Deloitte.

FinOps:
Maintaining security compliance and minimizing costs

Introduction to government security compliance

Protecting the security of government cloud environments is Job 0, a top priority for federal agencies as indicated by the Federal Information Security Modernization Act (FISMA); Federal Risk and Authorization Management Program (FedRAMP); Executive Order 14028; memos; and a wide range of policies, rules, and programs. Cybersecurity was identified as the key area of concern in the Council of Inspectors General's report, *Top management and performance challenges facing multiple agencies*, released in September 2023. However, when it comes to the cloud, if security is Job 0, FinOps is Job 0.5.

In the *2023 Gartner CIO and Technology Executive Survey,* 70% of government respondents indicated that cybersecurity programs and initiatives will see the greatest new or continued investment in 2023, and this trend will continue into 2024. As new or existing mandates are implemented, with a FinOps approach, agencies can better predict the costs of the increased cloud security before implementation, allowing for more accurate funding requests and preventing unexpected cost overruns to better balance costs, security, and speed to mission.

Security compliance brings additional but necessary expenses to cloud environments through a combination of native and third-party security tools that handle encryption, access controls, logging, and security monitoring, which generate large amounts of data to be processed and stored. FinOps can help agencies identify cost-effective solutions for implementing security controls and enhance cost-allocation processes to ensure that security measures are adequately funded in future fiscal years.

Optimization for security

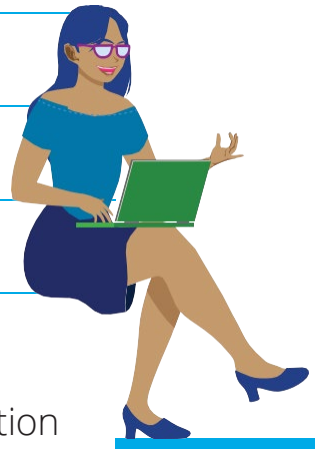
FinOps is the practice of bringing financial accountability to the variable spend model of cloud, enabling distributed finance, procurement, business leaders, development, and security teams to align and make organizational trade-offs between speed, cost, and quality.

Executive Order 14028, a zero trust mandate for federal agencies, sets the requirements for event logging and retention policies and other security policies. The level of implementation varies across agencies and even across systems within an agency. Agencies migrating to or developing systems/applications within the cloud should consider the level of logging, the storage requirements, and the associated costs during the planning and budgeting phases. Data transfer costs may also be a consideration for third-party monitoring tools. There are a wide range of configurations that can be enabled at varying points, most having an immediate impact on the cloud costs and usage. A small change to logging details or the cardinality of the log can create a minor or major change to cloud spend in a few days. This "plan and review" cycle creates logging costs that are predictable and measurable over time, allowing anomalies to be spotted quickly.

Understanding logging costs

Event logging costs fluctuate based on three factors:

1. **Frequency of event logs**
2. **Scope of observability (amount of data being logged)**
3. **Retention period length for storage of the dataset(s)**



In a well-maintained cloud environment, a FinOps team can plan and forecast logging based on retention periods and an understanding of the types of gathered logs and their intervals. An increase in logging over time is expected and should be factored into budgets and forecasts. However, if excess data is continually collected and retained, cloud spend for event logging can quickly balloon past prepared forecasts.

A recent use case

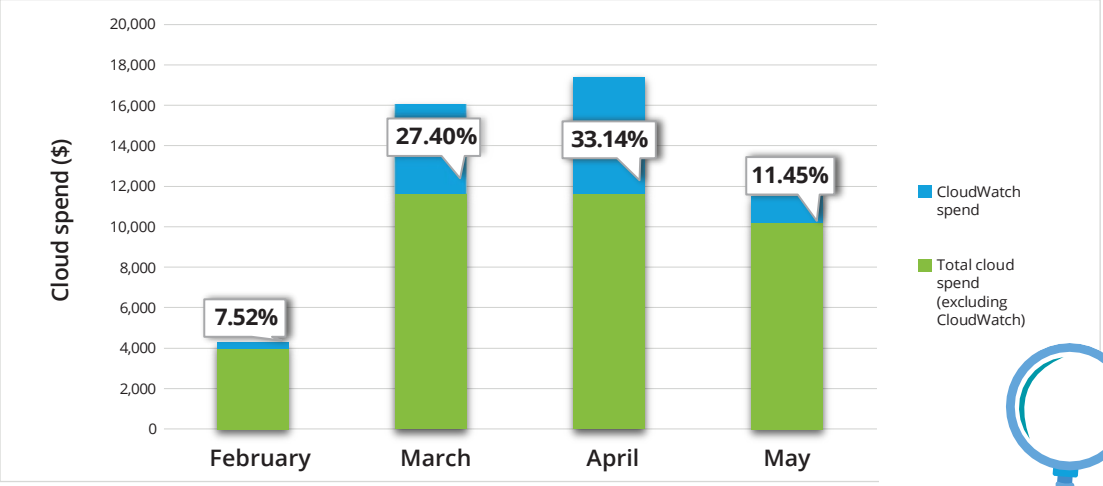
Deloitte performed a Cloud Spend Diagnostic for an organization that requested an evaluation to identify areas for cost reduction to avoid impending budget overruns. As part of the analysis, Deloitte identified a significant issue with the CloudWatch charges, which were a disproportionately large percentage of the organization's total expenses. Through further investigation, the team discovered that logging for a single resource represented more than 95% of total CloudWatch charges in the environment. After consulting with the Engineering team to identify the source of the high costs, it was determined that a single instance had its CloudWatch "Log_Level" set to "DEBUG". This meant that the "Log_Level" had not been reset to standard configurations when a debugging process to troubleshoot a previous issue was completed. The consequences of this neglected configuration change were twofold: creating unpredictable sources of cost, namely due to the large amount of data being generated and then the storage of that data.

The action plan

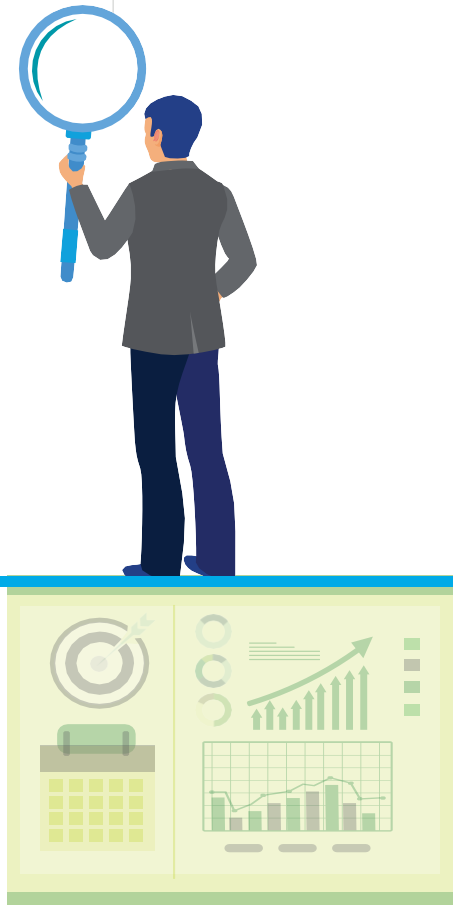
After identifying the cause of the large CloudWatch costs, Deloitte worked with stakeholders to confirm that the resource was no longer in active debugging mode and CloudWatch logging levels could be restored to standard configurations. As a result of the conversations, it was determined that "INFO" event logging was suitable for putting together the implementation plan, including cost monitoring and anomaly detection, to ensure costs from debugging did not run rampant again. The configuration was returned to the appropriate setting for the instance, which resulted in a 95% reduction in CloudWatch spend.

The graph below outlines the relationship between CloudWatch usage and the organization's costs over a four-month period of performance.

CloudWatch spend vs. total cloud spend



Had spending remained unchecked, logging expenses would have continued to climb month over month, costing the organization thousands of dollars each month. As shown in the above graph, the amount of CloudWatch spend as a percentage of the total cloud spend climbed from February to March to April, surpassing 33% for the month of April. While the increase in cloud spend from February to March was anticipated as a direct consequence of the organization building out its environment, there was not a significant increase in the proportion of CloudWatch spend. Through FinOps anomaly detection, the organization's percentage of CloudWatch spend decreased to just under 11.5%, which allowed it to save thousands of dollars per month. There are now guardrails in place to safeguard against these situations moving forward.



Next steps

While many may see FinOps and security as two separate functions, there is an increasing opportunity to collaborate and integrate the two to help ensure that security requirements are met while costs are accounted for and monitored to prevent unnecessary cloud spend. Reach out to learn more about how Deloitte can help your agency create a security and FinOps culture, or request a Cloud Spend Diagnostic today!

Contact us

Kris Ostergard
Managing Director
Deloitte Consulting LLP
+1 571 882 8722
kostergard@deloitte.com

Mike Rock
Senior Manager
Deloitte Consulting LLP
+1 571 858 1887
mirock@deloitte.com

Or contact us at
gpscloudfinops@deloitte.com

Deloitte.