Wiz for Cloud Security Posture Management

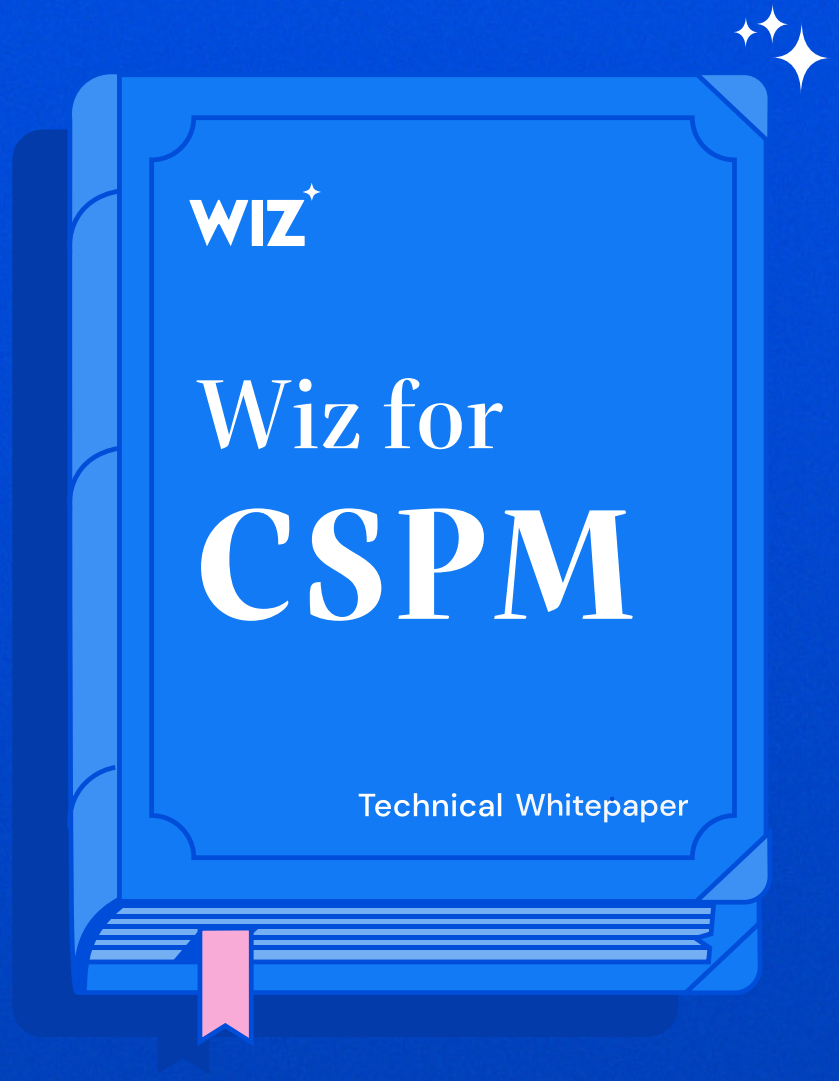


Table of Contents:

Why organizations need a Cloud Security Posture Management (CSPM) 3

Security in the cloud is a shared responsibility 3

Cloud environments are complex 3

Manual compliance 3

Siloed people, processes, and technologies 3

Operational inefficiency that slows down cloud adoption 4

What is CSPM? 4

The need for a better CSPM 5

Lack of context 5

Noise without prioritization 5

Operational inefficiency 5

Wiz for CSPM Reference Architecture 6

How do I use Wiz to improve my security posture? 6

Gain full visibility into my environment 7

Identify misconfigurations 7

Find toxic combinations 8

Prioritize issues 9

Understand my compliance status 9

Demonstrate compliance 10

Meet unique requirements 11

Democratize security in my organization 11

Remediate issues faster 12

Shift-left to identify issues in development 12

Success criteria for establishing a secure foundation with Wiz CSPM 13

Why organizations need a Cloud Security Posture Management (CSPM)

Security in the cloud is a shared responsibility

Cloud service providers (CSP) adhere to a shared responsibility model where the CSP is responsible for protecting the underlying infrastructure that run the cloud services, but customers are responsible for the security of the resource configurations, workloads, applications, and data.

Cloud environments are complex

Cloud environments are complex by nature, with multiple compute types from virtual machines, serverless, and containers, to multi-cloud environments. The dynamic nature of the cloud makes it easy to spin up resources in the click of a button, enabling organizations to scale their cloud footprint rapidly. The more the environment grows, the more resources there are to protect, and it becomes too time consuming for a human to manage the configurations of cloud resources manually.

Manual compliance

The increased complexity and scale of cloud environments creates new challenges of managing compliance at scale. Organizations need to ensure continuous compliance of their unique regulatory requirements across all their environments and their clouds and develop visibility and control into their new compliance processes. Traditional manual compliance processes cannot keep up with this scale, and organizations are left unable to successfully de-risk all their cloud environments at scale.

Siloed people, processes, and technologies

Organizations running in multi-cloud environments use different security tools for each CSP, resulting in different processes and unique expertise per tool. Additionally, traditional security tools only focus on a specific area of the security posture, for example vulnerability management, and the security data for each risk factor resides in the different tools. Organizations must correlate the data from each tool manually, resulting in further siloes in processes, operational overhead, and lack of holistic view.

Operational inefficiency that slows down cloud adoption

The cloud enables developers to develop faster than they ever have before. Developers are the ones spinning up resources in the cloud, but it is the security team's responsibility to ensure that the resources are secure. Security tools are not built for development teams in their core, and with the rapid pace of innovation, it becomes operationally challenging for security teams to detect risks early before they are exploited.

What is CSPM?

The category of security products, CSPM, was defined by Gartner to address the above challenges by continuously identifying risks in the cloud and assessing security posture across multi-cloud environments.

With so many different configurations on the cloud, it's easy to make a mistake that weakens the overall security posture of your environment. These mistakes often go unnoticed for long periods of time, putting the organization at risk of a breach. With CSPM, you can proactively identify these types of misconfigurations so you can remediate them before they are exploited. A CSPM maintains an inventory of cloud assets and runs risk analysis to detect any misconfigurations in your environment. It alerts you of misconfigurations and allows your team to act quickly and remediate any issues. CSPM also automates compliance on the cloud by evaluating the configuration of cloud resources against common standards and frameworks, helping organizations meet regulatory requirements.

A CSPM tool helps secure cloud workloads more efficiently and at a greater scale than you could if you relied on manual or periodic auditing of cloud configurations.

The need for a better CSPM

Since the product category of CSPM has been introduced, the CSPM offerings have gone through several iterations of improvements to adopt a more comprehensive and holistic view of security. Traditional CSPM tools only focus on cloud misconfigurations, missing out on many other risks that when combined with misconfigurations, could significantly impact security posture and increase your attack surface. The following are gaps of traditional CSPM tools that leaves organizations in need for a modern and holistic solution:

Lack of context

Legacy CSPM tools lack the context teams need to fully understand the risks in their environment. To get a full understanding of your security posture and the risks criticality, you need to consider more than just the misconfiguration of your resources, but how all other risks in your environment come together to create a toxic combination that requires your attention. Traditional CSPMs don't take into account other important risks such as vulnerabilities, network paths, identity exposures, secrets, malware, sensitive data, lateral movement and therefore lack a significant amount of information that is required to understand the toxic combinations in your environment.

Noise without prioritization

Traditional CSPMs give you a lengthy list of issues. How can your team prioritize these issues without a full understanding of their criticality? For example, a traditional CSPM shows a misconfiguration issue for a virtual machine that is publicly exposed. How would you know what the criticality of that issue is if we do not know what is running on the machine, its network paths, permissions, what data it can access, if it has a vulnerability, or if it could cause any lateral movement in your environment? This is all important information security teams need to know to reduce noise, prioritize, and focus on the critical risks in their environment.

Operational inefficiency

Traditional tools are often not comprehensive, missing support for cloud service providers or Kubernetes, resulting in teams using unique tools per CSP. In addition, since traditional CSPM tools lack the needed context, organizations must use additional security tools to get the full picture of their security posture. This results in a fragmented view of the organization’s security posture with security data residing in different silos. Often, these tools are owned by different teams and require different processes, creating further operational challenges in the organization.

Wiz for CSPM Reference Architecture

Unlike legacy CSPM tools, Wiz CSPM takes a modern approach to security in the cloud by looking across all risk factors to identify toxic combinations that put your environment at critical risk. Wiz does deep risk analysis not only of misconfigurations, but also across network exposures, secrets, vulnerabilities, malware, data, and identities. By using a unified risk engine across all risk factors, with the same back-end data model, Wiz is able to correlate all risk factors to understand toxic combinations in an environment. Risks are prioritized and modeled on the Wiz security Graph to give you the full context around risks with actionable insights so you can focus on the risks that matter.

Wiz doesn't require any agents, and simply connects to your CSP using APIs to scan for the resources in your environment without causing the operational overhead of agent-based tools.

How do I use Wiz to improve my security posture?

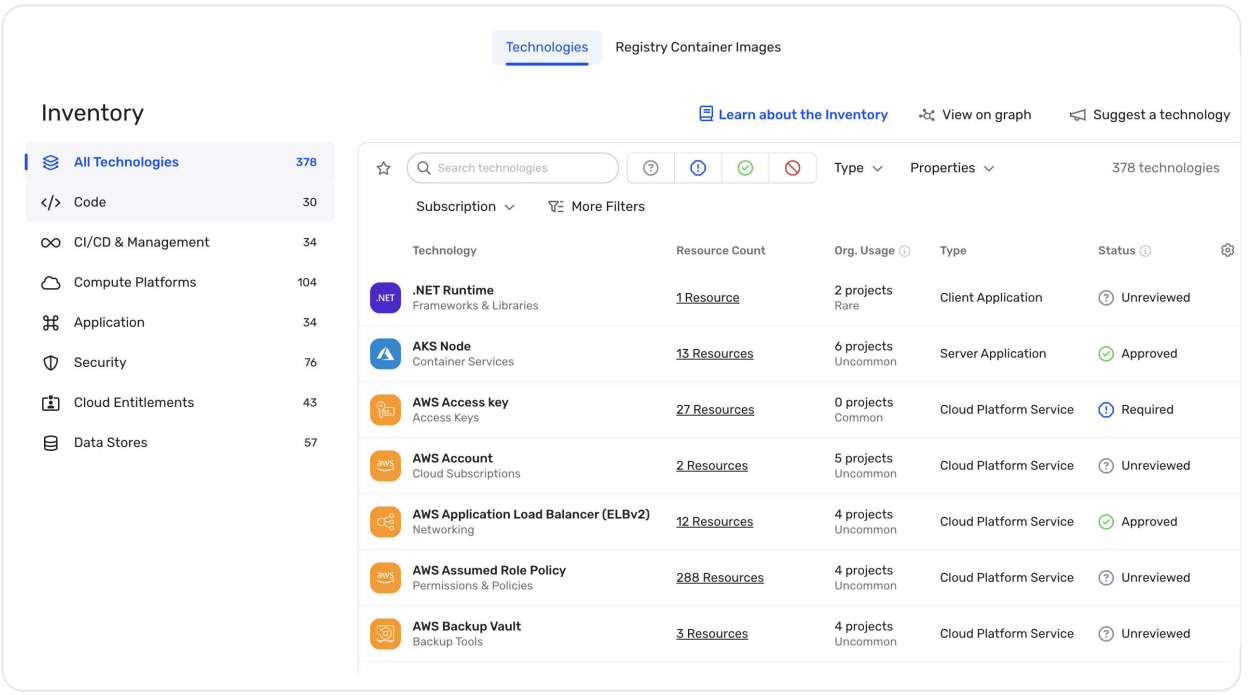
Wiz for CSPM Reference Architecture



1. Gain full visibility into my environment

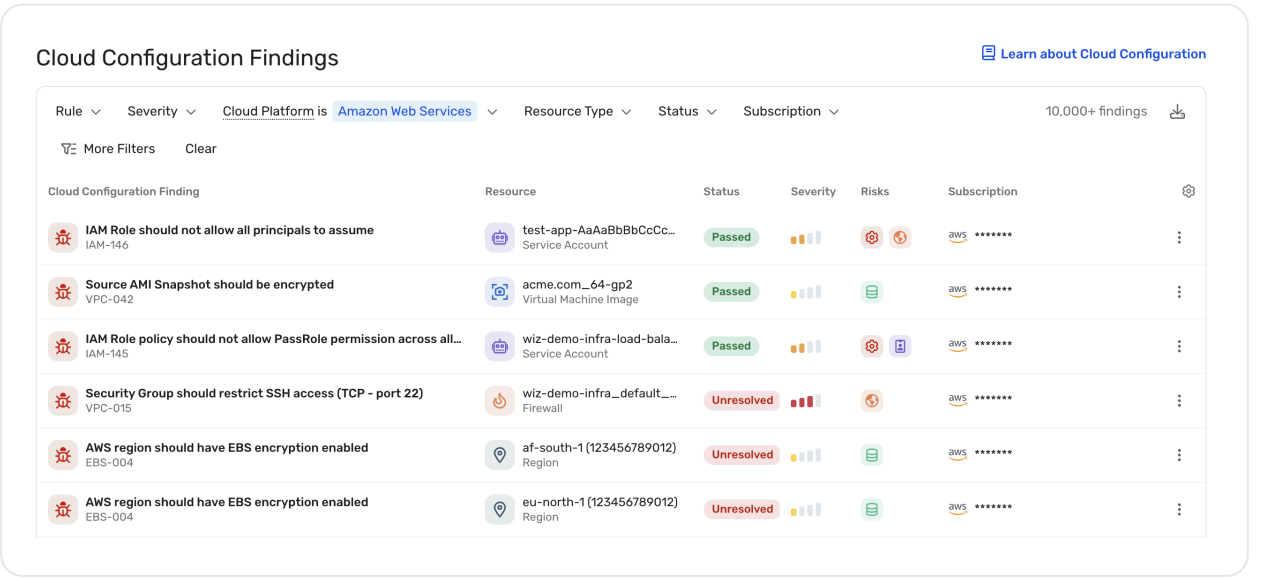
Connect Wiz to your cloud environment in minutes by granting Wiz read-only access on the organization level. You can connect Wiz to almost any virtualized compute platform out there: AWS, Azure, GCP, Alibaba Cloud, Oracle Cloud, Kubernetes, VMware, and you only need a single connector per cloud provider. Once connected, Wiz uses the cloud providers' native APIs to agentlessly scan your environment to give you visibility into your entire technology stack, both on the cloud layer, as well as the workload layer across virtual machines, containers, and serverless.

You can find the list of all detected technologies in your environment in the Inventory page, which gives you complete visibility into everything in your environment, including cloud services such as EC2, AKS, or S3, coding languages or frameworks such as Go, Python, or React, as well as operating systems or applications such as Linux, NGINX, Docker, or Ansible.



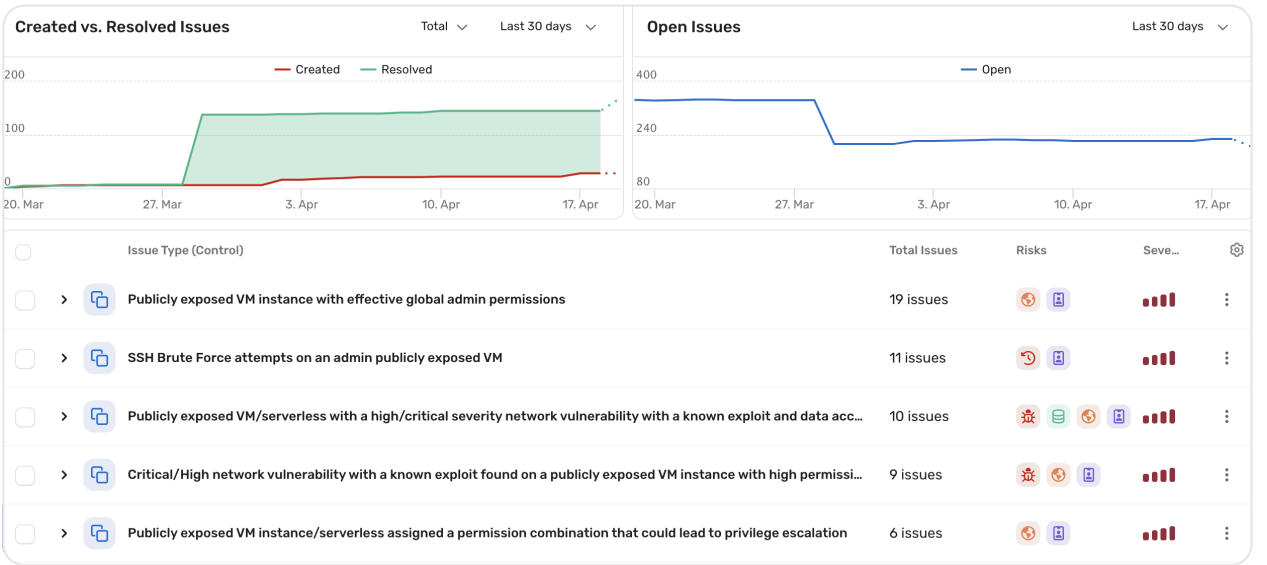
2. Identify misconfigurations

To identify misconfigurations on the cloud layer, you can view the Cloud Configuration Findings that are generated by Wiz for each misconfiguration found in your cloud resources. Wiz has over 2,000 Cloud Configuration Rules for frameworks such as CIS, NIST, PCI and others. To understand misconfigurations on the OS and application-level, you can view the Host Configuration Findings, which are generated by assessing over 10,000 Host Configuration Rules according to CIS benchmarks such as CIS Benchmark for Red Hat Enterprise Linux, Ubuntu Linux, NGINX, and Microsoft Windows Server. The findings generated for both cloud and host configuration rules have assigned severity so your team can prioritize findings based on criticality.



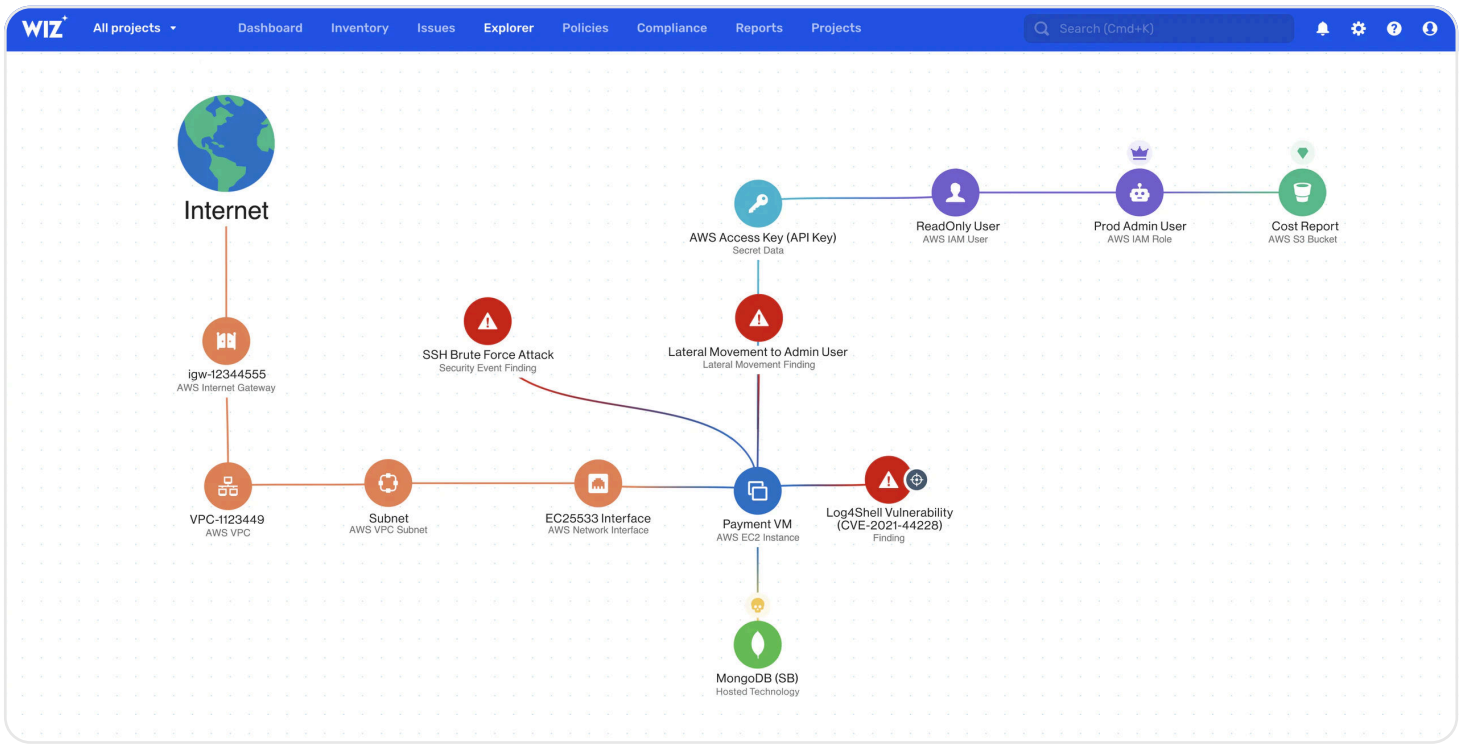
3. Find toxic combinations

To understand the real criticality of risks, you need to understand how different risks come together to create a toxic combination that can put your environment at critical risk. Wiz does deep risk assessment and automatically correlates risks across misconfigurations, vulnerabilities, networks, identities, secrets, malware, and data to identify the toxic combinations in your environment. Wiz calculates the effective network and identity exposures, and using attack path analysis can discover which misconfigurations can lead to lateral movement paths that compromise high-value assets. You can view toxic combinations in your environment on the Issues page, which lists all issues and their severity that are created by evaluating hundreds of built-in controls, for example for “Publicly exposed VM instance with effective global admin permissions “. Toxic combinations allow you to focus on the actual critical risks in your environment, rather than distracting noise.



4. Prioritize issues

Wiz builds a single risk queue that prioritizes what is the best next action for your team to take. You can view the risks you should prioritize from the Overview Dashboard, where you will find the most critical risks in your environment, with a breakdown based on risk factors such as secure configuration or external exposed issues. Issues are also modeled on the Wiz Security Graph, which pulls different security signals across the various layers of your cloud environment into a unified view. The graph makes it easy for anyone at any skill level to understand relationships between resources and the full context around risks. This enables your team to focus on the issues that matter, understand the real risk criticality, and respond to issues faster.



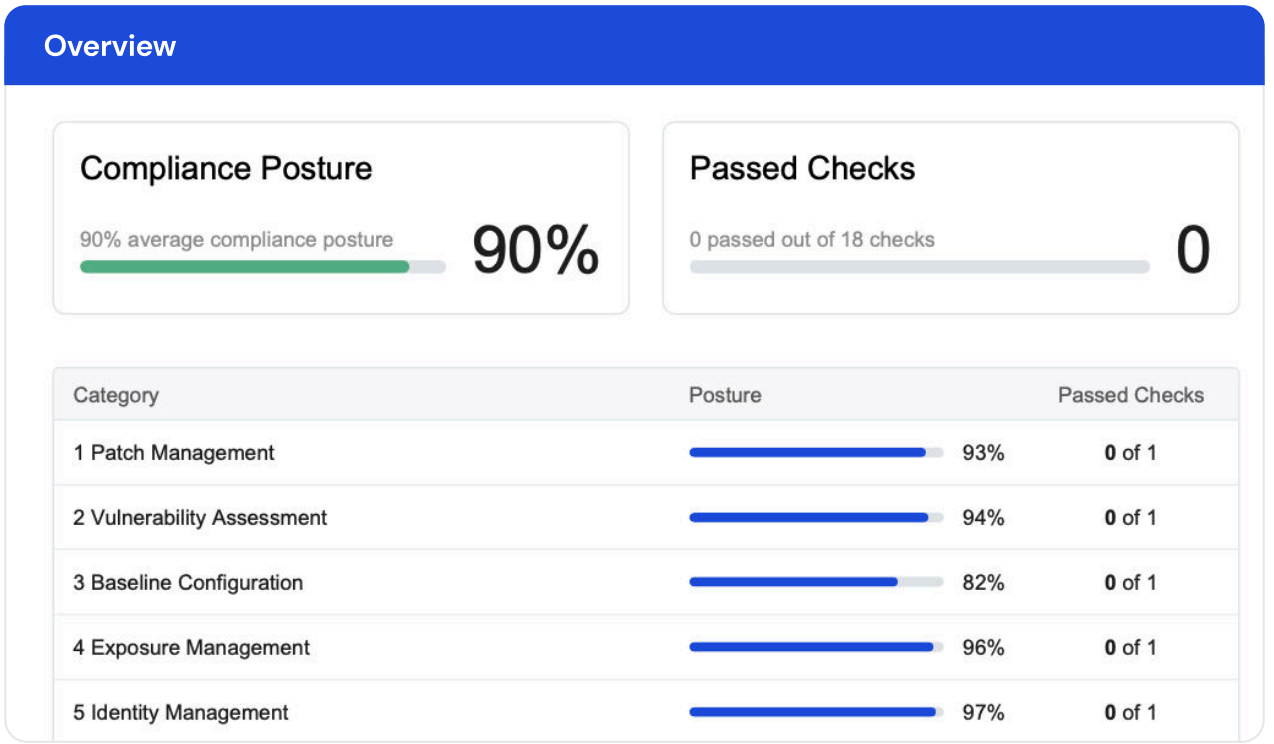
5. Understand my compliance status

Assess your environment against more than 100 built-in frameworks such as CIS, PCI, NIST, HIPAA, and GDPR on the Compliance page, where you will find your compliance status by framework or across multiple frameworks. The frameworks consist of built-in controls and misconfiguration rules that are mapped to the control lists and recommendations of each framework. You can find your overall compliance score for each framework, and view a heatmap of your overall compliance posture to understand where your weaknesses are.



6. Demonstrate compliance

Demonstrating compliance with your regulations can be a tedious process when done manually. With Wiz, you can quickly get a report of your compliance status across your entire environment with a click of a button. You can generate compliance reports on the Reports page, they can be as granular as a specific framework, business unit, or application or you choose from a high-level PDF report to share with stakeholders or a detailed CSV report for the DevOps and GRC teams.

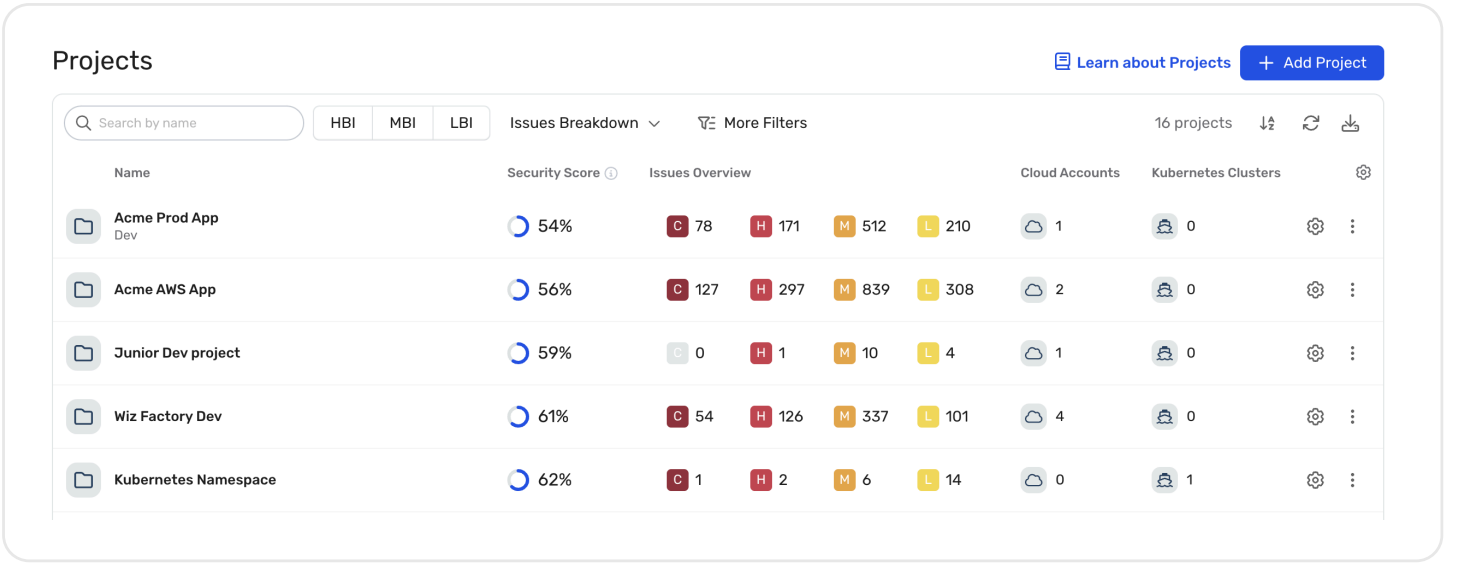


7. Meet unique requirements

One size doesn't fit all and in some cases, you might have unique regulations your organization must comply with that are not covered by the common frameworks. For unique needs based on your organization's domain and best practices, you can define a custom compliance framework and pick and choose which controls are needed for your organization. If you need further customization, you can also customize controls to check for unique scenarios by writing custom policies using Rego, which is the language used by OPA (Open Policy Agent).

8. Democratize security in my organization

Provide your teams with access to Wiz by defining RBAC controls to control what information users can see in Wiz and what actions they can perform. You can also set up granular environment segmentation and group cloud resources according to business units or applications using Projects. You can then define the RBAC controls to give developers access to track and remediate resources related to their projects. The Secure Configuration Dashboard provides developers with quick visibility into the most pressing configuration risks so they can prioritize remediation. Empower your developers with the context, prioritization, and specific remediation guidance so they can own remediation for risks related to resources they own.



9. Remediate issues faster

To ensure alerts for issues get addressed quickly, integrate Wiz with your existing ticketing system such as ServiceNow or Jira, so alerts go to the right people at the right time. Once alerted, your team can take advantage of the specific remediation guidance provided by Wiz for each issue, so you know exactly what action you need to take to remediate the issue. You can also set up automatic remediation to reduce manual processes by running playbooks in your environment. Wiz has built-in playbooks for some misconfiguration rules that you can deploy in your account, or you can create custom playbooks for specific use cases such as remediating misconfigurations on un-encrypted resources using your own keys.

10. Shift-left to identify issues in development

Integrate Wiz-cli, a locally deployed command line tool, in your CI/CD pipeline to detect and prevent security misconfigurations and vulnerabilities early in the development cycle. Empower your developers to prevent insecure resources from ever getting deployed and simplify operations by giving your developers and security team a single security policy spanning production and CI/CD pipeline.

```
[ec2-user@ ~]$ ./wizcli vm-image scan --id ami- --region eu-north-1 --subscriptionId
      _ _
 __ _(_)___  ___| (_)
 \ \ /\ / / |_  /  / __| | |
  \ V  V /| |/ /  | (__| | |
   \_/\_/ |_/___|  \___|_|_|
SUCCESS VM image scan analysis ready
OS Package vulnerabilities:
    Name: libkrb5-26-heimdal, Version: 7.5.0+dfsg-1
        CVE-2019-12098, Severity: LOW, Source: https://people.canonical.com/~ubuntu-security/cve/CVE-2019-12098.html
    Name: libudev1, Version: 237-3ubuntu10.46
        CVE-2021-33910, Severity: HIGH, Fixed version: 237-3ubuntu10.49, Source: https://people.canonical.com/~ubuntu-security/cve/CVE-2021-33910.html
        CVE-2020-13529, Severity: LOW, Fixed version: 237-3ubuntu10.49, Source: https://people.canonical.com/~ubuntu-security/cve/CVE-2020-13529.html
                        ⋮
    Name: gpg-agent, Version: 2.2.4-1ubuntu1.4
        CVE-2019-13050, Severity: LOW, Source: https://people.canonical.com/~ubuntu-security/cve/CVE-2019-13050.html
    Name: libxml2, Version: 2.9.4+dfsg1-6.1ubuntu1.3
        CVE-2021-3518, Severity: MEDIUM, Fixed version: 2.9.4+dfsg1-6.1ubuntu1.4, Source: https://people.canonical.com/~ubuntu-security/cve/CVE-2021-3518.html
        CVE-2021-3537, Severity: MEDIUM, Fixed version: 2.9.4+dfsg1-6.1ubuntu1.4, Source: https://people.canonical.com/~ubuntu-security/cve/CVE-2021-3537.html
        CVE-2021-3516, Severity: MEDIUM, Fixed version: 2.9.4+dfsg1-6.1ubuntu1.4, Source: https://people.canonical.com/~ubuntu-security/cve/CVE-2021-3516.html
        CVE-2021-3517, Severity: MEDIUM, Fixed version: 2.9.4+dfsg1-6.1ubuntu1.4, Source: https://people.canonical.com/~ubuntu-security/cve/CVE-2021-3517.html
        CVE-2020-24977, Severity: LOW, Fixed version: 2.9.4+dfsg1-6.1ubuntu1.4, Source: https://people.canonical.com/~ubuntu-security/cve/CVE-2020-24977.html
        CVE-2019-20388, Severity: LOW, Fixed version: 2.9.4+dfsg1-6.1ubuntu1.4, Source: https://people.canonical.com/~ubuntu-security/cve/CVE-2019-20388.html

Evaluated policy: Default vulnerabilities policy
Vulnerabilities: CRITICAL: 0, HIGH: 9, MEDIUM: 177, LOW: 146, INFORMATIONAL: 0
```

Success criteria for establishing a secure foundation with Wiz CSPM

- I have full visibility into my environment. I know what technologies are running including cloud resources, coding language, OS, and applications across VM, container, and serverless
- I am able to detect high-risk configuration findings both on the cloud layer as well as the host layer
- I understand the context around risks and their business impact. I understand how risks come together to create a toxic combination in my environment
- I can prioritize risks based on their criticality and focus on the most critical ones first
- My dev team has RBAC permissions to access Wiz and developers have visibility into the risks related to their resources and own remediation
- I get alerted on high-severity security issues using my existing ticketing system
- I identify risks early in development to ensure they won't reach production
- I comply with frameworks relevant to my organization and I can generate compliance reports to demonstrate my compliance
- When needed, I customize controls and frameworks to meet unique requirements
- I have automatic remediation in place to remediate issues where manual intervention is not required

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.