DSPM: Discover and protect your data in the cloud

According to Wiz research, data exposure risk is shockingly common. 47% of companies have at least one database or storage bucket exposed to the internet (either PaaS or hosted). Over 20% of those cloud environments have buckets containing sensitive data. Securing cloud data challenging. Organizations often leverage siloed data security tooling that is complex and often ineffective. They lack context, require manual effort, and often miss complex risks involving vulnerabilities and lateral movement.

Wiz Data Security Posture Management (DSPM) enables customers to get ahead of the data exposure problem with a comprehensive platform that understands data risks at the cloud scale. Customers can continuously monitor data exposure before it becomes a costly breach and arm their teams with all the context, they need to remediate issues. Wiz breaks down silos between cloud security, data governance, and development teams, organizations drive significant productivity gains by reducing friction and the ability to collaborate seamlessly.

Scan everything agentlessly

Wiz scans public and private buckets, data volumes, and databases, and accurately classifies sensitive data such as PCI, PHI, and PII as well as data that's unique to your business. Best of all, we do this without using any agents or network scanners.

Fix what matters

Wiz conducts a deep cloud analysis that automatically correlates data risks with other cloud risks to build a single prioritized queue of attack paths and toxic combinations of risk to reduce noise and focus teams on what is important.

Build bridges across teams

Wiz-cli integrates with the development pipeline to block deployments that violate security policies and that open data exposure attack paths.

A unified approach to cloud security

- ✓ Security Posture Management (CSPM/KSPM)
- ✓ Workload Protection (CWPP)
- ✓ Vulnerability management
- ✓ Infrastructure Entitlement Management (CIEM)
- ✓ CI/CD security (IaC, VM/container image, registry scanning)
- ✓ Cloud detection and response (CDR)
- ✓ Container and Kubernetes Security
- ✓ Data Security Posture Management (DSPM)

Wiz provides coverage for

AWS Azure GCP

Trusted by organizations worldwide

"We are not the data governance team, but we want to proactively protect our data in the cloud. The visibility that Wiz gives us into our data and how it maps to external exposure is key as we don't want to be in the news."

- Cory Zaner | Cloud Security Manager, Chevron Phillips

"Pairing engineers who understand the risks with the tools to remediate them is incredibly powerful. There are 10X as many environment owners, developers, and engineers using Wiz than there are security team members at FOX. This helps us to ensure that the products shipped across over 1,000 technologists across the company have security baked in, which is beyond the impact that a small and mighty cybersecurity team can have alone."

- Melody Hildebrant | CISO, Fox

"Choosing Wiz was a no-brainer — no other tool comes even close. I'm convinced that Wiz is the most friction-free way of running cloud security."

- Adam Schoeman | Interim CISO, Copper

Prioritize and stop attack paths targeting your most critical cloud data

Wiz Data Security Posture Management helps organizations discover which data is stored where, who can access what data, how data assets are configured and utilized across Identities, and how data moves across environments. Wiz now detects data such as PII, PHI, and PCI and adds this as a new risk factor to the Wiz Security Graph to enable:

Rapid, agentless visibility into critical data: Wiz scans public and private buckets, data volumes, and both hosted and managed databases and accurately classifies the data so organizations can easily answer the question of what data is located where.

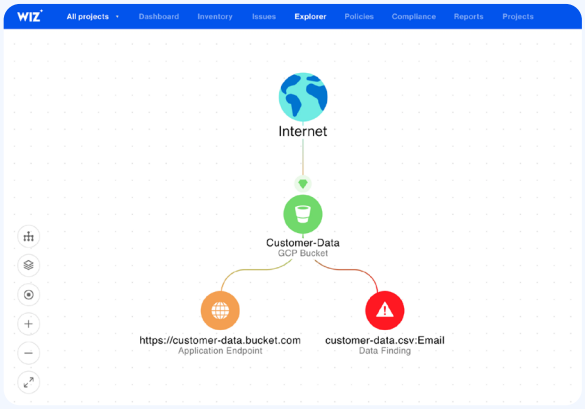
Continuous detection and prioritization of critical data exposure: Wiz conducts a deep cloud analysis that automatically correlates data risks with other cloud risks to build a single prioritized queue of attack paths and toxic combinations of risk to reduce noise and focus teams on what is important.

Identification of data lineage: Wiz uses schema matching across the entire environment to understand data flow and lineage, including when data is moved between environments or regions and improper storage of production data.

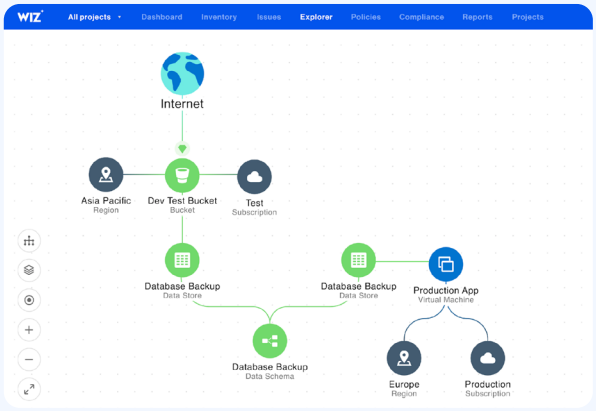
Automated compliance assessments: Wiz continuously assesses compliance to ensure security standards are consistently enforced across business units, regions, applications, and users.

Data exposure prevention: Wiz-cli integrates with the development pipeline to block deployments that violate security policies and that open data exposure attack paths.

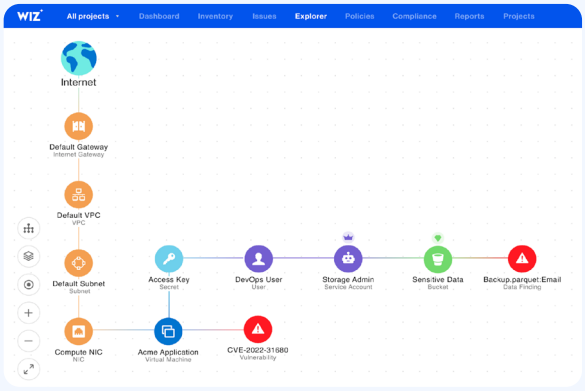
Integration with data security technologies: Wiz integrates with third party services like BigID and native tools like Amazon Macie to provide even more data context for risk prioritization and decision-making.



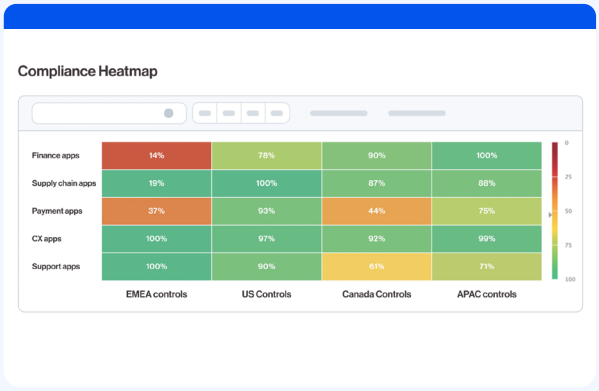
Wiz Security Graph visualization of a publicly exposed bucket containing customer emails



Wiz Security Graph visualization of a data flow where a database backup has been copied between test and production environments.



Wiz Security Graph visualization of a publicly exposed virtual machine with a critical vulnerability and lateral movement path to a bucket containing critical data.



Compliance heatmap assessing custom regional security standards across different business unit applications.

About Wiz

Wiz is on a mission to help every organization rapidly identify and remove critical risks in their cloud environments. Purpose-built for the cloud, Wiz delivers full stack visibility, accurate risk prioritization, and enhanced business agility. Wiz connects in minutes, using an agentless approach that scans both platform configurations and inside every workload. We perform a deep assessment that goes beyond what standalone CSPM and CWPP tools offer and find the toxic combination of flaws that represent real risk. Security, DevOps, and development teams then use Wiz's remediation workflow to proactively remove risks to harden cloud environments against attack. For more information, visit **www.wiz.io**.