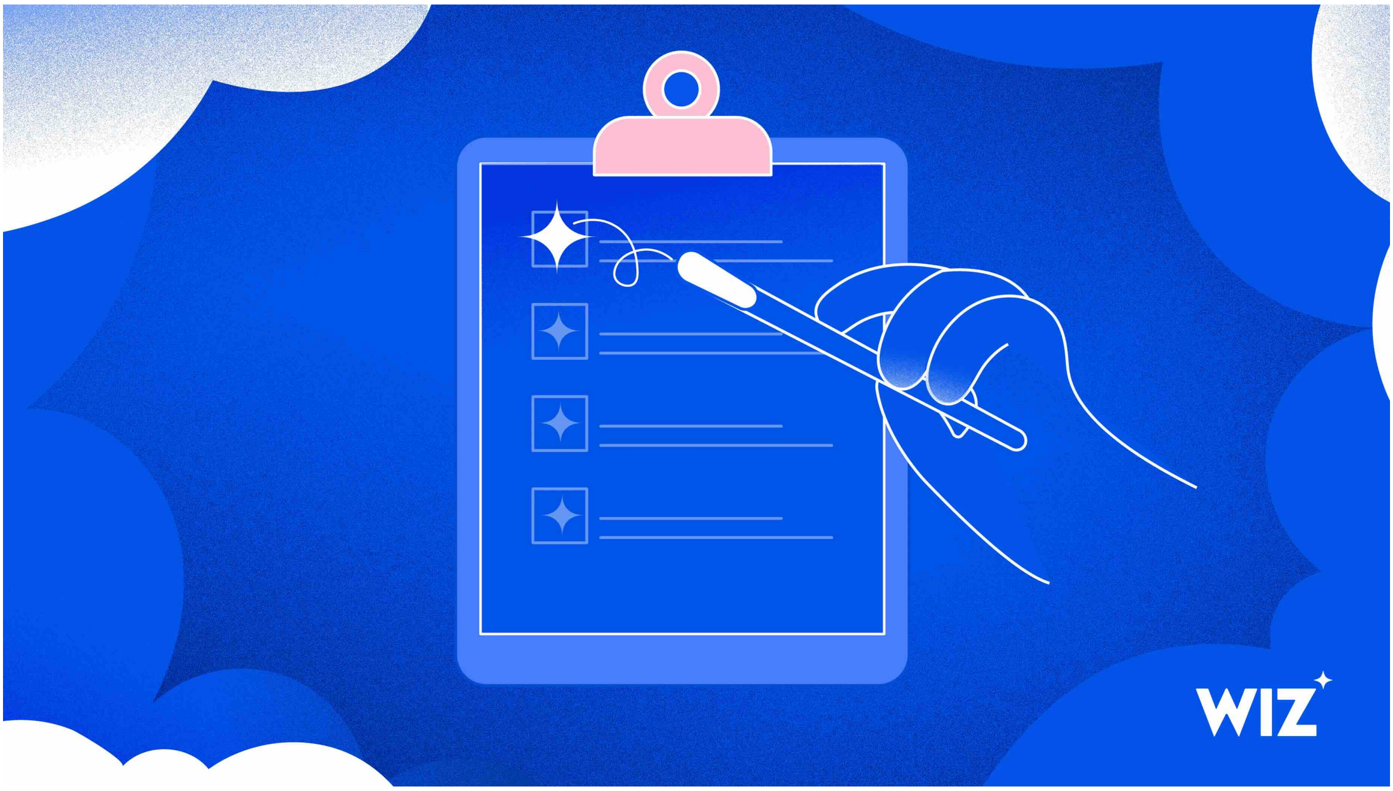
Compliance made easy with Wiz

Stay compliant with Wiz's 100+ compliance frameworks, generate quick compliance reports, and remediate issues faster with remediation guidance and auto-remediation.

Shaked Rotlevi, Daniel Klein March 14, 2023 4 minutes read



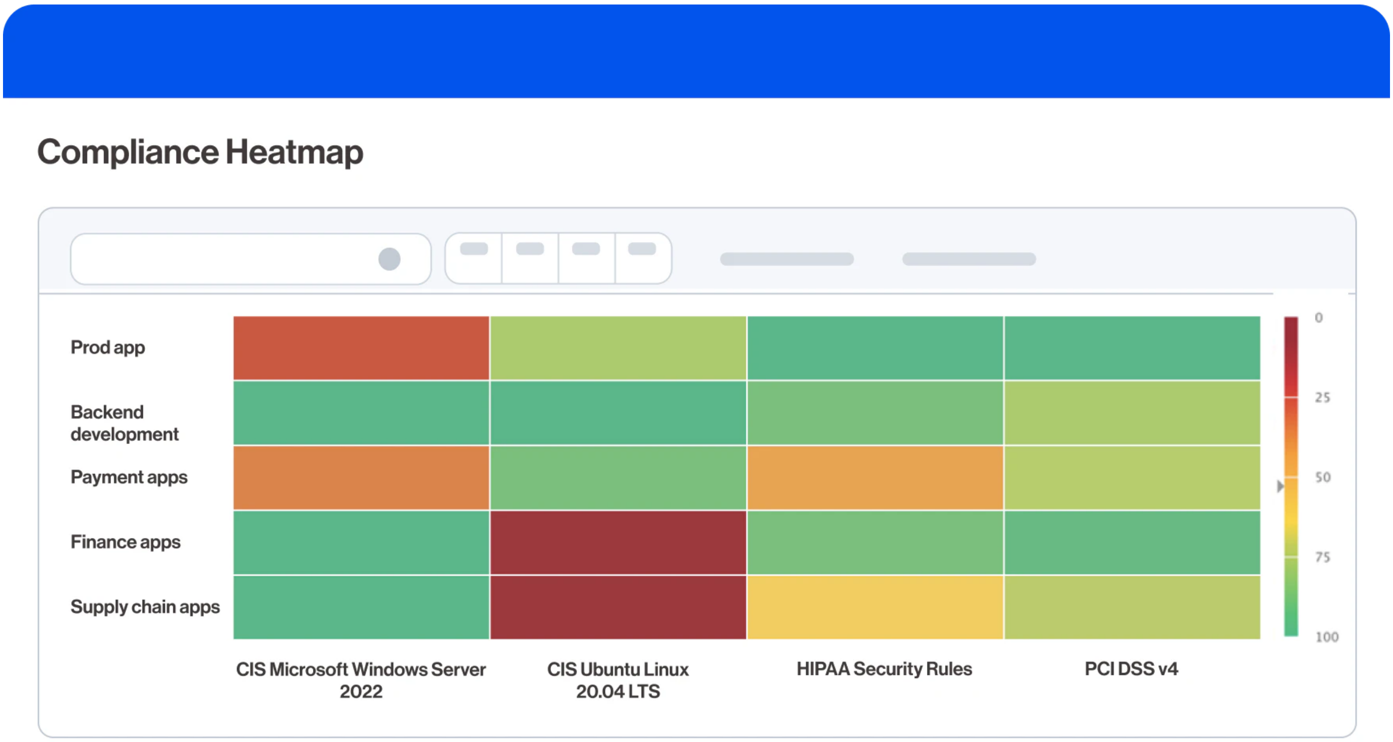
Editor's note: *In our first blog post* *for this series,*** *we talked about how you can assess your compliance posture across industry standards with Wiz's compliance heatmap. In this blog post, we will discuss additional compliance features that help you simplify compliance on the cloud.*

Staying compliant with frameworks like CIS and NIST in the cloud is challenging because it requires constant monitoring of complex and ever-changing regulations. It can be difficult to decipher legal language and align policies with regulations. It is also hard to understand how different fixes might improve your compliance posture. Wiz dramatically simplifies all these processes, saving you time, effort, and money. Wiz uses one policy across all your environments, so it doesn't matter if your workloads are running on AWS or Azure, Wiz will assess compliance across all your CSPs using the same policies. Let Wiz do the hard work of staying up to date with regulations and automatically assessing the compliance of your environment at scale, so you can focus on innovating your business.

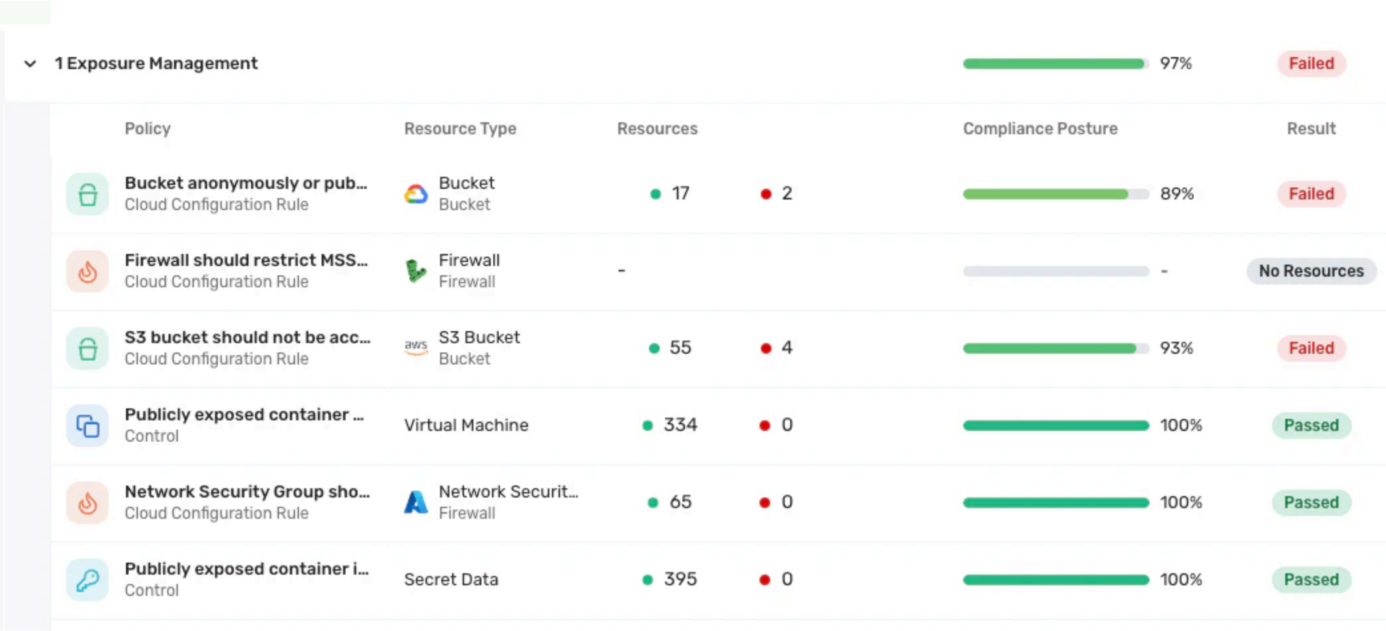
Wiz has over 100 built-in frameworks such as CIS, PCI, NIST, HIPAA, and GDPR and automatically assesses your environment against those frameworks so you can quickly understand your compliance posture. The frameworks consist of built-in controls and cloud configuration rules that are mapped to the control lists and recommendations of each framework. Wiz calculates your overall compliance score for each one of the frameworks and creates a heatmap for your overall compliance posture across all frameworks so you can have quick visibility.

Assess your hosts' compliance with built-in host frameworks

Assessing the compliance of your cloud configurations only gives you partial visibility into your compliance posture, as it lacks visibility into the OS and applications. We recently launched host misconfiguration rules, which check for misconfigurations on the OS and App levels without any agents. To extend our compliance offerings, in addition to having cloud frameworks, we also added over 60 built-in frameworks for host compliance such as CIS Benchmark for Red Hat Enterprise Linux, Ubuntu Linux, NGINX, and Microsoft Windows Server. The compliance status of the host frameworks is presented on the compliance heatmap together with the cloud configuration frameworks, giving you quick visibility into the weak areas in the compliance of your OS, applications, and cloud configurations, so you can address them quickly.



To gain a deeper understanding of your compliance score and understand where your weak areas are, you can drill down into a specific framework and see the different categories that constitute the framework and the status of each one of the rules.



1 Exposure Management 97% Failed

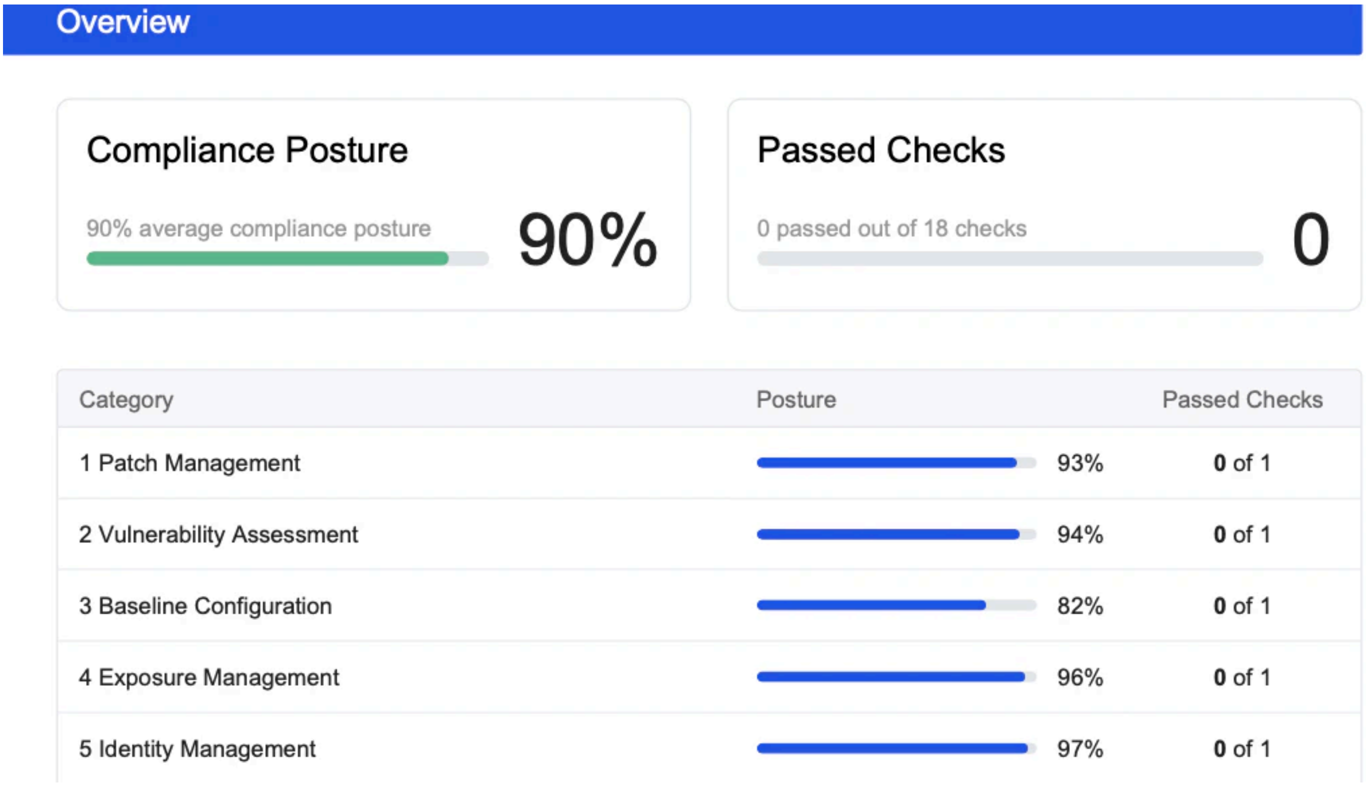
Policy	Resource Type	Resources		Compliance Posture	Result
Bucket anonymously or pub... Cloud Configuration Rule	Bucket Bucket	● 17	● 2	89%	Failed
Firewall should restrict MSS... Cloud Configuration Rule	Firewall Firewall	-		-	No Resources
S3 bucket should not be acc... Cloud Configuration Rule	aws S3 Bucket Bucket	● 55	● 4	93%	Failed
Publicly exposed container ... Control	Virtual Machine	● 334	● 0	100%	Passed
Network Security Group sho... Cloud Configuration Rule	Network Securit... Firewall	● 65	● 0	100%	Passed
Publicly exposed container i... Control	Secret Data	● 395	● 0	100%	Passed

Customize frameworks and controls to meet unique requirements

One size doesn't fit all, and some organizations have different regulations and standards they must comply with that are unique to them. For unique needs based on your organization's domain and best practices, you can define a custom compliance framework, where you can pick and choose which cloud security controls are needed for your organization to build a framework that reflects best your requirements. To give you further customization, you can also customize controls to check for unique use cases, both for cloud rules and host rules, and you can add those controls to a customized framework.

Create ongoing evidence records by generating granular compliance reports

Demonstrating compliance with your regulations can be a tedious process when done manually. With Wiz, you don't need to create manual reports anymore. 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 that can be as granular as a specific framework, business unit, or application or choose from a high-level PDF report to share with stakeholders or a detailed CSV report for the DevOps and GRC teams.



Overview

Compliance Posture

90% average compliance posture

90%

Passed Checks

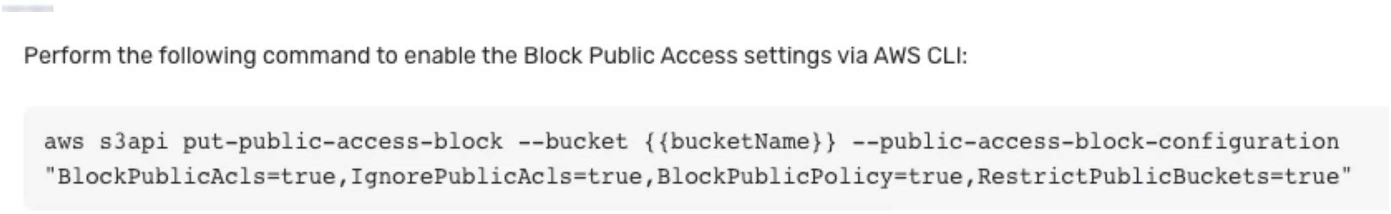
0 passed out of 18 checks

0

Category	Posture	Passed Checks
1 Patch Management	93%	**0** of 1
2 Vulnerability Assessment	94%	**0** of 1
3 Baseline Configuration	82%	**0** of 1
4 Exposure Management	96%	**0** of 1
5 Identity Management	97%	**0** of 1

Quickly remediate any issues with guidance and automatic remediation

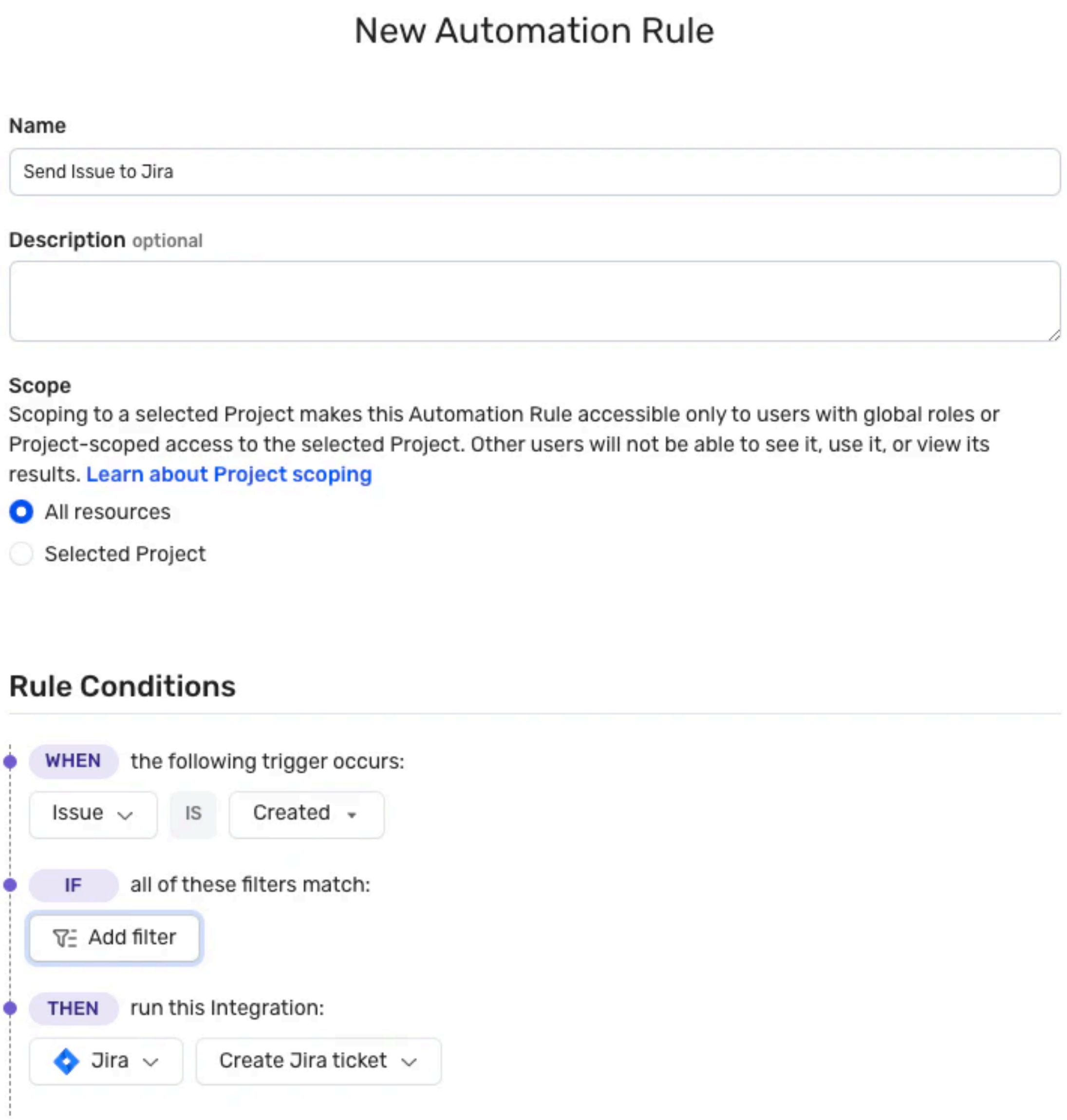
Once you identify the failing controls in your environment, it can be hard to know what the next step you need to take to address the failed checks. For any failed control in your environment, Wiz gives you specific remediation guidance so you can quickly respond to any issues. For example, to remediate the rule *S3 Bucket should have all 'Block Public Access' settings enabled,* Wiz provides the exact API call to make to resolve this issue:



Perform the following command to enable the Block Public Access settings via AWS CLI:

```
aws s3api put-public-access-block --bucket {{bucketName}} --public-access-block-configuration
"BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true"
```

If you would like to utilize the current tooling you have for ticketing or messaging, Wiz integrates with a wide variety of third-party tools so you can automate your responses to newly detected Issues. For example, you can send issues to your ticketing system, such as Jira or ServiceNow, to make sure alerts go to the right people and track progress in the same tools you use today.



New Automation Rule

Name

Send Issue to Jira

Description optional

Scope

Scoping to a selected Project makes this Automation Rule accessible only to users with global roles or Project-scoped access to the selected Project. Other users will not be able to see it, use it, or view its results. Learn about Project scoping

● All resources

○ Selected Project

Rule Conditions

WHEN the following trigger occurs:

Issue IS Created

IF all of these filters match:

Add filter

THEN run this Integration:

Jira Create Jira ticket

You can also set up auto-remediation to run in your environment and remediate specific misconfigurations using playbooks. Wiz has built-in playbooks for some of the misconfiguration rules that can be deployed in your account, and you can also create custom playbooks for specific use cases such as remediating misconfigurations on un-encrypted resources using your own keys.

Staying compliant on the cloud has never been so easy, get started now to see how Wiz can help you simplify compliance. You can learn more in the [Wiz docs](#) (login required). If you prefer a [live demo](#), we would love to connect with you.