WIZ

The Cloud Visibility Playbook: 10 Practices to Secure Cloud Environments

Checklist included!

Cloud computing brings complex security challenges, particularly for organizations new to this paradigm. One critical concern is achieving comprehensive cloud visibility, with traditional security approaches proving inadequate. With cloud environments in a constant state of flux, leveraging cloud-native security tools has become imperative for effective visibility and threat management.

In this playbook, we will examine the primary challenges associated with limited cloud visibility, explain the benefits of achieving comprehensive visibility, and detail cloud visibility best practices with actionable insights to bolster your organization's cloud security posture.

Challenges of limited cloud visibility

Traditional security methodologies often rely on perimeter-based defenses and static infrastructure assumptions. The resulting gaps in cloud visibility present several significant areas of concern:

- **Unnoticed critical risks:** Some 76% of respondents to a **Palo Alto Networks survey** said their cloud security tools create blind spots. Without adequate visibility, organizations may fail to detect critical risks and face security breaches.
- **Increased security risks:** Unidentified vulnerabilities and misconfigurations create an elevated risk profile. Misconfigured resources can lead to unauthorized access and sensitive data leaks.
- **Compliance difficulties:** Maintaining adherence to industry standards is challenging without complete visibility into your cloud environment. Compliance requires consistent monitoring and reporting, which is hindered by visibility gaps.
- **Ineffective resource allocation and risk prioritization:** Without clear insights, companies struggle with vulnerability prioritization, leading to inefficient use of resources and potential neglect of critical vulnerabilities.
- **Organizational silos:** Limited visibility often deepens organizational silos, preventing effective collaboration between cloud and security teams. This can result in cloud sprawl, where unmanaged and unmonitored resources proliferate.

The following table summarizes challenges with their impact and mitigation strategies.

Challenge	Impact	Mitigation strategy
Unnoticed critical risks	Potential security breaches	Agentless scanning for full coverage
Increased security risks	Elevated risk profile due to vulnerabilities	Regular vulnerability assessments
Compliance difficulties	Non-compliance with regulations	Centralized monitoring and reporting
Ineffective resource allocation	Wasted resources on low-priority issues	Risk-based vulnerability prioritization
Organizational silos	Inefficient collaboration	Cross-functional teams and shared tools

Benefits of gaining cloud visibility

The above issues highlight the need to adopt approaches designed to operate within highly dynamic environments and accommodate the unique characteristics of cloud infrastructures.

In contrast to traditional methods, cloud-native security utilizes automated processes and scalable solutions that are adaptable and can integrate seamlessly with cloud services. This enables companies to achieve comprehensive cloud visibility, delivering the following benefits:

- **Enhanced security posture:** Visibility allows organizations to identify risks and mitigate vulnerabilities proactively: "You can't secure what you can't see."
- **Centralized monitoring and compliance:** Facilitating centralized monitoring aids in maintaining compliance with regulatory frameworks. It ensures that security policies are uniformly enforced across all cloud services.
- **Effective risk-based prioritization:** With complete visibility, organizations can perform accurate vulnerability prioritization, focusing on issues that pose the most significant risk to business operations.
- **Data protection:** Visibility into where sensitive data resides and who can access it is crucial for implementing appropriate safeguards.
- **Operational efficiency:** Streamlined processes and automation result from comprehensive visibility, leading to increased operational efficiency.
- **Improved incident response:** Enhanced insights enable faster incident response times, meaning less potential damage.

10 best practices for cloud visibility

1 Agentless tracking of cloud inventory

Maintaining an up-to-date inventory of all cloud resources is essential. Agentless scanning ensures zero blind spots, enabling detection of all technologies running on virtual machines (VMs), containers, and serverless environments.

Actionable items

- Utilize cloud provider APIs for real-time resource discovery.
- Employ tools that support agentless scanning to avoid performance overhead.
- Ensure the accuracy of your inventory with regular audits.

2 Centralized monitoring

Centralized monitoring across multi-cloud environments delivers a unified view of your entire infrastructure. A "single pane of glass" approach simplifies management and enhances security oversight.

Actionable items

- Integrate cloud services into centralized logging and monitoring systems.
- Use dashboards to visualize key metrics and alerts.
- Standardize monitoring tools across different cloud platforms.

3 Configuration management

Tracking and managing the configuration of cloud resources is vital for security. Automated configuration checks can detect deviations from best practices.

Actionable items

- Implement configuration management tools that integrate with CI/CD pipelines.
- Define and enforce consistent policies for all your cloud environments.
- Regularly review and update configuration baselines.

4 Container visibility

Containers introduce additional layers of abstraction, necessitating specific strategies for visibility.

Actionable items

- Employ container security tools that scan images and monitor runtime behavior.
- Integrate security checks into the container development lifecycle.
- Monitor container orchestration platforms for unauthorized activities.

5 Vulnerability management

Companies must establish vulnerability management strategies tailored to cloud environments. You must also adopt scanning methodologies that facilitate extensive vulnerability coverage across cloud environments.

Actionable items

- Schedule regular vulnerability scans using cloud-native tools.
- Prioritize vulnerabilities based on contextual risk assessments.
- Integrate vulnerability data into a centralized management system.

6 Visibility into access and permissions

Establishing role-based access control (RBAC) and implementing the principle of least privilege minimizes risks associated with excessive permissions.

Actionable items

- Audit all identities, including human and non-human, for effective permissions.
- Monitor identity providers (IdPs) such as Okta for unusual activities.
- Assess SaaS applications, e.g., Snowflake or OpenAI, that interact with your cloud environment.

7 Data and AI security

Protecting sensitive data requires understanding its location, access permissions, and exposure levels. Securing AI models and pipelines is equally essential.

Actionable items

- Implement continuous data discovery classification.
- Monitor for data risks and correlate them back to cloud context to find attack paths to critical data.
- Ensure data encryption.
- Watch out for anomalies in data access patterns.
- Secure AI development workflows by implementing continuous inventory of all training data and models and risk assessments in AI pipelines.

8 Using cloud-native security platforms

Cloud-native tools are designed to address the complexities of cloud environments, offering advantages over legacy on-premises solutions.

Actionable items

- Use tools like Wiz to gain comprehensive visibility into cloud risks.
- Employ security platforms that correlate misconfigurations, vulnerabilities, identities, secrets, and data exposures to identify critical attack paths.
- Focus on detecting and mitigating complex cloud-native attack paths with graph-based context.

9 Cloud and risk mapping on a security graph

A security graph helps visualize the relationships between resources and risks, enhancing understanding of context around risks. A graph can analyze complex relationships to accurately detect cloud-native and complex attack paths.

Actionable items

- Use a security graph to map cloud assets and their interdependencies.
- Identify potential attack vectors through tools such as the Wiz Security Graph.
- Prioritize the most critical attack paths with context on the graph.

10 Monitoring for real-time threats

Real-time monitoring detects unusual activities promptly. However, make sure to have an incident response plan in place that caters to cloud-specific scenarios.

Actionable items

- Implement cloud-native monitoring solutions that analyze events and runtime activities.
- Conduct regular incident response drills.
- Establish automated alerting mechanisms for critical events.

Checklist: Cloud visibility best practices

- **Agentless cloud inventory tracking:** Ensure comprehensive resource detection without performance impact.
- **Centralized monitoring:** Consolidate monitoring tools and dashboards.
- **Configuration management:** Automate configuration checks and integrate with CI/CD pipelines.
- **Container visibility:** Secure container images and monitor runtime behavior.
- **Vulnerability management:** Utilize agentless scanning and prioritize vulnerabilities contextually.
- **Access and permissions visibility:** Implement RBAC and the principle of least privilege.
- **Data and AI security:** Protect sensitive data and secure AI pipelines.
- **Security graph mapping:** Visualize relationships between resources and risks.
- **Real-time threat monitoring:** Develop incident response plans and monitor cloud events.

Use case: How Bridgewater achieved zero critical issues in their cloud environment

Bridgewater's approach to achieving zero critical issues in its cloud environment highlights how collaborative efforts, clear risk guidelines, and shared responsibilities contribute to a robust security framework.

Bridgewater's security and IT teams jointly established an internal risk framework to identify and mitigate critical risks. This framework defines precise guidelines to qualify an issue as critical, such as external exposures or over-permissioned identities. Every two weeks, the teams meet to review and refine these guidelines, ensuring they stay relevant to evolving cloud threats. This regular cadence of reviews allows the team to maintain alignment on risk thresholds and address emerging threats swiftly.

Furthermore, instead of categorizing issues as "low-risk" versus "high-risk," any issue meeting its predefined criteria is treated as a verified critical issue and must be remediated within a designated service level agreement (SLA). This approach ensures that no vulnerabilities are overlooked due to subjective risk scoring.

To reinforce accountability, Bridgewater provides all teams with access to **Wiz.** By integrating the Wiz platform across their teams, Bridgewater enhances overall visibility and enables each team to contribute to maintaining a secure cloud environment. This empowers their teams to identify and remediate critical issues within their domain, promoting a culture of shared responsibility, where security is a collective goal rather than a siloed function.

Conclusion

By adopting best practices, such as those demonstrated in Bridgewater's framework, and leveraging tools like Wiz, organizations can navigate cloud security complexities with greater confidence. Emphasizing cloud visibility, proactive risk management, and cross-functional collaboration fosters a resilient and secure cloud environment.

Explore how Wiz can help your organization achieve complete cloud visibility and strengthen your security posture. **Request a Wiz demo today.**