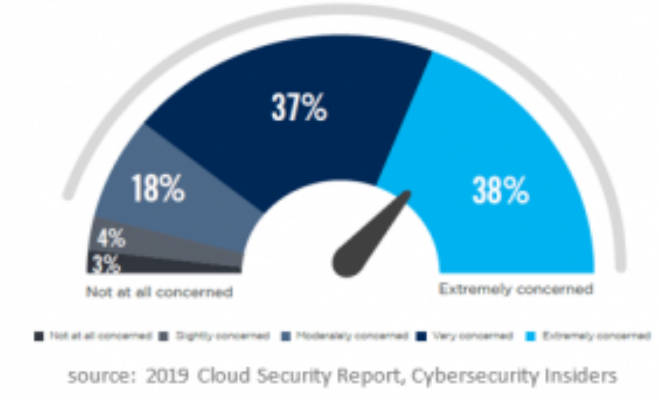
HOW TO SECURE YOUR PUBLIC CLOUD

INTRO

The public cloud is the incubator of change. Use of cloud IaaS (Infrastructure as a Service) and PaaS (Platform) services is growing 24% YoY, reaching $90 billion in 2020. Cloud sprawl, change velocity, scrum teams, CI/CD pipelines – your cloud footprint is constantly changing, which complicates cloud security. To underscore the point, 93% of IT execs are moderately to extremely concerned about their cloud security. This blog offers some guideposts on the journey to securing your public cloud, including items like automated configuration, cloud server patching, asset discovery, and more.



source: 2019 Cloud Security Report, Cybersecurity Insiders

AUTOMATE CONFIGURATION SECURITY & COMPLIANCE

Misconfigurations are the #1 cause of cloud security failures, so we begin here. AWS, Azure, and Google Cloud offer hundreds of IaaS and PaaS services in their catalogs which developers devour as they deploy cloud-native apps. Every instance of those IaaS and PaaS services must be appropriately configured to be secure, a responsibility which falls solely on the enterprise, not the

CSP.

Thankfully, the CIS (Center for Internet Security) publishes benchmarks detailing how to securely configure IaaS and PaaS services. Even so, enterprises continue to struggle. The list of high-profile exposures includes such misconfigured resources as:

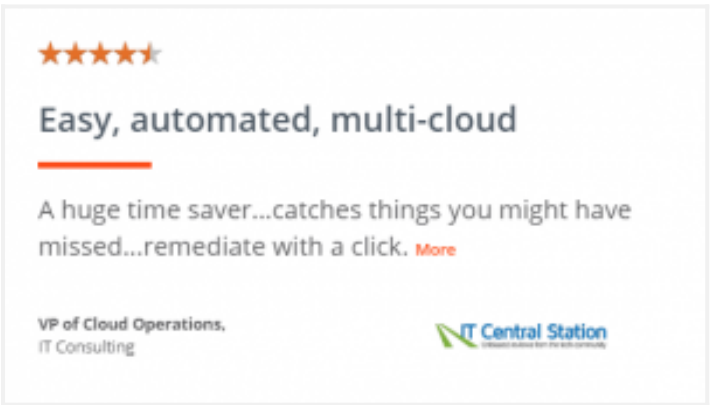
- S3 buckets (here, Lion Air, Ford, TD, Netflix, plus a non-exhaustive list),
- Elasticsearch clusters (Honda Exposes Vehicle Owner Records), and
- web application firewalls (Capital One 2019).

As the saying goes, an attacker only has to be right once. While automation has made it all too easy for bad actors to probe our cloud defenses, so too can automation become our best defense.

Automating policy-based configuration security checks against the CIS recommendations is a good start. These checks should not only happen on a periodic cadence (for trend analysis, etc.) but also the moment a new resource is deployed, or an existing resource modified. This is known as **event-driven security**. Yet simply pointing at a misconfig is not enough, which brings us to our next recommendation.

AUTOMATE REMEDIATION

Automated remediation brings many benefits, not the least of which is continuous, real-time security, plugging the gap immediately, in the moment of change, to prevent data exposure in the white spaces between scheduled sweeps. Just as the configuration policies are under centralized governance of your Security and Compliance Team, so too should remediation action, to drive consistent configurations across the dynamic enterprise. Exceptions can be managed/approved as needed. Automation also eliminates human error, diminishing the prospect of disruptive rework or costly service outages. Now, before you object about the dangers of automation run wild, be assured that we will soon discuss the virtues of change management.

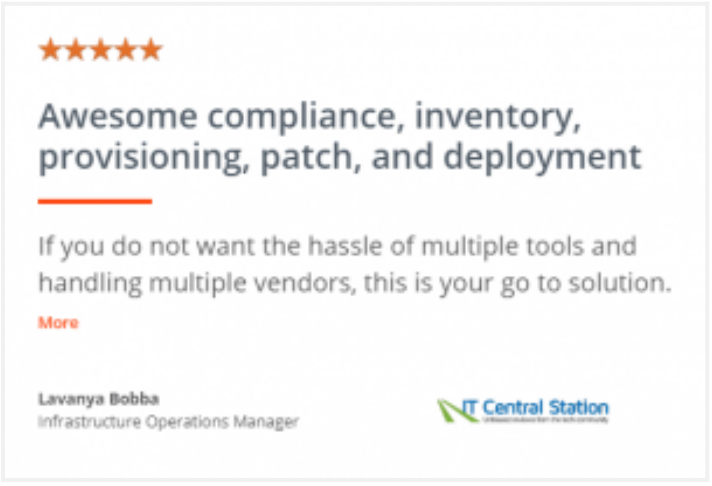


AUTOMATE CLOUD SERVER MANAGEMENT

Patching and OS compliance of virtual cloud servers are also the responsibility of enterprises under the Shared Responsibilities Model. Given that the speed and scale of change challenge cloud security posture management (CSPM), one might rightly infer that manual efforts to locate new cloud server instances and add to the backlog of servers to be patched are likely to fall short. Here too, automation is the solution.

Automatically find and enroll every newly deployed cloud server instance (e.g., AWS EC2) into an

automated server management solution. Then, you can schedule **automated patch jobs** to keep your cloud servers' guest OS patched and updated. Having a single context from which to manage servers, whether on-prem, virtual, or cloud is helpful and, where possible, highly recommended.



CLOSE THE LOOP ON INCIDENT & CHANGE MANAGEMENT

Given the pace of change and the importance of quickly resolving resource misconfigurations, automating incident ticketing and enrichment and orchestrating change management are key to managing change smoothly and maintaining an audit trail. Perhaps incident management is overkill for developers in their DEV accounts but consider production operations. The moment a misconfigured resource is identified in PROD, a security incident ticket is opened and supporting security details are automatically shared with the ITSM solution. The developer responsible for the app will be automatically alerted. When the developer goes to remediate the configuration, a change request is created, and the change management workflow initiated. Once approved, the change goes live, the CMDB updated, and the ticket closed. The vulnerability window is minimized, and a fully documented audit trail recorded.

KNOW WHAT'S IN YOUR CLOUD

Developers can be an eager and capable force multiplier for an overburdened Security and Compliance Team. Developers view their professional world through the lens of their application or microservice, so let's show them their cloud security posture through that same lens. Intuitively, this implies a need to know what resources are deployed and how they interconnect within their cloud footprint. With **asset discovery** automatically locating cloud resources and mapping their dependencies, developers can exert more directed force on their app's security and compliance. There is another key component to achieving this goal: simplify security.

DEMOCRATIZE CLOUD SECURITY

If we **simplify cloud security posture management for the developers**, we increase their cooperation in the common cause of securing our cloud footprint. An **automated** CSPM solution should ingest asset relationships and logical groupings to present the security posture of their IaaS, PaaS, and containerized resources in an **app-centric** view. This implies multi-tenancy – you have more than 1 development team, and they only need to worry about their app's posture. It also implies role-based access control – you would not want a developer changing the configurations of

resources which are not in their app. Ideally, the CSPM solution should be **multi-cloud**, because asking a developer to drive a handful of security solutions in AWS, another set in Azure, and yet another in Google Cloud is neither simple nor agile.

ARCHITECTURAL DESIGN SECURITY

A beautiful aspect of the public cloud is you can **build security into the design** of your business services. You can begin by understanding what architectural options exist with your CSP, and your organization's Cloud Architect should be able to provide valuable guidance to the app development teams. Consider the following simple example in Figure 1 built in AWS with a combination of IaaS and PaaS services.

Let's say you have some business service which you have migrated to the cloud and which now runs on an EC2 instance. This EC2 will be fed data records from your on-prem data center. For expediency and simplicity, data encryption/decryption is not shown but assumed.

Cloud network segmentation. Firstly, you can segment that workload off from any other workload in your cloud by **giving it its own VPC** (virtual private cloud). Some organizations will also dedicate a specific cloud account to each workload, shown here as well. Network segmentation is a means of mitigating blast radius, should a compromise occur.

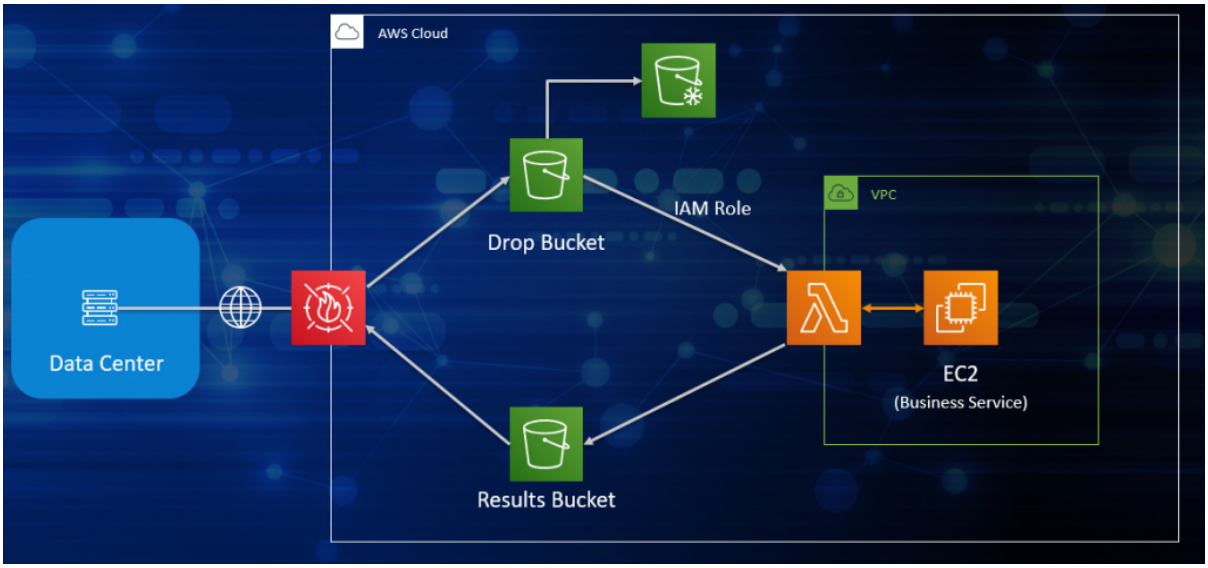


FIGURE 1: SIMPLE BUSINESS SERVICE ARCHITECTURAL DESIGN EXAMPLE

Web application firewall. A WAF is a highly effective means of protecting your cloud apps from common exploits, through security rules which you define to control and/or block certain types of traffic. For example, you can create a security rule to only accept traffic from specific IP addresses, such as from your on-prem data center.

Data IO and Service Endpoint. Once admitted through the firewall, the data are simplify dropped into an S3 bucket. (Every IaaS and PaaS resource in this example will be securely configured by your automated, policy-driven CSPM solution.) Data in the drop bucket will trigger a serverless AWS Lambda function to give the data to the business service running on the EC2. Results are returned to the Lambda function for transfer into the results bucket. Note that the Lambda function was the sole endpoint: only it could trigger the business service. IAM roles in this architecture are discussed in the next section.

IAM

Appropriate IAM roles and policies provide only the **least privileges** necessary to get the job done. In the example of Figure 1, you would create an IAM role for the Lambda function to access the S3 drop bucket, a separate IAM role for the Lambda function to trigger the EC2, and yet another to write to the results bucket. With appropriate IAM roles, only the Lambda function could write to the drop bucket in the example above.

Multi-factor authentication (MFA) is critical due to the broad access and to offset the risk of a cloud account takeover attack.

NOTE: MFA is mandatory for adequately protecting highly privileged accounts, as compromised admin credentials represent the greatest threat to an enterprise cloud.

The CIS benchmarks for IAM include several, high-value recommendations, including but not limited to the following:

1. DO NOT create IAM policies that allow full admin privilege
2. DO require MFA for all IAM users with a console password
3. DISABLE credentials which have been unused for more than 90 days
4. ROTATE access keys every 90 days or less

There are several additional rules within the framework which speak to the importance of least privileges.

OTHER RECOMMENDATIONS

In addition to IAM, CSPM, discovery, and architectural security, here are some other key points to consider in securing your public cloud footprint.

- **Key management**. Absolutely essential. Rotate data encryption keys regularly and store them separately from the decryption engine. Look for a managed key service from your CSP which greatly simplifies key management.
- **Encrypt data at rest and in transit**. Your CSP should have data encryption options when storing data. When transferring data between various cloud network segments, use encryption. These use cases also tie back to key management and IAM roles.
- **Event logging**. Storage is ridiculously inexpensive. There is no excuse not to enable event logging such as AWS CloudTrail, incredibly valuable for forensic analysis. After a certain time period, you can automate data transfer to long-term "cold" storage for more savings.
- **Automation**. To err is human, so automate what you can to minimize errors, rework, and disruption. Cloud configurations, discovery, and ticketing should be automated as much as possible to track with the speed and scale of change.

CULTURAL ASPECTS

Executives know the important role culture plays in helping organizations achieve their objectives. With the speed the cloud enables and the implications to your business, consider the following aspects to bolster your cloud security.

Foster cross-functional collaboration. Devise incentives that create collaborative muscle memory

among app developers, IT operations, and security experts. Offer career development opportunities such as cross-functional training and project assignments to spark new ideas. Invite Operations, Security, and Compliance to sprint retrospectives.

Encourage risk-taking. Do not punish teams for making small bets, iterating, and learning. Be open to new ideas and create an environment that makes it safe to fail.

Gamify security. Have a monitor on display – near the elevator, the break room, wherever – showing KPIs across various scrum teams' security posture. Healthy competition is good but keep it light: you want the developers sharing best practices.

SUMMARY

While devising an effective multi-cloud security strategy requires many interworking pieces and considerations, an easy win is to begin by addressing the #1 cause of cloud security failures, misconfigured IaaS and PaaS resources. A multi-cloud CSPM solution automates policy-driven configuration management and, ideally, remediation; policies and remediation actions would remain under centralized governance to drive consistency across the enterprise's rapidly changing cloud footprint. Moreover, one must also take care to automate cloud server patching and OS compliance, given how popular cloud IaaS services such as AWS EC2 or Azure VM have become.

Developers represent an eager and capable force-multiplier for an overburdened Security and Compliance department, so simplifying security for those developers is instrumental to success. Present an app-centric cloud security perspective to the various scrum teams, achieved by integrating your CSPM solution to automated asset discovery. Orchestration of incident and change management accelerates responsiveness and business agility. Architectural considerations can augment your security efforts, and the principle of least privileges should be central to cloud security.

CLOUD SECURITY SUCCESS CHECKLIST

- automate policy-based IaaS and PaaS resource configuration checks and remediation
- automate cloud server (AWS EC2, Azure VM) patching and OS compliance
- automate asset discovery and application dependency mapping
- orchestrate security incident and change management
- architect your cloud applications for security
- turn on event logging
- apply the principle of least privileges to IAM
- consider a managed key service
- encrypt data at rest and in transit

BMC SOLUTIONS

BMC has a wealth of solutions which work together to automate and secure the hybrid cloud enterprise.

- Adding **BMC Helix Vulnerability Management** to your arsenal super-charges security backlog grooming and automated remediation for hybrid cloud servers and networks.
- **BMC Helix ITSM** provides industry-leading incident management, while **BMC Helix Discovery**

enables security posture management through an app-centric lens.
- And **TrueSight Orchestration** keeps all the multi-faceted process runbooks running smoothly together.

To learn more about BMC Software's portfolio for securing the hybrid cloud enterprise, please visit bmc.com/remediate, or contact us for a conversation about your specific security challenges.