aqua

The Essential Guide to Cloud Security Posture Management

How CSPM automates security configuration across clouds

December 2020

Table of Contents

Introduction

The widespread adoption of public clouds has driven new levels of agility and innovation while radically transforming enterprise ecosystems. Organizations now operate across multiple public and private clouds, use a myriad of cloud services, and often have hundreds or even thousands of developers impacting (even unknowingly) their cloud infrastructure. In addition to cloud providers releasing new services and features at a record pace, cloud users also need to navigate complex compliance requirements from different regulators. Complexities quickly add up, and keeping track of all the setups and configurations needed to secure every single service gets incredibly overwhelming.

With the lack of visibility and control over ever-changing configurations, it's no surprise that cloud data breaches and exposures are extremely common.
Over the last two years, more than 30 billion customer records have been exposed in nearly 200 breaches due to cloud infrastructure misconfigurations[1]. Almost all successful attacks on cloud services include an exploit of various misconfigurations and mistakes made by the organizations. In the recent 2020 Verizon Data Breach Investigations Report, only hacking ranked higher than misconfigurations as a source of data breaches[2].

While cloud providers take great effort to secure their offerings, most organizations lack the necessary processes or tools to use them effectively. Some of the largest cloud breaches at companies like Imperva, Capital One, and CenturyLink happened due to simple configuration mistakes, be it an open AWS S3 bucket or excessive permissions. Gartner estimates that through 2025, at least 99% of cloud security failures will be the customer's fault, and 90% of the organizations that fail to control public cloud use will inappropriately expose sensitive data[3]. As the COVID-19 pandemic accelerated the transition to the cloud even further, data breaches will only continue to increase in scale and velocity.

This whitepaper covers the security challenges organizations face today with their cloud IaaS environments, what approaches can mitigate these risks, and why Cloud Security Posture Management (CSPM) is the solution that addresses these challenges most efficiently and effectively.

[1] The State of DevSecOps Report - Summer 2020, Accurics
[2] 2020 Verizon Data Breach Investigations Report
[3] "Is the Cloud Secure?", Gartner, 2019

Cloud Security Challenges

The Dynamic and Complex Nature of the Cloud

Cloud computing has forever changed IT environments. The time needed to spin up infrastructure has dropped dramatically, allowing organizations to deploy applications in the blink of an eye. While the cloud has significantly simplified the process of provisioning IT resources, it has also increased the possibility of human error.

The dynamic, software-defined nature of the cloud leads to frequent changes that are completely different from the traditional on-premises world. The configurations that used to exist only in the physical data center now exist entirely in the cloud as a software layer - allowing you to tweak settings on the fly. In a cloud-based world, everything is easy to change with just a few clicks, but at the same time, very easy to misconfigure.

> There are over 1.4M SKUs for sale across the major cloud providers
>
> *451 Research's Cloud Price Index*

One of the biggest cloud security challenges is the sheer complexity of the environment. Each major cloud provider offers a broad set of services spanning compute, storage, databases, analytics, networking, mobile, IoT, security, and much more. 451 Research's Cloud Price Index tracks a colossal 1.4M SKUs for sale from AWS, Google, Microsoft, Alibaba, and IBM[4].

Across the big three cloud providers, there are hundreds of different services, sub-services, regions, availability zones, and configuration options. While the services that different providers offer are similar in many ways, they aren't identical. Within each of them, there are dozens of unique settings, granular configurations, and specific authorization policies that make it very hard to ensure an environment meets proper security and compliance requirements.

[4] "Cloud Trends in 2020: The Year of Complexity, and its Management", 451 Research

To stay competitive, cloud providers are constantly rolling out new services and adding new features. For example, AWS now offers over 175 services across 77 Availability Zones within 24 geographic regions around the world - up from just over 100 services three years ago and 140 in 2018. In 2020, so far, AWS has announced over a thousand major service updates and launched nearly a dozen new services, making it extremely difficult for everyone to keep up.

Growth of AWS Cloud, 2018 vs 2020

2018		2020	
140	Services	175	Services
57	Availability Zones	77	Availability Zones
19	Geographic Regions	24	Geographic Regions
190	Countries	245	Countries

This pace of change is dizzying for administrators who were accustomed to the relatively static nature of their traditional on-prem environments. The sheer complexities of navigating cloud infrastructure can lead to configuration errors. One-click mistakes can easily escalate to a serious data breach if they aren't caught. The task of ensuring security only gets harder in a multi-cloud environment, which is rapidly becoming the norm for many organizations.

Multi-cloud World

Today, organizations increasingly use various cloud combinations, i.e., they simultaneously leverage multiple public and private clouds. According to Flexera's 2020 State of the Cloud Report, most companies embrace multi-cloud, with 93 percent of enterprises having a multi-cloud strategy. On average, they use 2.2 public and 2.2 private clouds[5].

> Multi-cloud strategies will reduce vendor dependency for two-thirds of organizations through 2024
>
> *Gartner, 4 Trends Impacting Cloud Adoption in 2020*

Several reasons have led to a significant rise in interest in multi-cloud deployments. Enterprises adopt multi-cloud to increase agility, take advantage of best-in-breed solutions, improve cost efficiencies, achieve better geographic coverage, and increase flexibility through choice. In addition to the core cloud benefits, a multi-cloud approach can help reduce vendor lock-in and ensure uptime in the event of a provider outage. For example, using several providers minimizes the effect of DDoS attacks by spreading traffic and services over multiple clouds, eliminating the risk of having a single point of failure. Gartner predicts that multi-cloud strategies will reduce vendor dependency for two-thirds of organizations through 2024[6].

With all the benefits of a multi-cloud strategy, there are serious challenges that come with it as well. Multi-cloud architectures are much more complex and, therefore, harder to manage. Due to the lack of visibility across diverse hosts and services spanning multiple vendors, as well as significant differences in the configuration of similar services between clouds (e.g., AWS EC2 vs. Azure Instances, or Amazon EKS vs. Google GKE) the environment becomes even more complicated to secure.

[5] 2020 State of the Cloud Report, Flexera
[6] 4 Trends Impacting Cloud Adoption in 2020, Gartner

The Human Element

Enterprises using IaaS/PaaS have, on average, at least 14 misconfigured services running at any given time, leading to an average of about 2,300 cloud misconfiguration incidents per month[7]. Part of the problem is that many organizations still lack adequate cloud expertise and skills. Since the cloud landscape is changing so fast, always having security-savvy experts in place for all the new services being released becomes a challenge. But the even more dramatic issues arise with the implementation of a "shift left" approach.

Overall, it's good practice - you're trying to address problems earlier in the SDLC and, therefore, you place more control in the hands of developers. As a result, large organizations now have dozens, hundreds, or even thousands of developers operating inside their cloud environments. Each of them is making changes, deploying infrastructure, and configuring services. However, not being security experts, developers often take the path of least resistance to get a new service up and running, which can lead to mistakes.

What's worse, developers can now make configuration changes at the beginning of the process without a clear understanding of how their actions might affect the infrastructure downstream. As everything in the cloud is interdependent, this quickly can lead to drift away from a secure and compliant environment. The reality is that it only takes one misplaced wildcard in a permissions policy or a single wrong click to introduce a security risk.

> Eight in 10 companies across the US have experienced at least one data breach due to cloud misconfigurations
>
> *2020 IDC Cloud Security Survey Highlights*

Cloud misconfiguration is one of the two most common initial threat vectors in data breaches. The IBM X-Force Threat Intelligence Index 2020 reports a nearly tenfold year-over-year increase in records exposed due to misconfigurations, accounting for 86% of the total records compromised in 2019[8]. With 21% of all files in the cloud containing sensitive data, the potential impact of such a breach can be much more damaging to the organization. It is estimated, that breaches due to cloud misconfigurations result in the average cost of a breach increasing by more than half a million dollars to $4.41 million[9].

[7] 2019 McAfee Cloud Adoption and Risk Report
[8] 2020 IBM X-Force Threat Intelligence Index
[9] 2020 IBM Cost of a Data Breach Report

The majority of the breaches involve misconfigured AWS S3 buckets, but also happen with databases like MongoDB, or Elasticsearch instances. AWS S3 (Simple Storage Service) is one of the most popular cloud storage tools for everything from server logs to customer data. There are legitimate use cases for an S3 bucket to be publicly accessible – as is the case when hosting public-facing assets on a website. But in most cases, they should be kept private and encrypted.

> Not every data breach happens due to cloud misconfigurations, but this element often plays a key role in the attack kill chain

S3 buckets have attracted a lot of attention in recent years due to many high-profile data breaches affecting companies like Uber, FedEx, Adidas, Shopify, Accenture, and even the United States Department of Defense. All these breaches had one thing in common – the administrator managing the service misconfigured some security settings, leaving it open to the public. And while not every data breach happens due to configuration issues, this element is prevalent and often plays a key role in the attack kill chain, as we've seen again in the recent attacks against vulnerable Redis server ports.

Shared Responsibility Model

In these data breaches, cloud providers are not technically at fault - no more than a door manufacturer would be responsible for burglary if the lock was left open. Security in the cloud is a shared responsibility between the customer and the cloud provider like AWS, Azure, or Google. It requires users to secure everything in the cloud, while the cloud provider ensures the security of the cloud itself.

In other words, cloud providers are responsible for securing the underlying infrastructure, while almost everything above the infrastructure layer is in the customer's court.

This means that cloud users are the ones responsible for properly configuring their own guest operating systems, databases, and applications. They should take care of such areas as network traffic security, OS and firewall configuration, application security, patching, identity, and access management, and, most critically, the safety of customer data. Regardless of the cloud service, you're responsible for securing your own space within that cloud.

Growing Compliance Needs

As personal, financial, and other sensitive data may be subject to strict compliance regulations, using public cloud services presents many compliance challenges. Moving data to the cloud doesn't exclude organizations from achieving and maintaining compliance with applicable regulatory requirements, certifications, and frameworks across different regions and industries. Major public cloud providers support popular compliance frameworks, such as HIPAA, GDPR, PCI-DSS, NIST, and others, but typically it doesn't come by default.

To stay compliant with the laws and regulations, organizations need to understand and deploy cloud services with specific configurations and in a very specific way. Each standard has its own set of rules and guidelines and must be configured to support any clouds an organization is using. Additionally, the regulatory landscape is always changing - many new standards have been born in the cloud, such as CIS benchmarks or AWS Well-Architected Framework. Retaining compliance becomes a never-ending task.

To sum up, organizations end up with a multifaceted challenge. The multitude of cloud services, their configuration options, combined with hundreds of developers and a changing regulatory landscape can quickly lead to configuration chaos. In addition, the speed of change in the cloud is now so high that mistakes are almost inevitable.

Solutions

There are several approaches to tackle these cloud infrastructure challenges:

Manual auditing

If you are just starting out with the cloud and don't use too many services, you may be able to audit your cloud infrastructure manually. But, overall, cloud environments have become too large and complex for the vast majority of enterprises to rely on manual security tools. Manual approaches simply cannot keep up with the constantly evolving nature of the cloud. Any review process would quickly become overwhelming and consume hours of developers' time.

> To find misconfigurations in complex environments is like trying to find a moving needle in a massive haystack

For example, even configuring only 10 services, each with varying granularities of authorization policies, across several accounts, different applications, and compliance contexts is extremely hard. Then, if you use multiple providers there are just too many settings to track. To find misconfigurations in such environments is like trying to find a needle in a massive haystack, and to make things worse, a needle that's constantly moving. Even if you could track them all, the time required to manually fix them would still leave you exposed.

Scripted reviews

Since manual security can't keep pace with a growing cloud footprint, organizations need automated tools to address these risks. Many teams start to script the review process based on industry best practices. Some organizations implement home-grown scripts, others use open-source tools, such as CloudSploit by Aqua.
By ensuring that the same review process is followed continuously, these tools are much better at detecting infrastructure weak points.

While this approach saves organizations a lot of time, maintenance and change management are still a big problem. You need a whole team to run it, review the results, and implement the changes. It's especially not well-suited for enterprise-scale, as in large organizations with many cloud accounts you will have to aggregate the individual scripts and provide visibility and data retention at the corporate level.

Cloud providers' native security tools and features

To assist organizations with their end of the shared responsibility model, all major cloud providers offer security hubs that provide a comprehensive view of customer services, such as AWS Security Hub, Azure Security Center, and Security Command Center for Google Cloud. While these offerings, as well as discreet security features attached to some services, can help organizations strengthen their cloud security posture, they are limited in scope. They address basic security requirements and don't provide a single-pane-of-glass view across all environments.

The cloud providers' approach has been one of making visibility and some basic security configurations easier but has steered clear of more advanced security controls. Moreover, built-in security tools will lock you in even further to one specific cloud provider.

Each of these approaches has certain limitations and doesn't provide full visibility, automation, and remediation to address the problem efficiently, especially at scale. A more comprehensive and consistent approach is necessary. Secure cloud configuration must be a dynamic and continuous process and include automated remediation.

To meet the needs of the changing environment, organizations with hundreds of developers continuously releasing new code into production should look for a fully automated cloud security and compliance assurance solution. That's where the concept of **Cloud Security Posture Management** comes into play.

What is Cloud Security Posture Management?

Cloud Security Posture Management, or CSPM, is a relatively new cloud security category designed to address configuration and compliance risks in your cloud infrastructure. The concept of CSPM is to enable organizations to automatically discover, assess, and remediate security configuration issues and gaps across multiple cloud providers and accounts. This approach ensures that at any given moment you have a consistent, secure, and compliant cloud infrastructure.

The CSPM term was coined by Gartner and according to their description, "CPSM offerings continuously manage cloud risk through the prevention, detection, response, and prediction of where excessive cloud infrastructure risk resides based on common frameworks, regulatory requirements and enterprise policies. The core of CSPM offerings proactively and reactively discover and assess risk/trust of cloud services configuration (such as network and storage configuration), and security settings (such as account privileges and encryption)"[10].

[10] Gartner, Innovation Insight for Cloud Security Posture Management, 2019

How CSPM Works

Unlike host-based security tools, CSPM solutions operate at the cloud provider control plane level and leverage APIs from the underlying cloud vendor.
This provides unique visibility into the configuration of the cloud services to automatically validate hundreds of settings across regions and accounts. With this access, CSPM tools assess the current security posture against best practices, policies, and compliance frameworks and help detect such issues as:

- Misconfigured storage buckets exposed publicly
- Compute and database resources with unintended public access
- The use of encryption in transit and at rest across cloud services
- User policy definitions to ensure least-privileged access to resources
- Changes to critical resources such as firewall rules, logging groups, or account settings
- Activity in unused or unexpected cloud provider regions or locations

> Through 2024, organizations implementing a CSPM offering and extending this into development will reduce cloud-related security incidents due to misconfiguration by 80%
>
> *Gartner, 4 Trends Impacting Cloud Adoption in 2020*

Critical elements of CSPM solutions:

Multi-cloud visibility

Most enterprises don't have comprehensive visibility into their cloud deployments and services while full visibility is crucial for tracking misconfigurations. Virtually all enterprise organizations of a certain size end up using more than one cloud provider, either by design or due to evolution (acquisitions, geographical coverage, special services, etc.). In contrast to the native cloud providers' tools, CSPM delivers single-pane-of-glass visibility across all environments, including multiple clouds, regions, and services, no matter how many you use.

CSPM solutions should provide different levels of automation, such as remediation guidance and auto-remediation, and include an option for building a self-securing infrastructure

Auto-remediation

It's not enough to just get alerts and reports about identified misconfigurations, organizations must be able to respond and take actions to remediate them. Since modern cloud environments have an overwhelming number of configurations that make it impossible to fix them manually, automation is key. To make it comfortable, CSPM solutions should be able to provide different levels of automation, such as remediation guidance and auto-remediation, and, ideally, include an option for building a self-securing infrastructure.

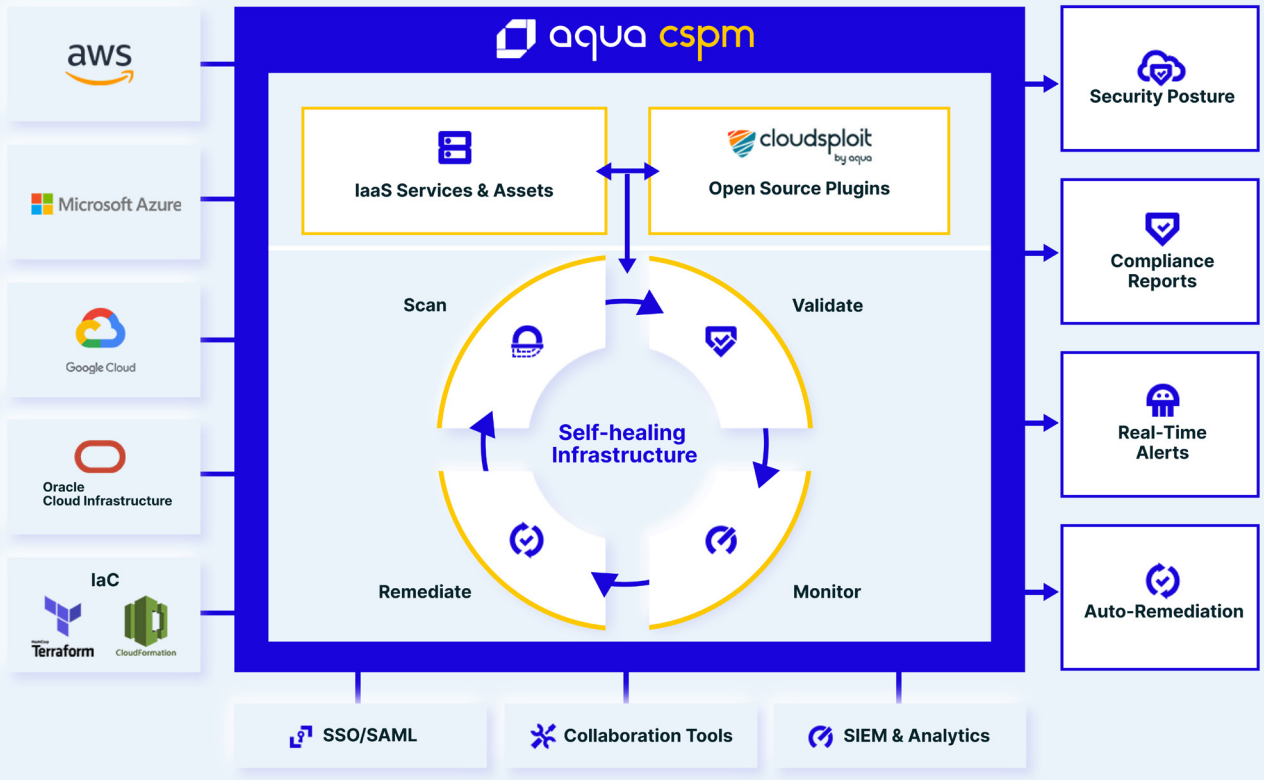
Compliance reporting

CSPM provides reporting for common compliance frameworks and standards, such as PCI-DSS, HIPAA, AWS Well-Architected Framework, GDPR, CIS Benchmarks, NIST, and ISO27001, and various custom compliance requirements. Organizations should have the opportunity to filter reports by region, cloud provider service category (e.g., AWS EC2, AWS S3), severity level, etc., and generate their own customizable reports.

Meet Aqua CSPM

Aqua CSPM is a cloud security auditing, monitoring, and remediation solution that scans your entire public cloud infrastructure for potential security risks, including misconfigurations, malicious API calls, and insider threats. With each scan, it securely connects to your cloud account through the APIs of the underlying cloud provider, collects the necessary data, and then checks it for potential risks and misconfigurations. For each configuration Aqua CSPM has a plugin – a piece of software that checks this specific setting and compares it to the corresponding best practice and, in case of misconfiguration, offers remediation steps.

Aqua CSPM Diagram



Main features of Aqua CSPM:

Visibility across your entire multi-cloud infrastructure

Aqua CSPM continually audits your cloud accounts for security risks and misconfigurations across hundreds of configuration settings and compliance best practices, enabling consistent, unified multi-cloud security for AWS, Azure, Google Cloud, and Oracle.

Transparency

Aqua CSPM maintains a central and open repository of best practices for cloud security and sends alerts when they are not being adhered to. The repository is continuously updated, based on new security configuration best practices developed by Aqua's experts.

Aqua CSPM provides self-securing capabilities to ensure your cloud accounts don't drift out of compliance

Automated and semi-automated remediation

Aqua CSPM not only detects configuration issues but also allows organizations to efficiently remediate them on an ongoing basis, offering several levels of control (assisted/manual/automated). You can get detailed, actionable remediation advice and alerts, or choose automatic remediation of misconfigured services with granular control over chosen fixes. Thus, Aqua provides self-securing capabilities to ensure your cloud accounts don't drift out of compliance.

Extensive compliance reporting

Aqua CSPM supports a broad list of industry standards and frameworks, such as PCI-DSS, HIPAA, AWS Well-Architected Framework, CIS Benchmark, GDPR, SOC 2 Type 2, ISO27001, NIST, as well as allows you to implement custom compliance requirements for specific types of checks and conditions.

Real-time control plane events monitoring

Sometimes scanning isn't enough, and real-time notifications for things like disabled MFA or other high-level security operations may be necessary. With the power of Amazon CloudTrail, Aqua analyzes in real-time each supported API call for violations of security best practices, potential compromises, or malicious activity. By providing visibility into all your cloud control-plane API calls, it enables teams to get alerts on certain API activity when seconds and minutes matter.

Built for enterprise scale

Supporting multiple users and teams across hundreds of cloud accounts, Aqua CSPM integrates with many SIEM and collaboration tools, including Splunk, Slack, OpsGenie, PagerDuty, Microsoft Teams, and more. Fully documented RESTful APIs make it easy for you to create additional integrations and automate workflows.

Infrastructure-as-Code template scanning

Aqua CSPM helps secure your infrastructure-as-code templates with its built-in IaC scanning engine. You can check Terraform and AWS CloudFormation templates for security issues before the deployment of the infrastructure itself. Applying this "shift left" approach in CSPM reduces risk and security incidents in production.

Extensible open source architecture

Based on CloudSploit open source project, Aqua CSPM has an open core architecture, whereby the entire scanning engine is open source. It provides full transparency into why, what, and how your cloud accounts are tested (you can check all the plugins on the respective GitHub page), enables users to easily develop new plugins to address specific issues in any cloud service and share them with the community.

Conclusion

With businesses rapidly moving to the cloud, understanding the unique cloud security challenges is essential for managing risks. However, many organizations struggle to find the right tools to adequately address them. An ever-increasing complexity of dynamic cloud environments and the current pace of change make manual configuration ineffective and, at a large scale, impossible. In such context, CSPM becomes critical for tackling security issues across the IaaS cloud stack.

With Aqua CSPM, organizations can continuously monitor and manage their security posture across multi-cloud infrastructure and detect thousands of threats in their cloud accounts. To amplify the benefits of the CSPM tool, it's essential to weave it into your larger cloud native security strategy, one that covers your entire technology stack from infrastructure to workloads.

Securing modern agile environments requires a holistic approach. It means embedding security across an entire application lifecycle: in the build process from the start and in a run-time environment as well. By combining cloud workload protection for VMs, containers, and serverless, with cloud infrastructure best practices you can achieve full-stack security across all your cloud native deployments.

Try Aqua CSPM on Aqua Wave

Get Started

Aqua Security is the largest pure-play cloud native security company, providing customers the freedom to innovate and run their businesses with minimal friction. The Aqua Cloud Native Security Platform provides prevention, detection, and response automation across the entire application lifecycle to secure the build, secure cloud infrastructure and secure running workloads wherever they are deployed. Aqua customers are among the world's largest enterprises in financial services, software, media, manufacturing and retail, with implementations across a broad range of cloud providers and modern technology stacks spanning containers, serverless functions, and cloud VMs.

aquasec.com
contact@aquasec.com
@AquaSecTeam
in/Aqua Security