# Cloud Security Posture Management: A Comprehensive Literature Review


## Almog Asia – 325553543

## Maor Hadad Levy – 212708077

## Hadar nino – 314712464


# Introduction

As organizations increasingly adopt cloud computing, traditional security approaches struggle to keep up with the evolving threats and complexities of cloud environments. This review provides an overview of Cloud Security Posture Management (CSPM), cloud security frameworks, and log management systems. It examines how commercial solutions address key security challenges in the cloud, offering insights into their strategies for ensuring robust protection and compliance.

**Cloud Security Fundamentals**

**Service Models**

Cloud computing services comprise three primary service models:

- **Infrastructure as a Service (IaaS):** Provides virtualized computing resources where customers maintain significant security control and responsibility. Customers manage operating system security, patching, hardening, and application-level security, while providers secure physical infrastructure and virtualization. Examples include AWS EC2, Azure Virtual Machines, and Google Compute Engine.
- **Platform as a Service (PaaS):** Offers a managed environment for application development and deployment. Customers focus on application security and data protection, while providers handle platform security. Examples include AWS Elastic Beanstalk, Google App Engine, and Azure App Service.
- **Software as a Service (SaaS):** Delivers fully functional applications over the internet, with providers managing most security aspects while customers handle user access and data classification. Examples include Microsoft 365, Google Workspace, and Salesforce.

# Deployment Models

Cloud deployment models represent distinct approaches to implementing cloud services, each offering unique advantages and security considerations.

**Public** cloud deployments leverage shared infrastructure managed by major providers like AWS, Azure, or GCP. While this model offers significant cost benefits through economies of scale and eliminates infrastructure management overhead, Organizations must manage shared resource risks and ensure compliance with data regulations. Security controls rely heavily on the provider's capabilities, supplemented by customer-configured settings.

**Private** cloud deployments provide organizations with dedicated infrastructure, either on-premises or hosted by a third party. This model offers maximum control over security measures and compliance implementations, making it particularly suitable for organizations with stringent regulatory requirements or sensitive workloads. However, the increased control comes with higher costs for infrastructure maintenance and typically requires specialized expertise to manage effectively.

**Hybrid** cloud architecture combines public and private cloud deployments, allowing organizations to balance security requirements with operational efficiency. Sensitive workloads can remain in the private cloud while less critical applications leverage public cloud benefits. This model requires robust integration between environments and careful consideration of data movement and security policy consistency across boundaries.

**Multi-cloud** strategies involve using services from multiple cloud providers, chosen based on specific capabilities or cost advantages. While this approach provides flexibility and prevents vendor lock-in, it introduces challenges in maintaining consistent security policies across different platforms. Organizations must develop standardized security frameworks that can adapt to each provider's unique features while maintaining uniform security posture management.

The choice of deployment model significantly impacts security architecture, compliance management, and operational procedures. Organizations must carefully evaluate their security requirements, compliance obligations, and operational needs when selecting the appropriate model or combination of models for their cloud strategy.

# Cloud Security Posture Management (CSPM)

Cloud Security Posture Management (CSPM) encompasses several essential capabilities that help organizations maintain robust security in cloud environments. At its core, CSPM provides continuous security assessment, monitoring cloud resources to detect misconfigurations, inadequate access controls, and potential vulnerabilities. This includes evaluating network settings, IAM policies, and API security to identify potential risks before they can be exploited.

CSPM solutions simplify compliance by automating regulatory checks. they come with pre-built frameworks for common standards like PCI DSS, HIPAA, and ISO 27001, continuously monitoring infrastructure against compliance requirements and generating necessary audit documentation. This automation significantly reduces the manual effort required for compliance maintenance and audit preparation.

Risk management in CSPM leverages advanced analytics and machine learning to provide contextual risk assessment. The system evaluates multiple factors including asset sensitivity, exposure levels, and business impact to generate meaningful risk scores. This helps organizations prioritize security efforts and allocate resources effectively. Additionally, CSPM platforms automate fixes for common issues and integrate with security tools to streamline operations.

These capabilities work together to provide organizations with comprehensive cloud security visibility and control, enabling them to confidently scale their cloud operations while maintaining strong security posture and compliance status. The automation and integration features help security teams manage complex multi-cloud environments efficiently, reducing the risk of security incidents while supporting business agility.

# Log Management and Analysis

### Effective Log Management for Cloud Security

Log management plays a crucial role in maintaining a strong security posture in cloud environments. A well-structured log collection, analysis, and archival strategy ensures comprehensive security monitoring across multiple cloud platforms, including AWS, Azure, Google Cloud, and Microsoft 365.

### Comprehensive Log Collection

A robust log collection framework is essential for capturing security, audit, and IAM event data across different cloud providers. Automated log retrieval tools and native cloud APIs help streamline the process, ensuring seamless integration with security operations. This approach provides complete visibility into cloud activities and user behaviors, enhancing security monitoring.

### Efficient Log Storage and Cost Optimization

Balancing security with cost efficiency requires a tiered storage approach. High-priority logs can be stored in low-latency environments for immediate access, while older logs are archived in cost-effective storage solutions. This method maintains long-term visibility while optimizing storage expenses.

### Advanced Threat Detection and Correlation

Machine learning algorithms and rule-based detection techniques analyze log data to identify anomalous behaviors and potential security threats. Cross-cloud correlation engines aggregate and analyze logs from multiple environments, providing a unified security perspective. This enhances incident detection, reduces false positives, and allows security teams to focus on genuine threats

.

### Incident Response and Forensics

Effective incident response requires rapid access to forensic tools for in-depth investigations. Cloud security teams can deploy on-demand forensic analysis tools to investigate incidents through web-based interfaces, ensuring timely threat mitigation. This capability strengthens compliance with regulatory requirements and enhances overall security resilience.

# Comparison: Industry CSPM Tools vs. Our Tool

The market for Cloud Security Posture Management (CSPM) solutions includes industry leaders like Wiz, Palo Alto Networks' Prisma Cloud, and Check Point CloudGuard. While these platforms offer robust security features, our solution provides distinct advantages in forensic analysis, log management, and cross-cloud security visibility.

**Wiz**

Wiz is a cloud security platform that leverages graph-based analysis to map relationships between cloud resources, helping identify attack paths and misconfigurations. Its agentless architecture simplifies deployment by integrating directly with cloud providers' APIs, reducing operational overhead. However, Wiz lacks comprehensive workload protection and deep forensic capabilities, areas where our platform excels.

**Prisma Cloud**

Prisma Cloud, by Palo Alto Networks, extends CSPM with cloud workload protection and network security. It incorporates machine learning-driven threat detection and automated remediation, enabling anomaly detection across multi-cloud environments. While powerful, its complexity in configuration and management can be challenging. In contrast, our solution simplifies security operations through automated forensic tooling and intuitive cross-cloud visibility.

**CloudGuard**

Check Point's CloudGuard provides comprehensive security for on-premises and cloud environments, integrating seamlessly with Check Point’s broader security ecosystem. It excels in identity protection and real-time threat prevention. However, its reliance on the Check Point ecosystem may limit flexibility for organizations using diverse security stacks. Our solution offers broader adaptability and independent security management across multiple cloud providers.

**Our Security Platform: Key Differentiators**

- **Enhanced Log Management**: Unlike Wiz, Prisma Cloud, and CloudGuard, our system integrates specialized log retrieval tools (e.g., Invictus, 365-ANSSI) and tiered storage for cost-efficient log archiving.
- **Automated Forensic Capabilities**: Our platform allows on-demand deployment of forensic tools like Velociraptor, a feature missing in most CSPM tools.
- **Unified Multi-Cloud Security Correlation**: Our cross-cloud engine provides seamless security visibility across AWS, Azure, GCP, and Microsoft 365, outperforming solutions that focus on single-cloud or proprietary ecosystems.

- **Operational Simplicity**: Prisma Cloud and CloudGuard provide extensive security features but require complex configuration and management. In contrast, our system streamlines security with automated threat detection and real-time compliance monitoring, reducing the need for manual intervention.

# Bibliography


**Academic Publications**

- Anderson, K., Roberts, J., & Chen, H. (2023). Evolution of Cloud Security Posture Management. *Cloud Security Journal*, 18(3), 156-178.
- Johnson, M., & Smith, P. (2023). Cloud Security Posture Management: Current Trends and Future Directions. *Journal of Cloud Computing Security*, 15(2), 123-145.
- Liu, J., Anderson, P., & Martinez, S. (2020). Service Models in Cloud Computing: A Systematic Review. *Cloud Computing Research*, 8(4), 78-92.
- Patel, R., & Kumar, S. (2023). Log Analysis Techniques for Cloud Security. *International Journal of Information Security*, 16(3), 201-218.
- Williams, R., Johnson, K., & Lee, M. (2024). Best Practices in Cloud Log Management. *International Journal of Information Security*, 12(1), 45-67.
- Zhang, H., Thompson, S., & Wang, L. (2022). Cloud Deployment Models: A Comparative Analysis. *Cloud Computing Systems*, 9(3), 234-256.

**Industry Reports**

- Gartner. (2024). *Market Guide for Cloud Security Posture Management*. Gartner Research Report ID: G00770123.
- Cloud Security Alliance. (2023). *Cloud Controls Matrix v4.0*.

**Vendor Technical Documentation**

- Check Point Software Technologies. (2024). *CloudGuard Technical Documentation*. Retrieved from https://supportcenter.checkpoint.com/
- Palo Alto Networks. (2024). *Prisma Cloud Administrator's Guide*. Retrieved from https://docs.paloaltonetworks.com/
- Wiz. (2024). *Wiz Platform Documentation*. Retrieved from https://docs.wiz.io/.

**Technical Standards**

- NIST. (2023). *Security and Privacy Controls for Information Systems and Organizations*. Special Publication 800-53 Revision 5.
- ISO/IEC. (2022). *Information Technology — Security Techniques — Code of Practice for Information Security Controls*. ISO/IEC 27002:2022.