Cloudy with a Chance of Security

How Mid-Sized Organizations Are Managing Biggest Cloud Security Challenges

Table of Contents:

Cloud changes everything. When a business relied exclusively on on-premises infrastructure, security teams and engineers enjoyed control over every facet of cost, performance, and security. With digital transformation efforts pushing swathes of infrastructure onto the cloud, new challenges are appearing at an unprecedented rate. Now, cloud environments have upended the ethos of not just centralized access - but the entire worldview of perimeter security.

Below, we walk through today's most pressing cloud security challenges, dive deep into the struggles previously facing four mid-sized organizations, and finally, demonstrate how Wiz can supercharge cloud security.

Today’s cloud challenges: To visibility and beyond

Cloud challenges can be as hard to pin down as their multifaceted attack paths; however, at Wiz, we know that identifying your current cloud challenges is the first step toward fixing them.

Lateral superhighways

We call the interconnected flaws an attacker could use “toxic combinations”: for instance, an exposed resource might have a secret which lets a hacker infiltrate a different part of the environment - which itself contains sensitive data. A similar toxic combination was the root cause behind the Capital One breach that, in September 2022, spiraled into a $190 million class action settlement. The complexity of cloud resources lend themselves to this tightly-interconnected layout of exploits that is almost impossible to stop with siloed and point solutions.

Lack of visibility

Lack of visibility is a defining challenge of cloud infrastructure. The complexity of cloud resources scales linearly with the quantity thereof, meaning that an organization freshly out of stealth may all of a sudden find themselves overwhelmed with patch lists and CVEs. Point solutions that address individual cloud security components are blindly firing demands at security teams without context. As a result, security professionals are unable to confidently say that they have full visibility into their cloud environments.

Bloated patch lists

The increased expansiveness of cloud resources has drastically increased each organization's asset spread - each of which still demands close monitoring and protection. Complicating things even further is the fact that traditional security controls don't truly fulfill cloud security needs. As a result, security teams are left spending hours on frantic patch installs that may not even intersect with actual attack paths.

New ownership models

These overarching architectural challenges rapidly trickle down to the organizational level. For instance - due to cloud - architecture is now largely owned by the teams that directly manage it. While development cycles have made incredible gains from this democratization, security has found themselves paralyzed in the sudden explosion of unique, third-party resources. Security teams continue to be deeply siloed, preventing the integration of cloud-native security perspectives and throttling progress toward true protection.

The talent drought

The struggle of today's architecture is having a drastic impact on talent acquisition. Often siloed and disconnected from engineering and dev teams - and the field itself often seen as a blocker - security has taken an increasing toll on employment rates. Current reports hint at an all-time-high demand for security analysts, with roughly 700,000 unfilled positions.

With cloud security becoming increasingly important, it becomes imperative that your organization's cloud security program is stocked with highly actionable and efficient tools. What if your tools could go even further - and turn security from a blocker into a value add?

Four tales of cloud troubles

Let's take a closer look at the struggles previously facing four Wiz customers. Across disconnected engineering teams and slapdash exploit management, their pre-Wiz stories may resonate with your own organization's.

SAI360

SAI360 is an integrated risk management company that provides compliance systems for corporate, environmental and governmental organizations. Their small security team shares the responsibilities of keeping 2000 cloud instances secure.

When Nick Bruno joined the security team as CISO 18 months ago, he was faced with a sprawling hybrid setup. While the team already had an agent-based security solution in place, their visibility was disorganized and broken. Complete visibility was almost impossible due to the fact that there was no easy way to identify a gap in agent coverage.

And for the endpoints that were protected, any identified vulnerabilities were pouring in with little rhyme or reason. For a security team of just 5, the pressure to find and patch instances affected by each vulnerability was mounting.

With no form of on-the-ground risk assessment, Nick and his team were left frustrated at the in-the-dark patching process; there was also a real sense of disconnect with the otherwise-engaged engineering teams. They needed a solution that looked beyond individual endpoints; one with contextual visibility, that put them and the development teams on the same page.

Renaissance Learning

Renaissance Learning's cloud-based assessment and learning programmes help students receive first-class education. Providing teachers and schools with a diverse portfolio of 16 products, CISO Bob Stasio currently manages a global team of 70 - they work on everything from IT security to enterprise applications. All in all, their 3000-strong environment had grown consistently since the mid-90s.

> **[Acquisitions] have to happen pretty quickly. If you're in security, you really don't want to get in the way and mess things up. But you also need to understand what you're buying...**

Throughout the decades, Renaissance's development had outgrown the development style of its first 2 products. The heavily siloed operations of each product was making each security element extraordinarily difficult to understand in context. Going to each group and individually withdrawing their security disposition, alongside their established vulnerabilities and priorities, made each silo a free-spinning cog, with no coordination in between. For Bob, attempting to prioritize risk management across the dozen different teams was a nonstop headache.

Alongside these pre-established hurdles, Renaissance Learning was also undergoing a period of rapid acquisitions. The speed of such takeovers meant that Bob, as a member of the diligence team, was tasked with an impossible job: you don't want to get in the way, but it's an imperative that risk is adequately judged before the purchase is made.

Overall, translating security - both inside and external to the core organization - into an accessible to-do list represented Renaissance Learning's greatest challenge.

Boost Security

Providing a platform for DevSecOps automation, newly-unstealthed Boost Security relies on a team of just 25 employees. AWS provides the backbone of their infrastructure, and - with the distinct focus that Boost places on supply chain security - the 3 inhouse security professionals have a reputation to guard. Already notching a number of large clients under their belt, Boost's cloud infrastructure is built to scale rapidly.

Francois Proulx, part of the Product Security team, notes how Boost's focus on infrastructure as code does - in theory - lend itself to a full picture of every potential vulnerability. However, even as an employee that has been with Boost since day 1, Francois recognized that they were missing a link. When it's all viewed as code, the true risk presented by each cluster and node was becoming incredibly difficult to contextualize with the human eye. The bigger picture was almost impossible to identify. This was compounded by the fact that Francois' team had a multi-disciplinary focus: responsible for application security and SOC2 compliance, they simply did not have the extra time to spend tracing out the wider regions and zones of every vulnerable cluster. As a result, the team was struggling to keep up with the cloud's threat model.

Maple

Finally, Maple is a Toronto-based telemedicine platform that connects patients with healthcare providers. Similar to Boost, security and privacy take center-stage as major differentiators. Staying at the forefront of security is a key component to Information Security executive Patrick Lafleur.

> Going to an engineering or DevOps team with a huge pile of problems is just never going to work

The wrench thrown into their works arrived in the form of Log4Shell. CVE-2021-44228, or Log4Shell, is a critical RCE vulnerability that was discovered in a popular Java library in 2021. Having seeped into millions of applications, this highly-accessible exploit was suddenly a core component of swathes of logging infrastructure. Patrick was able to prove that it wasn't present in any of their own in-house products. Whether it was somehow being pulled in from any third-party tool, however - the team of 4 was essentially left in the dark.

Alongside this short-term scramble, Patrick had also identified the weaknesses in their current security tooling. Throughout the hundreds of AWS instances they were overseeing, the various vulnerabilities would only be presented in a big list of issues.

Furthermore, the tools that don't provide enough context are timesinks of their own: somebody still needs to manually dig deeper into each flaw. Placing stacks of fixes on the engineering teams' workflows was not only accruing a huge backlog, but further cementing security as a major roadblock.

How Wiz transforms security

Whereas oldschool security measures have attempted to break cloud security into bite size pieces, this reductive approach has proven itself a detriment. Wiz transforms the way in which organizations approach their cloud security by stitching together every point security into a single platform that correlates, analyzes and protects across all domains.

Visibility that tracks

As attacks grow in complexity and coordination, security teams need to be given the same cross-operational force. Wiz is a cloud agnostic tool that deploys across your entire tech stack. This allows us to provide immediate visibility into every compute platform and application making up your cloud infrastructure. Instead of segmenting risk by cloud environment, Wiz focuses on your total cloud inventory - and the risks therein. From external exposures, to risky PII locations and container security vulnerabilities, Wiz collects each potential security concern. Finally, this hyper-granular data is contextualized and fed into the security graph.

For Kubernetes-heavy infrastructure, Wiz's ability to provide deep insight into deployment spots is a game changer. For AWS and Azure, security teams no longer need to jump across different native solutions, or attempt to juggle flaws manually. Wiz's simplicity and applicability allows us to provide protection for 35% of Fortune 100 companies, as well as small to mid-size companies - across all industries and sizes.

Security that's simplified

Wiz allows security to be translated into each team's native language. For the technical security teams, Wiz's contextual understanding allows it to discover toxic combinations across unpatched vulnerabilities.

These attack paths are then prioritized in order of severity - illuminating corners of your cloud that even experienced security leaders may have overlooked. This wipes out the noise plaguing your team, leading to leaner security teams and allowing you to upskill the talent you have. Even the rollout is one of the simplest out of any security tool - just connect up to your cloud environment's API, and let our industry experts make any necessary changes.

Wiz's contextual expertise is built to easily translate security to other teams. Integrating with various ticket systems, Wiz cuts out the fluff to show exactly who needs to do what. Prioritizing and using people's time in the most effective way possible extends even to the stakeholders. By bringing dev groups to the table and letting the data speak for itself, Wiz builds a security culture of multi-departmental ownership.

How to begin your journey to simple cloud security

Security no longer needs to be a speed bump in the road of product development - instead, Wiz ingrains security across the board, resulting in unprecedented time to value. The pace of security can now keep up with rapid scaling and even aggressive acquisitions. Supercharge your security and place the final piece of the DevSecOps puzzle in place with Wiz. To see a live demo, get in touch today.

Interested in learning more? Watch the webinar!

About Wiz

Wiz secures everything organizations build and run in the cloud. Founded in 2020, Wiz is the fastest-growing software company in the world, scaling from $1M to $100M ARR in 18 months. Wiz enables hundreds of organizations worldwide, including 30 percent of the Fortune 500, to rapidly identify and remove critical risks in cloud environments. Its customers include Salesforce, Slack, Mars, BMW, Avery Dennison, Priceline, Cushman & Wakefield, DocuSign, Plaid, and Agoda, among others. Wiz is backed by Sequoia, Index Ventures, Insight Partners, Salesforce, Blackstone, Advent, Greenoaks and Aglaé. Visit https://www.wiz.io/ for more information.