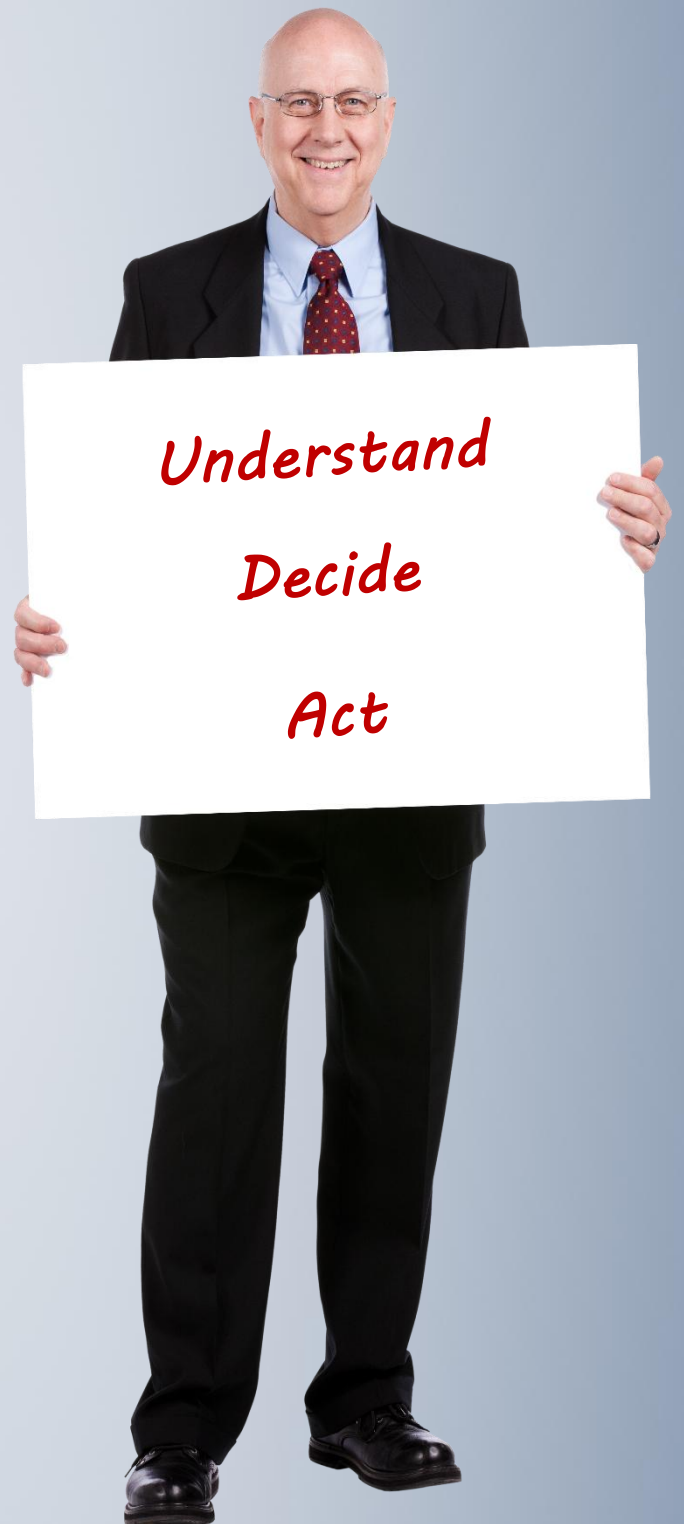


Understand, prioritize, and remediate operational
and security risk across your application
landscape by using AI-driven analytics,
automation, and contextual insights

IBM Concert

www.vpbis.com | **ValuePath**





IBM CONCERT PLATFORM. UNDERSTAND, DECIDE, ACT

"Understand, Decide, Act" represents the core operational framework of IBM Concert, agentic AI-powered IT Operations platform. This three-part cycle explains how the platform transforms overwhelming data signals into governed, automated resolutions.

Understand: Visibility & Context

Instead of forcing engineers to manually piece together disconnected alerts, Concert automatically ingests data from across hybrid cloud environments to build a comprehensive **application topology**.

- **Data Integration:** It absorbs code repositories, container images, cloud telemetry, and system dependencies.
- **Shared Context:** Powered by **AI**, it acts as a central hub to map how applications, networks, and infrastructure interact. This eliminates blind spots and instantly surfaces hidden risks like software vulnerabilities, compliance gaps, or expiring digital certificates

Decide: Prioritization & Insight

Once the system maps out the application ecosystem, it uses Gen AI to cut through technical noise and evaluate operational "posture".

- **Risk Prioritization:** It evaluates the severity of detected incidents or vulnerabilities, evaluating how far-reaching an outage or a breach would be across the business topology.
- **Strategic Recommendations:** Rather than just triggering a generic alert, it creates a "ranked list of concrete next steps" and generates smart, tailored mitigation steps in plain natural language.

Act: Orchestrated Automation

The final phase closes the execution gap by executing remediation safely, with optional human-in-the-loop governance.



Modern enterprise IT landscape has reached an inflection point. As architectures expand across hybrid cloud environments, microservices, and multi-cloud infrastructures, management has become increasingly fragmented. Engineering, Operations, and Security teams spend critical cycles navigating disconnected tools, sifting through millions of alerts, and performing manual triage.

IBM Concert® changes this dynamic. Built on IBM watsonx™, IBM Concert serves as the neural center of your enterprise application ecosystem. It provides real-time visibility, automated risk mitigation, and actionable intelligence—enabling CXOs, IT Leaders, and Enterprise Architects to transform operations from reactive firefighting to proactive, AI-driven governance.

While enterprise systems generate massive volumes of alerts and telemetry, they often lack application-level context, leaving teams unable to determine which vulnerabilities pose the highest business risk.

What is IBM Concert?

IBM Concert is an AI-powered enterprise management platform designed to deliver continuous control, risk management, and operational clarity across complex application lifecycle environments.

Rather than replacing your existing toolchain, IBM Concert connects directly to your enterprise topology -integrating telemetry, security scanners, CI/CD pipelines, and cloud services. By building a dynamic topology map of your applications and their underlying dependencies, Concert leverages generative AI to analyze operational context, prioritize critical vulnerabilities, predict disruptions, and recommend precise remediation workflows.

Why IBM Concert now?

The modern enterprise operates in an ecosystem defined by unprecedented hyper-complexity and rapid expansion. While hybrid cloud architectures and generative AI accelerate digital innovation, they simultaneously create operational blind spots, security exposure, and governance friction across disconnected toolchains. Modern IT environments generate millions of telemetry points, security alerts, and performance metrics daily, yet this abundance of raw data rarely translates into immediate operational clarity. Security scanners flag vulnerabilities without understanding application criticality, while performance monitoring tools detect anomalies without identifying the underlying code commit or infrastructure shift. IBM Concert bridges this critical gap by connecting directly to your entire ecosystem and building a dynamic, real-time map of your applications, dependencies, and environments.

IBM Concert helps organizations understand, prioritize, and remediate operational and security risk across their application landscape by using AI-driven analytics, automation, and contextual insights.

Concert brings together application inventory, analytics, and automation to deliver a unified view of operational health, risk, and posture across the application landscape. Concert evaluates critical indicators, referred to as **dimensions** to identify and prioritize risks that are related to vulnerabilities, compliance, certificates, resilience, and software composition. By using a shared data foundation and AI-driven intelligence, Concert helps you to focus on the most relevant risks and take informed action across development and delivery activities.

Concert works by ingesting and analyzing application data to provide contextual insight into operational risk.

At a high level, Concert:

- Ingests data from multiple sources, including application components, repositories, images, and environments.
- Builds an inventory and maps dependencies to create an application topology.
- Analyzes data across defined dimensions to assess risk and posture.
- Prioritizes risks based on severity and impact.
- Surfaces insights and recommendations



What IBM Concert delivers?

Concert helps to manage application risk and operational posture by transforming distributed application data into prioritized, actionable intelligence across the application lifecycle.

Gain a unified view

Concert ingests application components, repositories, images, and environments to build an inventory and application topology.

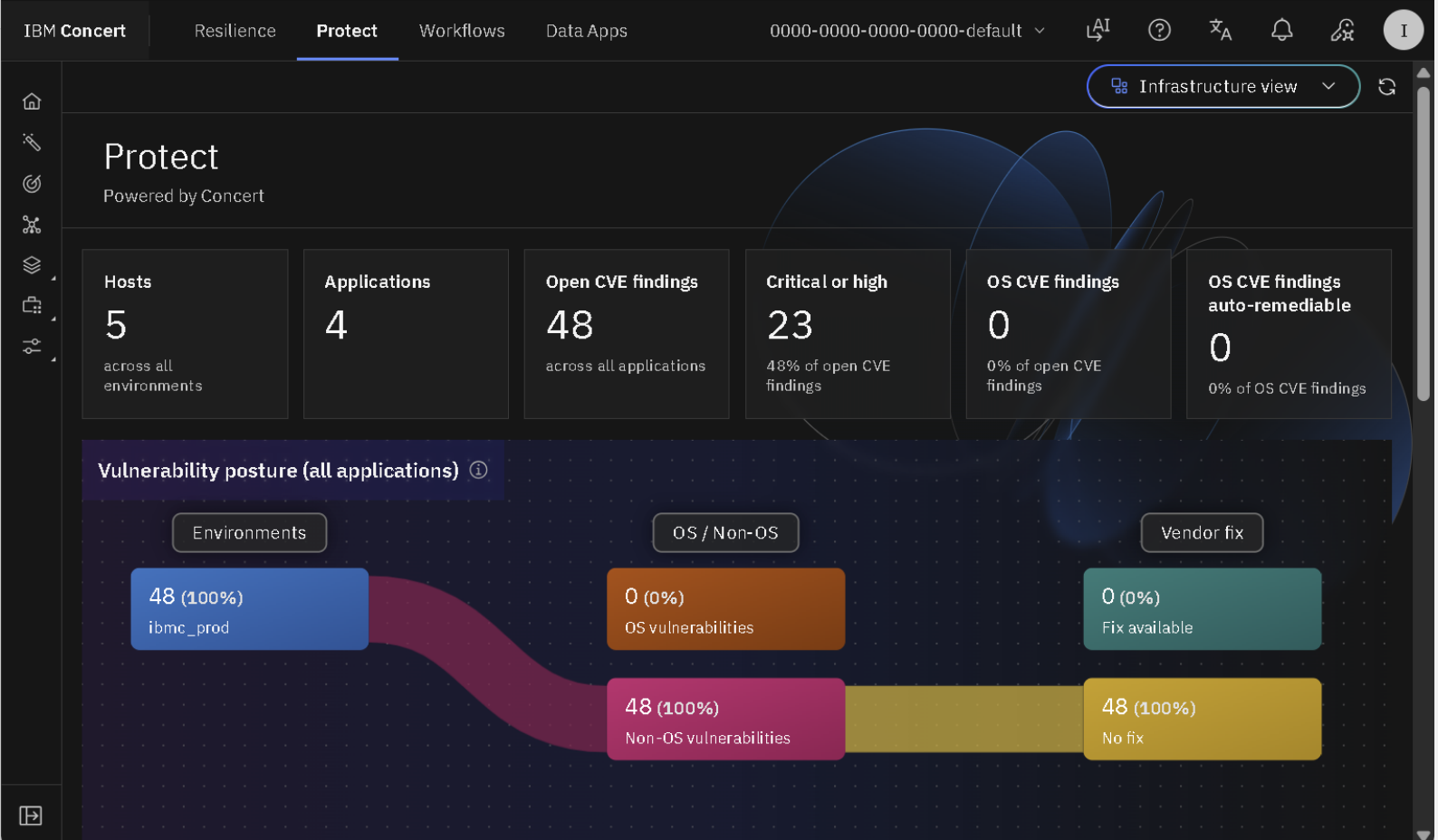
Identify and prioritize application risk

Concert evaluates application data by using critical indicators known as dimensions. By analyzing risk across vulnerabilities, compliance, certificates, resilience, and software composition, Concert helps to focus on the most impactful issues.

Persona-driven experience

Concert delivers a role-aligned experience that supports different responsibilities and objectives, while maintaining a consistent platform, data model, and intelligence for all users.

The modern enterprise operates in an ecosystem defined by unprecedented hyper-complexity and rapid expansion.



OBSERVE :: OPERATE :: OPTIMIZE :: PROTECT

IBM Concert **Resilience** Protect Workflows Data Apps 0000-0000-0000-0000-default AI ? 文A 🔔 👤 I

Postures 4 Profiles 12 **Libraries 10** Metrics 253 Compare assessments

Find by library name 📑 🔍 ↺ Create library

☐	Library name	↑	Description	
☐	Container Build Integrity Library Default		The following requirements are used to assess the security, efficiency, and maintain your container image quality	⋮
☐	Foundational Library Default		The following requirements are evaluated when you use this library	⋮
☐	Infrastructure assurance Default		Infrastructure assurance library	⋮
☐	Java Runtime Library Default		The following requirements are used to assess Java Runtime applications	⋮
☐	Message Queue Library Default		This library evaluates key non-functional aspects of message queue systems including throughput, reliability, scalability, and fault tolerance. It provides insights into system	⋮
☐	MongoDB Concert Metrics Library Default		The following requirements are used to assess MongoDB database instances using derived Concert metrics	⋮
☐	MySQL Concert Metrics Library Default		The following requirements are used to assess MySQL database instances using derived Concert metrics	⋮
☐	Node.js Concert Metrics Library Default		The following requirements are used to assess Node.js runtime applications using derived Concert metrics	⋮
☐	Runtime Production Readiness Library Default		The following requirements are used to assess the reliability and security of your workloads, as well as their adherence to Kubernetes best practices	⋮
☐	VM Integrity Assurance Library Default		The following requirements are used to assess VM health in terms of security, efficiency, and compliance	⋮

Items per page: 50 Items 1-10 < Page 1 >



www.vpbis.com | **ValuePath**