

The rapid growth of business applications has created fragmented data lakes and siloed tooling, increasing the costs and complexity of managing applications. Technology executives should consider a modern approach using AI-powered tools that provide a comprehensive view of application health.

Modern AI-Driven Automation Enables Application Resilience

April 2025

Written by: Jim Mercer, Program Vice President, Software Development, DevOps, and DevSecOps, and Stephen Elliot, Group Vice President, I&O, Cloud Operations, and DevOps

Introduction

In the modern digital economy, there is an insatiable appetite for secure digital experiences that new application architectures, operating models, and security methods can provide. Companies are increasingly adopting cloud-native technologies and microservices to stay competitive. However, managing a rapidly expanding collection of applications across multicloud environments has put IT teams on their heels as they grapple with growing staffing and business demands.

The scale and complexity of modern digital business applications are growing with increasing cross-dependencies and deployment platforms, including VMs and containers deployed by private, hybrid, and public multicloud scenarios. New organizational constructs, such as DevOps, platform engineering, and site reliability engineering (SRE), require teams to collaborate, share access to critical information, and better understand application dependencies across traditionally separate data silos. The need to improve application security and performance has never been greater as the C-suite recognizes that the technology architecture is now the business architecture.

While the cloud offers numerous benefits for driving scalability, resilience, and flexibility, it also introduces significant complexity to software development, security, management, and operations. This complexity will increase as underlying infrastructure expands to meet changing business requirements for security, compliance, time-to-market demands and, most recently, AI workloads. Most organizations have been trying to navigate these challenges using disconnected tools and practices across public, private, and hybrid cloud environments to streamline their cloud operations.

AT A GLANCE

KEY TAKEAWAYS

- » Organizations face rising application complexity and scalability challenges.
- » The growing digital economy and AI workloads are placing increased strain on application resilience.
- » Existing solutions are not capable of providing a complete picture of application health.
- » A modern approach combines existing tools with intelligent AI insights that provide information on application health across the silos of the modern application life cycle.

Application complexity permeates the entire software development life cycle (SDLC), from design and development to deployment and production. Increasingly, development teams must have a cursory understanding of security and performance requirements, owning some portion of responsibility for these mission-critical tasks. While shifting these types of tasks to developers may sound good, it is destined to fail without providing them with adequate support.

It is reasonable to estimate that several trillion lines of application code are currently in use, highlighting the massive scale organizations need to undergo to manage and maintain modern application portfolios. Without an understanding of the components that make up applications and how each one impacts the other, it is difficult to isolate problems before they cause a poor customer experience or unplanned downtime.

The growth of applications, code, and multicloud and hybrid cloud infrastructures is only placing a heavier burden on developers, SREs, and network engineers who need to troubleshoot, as well as operational teams that may be trying to manage costs. These teams must understand the costs across the complex sets of processes they support.

The C-suite is under pressure to do more with less and create competitive advantages with technology-driven capabilities. For example, understanding the best cost-effective cloud option for workloads is becoming a key requirement in many FinOps conversations. Providing a great, consistent customer experience through the delivery of high-performing digital services has become a driver of revenue and customer loyalty.

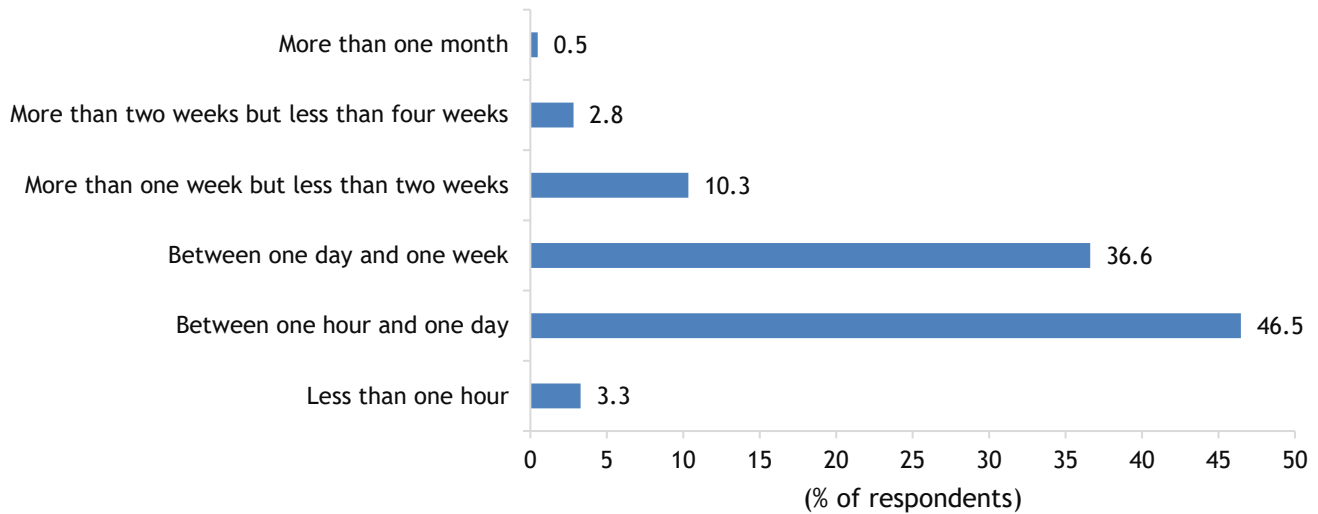
There is no holistic topological view of application risks, entities, and dependencies, leaving organizations to react to problems rather than proactively prevent them. The effort it takes to identify an issue, get the information to the best team, and solve (or prevent) problems has never been greater. The myriad teams and fragmented problems, incidents, and change management processes make it difficult to interpret all the complex data signals from applications and the tools that support and monitor them. Development, security, and operational processes are often the domain of separate teams with different and fragmented toolchains and data sources.

Each hour of an application outage can cost a business hundreds of thousands of dollars. Left unchecked, an outage can quickly add up to millions of dollars over a day. The person-hours spent trying to isolate application problems and develop a plan of action are a high operational cost to the business, with experienced developers making \$178,000 annually (source: [Payscale.com](https://www.payscale.com)). SREs tend to spend an inordinate amount of their time on problem and incident management rather than establishing the SRE practice in their technology organizations. IDC's November 2022 *AIOps and Observability Survey* estimated that an application outage costs a business about \$4.2 million per day, and for certain mission-critical applications, that amount may be significantly higher.

Figure 1 shows that despite modern software tooling efforts, just 3.3% of respondents attest to a mean time to restore (MTTR) of less than an hour when a production outage occurs. For most, MTTR takes hours, with over a third of the respondents (36.6%) indicating that it takes between a day and a week to restore an application service in production.

FIGURE 1: **Addressing Production Outages Takes a Significant Amount of Time**

Q What is the mean time to restore a service when a production outage occurs at your organization?



Source: IDC's DevOps Perceptions, Practices, and Tools Survey, November 2023

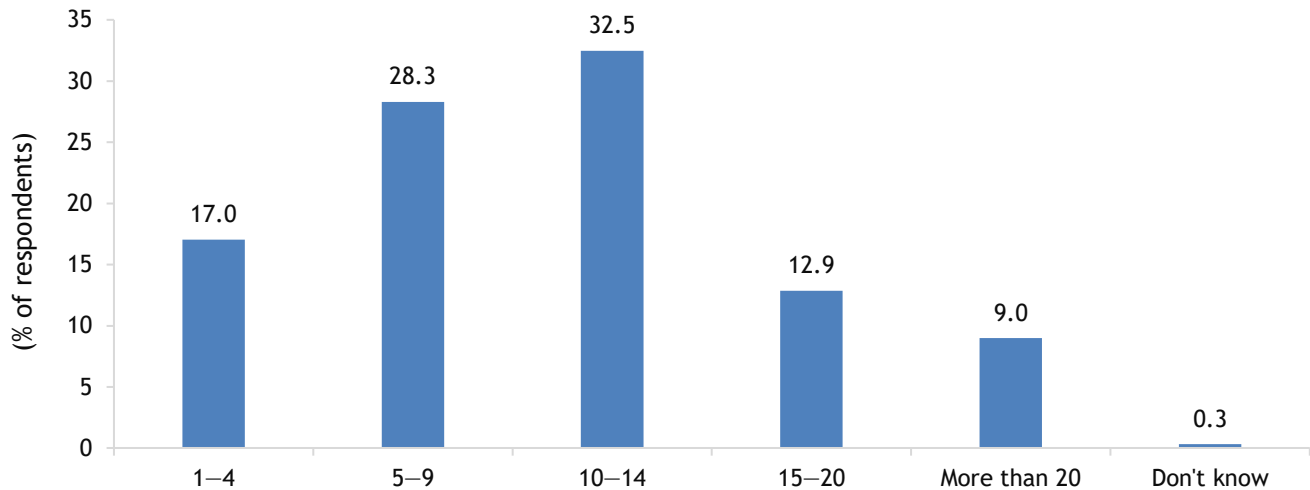
In most organizations, a significant portion of the responsibility for managing application complexity rests on a small group of highly skilled engineers and architects who often face the risk of burnout. These specialized skills are scarce, and developing the necessary expertise to understand and navigate intricate application architectures requires years of experience. This reliance on a limited talent pool can strain both the individuals and the organization, leading to the turnover of the most critical technical talent and highlighting the need for better strategies to address the mosaic of application components, resources, and dependencies.

The explosion of AI is introducing new workloads and adding significant pressure to existing application development and the creation of entirely new applications. This surge in AI-driven development not only complicates the architecture and maintenance of current systems but also necessitates new frameworks and tools to harness the potential of AI technologies effectively. Generative AI (GenAI) code generation makes code production faster than ever. However, 42% of developers indicated that their AI-generated code is often or always insecure, adding vulnerabilities to the application code that require remediation before deploying it into production (source: IDC's *U.S. Generative AI Survey*, April 2023).

Traditionally, organizations have attempted to keep pace with application complexity by adding new development, DevOps, security, and monitoring solutions. This approach has led to tool sprawl and siloed views of the application life cycle, each with a distinct set of insights that don't provide a holistic picture of application health. Figure 2 shows that most organizations attest to having 10–14 different tools just in the DevOps toolchain.

FIGURE 2: **Number of Different Tools Across the DevOps Pipeline**

Q Approximately how many different tools make up your organization's DevOps toolchains?



n = 311

Source: IDC's DevOps Perceptions, Practices, and Tools Survey, November 2023

Further, data from another survey shows that organizations also used 10–14 different DevSecOps tools (source: IDC's *DevSecOps Adoption, Tools, and Techniques Survey*, 2023). If we speculate that the numbers are similar for monitoring and observability, network management, and software development, organizations use 60 distinct tools across the application life cycle.

Siloed tools and environments and data complexity significantly hinder the development of revenue-generating applications. When teams must navigate disjointed systems and fragmented data, productivity drops as they spend more time managing these inefficiencies than on innovation and strategic growth. This compartmentalization creates barriers to collaboration and slows the decision-making process, detracting from the core objective of delivering value to the business through profitable applications.

For example, software composition analysis (SCA) tools build software bills of material (SBOM) and identify discovered common vulnerabilities and exposures (CVEs), but not all of them require the attention of development teams. Conversely, in a distributed cloud-native application, the SBOM may not accurately represent all application risks, leading to an inaccurate understanding of the true application risks. With an overwhelming number of findings and limited developer time, it becomes challenging to determine which issues need fixing, should be added to the backlog, and/or can be safely whitelisted. This situation underscores the need for better prioritization and risk assessment to ensure efficient use of developer resources.

It is no wonder that application security breaches have increased by 21% year over year from 2022 to 2023 (source: IDC's *DevSecOps Adoption, Techniques, and Tools Survey*, January 2023). This surge in security breaches illustrates the challenge organizations face in trying to fix the CVEs that truly put them at risk. Despite a wealth of data across a cacophony of security tools, organizations lack end-to-end visibility into the real application risks that they need to prioritize and remediate because it's a data swamp with too much noise and not enough signal.

While the metadata around applications is already available, it is often siloed in different tools and data sets, preventing organizations from proactively managing and controlling application resilience. This fragmentation leads to a disjointed view of critical information, hindering the ability to anticipate and respond to potential issues.

Organizations don't need to replace existing tools — they usually have enough. They need to modernize how they use them to proactively and intelligently address application risks that can threaten the business and its end customers.

Benefits

A New Approach to Application Resilience and Transparency

New management solutions that leverage existing organizational tool investments and AI will be essential to help organizations rethink how they deliver and build modern cloud-native applications. Instead of adding more tools, the focus must be on adding intelligence. By simplifying and optimizing application resilience through modern AI technology, organizations can proactively identify points of failure and address problems before they escalate into crises. This approach of leveraging AI enhances organizational resiliency and ensures that current tooling investments are maximized, providing a smarter, more efficient pathway to maintaining robust and reliable applications.

AI can capture the knowledge of the most experienced engineering staff, enabling interactive and automated capabilities across the application ecosystem. This advanced level of AI reasoning democratizes application management, allowing less experienced engineers to succeed and effectively manage a greater number of applications. By embedding expert knowledge into AI systems, organizations can ensure consistent application of critical insights and best practices, leading to more efficient and scalable management processes.

An intelligent approach to application management can significantly reduce application runtime costs by optimizing resource utilization and minimizing downtime. Integrating AI-driven insights and automation into the application management process preserves valuable engineering time, as engineers are no longer bogged down by the tedious task of isolating and remediating problems that application intelligence could have preemptively addressed. This proactive strategy identifies and resolves potential issues before they escalate, reducing the likelihood of costly disruptions. Consequently, organizations can allocate their engineering talent toward innovation and strategic initiatives rather than routine troubleshooting, resulting in cost savings and improved productivity.

Using an intelligent approach can strengthen feedback loops, effectively prioritizing operational application issues in the backlog based on their risk levels. By accurately assessing and categorizing these issues, development teams can focus on addressing the most critical problems first, thereby optimizing their efforts and resources.

Intelligently Manage Risk

Shifting from a narrow focus on output from point solutions to a comprehensive view of applications across diverse cloud environments and operational toolsets can further enhance efficiency. By adopting this approach, organizations can streamline operations and optimize resource allocation.

An intelligent approach to application management can significantly reduce the costs associated with developing and managing applications by optimizing resource utilization and minimizing downtime.

By leveraging discovery capabilities, organizations can ingest data from their existing tools, enabling them to use the discovered intelligence to adopt a risk-based strategy to enhance their application security and resilience postures. This strategy involves providing intelligent recommendations for remediation or acceptance of identified risks and identifying the root causes of security vulnerabilities based on the evolution of the application and its supporting infrastructure. Furthermore, organizations can prioritize potential risks based on factors such as operational impact, including blast radius, tier, and external exposure.

A couple of examples of improved resilience due to using AI across the application life cycle are:

- » Comprehensive monitoring between APM and ITSM solutions. For instance, being able to cross-reference application availability metrics from APM tests against IT tickets in the ITSM solution helps unearth resilience gaps that need to be further investigated with the APM tool.
- » Guaranteeing compliance with crucial security and privacy controls, such as NIST 800-53 and CIS benchmarks, entails tracking the drift of compliance standards over time and evaluating the potential impact of various remediation options. This analysis enables organizations to maintain a robust security posture while mitigating risks effectively.
- » Gaining insights into expiring application certificates prevents costly outages. These digital documents authenticate the identity of applications, servers, or users and facilitate encrypted communication, but when they expire unexpectedly, costly disruptions can occur. Organizations need to manage certificates proactively by prioritizing renewals based on their severity impact to prevent application downtime and ensure operational continuity.

Trends

As application and data growth accelerate, the challenges posed by increasing data variety, volume, and complexity are becoming more pronounced. IDC forecasts that over 1 billion new logical applications will be created by 2028 (see *1 Billion New Logical Applications: More Background*, IDC #US51953724, April 2024). These new applications will be distributed in nature using AI services, which will only exacerbate the existing complexity dilemma.

The emergence of GenAI and code generation, coupled with the intricate web of application interdependencies, will cause the complexity of technological challenges to grow exponentially. As AI advances and intertwines with the software development processes, the landscape becomes increasingly intricate, demanding innovative solutions to navigate and address the complexities effectively. This exponential growth underscores the pressing need for organizations to stay ahead of the curve by embracing cutting-edge technologies and methodologies, equipping themselves to tackle the evolving challenges of the new digital era head-on.

Considering IBM Concert

Originally designed to address IBM's internal application challenges, IBM Concert is the intelligence layer that unifies fragmented application data, transforming it into AI-driven insights and automated actions to strengthen risk and resilience. With built-in workflows, IBM Concert enables users to build automation that mitigates vulnerabilities, optimizes resilience, and promotes continuous application stability according to their unique architecture. It delivers a comprehensive, 360-degree view of application health, performance, and risk — turning insight into action at an enterprise scale.

Key capabilities of IBM Concert include:

- » **GenAI at its core:** Leverage GenAI to analyze and turn application data into strategic insights and recommendations.
- » **App360:** Consolidate information from various monitoring and analytics tools to present a unified dashboard, giving the user the power to address vulnerabilities, resilience gaps, compliance issues, expiring certificates, and more.
- » **Automated actions:** Unlock the full potential of applications with AI-driven automation, delivering precise recommendations, seamless integrations, and proactive actions to ensure optimal resilience and performance.
- » **Amplify existing automations:** Incorporate RPA tools, BPA tools, scripts, and other automation assets into larger workflows, maximizing existing investments in automation.

IBM Concert integrates with a company's existing tools, technology stacks, and vendors across the application life cycle, requiring no disruptions to existing teams. It enables organizations to optimize operations and leverage tailored insights for informed decision-making using the tools they already own. IBM Concert helps application owners, SREs, and users:

- » Operationalize risk and resilience by collecting and correlating data from multiple sources, providing a comprehensive view of an organization's posture.
- » Increase efficiency with prioritized insights and action-oriented recommendations with automated remediation to lower mean time to resolution.
- » Improve application awareness by understanding the dependencies and connections that make business applications tick.
- » Achieve enhanced security that focuses resources on the risk factors with the most significant impact on their applications.

IBM Concert App 360 provides a baseline view of an application that spans development, security, and IT operations, including:

- » Topology map of information flows and asset and workload locations across environments and toolsets (Arena view)
- » Data collection repository (Evidence store)
- » Application change log

IBM Concert uses application intelligence as a baseline and transforms how application owners and SREs address the risk and resilience management of business applications via:

- » **Resilience:** Unlock a new standardized and repeatable approach to application resilience using AI-powered insights.

- » **Vulnerabilities:** Minimize application security risks and speed up resolution by eliminating false positives and duplicates and prioritizing CVEs based on impact.
- » **Certificates:** Streamline certificate management by highlighting impending expiration and policy violations.
- » **Compliance:** Ensure continuous compliance with evolving security standards while minimizing resource use and maximizing security integrity.

Further, IBM Concert produces recommendations for each application phase (development, build, integration, deployment, operate, etc.) across the SDLC. The AI Assistant interface allows users to question those recommendations, gather additional context, and dig deeper to uncover things such as:

- » **AI-powered workflows:** IBM Concert Workflows provides an AI-powered automation engine that generates recommended workflows that users can quickly adapt to the nuances of their architecture. Concert Workflows allow enterprises to cover the full vulnerability life cycle, from identification to resolution, enabling scalable fixes across hybrid IT environments.
- » **App-centric insights:** IBM Concert collects and presents information at the application level, delivering insights that transcend infrastructure silos.
- » **App-centric prioritization:** IBM Concert analyzes connections, dependencies, and priorities within applications, presenting priorities based on real impact.
- » **Instant context:** The IBM Concert AI-driven UI provides the ability to instantly investigate the context of risk findings without building new data pulls or dashboards.

Challenges

IBM Concert is a new solution and approach to ensuring application resilience, but it faces the following challenges:

- » Competition exists with other observability and security monitoring solutions. Application topology mapping has been a staple in many observability solutions, but its data reach and security knowledge are limited.

IBM will need to articulate that IBM Concert is not meant to replace or compete with existing point solutions, discuss how it is designed to "meet you where you are," and highlight the key differences in the scope of the provided insights. It is critical to understand that IBM Concert is using a modern GenAI (watsonx) framework to enable organizations to scale and ensure the resilience of their application life cycle. The true value of IBM Concert is its ability to ingest metadata and turn it into knowledge about your application and business.

- » Data collection across the application life cycle, with a contextual understanding of security and performance requirements, is traditionally challenging and invasive.

Most solutions that rely on data collection depend on agents that need to ride along with the application workload. IBM Concert does not come with the overhead of a data collection agent taking advantage of readily available APIs to ingest information from the tools already in place across the entire application life cycle.

- » Cultural resistance to relying on AI intelligence and the ability to maintain accurate topologies with fast-changing data sources and application architectures pose challenges.

Most of this resistance is derived from the fear of job insecurity and feeling uncomfortable with using modern solutions. While these people problems are often more challenging than the technical ones, IBM needs to help organizations get their teams on board with the understanding that AI will not replace humans — humans who use AI will replace those who don't (thus it is good for their careers).

- » It will be challenging to bring disparate teams together to agree on a common outcome and dedicate time to data quality and ingestion requirements. Executives must commit to leading these projects for common objectives.

The IBM Concert buyer is not a single group, but it is all the groups and disciplines making up the application life cycle. When a prospective customer has very siloed teams, it may behoove IBM to lean into one particular area of the application life cycle to get some early buy-in and use that success to expand usage across the other teams in the application life cycle.

Conclusion

The explosion of new applications and the exponential growth of data have made managing applications increasingly complex for organizations, many of which are ill-equipped to keep pace. This growing complexity, coupled with poorly managed applications, often leads to frustration and costly production outages that have significant financial repercussions. As businesses adopt new organizational constructs such as DevOps, platform engineering, and SRE, the need for advanced collaboration and tools becomes evident. These teams must work together effectively to navigate the intricacies of modern application environments and ensure seamless operations.

New management solutions that integrate AI with existing tool investments, such as IBM Concert, are essential for modernizing cloud-native application management. This intelligent approach reduces costs by optimizing resource utilization and minimizing downtime and provides a comprehensive view of applications across diverse environments, allowing for better risk prioritization and streamlined operations. Therefore, organizations should consider how IBM Concert can help them manage the increased number of applications and complexity of the future by modernizing their application management practices.

About the Analysts



Jim Mercer, Program Vice President, Software Development, DevOps, and DevSecOps

Jim Mercer is a program vice president managing multiple programs spanning application life-cycle management (ALM), modern application development and trends, emerging generative AI software development, DevOps, DevSecOps, open source, PaaS for developers, and cloud application platforms. His focus areas are DevOps and DevSecOps Solutions research practices. In this role, he is responsible for researching, writing, and advising clients on the fast-evolving DevOps and DevSecOps markets. Mr. Mercer's core research includes topics such as rapid enterprise application development, modern microservice-based packaging, platform engineering, GitOps, application security, software supply chain security, and automated deployment and life-cycle/management strategies as applied to a DevOps practice.



Stephen Elliot, Group Vice President, I&O, Cloud Operations, and DevOps

Stephen Elliot manages multiple programs spanning IT operations, enterprise management, ITSM, agile and DevOps, application performance, virtualization, multicloud management and automation, log analytics, container management, DaaS, and software-defined compute. Mr. Elliot advises senior IT, business, and investment executives globally in the creation of strategy and operational tactics that drive the execution of digital transformation and business growth.

MESSAGE FROM THE SPONSOR

Apps without knowledge gaps with IBM Concert

Powered by watsonx, IBM Concert connects disparate application data and transforms it into actionable insights with AI-powered remediation for risk and resilience. IBM Concert brings a new level of intelligence to your observability, risk and resilience strategy, helping you achieve greater control, security, and efficiency in managing your applications.

Learn more about IBM Concert by [visiting our webpage](#).



The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use, and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)