everbridge xmatters

From alerts to autonomy

How AI is transforming incident management

Table of contents

Introduction

Incident management has become a defining capability of digital business resilience. As cloud-native architectures and distributed systems increase complexity, failures are no longer isolated events. They are cross-functional disruptions with real financial and reputational impact.

The traditional model of detect, notify, assemble, resolve was built for a simpler era. Today, signal volume exceeds human capacity, and speed is inseparable from business outcomes.

Artificial intelligence is transforming incident management from reactive coordination to intelligent orchestration, compressing time to understanding, enabling governed automation, and setting the foundation for autonomous resolution.

Chapter 1

The incident management era is changing

For years, incident management was treated as a downstream concern, something teams dealt with after systems failed. Alerts fired, pages went out, bridges were opened, and humans scrambled to restore service. The model worked well...until it didn't.

Today's digital environments are fundamentally different. Cloud-native architectures, microservices, APIs, and globally distributed infrastructure have dramatically increased both the frequency and complexity of incidents. Failures no longer originate from a single broken component; they emerge from interactions across systems, teams, and tools. As a result, the hardest part of incident response isn't notifying the right on-call resource, but rather understanding what's happening fast enough to act decisively.

And the stakes are rising.

In modern enterprises, even short outages can translate into meaningful financial and operational impact. Uptime Institute's outage research has consistently reinforced that outages are becoming more expensive and consequential as dependency on digital services grows.

Recent research also suggests the outage burden is widespread and recurring. A New Relic study found that significant downtime can cost $2 million per hour and contribute to substantial annual losses for businesses. Uptime Institute has noted that a significant share of major outages surpass the $100,000 threshold, reinforcing that outages are no longer "rare events," but high-cost business disruptions.

Taking all of this into account, what can you do? This is where artificial intelligence comes into play. Not as a futuristic concept, but as a practical necessity today.

AI is reshaping how organizations detect, understand, and respond to incidents. In observability platforms, AI can already identify anomalies, reduce noise, and surface patterns humans might miss. But the real transformation isn't happening at the edges of the stack. It's happening at the center of incident management itself.

A New Relic study found that significant downtime can cost

$2 million

per hour and contribute to substantial annual losses for businesses.

That's because incident management is where intelligence becomes execution.

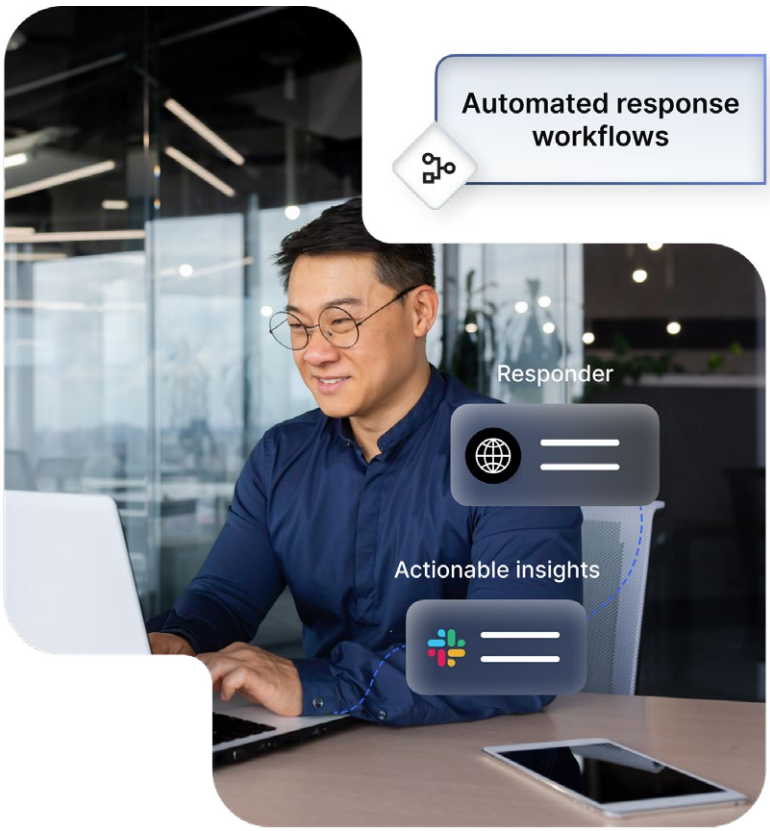
Platforms like xMatters represent a shift from reactive paging systems to intelligent orchestration layers, where AI helps teams make sense of chaos, coordinate action, and increasingly resolve issues automatically. Instead of humans manually stitching together alerts, ownership, dependencies, communications, and remediation steps in real time, AI-assisted incident management enables a new model: one in which workflows are triggered automatically, responses are coordinated consistently, and actions occur through governed automation.

What's changing is not only the complexity of incidents, but the reality that incidents are now inseparable from the digital business itself. The organizations that will outperform in the next decade won't be the ones that eliminate incidents entirely. They'll be the ones that respond with clarity and speed, using AI to compress time-to-understanding and orchestration to drive time-to-resolution.

The era of the incident isn't ending. But manual incident response is.

Want to know how xMatters can help you?

Request a demo



Chapter 2

AI across digital operations: The foundation is already here

To understand AI's impact on incident management, it's important to examine how it is already being used across digital operations.

In observability, AI has become table stakes. Machine learning models dynamically baseline metrics, detect anomalies, and surface patterns humans would miss. Logs are clustered and summarized. Traces are analyzed for latency and error propagation. Observability pipelines increasingly use AI to filter noise, enrich telemetry, and reduce data volumes before signals ever reach an operator.

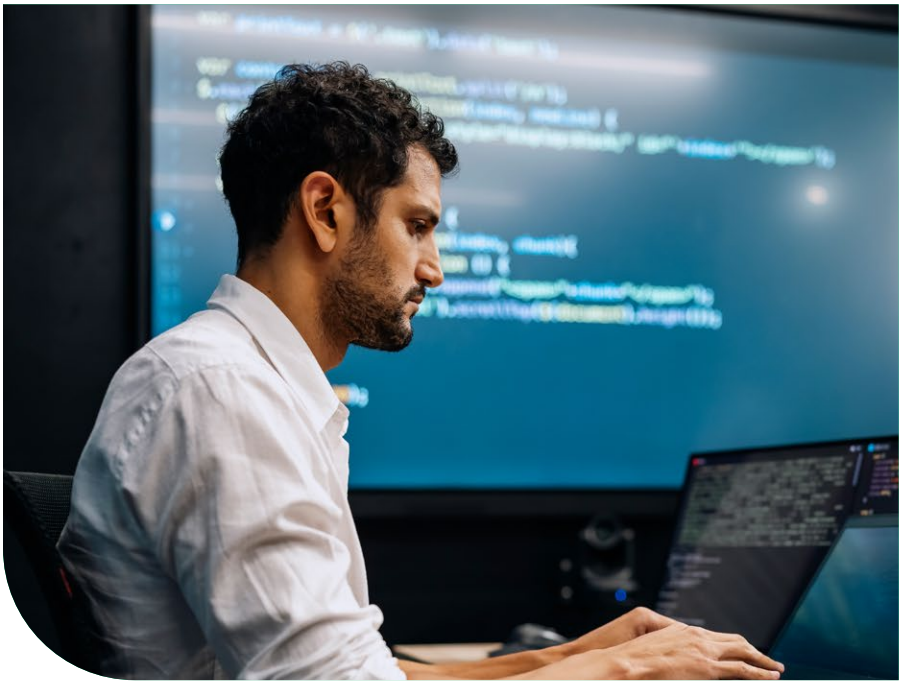
The shift isn't just technical. It's economical and operational. As digital services scale, they generate more telemetry than teams can afford to store or humans can feasibly interpret. In many environments, signal volume has outpaced human capacity with familiar results: noise, alert fatigue, and delayed diagnosis.

The business cost of those delays is becoming impossible to ignore. In the previously referenced New Relic report, they also noted that organizations face an annual median cost of $76M for high-impact IT outages, reflecting how common and costly major disruptions have become.

Organizations face an annual median cost of

$76M

for high-impact IT outages, reflecting how common and costly major disruptions have become.

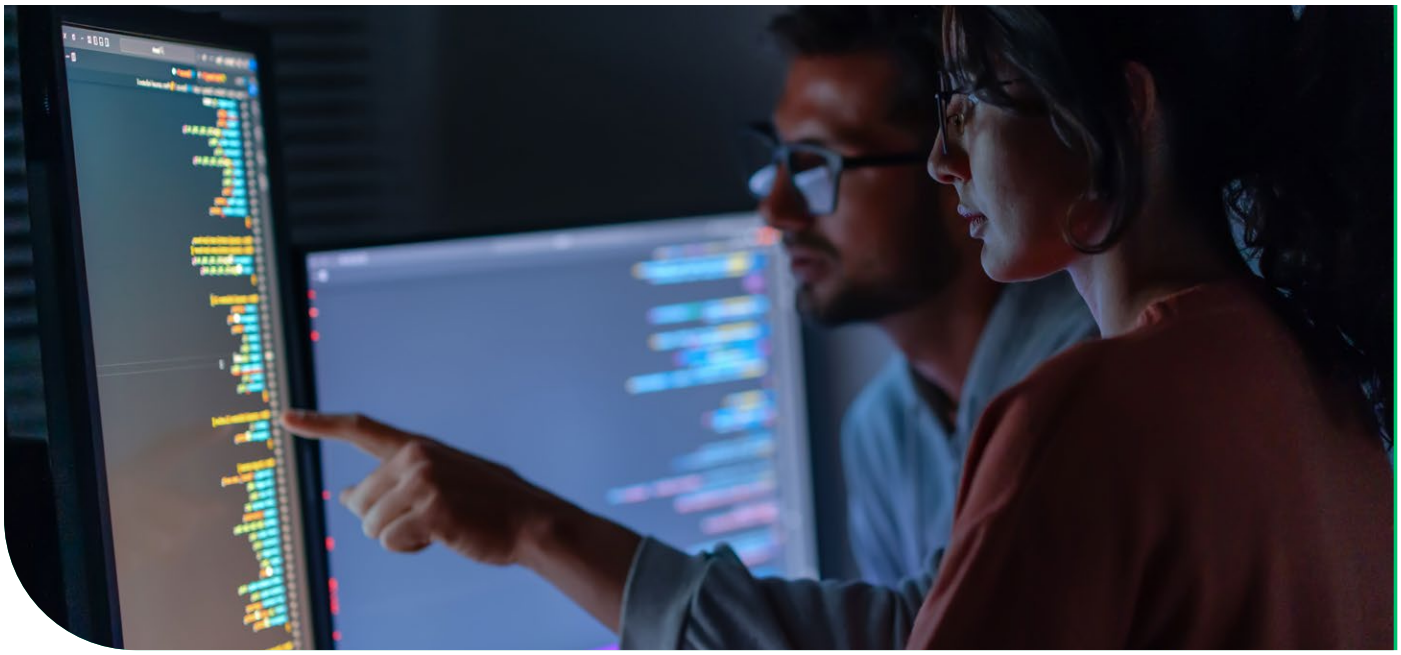


Elsewhere, AI copilots are changing how engineers work. Natural language interfaces generate code, suggest automation steps, and accelerate configuration. “Vibe coding” may sound informal, but it reflects a serious shift in which humans express intent and machines handle execution. This is shrinking the distance between ‘what should happen’ and ‘make it happen’, a major unlock for operations teams that have historically struggled to scale automation.

And yet, despite all of this progress, there’s a gap.

Most AI in digital operations stops short of action. It informs dashboards, highlights anomalies, and produces insights. But it doesn’t decide what should happen next. That responsibility still falls on humans. Humans who are often under extreme pressure when time is scarce, information is incomplete, and consequences are real.

Incident management sits directly in this gap. It is the point at which AI must evolve beyond analysis into orchestration, turning intelligence into safe, repeatable execution.



Chapter 3

Why incident management is the AI inflection point

Incident management is where signals become decisions and decisions become outcomes.

Unlike observability tools, incident management platforms must answer questions that are inherently operational and contextual:

- **Who needs to be involved?**
- **What services are actually impacted?**
- **What actions are safe to take right now?**
- **What must be communicated, to whom, and when?**

This is why AI applied to incident management is fundamentally different from AI applied elsewhere in the stack. It moves beyond analytics to decisions, and it's in decisions that operational risk lives.

In practice, most major incidents succeed or fail during handoffs. Time is lost aligning stakeholders, identifying service owners, deciding escalation paths, and coordinating responses across tools. This is the 'human middleware' problem, where humans bridge gaps between systems and teams.

At the same time, the financial and reputational stakes continue to rise. Gartner's widely cited benchmark estimates downtime cost at $5,600 per minute, and while the true number varies by company, it emphasizes the reality that incident response speed is directly tied to business impact.

xMatters was built around this reality. From the beginning, it was designed not merely to notify people, but to orchestrate response across teams, tools, and workflows. That orchestration layer is what makes meaningful AI possible. When AI is purpose-built for incident management, it understands services, ownership, dependencies, escalation policies, and automation paths. This is far more than simply summarizing alerts. It can guide and increasingly execute a response with policy-aligned guardrails.

Incident management becomes the control plane for digital operations. The system that turns insight into action at scale.

Gartner's widely cited benchmark estimates downtime cost at

$5,600

per minute

Chapter 4

The current state: AI as an incident copilot

Today, AI in incident management functions primarily as a copilot, augmenting human responders rather than replacing them. This is both intentional and appropriate.

In the high-stakes operational environments, the most immediate and widely trusted value of AI is speed to understanding. Instead of forcing responders to piece together dozens of alerts, logs, and chat messages, AI can:

- Generate concise incident summaries in natural language
- Reconstruct timelines automatically
- Highlight what changed, where, and when
- Reveal similar incidents and how they were resolved

This is already transforming the first 10-15 minutes of incident response, the period where confusion and context gaps often dominate. Faster understanding leads directly to faster decision-making, fewer escalations, and fewer costly handoffs.

Within xMatters, this intelligence is grounded in service context. Incidents aren't just collections of alerts; they're tied to real services, real owners, and real business impact. AI becomes far more valuable when it understands what matters.

And the need is real, as many teams are drowning in noise. A useful proxy for this challenge is the extent to which incident platforms have invested in noise reduction and event correlation.

AI also improves contextual awareness. By enriching incidents with service dependencies, runbooks, ownership data, and recent changes, responders spend less time searching and more time acting. The question shifts from "What is this alert?" to "What do we do next?"

This alone can shave critical minutes or hours off resolution times, particularly in distributed environments where root cause rarely lives in a single tool.

AI as an incident copilot is already transforming the first 10-15 minutes of incident response - the period where confusion and context gaps often dominate.

Chapter 5

From context to cause: AI and root cause reasoning

Root cause analysis has always been one of the most challenging aspects of incident response. In complex systems, failures rarely have a single cause, making certainty nearly impossible in the moment.

AI changes the equation by introducing probabilistic reasoning.

Rather than searching for absolute truth, AI helps teams evaluate likelihood. By correlating signals across telemetry, changes, and historical incidents, AI can surface the most plausible causes early, when they matter most.

This is no small shift. During a major incident, the cost of delay compounds quickly. Uptime Institute's Annual Outage Analysis emphasizes that outages remain expensive and consequential, with many organizations reporting significant total outage costs. Coverage of the previously mentioned Uptime Institute's findings reinforces that a large share of significant outages exceed $100,000, with a notable portion exceeding $1M.

In an xMatters-driven workflow, this reasoning is actionable. Suspected causes can trigger specific playbooks, remediation steps, or targeted escalations. AI doesn't just say "this might be the problem", it helps initiate the response tied to that hypothesis.

Importantly, this reasoning is transparent. Operators can see why a hypothesis was generated, what signals contributed, and how confidence was assessed. That transparency builds trust over time, which is essential before automation can expand beyond 'recommendations' into execution.

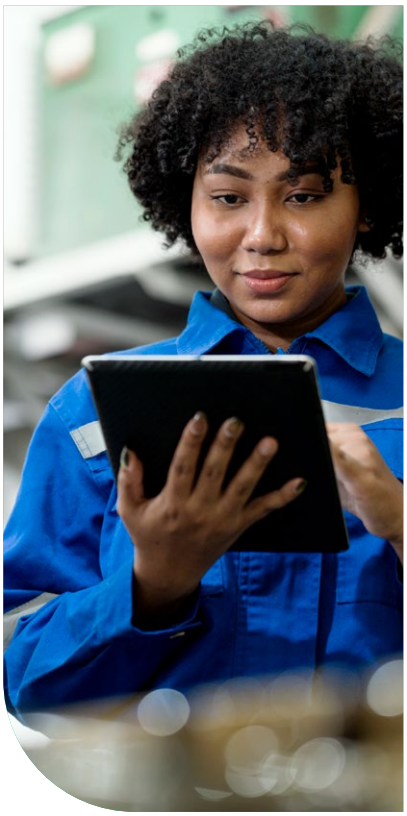
By correlating signals across telemetry, changes, and historical incidents, AI can surface the most plausible causes early, when they matter most.

Want to know how xMatters can help you?

Request a demo

Chapter 6

Automation today: Human-in-the-loop by design



Automation is where AI begins to move from insight to impact, but also where risk enters the conversation.

Most organizations are not ready for fully autonomous remediation across all services, nor should they be. Regulatory requirements, customer impact, and organizational maturity all demand caution.

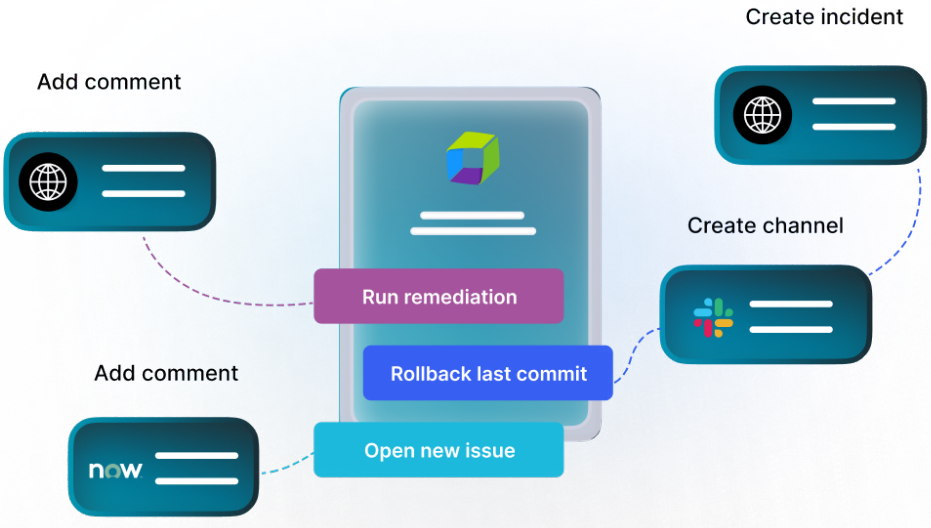
This is why human-in-the-loop automation is the dominant model today.

xMatters enables this balance by design. AI can recommend actions, trigger workflows, and prepare remediation steps while humans retain control over execution when necessary. Approvals, guardrails, and escalation paths ensure that speed never comes at the expense of safety.

At the same time, low-risk, repeatable scenarios can, and should, be fully automated. The industry has already seen how valuable this is: fewer repetitive pages, faster remediation for known patterns, and less operational toil.

This maturation mirrors a broader shift in operations priorities. Research and industry reporting on operational leadership trends show a rising focus on automation, AIOps, and modern incident management practices as core resilience investments.

Over time, trust grows. Human involvement decreases. Autonomy expands.



Chapter 7

The near future: Agentic incident management

The next phase of AI in incident management is agentic.

AI agents will no longer operate as isolated features. They will act as goal-driven participants in the incident lifecycle, monitoring conditions, executing multi-step plans, validating outcomes, and learning from results.

In this model:

- One agent may focus on detection and triage
- Another on remediation planning
- Another on communication and stakeholder updates

But agentic doesn't mean 'ungoverned.' In operations, autonomy must be earned.

This is where analyst guidance becomes a warning and a roadmap. Gartner predicts that over 40% of agentic AI projects will be canceled by the end of 2027, driven by escalating costs, unclear business value, or inadequate risk controls.

That prediction doesn't mean agents won't matter. It means the organizations that win will be those that operationalize agents within governed workflows, where policies, approvals, and auditability are part of the execution fabric.

The xMatters orchestration layer is critical here. Agents don't operate in a vacuum; they operate within governed workflows, tied to services, policies, and human oversight.

This isn't science fiction. It's the natural evolution of intent-driven operations.

Gartner predicts that over

40%

of agentic AI projects will be canceled by the end of 2027, driven by escalating costs, unclear business value, or inadequate risk controls.

Chapter 8

The end state: Human-on-the-loop

The ultimate goal of AI in incident management is not to remove humans but to elevate them.

In mature environments, AI resolves the majority of incidents autonomously. Humans move from responders to supervisors, defining policy, setting thresholds, and handling exceptions.

This is human-on-the-loop, not out-of-the-loop.

Every action is auditable. Every decision explainable. Every automation reversible. Trust is built through visibility and control.

This future aligns with the broader trajectory of embedded agent capabilities in enterprise applications. Gartner predicts 40% of enterprise apps will include task-specific AI agents by 2026. The question isn't whether agents exist. The question is whether they operate safely and with defined governance in environments where mistakes have consequences.

This xMatters philosophy aligns directly with this future: resilience at machine speed, governed by human judgment.

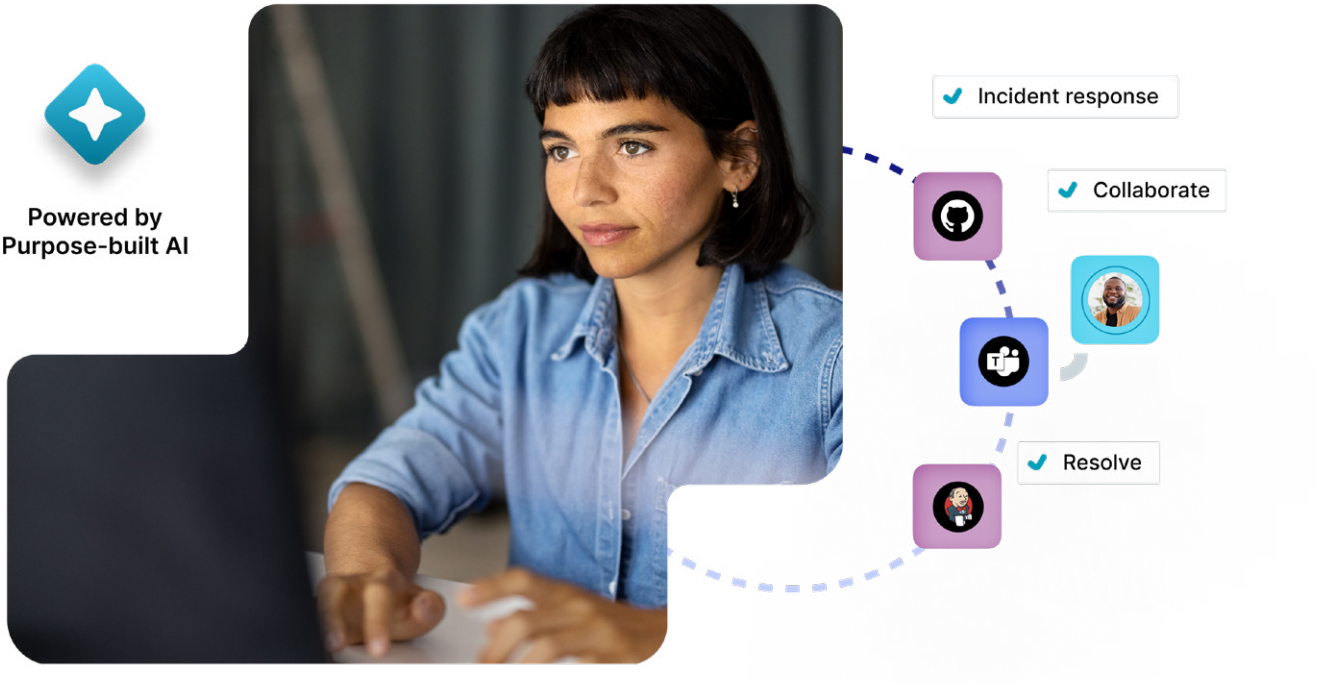
Gartner predicts

40%

of enterprise apps will include task-specific AI agents by 2026

Want to know how xMatters can help you?

Request a demo



Chapter 9

What to look for in an AI-powered incident management platform

Not all platforms are equally prepared for this future.

Organizations should look for:

- Native orchestration, not bolt-on automation
- Deep service context and ownership modeling
- Governed, explainable AI
- Extensibility across the digital operations ecosystem
- Proven enterprise scale and reliability

The temptation in the market will be to evaluate AI based on surface-level features like summaries, chat interfaces, and clever demos. But the enterprise value comes from execution, which is the ability to translate intelligence into safe action.

This is why orchestration is non-negotiable. AI without orchestration is insight without impact.

As AI becomes embedded into operational workflows, this will become the dividing line between platforms that inform teams and platforms that change outcomes.

Chapter 10

From response to resilience

Incidents will continue to happen. Complexity will continue to increase. But the way organizations respond is undergoing a fundamental shift.

AI is moving incident management from reactive coordination to proactive, autonomous resolution. Platforms like xMatters are not just keeping pace with this change; they are driving it. They are defining it by combining service context, orchestration, and governed automation.

The future of incident management isn't about faster pages.

It's about smarter systems.

Systems that can:

- Understand context quickly
- Coordinate the right response automatically
- Execute remediation safely
- Validate outcomes
- Keep stakeholders informed
- Continuously improve incident playbooks over time

Incidents aren't going away. But the cost of manual incident response is becoming unacceptable.