

# NEW BMC HELIXGPT ENHANCEMENTS RESOLVE NETWORK ISSUES AND VULNERABILITY AND CHANGE RISKS



Having the right contextual data is crucial for resolving network issues and understanding which security vulnerabilities to fix first, before they get exploited by bad actors. Additionally, assessing potential system and software changes by analyzing historic change data and current operational data can help prevent risky changes that are likely to cause issues.

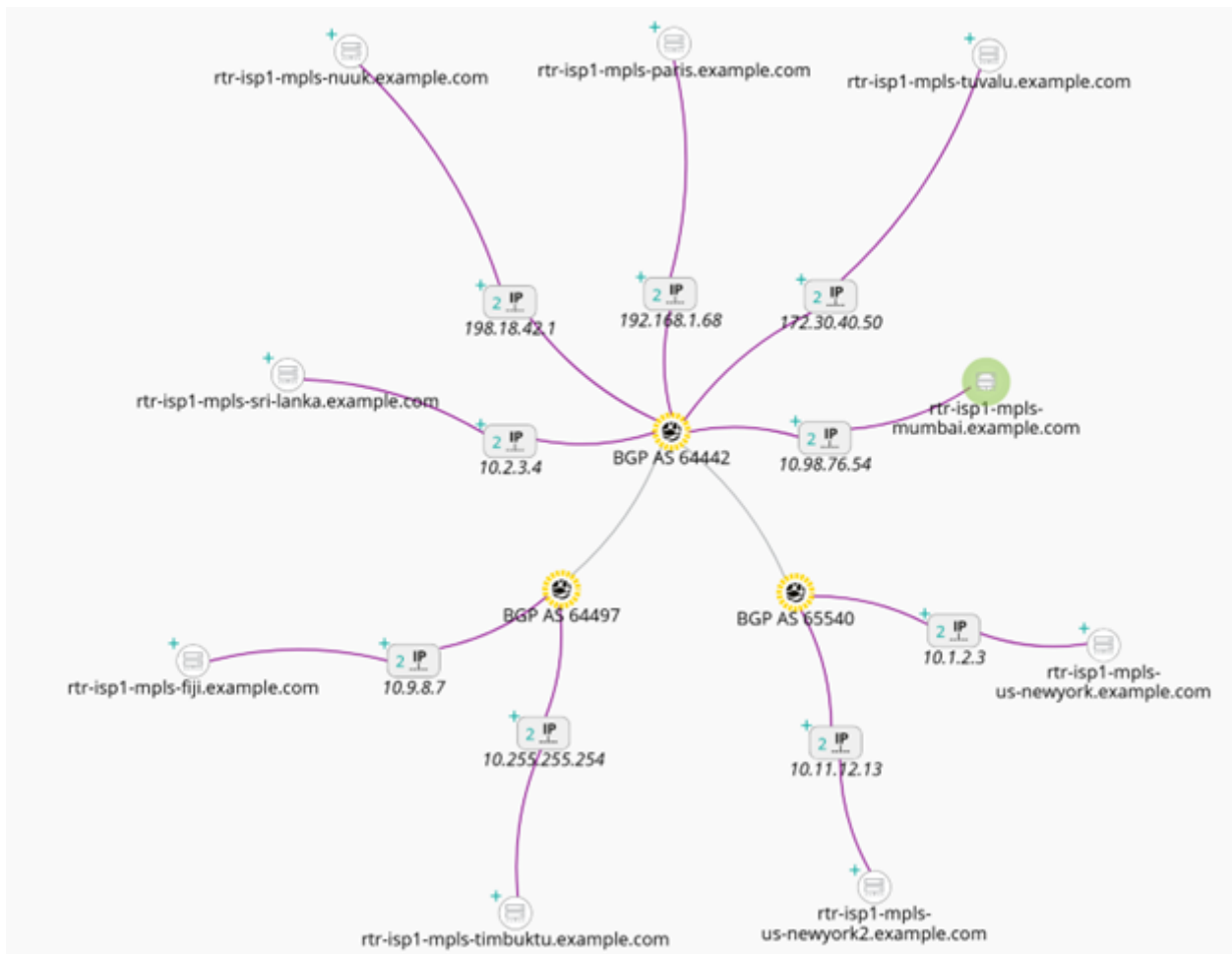
The latest BMC Helix ITOM 25.1 release helps network operations, IT operations (ITOps), and DevOps teams resolve network and cloud issues faster, address critical vulnerability risks with less manual effort, and reduce change failures with new key enhancements:

- **Network topology infrastructure discovery**—Discover network topology using BGP protocol and Oracle Cloud Infrastructure hosts faster using existing cloud API scans and credentials.
- **New just-in-time integrators for ServiceNow, Jira, Splunk, and Elastic**—Get artificial intelligence (AI)-driven insights, summaries, and recommendations for incidents from BMC Helix ITSM, ServiceNow, and Jira, plus situational log insights for a larger set of log data from BMC Helix Log Analytics, Splunk, and Elastic tools.
- **BMC HelixGPT Vulnerability Resolver**—Consolidate vulnerability data get a unified view of vulnerabilities impacting critical business services, and speed recommended remediations for those vulnerabilities with a built-in AI agent.
- **BMC HelixGPT Change Risk Advisor**—Identify risky changes for change managers and DevOps engineers by analyzing operations and service management data with the integrated AI agent.

# Network topology infrastructure discovery

Incomplete network topology discovery leads to poor network visibility and inaccurate root cause correlation. Insufficient visibility into complex network infrastructure makes it difficult to troubleshoot, identify issues, and perform root cause analysis. Incomplete topology combined with inaccurate correlation of network events can lead to misinterpretation of network issues and ineffective troubleshooting.

BMC Helix now discovers network logical topologies using Border Gateway Protocol (BGP) across IT infrastructure spanning data centers, campuses, and branches, etc. This functionality enables the BMC Helix platform to provide comprehensive network visibility and accurate root cause correlation across complex enterprise infrastructures for network operations managers and network engineers. Additionally, a new feature that discovers all cloud hosts in Oracle Cloud Infrastructure (OCI) via cloud APIs has been introduced. This enables network operations and ITOps to get a detailed discovery of these hosts without relying on IP-based SSH/PowerShell-based scans. Since it uses existing cloud credentials, it reduces the operational overhead and complexity of managing individual host credentials.

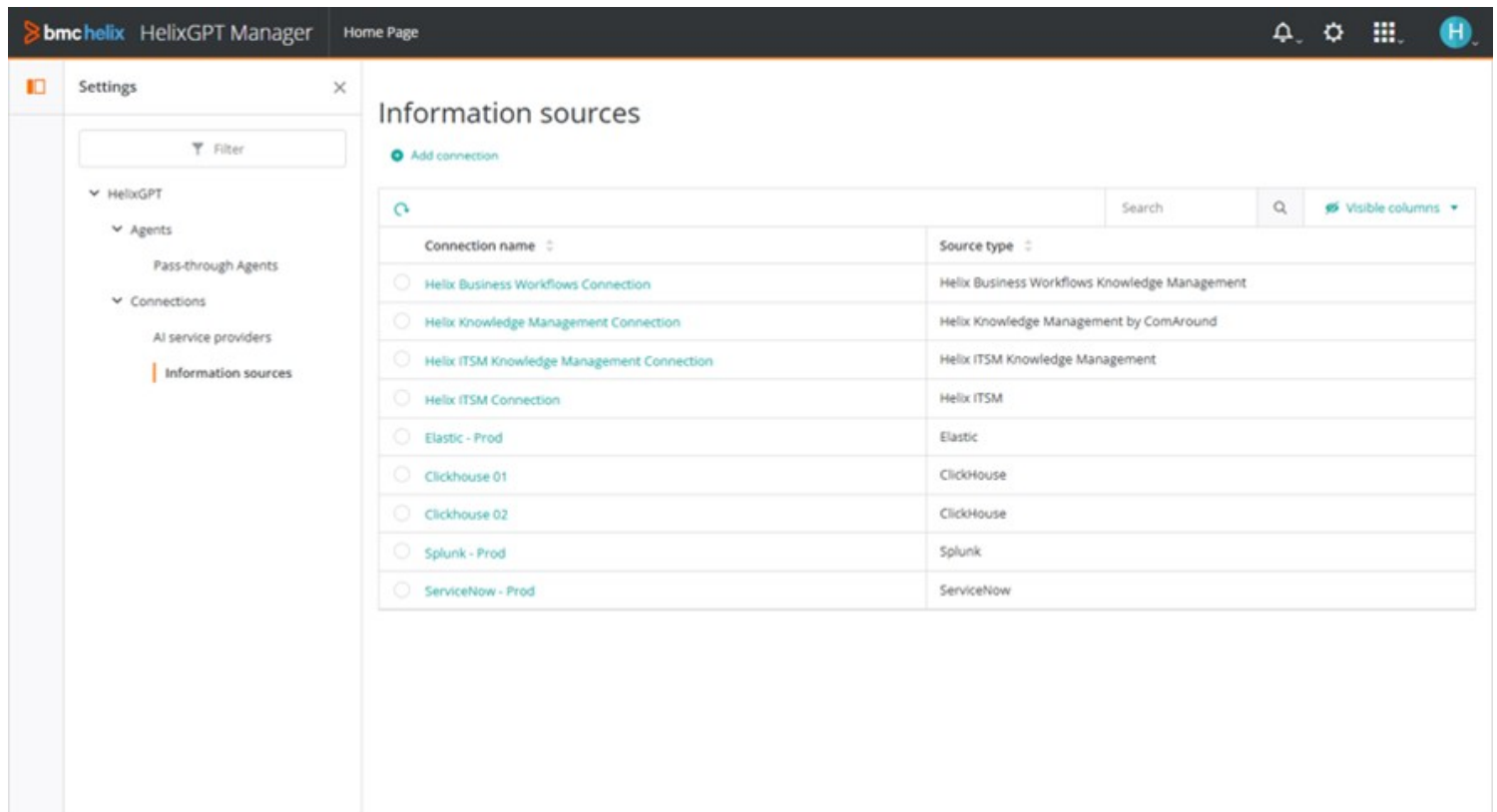


Network topology infrastructure discovery

## New integrators for ServiceNow, Jira, Splunk, and Elastic

Some of the most exciting capabilities of BMC Helix AIOps are the solution's ability to interact with a wide variety of tools and data to generate insights and execute tasks in a proactive manner. In the 25.1 release, new just-in-time integrators for ServiceNow and JIRA bring incident data into BMC Helix

AIOps to provide insights, summarization, and recommendations to fix production issues. The integrators for Splunk and Elastic enable BMC Helix AIOps to analyze just-in-time log data from Splunk and Elastic. This provides comprehensive, enterprise-wide log insights and a better understanding of trends and patterns within log data to identify the root cause of system issues.



BMC HelixGPT Just-in-Time Integrator Manager

## BMC HelixGPT Vulnerability Resolver

Security operations (SecOps) teams are responsible for identifying security issues for DevOps teams to fix. However, these security issues are so numerous, that it's difficult for DevOps teams to prioritize which issues to fix first. BMC HelixGPT Vulnerability Resolver, an AI agent within BMC Helix AIOps, helps security operations and DevOps teams improve compliance and risk management by providing: A risk view: Display vulnerability risks side by side and in context of the service health in the "Risks" tab within the BMC Helix AIOps UI.

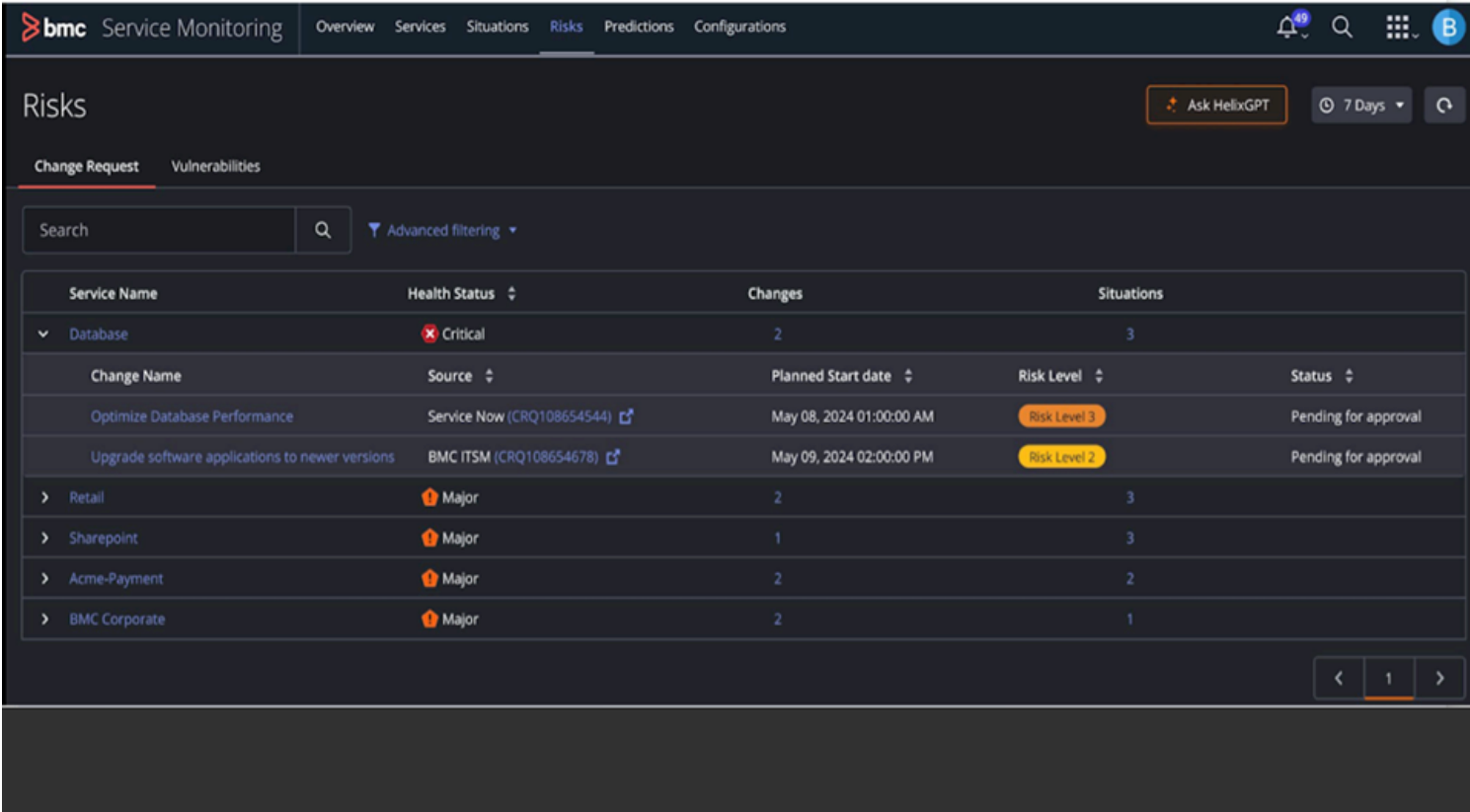
- **Criticality insight:** Help IT teams understand the impact on business services and enable them to prioritize remediation.
- **Vulnerability Best Action Recommendation (VBAR):** Get faster recommended remediations for critical vulnerabilities.

BMC HelixGPT Vulnerability Resolver enables DevOps teams to prioritize the order of vulnerability issues to fix, create remediation tickets for each affected asset in one click, and resolve vulnerabilities through patching or updating configuration changes.

# BMC Helix GPT Change Risk Advisor

Changes are the largest source of production issues. Most organizations don't have a single approach to delivering changes, which increases the risk of introducing bugs or performance issues in production. In the traditional change approval process, the change advisory board (CAB) makes the final decision to approve or reject proposed changes by performing risk analysis and directing the implementation of changes. For DevOps teams pushing thousands of changes daily, the CAB process is simply too slow, so DevOps teams follow their own practice of using automation and tooling to merge code changes and automate testing steps to deploy changes more frequently.

The recently announced BMC HelixGPT Change Risk Advisor is an AI agent designed to guide change management and DevOps teams in deploying system and software changes more rapidly and reliably. Change Risk Advisor analyzes historic change data and current operational data to present a change risk score so that change management, DevOps, platform engineering or site reliability engineering (SRE) teams can quickly assess the risk of making a change prior to putting it in production.



The screenshot displays the BMC HelixGPT Change Risk Advisor interface. At the top, there's a navigation bar with 'Service Monitoring' and tabs for 'Overview', 'Services', 'Situations', 'Risks', 'Predictions', and 'Configurations'. The 'Risks' tab is active. Below the navigation, there's a search bar and an 'Ask HelixGPT' button. The main content area shows a table of risks with columns for Service Name, Health Status, Changes, and Situations. The table is filtered to show 'Change Request' and 'Vulnerabilities'. The table lists several risks, including 'Database' (Critical), 'Retail' (Major), 'Sharepoint' (Major), 'Acme-Payment' (Major), and 'BMC Corporate' (Major). Each risk entry includes a change name, source, planned start date, risk level, and status.

Service Name	Health Status	Changes	Situations	
Database	Critical	2	3	
Change Name	Source	Planned Start date	Risk Level	Status
Optimize Database Performance	Service Now (CRQ108654544)	May 08, 2024 01:00:00 AM	Risk Level 3	Pending for approval
Upgrade software applications to newer versions	BMC ITSM (CRQ108654678)	May 09, 2024 02:00:00 PM	Risk Level 2	Pending for approval
Retail	Major	2	3	
Sharepoint	Major	1	3	
Acme-Payment	Major	2	2	
BMC Corporate	Major	2	1	

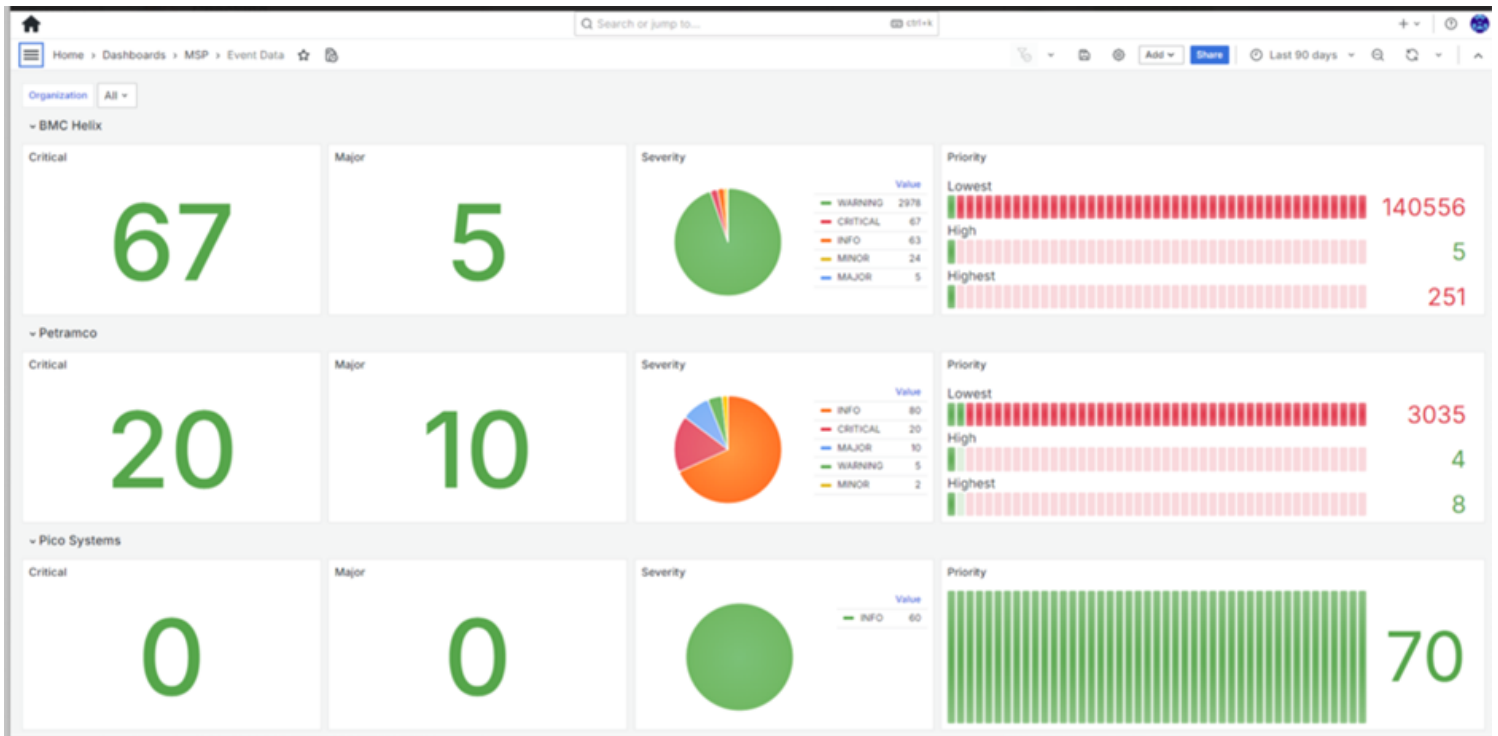
BMC HelixGPT Change Risk Advisor.

## New configurable dashboards for managed service providers (MSPs) and multi-tenancy users

In addition to all of the great new capabilities added to BMC Helix ITOM, MSPs or large organizations running multiple tenants of BMC Helix now have a dashboard view of critical issues across their tenant instances of the software that gives IT organizations:

- Visibility into critical data, including separate panels for each instance.
- The ability to look across hundreds of tenant instances for better and faster issue alerting and

response.



BMC Helix multi-tenant dashboard.

To learn more about how these new BMC Helix capabilities can help you transform your IT operations, [contact us for a consultation](#).