EBOOK

Use Automation to Address Misconfigurations and Cut Costs

Table of contents

Introduction

In modern Amazon Web Services (AWS) environments, upwards of millions of resources are added regularly and spread across various environments. Each has its own configurations, roles, and permissions. At any given time, many of these resources can be misconfigured and even accidentally left open to the public. In fact, 90% of organizations are vulnerable to security incidents due to cloud misconfigurations.[1] However, finding and remediating these issues can be difficult. The process of spinning up resources and workloads is often self-service, which means that centralized security teams do not always know who should take action.

Automated remediation can help by automatically tagging resources with owner IDs, notifying the owners, and even preventing them from creating noncompliant resources. **But for automated remediation to be most effective, it should be implemented incrementally and with care, using a crawl, walk, and run approach.** In this ebook, we share how this approach can work.

Approximately 1 in 4 organizations take 1 week or longer to resolve a misconfiguration when remediating manually, with 1 in 10 taking more than a month.[2]

[1] "Cloud misconfigurations on the rise: 2021 Cloud Security Report," Independent. 15 Sept. 2021.

[2] "2022 SaaS Security Survey Report" Cloud Security Alliance, April 2022.

Why automate remediation

Automated remediation solutions can range from basic notification and logging of misconfigurations to full-on automated remediation that executes workflows to automatically fix what is found. Its benefits include:

Time saved
Common issues are handled automatically, dramatically decreasing the hours IT currently spends addressing them.

Increased security and reduced risk
You can set up remediation automation to take immediate action before a security event occurs.

Improved compliance
Proof of the results of real-time corrections helps keep cloud environments compliant.

Consistency
With repeatable workflow actions, you get a clear picture of what is being done, even in different circumstances.

Consider an incremental approach

Mature automated remediation triggers and responds to alerts or events with actions that can turn on other security services like Amazon GuardDuty, prevent issues, or fix problems. But that's not to say you should automate remediation as much as possible from day one. Why try to run before you crawl or walk? Most organizations benefit from working through different automation phases, seeing what action would have been taken and understanding why it was the right path. Incremental progression creates trust in the process and allows organizations to see that it won't create problems when it is in place.

The rest of this book explains how this crawl, walk, run approach can work when supported by real-time visibility.

The most common cloud vulnerability is resource misconfiguration, which unauthorized users can exploit to access cloud data and services.[3]

[3] "Mitigating Cloud Vulnerabilities," National Security Agency, Cybersecurity Information, 2021.

Crawl before you walk: Use automatic notifications to find misconfigurations

Notification is the first step of the remediation process. That means it's also a good place to start your journey to automated remediation. Just like humans get the hang of moving on their own by crawling, automated notifications help you get used to the idea of automatic processes.

How automated notifications work

With automated notifications, the resource owner receives an alert from the source of their choice (such as a chat, an email, and/or a ticket) when there is a misconfiguration. The owner can see recommended manual remediation steps and the bots that can be created to automate the fix. Even if it might not require your intervention, knowing when there's a potentially troubling pattern that could point to a larger issue can help you prevent incidents or unauthorized access.

Alert notification drives efficiency

Another benefit of automatic notifications is efficiency. The owner of the resource and anyone else who needs to know about the misconfiguration receive an alert and become involved, eliminating the need for a security team to identify the owner—if they even receive an alert. Sending notifications to the rightful owner speeds up the remediation process even when the actual fix is done manually.

> "Misconfigurations can be the result of something as innocuous as someone having mistyped an IP address when attempting to connect to a networked resource."
>
> **Rapid7 Report**[4]

[4] "Breaches are out there, but that doesn't mean you have to be a target," Rapid7, 2021.

Walk before you run: Meet security policies and standards automatically

The notifications that there are misconfigurations open the door to more extensive automation. What can you set up to run automatically that can reduce misconfigurations and manual fixes further? Perhaps you want Amazon GuardDuty or AWS Config turned on for every account. Or maybe you need Amazon CloudTrail logs sent to an Amazon Simple Storage Service (Amazon S3) bucket so you can audit them and go back for investigation. Or maybe there are external NIST, CIS, and ISO standards you would like to align with, but are not sure how to set up.

In other words, you are ready to use automation not just to remediate a misconfiguration or privilege escalation issue, for instance, but also to help ensure standards are being met from all angles. In a sense, a lot of the preparation and legwork for automating fixes is in the works.

What happens when you walk?

In this middle phase of automation, you set policies and use automated remediation not only to enforce them but also to turn services, such as GuardDuty, on or off based on those policies, as well as clean up parts of your environment. So, for example, if someone removes an owner tag or badge, which can be difficult to keep track of, an automated remediation solution can replace it immediately. This maintains proper IT hygiene and eliminates the risk of potentially rogue assets hanging around your environment with no known owner.

How automating standards and policies work

You start by establishing the standards and policies your organization wants to follow. If you're not sure, automation solutions come with more than 30 compliance frameworks out of the box, including CIS, NIST, and ISO. These include CIS Benchmarks, which are account fundamentals that any organization can employ to improve the security and overall hygiene of cloud accounts. There are also AWS Foundational Security best practices for Cloud Solution Providers (CSPs).

Then, you set up your automated remediation solution to handle specific actions without human intervention, such as identifying when an account has one of those services turned off and automatically turning it back on. In addition, you can build custom compliance packs—from scratch or using out-of-the-box packs—and exclude resources and accounts from certain rules or policies.

> "Quite often novice administrators leave default security settings in place that are often too broad in their permissions."
>
> **AWS Administrator**[5]

[5] "The Harsh Realities of Cloud Security: Misconfigurations, Lack of Oversight and Little Visibility," CyberRisk Alliance, Business Intelligence, October 2022.

Ready to run: Embrace automation to address risk signals and control costs

Once notifications and policy enforcement have been running for a while and you've experienced the benefits, like the human who has crawled and then walked, it could be time to run. The previous phases are reassurance that this process will not "break" the cloud environment. Plus, these are the actions that give you the most control.

In the run phase, you're off to the automation races. Bots are quickly and easily created with no-code that execute workflows automatically when a policy is violated. As a result, you drastically reduce dwell time and have a consistent approach to fixing issues across your cloud.

What automating workflows can deliver

Automating workflows to execute fixes can open up a new world for you, where you can identify significant misconfigurations or noncompliant actions and either isolate or shut them down entirely in AWS. In addition, you can update resource configurations and AWS Identity and Access Management (IAM) roles and permissions, or even delete the non-compliant resource altogether. And as an added buffer these actions can be delayed, so you could automate a notification to the resource owner immediately and delay the actual isolation or deletion of the resource by 24 hours in order to give them time to manually make a fix. Think of it as having guardrails or bowling lane bumpers to make sure you don't drift out of your lane, which in this case is compliance.

Automating workflows also helps you remove resources that go unused or that have been over-provisioned. You can also de-risk your environment by removing resources that have been forgotten or overlooked when you assess your security posture or your environment for security and compliance. This can present additional avenues for security events or data loss.

Addressing risk signals and controlling costs

You can also use automation in this phase to take action based on risk signals and to keep costs down. For example, you can clean up port exposure by locking down a secure tunnel opened by Secure Shell (SSH) tunneling or a port left open by Remote Desktop Protocol (RDP). You can terminate instances that aren't tagged properly and aren't running a golden Amazon Machine Image (AMI).

Assets outside primary regions can also be terminated to keep non-main regions unused. Old API keys can be deactivated. And you can lock down Amazon S3 buckets, zeroing out access control lists (ACLs) and bucket policy.

Using Rapid7 InsightCloudSec, Qlik has applied startup and shutdown times to all subscriptions, accounts, and projects across AWS and other cloud environments, and they have seen a 60% reduction in costs.[6]

[6] "Rapid7 Enables an Expanding and Cohesive Multi-Cloud Security and Compliance Strategy," Rapid7.

The secret sauce: Real-time visibility and layered context

It's a common cloud security practice to rely on or decide to start remediation with multiple native tools, all of which have a different dashboard or a different account with different logins. In this highly fragmented and distributed environment, it can be challenging to manage all the tools and logins, not to mention acting on a risk signal that's flagging an incident or situation for investigation.

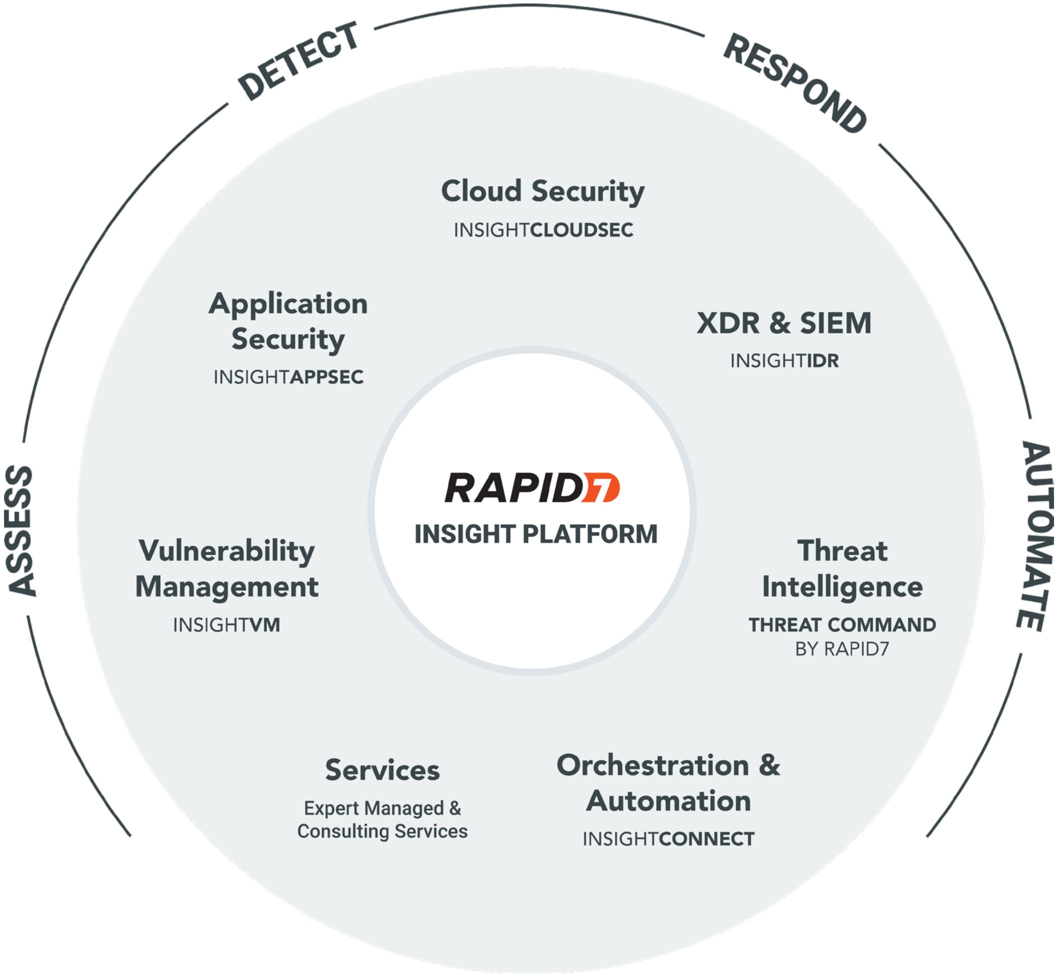
Time for a better view

Real-time visibility delivered in a unified platform is a major component in full-featured automated remediation solutions that can address this situation. Many cloud security solutions offer visibility in the form of scans that deliver views of the cloud landscape at some predefined cadence, most commonly once a day. But what about the misconfigurations that can be breached in minutes? Or stale data? You could be trying to automatically fix something that either no longer exists, has already been exploited, or has been fixed.

The benefits of the secret sauce

Real-time visibility can eliminate a trip down the wrong path or wasted effort. It can identify risk in your environment and automatically take action to remediate it before it can be exploited. Add layered context into everything running across your AWS environment, and your cloud security solution can effectively prioritize risk based on likelihood and potential impact of exploitation.

Seventy-eight percent of CISOs have 16 or more cybersecurity tools, and 12% have 46 or more.[7]



[7] Kasey Panetta, "The Top 8 Security and Risk Trends We're Watching," Gartner Insights | Information Technology, Nov. 2021.

Winning the race with improved efficiency and reduced risk

With Rapid7 InsightCloudSec, you can implement automated remediation incrementally so that you do not try to do too much too soon. You can establish standards and policies around cloud access and resource configuration, whether they're based on common industry frameworks or customized to specific business needs.

Enforce policies and remediate—without the human touch

Agentless, real-time visibility and native automation continuously track compliance across your organization and automatically enforce policies without the need for human intervention whenever compliance drift occurs. Native no-code automation in the form of bots can automatically remediate back to a state of compliance and initiate workflows such as notification, ticketing, and so on.

Layered context understands the layers of insight and data points, such as permissions, or an application that has a known vulnerability that could be exposed, and the potential impact if an exposure is reached by an unauthorized user, all based on the insight gathered. It also considers the business context that can be helpful and important to making automation more effective and more accurate.

Prioritize, enable services, and reduce risk

With Rapid7 InsightCloudSec providing real-time visibility and layered context into everything running across your AWS environment, you can effectively prioritize risk based on likelihood and potential impact of exploitation. You can also set up automation to ensure that native services such as Amazon GuardDuty or AWS Config are enabled at all times and turn them back on if disabled. And with InsightCloudSec, your teams can also identify and automatically shut down or delete unused or over-provisioned resources running across your environment to capture significant savings and reduce risk.

Conclusion

It is no secret that automated remediation can address the challenges of AWS environments that have thousands or millions of resources and a conglomeration of fragmented security tools. However, it is important that you take an incremental approach to automated remediation. So, if you are starting from a blank slate, consider taking the "crawl, walk, run" approach shared in this ebook.

There are Rapid7 tools and AWS services that can help you build an automated solution that delivers proper configuration, discovery-time remediation, procedural consistency, always-on cloud compliance, and time and cost savings.

Rapid7 is dedicated to helping you move to the cloud securely in tandem with AWS, our preferred cloud partner. Using purpose-built solutions and direct AWS integrations, Rapid7 helps you protect and monitor all of your AWS assets quickly, easily, and cost effectively.

You can find Rapid7 InsightCloudSec solution in AWS Marketplace.

AWS Marketplace