Application Security Testing & Exposure Management

zcrX

Test applications. Prioritize exposure.

zcrX tests application source code with static application security testing (SAST) and running applications with dynamic application security testing (DAST). Its console also brings together cryptography readiness, software vulnerabilities and dependency trust. Agents report posture from enrolled hosts and build systems; exploitation signals, severity and affected-host count guide remediation.

Available · Annual subscription; scope and quotation through an approved channel partner.

Who evaluates zcrX? · Vulnerability management, application security and platform engineering teams; managed security service providers overseeing customer tenants; and security leaders planning post-quantum migration.

Read the prioritization signals

CVE · Common Vulnerabilities and Exposures
Identifiers and records for publicly disclosed cybersecurity vulnerabilities. [1]

CISA KEV · Known Exploited Vulnerabilities
The US Cybersecurity and Infrastructure Security Agency’s catalog of vulnerabilities with evidence of exploitation in the wild. [2]

EPSS · Exploit Prediction Scoring System
FIRST’s estimate of the probability that a published CVE will be exploited in the wild in the next 30 days. It is a likelihood estimate, not a severity score. [3]

Definitions: [1] CVE Program · [2] CISA · [3] FIRST · [1] ↗ [2] ↗ [3] ↗

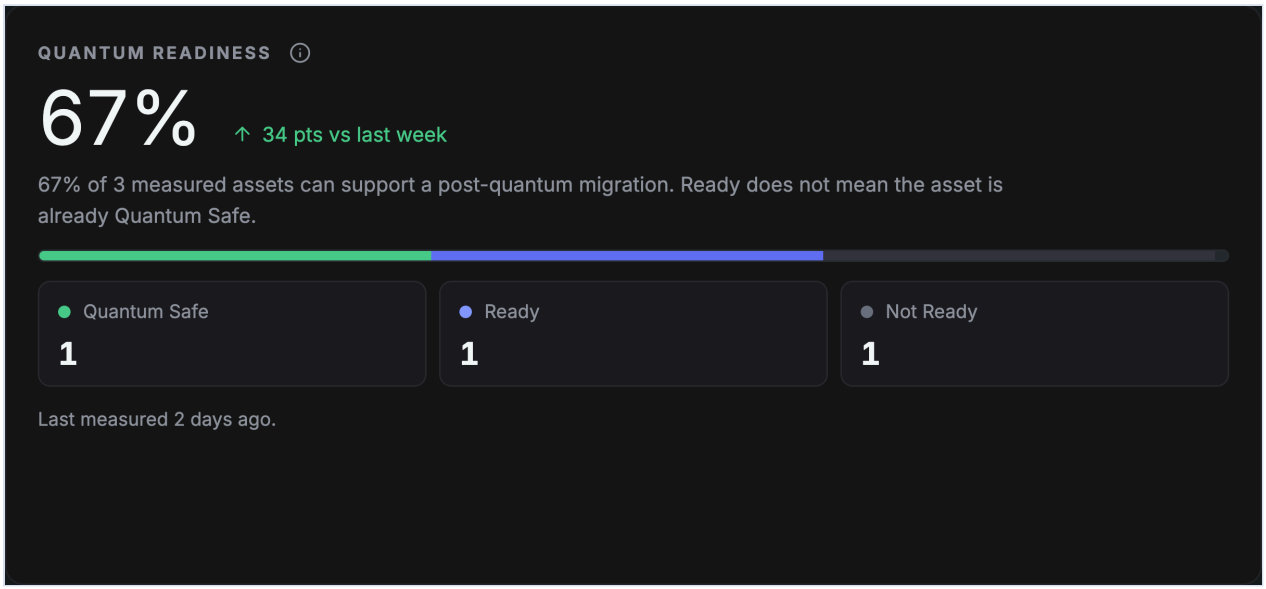
What each view helps you decide

Quantum-Ready Cryptography	Track certificate and algorithm inventory against post-quantum migration readiness.
Prioritized Vulnerability Fixes	Rank remediation by CISA KEV status, EPSS score and severity, not raw CVE counts.
Verified Supply Chain	Confirm dependency provenance by cryptographic proof or Agent attestation, across ecosystems.
One View for Providers	Manage every customer tenant's posture through delegated, least-privilege access.

Readiness and remediation priority

01 / Plan cryptographic migration

Cryptography posture: certificate and algorithm inventory scored quantum-safe, ready, or not ready



Complete quantum-readiness widget: the state legend and the distinction between Ready and Quantum Safe remain visible. Demo — fixture data, not live customer figures. English UI preserved. Open demo view ↗

> Cryptographic priorities reflect post-quantum migration urgency. In this example, Ready means migration-ready, not already quantum-safe; urgency remains unassessable without declared business context.

02 / See why a fix ranks first

- Software vulnerability posture: host and package findings matched to CVE advisories, CISA KEV status and EPSS score
- Remediation ranked by KEV, score and affected-host count, with the reason for each ranking
- Findings tracked against published, severity-based remediation windows, and flagged when overdue

Why it matters	Action
A critical advisory affects this package version; An affecting advisory is on CISA's Known Exploited Vulnerabilities catalog	View affected packages

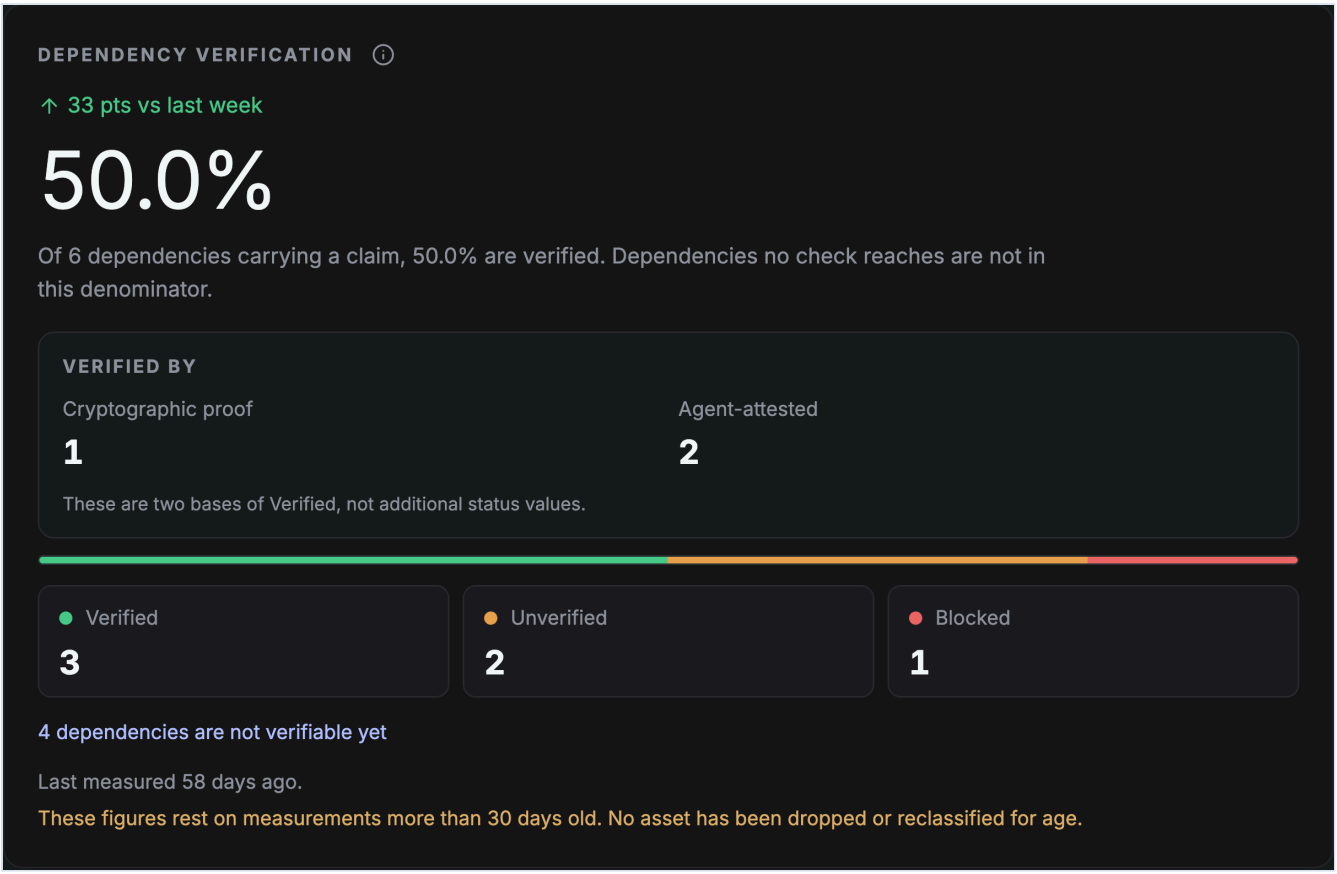
Complete “Why it matters” and “Action” columns for one priority row. The ranking reason cites a critical advisory and KEV membership; this is not a measured customer result. Demo — fixture data, not live customer figures. English UI preserved. Open demo screen ↗

> The software view also groups findings by age against published remediation windows. The original screen shows an unassessed host and a package with no fix available yet; neither state is evidence of a clean environment.

Verify dependency provenance

03 / Separate proof from missing evidence

Supply-chain posture: dependency provenance verified by cryptographic proof or Agent attestation, across npm, PyPI, Go and Maven



Complete verification widget: denominator, both verification bases and status legend. Agent attestation and cryptographic proof are bases of Verified, not extra statuses. Last measured 58 days ago; the >30-day warning is retained. No asset was dropped or reclassified for age. Demo — fixture data, not live customer figures. English UI preserved. Open demo view ↗

> In this example, dependencies that no check reaches are excluded from the verification denominator. Unverified, Blocked and Not verifiable yet remain distinct; the software's example percentages do not establish your environment's coverage.

Coverage to scope with your partner

npm · PyPI · Go · Maven · Linux hosts · Container images

Dependency provenance verified by cryptographic proof or Agent attestation, with ecosystem coverage and known-vulnerability counts.

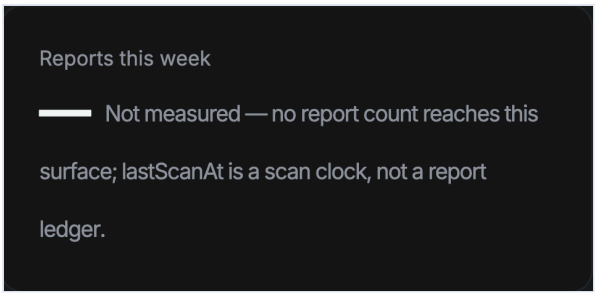
> The approved overview names these ecosystems and asset types. Confirm the specific operating-system versions, images and build environments during partner validation; the list is not an unrestricted compatibility guarantee.

Know what is measured—and who can enter

Agents and measurement boundaries

Lightweight Agents deployed to hosts and build systems for continuous scanning

The Agent fleet lists enrolled Agents, liveness and each host's measured domain status. A host without an Agent is not measured and is never assumed clean.

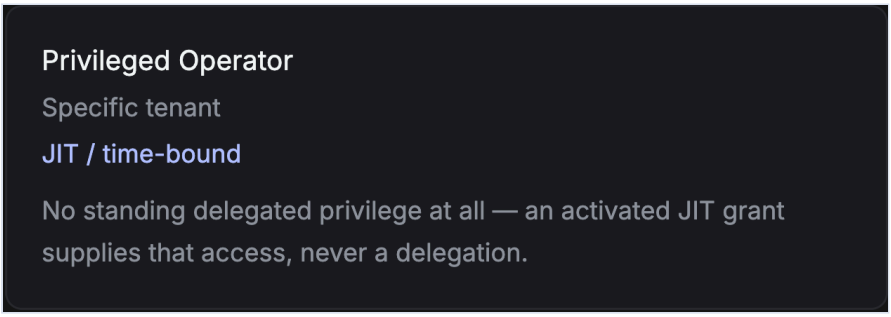


Complete "Reports this week" widget. The sample explicitly says Not measured and distinguishes a scan clock from a report ledger. Demo — fixture data, not live customer figures. English UI preserved. Open demo view ↗

Tenant access stays scoped

Multi-tenant provider control plane with delegated, least-privilege, time-bound access to each customer tenant

The provider control plane supports multiple customer tenants with delegated, least-privilege access, including pre-approved and just-in-time (JIT) approval policies. JIT access is time-bound.



Complete Privileged Operator role card. In this demo, an activated JIT grant supplies access; a delegation alone does not. The original screen also shows pending customer authorization. Demo — fixture data, not live customer figures. English UI preserved. Open demo view ↗

Keep the operational detail

- Product lifecycle and end-of-life tracking per software product
- CSV export for findings, dependencies and the Agent fleet

> CSV means comma-separated values; EOL means end of life. The cryptography, vulnerability and supply-chain views extend the zcr suite through continuous Agent-based measurement, rather than a one-time scan.

> Your channel partner provides first-line support, with zcr backing the partner. Specific support terms require validation.

Prepare a scoped evaluation

Questions before evaluation

Is zcrX available now?

Yes. zcrX is available as an annual subscription. Your channel partner confirms the scope, quotation and technical evaluation.

Does zcrX need software installed on every host?

zcrX deploys lightweight Agents to the hosts and build systems you enroll. A host with no Agent shows as not measured rather than being assumed clean.

How does zcrX decide what to fix first?

Findings are ranked by CISA's Known Exploited Vulnerabilities (KEV) status, EPSS score, severity and how many hosts they affect — not by raw finding counts.

Can zcrX manage more than one customer environment?

Yes. zcrX includes a provider control plane with delegated, least-privilege access to each customer tenant, built for channel partners managing more than one customer.

Bring these inputs to your approved partner

Inventory & permission	List applications, authorized test environments, hosts, build systems and ecosystem versions. Name the owners who authorize testing and Agent deployment.
Tenant boundaries	Name customer tenants, data owners and approval owners; agree the required delegated access and its duration.
Evidence to inspect	Choose sample findings, migration states, provenance evidence, CSV outputs and unknown/unmeasured cases to review.
Environment validation	Ask the partner to validate OS/version support, resources, network paths, installation privileges, capacity and required access. These specifics are not established here.
Commercial & delivery scope	Confirm edition, packaging, price, currency, unit, billing period, tax, effective date, support and delivery responsibilities in the partner proposal.

Technical demo

The public demo shows the three posture domains. For SAST/DAST, agree the applications and test environments with your channel partner.

Scoping conversation

Use the checklist to agree enrollment and validation, then request a scoped proposal and quotation. Contracting and delivery run through an approved partner.

Arrange evaluation through an approved partner ↗ Explore the sample demo ↗

Demo — fixture data, not live customer figures. English UI preserved.