

# Vulnerability Management Solutions



Wiz provides a complete suite of vulnerability management features that empower organizations of all sizes and maturities to assess, prioritize, and remediate vulnerabilities across clouds and architectures.

Most vulnerability management features operate completely agentlessly, dramatically reducing deployment friction and eliminating blindspots. Agentless vulnerability assessment can be supplemented by installing the Wiz Runtime Sensor on key workloads to validate vulnerabilities in runtime.

## Popular topics



### How vulnerability management works

Dive deep into the details of how Wiz detects, enriches, prioritizes, and manages vulnerabilities



### Vulnerability management tutorials

Follow step-by-step tutorials to learn how to use Wiz for vulnerability management



### Exporting vulnerabilities

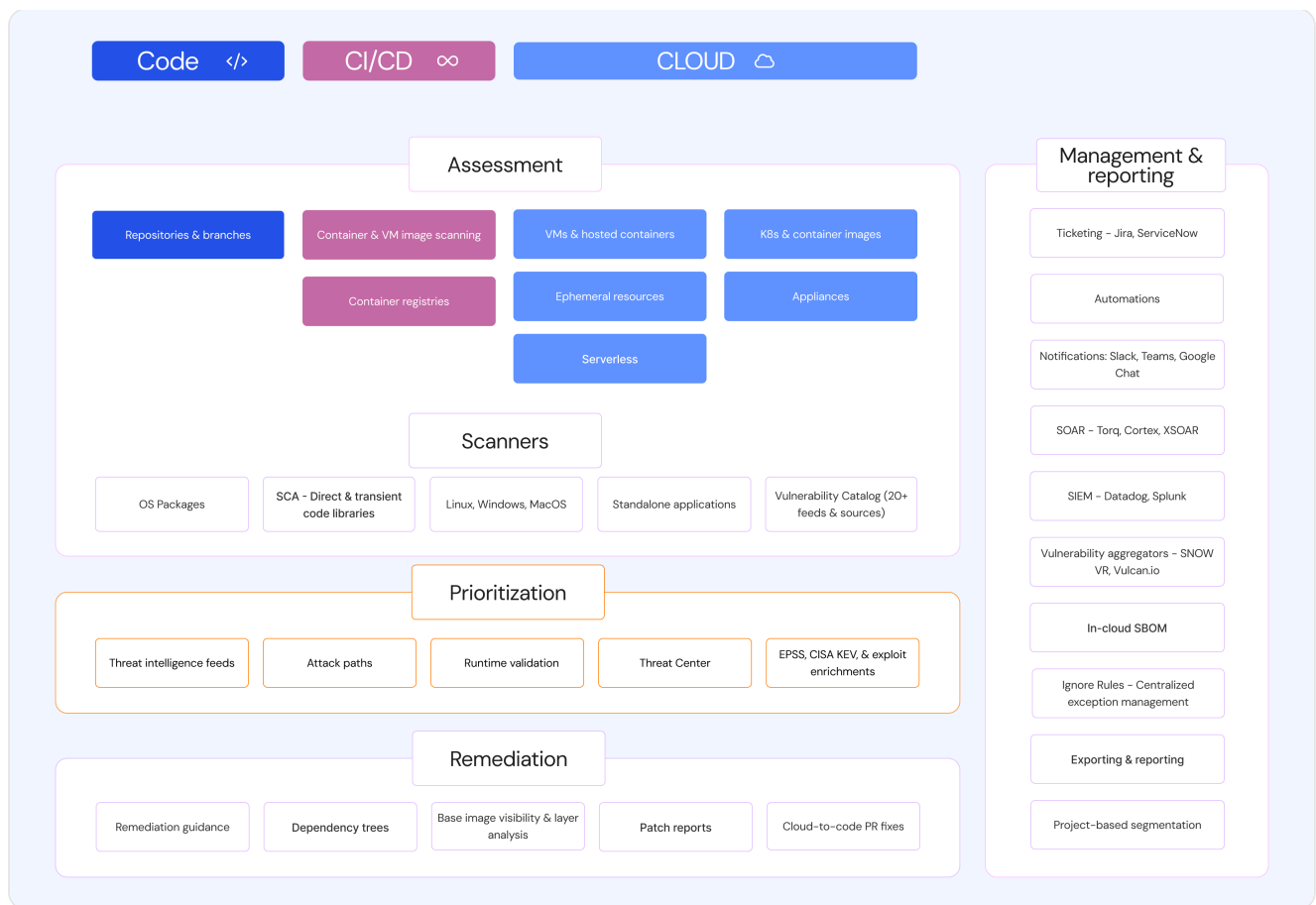
Use reports and/or the Wiz API to periodically export all detected vulnerabilities to a third-party tool



There's an entire recorded webinar on [vulnerabilities](#).

## Architecture

Wiz analyzes code, artifacts moving through the CI/CD pipeline, and resources running in your cloud for vulnerabilities.



Learn more about vulnerability management features:

Show All ↓

### ▼ Assessment

- Repository & branches—Secure code from the start and gain visibility into your vulnerable libraries as early as possible via Version Control System Connectors. [Learn about Version Control Scanning](#).
- Container & VM image scanning—Scan container and VM Images in CI/CD pipelines to detect vulnerabilities and optionally fail the build if any are found. [Learn about Wiz CLI](#).
- Container registry scanning—Auto-discover and connect cloud-based registries to ensure comprehensive coverage and vulnerability detection. [Learn about container registry scanning](#).
- Wiz Admission Controller—Prevent container images from being deployed if they have not passed the vulnerability policy. Learn about [Wiz Admission Controller](#) and [enforcing image trust](#).
- Full visibility into production—Leverage various detection methods (e.g. packages and code libraries) to detect vulnerabilities across clouds, with agentless workload scanning and runtime validation powered by the [Wiz Runtime Sensor](#).

### ▼ Scanners

The Wiz vulnerability management engine is an agentless scanner that natively supports the following capabilities:

- Linux, Windows, MacOS—Wiz natively supports scanning for vulnerabilities in Windows, MacOS and most of Linux distributions. See the complete catalog of [supported hosted technologies](#).
- OS Packages vulnerabilities—Across Windows and Linux.
- SCA—The vulnerability scanner analyzes code libraries dependencies (direct and transient) both in cloud and in code to detect vulnerabilities in open source libraries.
- Standalone applications—Applications installed manually (i.e. not via a package manager, Windows programs, etc.) are also supported for vulnerability scanning.
- Vulnerability Catalog—Wiz ingests [more than 20 sources and feeds](#) to assess for vulnerabilities. On the [Policies > Vulnerability Catalog](#) page, you can explore the full list of supported vulnerabilities and their sources.

#### ▼ **Prioritization**

Focus first on what matters the most and reduce noise using the power of context and toxic combinations:

- Intelligence feed-based severity—An extensive [vulnerability catalog](#) allows you to search and filter by different parameters, including EPSS, vendor severity, date, has fix, exploitability, CISA KEV exploitability, and more
- Attack path & risk-based prioritization—Reduce alert fatigue by correlating vulnerabilities with multiple risk factors, including external exposure, cloud entitlements, and secrets to surface the vulnerabilities that must be fixed first. [Learn about Controls and Issues](#).
- Runtime validation—Detect vulnerabilities executed in runtime using the Wiz Runtime Sensor. [Learn about runtime validation](#).
- Modify severity—Customize the severity of vulnerability findings for specific Projects or resources to align them with your internal logic and priorities
- Threat Center—Advisories for emerging cloud threats relating to ongoing cyber-attacks and critical vulnerabilities exploited in the wild that can impact your cloud. [Learn about the Threat Center](#).

#### ▼ **Remediation**

- Remediation guidance—Detailed remediation options and steps are added to every vulnerability finding
- Patch recommendations across app lifecycle—Identify and patch components with known vulnerabilities in different stages of the application lifecycle (Code

→ CI/CD → Cloud). [Learn about patch recommendations](#).

- Visibility into transitive dependencies—Detailed hierarchical views into workloads' software composition for precise vulnerability remediation guidance
- Base image visibility & layer analysis—Visibility into common third-party base images used to build your container images. [Learn about base image visibility](#).

### ▼ Management and reporting

Maximize the effectiveness and efficiency of your security team and developers by leveraging management tools:

- Ticketing—Open tickets in Jira, ServiceNow, etc. that include all of the information required for devs and DevOps to quickly apply the necessary fixes. Tickets opened from Wiz are automatically linked to the associated Issue to make it easy to follow up. [See all ticketing integrations](#).
- Automations—Define granular if/then rules to automatically open tickets, send messages, or run other Actions when new Issues are generated or existing Issues are updated. [Learn about Actions and Automation Rules](#).
- Notifications—Send Wiz insights to your colleagues preferred messaging tools, e.g. Slack, Teams, or Google Chat. [See all messaging integrations](#).
- SOARs, SIEMs & vulnerability aggregators—Send Wiz insights to your preferred tools to enhance your existing workflows and processes. See all [SOAR](#), [SIEM](#), and [vulnerability management](#) integrations.
- In-cloud SBOM—Identify and search for specific versions of deployed components in your environment to enable triage of zero-day vulnerabilities and analysis of licensing. [Learn about agentless SBOM](#).
- Centralized exception management—Automatically ignore vulnerability findings based on all, specific, or a filtered set of resources. [Learn about Ignore Rules](#).
- Integrations—Stream vulnerability data incrementally using third-party integrations with S3 buckets, Snowflake, SNOW VR, and more.
- Exporting & reporting—Report on vulnerabilities through Wiz reports for specific vulnerabilities or a filtered set based on vulnerability findings. [Learn about exporting vulnerability findings](#).


## Vulnerability management use cases

Vulnerability management spans multiple phases of the software development lifecycle:

Show All ↓

### ▼ Cloud

- Assess the vulnerability of all resources, including VMs, containers, container images, serverless resources, appliances, and ephemeral resources.
- Leverage various detection methods (e.g., packages and code libraries) to detect vulnerabilities across clouds, with agentless scanning.
- Detect vulnerabilities executed in runtime using the Wiz Runtime Sensor.
- Identify common critical severity exploitable vulnerabilities, and critical exploitable network vulnerabilities, as well as exploitable CVEs in the last 60 days.
- Identify attack paths involving vulnerabilities with multiple risk factors, including external exposure, cloud entitlements, and secrets, to surface the vulnerabilities that should be prioritized.
- Prioritize remediation by the number of affected resources or number of vulnerabilities per resource.
- Report on vulnerabilities through Wiz reports for specific vulnerabilities or a filtered set based on Vulnerability Findings.
- Use Ignore Rules to automatically ignore Vulnerability Findings based on all, specific, or a filtered set of resources.
- Use the agentless SBOM to identify and search for specific versions of deployed components in your environment, specifically for licensing and zero-day vulnerabilities.
- Streamline vulnerability findings incrementally using third-party integrations through built-in APIs to S3 buckets, Snowflake, SNOW VR, and more.
- Create custom boards to monitor and analyze vulnerabilities.

 Required deployments: [Cloud Connectors](#), [Kubernetes Connectors](#), [Runtime Sensors](#)

#### ▼ **</> Code**

- Identify vulnerable packages, libraries, etc. in developer IDEs or by running Wiz CLI locally
- Detect vulnerabilities in VCS repositories
- Automatically generate remediation suggestions for identified vulnerabilities in developer IDEs and VCS repositories and pull requests
- Optionally block pull requests that add vulnerabilities to VCS repositories
- Identify vulnerabilities in artifacts as they move through CI/CD pipelines and optionally block them

 Required deployments: [VCS Connector](#), [Wiz CLI](#), [IDE Integration](#)

## ∞ CI/CD

- Identify vulnerable packages, libraries, etc. in container images as they move through the CI/CD pipeline, and optionally block them from proceeding.
- Identify vulnerable packages, libraries, etc. in container images at rest in container registries.

🔗 Required deployments: [Wiz CLI](#) in the CI/CD pipeline, [Container Registry Connectors](#)

## Relevant portal pages

The built-in Vulnerability Management View can be used to focus on only the portal pages relevant to vulnerability management.

The screenshot shows the Wiz Vulnerability Management dashboard. The sidebar on the left contains navigation links: Boards, Issues, Findings, Inventory, Explorer, Policies, Reports, Settings, Connect, and Feedback. The main content area is titled 'Vulnerability Management' and features a 'Switch View' dropdown menu. The dropdown menu lists the following options: Exit View, Cloud Entitlements, Code & CI/CD Security, Container Security, Data Security, SOC, Security Posture Management, **Vulnerability Management** (highlighted with a red box), Only Dashboard Overview View, and Org Custom View. The dashboard displays 'Vulnerability Issues' with a count of 102 Critical Issues, 14 High Issues, 163 Medium Issues, and 482 Low Issues. A line chart shows a 50% increase in Critical Issues and a 12% decrease in High Issues. The 'Top Vulnerability Issues' section lists 77 rules, including 'Publicly exposed VM/serverless with ...' and 'Publicly exposed VM with high...'. The 'Publicly Exposed Containers With Latest Exploitable Vulnerabilities' section lists containers like 'payment-ap...' and 'tomcatapp...' with their respective vulnerabilities and findings.

Learn about the [Vulnerability Management View](#).

## Related topics

- [How Agentless Scanning Works](#)
- [Runtime Sensor](#)

🕒 Updated 22 days ago

Did this page help you?  **Yes**  **No**