

[← Blog](#)

Wiz becomes the first CNAPP to deliver integrated Data Security Posture Management

Wiz expands its platform to proactively eliminate attack paths to discovered critical data.



George Pisha

November 21, 2022

4 minute read



“Wiz alerts us with laser precision and all the context needed to take fast proactive action to **prevent issues** from becoming data breaches.”

Asonye Onwudebe

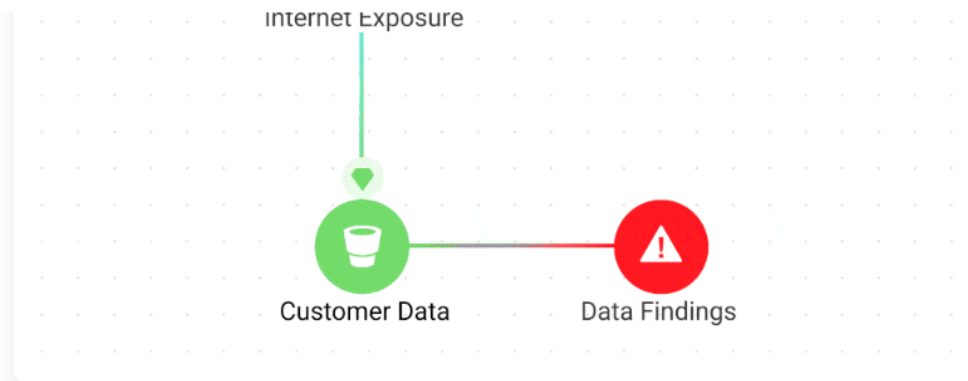
Cloud Security Architect, Chevron Phillips



When it comes to mission-critical data in the cloud era, exposure can become an incident in hours. [Research](#) has shown that an unsecured database can be breached in 8 hours flat. That's why we're excited to launch our new Data Security Posture Management (DSPM) capabilities to continuously monitor for critical data exposure so organizations can respond before a breach occurs. Our new features include visibility into PII, PHI, and PCI data; any exposure paths to that critical data that can be exploited; and how those exposure paths came to be. [DSPM](#) enables customers to proactively protect their cloud data, dramatically reducing the time it takes to discover and fix data exposure.

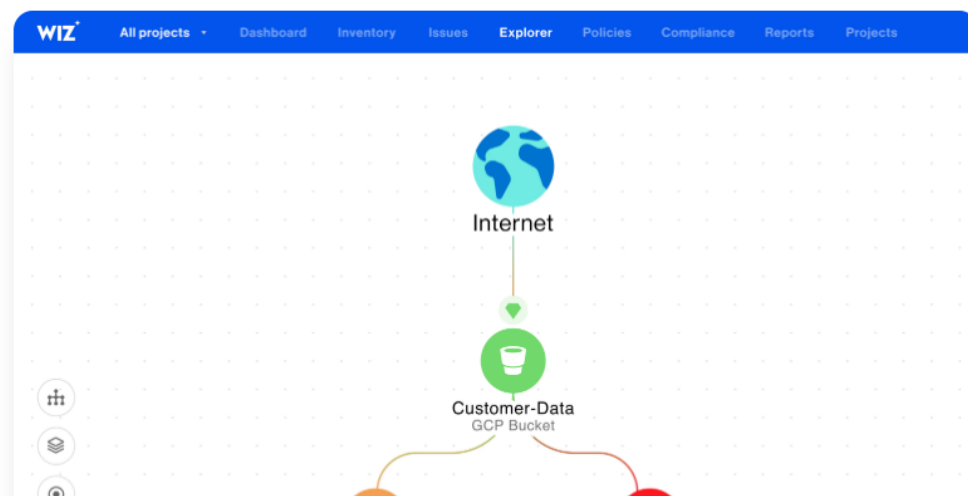


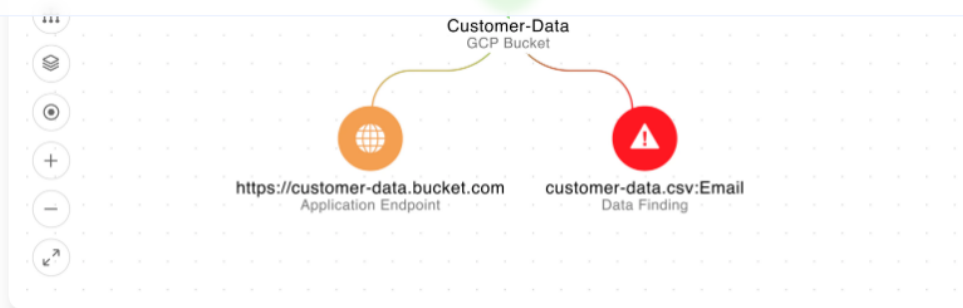
Orca Security Ltd.
Exhibit 2155
Wiz v. Orca
IPR2024-01190
Ex. 2155-001



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) of which over 20% of those cloud environments with publicly accessible buckets have buckets that contain sensitive data. Data leaks are reported in the news every week. Just recently in October 2022, Microsoft **reported** that a misconfiguration led to the exposure of tens of thousands of customer records. Attackers are aware of the value of sensitive data and the increasing difficulties in securing it. They continuously scan the internet for exposed databases and buckets. With the average cost of a data breach now over \$5 million, according to IBM's Cost of a data breach report 2022, eliminating this risk should be a top priority.

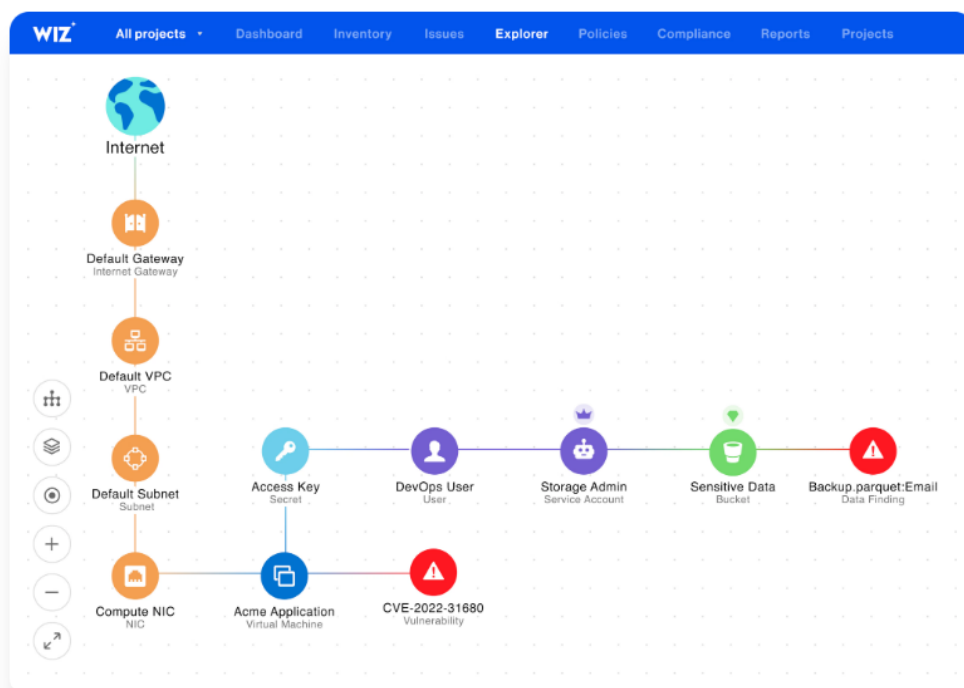
However, securing cloud data is a difficult problem. An organization with hundreds of data assets and tens of thousands of data items could have millions of individual configurations, permissions, and lifecycle policies to manage—this is far from a human-scale problem. Protecting a database from just simple network exposure is a complex problem that shows the limitations of taking siloed approaches to understanding cloud data risks. Traditional siloed tools don't capture the full picture when it comes to exposure and they completely miss complex risks that involve vulnerabilities and lateral movement. You would need many siloed tools that lack context and manual correlation across data and cloud to detect attack paths to critical data as they form. Wiz DSPM enables customers to get ahead of the data exposure problem with a comprehensive platform that understands data risks at cloud scale.





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

One such customer is Chevron Phillips Chemical Company, which uses Wiz to discover and protect mission-critical data. For Cory Zaner, Cloud Security Manager, "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." Asonye Onwudebe, Cloud Security Architect, explains further, "Wiz is our early warning system for critical data risks. Wiz alerts us with laser precision and all the context needed to take fast proactive action to prevent issues from becoming data breaches."



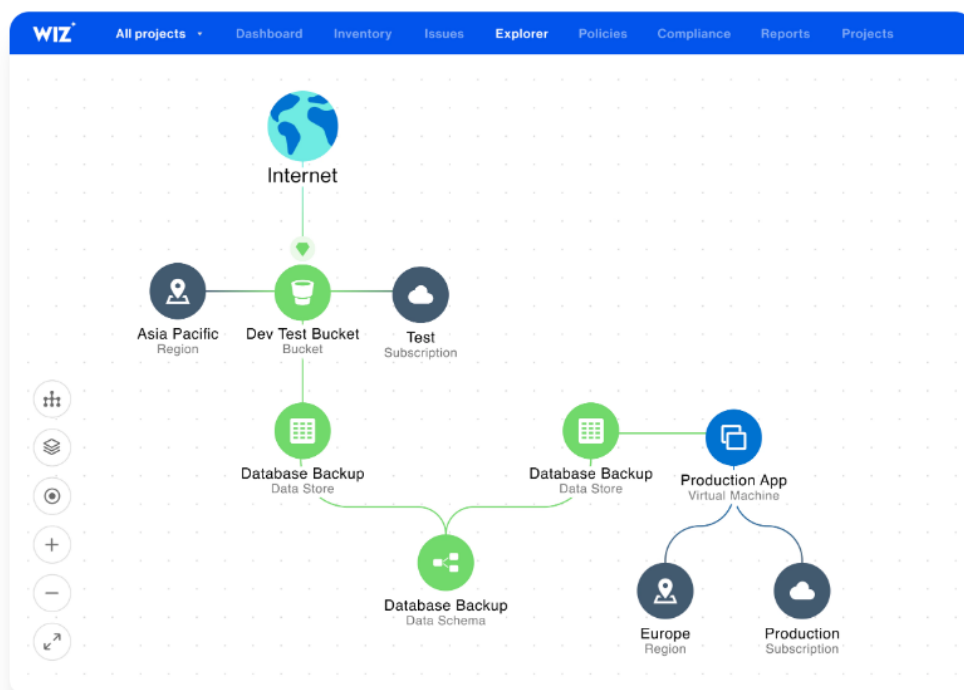
Wiz Security Graph visualization of a publicly exposed virtual machine with a critical vulnerability and lateral movement path to a bucket containing critical data.

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 human and non-human 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:

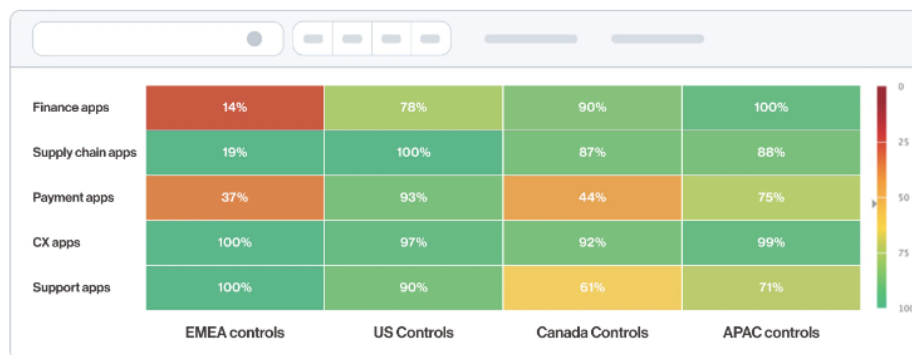
human and non-human identities, and how data moves across environments. Wiz now detects data such as PII, PHI, and PCI and adds this as a new risk factor to the Wiz Security Graph to enable:

- **Rapid, agentless visibility into critical data:** Wiz scans public buckets (AWS, GCP, and Azure), data volumes, RDS, Azure SQL, and Google SQL and 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 for 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 data flow where a database backup has been copied between test and production environments.

Compliance Heatmap



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

Wiz is extending its cloud-native application protection platform (**CNAPP**) with integrated data security posture management (DSPM) capabilities to detect cloud data exposure and prevent data breaches. Customers can now continuously monitor for data exposure before it becomes a costly breach and arm their teams with all the context they need to remediate issues. Wiz improves data security posture efficiently and allows teams to focus on prevention. This lowers the risk of a financial impact due to exposure or leakage of critical data. And, by breaking down silos between cloud security, data governance, and development teams, organizations drive significant productivity gains from reducing friction and the ability to seamlessly collaborate. This is one of the many ways in which Wiz helps its customers transform their **cloud operating model**. Today, our DSPM capabilities are in public preview and available for Wiz customers to begin using.

To learn more about Wiz and how you can proactively protect your mission-critical data, [contact us](#) to see a demo.



Tags

#Product & Company News

#Product

Continue reading



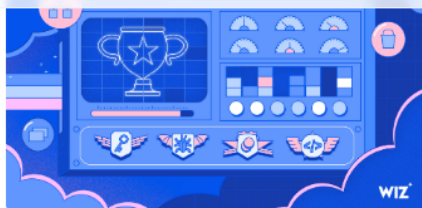


Wiz to acquire Dazz, transforming risk remediation from cloud to code



Assaf Rappaport
November 21, 2024

Together, we'll reinvent ASPM and code-to-cloud remediation.



Introducing The Champion Center: Operationalize and Measure Cloud Security Maturity Across Your Organization



Swaroop Sham, Shashank
Golla, Eden Naftali
November 20, 2024

Centralize security insights, scale adoption,
and demonstrate measurable cloud security
progress with Wiz



Wiz Remediation and Response – Now available for Azure and GCP environments



Swaroop Sham, Itay Arbel,
Chris Beckett
November 21, 2024

Powerful new remediation and response
capabilities enable the real-time
enforcement of organizational security...

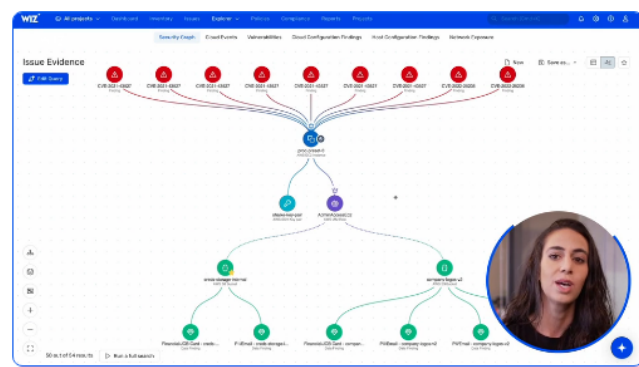
GET A PERSONALIZED DEMO

Ready to see Wiz in action?

“Best User Experience I have ever seen,
provides full visibility to cloud workloads.”



David Estlick
CISO of Texas and Vulnerability Management



Get a demo >



PLATFORM

Wiz CNAPP

Wiz Code

Wiz Cloud

Wiz Defend

Integrations

Environments

Documentation

LEARN

Customer stories

Train Your Team For Cloud

Blog

CloudSec Academy

Resources Center

Cloud threat landscape

Cloud Security Assessment

COMPANY

About Wiz

Join the team

Newsroom

Events

Contact us

Trust Center

Our partners

English (US) >



Get a demo >



PLATFORM

[Wiz CNAPP](#)[Wiz Code](#)[Wiz Cloud](#)[Wiz Defend](#)[Integrations](#)[Environments](#)[Documentation](#)

LEARN

[Customer stories](#)[Train Your Team For Cloud](#)[Blog](#)[CloudSec Academy](#)[Resources Center](#)[Cloud threat landscape](#)[Cloud Security Assessment](#)

COMPANY

[About Wiz](#)[Join the team](#)[Newsroom](#)[Events](#)[Contact us](#)[Trust Center](#)[Our partners](#)[English \(US\)](#) ▾

© 2025 Wiz, Inc.

[Status](#)[Privacy Policy](#)[Your California Privacy Rights](#)[Terms of Use](#)[Modern Slavery Statement](#)[Do Not Sell or Share My Personal Information](#)