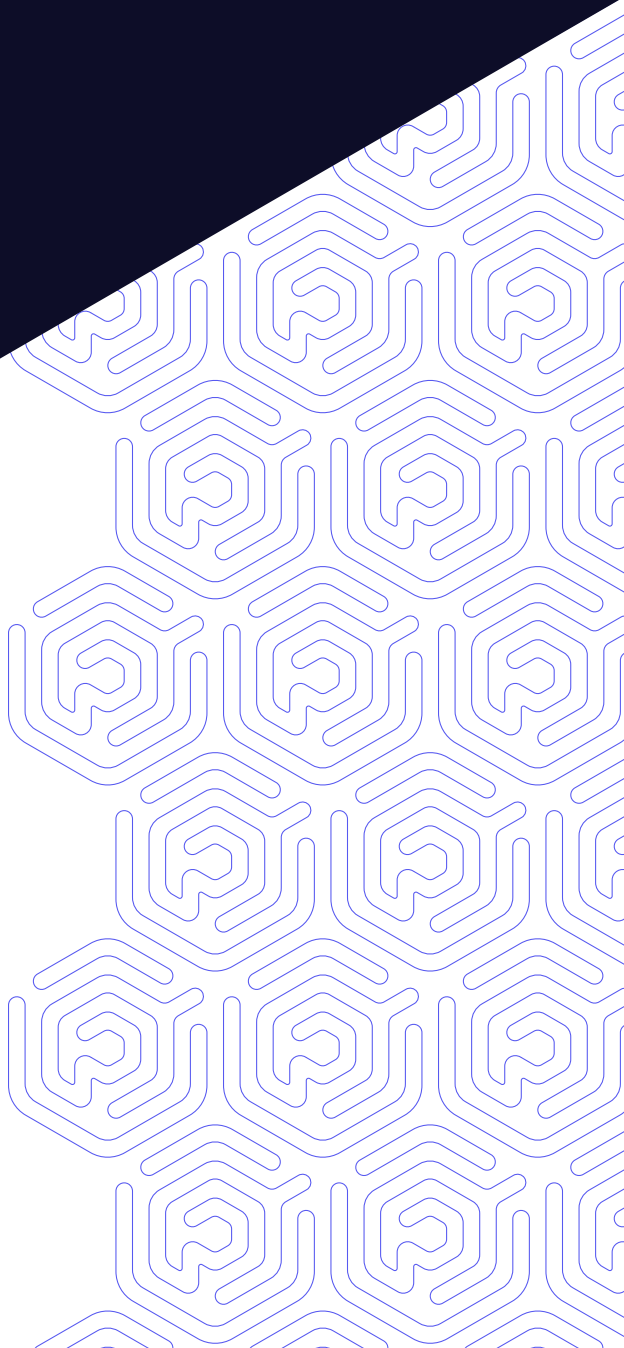
WHITE PAPER

Budget-Friendly Cloud Security

How to Balance Cost Optimization with Robust Security



praetorian

Cut your cloud costs without compromising your security posture.

INSIDE THIS REPORT

The value of cloud infrastructure lies in its scalability and flexibility; however, cloud service misconfigurations often result in soaring operating costs that overshadow these benefits. While cutting costs wherever possible is tempting, doing so only yields short-term gains. Cloud users instead need to take a security-conscious approach when optimizing cloud costs to mitigate the risk of more expensive compromises down the road. Praetorian has amassed extensive experience in helping to secure our customers' cloud environments, and we have identified effective strategies to help you minimize expenses while fortifying your cloud defenses.

By optimizing your cloud resource utilization and addressing security vulnerabilities in service configurations, you can significantly reduce your cloud environment's attack surface and boost your security posture. Malicious attackers are constantly ramping up the frequency and complexity of their offensive approach, making it crucial for organizations to have a clear view of their resources, configure services correctly, and leverage appropriate tooling for a defense-in-depth strategy. If these suggestions appear to be common sense, consider recent research that shows that a considerable volume of attacks trace back to resource misconfigurations and unpatched vulnerabilities.[1] Another concerning trend is that small and midsize businesses often lack visibility into their infrastructure as a service (IaaS) configurations and the capabilities necessary for continuous threat detection and removal.[2]

This paper will explore practical solutions to effectively secure your cloud infrastructure while simultaneously cutting costs to unlock the full potential of your cloud environment. With our approach, you will not have to compromise your balance sheet or your security posture.

1 **The Cloud Is Under Attack: The State of Cloud Security in 2023 | Goodchild |** https://www.csoonline.com/article/3684768/the-cloud-is-under-attack-the-state-of-cloud-security-in-2023.html

2 **The Reality of SMB Cloud Security in 2022 | Adam |** https://news.sophos.com/en-us/2022/11/29/the-reality-of-smb-cloud-security-in-2022/

Conduct Periodic Cost Assessments

Periodically assessing your cloud costs is essential for maintaining an efficient and cost-effective cloud infrastructure. Quarterly or semi-annual reviews of cloud costs can help identify areas for optimization and cost savings, and significant infrastructure or workload changes should trigger out-of-band assessments. Appropriate use of built-in notification features and target thresholds helps to bake in accountability from the start and serves as a starting point for out-of-band assessments. The data gleaned from these reviews are useful in highlighting over-provisioned or underutilized resources, as well as pointing security teams toward opportunities where they can take advantage of cloud service provider discounts.

Prioritizing budget and security

Annual reports on cloud industry trends indicate that only one-third of organizations correctly leverage cloud service provider discounts to maximize cost savings.[3] Yet, enterprises that make efficient use of Reserved Instances in AWS, for instance, can save up to 75 percent on their computing costs.[4] Implementing cost optimization strategies can reduce cloud waste and realize substantial cost savings. This begins with prioritizing a dual goal of cost savings and strong security posture for cloud services.

If you want to ensure long-term sustainability and establish a culture of security-conscious cost-optimization, educate your teams on the importance of responsible cloud resource usage, adhere to the principle of least privilege, provide training and resources to identify cost-saving opportunities and proper service configurations, and recognize those who contribute to cost-saving efforts and misconfigurations.

Establish cloud service evaluation criteria based on factors such as potential cost savings, level of effort required, and impact on your overall infrastructure. For immediate wins, focus on low-hanging fruit that requires minimal effort and has low operational impact first. Doing so builds momentum and demonstrates a clear business impact to help drive organizational consensus and buy-in for periodic reviews.

3 **2023 State of the Cloud Report | Flexera |** https://info.flexera.com/CM-REPORT-State-of-the-Cloud-2023-Thanks?revisit

4 **Accessing Reserved Instance Recommendations | AWS |** https://docs.aws.amazon.com/cost-management/latest/userguide/ri-recommendations.html

Deprovisioning extraneous cloud resources

Deprovisioning cloud resources that remain unused or underutilized, reach the end of their lifecycle, or pose security and compliance risks is essential to ensure a lean, efficient, and secure cloud environment. If you want to optimize cost savings without compromising security, you need to adopt a comprehensive cloud cost management strategy tailored to your organization's needs. Start by utilizing your cloud provider's built-in cost management tools, which provide valuable insights, cost optimization, and security risk identification. All of these empower you with centralized visibility and control. These tools also offer guidance on optimizing autoscaling features for different resources.

Make the most of autoscaling by adjusting resources dynamically according to workload changes. This involves evaluating workload patterns, configuring scaling policies, utilizing autoscaling groups, monitoring performance, setting up notifications, and continuously refining configurations to maximize scalability. Depending on your unique requirements, consider embracing serverless architecture to simplify resource utilization, minimize idle resources, maximize cost efficiency, and accommodate fluctuating demands.

Using cloud service providers' service tiers for cost optimization

Remember that cloud service providers offer numerous services to cover a broad range of use cases, and the vast majority of organizations only utilize a fraction of cloud offerings. Bearing that in mind, conduct a careful analysis of your organization's needs to determine the feasibility and applicability of serverless architecture. Its use does not always maximize efficiency for every organization's workload requirements.

Cloud resources often come with different options that cater to specific workloads and can minimize your expenses. For instance, AWS offers various storage tiers, such as Glacier or Standard-Infrequent Access, which are designed for users requiring long-term storage who can accept slower access windows. When you leverage tiered services focused on longer-term projections, you can significantly reduce costs without compromising data accessibility. While the "pay-as-you-go" model is a core benefit of

working with public cloud environments, you will save the most costs the more you can plan ahead and pre-allocate resources.

Take advantage of each cloud service provider's discounts, such as reserved instances or savings plans, for significant cost reductions with long-term usage commitments. Throughout the process, conduct regular assessments of your cloud resources and promptly deprovision any unnecessary ones. You can achieve streamlined resource management by using the automation tools your cloud service provider offers, or by utilizing third-party solutions.

Optimizing the process

When rightsizing cloud resources, evaluating your cloud architecture design and needs holistically is crucial to achieve optimal outcomes. You need to consider factors such as interdependencies, data flows, and performance bottlenecks as well as workload patterns, performance requirements, and anticipated growth. Delving into all these elements will enable you to develop a comprehensive list of your critical assets and capability requirements that is inclusive of your specific business context and needs. Ultimately, the goal is for your cloud services to have precision resource allocation that optimizes cost-efficiency and performance.

By aligning your resource adjustments holistically with industry benchmarks and best practices, you can proactively mitigate potential risks and safeguard your organization's sensitive data effectively. Finally, implement a clear governance structure that clarifies responsibilities for cloud cost management, identifies necessary tools and processes for monitoring and optimizing costs, and facilitates the integration of cost assessments and resource cleanup into the overall cost management strategy.

Centralize Cloud Resource Management

Organizations need a comprehensive understanding of cloud expenses and their correlation to business value. Cloud service providers offer tools that enable a

centralized view of costs and usage, management of bills and payments, and allocation of charges to specific business entities. You can tailor tagging and allocation strategies to drive strategic outcomes and maximize profitability, accurately attribute costs and usage, and prioritize investment decisions with end-user cost insights in mind. Studies into enterprise cost optimization strategies reveal that organizations leveraging real-time cost optimization solutions for cloud infrastructure can achieve up to 15 percent cost savings compared to those without such solutions.[5]

Implementing effective tagging strategies to monitor resource usage and costs

Tags are metadata labels you can attach to cloud resources for better management and organization. Cloud infrastructure tags fall into two types: standard and custom. Standard tags are predefined by the cloud service provider and are applied to resources by default. Examples of standard tags include "Name," "Environment," and "Cost Center." On the other hand, custom tags are created by users and can be used to label resources according to their specific needs. Cost allocation tags, for example, are custom metadata tags to help you categorize and allocate costs across different departments, projects, and teams.

Effective tagging categorizes cloud resources based on attributes, enabling you to identify underutilized resources and make informed decisions for cost reduction. Tagging facilitates accurate cost allocation to specific business entities for transparency and accountability, tracks resource usage patterns, uncovers cost-saving opportunities, supports data-driven decision-making for resource optimization, and simplifies resource cleanup by clarifying ownership and usage patterns to efficiently remove unused resources. From a security standpoint, an effective tagging strategy also enables you to run a more accountability-driven cloud security program that facilitates easier identification and management of security-sensitive assets.

Identifying which tags you need

To achieve accurate tracking, categorization, and visibility of your assets, start by identifying critical resources and selecting valuable metrics for usage and

5 **Market Guide for Cloud Workload Protection Platforms | Gartner |** https://www.gartner.com/en/documents/4003465

spending insights. Your list should include, but not be limited to, virtual machines, databases, storage accounts, and network resources, as well as core metrics like utilization, cost, and performance data. Accounting for your cloud resources, guided by an overall strategy, establishes a proactive approach to security monitoring and consistent application of security controls. Your due diligence will pay dividends by bolstering your organization's resilience in the face of potential security incidents.

Establishing your tagging strategy

From there, establish a tagging strategy that aligns with your organization's objectives and needs. This step should include the following elements:

- **Defining a consistent set of tag keys**
- **Creating clear naming conventions for tag values**
- **Establishing a clear process to ensure consistent tag application across your organization**
- **Setting up auto-tagging solutions alongside a manual resource tagging effort to gain full coverage of your cloud resources**
- **Defining roles and responsibilities for managing tags (which will come in handy when determining which resources can be deprecated to save costs**

A well-designed tagging system will enable your organization to track usage patterns better and identify areas where resources are overprovisioned or underutilized. You can use this information to make informed decisions about which resources to scale.

Gaining insight into cloud usage

After you tag data according to your strategy, analyze the metadata to derive insights. One approach is filtering and aggregating data based on tags using standard tools from your cloud service provider, which can help enumerate usage and identify patterns. Alternatively, you can use data visualization tools like

dashboards to display key metrics and trends in real-time. This information can be invaluable in helping your team understand how resources are used, where inefficiencies may occur, and where cost-saving opportunities may exist.

You can also export data to analyze using third-party tools, such as machine learning and statistical analysis toolsets, which identify patterns and correlations that may not otherwise become apparent to human operators until much later. Ultimately, the key to analyzing tagged data is to identify actionable insights that can lead to optimized cloud usage and reduced costs over time.

Implementing automated cleanup to reduce unused or unnecessary resources

Resource cleanup, the process of identifying and removing unused or unnecessary resources from your cloud environment, can help you optimize resource usage, prevent unnecessary costs, and decrease the attack surface of your cloud environment. You can delete or archive unneeded resources manually or through automation. Define resource ownership, establish resource use and cleanup policies, and regularly review and evaluate resources for potential cleanup to minimize the number of resources that a malicious attacker could exploit.

Keeping resources running impacts spending and can introduce security vulnerabilities. A robust resource lifecycle management strategy optimizes costs and improves security by reducing your attack surface, promptly decommissioning unused resources, and minimizing unauthorized access. Monitoring and auditing enhance visibility, enabling effective detection of anomalies and security incidents. A streamlined resource lifecycle facilitates efficient incident response and ensures compliance with regulations and data protection standards, strengthening your overall security posture.

Applying this to sandbox environment management

Cloud security leaders face an ongoing challenge with the effective management of developer sandboxes. These isolated environments allow developers to experiment and test their workloads without affecting the production infrastructure, but they can also pose security risks if not properly managed. Sandbox environments often have fewer restrictions on resource provisioning, which can lead to the creation of unnecessary

or misconfigured resources, uncontrolled resource usage, mismanagement of access controls, inadequate data protection measures, and neglecting to regularly deploy updates and patches that could potentially expose sensitive data or create entry points for malicious attackers. Your organizations should strike a balance between security and developer flexibility by implementing proper governance, establishing clear data protection policies, conducting periodic security audits, and closely monitoring usage to mitigate these risks.

Therefore, automating the identification and termination of inactive or underutilized sandbox environments, for instance, yields multiple benefits. First, it optimizes resource utilization by reclaiming idle environments, which reduces waste and improves cost efficiency. Second, it eliminates unnecessary expenses associated with unmonitored environments, mitigates security risks by reducing the attack surface, and ensures operational efficiency by simplifying resource management. Lastly, it enables scalability and agility in managing sandbox environments, supporting dynamic resource allocation and rapid deployment.

Adding cost governance strategies to optimize cost reduction efforts

Cost governance strategies are policies and procedures organizations implement to manage and optimize your cloud infrastructure costs, including cost scorecards. Cost scorecards track and analyze cloud costs, providing insight into the effectiveness of your cost management efforts. Implementing a comprehensive cloud cost governance strategy will enhance your organization's cloud security posture by providing increased visibility, optimizing resource utilization, ensuring compliance and risk management, enabling automation and control, and allowing for proper budget allocation toward security measures.

When developing a cost scorecard, establish your goals and performance metrics, such as cost per application or user. Next, collect data from different sources, such as cloud service provider billing data, to establish a baseline and track progress over time. Establish a cross-functional cost governance team, define clear roles and responsibilities, and create a communication plan to inform stakeholders about the cost governance process. Define policies and procedures, regularly monitor costs, and use automation tools to improve efficiency and accuracy.

Appointing a party or individual responsible for costs

Appointing a responsible party for cost management is essential to maintaining an efficient, secure, and cost-effective cloud infrastructure. This practice promotes accountability, effective cost management, and alignment of financial decisions with security priorities. Responsible parties must be empowered to implement alerting and management mechanisms to ensure they become aware of any cost overruns or usage anomalies. They should have a strong understanding of cloud services, costs, and usage patterns. Additionally, they must possess the appropriate level of authority to make cost optimization decisions and implement policies and procedures that support the organization's overall cloud cost management strategy.

Organizing your cloud environment for better cost management and accountability

Cloud environment management is crucial as each cloud service provider offers different types of accounts, subscriptions, and projects. Among these are root accounts, Identity and Access Management (IAM) accounts, and member accounts, to manage access and resource permissions. You should develop a strategy for organizing and managing your environment to ensure that it aligns with your business objectives and supports your security and cost optimization goals.

Key elements in this type of strategy include the following:

- **Developing naming conventions for each of your accounts, subscriptions, and projects**
- **Implementing strict access controls and permissions**
- **Regularly reviewing and auditing each environment to ensure it aligns with business objectives**

Separating accounts, subscriptions, or projects will result in greater visibility and control over resource usage, access, and cost.

This practice also reduces your attack surface. When you isolate environments based on function, you can more easily apply security controls and permissions only to the necessary environments, reducing the risk of unauthorized access to sensitive data or resources. Monitoring and audit activities are also simplified within the environments, as security teams can quickly identify potential security incidents. Finally, should a breach occur, it will be less likely to affect all environments in the organization, limiting the impact of the incident and reducing the risk of data loss or system downtime.

Link Incident Accountability to Cloud Cost Reduction Efforts

Cloud security incidents can have significant financial implications, including the cost of data loss, downtime, and recovery. They can also result in reputational damage, loss of customer trust, and degraded employee productivity. Your proactiveness in conducting comprehensive cost analysis will help your organization understand cloud incidents' impact holistically.

You need to delineate stakeholders in advance and establish playbooks for accountability measures and root cause analysis. Doing so will enable your organization to more robustly mitigate the effects of potential incidents and provide a basis for making security tooling and capability investment decisions.

Stakeholders and the shared responsibility model

In a secure cloud environment, incident response involves coordination among various stakeholders and teams. Essential roles include the following:

- Security team – monitoring and responding to security incidents,
- Cloud service provider – offering infrastructure and tools for incident detection and response, and
- Customers – securing their applications and data and reporting incidents.

All stakeholders must understand their roles and establish a clear plan to ensure effective incident response. This playbook defines processes for incident reporting, severity assessment, and appropriate response actions.

Embracing the shared responsibility model is crucial for security and cost optimization so you can actively monitor your infrastructure and respond to incidents effectively. As always, promptly report incidents to your cloud security provider so they can provide the necessary tooling and address any infrastructure requirements.

Accountability measures and root cause analysis

Accountability measures can help your organization identify areas for improvement, promote responsible use of cloud resources, and ensure that cloud cost management practices are aligned with your business goals. Your team must define roles and responsibilities for cloud cost management to help ensure that individuals are held accountable for their actions and decisions related to cloud usage.

An example of such a measure would be implementing a cloud usage policy that outlines guidelines for responsible cloud usage, including rules for resource allocation, usage quotas, and access controls. Your organization could then do the following:

- Conduct regular audits of cloud usage and cost data to identify areas of overprovisioning or underutilization
- Adjust resource allocation as needed
- Implement cost allocation and chargeback systems
- Establish clear governance structures for cloud cost management
- Provide training and education for employees on responsible cloud usage

Root cause analysis involves identifying an incident's underlying cause or causes and taking appropriate steps to prevent similar incidents. This is essential for identifying accountability and responsibility for incidents and minimizing the risk of future incidents. Effective root cause analysis involves interviewing stakeholders, reviewing logs and system data, and using software tools to identify patterns and anomalies.

Use Anomaly Detection to Detect Incidents in Progress

Detecting anomalies in your cloud infrastructure is crucial for maintaining a secure and efficient cloud environment. Therefore, detecting anomalies is pivotal to maintaining a robust and optimized cloud environment to aid in identifying and preventing incidents in real time. By leveraging advanced algorithms and proactive automation, anomaly detection empowers you to stay one step ahead of potential security threats.

Approaches to anomaly detection

Enhancing your organizational security can involve multiple approaches, such as machine learning, behavior analysis, and threshold-based monitoring. Machine learning algorithms analyze diverse data sources to detect anomalies that deviate from standard practices, providing early warnings of potential security incidents. Behavior analysis

monitors user behavior and system activity, identifying unusual patterns indicative of a breach, like tracking login attempts from unique locations or atypical times. Threshold-based monitoring sets specific thresholds for metrics or behaviors, issues alerts when thresholds are exceeded, and utilizes anomaly correlation to link anomalies across data sources and identify potential security incidents.

Implementing anomaly detection follows a three-step process.

1. Establish a baseline of your organization's typical network traffic, user activity, and relevant data points.

2. Select appropriate anomaly detection methods based on your infrastructure's characteristics and desired incident detection criteria.

3. Define incident response procedures, including containment, root cause analysis, and remediation measures. Establish communication guidelines with stakeholders and authorities, and procedures for preserving and interpreting evidence to prevent future incidents.

Have your organization achieve more effective detection and incident response capabilities by using the Center for Internet Security (CIS) benchmarks as guidelines. The cybersecurity industry recognizes these benchmarks as best practices for securing various technologies, including cloud environments. They provide actionable recommendations for security controls, logging configurations, and monitoring settings, which are essential for maintaining a robust security posture. Periodically updating your cloud environment to ensure alignment with CIS Benchmarks empowers your organization to tackle emerging threats and technological advancements. This ultimately facilitates more effective incident response and strengthens security resilience in cloud environments.

While having your organization follow CIS benchmarks is a step toward a more secure cloud environment, it is not a cost-saving strategy in itself. For instance, some CIS guidelines advise organizations to enable logging for elastic load balancers and flow logging everywhere in your cloud environment. Following this advice can be cost-intensive with minimal security benefits for some organizations, depending on the organizations' maturity and ability to action collected data. While it may be tempting to label a secure cloud environment as priceless, the reality is that assigning value is necessary. Every effort you make to enhance the security of your cloud environment is worthwhile, but if you must prioritize then you should do so with the intention of reducing costs without compromising on security.

Conclusion

Optimizing cloud costs while maintaining a strong security posture is crucial for your organization's maturity. At Praetorian, we understand the importance of balancing these priorities, and we encourage you to take action to implement these best practices to reduce your cloud costs while maintaining a high level of security. Regularly assessing your cloud costs and implementing security measures can lead to long-term success and sustainability for your organization's cloud usage.

Security and cost-savings are not mutually exclusive and each step you take in strengthening your organization's security posture is an investment to help reduce the potential cost of malicious attacks against your organization. Not all cloud services and features, tiered discount plans, or security benchmarks are right for every organization; if there was a one-size-fits-all answer, cloud security would be very simple. Start with understanding your cloud environment first and foremost to make a tailored assessment of your organization's architecture, security, maturity, and budgeting needs.

Praetorian is here to help ensure your attack surface management and cloud security align with industry best practices. Don't wait to reduce your cloud costs and improve your security posture. Contact us today to learn more about our cloud security services and how we can help you achieve your goals.