Augmenting Native Cloud Service Provider Security

Introduction

Most organizations already have some level of cloud infrastructure services (IaaS, PaaS, FaaS, or serverless) and as more workloads migrate to, and are built on, the cloud, the top cloud security concern for any organization is a data breach. To underscore this point, breaches uncovered in March 2019 alone include the exposure of thousands of doctors' notes by Meditab, 1.5 million customer records by Gearbest, 2.4 million client records from Dow Jones, and 809 million customer records by Verifications.io.

All of the above breaches were due to misconfigurations and mistakes made by the Cloud Service Provider (CSP) customer, not due to vulnerabilities or failures in the underlying CSP service. It drives the question — are current approaches to managing cloud security controls sufficient to prevent a breach? Put another way, what do organizations need to do to augment or boost their current cloud security approach to better manage breach risk at an acceptable level in the cloud?

Leveraging CSP security controls is essential, and, for some cloud implementations, is sufficient to manage public cloud workload risk. For most enterprises, however, these controls alone are not adequate to address the core aspects of cloud security: audit, visibility, protection, detection, and automation. As discussed in this report, aligning cloud complexity with organizational risk appetite is key to determining when and how to augment CSP security controls.

Most Cloud Breaches are Due to Misconfigurations

Breaches of data in the cloud are on the rise, not breaches of the underlying cloud provider's infrastructure. This distinction between CSP and customer is vital since with cloud providers there is an explicit shared responsibility relationship. The cloud provider is responsible – and typically successful in – securing the underlying components of cloud services. The customer is responsible for securing how they use the cloud services, including properly configuring identity and access management (IAM), storage and compute settings, threat analysis and defense, and the security of the application and data processed and stored on the cloud.

If the underlying cloud infrastructure is secure, then responsibility for cloud breach must lie with the cloud customer. As Gartner states, "through 2022, at least 95 percent of cloud security failures will be the customer's fault."

The If cloud breaches are typically due to misconfigurations, then organizations must implement controls that quickly – and automatically – prevent or detect and remediate these errors. To this end, CSPs offer a plethora of security controls. For example, Amazon AWS provides more than 30 different cloud-security related services (e.g., GuardDuty, CloudTrail, CloudHSM, CloudWatch, etc.), including the recent beta release of AWS Security Hub. These controls are essential, playing a primary role in secure cloud configurations, though just turning them on does not guarantee secure cloud configurations.

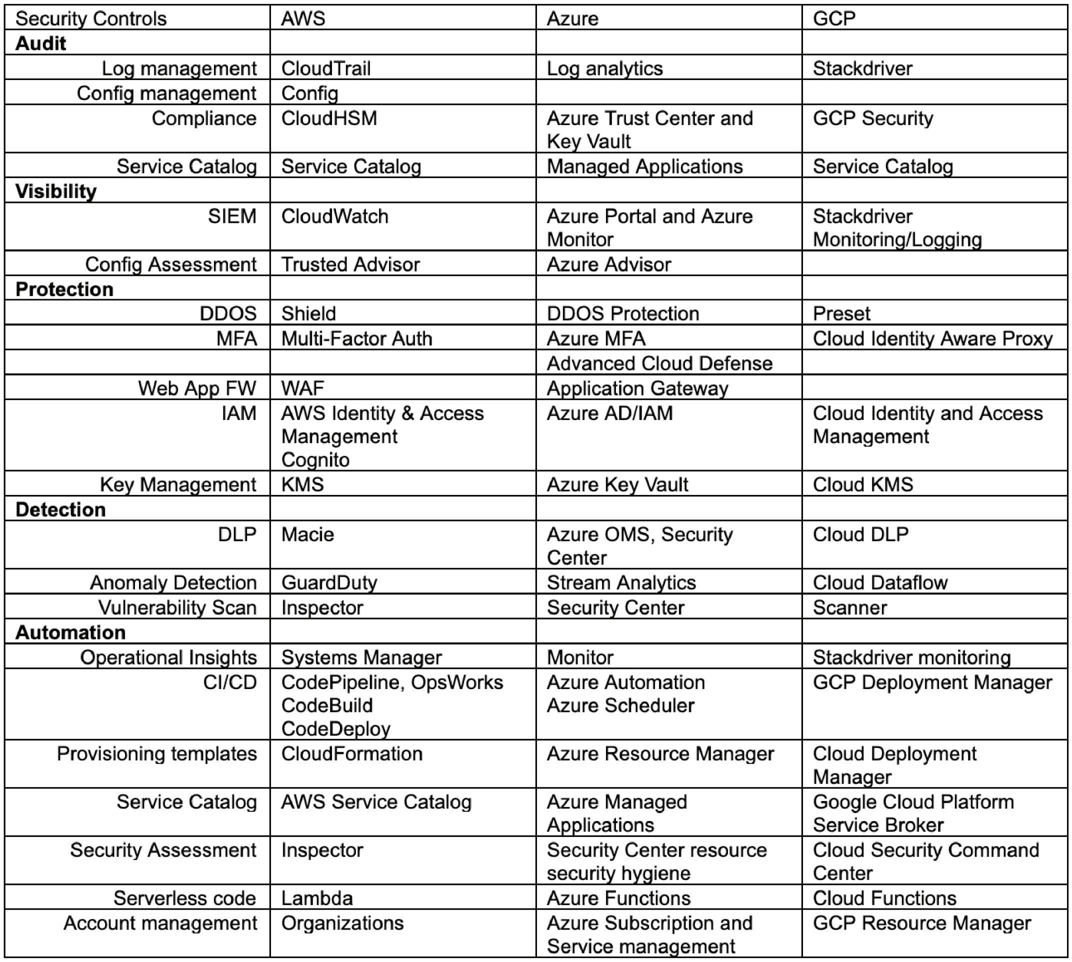
Secure cloud configuration must be a dynamic and continuous process. At a base level, there is the configuration of the cloud infrastructure (e.g., blocking SSH ports, and IAM). Next, there is the configuration of the CSP security controls (e.g., enabling log monitoring and encryption). And, finally, SecOps teams must address changes to settings (e.g., detecting and acting on a threat actor turning off logging to cover their tracks).

So, what controls detect and prevent misconfigurations? To answer this question, we align CSP controls against core aspects of cloud security: Audit, Visibility, Protection, and Detection. These core aspects build on the NIST Cybersecurity Framework (NIST CSF). To augment the NIST CSF and better align it to cloud security, we include automation as a core aspect. Automation is so central to cloud operations that there are a series of controls necessary to monitor, track, and enforce automation functions

CSP Security Controls

The Table 1 lists the CSP security controls available from the three major CSPs: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). These tools are necessary to manage and protect cloud workloads because, often, particularly for detective controls, these tools can provide visibility and control at a level not possible with external tools. For example, AWS GuardDuty leverages DNS logs, which aren't made public to external security services. These detective tools enable users to derive insights from attack patterns and techniques so they can act more quickly. In the case of AWS, using services like Inspector for vulnerability scanning, or GuardDuty for network intrusion, or Macie for anomalous behavior detection improves the overall security response.

Table 1 on the following page



Security Controls	AWS	Azure	GCP
Audit			
Log management	CloudTrail	Log analytics	Stackdriver
Config management	Config		
Compliance	CloudHSM	Azure Trust Center and Key Vault	GCP Security
Service Catalog	Service Catalog	Managed Applications	Service Catalog
Visibility			
SIEM	CloudWatch	Azure Portal and Azure Monitor	Stackdriver Monitoring/Logging
Config Assessment	Trusted Advisor	Azure Advisor	
Protection			
DDOS	Shield	DDOS Protection	Preset
MFA	Multi-Factor Auth	Azure MFA	Cloud Identity Aware Proxy
		Advanced Cloud Defense	
Web App FW	WAF	Application Gateway	
IAM	AWS Identity & Access Management Cognito	Azure AD/IAM	Cloud Identity and Access Management
Key Management	KMS	Azure Key Vault	Cloud KMS
Detection			
DLP	Macie	Azure OMS, Security Center	Cloud DLP
Anomaly Detection	GuardDuty	Stream Analytics	Cloud Dataflow
Vulnerability Scan	Inspector	Security Center	Scanner
Automation			
Operational Insights	Systems Manager	Monitor	Stackdriver monitoring
CI/CD	CodePipeline, OpsWorks CodeBuild CodeDeploy	Azure Automation Azure Scheduler	GCP Deployment Manager
Provisioning templates	CloudFormation	Azure Resource Manager	Cloud Deployment Manager
Service Catalog	AWS Service Catalog	Azure Managed Applications	Google Cloud Platform Service Broker
Security Assessment	Inspector	Security Center resource security hygiene	Cloud Security Command Center
Serverless code	Lambda	Azure Functions	Cloud Functions
Account management	Organizations	Azure Subscription and Service management	GCP Resource Manager

Table 1 - CSP Security and Management Tools

Essential and Sufficient to a Point

CSP security controls address audit, visibility, protection, detection, and automation requirements to a point. There is an inverse relationship between the effectiveness of these controls and the complexity of the cloud environment. To illustrate, AWS CloudTrail does an excellent job as an audit control, recording events (e.g., API calls, AWS SDKs, command line tools, AWS Management console, and other AWS services). Of course, CloudTrail is only useful when turned on and – not surprisingly – an attacker's first move is often disabling CloudTrail. Blocking this threat requires detective controls to identify when CloudTrail is turned off, preventive controls to prevent services from starting without CloudTrail enabled, and reactive controls to restart CloudTrail in the event of misconfiguration or malicious action.

To accomplish these tasks natively on AWS requires the following steps (and similar steps in multi-cloud scenarios across multiple cloud providers using their specific approaches):

1. **Writing Lambdas to orchestrate these actions**
2. **Programming CloudFormation to make sure all infrastructure templates have CloudTrail enabled**
3. **Setting CloudWatch to alert on a CloudTrail stop action**
4. **Relying on GuardDuty to detect and respond to the action**

Yes, this is only four steps, but consider that logging is just one of the hundreds of requirements for ongoing cloud security and the complexity of managing this at scale across multiple clouds. To provide some perspective, this requirement equates to the Center for Internet Security (CIS) requirement 6.2 “Activate audit logging.” There are seven CIS audit logging requirements to be set, validated, and re-checked regularly in AWS.

Seven requirements are still not an excessive demand on a SecOps team but add in a GCP workload, and the number doubles. Deploy workloads across all three clouds and the requirements more than triple. And, this is just the underlying configuration, not the additional AWS Lambdas, Azure functions, and GCP cloud functions necessary to detect log setting changes and the resulting reset actions. Considering that this is only one of nearly 200 CIS recommendations, implementing these recommendations, particularly across a multi-cloud environment, becomes a considerable task.

A pre-Script-ion For Brittle Security

Automation of cloud services is a double-edged sword. On the one hand, automation drives better security by automating security controls with dramatic, tangible benefits. Automating security can reduce the incidence of a breach and, according to the 2018 Ponemon report, businesses that have security automation reduce the cost of a breach by 35%. The flip side of the automation sword is the misconfiguration of controls where automating cloud provisioning can act as a force multiplier. In other words, things can go very well or very poorly, very quickly, due to automation. For example, provisioning of serverless computing (e.g., AWS Lambda) without proper automation of dynamic and static code testing could result in vulnerable code launching into production quickly and quietly.

Sure, it is possible to write 100’s of scripts using cloud-native tools to enforce CIS benchmarks and detect and respond to changes to manage cloud risk. However, not only is this a brittle and unsustainable strategy, as complexity increases, relying entirely on CSP toolsets becomes unmanageable for the following reasons:

- Writing JSON or YAML code for Lambdas and functions ties up senior security resources (a resource in critically short supply). Further, custom development required to write these scripts often ties to a single individual on the SecOps team. Without significant governance and discipline to treat these scripts with the same level of management as application code (i.e., policy as code) this may result in a single point of failure when Sally moves on to a new job

- A unified approach to security and compliance for auditors and executives. There is a lack of consistency of toolsets across availability zones, regions, or organizational level, depending upon the CSP.

- Managing compliance (from a configuration standpoint) across different providers and cloud environments raises the potential of compliance gaps

- Coordination of remediation action to address misconfigurations and compliance gaps becomes disjointed and siloed when solely relying upon CSP controls in a complex cloud environment

Managing Risk Against Cloud Complexity

Going back to Gartner's projection about cloud security failures being due to human error, as the complexity of the environment increases, so too does the opportunity for error. As shown in figure 1, the relationship between CSP security controls, cloud complexity, and risk is not a simple straight-line equation. As complexity increases, so too does risk, but your organization may be at very high risk even in a basic cloud environment.
ajgdfg

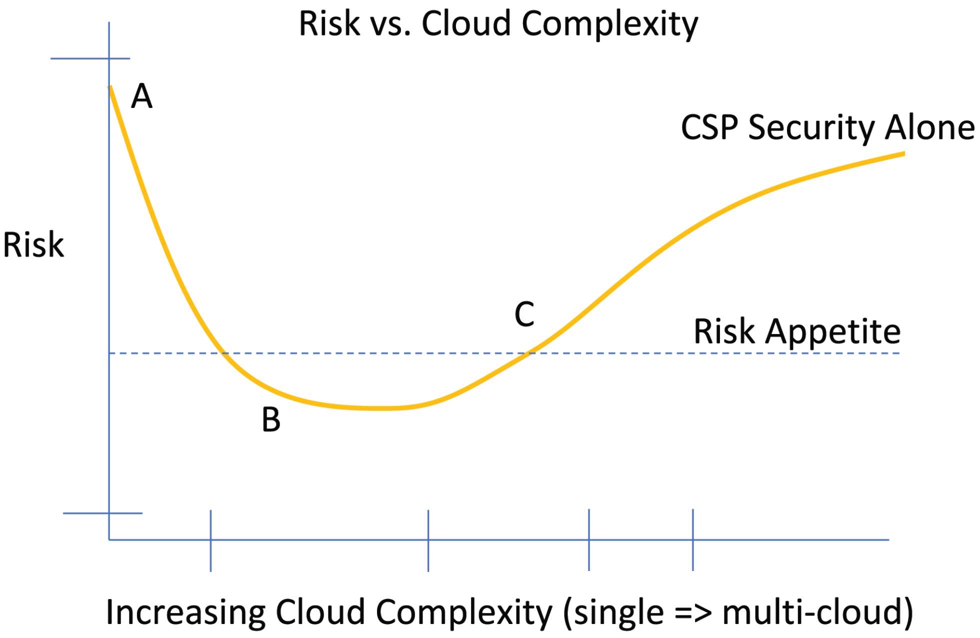


Figure 1 - Risk vs. Cloud Complexity

At point A, organizations deploying cloud workloads without implementing CSP security controls are assuming a level of risk way above the corporate risk appetite. One open SSH port or one weak AWS Console password is all it takes to give adversaries a natural entry point.

Point B is the sweet spot for CSP security controls. For an organization with minimal public cloud complexity (i.e., number of workloads, clouds, zones, etc.) proper and diligent implementation of CSP security controls is necessary and sufficient to bring cloud risk below the corporate risk appetite level and on-par with on-premises IT workload risk. The CSPs will argue that their intrinsic security posture makes it possible for lower risk in the cloud than on-premises for organizations at this level of cloud complexity.

As complexity increases (point C), the CSP controls remain essential but rapidly become insufficient to maintain risk. The challenges of managing controls across diverse cloud environments with different approaches, capabilities, UIs, and architectures make it impractical and unsustainable to rely on CSP controls alone. Even those organizations that are single-cloud today can quickly become multi-cloud due to business requirements, developer preference, or M&A activity. The goal of enterprise security should be to adopt a cloud security approach that enables and supports rapid business shifts and is forward-looking. This security approach accelerates corporate innovation and profitability.

Gaining Security Effectiveness While Managing Risk

If your organization is further to the right on the chart, the ideal way to normalize cloud risk is augmenting CSP security controls with a unifying security control layer. This unifying security control layer facilitates the right balance of audit, visibility, protection, detection, and automation as a basis for managing risk in the cloud. For example, audit is only as effective as visibility since one can only record what one sees. Similarly, organizations must balance protection and detection controls. Both are essential to blocking a breach. However, heavy-handed protective controls can drive up IT friction by putting limits on developers. For example, instituting rules that prevent all SSH and RDP ports (blocking test and development access) versus a more nuanced rule set that prevents RDP/SSH in a specific context, for example in production only.

DivvyCloud provides a unification layer to work in concert with the underlying CSP security controls. By leveraging a resource model they delivers universal monitoring and controls across clouds including AWS, Azure, GCP, Alibaba Cloud, and Kubernetes. DivvyCloud monitors and remediates cloud and container misconfigurations and policy violations. Allowing customers to achieve continuous security and compliance and realize the benefits of cloud and containers.

DivvyCloud sits inside the virtual private cloud, providing the visibility, governance, and trust necessary to address cloud security.

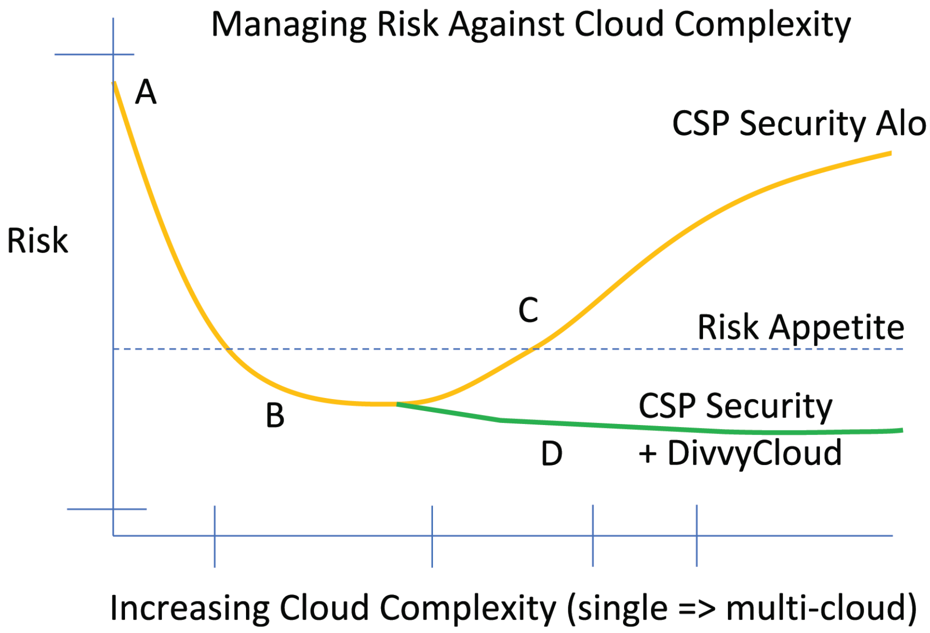


Figure 2 - Managing Risk Against Cloud Complexity

As shown in Figure 2, adding a solution like DivvyCloud facilitates keeping cloud risk below the enterprise risk appetite. By balancing and augmenting the audit, visibility, protection, detection, and automation aspects of CSP controls, DivvyCloud improves cloud security by:

- Sitting inside the VPC with protected visibility of Continuous Integration/Continuous Deployment (CI/CD) activity. Placing guardrails around which DevOps can safely provision and configure resources.

- Adding a unified compliance configuration management layer across clouds for maintaining compliance with standards and regulatory requirements including PCI-DSS, HIPAA, GDPR, SOC 2, ISO 27001, CSA CCM, and CIS benchmarks.

- Simplifying risk management through extensive use of controls and automated workflows that align with security standards like NIST CSF and NIST 800-53, reducing both the level of work and level of SecOps resources necessary when compared to managing risk with CSP security tools alone.

- Automating protective security control establishment and enforcement to strengthen and support detective controls.

Conclusion

Breaches of cloud data are on the rise, and the primary cause is a misconfiguration of cloud workloads (including serverless workloads) and the CSP user interfaces to manage the workloads. The good news is CSPs provide a wide range of comprehensive security tools to help manage the audit, visibility, protection, detection, and automation of these workloads. The not so good news is achieving the right balance of cloud security is increasingly difficult as the complexity rises. For simple cloud implementations – with proper setting of security controls – CSP tools are sufficient to manage enterprise risk in the cloud. For more complex deployments, CloudOps or SecOps teams require a unifying security control layer to balance and boost the audit, visibility, protection, detection, and automation aspects of CSP controls to manage enterprise risk in the cloud.