

Reset the Limits of IT: The Hidden Value of Prevention



The cost of downtime

Every year, businesses worldwide spend trillions of dollars responding to problems that were predictable, preventable, and in many cases, widely recognized long before they became crises. In fact, the cost of these issues is staggering.

Yet despite these expensive consequences, most organizations continue to invest far more in responding to problems than preventing them.

\$300,000/hour

The cost of a single hour of downtime for more than 90% of mid-size and large enterprises.¹

\$1 to \$5 million/hour

The cost of a single hour of downtime for 41% of large enterprises.²

1. *ITIC 2024 Hourly Cost of Downtime Report Part 1*, ITIC Corp, September 3, 2024.
2. *ITIC 2024 Hourly Cost of Downtime Report Part 2*, ITIC Corp, September 10, 2024.

The cost of reactive operations

For IT teams, firefighting has become part of the job. Service outages, security incidents, and a seemingly endless stream of support tickets consume time, energy, and resources. They may resolve each issue, but each reactive response serves as a tax on IT's capacity. As a result, IT teams can't tackle many of their most important issues, limiting their capacity to innovate, transform, and evolve.

Today, responding to major incidents often requires bringing stakeholders beyond IT together in a war room to coordinate remediation in real time. However, communication delays and assumptions multiply the risk as teams begin to form their own interpretations of the incident. Each detection and response tool highlights the risk from its own perspective, leaving responders to manually synthesize competing narratives under pressure. Without clear context and holistic understanding, the response becomes chaotic, consuming valuable engineering resources and time.

THE 1-10-100 RULE*

\$1	\$10	\$100
to prevent an issue	to fix an issue while it's in progress	to fix an issue after it reaches the customer

**Estimated.*

While the exact numbers vary by industry, the principle remains the same: the later an organization discovers an issue, the more expensive it becomes to resolve.

Instead, imagine a world where success is measured by the number of incidents resolved before they become a ticket; the vulnerabilities remediated before they cause a crisis; and the outages prevented before they disrupt operations.

The future of IT is not built on responding to crises faster. It's built on preventing crises from happening in the first place. That's why, to reset the limits of IT, organizations must move from a culture of reaction to one of prevention, shifting both mindset and budget away from reactive resolutions toward proactive measures that stop incidents before they ever start.

The shift to prevention

**PREVENTION HAS A
VISIBILITY PROBLEM:
WHEN IT WORKS,
NOTHING HAPPENS.**

True transformation occurs when IT teams shift from reaction to prevention. Not only does prevention stop incidents and their related costs from occurring, but it also creates efficiency and reduces overspend. In fact, a simple one-to-two-percent improvement could translate into thousands—or even millions—of dollars in savings. If preventing incidents costs \$1, resolving them while they are happening costs \$10, and fixing them after they reach the customer costs \$100, where would you prefer to invest?

Yet despite the compelling economics of prevention, many organizations remain focused on fixing alerts and outages through frantic firefighting and manual ticket handling. They invest in disjointed monitoring and alerting tools to help accelerate incident resolution. And while these investments are valuable, the approach of many organizations is to manage and remediate problems after they arise.

Until the focus shifts toward prevention, executives will continue to ask, “Why didn’t you catch the issue earlier?”

Today, organizations collect vast amounts of data to detect, diagnose, and respond to issues as quickly as possible. While this visibility helps to improve incident response, it often comes at a cost: growing data volumes, escalating compute requirements, and increasing tool complexity.

A prevention-first approach employs AI and AI agents to calculate change risks, identify anomalies across multiple data sources, predict service health, reduce false positives, and proactively address issues. Not only does this prevention-first approach result in fewer incidents, but it also enables a more efficient, cost-effective operating model that drives proactive reliability.

Prevention also addresses concerns about the rising costs of large language models (LLMs). In most organizations, AI agents burn tokens on investigations that never needed to happen. These AI agents close tickets because they’ve alleviated the symptoms, only to have the issue resurface again as a new ticket. Agents can also waste tokens hunting through stale, disconnected data that leads to a dead end instead of delivering an optimized response supported by a live service model.

Done well, prevention mitigates change risk, cuts token consumption at the source, and eliminates root causes before they cause an incident. It prevents multiple investigations of the same failures, and grounds investigations in a current service model, enabling IT teams and AI agents to reach a logical conclusion in fewer steps.

Prevention in practice

When put into practice, prevention offers several benefits to organizations, including:

→ **Reduced downtime and cost**

Reacting to incidents is expensive and laborious. Preventing incidents from happening in the first-place cuts costs substantially. Using capabilities such as automated change risk assessments, anomaly detection, predictive analytics, and automated remediation, IT teams can detect service degradations before they go down, scale the right components at the right time rather than overprovisioning everything “just in case,” and catch security vulnerabilities before they cause a breach.

→ **Continuous learning and reliability**

Prevention is not just about catching problems sooner. It’s also about continuously understanding normal system behavior to identify risky changes, emerging system or application issues, and vulnerabilities rather than relying solely on alerts. This shift from reactive monitoring to proactive detection and change planning is where AI becomes essential. AI can continuously analyze behavior patterns across thousands of signals, identify combinations of leading indicators that historically precede failure, and surface those risks before they bring the system down, reducing the strain on engineering and operations teams.

→ **Reclaimed capacity**

Organizations hedge system capacity against the uncertainty of outages. They over-provision infrastructure as a safety margin, overlap observability platforms in an attempt to spot every problem, and increase telemetry data volumes to capture every angle. Better change-risk confidence and dependency visibility let teams right-size safety margins instead of padding them by default. And correlation and noise reduction cut through redundant alerts, enabling organizations to consolidate observability licensing and rationalize telemetry ingest, storage, and compute. The payoff isn’t just lower cost, but reclaimed capacity to reinvest where it matters.

→ **Faster innovation**

Proactive incident prevention fosters an environment of innovation and continuous improvement, allowing engineers and operations teams to shift their focus from manual debugging and filling out change forms, to building and delivering core product capabilities. As a result, they gain a newfound confidence grounded in smart, effective tooling and automated processes that lead to better employee experiences and increased innovation that propels the business forward.

Prevention increases capacity and reduces spend to free up cash

VALUE DRIVER	OPERATING ENVIRONMENT	IMPACT POTENTIAL	VALUE
Infrastructure over-provisioning and defensive capacity	Annual infrastructure run rate supporting critical services	Increased efficiency with improved change-risk confidence and dependency visibility greater confidence in capacity requirement	\$\$\$
Observability platform licensing and support	Annual spend across multiple observability platforms, excluding telemetry pipeline costs	Reduced costs through consolidation of overlapping tooling and retirement of redundant platform capabilities	\$\$
Telemetry ingest, storage, and compute	Annual telemetry data management costs, including logging, processing, storage, and analysis	Reduced costs via correlation, noise reduction, telemetry rationalization, and fewer incidents and outages	\$\$
Engineering time reclaimed from operational maintenance	Engineers engaged in incident response, change validation, or operational reconciliation	Recovered capacity through fewer interruptions, automated context gathering, and reduced human resource consumption during incidents and changes	\$\$\$
IT operations productivity improvement	IT operations works on avoidable issues	Improved productivity via contextual triage, automated correlation, and risk-aware workflow automation	\$\$\$
Major incident recovery effort reduction	Annual major-incident response and escalation effort across IT and engineering teams and business impact of outages	Reduced recovery effort and business impact through reduced MTTR, and fewer prolonged war-room events; less impact on business from outages	\$\$\$
Vulnerability remediation	Manual effort to identify and mitigate vulnerabilities	Reduced manual effort, faster automated remediation, and reduced vulnerability risk	\$\$

The compounding value of prevention

A prevention-focused approach increases revenue and profitability because every dollar invested in prevention delivers value that compounds over time.

When it's done right, prevention compounds value. Organizations see fewer tickets, incidents, and negative business impacts. And as they prevent one issue, they create knowledge and automation to stop the same issue from happening again in the future. However, effectively shifting to prevention requires that IT teams have a comprehensive understanding of the structure, state, and evolution of the complete digital environment, including:

- Underlying infrastructure data
- Service mapping
- Telemetry
- Workflow patterns
- Historical learnings

In addition, they need to understand the landscape of incidents, changes, configurations, post-mortems, and runbooks. These inputs are critical for AI agent training, turning organizational knowledge of causes, impact, and resolutions into proactive incident prevention.

Lower fixed costs

Fixing issues now prevents expensive system failures later.

Saved time

Engineers can build new features instead of fixing old bugs.

THE COMPOUND EFFECTS OF PREVENTION

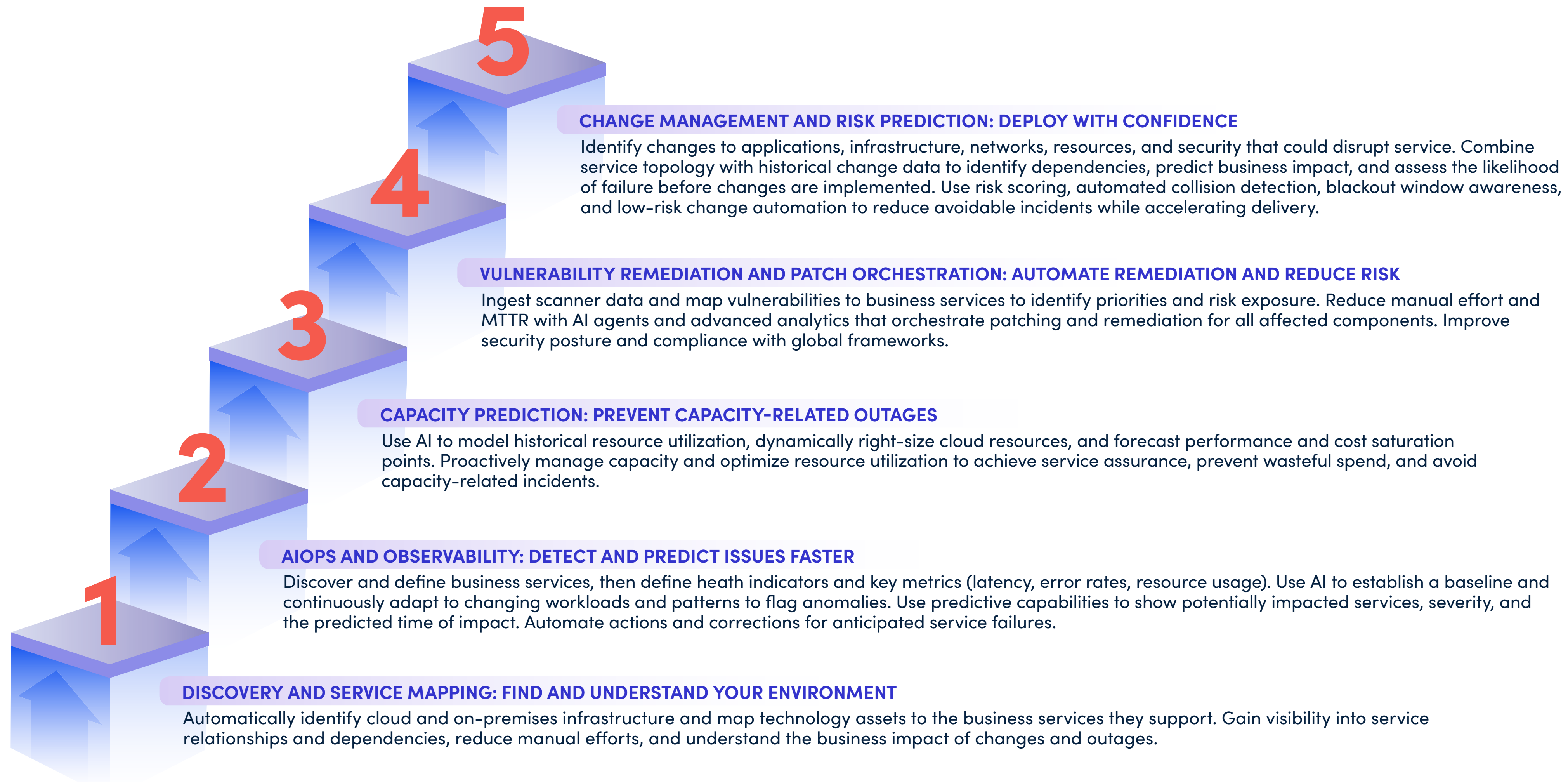
Increased morale

Less firefighting lowers stress and reduces burnout.

Greater trust

Customers remain happy and retention soars.

5 steps to deliver prevention



Helix delivers an integrated approach

Every hour that an IT team spends stitching together disparate tools is an hour diverted from preventing outages. Even worse, disjointed solutions create gaps, redundancy, and uncertainty across critical data and systems. Helix has a different story to tell.

Rooted in the most integrated prevention platform in the industry, the Helix ServiceOps solution helps IT teams shift their focus from managing fragmented tools to preventing issues and delivering measurable outcomes.

[Helix Discovery](#) maps the estate; [Helix AIOps](#) watches it in real time; [Helix Automation and Compliance](#) orchestrates secure and reliable patch deployment; and [Helix ITSM and Knowledge Management](#) provide the operational record and manage changes effectively. In addition, our [AI agents](#) reason across this entire ecosystem, driving AI agents to take action and draw intelligence from a shared pool of data and context.

With Helix, IT teams can confidently:

- Explain their conclusions—and the reasoning behind them
- Use the LLM of their choice
- Keep data within regional boundaries
- Define the level of autonomy for each agent, from recommendation to independent action
- Govern AI agents consistently as adoption grows

IT success starts with prevention

The ability to quickly resolve service outages and incidents is critical, but the ability to prevent them is transformative. By identifying risks early and addressing them before they affect users, IT organizations can reduce costs, improve reliability, and create more efficient and resilient operations to handle growth in innovation. In the years ahead, the most successful IT teams will earn recognition for silence, stopping outages before they occur, eliminating risks before they materialize, and delivering the uninterrupted experiences users expect.



What would prevention be worth in your environment?

You've seen the math: a single hour of downtime costs six to seven figures, and every dollar spent preventing an issue saves ten to a hundred more downstream. The only unanswered question is what that math looks like inside your organization.

[Talk to a Helix expert](#) and find out with a short conversation about your infrastructure spend, your incident volume, your team's lost hours.

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.



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 2026 BMC Helix, Inc.

