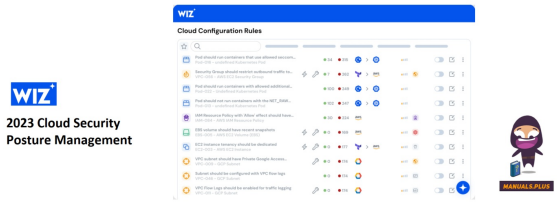
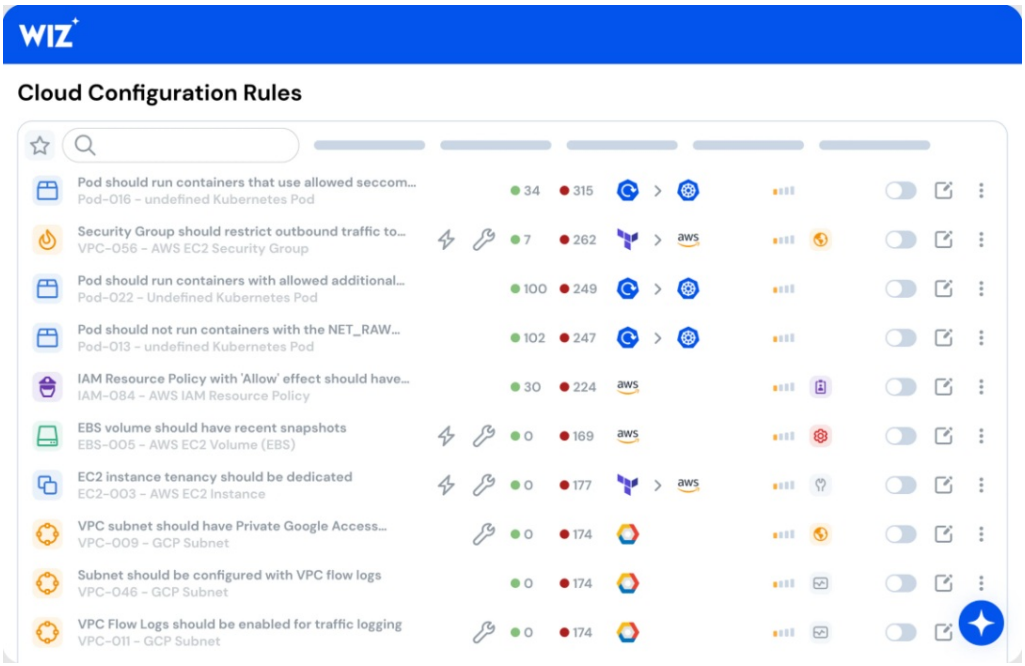


WIZ 2023 Cloud Security Posture Management User Guide

Contents

1 WIZ 2023 Cloud Security Posture Management
2 Product Information
3 Product Usage Instructions
4 FAQ
5 Intro to cloud security
6 The unique challenges of security in the cloud
7 What is Cloud Security Posture Management?
8 Key features of legacy CSPM tools
9 What gaps do legacy CSPM tools have?
10 How does a modern CSPM bridge the gaps of legacy CSPM?
10.1 Modern CSPMs include these additional capabilities to enrich the context of legacy CSPMs:
11 Legacy CSPM vs modern CSPM feature comparison
12 Key requirements of a comprehensive modern CSPM
13 Getting started with CSPM
14 Request for proposal template
15 About Wiz
16 Documents / Resources
16.1 References
17 Related Posts

WIZ 2023 Cloud Security Posture Management



Product Information

Specifications

- **Product Name:** Cloud Security Posture Management (CSPM) Tool
- **Function:** Manages cloud security risk and provides compliance assurance in the cloud
- **Purpose:** Helps organizations tackle security challenges in dynamic cloud environments
- **Market Availability:** Various CSPM tools available in the market

Product Usage Instructions

Introduction to Cloud Security

- More organizations are moving to the cloud for its benefits.
- Security needs have evolved due to dynamic cloud environments.
- Security strategies need to adapt to the fast nature of the cloud.

What is Cloud Security Posture Management (CSPM)?
CSPM continuously manages cloud security risk and ensures compliance in the cloud.

Key Features of Legacy CSPM Tool

- Provides basic security measures
- Limited visibility and control
- Manual compliance checks
- May not address modern security challenges effectively

How Does a Modern CSPM Bridge the Gaps of Legacy CSPM?

- Enhanced visibility and control

- Automated compliance checks
- Addresses modern security challenges efficiently
- Integrates with cloud-native technologies

Getting Started with CSPM

- Evaluate your organization’s security needs
- Research and compare different CSPM tools
- Implement the chosen CSPM tool in your cloud environment
- Regularly monitor and update security configurations

FAQ

- **What are the key requirements of a comprehensive modern CSPM?**
  A comprehensive modern CSPM should offer enhanced visibility, automated compliance checks, integration with cloud-native technologies, and effective management of modern security challenges.
- **How can I ensure successful cloud adoption with CSPM?**
  By selecting a suitable CSPM tool, regularly monitoring and updating security configurations, and ensuring collaboration between development and security teams, you can facilitate successful cloud adoption with CSPM.

Intro to cloud security

- The cloud offers organizations scalability, reliability, reduced costs, and increased performance, enabling them to move fast and innovate their business. Organizations can now scale up and down their infrastructure as they need, removing the overhead of buying and maintaining servers on-premises. Cloud service providers manage a scalable, reliable, and secure global infrastructure allowing organizations to focus on their core business and innovate at a much faster pace than they have ever been able before.
- More and more organizations are moving to the cloud to take advantage of its many benefits. The increase in the shift to the cloud has created a wide range of new security needs along with it. The rise of dynamic and ephemeral environments within the cloud has increased complexity and created unique and unpredictable interactions. As a result, security teams need to adjust their security strategies to adapt to the dynamic and fast nature of the cloud.
- Gartner has defined a new category of security tools called Cloud Security Posture Management (CSPM) to help organizations tackle these challenges. CSPM is a solution that continuously manages cloud security risk and provides compliance assurance in the cloud. With so many CSPM tools in the market, it can be challenging to choose the right tool for your unique requirements.
- This guide is intended to help you choose a comprehensive CSPM tool that is the best fit for your organization by examining the capabilities of legacy CSPM tools vs modern CSPM tools and identifying the key requirements that your comprehensive CSPM tool must have.

The unique challenges of security in the cloud

Security on the cloud is a shared responsibility

Many organizations assume their cloud service provider (CSP) is entirely responsible for their security. However, CSPs adhere to a shared responsibility model where security and compliance are shared between the CSP and the customer. The CSP is responsible for protecting the underlying infrastructure, including hardware, software, networking, and facilities that run the cloud services. Customers assume responsibility and management of their workloads,
applications, data, and secure resource configurations.

Cloud environments are complex

- Cloud environments are complex by nature. Customers run multiple compute types, from virtual machines to serverless and managed databases, and often have a multi-cloud environment. The dynamic nature of the cloud enables organizations to spin up new resources in the click of a button. With this new speed and scalability, organizations' cloud footprint grows in an extremely fast and dynamic manner. The more it grows, the more there is to protect, the more complex the environment gets, and the harder it is to manage the configurations of cloud resources at scale.
- With so many configurations and such complex environments, it becomes too time consuming for a human to manage and control the configurations of all the resources. This leads to a lack of visibility into everything running in the environment. Lack of visibility can result in misconfigurations going unnoticed for extended periods, and these misconfigurations can result in a breach.

Manual compliance
The increased complexity and scale of cloud environments creates new challenges of managing compliance at scale. Organizations need to ensure continuous compliance of their unique regulatory requirements across all their environments and their clouds and develop visibility and control into their new compliance processes. Traditional manual compliance processes cannot keep up with this scale, since cloud environments change so rapidly and require
a proactive continuous approach to compliance. With manual compliance processes, organizations are left unable to successfully de-risk all their environments at scale.

Siloed people, processes, and technologies
Organizations often run their workloads in a multi-cloud environment, and teams are left to manage multiple security tools for the different CSPs. Each cloud environment has its own unique tools, and security teams are required
to ramp up on each tool and manage and monitor the tools across the different clouds. This requires a unique process per tool and results in different silos per cloud. Additionally, traditional security tools only focus on a specific area of the security posture, for example vulnerability management, or configuration and compliance management. The security data for each area resides in the different tools, and is often owned by different teams, resulting in further silos in the people, processes, and technologies and a lack of a holistic view and context.

Operational inefficiency that slows down cloud adoption
The cloud enables developers to develop faster than they ever have before. Developers are the ones spinning up resources in the cloud, but it is the security team's responsibility to ensure that the resources are secure. With the rapid pace of innovation, it becomes operationally challenging for security teams to ensure secure configuration and detect risks early before they are exploited.

What is Cloud Security Posture Management?

- With so many challenges, there is a need for a cloud native, comprehensive, and consistent approach to cloud security. The new category of security products defined by Gartner, CSPM, addresses these challenges by continuously identifying risks in the cloud. CSPM tool automates security and provides compliance assurance in the cloud, reducing the manual effort needed to secure cloud environments even as they grow larger and

more complex.

- When you deploy a workload in the cloud, there are a variety of configurations that affect the way it operates. Identity and Access Management (IAM) configurations define who can view, modify, and run cloud workloads. Network settings control which other resources a workload can interact with over the network. Platform-specific configurations, such as environment settings defined inside container images or RBAC policies in Kubernetes, add yet more layers and variables to cloud workload configurations.
- With so many different configuration options, it's easy to make a mistake that weakens the overall security posture of your cloud environment. These mistakes often go unnoticed for long periods of time, putting the organization at risk of a breach. CSPM identifies misconfigurations in your environment automatically and alerts on them, allowing your team to act quickly and remediate any issues. CSPM helps you secure cloud workloads more efficiently and at a greater scale than you could if you relied on manual or periodic auditing of cloud configurations.
- Since the product category of CSPM has been introduced, the CSPM offerings have gone through several iterations of improvements to adopt a more comprehensive and holistic view of security. Legacy CSPM tools have a tunnel vision on cloud resources misconfigurations, missing out on many other risks that could significantly impact security posture and increase attack surface. New cutting-edge modern CSPM tools perform a much deeper risk analysis
- by considering additional risks that could result in toxic combinations such as vulnerabilities, secrets, or malware. Modern CSPMs improve your security posture by enabling you to better understand the criticality of risks, prioritize them, and improve your operational efficiency.

Key features of legacy CSPM tools

Visibility into configuration of resources
CSPM provides you visibility into your cloud resources across all your cloud environments. It identifies all your cloud resources and keeps an inventory of all the resources and their status.

Automatic and continuous detection
CSPM discovers your cloud resources automatically. As resources are deployed in your environment, CSPM detects those resources in real-time. This enables organizations to continuously monitor their existing resources and have their up-to-date status.

Misconfiguration rules
CSPM identifies misconfigurations in your environment by evaluating your current configurations against a set of best practices policies. It then alerts you of any resources that are not configured securely to allow your team to act on the misconfigurations fast.

Compliance standards and frameworks
CSPM runs risk assessment against common compliance standards and frameworks to allow you to meet your unique regulatory requirements. CSPM displays the status of the controls that are evaluated against the compliance framework and gives you the ability to set up remediation actions for those controls that could be triggered automatically.

Multi-cloud consistency
CSPM gives you consistent visibility and policy enforcement across multiple cloud service providers and Iaas, SaaS, and PaaS Platforms. With CSPM, organizations only need to use one tool across all their environments, significantly improving operational efforts.

What gaps do legacy CSPM tools have?

Lack of context
Legacy CSPM tools lack the context teams need to fully understand the risks in their environment. To get a full understanding of your security posture and the risks criticality, you need to consider more than just the misconfiguration of your resources, but how all other risks in your environment come together to create a toxic combination that requires your attention. Legacy CSPMs don't take into account other important risks such as vulnerabilities, network paths, identity exposures, secrets, malware, sensitive data, lateral movement and therefore lack significant amount of information that is required to understand the toxic combinations in your environment.

Noise Without Prioritization
Legacy CSPMs give you a lengthy list of issues. How can your team prioritize these issues without a full understanding of their criticality? For example, a legacy CSPM shows a misconfiguration issue for a virtual machine that is publicly exposed. How do we know what the criticality of that issue is if we do not know what is running on the machine, what are the network paths to the machine, its permissions, what data it has access to, if it has a vulnerability, and if it could cause any lateral movement in your environment. These are the pieces of information security teams need to reduce noise, prioritize, and focus on the critical risks in their environment.

Operational Inefficiency
Legacy tools are often not comprehensive, missing support for cloud service providers or Kubernetes, resulting in teams using unique tools per CSP. In addition, since legacy CSPM tools lack the needed context, organizations must use additional security tools to get the whole picture of their security posture. These tools include vulnerability scanning, CIEM, malware scanning, data protection, or container security tools. This results in a segmented view in the organizations' security posture and the security data residing in different silos. Often, these tools are owned by different teams and require different processes, creating further operational challenges in the organization.

How does a modern CSPM bridge the gaps of legacy CSPM?

- To complement the misconfiguration scanning and compliance checks covered by legacy CSPMs, modern CSPMs consider additional security risks to provide you with actionable context into risks in your environment so you can quickly remediate them.
- Legacy CSPM can alert that a virtual machine is publicly exposed, but the context around that machine is what allows security teams to really prioritize one finding over another. Let's assume that now we know that the same VM also has data access to sensitive data and a vulnerability with a known exploit. Or that the exposed VM has cleartext cloud keys that allow highly privileged cross-account access. These are examples of risks teams want to remediate right away. Without the needed context, security teams are unable to fully understand the criticality of risks in their environment.

Modern CSPMs include these additional capabilities to enrich the context of legacy CSPMs:

Agentless workload scanning
To gain full visibility into your environment you must also understand the workloads running in your environment and how they are configured. A modern CSPM gives you visibility into your workload configurations using an agentless workload scanner. The agentless scanner identifies the configurations of the OS, applications, and libraries across all compute including virtual machines, serverless, and containers. Removing the need for agent-based scanners, modern CSPM eliminates the security blind spots, performance impact, and ongoing maintenance required for agent-based solutions.

Cloud risk assessment at the cloud, app, and OS layers
Understanding the misconfigurations on the cloud level is not enough Organizations need misconfigurations rules assessing each layer of their cloud environment including the security of their applications. Modern CSPMs support host and application-level misconfiguration assessment against CIS benchmarks to enhance compliance and reduce risk.

Agentless vulnerability detection
Vulnerabilities can allow attackers to execute code in your environment or elevate their privileges. Because Vulnerabilities are such a common attack surface, understanding how each compute instance in your environment is vulnerable is crucial to assessing potential risks. Modern CSPMs uncover vulnerabilities across your cloud environment without deploying agents. Vulnerabilities are discovered across virtual machines, containers, and serverless resources and enrich the context for teams when prioritizing risks and understanding toxic combinations.

Contextual secure use of secrets
Secrets are one of the most common lateral movement paths used by attackers. In many cases, secrets are unnecessarily left exposed on workloads, or used where better cloud-native solutions are available. Modern CSPM detects leaked secrets or credentials that attackers might use in attempts to access sensitive assets or take over accounts.

Contextual malware detection
Misconfigurations can enable malicious actors to perform lateral movement and spread malicious code in your environment. Malware poses a risk on your resources that is critical and needs to be addressed urgently. Modern CSPM continuously scans all compute resources in your environment, VMs, container images, and serverless functions for potentially malicious software and identifies any resources that are at risk for you to prioritize.

Data Security Posture Management
It is important to understand where your sensitive data resides and who has access to it so you can successfully protect it. 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. Modern CSPM provides DSPM capabilities, continuously monitors for critical data exposure so your organization can respond before a breach occurs. These capabilities include visibility into PII, PHI, and PCI data, detection of any exposure paths to that critical data that can be exploited, and how those exposure paths came to be. This information enables you to proactively protect your cloud data and dramatically reduce the time it takes to discover and fix data exposure.

Kubernetes Security Posture Management
As more and more organizations containerize their workloads and choose to deploy them with Kubernetes, managing Kubernetes cluster security becomes a requirement to ensure a secure posture. A modern CSPM provides Kubernetes posture management capabilities, continuously monitoring Kubernetes clusters to identify misconfigurations and assess them against CIS Foundation Benchmarks for Kubernetes, EKS, AKS, and GKE.
AI Security Posture Management

Many organizations are rapidly innovating with AI, often leading security
teams to face a lack of visibility into new AI services being introduced into the environment, making it hard to secure them. To keep up with the pace of AI innovations, organizations need a modern CSPM that can provide them with 100% visibility into their AI pipelines, detect misconfigurations, and reveal attack paths to AI services.

Attack Path Analysis
Lateral movement in your cloud environment can lead to compromised high-value assets such as admin identities or crown jewel data stores. A modern CSPM can immediately identify escalation paths in your environment that allow threat actors to gain access to your crown jewels enabling you to address even the most sophisticated and hidden risks swiftly.

CI/CD Scanning
It is important to adopt a shift left strategy and identify misconfigurations early in your development cycle. Modern CSPMs integrate with your CI/CD pipeline to detect risks early, alerting on vulnerabilities, misconfigurations, and exposed secrets proactively before deployment. This allows developers to fix the risks before they go to production, making application delivery faster and more secure.

Comprehensive RBAC support
Organizations use a CSPM tool across all their environments to ensure consistent security. However different teams own different parts of the development, and it is important for a modern CSPM to have granular

environment segmentation to align with the development separation. A modern CSPM lets you group your cloud resources according to their users or purposes and define RBAC controls to give developers access to track and remediate only resources related to their projects.

Legacy CSPM vs modern CSPM feature comparison

Key Features	Modern CSPM	Legacy CSPM
Compliance Standards and custom frameworks	✓	✓
Near Realtime Configuration Evaluation	✓	✓
Agentless Cloud Workload Scanning	✓	✗
Contextual Cloud Risk Assessment	✓	✗
Offline Workload Scanning	✓	✗
Agentless and Contextual Vulnerability Detection	✓	✗ Requires an agent
Agentless and Contextual Secure Use of Secrets	✓	✗ Requires an agent and cannot identify lateral movement.
Agentless and Contextual Malware Detection	✓	✗ Requires an agent installed on the workload and manual correlation.

Data Security Posture Management	✓	✗
Kubernetes Security Posture Management	✓	✗
AI Security Posture Management	✓	✗
Effective Network Analysis	✓	✗
Effective Identity Analysis	✓	✗
Multi-hop lateral movement	✓	✗
CI/CD scanning	✓	✗
Comprehensive RBAC support	✓	✗

Key requirements of a comprehensive modern CSPM

When choosing a CSPM solution for your organization, there are the key capabilities you should ensure the CSPM must have to be considered comprehensive and modern.

Importance of configuration evaluation at every layer
Data breaches have significant impact on business and most breaches are a result of errors involving cloud misconfigurations. To truly protect your environment against misconfigurations, it is important for a comprehensive CSPM to evaluate misconfigurations at every layer of your environment. CSPM should have configuration checks at the cloud layer, as well as the application and host layer. It is important for it to also have full Kubernetes support and remediation actions.

Importance of contextual risk assessment and high-fidelity alerting
Context is what allows organizations to identify the toxic combinations in their environment and identify risks before they are exploited. It is important for a CSPM to provide a deep contextual risk assessment considering full scope of risks including vulnerabilities, network paths, identity exposures, secrets, malware, data exposures, and lateral movements. Context enables better prioritization, providing organizations with actionable insights into the actual critical risks in their environment. It is important for CSPM to have high-fidelity alerting, removing the noise and alert fatigue of traditional tools, and allowing teams to focus on the risks that matter.

Importance of continuous and comprehensive governance
Cloud governance needs to be automated and continuous to successfully assess a constantly changing and dynamic environment. CSPM should monitor the compliance of your environment on an ongoing and continuous basis. It is important for it to be comprehensive and cover all industry standards to help organizations meet their

regulatory requirements. CSPM should provide the flexibility for customization of controls so you can enforce the right checks
for your organization, as well as customization for compliance frameworks for your unique requirements. It should be consistent across all clouds, allowing organizations to use one policy across all environments.

Importance of IaC scanning
Organizations are shifting left to identify risks early in their development cycle. It is important for CSPM to support IaC scanning to secure environments from the start and empower developers to fix vulnerabilities, misconfigurations, and exposed secrets proactively before deployment. IaC scanning simplifies security operations by providing a single policy for both developers and security teams and increases the organization's security posture.

Getting started with CSPM

Once you choose the right CSPM tool for your organization, here are a few steps to help you get started:

1. Connect your cloud environment at the organization-level to cover all your accounts.
2. Enable scanning for all resources in your environment.
3. Group your cloud resources into projects and provide your users with RBAC permissions to the projects they need access to.
4. Once your environment is fully connected, you will likely discover dozens of critical and high severity issues. Address critical and high severity issues first.
5. Inspect any configuration issues and identify remediation and mitigation steps required. Consider setting automatic remediations where mitigation can be done without human intervention.
6. Connect the CSPM with your ticketing system to automatically create tickets when new issues are identified.
7. Inspect the status of your environment against the compliance frameworks that apply to your organization and identify controls that are non-compliant. Identify areas for improvement in your overall compliance posture based on compliance reports.
8. If your organization has any unique requirements not covered by the CSPM's controls, create custom policies to be evaluated across your environment
9. Shift left by integrating the controls with your CI/CD pipelines to prevent any misconfiguration from reaching to production

Request for proposal template

Choosing a vendor for your CSPM solution is a major decision. We have put together a Request for Proposal (RFP) template for you to consider when evaluating your CSPM vendor to ensure the solution is comprehensive and modern.

Requirement	Vendor Response
Resource and Workload Inventory	
What Code technologies do you provide visibility into? (Frameworks, Libraries, Softwar e Build Systems, Collaboration Software, Scripting Languages, etc.)	

What CI/CD tools do you provide visibility into?	
What Compute Platforms do you provide visibility into? (Cloud Subscriptions, Container Services, Serverless, Virtual Machines, Operating Systems, Networking, etc.)	
What Application and Data Platforms do you provide visibility into?	
What Security and Identity tools do you provide visibility into?	
Describe the visibility you provide into Workloads across Virtual Machines, Containers, and Serverless Functions.	
Demonstrate level of visibility into managed Kubernetes across EKS, AKS, GKE, and O KE.	
Demonstrate visibility into non-public Kubernetes API endpoints via private end points.	
Do you generate resource mapping relationships? Explain what relationships you map.	
Can you easily flag unwanted technologies in our environment?	
Governance	
Demonstrate support for compliance frameworks [SPECIFIC FRAMEWORKS].	
Demonstrate support for OS and applications compliance benchmarks [SPECIFIC BENCHMARKS].	
Demonstrate support for custom compliance frameworks.	
Demonstrate support for OS and applications compliance benchmarks [SPECIFIC FRA MEWORKS].	
Ability to create compliance reports based on account/subscription.	

Demonstrate ability to compare compliance posture across multiple frameworks in one view.	

Do you provide the ability to apply compliance frameworks to any level of operation (clo ud provider, account, grouping of resources)?	
Do you provide the ability to disable/enable or create policy exceptions as required?	
Demonstrate ability to prove compliance via reporting with timestamps.	
Do you provide a library of security policies?	
Do you provide the ability to build custom security policies?	
Do you provide a library of host configuration policies?	
Do you provide ability to build custom host configuration rules?	
Demonstrate ability to detect weak authentication of assets (e.g., VMs with password e nabled SSH authentication that are publicly exposed).	
Demonstrate ability to detect high risk configuration findings.	
Risk Assessment	
Demonstrate ability to monitor and report on the most critical attack vectors across net work, identity, vulnerabilities, secrets and configuration analysis.	
Demonstrate ability to prioritize security issues according to the environmental layout (e.g., External exposure, assumed privileges, business impact).	
Demonstrate ability to detect vulnerabilities on VM's, Containers, and Functions.	
Do you have the ability to detect vulnerabilities on powered off VM's?	
Demonstrate detection of weak authentication methods on VM's, Containers, and Funct ions.	
Demonstrate ability to detect exposed secrets on VM's, Containers, and Functions.	
Do you provide the ability detect end of life version of defined software packages?	

How do you generate automated risk scoring to prioritize resource risk?	

Demonstrate ability to detect systems that require restart.	
How do you manage the detection of multiple occurrences of the same misconfiguration on a resource?	
Demonstrate ability to detect API services without authentication set.	
Demonstrate ability to query functionality for custom searching.	
Do you provide the ability to customize and export query results?	
Demonstrate ability to provide complete audit trail of all user activities within platform.	
Do you scan for malware across cloud environments?	
Vulnerability and Patch Management	
Demonstrate ability to detect vulnerabilities in container images.	
Demonstrate ability to detect vulnerabilities in currently running containers.	
Demonstrate ability to detect vulnerabilities in container images without repository acce ss	
Demonstrate ability to detect vulnerabilities in container images hosted in a container re gistry	
Do you provide the ability to scan private container registry?	
Demonstrate ability to detect vulnerabilities in container images in self-deployed docker /Kubernetes	
Demonstrate ability to detect vulnerabilities in VMs	
Demonstrate ability to detect library-based vulnerabilities in VMs and containers (e.g., Python, Java).	

Detail the level of context provided for vulnerabilities.	
Provide examples of advanced queries on vulnerabilities.	
Demonstrate ability to detect vulnerabilities on publicly exposed resources.	

Demonstrate ability to detect vulnerabilities on highly privileged resources.	
Demonstrate ability to detect vulnerabilities on critical risk assets.	
Demonstrate ability to detect unpatched OS on compute nodes and instance groups.	
Demonstrate ability to detect unpatched Kubernetes clusters.	
Demonstrate ability to detect publicly exposed unpatched VMs and containers.	
Demonstrate ability to detect publicly exposed containers running on a compute node with unpatched kernel	
Demonstrate ability to detect end-of-life Hosted technologies running on public facing c ompute instance	
Demonstrate ability to detect highly privileged unpatched assets and assets with critical risk.	
Provide list of threat and vulnerability databases you source information from.	
Exposure Analysis	
Demonstrate ability to provide network reachability map of resources and workloads.	
Demonstrate ability to detect publicly exposed resources and containers.	
Demonstrate ability to detect Kubernetes clusters with publicly exposed APIs.	

Demonstrate ability to detect ingress rules on any port and destination.	
Do you provide built-in intelligence that is able to identify known suspicious IPs connecting to workloads?	
Demonstrate ability to detect poorly separated network traffic.	
Demonstrate ability to detect resources accessible from other subscriptions.	
Demonstrate ability to detect geo-location traffic from unrecognized regions.	
Demonstrate ability to detect resources accessible from other Vnets.	

Demonstrate ability to detect all resources exposed publicly behind load-balancers.	
Demonstrate ability to provide intuitive visual interface to analyze & investigate network traffic in either north-south or east-west directions.	
IAM and Secrets	
Demonstrate ability to capture IAM activity for users & roles (create, modify, delete).	
Demonstrate ability to detect overly permissive access.	
Do you recommend permission sets based on utilization? Do you recommend permissi on sets based on utilization?	
Demonstrate ability to detect who has access to specific resources.	
Demonstrate ability to detect users/roles with elevated permissions on resources	
Demonstrate ability to detect over-privileged permissions on containers.	
Demonstrate ability to detect over-privileged permissions on serverless workloads.	

Demonstrate ability to detect exposed secrets on VMs, containers, and functions.	
Demonstrate ability to detect exposed secrets on public and private buckets	
Demonstrate ability to detect secrets (certificates, access/encryption keys, cleartext data, etc.).	
Demonstrate ability to detect lateral and cross-account movement via compromised ac cess keys or stolen permissions.	
Demonstrate ability to identify cloud services that can access data.	
Demonstrate ability to find inactive admin users and groups.	
Demonstrate ability to find exposed SSH private keys.	
Demonstrate ability to detect exposed private keys of domain certificates	
Demonstrate ability to find resources using service accounts with admin permissions.	

Demonstrate ability to find certificates nearing expiration and exposed certificates.	
Demonstrate ability to find cleartext cloud keys allowing high privileges.	
Demonstrate ability to find attack path to high value assets.	
Security Automation	
List the ticketing platform(s) you support.	
Provide details on workflow actions for notifications.	

Demonstrate ability to generate rule sets based on conditions and criteria.	
Demonstrate ability to send notifications with context on risk (can be customized to enrich if required).	
List what SIEM tools are supported.	
List what SOAR tools are supported and remediation playbooks available.	
Do you support auto-remediation? Provide examples and details.	
List what vulnerability management and response tools are supported.	
Demonstrate ability to obtain recommendations against misconfigurations and to execute auto-corrective actions.	
Demonstrate ability to generate management policies for CSPs (AWS SCP, Azure Polic y) for preventive control.	
DevSecOps	
Demonstrate ability to integrate controls as part of a deployment pipeline to validate infr astructure-as-code (IaC) is compliant with defined policies.	
Demonstrate ability to validate IaC templates are compliant before enterprise use.	
Demonstrate ability to scan VM images (e.g., AMI) and container images for vulnerabilit ies and exposure.	
Demonstrate ability to scan container images for exposed secrets in the CI/CD pipeline.	

Demonstrate ability to scan virtual machine images for exposed secrets in the CI/CD pi peline.	
List what CI/CD tools you integrate with.	

List customer references who have successfully implemented a DevSecOps strategy u sing your product.	
Data Security	
Demonstrate ability to identify sensitive data (PII, PCI, PHI and secrets)	
Do you provide the ability to scan public and private cloud storages (AWS S3, Azure Bl ob Storage and GCP Cloud Storage)?	
Do you provide the ability to scan managed and self-hosted SQL databases?	
Do you provide the ability to scan managed and self-hosted No-SQL databases and identify sensitive data?	
Do you provide the ability to scan workload OS and Data disks and identify sensitive dat a?	
Do you provide the ability to ingest classified tags from external sources like BigID or Macie?	
Demonstrate ability to detect unintentionally moved or copied between environments, r egions, or clouds	
Demonstrate ability to detect and alert on externally exposed workloads (VM, container, Serverless) with possible lateral movement to sensitive data	
Demonstrate ability to detect and alert on externally exposed cloud storage with sensiti ve data	
Demonstrate ability to create custom classifiers	
Ai Security	
Do you provide the ability to detect AI technologies, SDKs, and services? (Sagemaker, Bedrock, VertexAI, Azure OpenAI, OpenAI)	
Do you provide visibility into AI pipelines on a graph?	
Do you provide the ability to detect misconfigurations in AI services?	
Do you provide the ability to detect risks in AI pipelines across vulnerabilities, identities, exposures, and sensitive data?	

Do you provide the ability to detect sensitive data used for AI training?	
Do you provide the ability to detect attack paths in AI pipelines?	
Do you provide the ability to detect lateral movement paths from AI pipelines to cloud e nvrionments?	
Do you correlate secrets found in AI pipelines to cloud context and vice versa?	

About Wiz

Wiz transforms cloud security for customers – including 40% of the Fortune 100 – by enabling a new operating model. With Wiz, organizations can democratize security across the development lifecycle, empowering them to build fast and securely. Its Cloud Native Application Protection Platform (CNAPP) drives visibility, risk prioritization, and business agility, and is #1 based on customer reviews.
Visit **https://www.wiz.io/** for more information.

Documents / Resources

	**WIZ 2023 Cloud Security Posture Management** [pdf] User Guide 2023, 2023 Cloud Security Posture Management, Cloud Security Posture Management, Securit y Posture Management, Posture Management, Management

References

- ✦ **Wiz: #1 Cloud Security Software for Modern Cloud Protection**
- **User Manual**