WIZ Microsoft

Security at the speed of development with Wiz and Microsoft Azure

The rapid adoption of cloud-native development across industries has transformed the speed and scale of business innovation. It has also introduced complex security challenges.

Modernizing development with cloud-based AI has helped organizations increase productivity to better serve their employees, partners, and customers. However, security teams need help keeping up with the speed of development teams using new AI technologies.

To address these challenges, security leaders must move from a traditional reactive approach to threats to a proactive, integrated approach that ensures maximum productivity without compromising safety.

The intersection between AI development and cloud security is critical, and organizations do not need to manage this alone. Wiz and Microsoft offer a solution to help organizations achieve this balance. The partners make building and deploying secure AI applications in Microsoft Azure easy, using Wiz's security platform and AI Security Posture Management (AI-SPM) services.

With Wiz and Microsoft, companies can innovate confidently with security built into every stage of the AI pipeline.

The intersection between AI development and cloud security is critical to address, and organizations do not need to manage this alone.

70%+

of organizations use managed AI services

39%

of organizations that implement managed services use Microsoft's Azure AI Services

53%

of cloud environments have OpenAI and Azure OpenAI SDKs

228%

is the growth of deployed Azure OpenAI instances in 2023

Wiz State Of AI In The Cloud Report 2024

Operational challenges facing security teams

Lack of visibility

Generative AI increases development speed, causing security teams to lose visibility across workloads, containers, APIs, and serverless functions. Teams need unified tools to have comprehensive visibility into undetected vulnerabilities, misconfigurations, or exposed assets that attackers might exploit.

Alert fatigue

Traditional security tools generate a flood of alerts, many of which need more context or are low-priority. This lack of context creates alert fatigue, where security teams struggle to identify and act on the most critical risks in a sea of notifications.

Development workflows

The fast-paced nature of DevOps workflows can put security teams at odds with developers. Developers often see security controls as roadblocks hindering their ability to code and ship features quickly. Conversely, security teams frequently struggle to insert themselves into the DevOps process without causing friction. This lack of alignment and collaboration increases the risk of vulnerabilities slipping through undetected.

Complex hybrid and multi-cloud environments

A multi-cloud or hybrid strategy helps organizations get the most out of their tools. This approach provides flexibility but increases the complexity of consistently managing security across environments. Security teams must oversee varying tools, configurations, and compliance requirements across platforms, which can lead to inconsistencies and inefficiencies.

Outdated processes
Traditional security strategies tend to focus on reactive measures, which are ineffective against the speed and scale of development in AI environments. Without security guardrails or proactive strategies, misconfigurations and vulnerabilities can make their way into production and increase the risk of breaches.

Emerging threats
As cloud adoption accelerates, attackers develop new techniques to exploit cloud environments and tap into pipeline vulnerabilities, such as misconfigured services and over-privileged accounts. Security teams must keep pace with these emerging threats by continuously learning and adapting on top of their existing workloads.

Resource constraints
Staffing skilled security teams due to an ongoing talent shortage, lack of budget, or both is an ongoing challenge for many organizations. As teams are stretched thinner, the workload—and the cyber threats—continue to grow.

Regulatory compliance
An increasing number of regulations and governance policies impact cloud environments. Without automated compliance tools, organizations may face significant legal and financial issues due to their inability to adhere to regulatory requirements.

Addressing these challenges requires solutions designed specifically for the cloud. These solutions must prioritize visibility, collaboration, and automation—enabling teams to scale security at the speed of development.

The pillars of effective security in cloud and AI environments

AI's surging use impacts how organizations secure their cloud environments. To address the security challenges AI environments and emerging threats pose, organizations must implement strategies and tools to secure data and workloads—without slowing innovation.

Here's how organizations can tackle these security challenges:

Achieve comprehensive visibility

Visibility is the cornerstone of effective cloud security. Companies need tools that provide a unified view of their cloud environments, spanning all AI, workloads, containers, APIs, and other resources.

This requires:

Agentless integrations with cloud platforms

Tools that map interdependencies between resources

Real-time dashboards and analytics to monitor changes and maintain situational awareness

With deeper insights into their infrastructure, security teams can address vulnerabilities before attackers attempt to exploit them.

Shift-left security

Embedding security early in the AI development lifecycle (known as "shift-left" security) ensures vulnerabilities are identified and mitigated during the design and build phases.

Security teams must integrate automated security checks into CI/CD pipelines to catch misconfigurations before deployment. They must also enforce guardrails that prevent developers from creating risky configurations.

Shift-left security helps organizations take a proactive security stance to reduce the likelihood of introducing vulnerabilities into production. This approach saves time and resources while improving the organization's security posture.

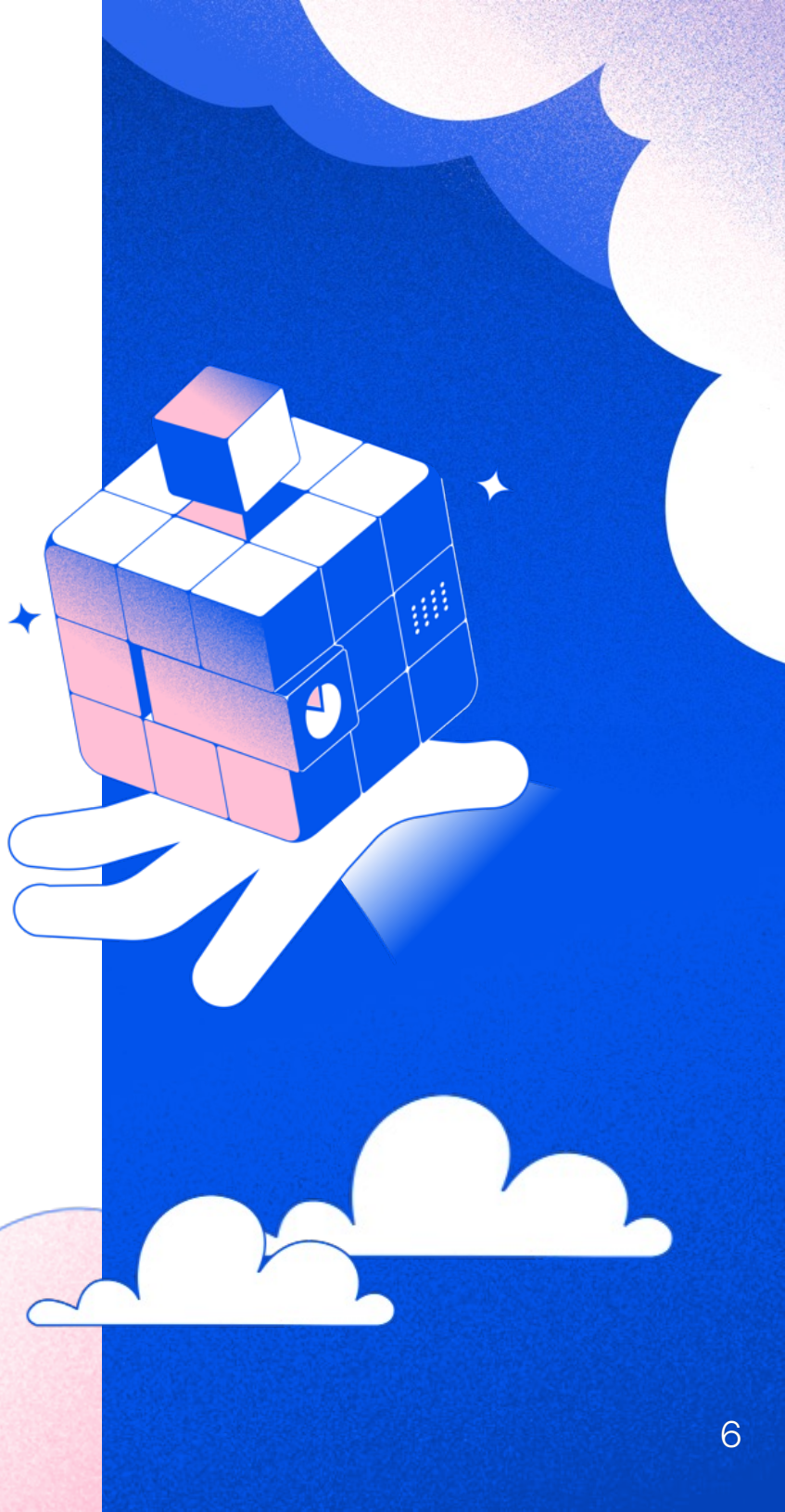
Automate repetitive tasks

Automation is critical for scaling security in AI environments. Organizations need automated solutions to triage and prioritize alerts, helping security teams focus on high-risk issues.

In addition, they need AI-driven tools to:

- **Analyze vast amounts of telemetry data**
- **Surface meaningful threats**
- **Execute automated workflows to patch vulnerabilities, roll back misconfigurations, and maintain compliance**

With these automations, teams can concentrate on more strategic activities, such as threat hunting and process improvement.



Create a culture of collaboration

Improving securing posture in the cloud and with AI relies on close alignment between development and security teams to reduce friction and accelerate issue resolution.

Organizations can create this culture of collaboration by:

- Using shared tools and platforms that integrate seamlessly with DevOps processes
- Establishing clear roles and responsibilities between teams to eliminate silos
- Offering training to ensure developers understand security requirements and best practices

This collaborative approach ensures security is treated as a shared responsibility, leading to faster and more effective risk mitigation.

Adopt context-driven threat management

Legacy security tools can overwhelm teams with alerts, many of which lack actionable context. To overcome this, companies need tools specifically designed for cloud security.

A comprehensive solution should be able to correlate alerts with real-world risks, visualize attack paths to high-value assets, and provide context-rich recommendations to help teams quickly address critical vulnerabilities.

Expert providers enable teams to manage identity, access, and compliance at scale. This expertise integrates with provider APIs and provides teams with ongoing support and intelligence.

By partnering with trusted security providers to implement a secure-by-design strategy, organizations can create a robust security foundation for their AI initiatives. This strategy will minimize risks, fuel innovation, and allow developers to confidently explore the power of AI within cloud environments.

Top drivers for organizations to incorporate security processes into development

73%

want to establish a more proactive cybersecurity posture

71%

need cybersecurity to keep pace with the continuous development of new code

57%

want more collaboration between cybersecurity, development, and operations teams

52%

seek greater operational efficiencies via automation

45%

need to meet and maintain compliance with industry regulations

Wiz's approach to cloud-native security

Wiz is purpose-built to secure cloud-native environments. Its platform offers unmatched visibility and insights to help organizations stay ahead of threats. Wiz's unique security approach focuses on three core principles:

See and secure everything

Achieve full-stack visibility across cloud-native environments. Organizations get a comprehensive map of workloads and their connections by gathering telemetry from virtual machines, containers, serverless functions, and APIs.

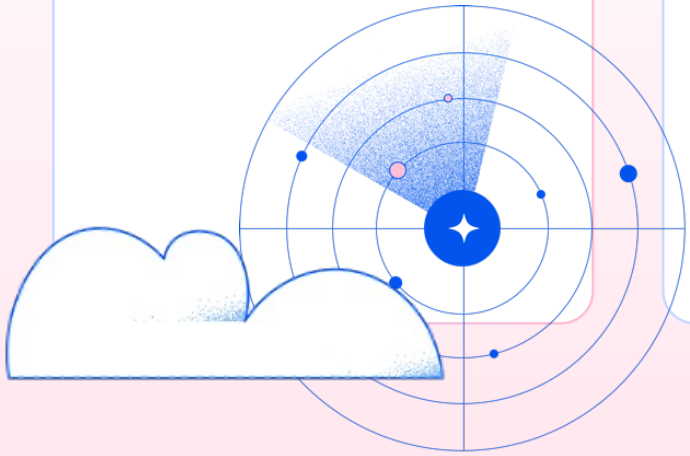
Organizations use this unified view to:

- Eliminate visibility gaps in cloud environments
- Assess the potential impact of vulnerabilities based on attack paths
- Monitor access permissions

Get threat detection with context

Wiz uses graph-based threat modeling to contextualize risks and prioritize issues. This context helps teams:

- Highlight critical vulnerabilities within complex workloads
- Map attack paths
- Integrate findings into developer workflows to streamline remediation



Automate for greater efficiency

Wiz automates manual and time-consuming tasks so security teams can focus on resolving threats.

Teams auto-prioritize alerts based on severity and business impact. Auto-prioritization helps teams implement proactive policies that:

- Prevent misconfigurations during development
- Reduce response times
- Integrate with DevOps tools for seamless workflows

Microsoft's comprehensive cloud security features

Microsoft Azure offers a robust, multi-layered security framework that protects workloads and data in highly dynamic cloud environments. With its suite of integrated tools, Microsoft helps organizations innovate freely—and with a strong security posture.

Built-in cloud security
Microsoft offers several security features to help organizations monitor, detect, and respond to threats. The cloud-native SIEM solution Microsoft Sentinel uses intelligent analytics to detect threats and automate responses. This built-in security allows organizations to respond quickly to incidents and significantly reduce resolution times.

Support development teams
Microsoft's cloud infrastructure is designed for scalability. It integrates seamlessly with modern DevOps workflows to improve collaboration and efficiency.

Microsoft Azure DevOps embeds security checks directly into the CI/CD pipelines, ensuring vulnerabilities and misconfigurations are identified and addressed early in the software development lifecycle. By automating these processes, Microsoft helps organizations "shift-left" with their security, mitigate risks before they reach production, and reduce costly rework or delays.

Improve cross-team collaboration
Microsoft's tools are designed to enhance cloud security and promote collaboration between traditionally siloed teams. By embedding security into development workflows and providing shared platforms for monitoring and issue resolution, Microsoft helps security teams align with developers to address risks earlier and more efficiently. This alignment ensures security keeps pace with continuous development without introducing unnecessary risk.

Wiz and Microsoft bridge the gap between AI development and security

Organizations implementing cloud services such as Microsoft Azure to quickly release applications need a practical security approach to manage security risk.

Wiz and Microsoft combine cloud environment and workload telemetry, giving organizations a comprehensive solution for understanding risk exposure and proactively reducing attacks.

Together, Wiz and Microsoft address the complex security challenges of modern cloud-native development while enabling businesses to explore the potential of Open AI.

Wiz enhances Microsoft's security capabilities

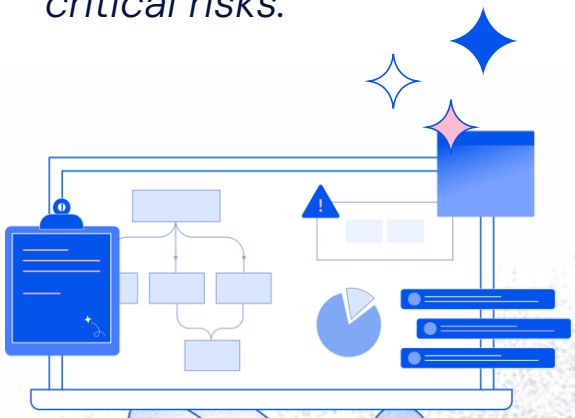
Wiz and Microsoft help companies maximize their existing Microsoft Azure investments, streamline workflows, and improve their security posture in the face of emerging threats.

By providing an additional layer of visibility and protection through agentless integration with Microsoft Azure APIs, Wiz automatically discovers and maps all AI resources, technologies, and dependencies. This comprehensive view of the cloud ecosystem helps organizations eliminate visibility gaps and understand relationships between components, data flows, and potential attack paths.

Teams also uncover misconfigurations and vulnerabilities to identify high-risk scenarios that may lead to breaches. This identification simplifies the prioritization of remediation efforts.

Wiz brings contextualized threat intelligence to Microsoft Azure environments, providing actionable insights that allow security teams to focus on the most critical risks. By integrating seamlessly with Microsoft's security ecosystem, including Microsoft Defender for Cloud, Wiz simplifies security operations and improves information sharing.

Wiz brings contextualized threat intelligence to Microsoft Azure environments, providing actionable insights that allow security teams to focus on the most critical risks.



Wiz helps accelerate Microsoft Azure AI adoption

Wiz enables organizations to adopt AI rapidly and securely by integrating advanced security measures that don't compromise speed or agility.

By partnering with Wiz and Microsoft, organizations can quickly secure their cloud and AI workflows without disrupting development processes or affecting application performance. With security built into early development stages, security teams can proactively identify risks and prevent vulnerabilities before AI applications reach production, reducing the likelihood of costly delays and incidents.

Wiz and Microsoft also provide compliance and governance tools that simplify compliance with regulatory standards. These tools provide real-time compliance assessments and guidance, helping businesses scale their operations securely while staying on the right side of regulations.

By partnering with Wiz and Microsoft, organizations secure their cloud workflows quickly without disrupting development processes or affecting application performance.

Wiz protects Microsoft Azure workloads:

- Get in-depth defense, including prevention, agentless visibility, and risk reduction
- Prioritize network and identity misconfigurations with a graph-based network and identity engine
- Get active detection and response with real-time monitoring
- Discover misconfigurations that compromise high-value assets

Wiz secures Microsoft Azure environments:

- Protect Microsoft Azure clouds in minutes with a 100% API-based solution
- Cover the entire cloud stack, including all VMs, containers, serverless, and PaaS
- Scan every Microsoft Azure layer without agents to detect vulnerabilities
- Model effective security posture by compiling all settings, compensating controls, and relationships

Wiz and Microsoft also provide compliance and governance tools that simplify compliance with regulatory standards. These tools provide real-time compliance assessments and guidance, helping businesses scale their operations securely while staying on the right side of regulations.

As organizations race to scale their cloud-native infrastructure and AI capabilities, the need for security and visibility across environments has never been more critical.

Wiz and Microsoft make it easy for customers to secure their cloud instances and stay protected while working with AI. Together, they help organizations proactively address and prevent threats while enabling secure innovation.

See how Wiz and Microsoft transform security

What can organizations expect when partnering with Wiz and Microsoft?

- **Eliminate** the overhead of deploying and managing agents
- **Reduce** manual efforts in identifying, correlating, and remediating separate risks
- **Speed up** remediation across security and development teams
- **Reduce** the costs of licensing, deployment, integration, training, and support of point-security tooling
- **Keep** development teams focused on building by eliminating unnecessary work
- **Improve** security workforce efficiency by rapidly identifying the latest threats
- **Eliminate** data visibility gaps and use contextual information to help security teams remediate high-risk issues

WIZ Microsoft