployment and automation. The research evaluates complementary detection capabilities, operational overlaps and the scalability of hybrid CSPM across multi-cloud environments.

This study employs a mixed method approach combining systematic literature review, practical implementation and industry validation. Results show that hybrid CSPM architectures outperform single-platform solutions across several metrics. The unified framework demonstrates that Prowler and MDC's free tier offer significantly complementary capabilities, enhancing overall visibility and security coverage.

This research advances the development of unified CSPM models, leveraging the multi-cloud capabilities of both Prowler and Microsoft Defender for Cloud. It offers actionable insights for practitioners including tool section criteria, integration architectures and implementation roadmap. The proposed collaboration framework helps organizations optimize cloud security investments while ensuring broad protection across multi-cloud environments.

Keywords: Hybrid CPSM, Prowler, Microsoft Defender for Cloud, Unified Cloud Security Posture Management, Cloud Security Auditing

Table of Contents

1. Introduction 3
1.1 Motivation of The Study 3
1.2 Research Questions 4
2. Related Work 4
2.1 CSPM Definition, Tools & Capabilities 4
2.2 Cloud Managed CSPM Tools Vs Open-Source CSPM Tools 6
2.3 Adoption and Challenges 6
2.4 Cloud Security Auditing Challenges: 7
2.5 Literature Gaps and Research Justification 8
3 Research Methodology 9
3.1 Qualitative Research 9
3.2 Quantitative Research 9
3.3 Experimental Research 10
4 Design Specification 10
5 Implementation 11
5.1 Tool and Technologies Used 11
5.2 Implementation Flow 12
5.3 Questionnaire Administered 13
6 Evaluation 13
6.1 Results Visualization & Evaluation 14
6.2 Results Discussion 15
7 Conclusion and Future Work 18
Appendix 19
1.3 List of Abbreviations 19
1.4 Research Paper Summary: 19
References 22

1. Introduction

Cloud computing continues to transform how businesses operate in the digital age its adoption has become an indispensable IT strategy in companies of all sizes. The benefits it offers: scalability, reliability, enhanced productivity and performance, cost efficiency, enhanced security features and it being a catalyst for innovation make it a must have for businesses. Cloud computing services are leveraged through three main models: IaaS, PaaS and SaaS. The cloud security landscape is always evolving with cloud service providers (CSP) improving their services offering and the cloud service customers (CSC) leveraging more services for their operations across different CSPs.

Cloud security operates under a shared responsibility model where both the service providers and customers play a role in securing their estate The shared responsibility model defines the division of responsibilities between the cloud service provider and their customers based on the chosen service model type. With IaaS models, the bulk of security responsibilities falls on the cloud customer while in PaaS the responsibilities are shared more evenly and the cloud provider handles majority of the security responsibility in SaaS model. Although the shared responsibility model may vary slightly between CSPs, cloud customers are responsible for their data, managing client and endpoint protection and identity management across the three service models. The research paper is focused on cloud security from a cloud customers responsibility's perspective.

1.1 Motivation of The Study

As the cloud adoption rate increases, the attack surface expands which leads to an increase in cloud operations targeted attacks. According to (SentinelOne, 2025)," More than 79% of organizations use more than a single cloud provider, and the increasing complexity of multi-cloud environments leads to a rise in cloud misconfigurations". Some of the cloud security issues include: data breaches, poor IAM and weak configurations while some of the major threats include: account hijacking, insider threats, regulatory compliance, limited visibility, skills gap and evolving attack surface. (SentinelOne, 2025) reported that 80% of companies experienced an increased frequency in cloud security breach in 2024 attributing 15% of these attacks to failed audits. Cloud security audits help to stay ahead of the challenges. (Cambric and Ratemo, 2023) As companies grow, there's a need to make sure the IT controls for a company have been reviewed, adapted and equally applied and assessed to address the criticality of cloud services used

"Auditing is not an idea but a process" defined in ISP 19011 (N. Carter, 2003). Cloud security auditing plays a significant role in operations as effective audits enable organizations to benchmark against regulatory frameworks, validate their implementation of cloud security best practices and continuously monitor their cloud assets. This is done using CSPM tools. According to the WEF global cybersecurity report, while 78% of leaders from private organizations were of the opinion that cyber and privacy regulations effectively reduce risk in the organization's ecosystems. Two thirds of them cited the complexity and proliferation of regulatory requirements as a challenge (Jurgens and Dal Cin, 2025). Some of the compliance frameworks followed include: NIST, ISO 27017 & 27018, CSA STAR, and Cloud service provider well-architected frameworks. The frameworks and their mapping in cloud security audits are discussed in-depth in the implementation section.

Cloud security audit process is a combination of tools, techniques and people. This paper evaluates the collaboration of open source and cloud-native CSPM tools to improving cloud security posture:

- Cloud-native CSPM tools which are provided and managed by cloud service providers which are integrated in their own cloud environments i.e., Azure's Microsoft Defender for Cloud, AWS Security Hub and Google Cloud Security Command Center.
- Open source CSPM tools developed and maintained by open-source communities or individual contributors. i.e., Scoutsuite, Prowler and Cloudsploit.

(John Jonathan, 2023) One of the primary challenges in cloud security is the speed and scale at which resources are provisioned and configured. Traditional cloud native security posture management systems while powerful within their respective systems, often lack the flexibility, granularity or multi-cloud interoperability required to achieve unified security posture across heterogenous cloud operations. On the other hand, open source CSPM tools offer flexibility and community driven innovation but may struggle with scalability and enterprise grade support. This study is significant as it investigates the collaboration of the two toolsets.

1.2 Research Questions

This research paper aims to evaluate the tools and how a hybrid collaboration can be achieved for a granular cloud security posture and an improved cloud security audits process flow: The research will be answering the following questions:

- How can open-source tools be used in collaboration with cloud native tools to improve cloud security postures in multi-cloud environments?
- Can a unified CSPM deployment framework successfully orchestrate both tools simultaneously without compromising their individual capabilities?
- How do the tools complement each other? What is their granularity level and their integration capabilities?
- Is there a unified cloud security audit and assessment process flow in use for cloud security professionals?

A survey on the collaboration of the two set of tools will be conducted on a select group of cloud security engineers to evaluate their responses. A cloud environment on which the tools will be architected to evaluate their effectiveness. Findings obtained will allow for the evaluation of how their combined use enhances visibility, granularity, depth and clarity in cloud security audits, this research will support organizations adopting a more unified and effective cloud security audit strategies. Academically, the research contributes to the underexplored domain of CSPM tool interoperability offering a fresh perspective on tools synergy over isolated evaluation. Technically, the research equips security engineers, cloud security architects and cloud security engineering teams with evidence-based insights and integration processes that can improve the precision of how they achieve cloud security postures.

The following sections are organized into: Section 2 which delves into the literature review, Section 3 reviews the qualitative and quantitative methods used in support of this research. Section 4 demonstrates the practical implementation of this research's study and the results discussion and finally is Section 5 conclusion and future work section.

2. Related Work

Cloud computing has rapidly transformed how organizations handle technological operations, in doing so it also introduces complex security risks that necessitate robust posture management and continuous auditing. CSPM tools have emerged to address the challenges. This section synthesizes current academic research, industry research and empirical studies on CSPM tools. The review explores the tools used, key challenges faced in the adoption of CSPM tools, gaps that exist between native and open-source tools and cloud security auditing process.

2.1 CSPM Definition, Tools & Capabilities

Cloud security posture management (CSPM) is the continuous practice of monitoring cloud environments to detect and remediate misconfigurations, security risks and compliance violations. (Palo Alto Networks, 2015) Organizations use CSPM in public clouds and multi-cloud environments to reduce the likelihood of breaches and improve regulatory compliance. CSPM tools help organizations identify IAM issues such as over-privileged accounts, missing audit logs, missing MFA

and unrotated keys or passwords. Automated CSPM tools analyze large volumes of data across cloud services to detect hidden patterns and potential risks that might be overlooked manually.

(Kadar, 2023) reinforces this by detailing how CSPM tools such as Prisma cloud, AWS Security Hub and Trend Micro Cloud one offer features like real-time monitoring, automated remediation, compliance assessment and centralized dashboards. These features help manage risk across multi-cloud environments while improving visibility and alignment with standards such as PCI-DSS. This posture management practice employs a combination of techniques and tools to enforce cloud security and deliver the capabilities illustrated in the image below:

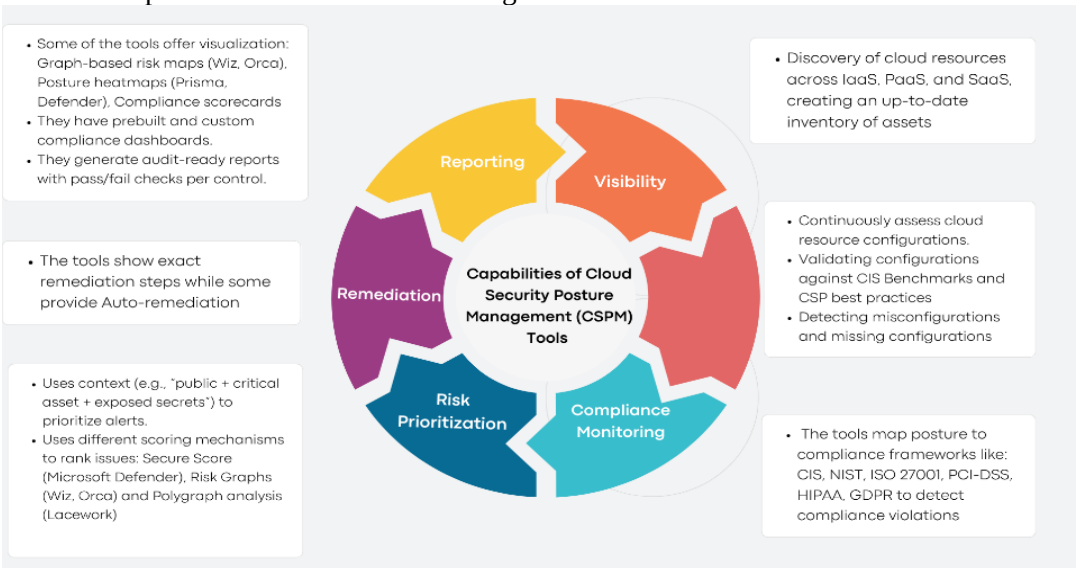


Figure 1:Cloud Security Posture Management Capabilities

As the technology landscape shifted to cloud computing, traditional security tools proved inadequate, prompting the emergence of specialized cloud security tools. CSPM tools are gaining prevalence as a critical component of cloud security strategies with organizations achieving reduced security risks, improved compliance and enhanced visibility from them issues that would otherwise pose severe reputational and financial consequences. (FNU Jimmy, 2023) regards cloud security posture management as a strategic approach that has emerged helping organizations proactively manage their cloud security posture. By automating risk detection and remediation, CSPM tools help reduce the manual effort required for security audits, allowing teams to focus on more strategic tasks. Rahman et al. (2024) empirical evaluation of CSPM tools yielded that leveraging CSPM tools for continuous monitoring and automated remediation significantly reduce cloud security incidents by 76% and misconfigurations by 63%. The authors emphasize on the operational efficiency gained, achieving a 40% improvement in response time and a 35% drop in critical incidents requiring manual intervention.

The current market of CSPM tools is evolving to keep up with the changing nature and exponential adoption of cloud operations. The CSPM tools used can be categorized into 3: Cloud-managed: AWS Security Hub, Azure's Microsoft Defender for Cloud, Google Security Center, Vendor-managed tools: Prisma cloud, Lacework, Wiz, Dome9, Check Point and Open-source tools: Prowler, Scoutsuite, CloudSploit. Different metrics are used to evaluate the CSPM tools to better influence the choice on which tool to work with. Some factors favoring the choosing of some tools include: A tool that provides a multi-cloud posture, granular coverage for cloud -native environments and agentless fast deployment.

Category	Tool	Clouds Supported	Risk Prioritization	Types of Findings	Compliance Standards	Remediation Guidance	Export Formats	Risk Scoring
Cloud Managed	AWS Security Hub	AWS only	Basic : AWS severity-based	IAM, network, S3, logging, compliance	AWS Best Practices, CIS AWS Benchmark, PCI DSS, NIST	Partial; linked AWS docs	CSV, JSON, CloudWatch	Basic severity score
	Microsoft Defender For Cloud	Hybrid+ AWS, GCP and Azure	Advanced: attack paths, workload context	IAM, containers, networking, workloads, compliance	Microsoft CSB, CIS, NIST, PCI DSS	Full: inline remediation, automation	CSV, JSON, Power BI	Contextual risk score
Vendor Managed	Wiz	AWS, Azure, GCP, OCI, Alibaba Cloud, VMware vSphere +	Advanced: context-aware, attack path analysis	IAM, misconfigurations, workload vulnerabilities, threat exposure	PCI DSS, HIPAA, SOC 2, GDPR, NIST, CIS	Full: automated workflows, integration	CSV, PDF, dashboards	Attack path + exploitability score
Vendor Managed	Prisma	AWS, Azure, GCP, OCI, Alibaba Cloud, IBM Cloud +	Advanced: risk engine and user behavior context	IAM, misconfigurations, vulnerabilities, misused identities	20+ standards incl. NIST, ISO 27001, CCPA, etc.	Full: detailed remediation steps + automation	PDF, CSV, dashboards	Comprehensive risk engine
Open-Source	Scoutsuite	AWS, Microsoft Azure, GCP, Alibaba Cloud, Oracle Cloud	None: rule-based only	Misconfigurations based on rules	It uses built-in rules inspired by real-world security incidents, vendor documentation (AWS, Azure, GCP), and common cloud security best practices.	Partial: manual remediation suggestions	JSON, HTML	None
Open-Source	Prowler	AWS, Azure, GCP + Kubernetes	None: basic severity	AWS/Azure misconfigurations, compliance gaps	HIPAA, GDPR, CIS, NIST, CSA, etc.	Partial:	CSV, JSON, HTML, Power BI	Basic severity rating

Table 1: Commonly used CSPM tools comparison

2.2 Cloud Managed CSPM Tools Vs Open-Source CSPM Tools

While all three categories of CSPM tools works towards the same objective, their level of effectiveness and granularity varies across the tools based on different factors. Vendor and cloud provider managed tools are rich in features but lack flexibility and are often expensive delineating some organizations. Rahman et al. (2024)**'s** cites that AWS Config, Microsoft Defender for Cloud and Prisma cloud are effective in compliance enforcement and anomaly detection. Open-source tools offer customizable frameworks, are free to use and cater to multi-cloud strategies. However, they are often limited in scalability and support.

Leauau et al. (2024) compares cloud -managed and open-source tools highlighting Defender for Cloud's native integration, attack path analysis, and compliance mapping. They also evaluate a custom solution using CloudQuery, NeonDB and Grafana noting its flexibility but limited visibility and integration. While their study details how each solution independently enhances cloud security posture, it concludes that neither solution is sufficient alone, a collaborative model would provide broader coverage and more granular insights. This aligns directly with the focus of this research. Similarly, (Hamid Ghazizadeh, Tamm and Reiner Creutzburg, 2024) work underpins the relevance of hybrid CSPM approaches by evaluating open-source tools (Nessus, a vulnerability scanning tool and Metaspoilt for exploitation) and Azure Security Center, each tool deployed independently plays a distinct role in cloud security audit pipelines.

While (Kadar, 2023) study provides a descriptive comparison of widely adopted tools such as Prisma Cloud and AWS config, it does not explore how these tools can integrated with open-source tools in a hybris setup, introducing a gap in implementation strategies for cloud security posture enhancement.

2.3 Adoption and Challenges

The adoption of CSPM tools hasn't been without challenges. While CSPM tools seek to help organizations improve their cloud security posture, some of the clouds, like Oracle lack support in most of the commonly used tools, which challenges organizations capabilities to achieved a unified security posture across multi-cloud environments. The lack of integration across cloud managed, vendor managed and open-source tools for a hybrid implementation results to using the tools in isolation. Cost and customizations of the tools also poses a challenge for most organizations. Rahman

et al. (2024) cites 38% organizational resistance to automation and 47% cost concerns as deterring factors to adoption of CSPM tools.

(Sharma H, 2020) work supports there's a challenge of tool interoperability being a barrier to achieving unified cloud security posture. Their work examines the effectiveness of CSPM tools in multi-cloud environments focusing on the operational challenges: the evolving cloud threat landscape, complexity of multi-cloud, changing regulatory requirements, and integration of CSPM tools with existing security infrastructure which limit the adoption of CSPM tools in organizations. The study proposes policy as code and SIEM/SOAR integrations as strategies to adopt. However, it doesn't delve into how cloud-native and open-source CSPM tools can be orchestrated together to enhance real-time posture visibility and compliance, a gap that this research seeks to bridge by exploring a hybrid approach.

2.4 Cloud Security Auditing Challenges:

Cloud security auditing plays a critical role but faces a complex set of challenges stemming from the dynamic, distributed and ephemeral nature of modern cloud environments, mapping to compliance, expertise and understanding of the shared responsibility duties. Hashizume et al. (2020) argues that cloud systems suffer from a lack of holistic and uniform security solutions due to diversity of services and architectures. This fragmented landscape necessitates CSPM frameworks that support interoperability and cross-platform visibility such as the hybris model proposed in this study.

Companies leveraging multiple service providers across IaaS, PaaS, and SaaS deployment models create a fragmented risk ownership which demands detailed audit strategies and provider-wide evaluations (Gupta, n.d.). This often renders traditional audits insufficient.
Hybrid auditing strategies that integrate open-source tools with CSP managed solutions offer greater flexibility and deeper control, but they also introduce operational overhead, data integration hurdles and the need for expertise to correlate findings. (Gupta, n.d.) addresses the need to evolve traditional audits processes, arguing that the relationship between auditing scope and compliance obligations is strongly linked to deployment models. The works presents that a comprehensive cloud audit checklist that details practical steps auditors can take to map compliance strategies to cloud operations.

(Gupta, n.d.) compliments (Rajesh Yalavaguli Seetharamarao, 2023) who emphasizes that one of the greatest challenges in auditing cloud environments is the lack of a unified approach that aligns with the diverse compliance expectations across the diverse regulatory frameworks. This fragmentation leads to inconsistent audit depth and scope across different CSPs further complicating organization's ability to maintain continuous security assurance. As evidence in notable incidents such as the Toyota's decade hack, where a misconfigured storage database bucket led to a data leak that affected 2.15 million customers dating back to 2012 or the Capital One's misconfigured AWS instance incident. Cloud security failures are often rooted in either misconfigurations or weak security practices. These cases underscore the critical importance of proactive auditing mechanisms.
Choosing the right framework to align cloud operations from the wide array of cloud security frameworks and standards is a challenge to most organizations. The frameworks vary widely in auditability, cloud specificity, and regulatory alignment while supporting different concerns: security & risk management, operational governance and regulatory compliance.

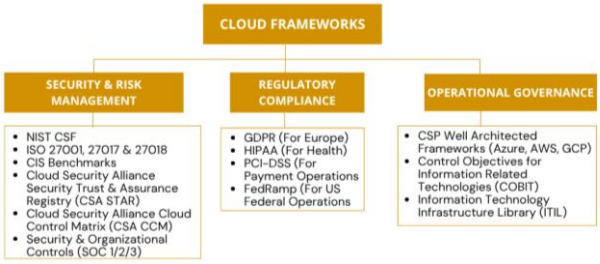


Figure 2: Cloud Frameworks Used

The regulatory framework complexity extends to cloud security audits as frameworks are foundational for CSPM tools. (Chauhan and Shiaeles, 2023) emphasizes that these inconsistencies make it difficult for organizations to implement frameworks consistently, especially when multiple tools or environments are involved. Their analysis found that even mature frameworks like COBIT 5 and ISO/IEC 27017 lack standardized regulatory mappings, hindering audit precision. This challenge directly impacts CSPM tools, which rely on framework mappings to perform compliance driven checks. The fragmentation underscores the need for unified, interoperable frameworks to improve cloud security audits and support seamless tool integration. Without this alignment, collaborative CSPM approaches risk generating incomplete or conflicting assessments of cloud security posture.

Framework	Primary Focus	Scope	Implmentation Approach	Audit/Certifiable	Cloud-Specific	Mapping/Interoperability
CSP Well-Architected Frameworks	Architecture best practices (security, cost, performance)	Cloud infrastructure & operations	Prescriptive	No formal certification	Yes	Limited; aligns loosely with general best practices
CSA STAR	Assurance, transparency, certification of cloud providers	Cloud service providers	Risk-based + maturity levels	Yes (Levels 1-3)	Yes	Built on CSA CCM, maps to ISO 27001
NIST CSF	Cybersecurity risk management	Enterprise-wide: IT/OT/cloud	Risk-based	No formal certification	Cloud-adaptable	Maps to ISO, COBIT, NIST 800-53
ISO/IEC 27001	Information security management systems	Organization-wide	Prescriptive	certifiable	Cloud-applicable	Forms base for 27017 & 27018
ISO/IEC 27017	Security controls for cloud services	Cloud services both the provider + customer	Prescriptive	Guidance only (not certifiable alone)	Yes	Extends ISO 27001
ISO/IEC 27018	Privacy in cloud environments	Protection of PII in cloud	Prescriptive	Yes, tied to ISO 27001	Yes	Extension of ISO 27001
CIS Benchmarks	Hardening guides	Cloud platforms, OSs, DBs, etc.	Prescriptive	No	Yes	Maps to NIST, CSA CCM
CSA CCM	Cloud-specific control framework	17 domains covering cloud security	Control-based	No (but used in STAR)	Yes	Maps to NIST, ISO, PCI DSS, COBIT
SOC 2	Trust service principles (security, availability, confidentiality)	Service organizations (incl. cloud)	Audit-based	Yes (via CPA audit)	Yes (general)	Aligns loosely with ISO and NIST

Table 2: Cloud Compliance Standards Comparison

(Sharma H, 2020)'s study supports that, limited resources and expertise impacts the effective implementation and management of CSPM tools proposing for organizations to leverage managed security services, invest in their security teams or use automated tools. The human element in cloud security can viewed from two views: security misconfigurations introduced by humans and expertise needed to secure the systems. Personnel responsible for cloud operations need to be skilled to securely deploy resources, create secure processes for handling cloud security process and utilize tools to evaluate and strengthen the security posture. (Taha, Ramo and Alkhaffaf, 2021) presents an evidence-based evaluation of the impact of external auditor–cloud specialist engagement on cloud auditing highlighting the need for external auditors to collaborate with cloud security specialists when performing cloud security audits. Their research highlights that non cloud security and cloud computing savvy auditors had a harder time auditing cloud operations as compared to using cloud security auditors or having a collaboration of auditors and cloud security skilled professionals.

2.5 Literature Gaps and Research Justification

While existing academic literature and industry research addresses the strengths of both cloud-native and open-source CSPM tools, the reviewed studies fall short of a technical implementation that has a

unified collaborative approach that integrates the two for cloud security auditing purposes. This underscores the need for research that operationalizes hybrid models for deeper audit coverage, posture visibility and tool synergy, an area this paper seeks to explore**.** While Hashizume et al. (2021) presents a comprehensive categorization of cloud security threats, their study like many others stop short of proposing a concrete implementation of strategies for CSPM interoperability. This highlights a significant research gap in this thesis.

This study builds on (Leaua et al., 2024)'s work which focuses on evaluating two CSPM tools; Both plans of Defender for Cloud for Azure resources and a custom open-source CSPM tool built on AWS using Grafana and CloudQuery for AWS resources. The work sets the foundation for evaluation of CSPM tools in the cloud. The two tools are evaluated both independently and a comparison of both is done. This study goes the extra step to build on (Leaua et al., 2024) future work proposition for a hybrid CSPM tool. (Paidy & Chaganti, 2025) presented an audit driven CSPM framework integrating both AWS and Azure native tools with open-source tools like Cloud Custodian. Their findings support the growing trend towards hybrid models, a direction that this research builds on by focusing on Prowler and Microsoft Defender for Cloud.

3 Research Methodology

This chapter presents a methodological framework adopted for this study. The research employs a mixed-method approach. The methodology integrates qualitative insights, quantitative data and hands-on experimentation to provide a multi-faceted understanding of CSPM tools and their interoperability. The practical demonstration will serve as empirical evidence to support this research's hypothesis on the benefits of hybrid CSPM approaches.

3.1 Qualitative Research

The qualitative research was conducted through an in-depth review of academic literature works, industry research, technical standards, cloud security best practice guidelines and publication. The sources used include: previous literature review dating back to 2021, e-books, cybersecurity reports and online articles. The literature review focused on:

- The evolution of CSPM tools
- The distinction between native and open-source platforms
- Audit and compliance challenges in cloud security
- Existing models and frameworks that inform posture management.

The thematic analysis supports the development of the research's theoretical framework aiming at building a conceptual understanding of CSPM tools, identify their limitations and reveal research gaps to integration and interoperability. The qualitative research informs the design of the hybrid implementation model.

3.2 Quantitative Research

The quantitative research involved the design and deployment of a structured survey distributed to cloud security practitioners across various industries. The survey includes both closed and open-ended questions, categorized into five sections:

- The participants background
- Tool usage; native and open source
- Tool collaboration and integration practices
- Cloud audit frequency and priorities
- Posture management effectiveness and recommendations.

The data collected from the survey will be analyzed using descriptive statistics to identify trends, effectiveness of CSPM tools and practitioners' perspective on the value of hybrid CSPM implementations. The results will be used to triangulate findings from the literature and experimental implementation.

3.3 Experimental Research

To validate the practical feasibility and effectiveness of a Unified Cloud Security Auditing Framework (UCSA), the experimental aspect focuses on a manual implementation of a hybrid CSPM model within a controlled Microsoft Azure environment**.**

4 Design Specification

This section outlines the design specifications of the Unified Cloud Security Audit (UCSA) framework proposed in this research that aims to combine the strengths of cloud-native and open-source CSPM tools to achieve comprehensive and granular cloud security posture. The architecture is based on a comparative multi-tool audit model that integrates findings from Microsoft Defender for Cloud (MDC) and Prowler. Building on the modular architecture proposed by (Paidy & Chaganti (2025), this study leverages Prowler for its granular AWS audit capabilities alongside Defender for Cloud's deep integration within Azure, thereby enhancing cross cloud security posture through a hybrid CSPM strategy.

Prowler is an open-source cloud security posture management tool. It has support for hybrid and multi-cloud environments; Azure, AWS, Kubernetes and Google GCP. It's agentless, so it's easily integrated into existing environments. It evaluates compliance against industry standards such as CIS, NIST CSF, NIST 800, PCI_DSS, GDPR, SOC2, MITRE ATT&CK, CISA, FedRAMP and Cloud service providers benchmarks. Microsoft Defender is a Microsoft managed CSPM tool. It spans multi-cloud environments; Azure, AWS and GCP. It maps workloads to Microsoft Cloud Security Benchmarks as the compliance standard. It's available in two plans; A Foundational CSPM, which is the free plan and Defender CSPM the paid plan (dcurwin, 2025). This implementation utilizes the foundational CSPM.

This design leverages automation and multi-tool integration to enhance visibility and compliance alignment. To achieve the hypothesis of this research, the image below shows the design implementation model of this research. The architecture diagram of the hybrid CSPM implementation:

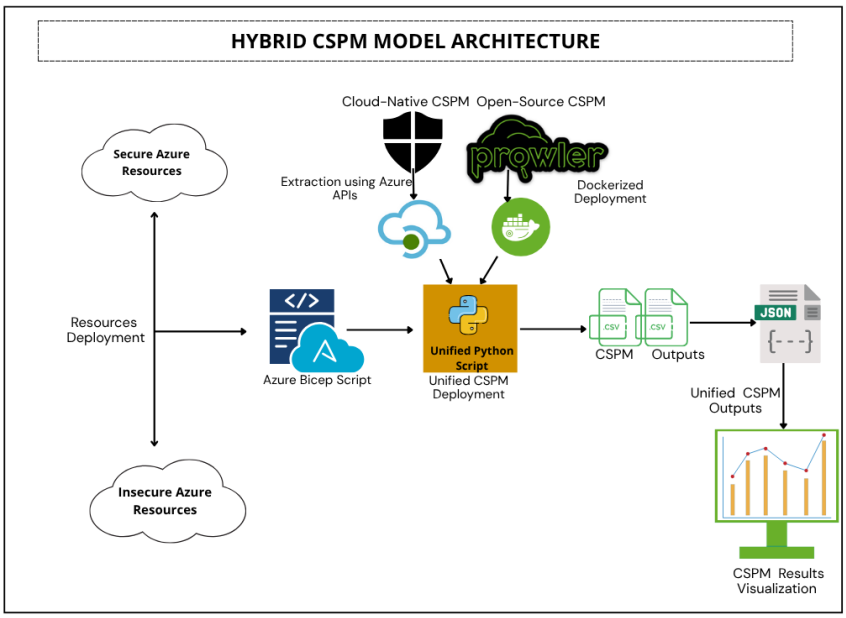


Figure 3: Design Model - Hybrid CSPM Model

The initial architecture diagram as illustrated in Figure 3, was not fully successful as detailed in the implementation section of this study. The approach that was used is discussed in the

implementation section and the revised diagram of the hybrid CSPM implementation is illustrated in Figure 4.

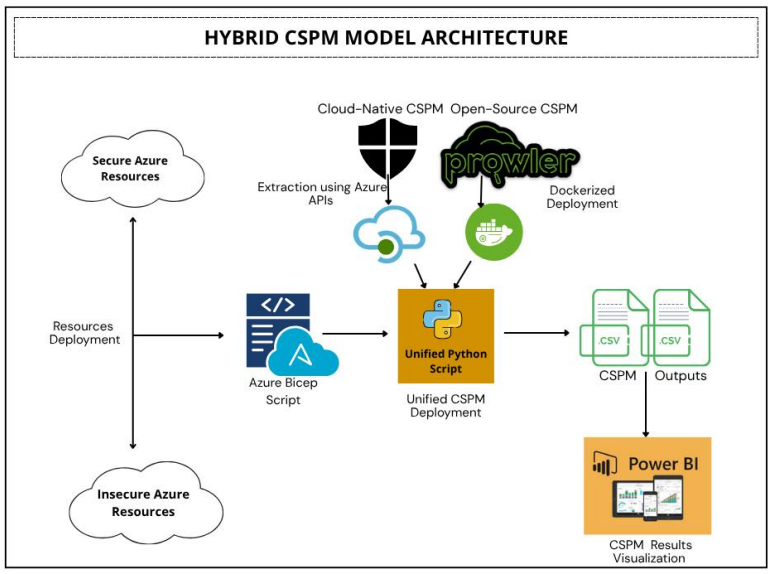


Figure 4: Revised Design Model - Hybrid CSPM Model

The underlying framework has a 3 layered approach:

- The Assessment Layer: which consists of individual audit tools that collect findings on cloud misconfigurations, security risks and compliance gaps. Each of these tools operates independently on the same Azure environment. The tools are deployed using a unified python script.
- The Data Consolidation Layer: The output from the two tools is normalized and aggregated into a central reporting format; CSV and HTML. A structured criteria is used to compare the tool's findings in terms of coverage, risks scoring, remediation guidance and alignment to industry standards.
- The Evaluation and Reporting Layer: This component maps findings to compliance controls, analyzes overlaps and gaps across tools and presents the insights visually using Power BI dashboards.

This research proposes a model for cross-tool audit synthesis. This model outlines how multiple CSPM outputs can be integrated and analyzed to improve accuracy and visibility.
The core requirements that informed the framework design include:

- Support for Azure cloud environments
- Compatibility with industry-recognized benchmarks like CIS and NIST.
- Availability of structured output formats
- Automation potential for continuous audits

5 Implementation

The UCSA framework was implemented by auditing a simulated Azure environment using Microsoft Defender for Cloud and Prowler. The final stage of implementation focused on collecting and analyzing outputs, generating insights and evaluating tool performance based on predefined criteria.

5.1 Tool and Technologies Used

- Cloud Platform: Microsoft Azure was used to deploy the simulated environment. Azure for Students subscriptions was used.
- Audit tools:

    - Microsoft Defender for Cloud – native security recommendations and regulatory compliance data
    - Prowler- Open-source CLI based CIS benchmark scanner
- Development and Execution
    - Azure Bicep as Infrastructure as Code for deploying the blend of secure and insecure resources
    - Python script for unifying the deployment of the tools.
    - Azure CLI – for authenticating and managing Azure resources
    - Bash Shell- for executing scanning commands and handling outputs
- Data Analysis and Visualization:
    - Power Bi- for developing interactive dashboards summarizing the results.

5.2 Implementation Flow

1. Resources Deployment: A blend of secure and insecure resources are deployed suing Azure Bicep.
2. Script Deployment: The unifed_cspm.py has 3 phases to it
    a. Security assessment via Prowler: The script launches a docker container running the prowler CLI. An authenticated service principal is used to secure access. The output is generated in JSON, CSV and HTML formats for flexible reporting and visualization.
    b. Security assessment via Microsoft Defender for Cloud: Authentication to Azure is achieved using Azure SDKs from the Azure CLI. The SDKs retrieve security assessments focusing on the severity, risk factors, resource metadata details.
3. Execution Trigger:
    a. Manual Execution: The unified_cspm.py script runs immediately when invoked.
    b. Scheduled Execution: A scheduling mechanism is used to trigger it to run on the 14th of each month at 9:00am. This move is so as to achieve a monthly security posture.
4. Results & Visualization:
    a. Data Integration: The outputs from Prowler and Defender are merged into a unified JSON file, unified_results.json. The script also preserves individual CSV results of the tools for use in Power Bi for visualization. The reports contain security misconfigurations, policy violations and compliance gaps.
    b. The CSV files are loaded and transformed into Power to clean them up before performing the visualization analysis. The PowerBi boards are static not real-time. In future, real-time boards would be used.
5. Automation Cycle: The initial run occurs immediately if the current date is not the 14th. Subsequent runs are triggered automatically each month on the scheduled date.

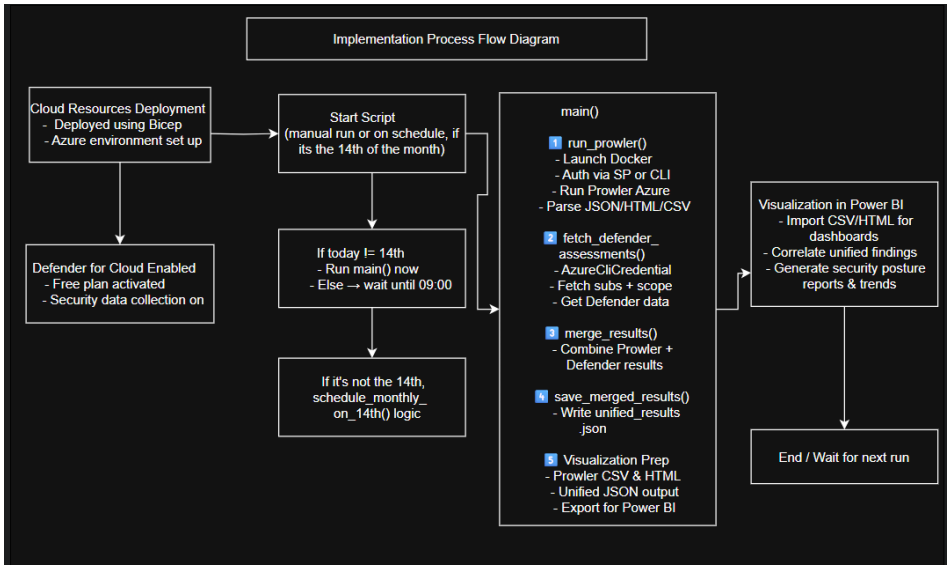


Figure 5: Implementation Process Flow

5.3 Questionnaire Administered

A structured questionnaire was created using Google Forms to collect insights from cloud security professionals and consultants. The survey aimed to assess their perception around the effectiveness, usability and limitations of combining cloud-managed CSPM tools like Microsoft Defender or Hub for Cloud or AWS Security and Open-Source SPM tools like Prowler or Scoutsuite. It included both closed-ended and open-ended questions focused on tool familiarity and audit reporting preferences. The form was shared to a subset of 10 cloud engineers; juniors new to the field with <1 year experience, 3-5 years experiences engineers and 5+ experienced engineers. Each of the groups offered a different insight into how they use CSPM tools, what they hope different and how the tools can be improved to enable them execute their duties diligently. The responses were collected for analysis in the Results and Evaluation phase.

This implementation validated the UCSA framework by demonstrating how hybrid tool usage can improve cloud security audit depth. The next section presents the findings from the survey and the experimental implementation evaluating the success of the hybrid CSPM collaboration model.

6 Evaluation

This section evaluates the findings from the practical implementation of the Unified Cloud Security Audit (UCSA) Framework, integrating both open-source, Prowler and cloud managed CSPM, Microsoft Defender for Cloud across a hybrid deployment of secure and insecure resources in Azure. The section also incorporates insights derived from the targeted survey assessing real-world CSPM tool usage by cloud practitioners. The practical implementation of the hybrid model achieved in three phases:

- Phase 1: Resource deployments in Azure cloud were successful
- Phase 2: A python script that unifies the deployment of Prowler and MDC was successfully initiated.
- Both Prowler and MDC produced their respective security assessment outputs in CSV format, albeit individually. While the framework aimed to unify not only tool execution but also result generation into a single consolidated output, attempts to merge the outputs into one CSV proved suboptimal. The unified file lacked clarity due to inconsistencies in result formatting and metric categorization across tools. This technical limitation highlighted the complexity of standardizing outputs from heterogenous tools and pointed to an area needing further fine-tuning.

- Phase 3: The objective was to generate unified results in a json format. However, the results output fell short of the objective, shining light on the need for the development of a results synthesis engine in future that has a standardized results schema.

6.1Results Visualization & Evaluation

The results were inspected and evaluated in two ways; a manual review of the CSV files generated and a visual analysis using Power Bi. The manual inspection allowed for the quality of results be inspected, allowing for the identification of similar fields across both tools albeit different names that capture the severity of the risks, the risks identified, affected resources, remediation steps. This section captures the visualization boards done on the CSPM tools to better evaluate them. The boards were useful in understanding how the two CSPM tools work from a visual perspective.

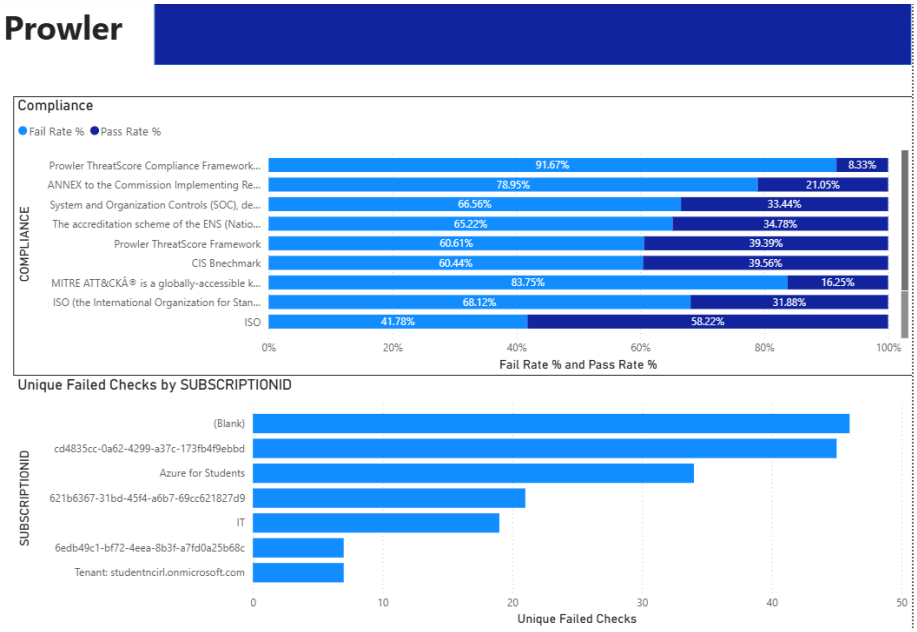


Figure 6: Prowler - Power Bi Visualization

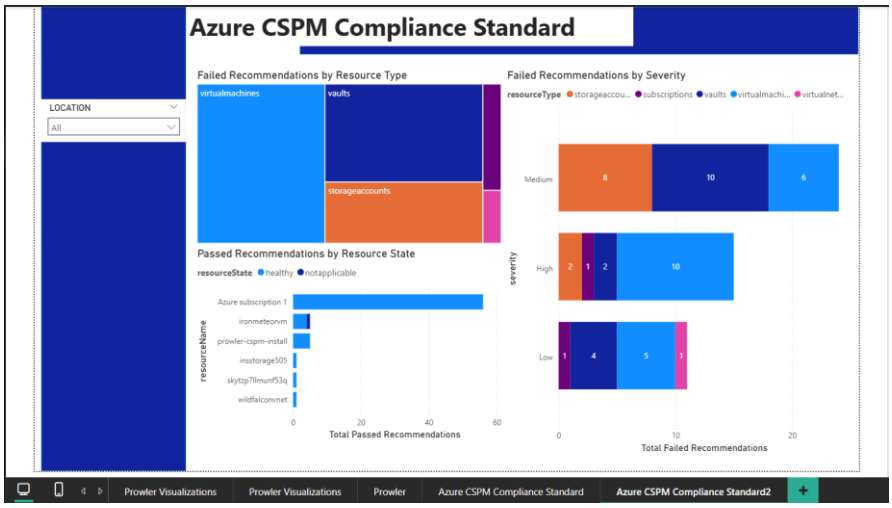


Figure 7: Cloud Managed MDC- Power Bi Visualization

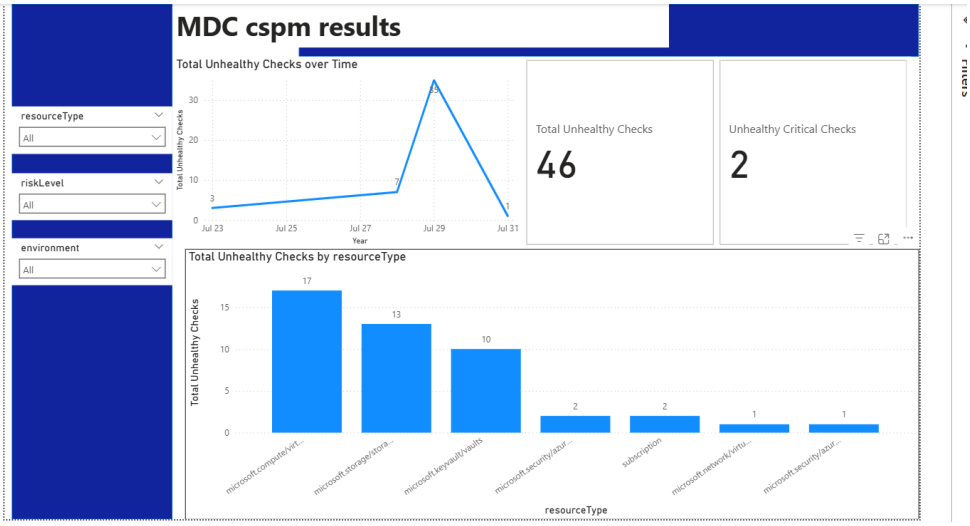
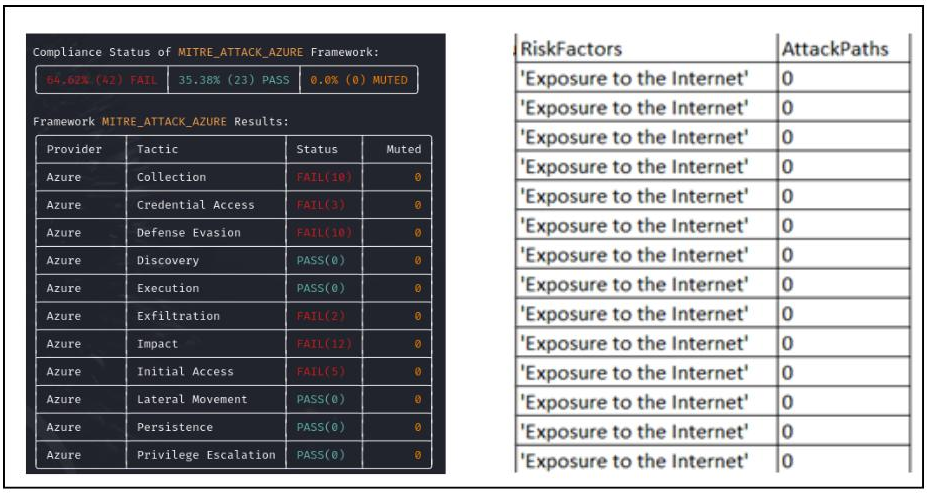


Figure 8: Cloud Managed MDC- Power Bi Visualization -2

6.2 Results Discussion

Despite the lack of a unified output file, the individual CSVs enabled rich visual analysis Power BI. Visualizations demonstrated several key insights:
Prowler's strengths:

- Remediation: Prowler's remediation process flow was more granular than MDC. and included a description on whether, the feature was enabled on default or users had to enable it themselves alongside reference links for further reading.
- Compliance: Prowler offers a wider selection of compliance frameworks, enforcing granular compliance as organizations can evaluate their operations against based on their cybersecurity strategy ensuring that they have visibility over all their compliance posture.
- Customization: Prowler is customizable to run specific checks, scan specific regions or services and also produce the outputs in the specified preferred formats.
- Deployment: Prowler is easy to deploy in ephemeral environments using docker making it lightweight.
- Usability: It's ideal for manual audits, custom scripts and is easy for teams of all skillset levels to work with.
- Attack Surface Metrics: Prowler also offers a MITRE ATT&CK analysis, while MDC that can only be achieved using the paid plans. The free plans, 'Attack Path' output that field in the CSV file as an empty column as shown in Figure 8.



Compliance Status of MITRE_ATTACK_AZURE Framework:

64.62% (42) FAIL	35.38% (23) PASS	0.0% (0) MUTED

Framework MITRE_ATTACK_AZURE Results:

Provider	Tactic	Status	Muted
Azure	Collection	FAIL(10)	0
Azure	Credential Access	FAIL(3)	0
Azure	Defense Evasion	FAIL(10)	0
Azure	Discovery	PASS(0)	0
Azure	Execution	PASS(0)	0
Azure	Exfiltration	FAIL(2)	0
Azure	Impact	FAIL(12)	0
Azure	Initial Access	FAIL(5)	0
Azure	Lateral Movement	PASS(0)	0
Azure	Persistence	PASS(0)	0
Azure	Privilege Escalation	PASS(0)	0

RiskFactors	AttackPaths
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0
'Exposure to the Internet'	0

Figure 9: CSPM Tools- MITRE Specification Comparison

Defender for cloud's strengths: Some of the favouring factors for MDC as a CSPM tool are that:

- Realtime: the checks are conducted in real-time, as more resources are deployed the secure score is updated**.** This is shown in Figure 7: Cloud Managed MDC- Power Bi Visualization -2
- Built-in recommendations: MDC has actionable recommendations based on Azure security benchmark standard
- Auto fix feature: Some of the recommendations proposed can be auto-remediated using Policy as code.
- Multi-Cloud capability: MDC's free plan offers a unified dashboard for integration of other clouds using connectors. It integrates to AWS and GCP clouds offering Multi-cloud CSPM capabilities. This makes it an attractive tool for security teams aiming to unify operations.

Overlapping features:

- Compliance: Both utilised compliance standards to evaluate the cloud deployments. However, the granularity of the standards differed.
- Multi-Cloud visibility; both tools serve multi-cloud environments.
- Recommendations: Both tools offer security recommendation, differing in the depth of the recommendations.

Gaps identified: some of the gaps identified include:

- Quality of recommendations: MDC offer abstracted recommendations while recommendations from prowler were granular detailing not only the step by step but also the nature of recommendations, if any of the control is enabled by default or not. Which enables the security teams of all technical skills levels from juniors to remediate any arising issues and understand cloud security better.
- Extra Features: Some features missing in MDC's free plan like attack paths, were covered in Prowler's MITRE ATT&CK check that defined the security issues as per the MITRE ATT$CK process flow.
- The real-time continuous assessment feature missing in Prowler which only calculates the security posture on runtime. Prowler allows for automation and to be run on schedules, introducing extra overhead effort while with MDC that's an inbuilt functionality
- Auto fix feature: While both excel at detection issues, MDC has a partial auto fix capability supported by Policy as Code, which is missing in Prowler. This sets the foundation for features that future hybrid CSPM tools that integrate AI into the remediation process would consider.
- Compliance Depth: MDC offers limited compliance standards to align with; Microsoft cloud security benchmark, azure CSPM, CIS Azure Foundations v2.0 and v3.0 while Prowler offers

CIS 2.0, 2.1, 2.3, ISO_27001-2022, MITRE ATT&CK, PCI DSS 4.0, SOC2 and a prowler_threatscore standards to work with.

- Customization: MDC is limited to built-in recommendations while Prowler allows for fully customizable rules and check.

Survey results reinforced the practical significance of the hybrid approach. The 43.8% used 87.5% of surveyed cloud practitioners reported using only a cloud CSPM tool as shown in figure 9:40.9% used a blend Scoutsuite and Prowler open CSPM tools as shown in figure 10: The professionals cited factors such as cost, deployment complexity and a lack of interoperability between tools as the primary barriers to adopting multiple solutions. 75% of respondents indicated a desire for unified CSPM deployments and scalability across multi-cloud environments, highlighting a clear gap in the current tool landscape. 40.9% of the professionals indicated using multiple CSPM tools while conducting CSPM tools; a combination if Prowler, Scoutsuite, Cloudsploit and a manual inspection of the cloud-managed CSPM tool, citing how it can sometimes be tedious to keep going back and forth through the tools and the time consumed. The professionals underscored the significant impact of CSPM tools in cloud security auditing tasks expressing the openness to implementing a hybrid CSPM model in their organisations.

The survey also revealed that the challenges for adoption of CSPM tools included; Unified deployment which the use of a unified python script implemented in the research caters to and tools efficiency and defining what compliance standard to align with. The other challenge identified was the scalability to multi-cloud environments with cloud practitioners acknowledging their growing cloud security operations to multi-cloud deployments. The practical implementation of this research argues that this hybrid CSPM model is scalable to multi-cloud environments as both MDC and Prowler allow for integration of multi-cloud environments; AWS and GCP. Furthermore**,** two thirds of survey respondents cited the cost of CSPM tools as a significant cost concern for their organisations especially smaller organizations with leaner budgets. This research's implementation utilises open-source and free plan version of CSPM tools vouching for that free CSPM tools can deliver on achieving a granular and effective cloud security posture.

The study develops a cloud standards comparison matrix that can be used to identify the right compliance framework for the organisations. The use of the cloud compliance matrix alongside (Gupta, n.d.)'s proposed cloud security audit checklist contributes to an improved cloud security auditing process, harmonizing the process. The visual insights from the tools confirmed the hypothesis that no single tool provides a comprehensive view of cloud risk posture. Instead, hybrid deployment can amplify visibility and context by balancing the best of both open-source and cloud native CSPM tools; MDC's breath with Prowler's depth. The findings from this research align with Leauau et al. (2024) view that a hybrid model allows for more value and an improved cloud security posture as compared to using the tools independently.

Overall, the UCSA framework demonstrated the feasibility of deploying integrated CSPM tools while surfacing the challenges related to unified output generation and standardization. The implementation successfully implemented a unified script, data aggregation and visualization features of a hybrid CSPM tool. This discussion affirms that while tool integration is technically achievable, true operational unification especially at the results level remains a challenge requiring tooling innovation and results schema harmonization across the tools. (Paidy & Chaganti, 2025)'s validates this study's implementation, that no single native tool provides full multi-cloud posture visibility. Both papers recommend hybrid models for broader coverage.

7 Conclusion and Future Work

This research proposed and evaluated the unified cloud security audit (UCSA) framework, a hybrid approach to CSPM that integrates cloud-native and open tools working with Prowler and Microsoft Defender for Cloud's free plan to enhance granular cloud security posture through complementary capabilities. The framework was implemented through a unified python script deploying the CSPM tools and the results visualized in Power Bi supplemented by feedback from industry practitioners.

The findings obtained affirm that a hybrid CSPM model is operationally viable and can yield richer insights than using either tool alone. The UCSA framework surfaces actionable security posture data, uncovered configuration gaps and emphasized the strengths of each tool in a parallel comparison. It also highlighted a pressing need for standardized reporting formats, cross-tool output normalization and interoperable security scoring models to achieve a truly unified analysis experience. The survey findings further validated the relevance of this work. Many practitioners till rely on single-tool setups, constrained by cost, complexity and perceived redundancy. However, a growing number recognized the value proposition of hybrid CSPM, especially for multi-cloud deployments and external audit readiness. Hybrid CSPM models bridge cloud-native platform limits with deep custom tooling. It improves multi-cloud readiness and supports technical auditing, compliance tracking and decision making.

Future work can build on this research in several key areas:

- As CSPM solutions evolve, integrating threat intelligence feeds and SIEM/SOAR pipelines as recommended by (Paidy & Chaganti,2025) presents a promising avenue to extend this hybrid architecture into a proactive, intelligent and automated cloud security fabric.
- Output normalization layer; developing a translation engine that ingests diverse CSPM outputs and produces a standardized, unified report schema.
- Multi-cloud extension: expand the framework beyond Azure to include AWS and GCP cloud environments using the Microsoft defender for cloud multi-cloud integration feature.
- Machine learning and AI integration: Integration of basic ML models for fine tuned alert prioritization and AI for automated remediation process of issues identified as critical and high-risk severity.
- A cost benefit analysis; to quantify the ROI of using a hybrid CSPM setup, factoring in human effort, tool licencing and risk reduction metrics.
- Automation: The automation of the integrated CSPM python script to run based on the cloud practitioner's frequency of choice; every 2 weeks, or monthly. Future research explores the possibility of integrating AI into remediation process of issues identified.

In conclusion, this study contributed a replicable cost-effective framework that lays the groundwork for future CSPM toolchains capable of providing holistic, cross-cloud and collaborative security audits. As the cloud ecosystem becomes more complex, the rise of AI expanding the threat landscape, such hybrid approaches will be pivotal in securing infrastructure while maintaining operational efficiency.

Appendix

1.3 List of Abbreviations

CSC: Cloud service customer
CSP: Cloud service provider
CSPM: Cloud Security Posture Management
JSON: JavaScript object notation
HTML: Hypertext markup language
CSV: Comma separated values
UCSA: Unified Cloud Security Auditing Framework
CLI: Command line interface
AWS: Amazon web services
GCP: Google cloud platform
IAM: Identity and Access Management

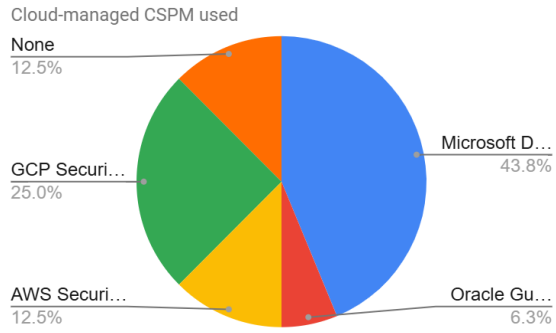


Figure 10: Cloud Managed CSPM Tools Used

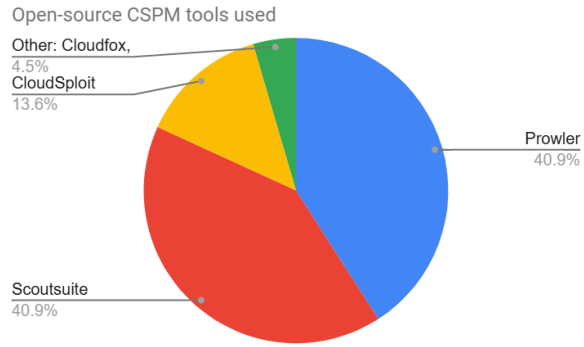


Figure 11: Open-source CSPM Tool Used

1.4 Research Paper Summary:

Reference	Focus	Methodology	Shortcoming/Contribution
Kadar, Abas. (2023).	This paper explores the key tools and approaches available to enhance cloud security, focusing on the features, benefits, and strategies that organizations can implement to safeguard their cloud against evolving threats	The paper is conceptual in nature. It relies on secondary research to review existing tools, frameworks, features and industry examples to provide a landscape of CSPM usage and its benefits	The research lacks empirical data or testing. It talks about the CSPM tools tool features, but doesn't conduct any tool performance comparison. The CSPM tools are considered independently, interoperability isn't explored
Hashizume et al. (2020)	The paper provides a systematic categorization of security challenges in the cloud. It analyzes academic publications to identify gaps in holistic, automated and continuous cloud security monitoring.	It uses a systematic literature review of a dataset of 106 selected papers.	The paper is contextual, it classifies challenges but does not evaluate or test any security tools or architectures to simulate the threats.
(Chauhan and	This research is focus on the	This study conducts a	This study lacks depth. It does not go

Shiaeles, 2023)	evaluation of the various frameworks, assisting in making educated decisions about selecting and implementing suitable security measures for cloud-based systems.	literature review and a contextual analysis of each cloud related frameworks mentioned	in detail to outline how different standards can be applied to different environments, based on their scope and objectives. It serves as a knowledge hub painting the picture of the existing frameworks and their advantages.
(Leaua et al., 2024)	The study explores CSPM solutions, analyzing (two paid plans of Microsoft Defender) on Azure and an open-source alternative solution (custom CloudQuery CSPM on AWS Cloud resources). This comparison provides insights to understand their respective advantages and disadvantages to determine which solution is more suitable for specific cloud environments.	This study utilizes a mixed method approach; a literature review, and a practical implementation of the individual CSPM tools in their respective cloud environments.	The study analyses two implementations of CSPM tools independently, setting the foundation for the exploration of a hybrid CSPM tool aligning with this paper's objective.
(John Jonathan, 2023)	This article explores the range of tools available for effective cloud security posture management, evaluating their features, functionalities, and how they contribute to securing multi-cloud and hybrid cloud infrastructures.	A textual analysis of major CSPM tools used, evaluating their features and functionalities.	
(FNU Jimmy, 2023)	This paper explores the evolving landscape of CSPM, highlighting tools and techniques used. It discusses cloud-native security services, third-party CSPM solutions, and artificial intelligence-driven automation. Developing an AWS focused CSPM tool capable of advanced threat detection, proactive monitoring, and real-time misconfiguration alerts.	It uses a mixed method approach: Systematic Literature Review, Comparative Analysis of CSPM Tools case studies & practical implementation and Data analysis	The CSPM tool designed caters to an AWS environment and does not scale to other cloud environments
Elizabeth Oluwagbade, 2025	presents a framework for evaluating cloud security in multi-cloud and hybrid environments delving into methodologies that are used to benchmark across diverse architectures, the security metrics considered and the best practices for securing multi-cloud and hybrid cloud.	A literature analysis of the benchmarking methodologies used for multi-cloud and hybrid cloud security architectures	She compares the frameworks (Zero trust, CSPM and shared responsibility), standards (NIST, ISO 27001, GDPR & HIPAA), tools and strategies organizations can evaluate to develop a standardized approach to cloud security benchmarking.
Gunjan Gupta, 2022	Their research presents a comprehensive cloud audit checklist that details the practical steps auditors can take to map compliance strategies to cloud operations.	A combination of qualitative and constructive research methodology was used.	The study develops a cloud security audit checklist to be used by cloud security professionals in the execution of their tasks. The paper does not show the implementation of the audit in a real cloud audit in a real cloud environment.
(Sharma H, 2020)	The paper presents strategies for effective CSPM implementation. It delves into future directions in CSPM, highlighting emerging trends like AI integration, zero trust architecture, and advancements in compliance automation.	It uses a combination of literature review, applying mathematical modeling to evaluate CSPM efficiency and analyzing case studies	The paper serves as a knowledge hub analyzing effectiveness of current CSPM solutions in managing security across diverse cloud platforms and case studies on the implementation of CSPM in real life.
(Rajesh Yalavaguli Seetharamarao, 2023)	The work observes the gap in fragmented cloud security audit and proposes a unified strategy detailing auditing procedures to be adopted while auditing cloud environments building on the recognized cloud	The research method for this study focuses on research on professional literature	This paper serves as a knowledge hub identifying cloud security breaches, legal guidelines that impact cloud computing and proposed audit considerations for a unified auditing strategy

	compliance frameworks.		
(Rahman, A., Md Ashrafuzzaman, Jim and Sultana, R., 2024).	This study explores the effectiveness of CSPM tools in cloud computing	Through a mixed-method approach, combining a comprehensive literature review, a survey of IT security professionals, and detailed case study	This research provides a robust evaluation of CSPM tools' capabilities, the challenges associated with their implementation and identifies critical barriers to CSPM adoption
(Hamid Ghazizadeh, Tamm and Reiner Creutzburg, 2024)	Presents an analysis of automation tools used, evaluating Azure CSP - native (Microsoft Defender) and open-source tools (OpenVAS and Metasploit). They examine the tools' role in improving security posture through automation, vulnerability detection and penetration testing in multi-tenant	Through a mixed-method approach, combining a comprehensive literature review, a technical implementation of the tools to better review their capabilities	Their work focuses on automated penetration testing, mapping OWASP API issues and enumerating cloud API vulnerabilities using cloud native and open-source tools and not on cloud security auditing. Their research shows other powerful capabilities of the tools.
(Paidy & Chaganti, 2025)	This study proposes an audit driven Cloud CSPM tool. Which proposes a robust architecture integrating both native tools (like AWS Config, Azure Policy) and third-party tools (OPA, Cloud Custodian).	This study utilizes a mixed method approach; a literature review, and a practical implementation of the custom audit driven CSPM tool	An audit driven CPSM tool is deigned setting the foundation for this study, a chance to compare the execution of a custom built cspm tool alongside this paper's implementation of a cloud managed vs open-source tool implementation
(Sharma H, 2020)	The paper presents strategies for effective CSPM implementation. It delves into future directions in CSPM, highlighting emerging trends like AI integration, zero trust architecture, and advancements in compliance automation.	It uses a combination of literature review, applying mathematical modeling to evaluate CSPM efficiency and analyzing case studies	The paper serves as a knowledge hub analyzing effectiveness of current CSPM solutions in managing security across diverse cloud platforms and case studies on the implementation of CSPM in real life.
(Rajesh Yalavaguli Seetharamarao, 2023)	The research highlights the vulnerabilities in cloud environments. The work observes the gap in fragmented cloud security audit and proposes a unified strategy detailing auditing procedures to be adopted while auditing cloud environments building on the recognized cloud compliance frameworks.	The research method for this study focuses on research on professional literature	This paper serves as a knowledge hub identifying cloud security breaches, legal guidelines that impact cloud computing and proposed audit considerations for a unified auditing strategy
(Rahman, A., Md Ashrafuzzaman, Jim and Sultana, R., 2024).	This study explores the effectiveness of CSPM tools in cloud computing	They combine comprehensive literature review, a survey of IT security professionals, and detailed case study	This research provides a robust evaluation of CSPM tools' capabilities, the challenges associated with their implementation and identifies critical barriers to CSPM adoption

References

Chauhan, M. and Stavros Shiaeles (2023). An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network*, [online] 3(3), pp.422–450. doi: https://doi.org/10.3390/network3030018

Dcurwin (2025). Cloud Security Posture Management (CSPM) - Microsoft Defender for Cloud. [online] Microsoft.com. Available at: https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-cloud-security-posture-management

Diogenes, Y. and Janetscheck, T., 2022. Microsoft Defender for Cloud. Microsoft Press.

Ghazizadeh, H., Tamm, G. and Creutzburg, R. (2024). Automated Tools for Cloud Security Testing. Electronic Imaging, [online] 36(3), pp.319–1319–7. doi: https://doi.org/10.2352/ei.2024.36.3.mobmu-319

Gupta, G. (n.d.). Managing Compliance and Auditing in Cloud. [online] Available at: https://www.theseus.fi/bitstream/handle/10024/749769/Thesis_gupta_gunjan.pdf?sequence=2

Jimmy, F. (2023). Cloud security posture management: tools and techniques. *Journal of Knowledge Learning and Science Technology ISSN: 2959-6386 (online)*, [online] 2(3). doi: https://doi.org/10.60087/jklst.vol2.n3.p622

John, Jonathan. (2023). EXPLORING TOOLS FOR EFFECTIVE CLOUD SECURITY POSTURE MANAGEMENT. Available at: https://www.researchgate.net/publication/387172661_EXPLORING_TOOLS_FOR_EFFECTIVE_CLOUD_SECURITY_POSTURE_MANAGEMENT

Jurgens, J. and Dal Cin, P. (2025). Global Cybersecurity Outlook 2025. [online] World Economic Forum. World Economic Forum. Available at: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

Kadar, Abas. (2023). ENHANCING CLOUD SECURITY: POSTURE MANAGEMENT TOOLS AND APPROACHES. Available at: https://www.researchgate.net/publication/387172756

Leaua, M.S., Alexandru Chiş, Titus-Constantin Bălan and Lucian Florin Ilca (2024). Assesment of Cloud Security Posture Management Scenarios. [online] pp.1–6. doi: https://doi.org/10.1109/roedunet64292.2024.10722349

N. Carter, "Auditing the ISO 19011 Way. BSI British Standards Institution," Auditing the ISO 19011 Way. BSI British Standards Institution, 2003.

Oluwagbade, Elizabeth. (2025). Benchmarking Cloud Security: Comparing Metrics Across Multi-Cloud and Hybrid Architectures. https://www.researchgate.net/publication/389357125_Benchmarking_Cloud_Security_Comparing_Metrics_Across_Multi-Cloud_and_Hybrid_Architectures

Paidy, Pavan & Chaganti, Krishna. (2025). CLOUD-NATIVE SECURITY POSTURE MANAGEMENT IN AWS AND AZURE: AUDITDRIVEN APPROACHES TO RISK AND COMPLIANCE. 61-71. 10.5121 https://aircconline.com/csit/papers/vol15/csit151106.pdf

Palo Alto Networks. (2015). What Is CSPM? | Cloud Security Posture Management Explained. [online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-cloud-security-posture-management

Rahman, Anisur & Ashrafuzzaman, Md & Jim, Md Majadul Islam & Sultana, Rebeka. (2024). CLOUD SECURITY POSTURE MANAGEMENT AUTOMATING RISK IDENTIFICATION AND RESPONSE IN CLOUD INFRASTRUCTURES. *Academic journal on science, technology, engineering & mathematics education.*, [online] 4(3), pp.151–162. doi: https://doi.org/10.69593/ajsteme.v4i03.103

Rajesh Yalavaguli Seetharamarao (2023). A Unified Approach Towards Security Audit and Compliance in Cloud Computing Environment. *2021 14th International Conference on Developments in eSystems Engineering (DeSE)*, [online] pp.623–629. doi: https://doi.org/10.1109/dese60595.2023.10469536

SentinelOne. (2025). 50+ Cloud Security Statistics in 2025. [online] Available at: https://www.sentinelone.com/cybersecurity-101/cloud-security/cloud-security-statistics/#:~:text=80%25%20of%20companies%20have%20encountered,operational%20delays%2C%20and%20poor%20performance

Sharma, H. (2020). *EFFECTIVENESS OF CSPM IN MULTI-CLOUD ENVIRONMENTS: A STUDY ON THE CHALLENGES AND STRATEGIES FOR IMPLEMENTING CSPM ACROSS MULTIPLE CLOUD SERVICE PROVIDERS (AWS, AZURE, ... Research · February 2020 CITATIONS 0 READS 599*. [online] Available at: https://www.researchgate.net/profile/Himanshu-Sharma-197/publication/383301812

Shinesa Cambric; Michael Ratemo, Cloud Auditing Best Practices: Perform Security and IT Audits across AWS, Azure, and GCP by building effective cloud auditing plans, Packt Publishing, 2023.

Taha, A.A.D., Ramo, W. and Alkhaffaf, H.H.K. (2021). Impact of external auditor–cloud specialist engagement on cloud auditing challenges. Journal of Accounting & Organizational Change, ahead-of-print(ahead-of-print). doi: https://doi.org/10.1108/jaoc-08-2020-0111