Cloud Platform Security and Monitoring

Joe Partlow, CTO
3 Steps to Securing Enterprise Data on Cloud Platforms

How to improve security and monitoring of Amazon Web Services, Microsoft Azure and Google Cloud Platform

Enterprises have leveraged cloud platforms such as Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP) to facilitate web applications for years, and the platforms have proven effective and reliable. That’s why many enterprises have begun taking advantage of the scalability provided by these platforms to assist with traditional network needs such as Directory Services, user document storage, and internal operational applications.

While this can deliver accessibility and storage benefits, many organizations that move critical infrastructure to these cloud platforms mistakenly assume that the cloud provider also delivers sufficient visibility and monitoring of the cloud environment — and therefore fail to configure critical controls and secure architecture practices, leaving them vulnerable to attacks.

Yet by properly configuring the excellent controls provided by popular cloud platforms, monitoring performance and security information and event management (SIEM) integration, and partnering with the right Cloud Application Security Broker (CASB), enterprise organizations can ensure consistent and convenient security of their data stored on AWS, Microsoft Azure and GCP.

Common Cloud Platform Risks

To begin securing cloud-based data, enterprise architecture and security teams must first understand that configuring these cloud-based security options is not straight forward, though many of the risks facing a standard on-premise architecture — such as improper segmentation, overly permissive firewall rules or weak passwords for remote servers or VPNs — still exist in a cloud environment.

Systems must also log and monitor new risks, including exposure of application program interface (API) keys in source repositories or open web directories, overly permissive data storage buckets and Secure Shell (SSH) keys available openly in source repositories. Attackers have successfully used all of these to breach systems recently.

Cloud environments are also not exempt from any compliance regulations required for on-premise environments. Business leaders often assume that cloud platforms provide these key controls, and only realize that’s not happening when a violation occurs.

Default configurations for AWS, Azure and GCP often don’t turn on event logging, encryption, data retention, multifactor authentication or other preventative controls that ensure compliance. They also don’t automatically correlate information to SIEM and logging systems and will need to be setup properly to comply with General Data Protection Regulation (GDPR) rules.
Step 1: Configuration that maximizes security of cloud platform architecture

Most cloud platforms include some built-in security features and applications to ensure proper data protection, and knowing which features your platform already provides is critical for determining which services you can expect from your provider, and which services internal security teams must perform.

Amazon Web Services (AWS)

AWS seems to have the most flexible automation and DevOps capabilities with its comprehensive API and scripting abilities, and includes many powerful networking options to secure the environment. Some common techniques used for securing the AWS environment include:

- **VIRTUAL PRIVATE CLOUDS (VPC)**
  Provide network isolation that can take advantage of subnet segmentation with public and private subnets.

- **CLOUDTRAIL LOGGING**
  Enable visibility into potentially unauthorized changes to the platform.

- **SECURITY GROUPS**
  Lock down individual Elastic Compute Cloud (EC2) instances or categories of instances; functions much like a virtual firewall.

- **AWS RDS (RELATIONAL DATABASE SERVICES)**
  At-rest encryption for data.
Microsoft Azure

Azure provides many built-in security mechanisms and currently has more application-specific protections than AWS or GCP. Here are the common items used to lock down the Azure environment:

• OPERATIONS MANAGEMENT SUITE (OMS)
  Perform event viewer searches, runbook automation using PowerShell (similar to AWS Lambda functionality) and improve visibility into the environment with built-in dashboards.

• AZURE APPLICATION GATEWAY
  Web application firewall (WAF) and load-balancing capabilities.

• SQL THREAT DETECTION
  Monitor potential vulnerabilities, access or injection attempts to the databases in Azure.

• STORAGE ENCRYPTION
  Service to automatically encrypt when writing data, also can encrypt VM disk via bitlocker and perform SQL transparent data encryption (TDE).

• AZURE VIRTUAL NETWORK (VNET)
  Similar to the AWS VPC, used to isolate networks away from each other.

• NETWORK SECURITY GROUP (NSG)
  Built-in firewall capabilities within Vnets.

• SECURITY CENTER
  Provides policy management, threat detection, and alerting and dashboard visibility.

• AZURE ACTIVE DIRECTORY IDENTITY PROTECTION
  Provides features such as light user behavioral analytics (UBA) and single sign-on (SSO) capabilities. An extremely powerful feature is the ability to extend your local Active Directory configuration to Azure, greatly reducing duplication of efforts around user management and permissions.

The Azure Security Center application is an invaluable tool that provides many security enhancements around setting security policies and recommendations, application whitelisting to restrict unauthorized applications from running and “just in time” virtual host access by allowing inbound traffic for the NSG for a set amount of time based on role. Security Center can also ingest threat intelligence from other products such as Office 365, the Microsoft Digital Crimes Unit and the Microsoft Response Center — providing additional threat correlation from their wide customer base. Also included: Behavioral Analytics that can identify suspicious process execution, malware infections, lateral movement attempts, malicious scripting or bad outgoing traffic.
Google Cloud Platform (GCP)

Google's cloud environment also provides a VPC environment similar to the AWS platform but with less overhead infrastructure than traditional VPCs. GCP also allows for the traditional segmentation, firewall and access control feature most cloud platforms provide.

One of the major security-specific features is the Cloud Security Command Center, which provides key features for monitoring and securing the GCP platform, including:

- **ASSET DISCOVERY AND INVENTORY SCANNING**
  Scans the App Engine, Compute Cloud and Cloud Storage/Datastore platforms.

- **CLOUD DLP**
  Discover potentially sensitive data contained in the data storage buckets.

- **APPLICATION VULNERABILITY SCANNING**
  Uncovers potential injection and scripting vulnerabilities in hosted applications.

- **ACCESS CONTROL MONITORING**
  Ensures the correct access control policies are in place.

- **ANOMALY DETECTION**
  Identifies potential threats from botnets, malware communications or other suspicious traffic in or out of the GCP environment.

- **INTEGRATION WITH TOP SECURITY TOOLS INCLUDING CLOUDFLARE, CROWDSTRIKE, PALO ALTO NETWORKS AND QUALYS**
  Detects potential distributed denial-of-service (DDoS) attacks, infected endpoints, policy violations, network attacks and per-instance vulnerabilities.

- **INTEGRATION WITH THE STACKDRIVER LOGGING PLATFORM AND CUSTOM APIS**
  Integrates with other business intelligence tools such as Tableau or Power BI.

Google’s cloud environment also provides a VPC environment similar to the AWS platform but with less overhead infrastructure than traditional VPCs.
Step 2: Monitoring the cloud through SIEM integration

To see what is happening in the cloud environment and export those logs into an alerting engine such as a SIEM, enterprise organizations must plan a cloud-logging strategy, which begins by answering the following questions:

- **WHERE WILL THE LOG AGGREGATION AND FILTERING TOOLS RESIDE?**
  This often depends on the location of the data, but it’s more efficient to have the collection tools doing the filtering and aggregating as close to the source as possible. Compliance may dictate where the raw log data has to live. France, Germany, and many other countries have strict laws against exporting potentially sensitive personally identifiable information (PII) as well as the new EU GDPR regulations.

- **HOW BIG ARE THE INTERNET CONNECTIONS BETWEEN YOUR CLOUD ENVIRONMENT AND LOCAL DATA CENTERS?**
  It may be more cost effective to keep the raw data at both places and send the actionable events used in your alerting rules to the central SIEM or monitoring tool. Sometimes there may be a logical split in your organization to make this more feasible — for example separate, distinct corporate divisions or business units.

- **HOW WILL YOU COLLECT AND PARSE CLOUD INFRASTRUCTURE LOGS?**
  In addition to the standard operating system or application logs from the servers, many essential “behind the scenes” cloud infrastructure logs should also be gathered and monitored for unauthorized/malicious activities.

After answering those questions, consider the common methods of log collection and SIEM integration used by your cloud provider — detailed below.

---

**AWS**

Amazon includes a consolidated way to pull all AWS logs via the CloudTrail product. CloudTrail logs all application program interface (API) calls to the environment from the console API or command-line interface (CLI). It uses a RESTful API to integrate into the other AWS applications and can aggregate logs from multiple instances and regions.

Some of the more actionable CloudTrail logs are starting or stopping of an instance, creation or deletion of users within AWS and logins to the platform. The CloudTrail log is formatted differently for many AWS resources but each event mostly contains the following information:
Azure

Azure has a couple different ways to log the events happening within the architecture. The easiest method uses the Azure Event Hub functionality to configure your Azure applications to send all the logs to these Event Hubs that function like a typical event broker, such as Kafka or Redis, and provide queuing and streaming capabilities.

Applications that provide the most essential logs are from the Azure Resource Manager, which logs all the administrative activities and the Security Center logs that collect from agents on all the Azure hosts and the built-in host-based Intrusion Detection Systems (IDS). Other useful applications include the Network Security Group Flows — which logs connections to and from virtual machines — and Azure Active Directory, which logs normal administrative Active Directory activities such as authentication success or failure, users and groups created or deleted, and account lookup information.

A second method is to use Log Analytics, which is a part of the Operations Management Suite (OMS). Source data is stored in the repository for alerts, dashboards, searching or export and captured using agent on either Windows or
Google provides a convenient logging infrastructure with its Stackdriver platform. Stackdriver can feed into a publisher/subscriber (pub/sub) model that is easily integrated with a SIEM or open source logging tool.

Start by creating a project within GCP that contains your various Google resources that will be generating logs. Once the project is setup, create a pub/sub that contains all logs for the project, or isolate the logs for each resource by creating a pub/sub for each.

Below is a sample logging pipeline to consume logs, as defined by the Google team:
Step 3: Expanding security through Cloud Application Security Brokers (CASBs)

While not an all-encompassing enterprise platform, CASB solutions provide granular auditing capabilities at the application or site level and require the same logging and monitoring considerations as the full-fledged cloud platforms.

Most CASB solutions have similar capabilities or deployment considerations via proxy or API, and are essential for incident response and forensic investigations since monitoring and alerting on unauthorized access to cloud services is often critical to detecting potential insider threats. Compromising Salesforce, Office 365 or Dropbox could be devastating to an organization since many of the corporation’s sensitive documents are stored in one or more of those applications. Data classification and/or DLP needs to also extend to these cloud services for consistent coverage and management.

While providing an additional layer of security is the primary function of CASBs, comprehensive IT security providers such as ReliaQuest offer advanced services that turn security activities into valuable business insights.

The ReliaQuest Answer

Building on our ingestion layer called rqTRANSLATE, ReliaQuest has created data storage capabilities in the major cloud platforms that can scale and adapt to handle the most demanding enterprise data analytics needs in a module called rqVISION.

rqVISION is an optional capability that helps determine what data needs to be processed by the different technologies such as SIEM or EDR, and what data sources or individual events don’t make sense to process in those technologies. This other data is often useful for investigations, hunt activities, long-term trending or providing insights to other areas of the company, such as application development, infrastructure or business intelligence teams.

Some data processed while securing cloud platforms may not have high relevance for security tools, but it can have a major operational benefit to the organization by providing valuable
business intelligence. rqVISION gives the organization the ability to store and analyze as much of this type of data as it would like for as long as it would like, leveraging the scalability provided by cloud platforms.

The flexibility of cloud platforms makes it possible to allocate the storage level required by compliance standards or as deemed necessary for analytics — based on the amount of data and desired storage length — in a pay-as-you-go model.

rqVISION also delivers data visualizations according to the specific needs of each enterprise, tailoring output to each individual enterprise organization and providing data insights to other business analysis teams beyond just those in security.

When paired with proper cloud platform security configuration and sophisticated monitoring of performance and SIEM integration, rqVISION can ensure consistent security of data stored on AWS, Microsoft Azure and GCP, while also giving businesses a competitive advantage and actionable-insights to better meet customers’ needs.