Policy and Security Automation using AWS Control Tower

Contents

Renewing the approach to cloud account vending

As automation and X-as-code proliferate the cloud space, many organizations are beginning to rethink their cloud account management processes. Traditional cloud account management relies on lengthy review and approval cycles, precise coordination between multiple teams, and perfectly choreographed hand-offs. Organizations are seeking to automate this process and cut down on wait times for newly vended accounts with security guardrails to increase velocity of workloads migrating to AWS.

AWS Control Tower has enabled organizations to accelerate their cloud account vending process. As a result, developers can now more easily obtain an AWS account and begin deploying workloads using native resources. This approach is in line with leading principles such as Agile and treating developers as customers; however, with this greater speed comes a need to secure not only the deployed resources, but also the cloud account itself and the processes used to create it. Deloitte set out to address these challenges by building Deloitte Cloud Account Management (DCAM), an offering built on top of Control Tower to help automate account provisioning and deploy preventive, detective, and corrective policy into existing and newly created accounts. The goal of these policies is to help establish a secure account baseline that limits developers' reach, enhances the Security Operation Center (SOC)'s visibility, and maps to compliance standards pertaining to highly regulated industries.

Challenge and context

Challenge: Lack of centralized management

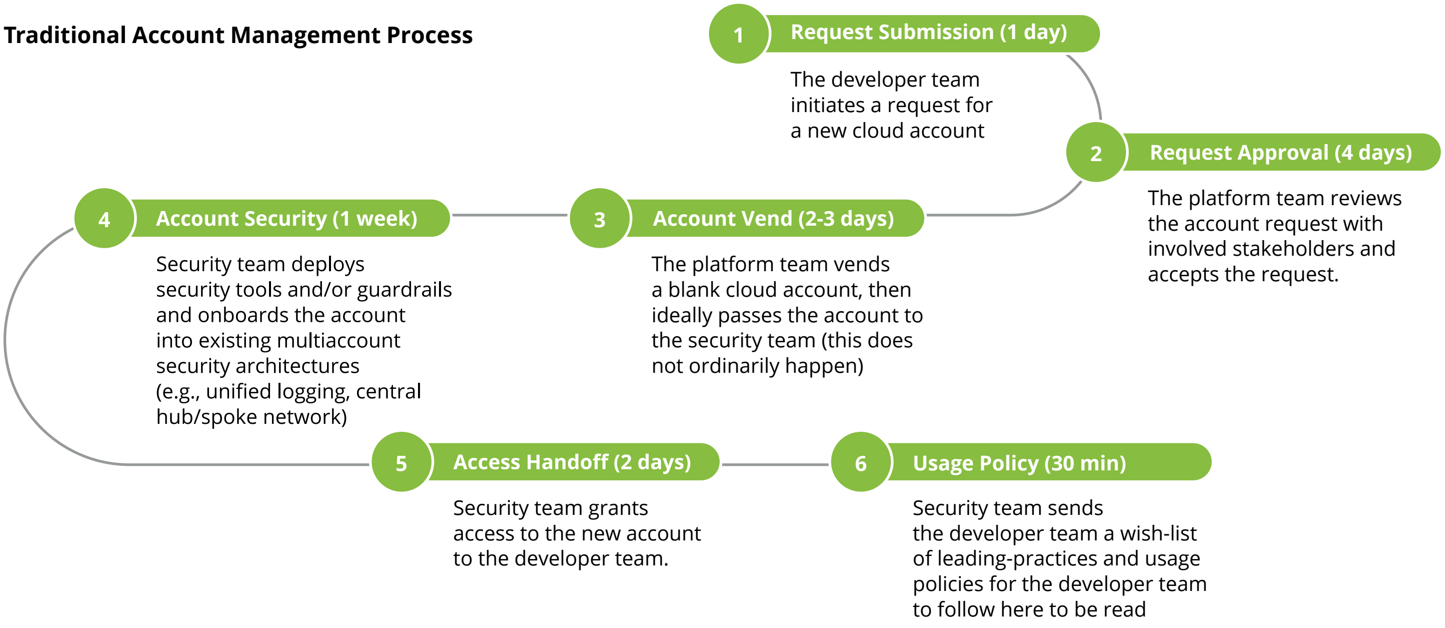
Companies moving to Cloud consistently underestimate the risks associated with an inconsistent cloud account management strategy. However, while an organization's presence in the cloud grows, minor variations in account baselines will turn into unmanageable number of alerts and results in risk exception culture and threat vectors being realized, leading security incidents.

Many organizations are facing account management challenges due to a lack of centralized cloud management that extends from the AWS organization level down to the resource level. This generally impacts the efficiency of roles, applications, services deployment, real-time visibility into identity and access management (IAM), and swift threat detection and response.

Traditional account management

Unfortunately, traditional account management procedures lack strategic and effective automation capabilities, resulting in a slow, painstaking process for those involved. The overall process may span over several weeks and can even last one or more months in some instances (see Figure 1). Ultimately, Deloitte has found that organizations that utilize automation can help to drastically reduce delays in account provisioning and improve the security posture of provisioned accounts.

Traditional Account Management Process



1 **Request Submission (1 day)**

The developer team initiates a request for a new cloud account

2 **Request Approval (4 days)**

The platform team reviews the account request with involved stakeholders and accepts the request.

3 **Account Vend (2-3 days)**

The platform team vends a blank cloud account, then ideally passes the account to the security team (this does not ordinarily happen)

4 **Account Security (1 week)**

Security team deploys security tools and/or guardrails and onboards the account into existing multiaccount security architectures (e.g., unified logging, central hub/spoke network)

5 **Access Handoff (2 days)**

Security team grants access to the new account to the developer team.

6 **Usage Policy (30 min)**

Security team sends the developer team a wish-list of leading-practices and usage policies for the developer team to follow here to be read

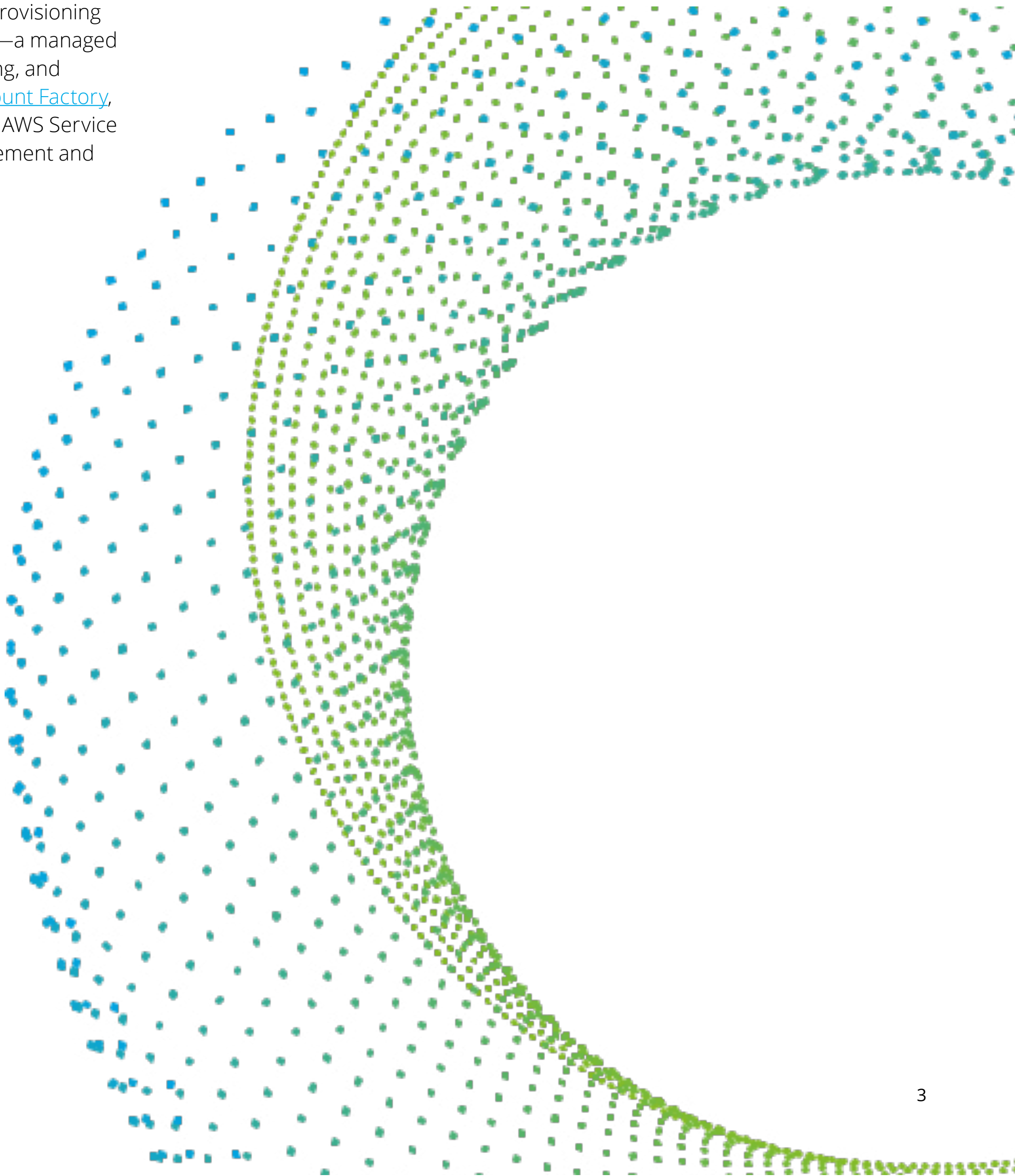
Figure 1 - Deloitte perspective of a typical example of traditional, manual account request and creation process.

Upon further analysis of the traditional account management process, Deloitte identified the following key takeaways:

- The existence of multiple handoffs slows the pace significantly.
- Security is not automated into the account provisioning process; and so, securing the account is often the most time-consuming step.
- Developer teams who have had to wait weeks for their new cloud account often blame security for the delayed process, and they are not likely to take heed of security's usage policies if it means more slowdowns.

What is Control Tower?

To help expedite and secure the account provisioning process, AWS implemented Control Tower—a managed service that automates the request, vending, and governance of AWS accounts through Account Factory, a console-based product that's part of the AWS Service Catalog. This solution provides the management and governance of secured landing zones and guardrails even for sensitive or highly regulated industry workloads at scale. By replacing their traditional account management process with Control Tower, companies can scale their AWS environments via automation (for more information on control tower features or capabilities see AWS documentation: What is Control Tower). But, as companies adopt Control Tower and scale their environments out, the need for a secure account baseline will grow proportionally. Deloitte has set out to address this need by building a solution on top of Control Tower that adds additional layers of security controls. In the subsequent sections we will dive deeper into the details of the solution.

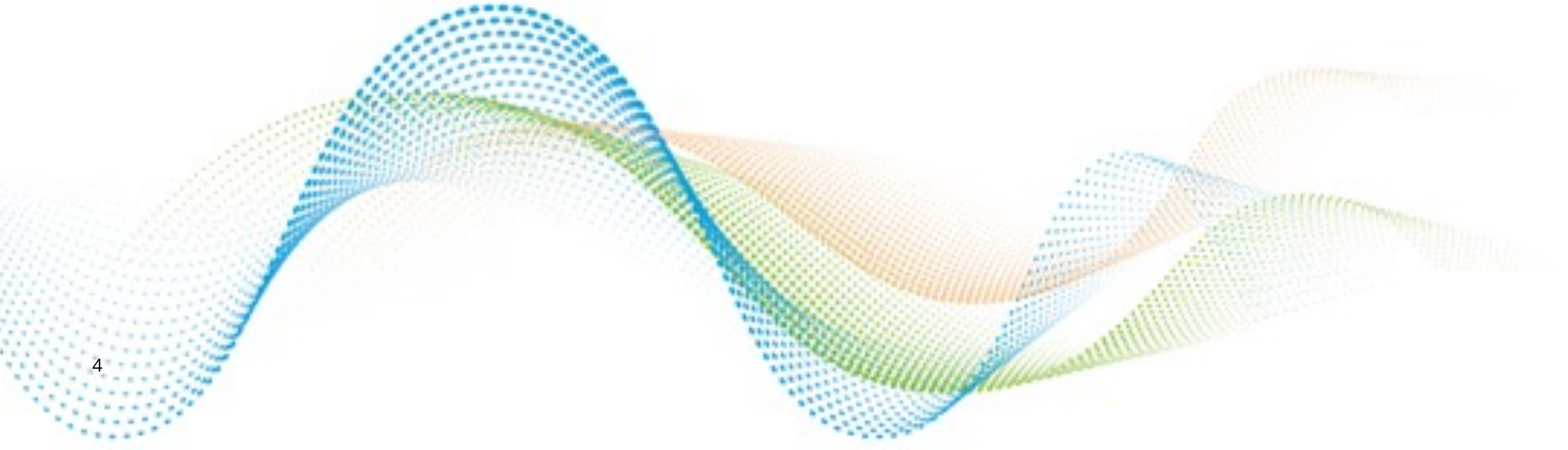


Solution Overview

DCAM exemplifies how companies can build on Control Tower to ease major frustrations encountered by security teams when deploying new accounts, such as: inability to keep up with large backlogs of new account requests, lack of visibility into newly vended accounts, and inconsistencies in account baselines leading to baseline drift.

To address these challenges, Deloitte's approach prioritized shifting Security left by building the entire solution as-code, to enforce consistency in account requests, deployed policies, and account baselines overall. An 'as-code' approach also enables repeatability in processing account requests. Additionally, Deloitte worked under the requirement that every component of the solution must easily integrate with multi-account CI/CD pipelines. AWS recently released pipelines for Control Tower environments (explained further below) that would enable organizations to standardize account baselines. By leveraging these pipelines, Deloitte could deliver their security assets and policies in a consistent and transparent manner.

This approach should resonate with many organizations, as it mirrors the goals that security organizations strive to implement in their own companies. By focusing on fully as-code and CI/CD-enabled solutions from the time of account creation, organizations can set these healthy security practices as a precedent for developer teams to follow by enabling guardrails.



Solution Components

Deloitte's DCAM solution rests on the innovation built by AWS. By leveraging AWS tools and solutions, Deloitte helps to reduce the number of components to manage, and those components managed by AWS will be backed by AWS SLAs. To complement AWS's solutions, DCAM's custom components extend security capabilities covered by AWS and bring those capabilities together into a cohesive solution. Ultimately, the various components included in DCAM make up a mosaic that can stretch farther than a custom-only or AWS-only approach. This is an important consideration when implementing Control Tower, as AWS is constantly expanding their security capabilities; so, it is up to the organization to develop alongside AWS rather than defaulting to custom solutions.

The foundational component of AWS Control Tower is the Controls Library (formerly called Guardrails), which are a set of preventive, detective, and proactive controls that enforce Cloud accounts' intended purposes. For example, one Control Tower control enforces that S3 buckets in the Log Archive account should be immutable by any person. Deloitte often recommends expanding upon these native controls, as is done in DCAM, by building a set of service control policies (SCPs) that can be implemented alongside them. These SCPs can enforce internal company standards, such as naming policies, tagging policies, and the blocking of company-prohibited AWS services.

On top of these custom preventive policies, Deloitte recommends implementing detective policies through AWS Control Tower, Config, Security Hub, GuardDuty, Inspector, and Macie. Detective policies that are enabled at the organization level will evaluate in every account, and the logs and findings from these services can be configured to automatically be sent to a central hub account. The goal of these detective policies is to provide visibility into misconfigurations and suspicious activity that would be too detrimental to the application's integrity to outright prevent. For example, broadly enforcing a standardized set of security group rules could overwrite existing security group rules that are critical to the application; so, in this case, it may be more efficient to simply detect out-of-compliance security group rules and perform a more precise and thoughtful remediation.

Layering onto the preventive and detective policy should be a set of corrective policies, enabled via auto-remediation. Pairing with the deployment of AWS Security Hub, DCAM deploys AWS Security Hub Automated Response & Remediation (SHARR). SHARR will take Security Hub findings, which are themselves mapped to industry standards such as CIS and PCI and run automated remediations on them from a single hub account. By complementing an org-level Security Hub deployment with SHARR, organizations can simultaneously view org-wide findings from a single account and remediate them without having to leave the hub account.

To extend the security benefits of AWS SHARR, DCAM also deploys Deloitte's custom Auto-Remediation Accelerator. Much like Control Tower's controls library, SHARR covers controls that map to AWS leading-practices and security baselines; however, organizations often need additional auto-remediation that can enforce internal policies and identify exception cases. Deloitte utilizes event-driven auto-remediation, so that the remediation action is triggered in near-real-time to decrease the amount of time that a resource is vulnerable. Deloitte's auto-remediation also allows for exception handling, so that specific resources can be exempt from auto-remediation if there is a business case. Additionally, custom auto-remediation can allow for customized default values for specific AWS services or accounts. This unlocks the potential to enforce company policies such as, "which encryption keys should be used in which AWS accounts," which is expanded upon in the Solution Benefits section.

What ties the entire solution together is, of course, standardizing this solution set across all AWS accounts. DCAM accomplishes this by leveraging AWS-created CI/CD pipelines, namely Customizations for Control Tower (CfCT) and Account Factory for Terraform (AFT). These two pipelines are integrated with Control Tower to support fully as-code account requests and customizations that can be managed from the organization's Version Control System (VCS). By building DCAM to be compatible with these pipelines, the solution enables users to deploy and enforce the policy-driven account baseline described above almost instantaneously at the time of account creation. Thus, the amount of time spent between account creation and hand-off to developer teams can be reduced. This acceleration will lower development costs, embed security into the account creation process, and reduce the friction between security and development teams.

Solution benefits

Deloitte Cloud Account Management enables the automated creation and provisioning of multiple accounts in a standardized format with security controls baked into the account template. These controls are layered to protect sensitive workloads and align with the needs of highly regulated industries. It is important to deploy and manage these controls in four categories, each delivering its own set of benefits – Automate, Prevent, Detect and Remediate:

- **Automate:** Customizations of the landing zone are achieved through Terraform infrastructure-as-code (IaC), CloudFormation templates and Service control policies (SCPs). Automated pipelines enable standardized deployment into all AWS accounts. Hence, the same security baseline is applied consistently on account creation and account updates. Multi-account security architectures leverage these pipelines, including internal architectures of enterprises. The diagram below (Figure 2) describes the process by which AFT provisions and customizes AWS accounts entirely via Terraform templates.
- **Prevent:** Custom Service control policies (SCPs) can augment Control Tower's out-of-the-box preventive controls and be tailored to fit each organization's needs. These SCPs are tailored to prevent specific activities on a client-by-client basis (e.g., using prohibited AWS services, adhering to naming standards). Preventive policy is often the quickest and simplest means to lay down guardrails when enabling new services and establish access perimeters (see the example in Figure 3 below). However, too strong of a focus on preventive policy will force developers to either slow down their processes, or, if possible, bypass security policy somehow. For that reason, Deloitte also deploys a robust set of detective policies.

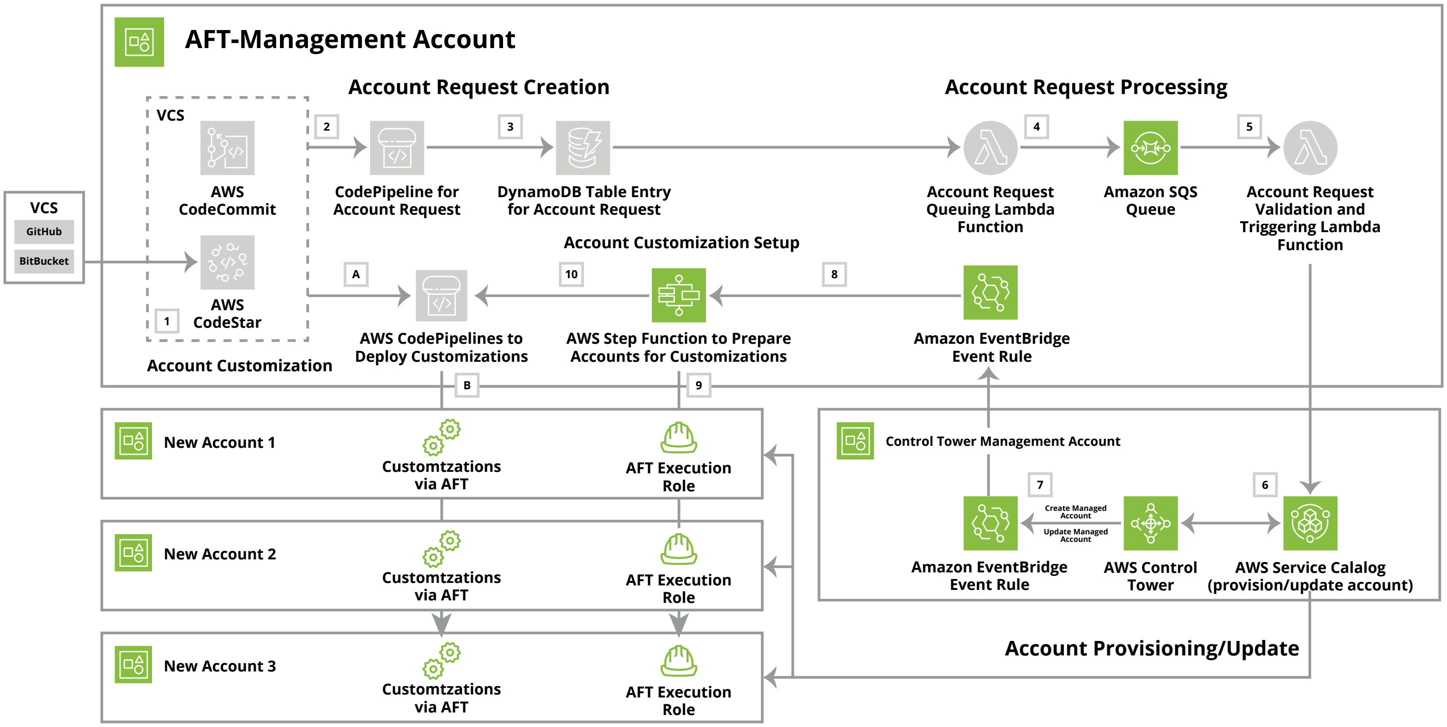

AFT-Management Account
Account Request Creation
Account Request Processing
VCS
2
3
4
5
AWS CodeCommit
CodePipeline for Account Request
DynamoDB Table Entry for Account Request
Account Request Queuing Lambda Function
Amazon SQS Queue
Account Request Validation and Triggering Lambda Function
VCS
GitHub
BitBucket
Account Customization Setup
A
10
8
AWS CodeStar
1
AWS CodePipelines to Deploy Customizations
AWS Step Function to Prepare Accounts for Customizations
Amazon EventBridge Event Rule
Account Customization
B
9
New Account 1
Customtzations via AFT
AFT Execution Role
Control Tower Management Account
7
6
Create Managed Account
Update Managed Account
New Account 2
Customtzations via AFT
AFT Execution Role
Amazon EventBridge Event Rule
AWS Control Tower
AWS Service Calalog (provision/update account)
Account Provisioning/Update
New Account 3
Customtzations via AFT
AFT Execution Role

Figure 2 - Architectural overview of AWS Account Factory for Terraform (AFT) pipeline for provisioning/updating AWS accounts. Steps 1-3 detail the automated account request process, where requests are submitted as-code from the VCS and are cataloged and processed in order. Steps 4-6 show the automated account provisioning process, where AFT pushes the account request to Control Tower and Service Catalog to provision the account itself. Steps 7-10 show the process of preparing accounts for customization, wherein an event-driven architecture deploys a role into the new account for AFT to assume when deploying customizations, as well as sets up a pipeline for AFT to deploy account-specific customizations. Finally, steps A-B detail the process for pushing account customizations (i.e., security baselines), where customizations are defined as Terraform files in the VCS and are deployed via newly-created pipelines into the target accounts.

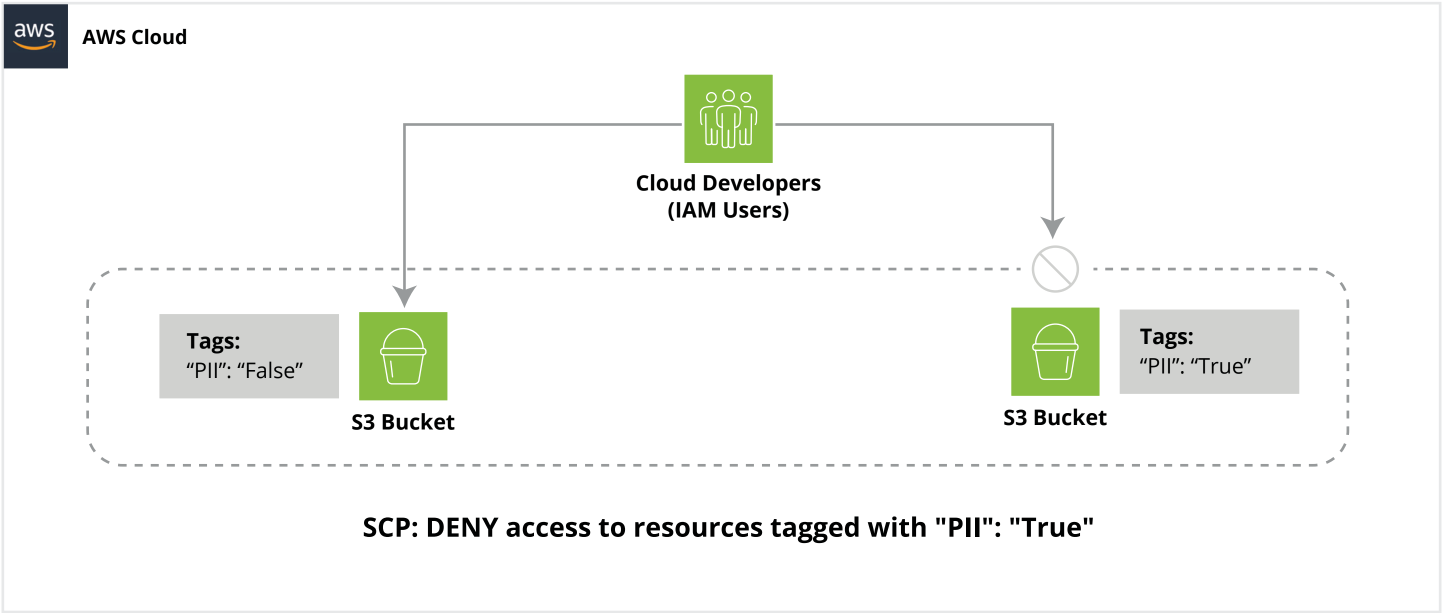


Figure 3 - Preventive SCP to block access to S3 buckets tagged with "PII": "True".

- **Detect:** Detective policy allows ongoing monitoring of non-compliance and suspicious behavior across AWS accounts. These policies are, by nature, non-intrusive; so, they give the security team visibility without breaking any critical applications or infrastructure. Detective policy can be easily enabled through AWS Security Hub and GuardDuty, among others. Security Hub facilitates AWS security leading practice checks and detects any deviations from the security standard, while GuardDuty continually monitors and detects any harmful threats and generates in-depth security findings for mitigation. Security Hub can also serve as a central destination for security alerts originating from any AWS-native and third-party security tools (see Figure 4). From Security Hub, findings and alerts can be configured to appear on the Control Tower console itself, if so desired. DCAM utilizes these AWS security services and offers additional industry mappings relevant to highly regulated industries (e.g., CIS, PCI, HITRUST, FedRAMP). These policies can then be grouped by affected service, enabling further visibility into insecure configurations and use of newly enabled AWS services.

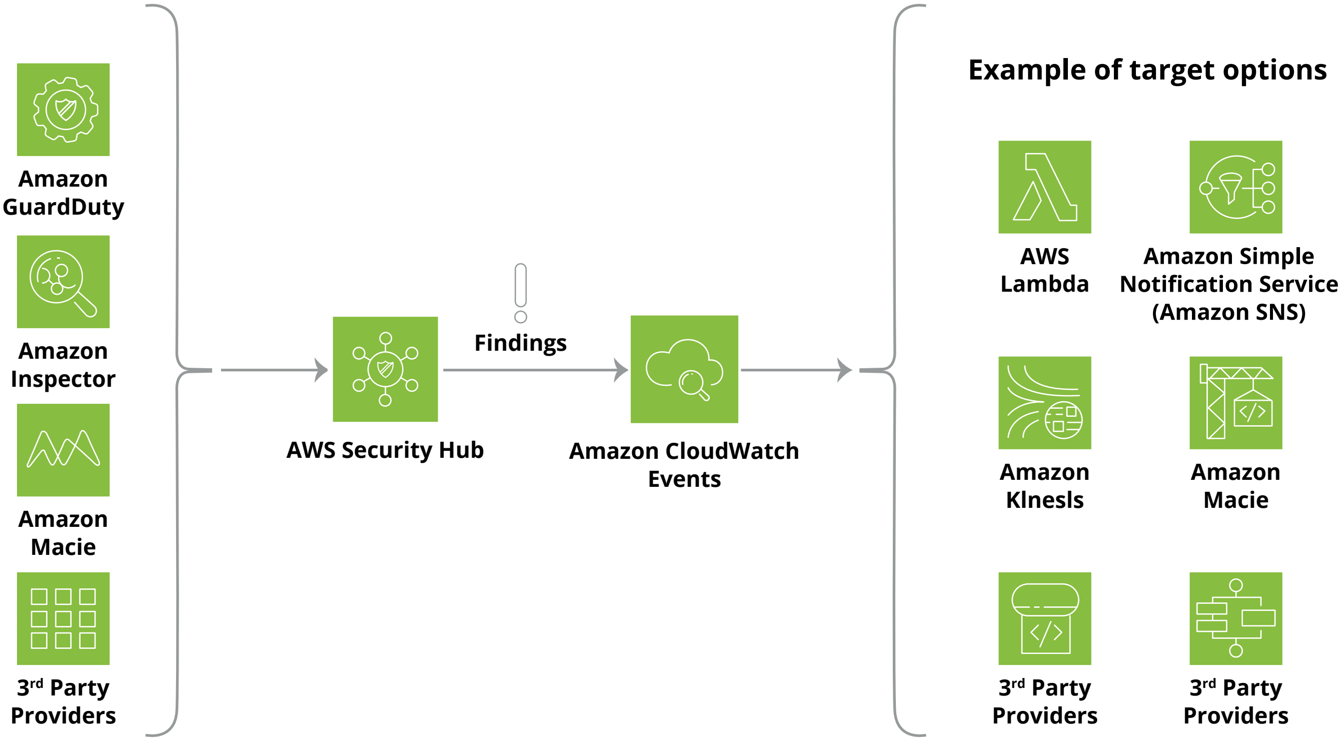


Figure 4 - DCAM leverages AWS's ability to centralize security alerts into a single account and manage these alerts through a single Security Hub instance. Picture taken from AWS Whitepaper: Navigating GDPR Compliance on AWS, April 2022

- **Remediate:** Auto-remediation has become a cornerstone of continuous compliance. DCAM uses auto-remediation policy to help enforce strong security standards that can integrate with, and not oppose, the development process. Deloitte's custom auto-remediation is both cloud-native and event-driven, so remediation happens in near-real-time. This architecture corrects vulnerabilities in seconds to minutes, a drastic improvement from most auto remediation tools. Remediations are most beneficial when mapped to detective policy, as is the case with SHARR and Deloitte's custom Auto-Remediation; and, in most cases, remediations should also be mapped to industry standards. This allows for companies to help improve their security posture against industry benchmarks without a large toll on SOC teams. Additionally, one of DCAM's differentiators is that its remediations allow for customizing default and exception cases (see Figure 5), which is enabled by an event-driven architecture; so, remediation actions can be tailored to the use-case, as opposed to the "one-size-fits-all" approach that is common in auto-remediation.

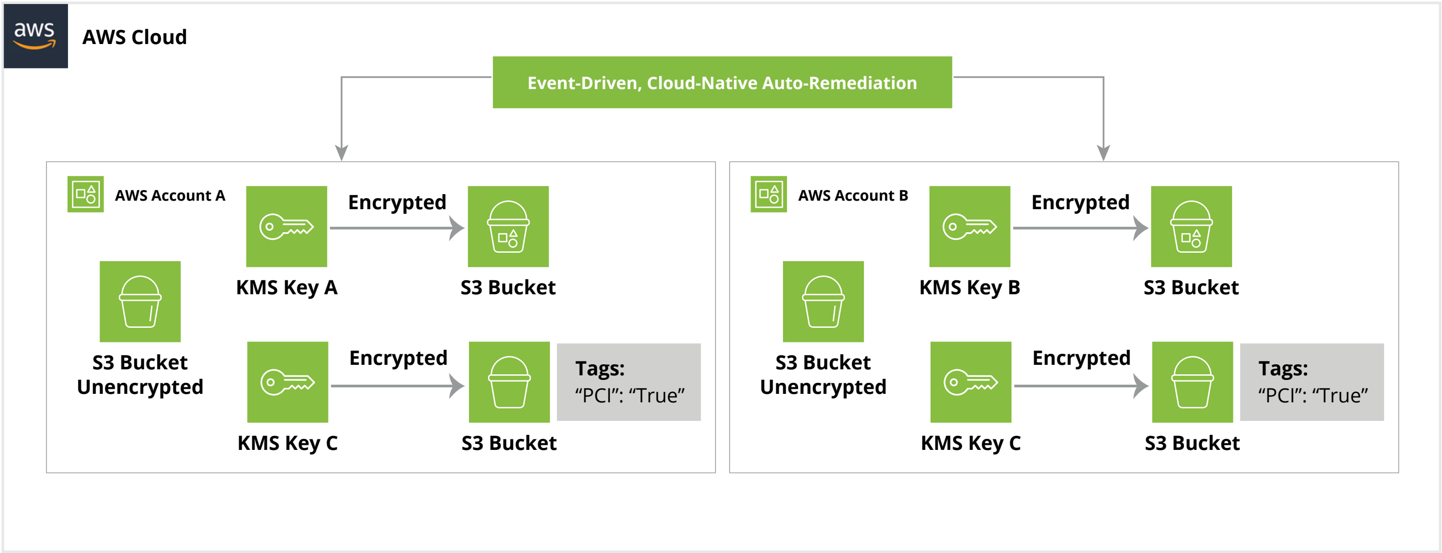


Figure 5 - By defining default and exception cases, DCAM's custom auto-remediation can enforce a standardized encryption strategy where resources in account A get encrypted with KMS key A, while resources in account B get encrypted with KMS key B. Then, across all accounts, resources with "PCI": "True" tag get encrypted with KMS key C. This capability is made possible by building entirely cloud-native auto-remediation workflows that are event-driven.

Conclusion

AWS Control Tower has become the bedrock of modernized cloud account management for hundreds of organizations that use it. The service has helped enable companies to provision and govern AWS accounts faster than ever before, in turn enabling developers to increase both their efficiency and their output. However, to realize the full potential of AWS Control Tower, companies should build policy-driven account security baselines that can integrate with Control Tower's account vending. If done correctly, this exercise can increase visibility into cloud accounts, standardize the policies that govern developers within each account, and accelerate security to scale alongside developers and the organization's cloud estate.

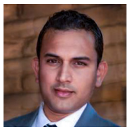
To schedule a demo of DCAM and learn how to modernize cloud account management at your organization, reach out to the authors listed below.

Authors

Aaron Brown

Deloitte & Touche, LLP
Partner, Cyber Risk Services
AWS Alliance Leader

aaronbrown@deloitte.com



Ravi Dhaval

Deloitte & Touche, LLP Senior
Manager, Cyber Risk Services AWS
Practice and Innovation Lead

rdhaval@deloitte.com

Samuel Sharon

Deloitte & Touche, LLP Senior
Consultant, Cyber Risk Services
DCAM and Control Tower Lead

sasharon@deloitte.com

Oumie Juwara

Deloitte & Touche, LLP
Analyst, Cyber Risk Services
AWS Security Architect

ojuwara@deloitte.com

Special Thanks

Steve Bollers (AWS), for his technical review and insights

Jeff Kaiserman (AWS), for his technical review and insights

Deloitte.

About Deloitte
Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the "Deloitte" name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.

Designed by CoRe Creative Services. RITM1396170