

AI Ops and observability for the AI era: 6 key capabilities

Explore the technology that powers BMC
Helix AI Ops and observability

Table of contents

- 03** Executive summary
- 04** Digital transformation: How AIOps overcomes four critical challenges
- 05** Key capability #1: Service-centric probable cause analysis
- 07** Key capability #2: Cross-domain event ingestion and correlation
- 09** Key capability #3: Pattern recognition and clustering
- 11** Key capability #4: Automated asset discovery and dynamic service modeling
- 13** Key capability #5: Major incident prediction
- 14** Key capability #6: Remediation and automation
- 15** AIOps and observability for the AI era

Executive summary

Artificial intelligence for IT operations, or AIOps, is a paradigm shift that allows machines to resolve IT issues with human oversight.

It is a multi-layered technology that enhances the operations of IT by using machine learning (ML) and advanced analytics to analyze big data sets obtained via different monitoring tools to help proactively detect and recommend fixes to system and application performance issues.

Despite solutions that help IT operations (ITOps) teams respond to events and alerts such as correlating, auto-ticketing, and war room troubleshooting, they require significant resources to staff, develop, and maintain. None provides asset management and capacity planning capabilities to balance the need to do more with less.

From operations overload to strategic control, BMC Helix AIOps solutions support IT teams by automating ITOps while providing human oversight in a collaborative model. With a system of AI agents (agentic AI) that provide proactive assistance in root cause analysis, incident response, and risk remediation, organizations prevent issues and improve business resilience without expanding the team size. This frees up skilled resources to focus on strategic work that drives transformation. It also closes the skills gap by providing junior staff with on-the-job guidance.

With an open AI platform that includes observability and integrated ITSM workflows, BMC Helix AIOps maximizes operational efficiency, strengthens compliance, and multiplies productivity. Let's take a closer look.

Digital transformation: How AIOps overcomes four critical challenges

Digital transformation is essential for competitive differentiation and growth. If companies aren't already introducing the latest digital services and business models that customers demand, they're working quickly to do so. This puts unprecedented pressure on IT to play a more strategic role in the organization—and introduces significant challenges.

AIOps can solve many of the common issues experienced by IT teams as they navigate digital transformation and expand their strategic role. With an open AIOps approach, you can:

Break down data silos

For many organizations, the inability to manage large volumes of data is a key reason they haven't been able to monitor events and systems effectively. With a dynamic and rationalized graph database of your IT landscape, where all types of ingested data (metrics, events, logs, traces, topology, changes) are normalized and modeled into a service model, AIOps breaks down silos for faster root cause analysis.

Eliminate operational noise

Event noise is a major concern for ITOps teams because it creates alert fatigue, decreases IT team productivity, and increases mean time to restore (MTTR), which causes higher operating costs, performance and availability issues, and risks to the business. AIOps reduces event noise by correlating incidents and providing visibility into the true source(s) of the problem.

Deliver a seamless customer experience

Ensuring a seamless customer experience with predictive analytics is an important business objective. AIOps makes complex automated decisions by proactively collecting and analyzing data. By leveraging this data, it can assess impact and predict future events that may affect availability and performance.

Upskill ITOps staff

As the IT tech stack continues to evolve, it is becoming increasingly difficult to find professionals with the up-to-date expertise to implement and manage these tools effectively. AIOps solutions with agentic AI capabilities have the potential to eliminate human toil for site reliability engineers (SREs) and DevOps engineers and fix the skills gap by providing on-the-job training for junior IT staff members.

Key capability #1: Service-centric probable cause analysis

Probable cause analysis provides proactive, automated determination of root causes across business services to cut through the noise and reduce MTTR. It enables operations teams to learn how the infrastructure is configured and understand the relationships between applications, networks, and infrastructure, and provides the most likely cause as a starting point for investigation. With AIOps, you can:

- View the top-scored causal configuration items (CIs) and related events for any impacted service.
- Determine probability based on time, metrics, events, changes, and topology.
- Change the time window to view how the probability has adjusted over time.
- Drill down into full analysis details including events, metrics, changes, and topology.

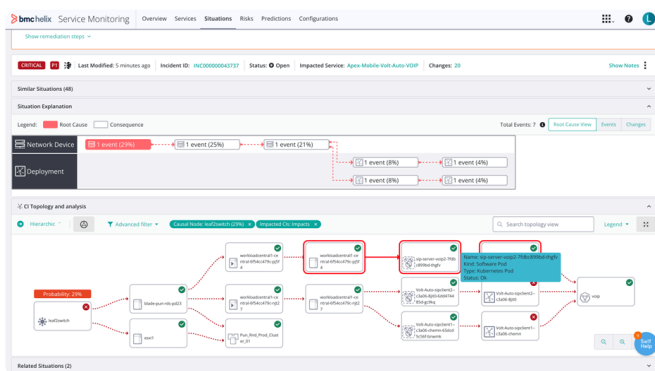


Figure 1. A visual map clarifying the relationship of a service and its impact.

How it works: Identifying probable cause with an algorithm

Service-centric probable cause analysis is a key differentiator for BMC Helix AIOps and observability. The solution helps operations teams understand the top-scored causal CIs and related events for any impacted service to determine the most likely root cause(s) of a potential problem or issue.

The analysis is extensive and factors in time, metrics, events, changes, and topology. Operations teams can also view how the probability has changed over time and drill down into the details.

The algorithm works in three phases, each impacting how the system identifies an accurate probable cause:

- 1. Collect.** First, it collects all the relevant data such as events, metrics, logs, incidents, and change requests across the topology in the dynamic service model. Ingestion of changes through integration with BMC Helix IT Service Management (ITSM) is built into the solution.
- 2. Rank.** Next, it runs a ranking algorithm that uses criticality, time proximity, graph depth, and cardinality factors to determine the causality rank order of nodes and events.
- 3. Learn.** Finally, it uses ML and statistical models built from feedback and historical causality analysis to classify nodes and events that are causal. This improves accuracy for both the probable causes and their statistical probability.

Topology

The topology for a technical/application service clarifies the relationships between infrastructure, applications, and services. The correlation includes millions of data points like topology, performance metrics, events, logs, changes, and baselines. Nodes that are “deepest” or “lowest” in the graph of a service will usually have a higher causality than upstream nodes closer to the service node. For example, database or network devices that are typically the deepest nodes in the service model would have a higher rank than the other dependent nodes above them.

The second aspect of topology is understanding the cardinality of relationships from each node, usually called centrality in graph theory. The higher the number of relationships from a node, the higher the probability that it is a causal node.

Ranking

The ranking algorithm in BMC Helix AIOps takes a multi-dimensional factor approach that evaluates each node and event across factors such as time, priors, and graph parameters like depth and cardinality to get an accurate score. Usually, events and changes that are closer to the service degradation have a higher causality than events that happened several hours or days earlier. A weighted score based on numerous experiments accounts for these factors.

Feedback and historical cause analysis

Using probabilistic methods on historic data, BMC Helix AIOps analyzes the past patterns of causality and outages for each node and identifies the “most causal” or “most failure-prone” nodes. The feedback from the past event patterns is used as ground truth for training a classifier to determine whether a given event on a node is the cause. Combining this with the ranking algorithm provides enhanced accuracy for identifying root causes.

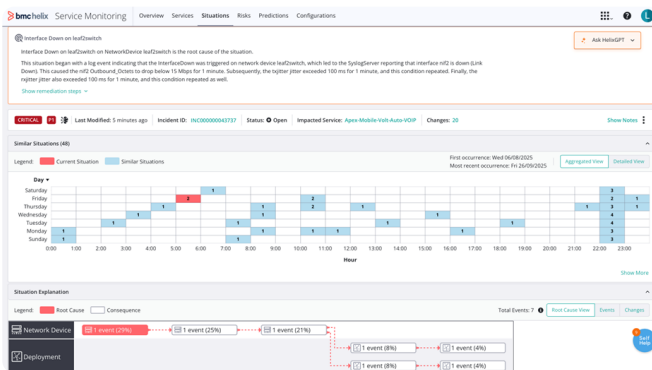


Figure 2. Identifying the causal nodes with clear explanation.

Key capability #2: Cross-domain event ingestion and correlation

BMC Helix AIOps supports a wide variety of integrations and REST APIs to streamline data ingestion from multiple monitoring tools or sources, including infrastructure, network, application, and monitoring tools for cross-domain analysis.

The solution collects events, incidents, changes, telemetry, and topology data from BMC Helix and third-party products across hybrid environments, normalizing and processing them through AI/ML to reduce event noise and correlate with application topology and business services for faster root cause analysis.

How it works: The situations algorithm

BMC Helix AIOps uses ML to correlate events into meaningful situations or incidents based on patterns of textual similarity, time-based proximity, topology context, and multi-dimensional, attribute-level matching among events. For example, it can group events by service, topological and temporal proximity, event co-occurrence, host, and textual similarity in a situation. The events used for generating situations can originate from multiple sources, such as applications, networks, or infrastructure.

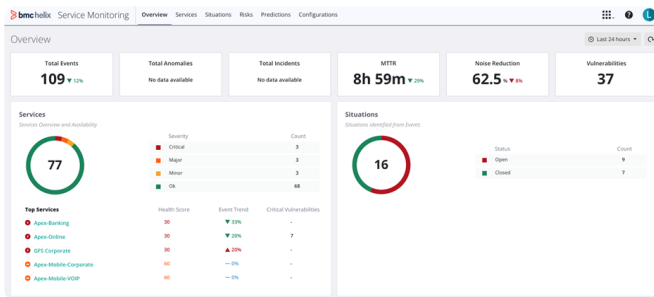


Figure 3. Situations or incidents identified from correlated events.

The algorithm works in five phases:

- 1. Group.** As events are ingested, they are first combined into distinct groups based on “group by” fields, which can be a service field or any other categorical field. This allows users to have control over the scope of events to which the clustering algorithm will be applied and ensures that clusters stay within certain boundaries (e.g., only within same service).
- 2. Embed.** Next, the system generates a vector representation of the event using advanced embedding techniques that can include text, TF-IDF, Google BERT, graph, or contextual knowledge-driven embedding techniques. Its uses offline methods to learn embeddings based on historical data.
- 3. Search.** It compares the vector representation of the new event with the representations of the other events in situations to determine cluster membership. This step can result in new situations or evolve existing ones by continuously adding new events to it.

4. Title generation. The system generates meaningful titles for the clusters based on topic-modeling algorithms.

5. Situation lifecycle state management. As events change state, get added to a situation, or time elapses, the state and severity of the situation changes along with it. For example, a situation will be closed when all events in the situation are closed. A situation can also close after a configurable period of time if no new events are added. Using both time and state of events influences the state and severity of a situation.

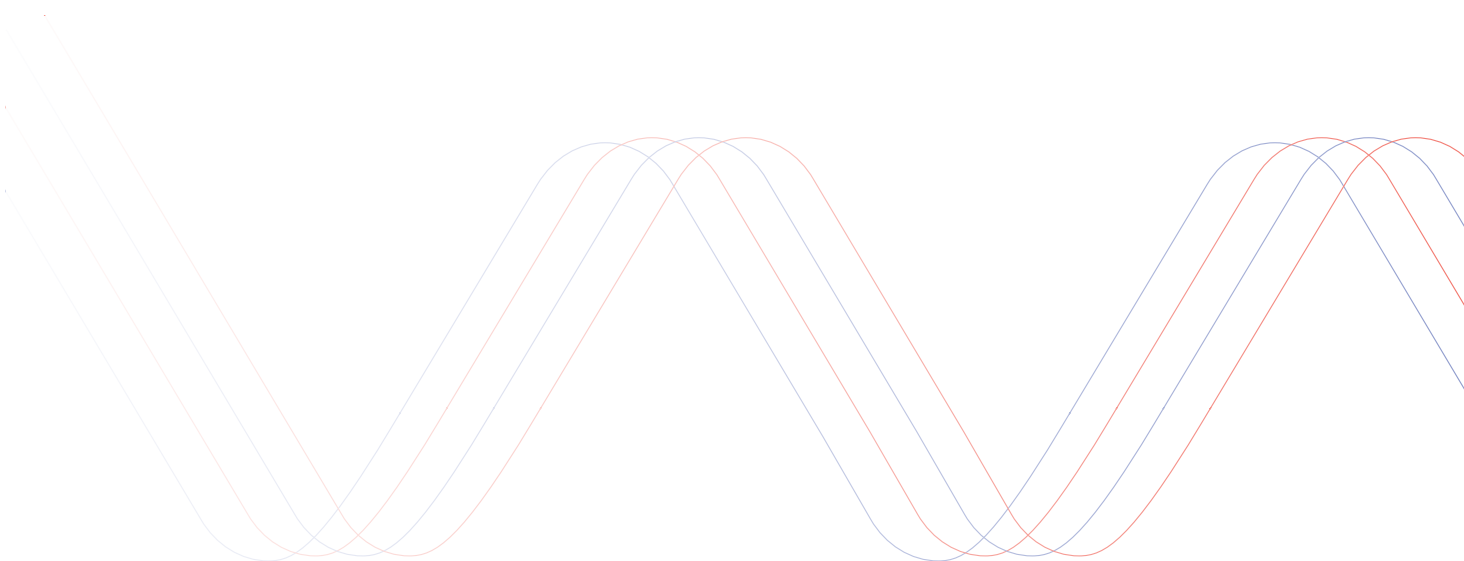
Situations	Occurred	Similar Situations	Related Situations	Type	Severity	Priority	Status	Incident ID	Automations	Action
Apex Mobile-Core-Network-South - Log event in...	8 hours ago	-	2	-	CRITICAL	P1	Open	INC00000043855	-	-
Apex Online-Core-Network - Log event interfac...	8 hours ago	-	2	-	CRITICAL	P1	Open	INC00000043756	-	-
Apex Mobile-Vish-Auto-VDSP - Log event interfac...	9 hours ago	49	-	7	CRITICAL	P1	Open	INC00000043757	-	-
Apex Mobile-Core-Network-South - Log event in...	9 hours ago	49	-	3	CRITICAL	P1	Open	INC00000043802	-	-
Apex Online-Core-Network - Log event interfac...	9 hours ago	53	-	7	CRITICAL	P1	Open	INC00000043756	-	-
Apex Online-Core-Network - Log event interfac...	9 hours ago	53	-	21	CRITICAL	P1	Open	INC00000043841	-	-
Apex Banking-Core-Network - Significant packe...	15 hours ago	-	2	-	CRITICAL	P1	Open	INC00000043442	-	-
Apex Banking-Core-Network - Significant packe...	15 hours ago	43	-	5	CRITICAL	P1	Open	INC00000043442	-	-
Apex Banking - Significant packet loss and incre...	15 hours ago	42	-	9	CRITICAL	P1	Open	INC00000043441	-	-

Figure 4. Generating a meaningful title for the situation.

Key capability #3: Pattern recognition and clustering

BMC Helix AIOps applies predictive, causal, and generative AI (GenAI) techniques to help predict service disruptions, determine the root cause, and derive insights to recommend remediation actions. Intelligent event clustering cuts through alert noise, enabling IT teams to focus on the critical issues that matter most. Events, tickets, changes, and telemetry data correlation are performed to predict trends and uncover underlying causes. This provides context for GenAI to execute the last mile and generate summaries and insights to improve service resiliency and avoid future disruptions. It can also:

- Trigger events and notifications based on a single metric or group of metrics behaving abnormally.
- Reduce event noise using sensitivity controls to manage the detection.
- Generate events with detailed graphs showing the anomalous metric or metrics.
- Use the Random Cut Forest (RCF) unsupervised algorithm to generate anomalies.
- Generate the issue summary and prescribe remediation actions based on past similar situations, tickets, defects, logs, and knowledge base data.



How it works: Anomaly detection algorithms

BMC Helix AIOps uses statistical and unsupervised ML algorithms to detect anomalies in a time series. The anomaly detection first discovers patterns of “normal” behavior in the data to build a model and then uses that model to identify outliers—those data points that fall outside of what is normal.

The system leverages two different algorithms for anomaly detection. One is a highly efficient and scalable univariate anomaly detection algorithm for single metrics. The second is a robust multivariate anomaly detection algorithm that builds a model for a group of related metrics. Multivariate anomaly detectors are computationally more complex as they model a group of metrics, such as all key service metrics or entity metrics, but they can also surface interesting interactions among different metrics.

Univariate metrics enable the system to learn the distribution of each seasonal time series for an hourly time slot (e.g., Monday 9 am–10 am, 10 am–11 am, etc.) and use this to detect anomalies. When the current value of the metric is substantially in the tail of this distribution (such as > 99.5 percentile), then an anomaly is raised. This approach is better than simpler statistics such as mean or median because the data distribution is captured for a time series and combined to produce anomalies that lie outside of the normal distribution of data. This approach can also scale better than others, as it uses unique digests for accurately estimating extreme quantiles with limited memory usage.



Figure 5. Detecting anomalies using multivariate metrics.

For multivariate metrics, BMC Helix AIOps allows defining systems of related metrics, such as a key performance indicator (KPI) group, and detects anomalies that capture the relationships and interactions among these metrics. It uses the RCF anomaly detection algorithm to enable this capability.

Finally, GenAI is used to train large language models (LLMs). The LLM comes pre-trained with domain knowledge on how to solve common operational issues and can optionally be further fine-tuned with customer data in a secure-tenant model to help improve the accuracy of the response.

Key capability #4: Automated asset discovery and dynamic service modeling

BMC Helix AIOps offers best-in-class automated asset discovery with dynamic service modeling to provide critical context for troubleshooting and impact analysis. The dynamic service model is the foundational building block of a business service, providing the domain-specific knowledge as an input to the AI pipeline. This helps build cause-and-effect relationships and weed out nonsense correlations and hallucinations.

BMC Helix AIOps does this at scale, supporting some of the world's largest financial services companies, telcos, and government institutions by simplifying the creation of business service models using blueprints that dynamically traverse all layers to automatically connect the application topology to hosts and network devices.

BMC Helix AIOps also:

- Acts as a unique datastore across the BMC Helix platform for assets and relationships.
- Allows third-party data from application performance monitoring (APM) tools to provide application-specific details about software components and their relationships across cloud, mainframe, and container topologies.
- Streamlines dynamic service model updates and usage for AIOps and ITSM.
- Provides rich visualization, search, and impact analysis.
- Correlates, analyzes, and combines data into a unified topology view using AI-powered service modeling.

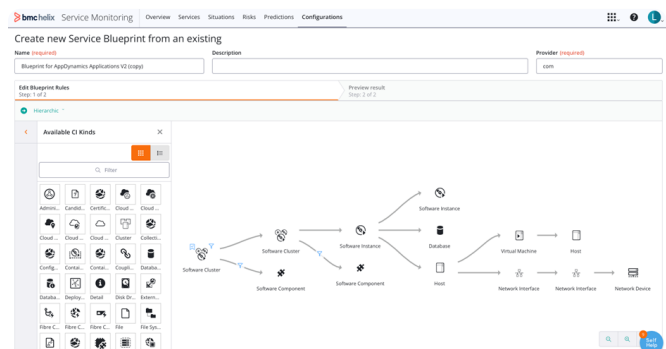
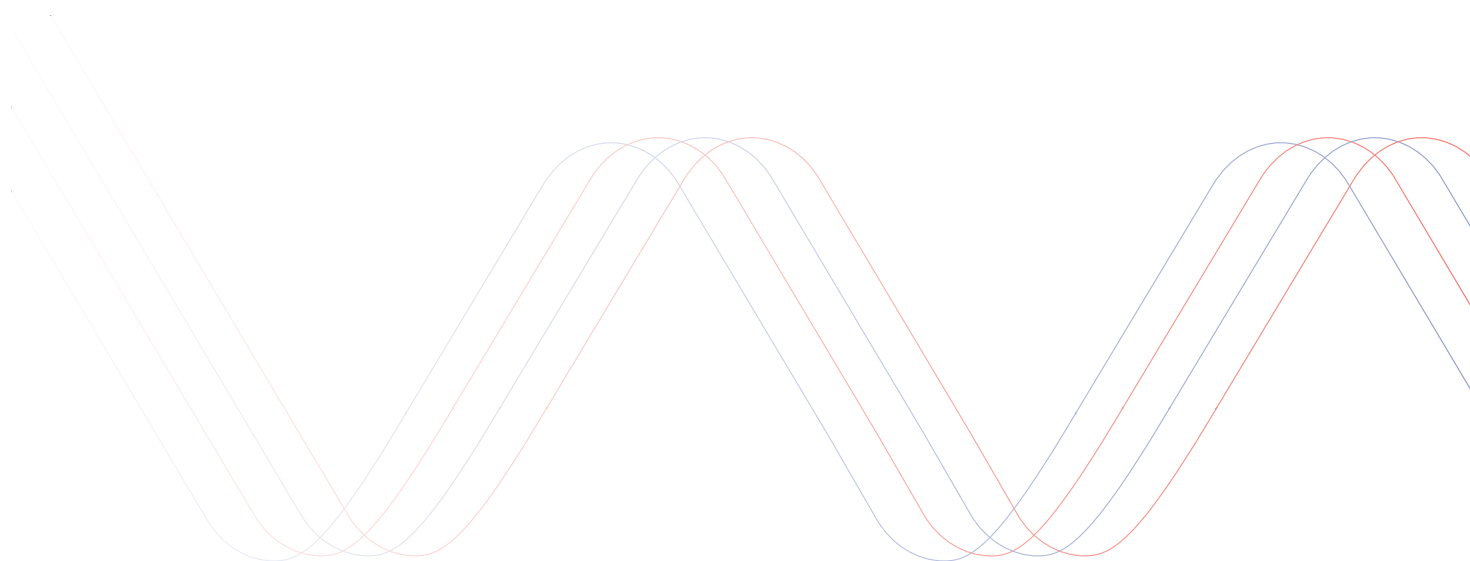


Figure 6. Creating a new service model from a blueprint.

How it works: Dynamic service modeling with blueprints

BMC Helix AIOps normalizes all types of ingested data (metrics, events, logs, traces, and topology) with a dynamic and reconciled graph database of your IT landscape via the following modeling steps:

- 1. Identify services for modeling.** Identify end-user services that you want to model and add service details as inputs to the service modeling tool. An APM tool can provide application-specific details about software components and their relationships across cloud, mainframe, and container topologies. Infrastructure and network monitoring tools and scanning tools can detail the infrastructure's connectivity to underlying virtual and physical devices, such as servers, databases, switches, routers, firewalls, and load balancers.
- 2. Use blueprints.** Discovery and monitoring tools can provide service blueprints to simplify creating and maintaining dynamic service models. These service models support modern technologies like microservices, Kubernetes, cloud services, application performance tracking, and mainframes to keep accurate tabs on all IT resources and relationships. Blueprints make it easy to express a simple rule that identifies all the elements of your service. Define the rule once and apply it to as many services as needed.
- 3. Calculate service health score.** Using ML algorithms to calculate a service's current and historical health based on indicators, abnormalities, and events in the service model's components helps to identify root causes of health impacts or service performance degradation and quickly understand the scope of the impact.



Key capability #5: Major incident prediction

With BMC Helix AIOps, you can predict major incidents by analyzing multiple parameters, including events, metrics, incidents, and change requests.

How it works: Predicting major incidents

BMC Helix AIOps predicts major incidents for a technical/business service using deep learning and statistical models. The algorithm looks for leading indicators that can correlate well with an impending service degradation, outage, or major incident by using combined data from monitoring and service management solutions. There are two phases to the algorithm.

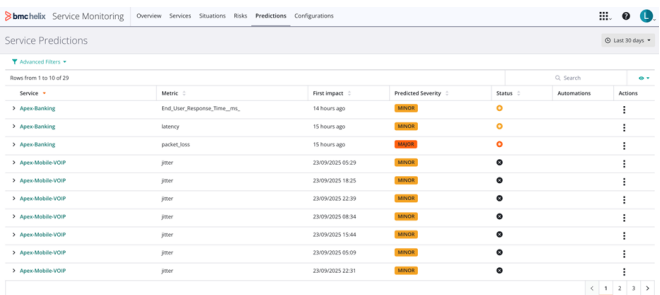
Offline training phase

The system uses three to 12 months of historical data for metrics and events for each service and looks for patterns that indicate a strong correlation between past data and future major incidents. Deep learning models such as long short-term memory (LSTM) are trained and evaluated for their precision/recall to determine whether they can be used for prediction. If they have high accuracy, they will be deployed for online inference.

Short-term forecasting models are built for selected time-series data. These may include Holt-Winters; Box-Jenkins (a.k.a. SARIMA with automatic trend regression and prediction); linear (ordinary and robust); polynomial trend with seasonal component; multiplicative exponential trend with seasonal component; and exponential damping.

Online inference phase

As real-time data flows in, the deep learning models, real-time incident correlation, and forecasting models are evaluated to generate leading indicator scores. Using an ensemble of these leading indicator scores, a major incident is predicted. If a major incident was already predicted for this service in the previous evaluation period, then the state of the service is updated with the new prediction.



Service	Metric	First Impact	Predicted Severity	Status	Automations	Actions
> Agave-Banking	End_User_Response_Time_mts	14 hours ago	High	●		
> Agave-Banking	latency	15 hours ago	High	●		
> Agave-Banking	packet_loss	15 hours ago	High	●		
> Agave-Mobile-VDP	jpsr	20/05/2025 09:29	High	●		
> Agave-Mobile-VDP	jpsr	20/05/2025 18:25	High	●		
> Agave-Mobile-VDP	jpsr	20/05/2025 22:09	High	●		
> Agave-Mobile-VDP	jpsr	20/05/2025 08:34	High	●		
> Agave-Mobile-VDP	jpsr	20/05/2025 15:44	High	●		
> Agave-Mobile-VDP	jpsr	20/05/2025 05:09	High	●		
> Agave-Mobile-VDP	jpsr	20/05/2025 22:31	High	●		

Figure 7. Predicting the severity of situations for a timely response.

Key capability #6: Remediation and automation

A challenge that SREs and DevOps teams encounter is the inability to identify the main cause of incidents and apply better actions, leading to difficulty in addressing incidents promptly. BMC Helix AIOps continuously learns and improves its understanding of associations between events or patterns of events to recommend remediation actions. The solution offers a BMC HelixGPT Planner agent, along with an agentic AI system that considers your organization's unique data and processes when analyzing the root cause and formulating an action plan. The system learns from your incident data, chat scripts, and root cause analysis, correlating them with dependency graphs and change logs to help resolve the problem quickly.

Through integrated workflows between BMC Helix AIOps and BMC Helix ITSM systems, incident management is automated by creating an incident in BMC Helix ITSM with impacted service and CI details. This eliminates context switching and reduces the number of tickets created, associated costs and incident noise, and hours or days of troubleshooting.

Regulatory frameworks emphasize proactive risk management, requiring comprehensive service mapping, constant monitoring, and vulnerability assessments. BMC Helix provides real-time monitoring and modeling and predictive, causal, and generative AI to recommend corrective actions. The BMC HelixGPT Vulnerability Resolver agent empowers teams to quickly identify which services carry the highest risk and prioritize remediation efforts. Automated remediation processes restore services quickly while minimizing operational risks.

Vulnerability Details											
Vulnerability Microsoft Windows "Runas" Password Length Local Disclosure											
The "Runas" Password Length Local Information Disclosure vulnerability in Microsoft Windows is a security issue where the length of a password used in the "Runas" command can be disclosed to a local attacker. The "Runas" command in Windows allows a user to run specific programs or tasks with different user privileges, typically higher or administrative privileges.											
Severity	Critical	Risk Score	4.5	CVE ID	CVE-2009-0328 v1	CVD Score	4	Impacted Systems	Active Payments > 3	Impacted Assets	168
Categories: Database First Reported: 2009-03-10											
Generate remediation											
Impacted Assets											
Records from 1 to 16 of 168											
Advanced filter:				Filter by active payments				Search		Visible columns	
☐	Asset Name	Status	2	Automation	Change Tickets	Contact	Dept	Email	Environment	Location	
☒	lappin@...	Kat (by 122 days)	Affected	1 Available	AJ009634345 v1	HR	Sales	Dms	Dev	Pure	
☒	Arnie.Rapchinsky@...	Kat (by 122 days)	Affected	-	-	IT	Production	Web	QA	San Jose	
☒	Arnie.Benckendorfer@...	Kat (by 122 days)	Not affected	Automation Planned	AJ009612346 v1	Accounts	Operations	DMS	Production	Munich	
☒	wc-ws-cc-sql@ph.com	Kat (by 122 days)	Affected	Automation Planned	AJ009612345 v1	Maintenance	Legal	Email	Pre-prod	Toronto	
☒	gao@merit.com	Kat (by 122 days)	Affected	Automation Planned	AJ009612346 v1	Customer service	Finance	Web	QA	Felipe	
☒	skw-nr-gst@fmc.com	Kat (by 122 days)	Affected	-	AJ009639811 v1	Customer service	Legal	Email	Dev	San Jose	
☒	skw-dmnp@fmc.com	Kat (by 122 days)	Affected	-	AJ009654224 v1	IT	Sales	DMS	QA	Pure	
☒	skw-as-dm@fmc.com	Kat (by 122 days)	Under investigation	Not Available	-	Accounts	Finance	Web	Production	Munich	
☒	mrgn@fmc.com	Kat (by 122 days)	Not Affected	1 Available	AJ009123678 v1	Maintenance	Production	Web	Dev	Munich	
☒	skw-gst@fmc.com	Kat (by 122 days)	Affected	1 Available	AJ009194823 v1	HR	Operations	DMS	Pre-prod	Felipe	

Figure 9. See assets impacted by a critical vulnerability.

How it works: Intelligent automation and remediation

- Make existing playbooks from Anisible available as executable actions.
- Trigger actions without pre-configuration.

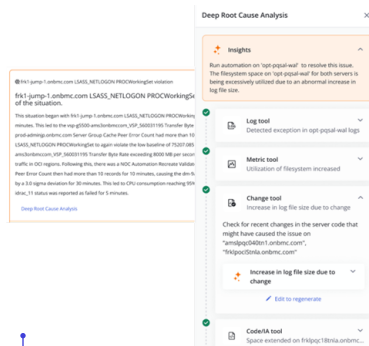


Figure 8. Deep root cause analysis provides insights for remediation.

AIOps and observability for the AI era

The AIOps market is experiencing continuous convergence with adjacent technology tools. Infrastructure monitoring solutions, observability platforms, and ITSM tools are all offering AIOps capabilities, but the ROI from AIOps efforts will come down to workflows.

If AI doesn't fit into how operators do their jobs and is tied to business-specific challenges, real value will not be realized. As AI continues to transform IT work, IT leaders must take a strategic approach to rethinking their workflows and implement AI and agentic systems into specific processes to drive valuable outcomes. It's an exciting time to be in ITOps as we move beyond simple automation to creating autonomous, goal-oriented AI systems that accelerate incident response, augment IT work, and enhance uptime and reliability.

BMC Helix's multi-year effort to design an AI-driven platform with GenAI and retrieval-augmented generation (RAG) throughout is powering a system of purpose-built AI agents that provide proactive assistance in root cause analysis, incident response, and capacity optimization. Our AI agents are also integrated with tools like Microsoft Teams to accelerate response and improve collaboration.

From operations overload to strategic control, BMC Helix AIOps supports IT teams by automating ITOps while providing human oversight in a collaborative model. Our BMC Helix AIOps and observability approach integrates with our own BMC Helix ITSM, BMC Helix Discovery, and BMC Helix CMDB solutions, opening the door for significant tool rationalization and operations optimization.



For more information

To learn more about BMC Helix AIOps and observability, please visit:

www.helixops.ai

About BMC Helix

BMC Helix, now an independent company, helps the world's most forward-thinking IT organizations turn AI into action—unlocking human potential to multiply productivity so teams can focus on the work that matters most. With an industry-leading, AI-powered, open platform, BMC Helix delivers a dynamic fleet of AI agents that augment work across enterprise IT service and operations management to anticipate needs, automate solutions, and accelerate outcomes for ServiceOps.

Turn AI into action.



Helix and other Helix marks are exclusive properties of BMC Helix, Inc. and are registered or may be registered with the U.S. Patent and Trademark Office and in other countries. BMC, BMC Software, the BMC logo, and other BMC marks are the exclusive properties of BMC Software, Inc. and are registered or may be registered with the U.S. Patent and Trademark Office and in other countries. © Copyright 2025 BMC Helix, Inc.

