The Ultimate Guide to Cloud Security Automation

torq

Contents

1

Introduction

Cloud security is great. Automated cloud security is much better.

After all, security without automation leaves you subject to two major shortcomings. First, it significantly increases the time and effort required to secure your resources – which in turn means that you have fewer staff available to perform work that actually creates business value, as opposed to simply checking off basic requirements like security.

And second, security automation across cloud environments significantly reduces the risks of oversights or errors that could leave gaping holes in your security posture. When you rely on manual workflows to detect, assess, and remediate cloud security vulnerabilities, you run the risk that engineers might overlook a threat or mistakenly apply the wrong configuration. In contrast, automation delivers consistent security operations, no matter how large your environment is or how rapidly it changes.

What all of the above means is that, while applying security safeguards to your cloud environment is a basic first step in addressing security threats, modern cloud security requires more. It needs to be automated across all layers of your cloud environment and against all types of vulnerabilities that threaten your environment.

We’ve prepared this eBook to help developers, IT teams, and security professionals do just that: automate security across the cloud. As we’ll see, this is not a simple or singular task; cloud security automation requires embedding automation into a variety of distinct cloud workflows. But it is a task that can be handled by a single, comprehensive security automation framework, like Torq, which was built to help automate and accelerate security operations across environments of all types.

2

What Is Cloud Security Automation?

Before diving into what a cloud security automation strategy entails, let's make clear what cloud security automation means.

Cloud security automation is the use of software tools to identify, understand, and respond to security threats of all types within cloud environments. In other words, when you automate cloud security, most of the tasks required to find and remediate threats within your cloud environment can be handled by software – with limited, if any, manual intervention by human engineers.

It's worth noting that, unlike some other aspects of cloud administration (like Infrastructure-as-Code or cloud account management), cloud security automation is about more than just provisioning security configurations within the cloud. Applying security policies within your cloud environments is part of what cloud security automation enables. But equally important is the ability to detect threats and vulnerabilities, determine how serious they are, and react to them in an automated manner.

Also central to effective cloud security automation is the ability to plug non-technical stakeholders into the process. Unlike cloud administration in general, cloud security administration isn't something that only experienced engineers should be able to implement. Instead, using no-code tooling, cloud security automation platforms should enable any stakeholders to define vulnerability detection and remediation rules that help govern whichever cloud resources they manage.

Why You Need to Automate Cloud Security

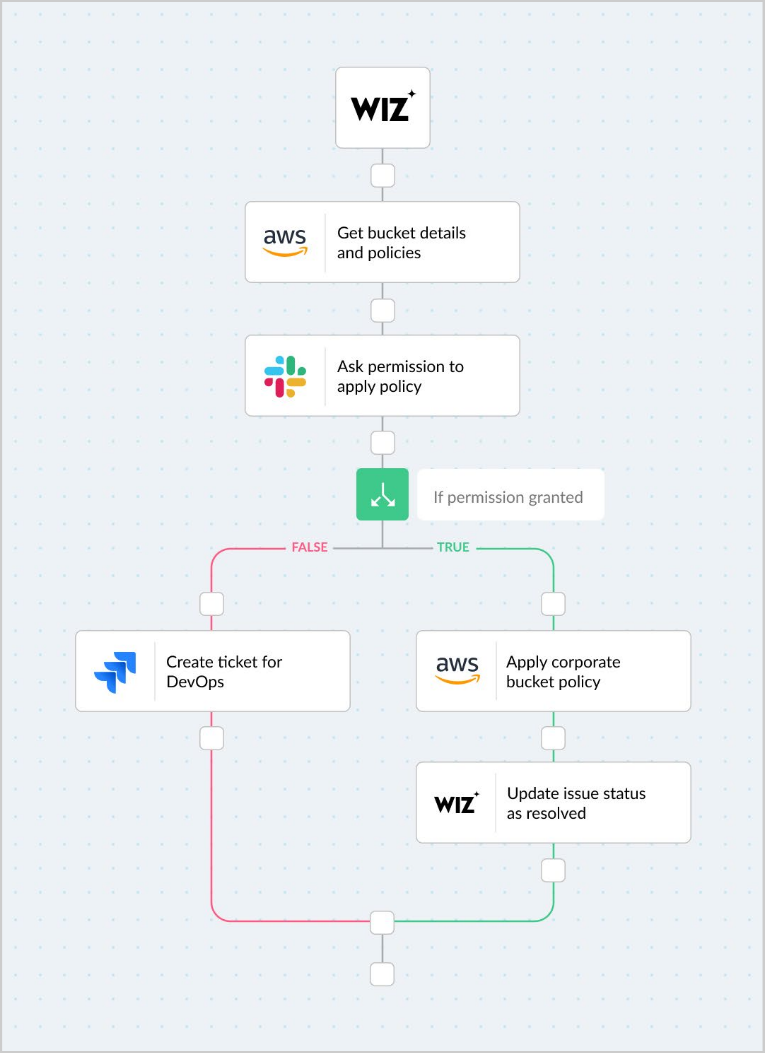
Again, cloud security automation provides two key benefits:

1. **Efficiency:** When you automate cloud security, you require fewer staff resources to keep assets secure.

2. **Consistency and accuracy:** Automation helps ensure that security policies are enforced consistently, reliably, and accurately across your entire cloud environment.

Both of these benefits are important for any business that uses the cloud. But they are growing increasingly critical as cloud environments become more and more complex and dynamic. When you use dozens of cloud services, and when you migrate to multicloud or hybrid cloud architectures, the ability to automate security across all of your resources becomes even more important.

Indeed, at a certain point, attempting to manage security manually across large-scale cloud environments simply becomes impractical due to the personnel resources it ties down, as well as the difficulty of enforcing security rules consistently across large and complex environments.


WIZ
Get bucket details and policies
Ask permission to apply policy
If permission granted
FALSE
TRUE
Create ticket for DevOps
Apply corporate bucket policy
Update issue status as resolved

An example of a **cloud security posture management** workflow template for Wiz.

3

Automating Cloud Security, Layer-By-Layer

There are a variety of services and operational layers within a typical cloud environment. Cloud security automation requires the ability to automate security across all of them.

Cloud Security Posture Management (CSPM)

Cloud Security Posture Management, or CSPM, refers to the identification and remediation of security risks within cloud environment configurations. CSPM works by assessing your cloud infrastructure configurations and detecting settings within them that could enable or exacerbate security vulnerabilities.

For example, a CSPM workflow might identify a cloud storage bucket whose data is accessible by anyone on the Internet, which may create a data privacy risk. Or, it could detect a Kubernetes pod that is not isolated at the network level from other pods, increasing the potential scope of an attack in the event that the pod becomes compromised.

CSPM risks like these could be flagged so that humans can respond to them. What's even better, however, is automatically remediating the risks where possible, so that they can be fixed immediately and without distracting engineers.

Due to the sheer scale and complexity of cloud configurations, it's simply not practical to attempt to assess and address CSPM security risks manually. Teams need a framework that allows them to define security risks based on their specific cloud use cases; after all, a configuration that poses a major risk to one cloud application or data set may be perfectly secure for another, depending on how the cloud resource is being used. The framework should then be able to assess configurations across cloud services of all types – as well as within multiple clouds – to detect risks.

And the best CSPM automation tools can go a step further by automatically remediating risks as they discover them, or as new risks emerge within constantly changing cloud environments.

Cloud Workload Protection

While CSPM is useful for mitigating vulnerabilities within the way cloud services themselves are configured, it typically can't address risks associated with specific workloads and the way they are configured.

For example, if you deploy containers on a public cloud using Kubernetes or a Containers-as-a-Service (CaaS) platform, CSPM alone won't identify all of the security risks within the way your containers are configured.

To address these risks, you must automate another facet of cloud security – workload protection. Cloud workload protection automation allows you to define and enforce security rules specific to the applications or workloads you run within the cloud.

In the case of cloud-based containers, workload protection automation provides capabilities such as identifying containers that are deployed in privileged mode (which is a major risk because those containers can access host-level resources) or ineffective Kubernetes Security Context settings (which may leave your Kubernetes applications with inadequate security protections).

Identify Lifecycle Management

Managing cloud identities in a secure fashion is no simple task. Although cloud service providers offer Identity and Access Management (IAM) that allows administrators to define roles and privileges within cloud environments, a major risk that IAM doesn't address on its own is that access needs often change over time. An access privilege that is assigned to a user may cease to be valid if the user's role within the organization changes, for example, or the user moves to another company.

While you can't detect risks like these using standard IAM tooling, you can use cloud security automation frameworks to define rules about identity management. You can, for example, specify that all roles and privileges for a user be revoked whenever the user leaves your organization, then let your security automation platform enforce that requirement automatically.

The result is consistent, secure enforcement with no disruption to your IT staff, even within large-scale cloud environments that include thousands of IAM policies and constantly changing user roles.

Automated Threat Hunting

In the cloud, threat hunting is the proactive identification of threats or breaches within your cloud environment, even if the threat hasn't yet fully materialized. To perform threat hunting effectively, you need deep cybersecurity expertise, as well as up-to-date data about the latest exploit techniques that malicious actors are deploying.

The problem that many organizations face when it comes to threat hunting, however, is that these two assets – specialized security expertise and real-time threat intelligence – are often difficult to operationalize. You can pay cybersecurity firms for threat reports, but it's still an enormous amount of work to translate those reports into actionable threat detection operations within your environment – if you approach it manually.

With cloud security automation, however, you can implement rules that automatically adjust your security policies based on the latest threat data. You can, for example, configure threat detection rules to be updated whenever a new exploit technique is discovered. That way, you'll know you're covered against the latest threats without having to wait on your security engineers to update your defenses manually.

Security Alert Remediation

Another major challenge that the typical organization faces when it comes to cloud security is coping with the tremendous volume of alerts. It's easy to generate an alert about a potential threat or vulnerability. It's much harder to determine which alerts require immediate action, which deserve secondary priority, and which are false positives.

Security automation mitigates this challenge by helping you sort alerts into the right categories automatically. Based on criteria you define, you can configure your cloud security systems to generate different types of alerts that reflect the seriousness of a given threat or the importance of affected resources to your operations.

What's more, because security automation allows you to remediate many risks automatically, you can reduce the total number of alerts that human engineers have to respond to. When software can fix problems like misconfigurations for you, you end up with many fewer security alerts sitting in your queue.

Toil Reduction

On a similar note, cloud security automation plays a central role in addressing the bane of engineers everywhere: toil, which means endless, exhaustive work that drives little value.

When you rely on manual effort to manage cloud security, you end up with mountains of toil. Your engineers spend much of their time performing repetitive tasks that never really move the needle.

Toil is bad for team morale, since most technicians will become bored when they spend their days fixing the same types of problems. It's also bad for the business because it means engineering resources are sunk into work that doesn't create business value, making it harder to develop new services or products.

When you automate cloud security, however, you mitigate toil because mundane tasks – like looking for and responding to threats – can be performed automatically. The result is engineers who have more time to do work that is truly meaningful – for them as well as for the business.

Citizen Security

It's not just engineers who benefit from cloud security automation. When you implement an automation framework that can secure cloud resources of all types without requiring special expertise, you enable everyone in the organization to play a role in security.

That's important, of course, because modern security threats are not just the problem of security engineers or other technical staff. Today's threat actors routinely target non-technical users through attack techniques like phishing. What's more, engineers don't always have clear visibility into the business needs of non-technical users, which can lead to misalignment between security rules implemented by engineers and the actual needs of the departments they support.

When everyone is empowered to write security automation rules, however, non-technical users can define and enforce their own security needs. Doing so leaves ordinary users in a much stronger position to defend themselves against threats. It also helps ensure that security rules support, rather than hinder, business operations.

Multicloud and Hybrid Cloud Security

It's hard enough to manage cloud security when you use just one cloud platform. But when you use multiple clouds as part of a multicloud strategy – or, similarly, if you combine public cloud and private infrastructure to create a hybrid cloud environment – detecting and remediating threats becomes especially challenging.

That's true due not just to the increased scale and complexity of multicloud and hybrid cloud environments, but also to the fact that you can't usually rely on a single cloud vendor's tooling to manage threats within more than one cloud.

Instead, you need a third-party security automation framework that allows you to define and enforce security rules across all of your clouds and cloud services – regardless of which cloud IAM frameworks you are working with, which monitoring tools your various cloud providers offer, and so on. Cloud security automation means you can unite all of your clouds under a single automation framework and manage security risks centrally.

6

Conclusion: The Essence of Cloud Security Automation

Cloud security automation is no longer simply a nice-to-have feature. It's absolutely essential for businesses that operate cloud environments of any meaningful size or complexity. You can't hope to stay ahead of threats across the various layers of your cloud environment using manual approaches alone; nor can you rely on cloud providers' own security tooling, which doesn't work across multiple clouds and which lacks advanced automation features.

Torq's no-code security automation platform connects across all your cloud services and environments, and automates security processes throughout your entire cloud security stack. Anyone – not just engineers with coding skills – can easily create automated workflows that run on demand, or in response to security risks and alerts.

By delivering powerful automation across all your cloud security use cases, Torq helps you remediate risks faster and improve your organization's overall protection. Get started today!

torq

Torq is a no-code automation and orchestration platform for security and operations. We empower frontline security teams in their journey to becoming more efficient by allowing them to automate processes using our easy workflow builder, limitless integrations, and numerous prebuilt templates.

Built as an enterprise-grade software-as-a-service, Torq can be adopted with ease, delivering results within minutes, unlike traditional security automation solutions that require weeks or months of investment prior to providing value.