RAPID7

EBOOK

Drive Cloud Security Forward

With continuous security and compliance delivered by Rapid7 and AWS

aws

Table of contents

Introduction

The cloud has given businesses the ability to transform and scale in ways that we once thought were impossible. But the urgency to move workloads and data to the cloud often seems to force a choice between slowing the pace of innovation or taking on massive unmanaged risk. In most cases, speed wins when innovation is on the line. Choosing speed over managing risk, however, can be devastating at a time when cyberattacks on cloud environments have increased. Making an environment easier for developers to access in the interests of acceleration can open it up to an attack if you aren't careful.

Seeking out issues that can leave you vulnerable to attacks and removing them can prevent your most sensitive and valuable data from falling into the hands of an adversary. And you can do it without sacrificing speed or delaying innovation. InsightCloudSec, a cloud-native security platform from Rapid7, integrates with Amazon Web Services (AWS) to help protect even the most complex cloud and container environments from vulnerabilities, policy violations, threats, and identity and access management (IAM) challenges. This eBook shows you how.

Today's cloud security challenges

As of 2020, 81% of organizations had at least one application running on the cloud. Of those organizations, 83% say they currently use hybrid cloud approaches, and 93% of them say they will implement a multi-cloud strategy by 2022. By the end of 2021, 28% of businesses will be using cloud containers and serverless computing.

With the cloud's high rate of adoption in all its many different forms, the threat landscape is growing. To complicate the situation, many organizations have given DevOps teams self-service access to the underlying infrastructure to take advantage of the speed and scale of the cloud. Although this helps drive faster innovation, the fact that many developers are not trained security experts mean they can accidentally introduce configuration issues that leave parts of your data exposed. This creates a cross between a fuzzy gray area and a fine line. How do you balance speed and easy developer access with protecting cloud environments from attacks?

Another challenge is identity and access management (IAM). When it comes to cloud IAM, security and operations teams are struggling to analyze permissions because of overlapping IAM layers. This visibility continues to fall as cloud deployments grow and cloud IAM complexity increases with scale. The result is a tangled puzzle of overlapping IAM policies.

The good news is that cloud security technology is catching up with the threats and reducing them quickly. With this technology, your security team has the power to find and fix vulnerabilities, detect and respond to attacks, and optimize security workflows—without slowing your development team down. The Rapid7 InsightCloudSec security solution is a fully integrated, cloud-native security platform designed to help you drive cloud security forward.

Safely speed up your cloud adoption with three key approaches: An overview

There are three approaches that are key to keeping your cloud protected. This high-level overview summarizes them to give you an idea of what they entail. That will help you better understand how InsightCloudSec can help you address each one.

Shift left

What does it mean to shift left? Basically, you are adding security to the DevOps process much earlier—shifting it "left." A single, consistent set of security checks that run throughout the continuous integration and continuous delivery (CI/CD) pipeline can help solve problems at their root cause—and keep them from reappearing. Shifting left has the additional benefit of bringing developers and security teams together to make the right decisions as early as possible. With this approach, delays in the deployment or operationalizing stages of the CI/CD pipeline are rare, and your development and security teams can establish a stronger collaborative bond.

Reduce noise

With its multitude of logs, different monitoring agents, and separate solutions, cloud security can be noisy and confusing. What used to be 500 physical servers in a data center are now thousands of cloud instances that are constantly being spun up and shut down. With that huge volume and speed of change, minor and mostly harmless issues pop up all the time. They can be a distraction that makes it hard for security or DevOps teams to identify the rare major problems when they do pop up. It's the classic needle in a haystack scenario. To reduce the noise, you can unify visibility across your entire cloud. Teams can see and understand potential risks and vulnerabilities more easily. In addition, normalizing technology, applying compliance frameworks, and providing rich context about interconnected assets can also vastly simplify risk assessment.

Automate workflows

The evolving nature and speed of change in cloud environments have outstripped the human capability to manage and remediate issues manually. Automating workflows eases that particular pain. One example is creating automatic workflows for investigations that search logs to detect threats. Another is automating workflows by pulling data from the cloud in real time. Essentially, automated workflows speed up remediation and reduce busywork so that your security team can focus on the bigger cloud protection picture. Automation is key to achieving security at the speed of scale.

Shift left with workload protection and code analysis

With InsightCloudSec, you can rest easy knowing that your dev, cloud, and container environments are being continuously protected against vulnerabilities and policy violations. It starts with a two-tiered security posture management (CSPM) approach that includes API polling and event-driven notification for faster detection of changes. This approach provides critical configuration protection by continuously monitoring for configuration changes to cloud and container services.

Increase DevOps control

Providing self-service access to developers, if not approached properly, can lead to a loss of control for the security team. Numerous standards and frameworks can help you establish baseline policies to ensure that your use of the cloud is secure, compliant, and well-governed. But how do you use which and when?

InsightCloudSec takes on the difficult task of answering that question for you. It delivers hundreds of out-of-the-box policies that you can use to automate the detection and remediation of policy violations. These policies map back to the major standards and frameworks, including PCI DSS, HIPAA, GDPR, SOC 2, ISO 27001, CIS AWS, CIS Kubernetes, NIST CSF, NIST 800-53, FedRAMP, and CSA CCM. You can also modify and create your own policies as well as merge or create new compliance packs. Plus, security guardrails for Kubernetes give your developers the freedom to innovate while also maintaining compliance with best practices for workloads running on Kubernetes and AWS.

Add consistent security checks of IaC templates before you deploy

Rapid7 InsightCloudSec provides a consistent set of security checks and exemptions for infrastructure-as-code (IaC) templates like AWS CloudFormation, which help DevOps teams automate and manage their infrastructure as part of the CI/CD process. But when launching IaC templates, it can be easy to make small mistakes. For example, acl = “public-read” in a code snippet for a template would expose an Amazon Simple Storage (Amazon S3) bucket to the public internet. ACL stands for Access Control List, and it should be set to “private” in most cases. This is just one property in a template that needs scrutiny; there can be tens of thousands of these across different templates and assets. Constantly checking these properties for errors can be extremely tedious and time-consuming.

AWS has cloud-native security services like Block Public S3 to help mitigate these kinds of issues. InsightCloudSec leans into those AWS controls, making it easier for you to take advantage of the security that AWS provides. The Rapid7 InsightCloudSec IaC Security feature ensures that these templates follow best practices and company policy as early as possible, while minimizing developer frustration and delays caused by inconsistent checks at each stage of the CI/CD pipeline.

Isolate templates from the noise with simulation

Contextual IaC Analysis analyzes your IaC templates in a simulated version of your actual environment. It can help you uncover errors in a specific template that might be hidden in the noise of a multitude of IaC templates, along with potentially risky configurations, before deploying.

Reduce noise with visibility and IAM governance

InsightCloudSec provides unified visibility and simplicity across complex cloud and container environments to reduce the noise and amplify the signal. You can see your entire cloud footprint in one place for the first time, including everything you need to protect and how you can do it. InsightCloudSec eliminates the processes of working through an overlapping IAM policy stack that consists of multiple permit/deny decision points for every cloud asset and determining effective permissions using extensive Venn diagram analysis.

Customer case study: Qlik reduces noise

SaaS software company Qlik needed to ensure its cloud resources and data were secure, even as it expanded its cloud footprint. In less than three days with InsightCloudSec, Qlik gained deeper, more actionable insights into its cloud environments. The Qlik team was also impressed with the contextual information InsightCloudSec provided, such as helping distinguish the risk levels of different cloud storage tools.

Qlik

Use compliance reporting with easy-to -read visualizations

How does InsightCloudSec provide this visibility, monitoring, and simplified policy management? It starts with compliance reporting that checks multi-cloud environments against dozens of industry and regulatory frameworks. Then, it provides an easy-to-read visualization of compliance. As a result, you can effortlessly report on policy governance, minimizing drift and saving significant time and money every time an audit is required. This reporting is customizable to give you the flexibility to scope your reports and customize compliance checks to address your own internal policy requirements.

Streamline IAM and reduce excessive entitlements

AWS has a robust IAM feature set. Rapid7 has capabilities that help reduce noise around IAM management in AWS. InsightCloudSec includes an IAM governance feature feature that deconstructs and reconstructs the cloud IAM policy stack by creating an IAM boundary view. The IAM boundary view consists of three lenses that operations staff, analysts, incident response staff, and auditors can use to analyze and simulate their cloud IAM environment. Using these lenses, your teams can quickly identify all the resources a federated user has access to along with why and what they did to gain access.

To help reduce excessive entitlements and streamline least-privilege access controls, Cloud Infrastructure Entitlements Management (CIEM) from Rapid7 analyzes the complex roles and identities of cloud environments. You can adopt a least privileged access security model across your cloud and container environments to minimize the blast radius of malicious activities.

Accelerate response and remediation with automated workflows

Automating workflows with Rapid7 can accelerate your time-intensive, highly manual response and remediation processes. You also get flexibility and blazing-fast remediation time.

Case study: Automating workflows at Discovery, Inc.

Automation through InsightCloudSec, including security baselines, identity checks, resource consumption checks, and automated policies, is enabling more efficient and effective corrective issues at mass media giant Discovery, Inc.

"InsightCloudSec gives us the ability to automate governance, offer flexibility, allow better insight and tighter controls, and enhance compliance, all at the same time. When I think about all the automation we can do, it can span a whole breadth of types of enforcement. It's a very flexible toolbox that we can dip into."

Dave Duvall
Chief Information Officer at Discovery, Inc.

Discovery

Automate with flexibility

The Rapid7 approach is to offer your security team the flexibility to automate in a way that makes sense for you. You can set your automation to be only as strict as you need it to be in any given situation. You can start with lighter weight automation steps like sending notifications to the owner of resources that are not compliant via a chatbot or creating tickets, tasks, or incidents in project management tools. Automating issue remediation directly from the product, such as isolating or killing off a non-compliant resource that is posing significant risk to the environment. The flexibility of the approach also enables you to go straight to automated remediation or put everything together.

Automatically remediate issues in less than 60 seconds

InsightCloudSec can automate notification and response workflows for real-time remediation without humans in the loop. InsightCloudSec has the capability to augment standard polling-based harvesting with event-driven harvesting (EDH). It pulls data from CloudWatch Events and AWS CloudTrail into a central Eventbus for InsightCloudSec in real-time, which makes it possible to find and automatically respond to or remediate issues in 60 seconds or less. This is drastically faster and more efficient than the hours-long, manual process that it may take with other similar tools.

This dynamic approach to data collection not only improves the cadence for providing resource visibility and opportunities for remediation, but it also enriches the data with lifecycle changes that enable auditing capabilities.

How to drive cloud security forward with Rapid7 and AWS

Rapid7 and AWS enable innovation and empower digital transformation with solutions that drive security forward. AWS and Rapid7 provide services that protect your data, apps, and network across hybrid cloud environments.

Security with AWS: Shared Responsibility Model

Security on AWS starts with the Shared Responsibility Model. AWS operates, manages, and controls the components from the host operating system and virtualization layer, down to the physical security of the facilities where the service operates. The rest is up to you. However, to help you with your responsibility, AWS offers telemetry services like Amazon CloudWatch and Amazon CloudTrail to provide key insights into the status of your applications. In addition, AWS Security Hub collects security data from across AWS accounts, services, and supported third-party partner products, including the Rapid7 InsightCloudSec platform, and helps you analyze your security trends and identify the highest priority security issues.

Rapid7: Up-to-date support for multiple AWS services

Rapid7 offers integrated, advanced security capabilities that complement and enhance the native AWS services. A single set of tools secures your hybrid environment, allowing your developers and security teams to have a consistent approach wherever they need it. But it doesn't stop there. To be meaningful, AWS compliance checks must be current, especially since AWS adds about 200 new services a week. Because cloud is always changing, Rapid7 supports new and updated AWS services, often as quickly as two days after they are released. This commitment to staying current with AWS releases is unwavering.

Summary

With InsightCloudSec, Rapid7 provides a fully integrated cloud-native security platform that enables organizations to drive cloud security forward through continuous security and compliance. InsightCloudSec runs on AWS and integrates with AWS services to help protect even the most complex cloud and container environments from misconfigurations, policy violations, threats, and identity and access management (IAM) challenges. Automated, real-time remediation helps you respond more quickly to security or compliance risks.

Learn more about InsightCloudSec

Request an InsightCloud Sec demo

Visit Rapid7 in the AWS Marketplace

Simplify your procurement and explore discounted pricing