ignio

Intelligent Incident Management

digitate

Intelligent Incident Management

ignio™ AIOps, uniquely blends intelligence and automation to improve the effectiveness and efficiency of Enterprise IT datacenter operations. It brings reliability, agility and resiliency into IT operations by learning context, managing alerts, handling incidents, performing actions and optimizing operations proactively. In this paper, we will look to understand ignio's ability to autonomously handle IT incidents. By leveraging this unique feature of ignio, enterprises can achieve upto 90% reduction in MTTR of IT incidents

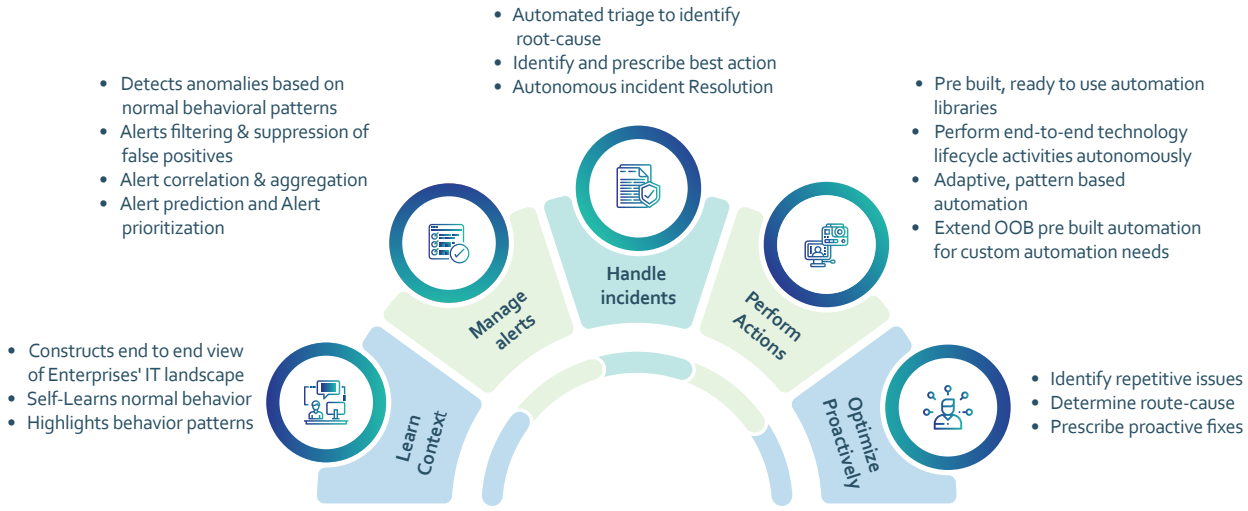


Figure 1: Key Features of ignio™ AIOps

1. Context

Despite the increasing focus on ensuring agile and robust IT systems, the fact is that IT-related outages exist—and they are expensive. The following examples from the recent past illustrate this:

IT upgrades at a bank left a large number of customers unable to access internet and mobile banking services. A planned weekend downtime ended up becoming an incident that caused months of disruption. Many customers experienced problems logging in, while others were shown details from other people's accounts or inaccurate credits and debits within their own .

A widespread computer failure at a leading hospital chain left doctors and hospital staff unable to access patient files, blood and x-ray results. It caused a backlog, as there were patients whose appointments were not cancelled, and medical notes could not be saved on these systems.

Notable airline IT outages have resulted in the cancellation of hundreds of flights from their main hub. It took these airlines several days to restore normal operations, and they had to face bottom-line pressure due to the costs associated with these outages, both from an operations as well as a customer point of view.

These and numerous more such examples make it evident without a doubt that the state of the art of incident management has serious limitations. Some commonly observed pain areas are the following:

Long delays in finding the cause behind an incident: More often than not, the time taken to resolve an incident is longer than the down time that the business is able to sustain. Based on general experience, at least 70% to 90% of incident lifecycle time is spent on the isolation of the root cause.

Trial-and-error approach: Much of incident resolution processes do not follow structured methodologies for resolution. The resolution process is more in an art form and involves trial-and-error based on intuition and past experience. This leads to resolutions that are often not right the first time. More importantly, this leads to inefficient and fragile systems.

People dependence: For certain incident types and affected systems, there is an acute dependence on people whose availability or bandwidth cannot be guaranteed. This adds to the headwinds on an already slow incident resolution process. Intelligent alerts management.

2. What causes pain

Given the impact on business, it is extremely critical to move IT away from a constant fire-fighting operation into a simpler, faster and proactive entity. But what makes IT reactive and inadequate to avoid or deal with outages in the first place?

01 **Scale and complexity:** Environments are increasing in complexity leading to large siloed teams, complex processes, technology diversity, and high frequency of macro and micro induced changes.

02 **Reduced visibility:** The rapid growth of large and complex environments has led to reduced visibility in understanding critical business systems, and how technology components and tools map to them. The problem further aggravates by insufficient instrumentation and logging.

03 **Constant change:** The business as well as the technology landscape observes constant evolution, making it difficult for incident management to keep-up and adapt.

04 **Shrinking operations budgets:** The see-saw battle between RTB and CTB budget allocations never seems to stop.

These situations are commonly correlated with IT instability and business impacts such as revenue loss and poor customer experience.

3. Intelligent Incident Handling?

How can we reduce MTTR and improve the FTR ratio and make the incident management more efficient and effective? The solution lies in an intelligent machine that can augment people on both dimensions:

Effectiveness: It should augment effectiveness by identifying and prioritizing what needs to be acted upon, identifying root cause, and prescribing an action.

Productivity: It should augment productivity by performing the action autonomously.

To reach this level of sophistication, the system must achieve high-levels of maturity simultaneously along two dimensions:

Ability to reason

Ability to act

1.1 Ability to Reason

The reasoning ability can be defined by four levels of maturity:

Descriptive:

The basic level of reasoning consists of the ability to describe the as-Is state of the system. It essentially answers the question "What happened?"

Diagnostic:

The next level of reasoning provides the ability to diagnose using various forms of causality analysis. This reasoningability answers the question "Why did it happen?"

Predictive:

While the previous two reasoning abilities are reactive in nature and can at best provide insights about the system, the predictive reasoning provides foresight and answers the question "What will happen?"

Prescriptive:

prescriptive reasoning forms the most sophisti-cated level of reasoning and answers the question "What should be done about any described, diagnosed or predicted insight?"

With prescriptive level of maturity, a cognitive system can answer the questions "What should we do?", "When?", and "Why?". In fact, with prescription, the system can prevent or eliminate issues through proactive actions. The reasoning ability is made possible by robust AI solutions empowered by creative use of statistics, data mining, and machine learning.

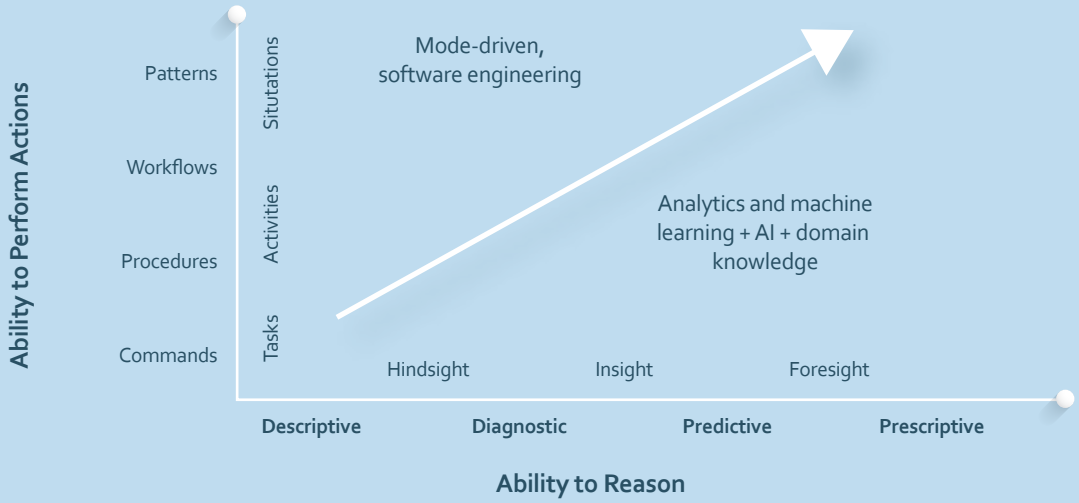


Figure 2: Ability to Reason and Ability to Act

1.2 Ability to Act

The other important dimension of a cognitive system is its ability to act. This dimension can be defined by following levels of maturity:

Perform tasks: The basic level of automation provides the ability to perform point or task automation solutions. This maturity level provides the ability to perform atomic operations, such as OCR tools to extract text from images, monitoring an SAP environment, etc.

Perform activities (Robotic automation): The next level of maturity provides end-to-end process automation and is defined as a composition of tasks. The traditional approach to automation has been robotic automation, which relies upon fully-prescribed and fixed composition logic. This approach only works well when the process steps are context-independent and do not change over time.

Handle situations (Intelligent automation): This is the most sophisticated level of automation, where the end-to-end procedure for performing the activity is inferred and constructed dynamically based on the context. This behavior is much like how humans carry out activities. For instance, the procedure to meet someone for coffee depends upon where you are, the location of the coffee shop,etc., and the meeting is constructed on-the-fly using context, reasoning patterns, and skills.

Most products in the market are attempting to achieve higher levels of maturity along only one of these dimensions. An intelligent incident management system needs to be designed to achieve high maturity levels simultaneously, along both of the higher dimensions.

Figure 3: Integration of ignio with the enterprise IT

4. Our solution : ignio

ignio AIOps provides an intelligent virtual expert that can augment effectiveness and efficiency of people. It has the ability to "understand and learn" the landscape, "reason" to generate insights and make decisions, and back it up with pre-built automation content to perform actions, including executing incident fixes and initiating service and change requests. It enables this with its unique blend of data mining, reasoning, machine learning, and model-driven software engineering.

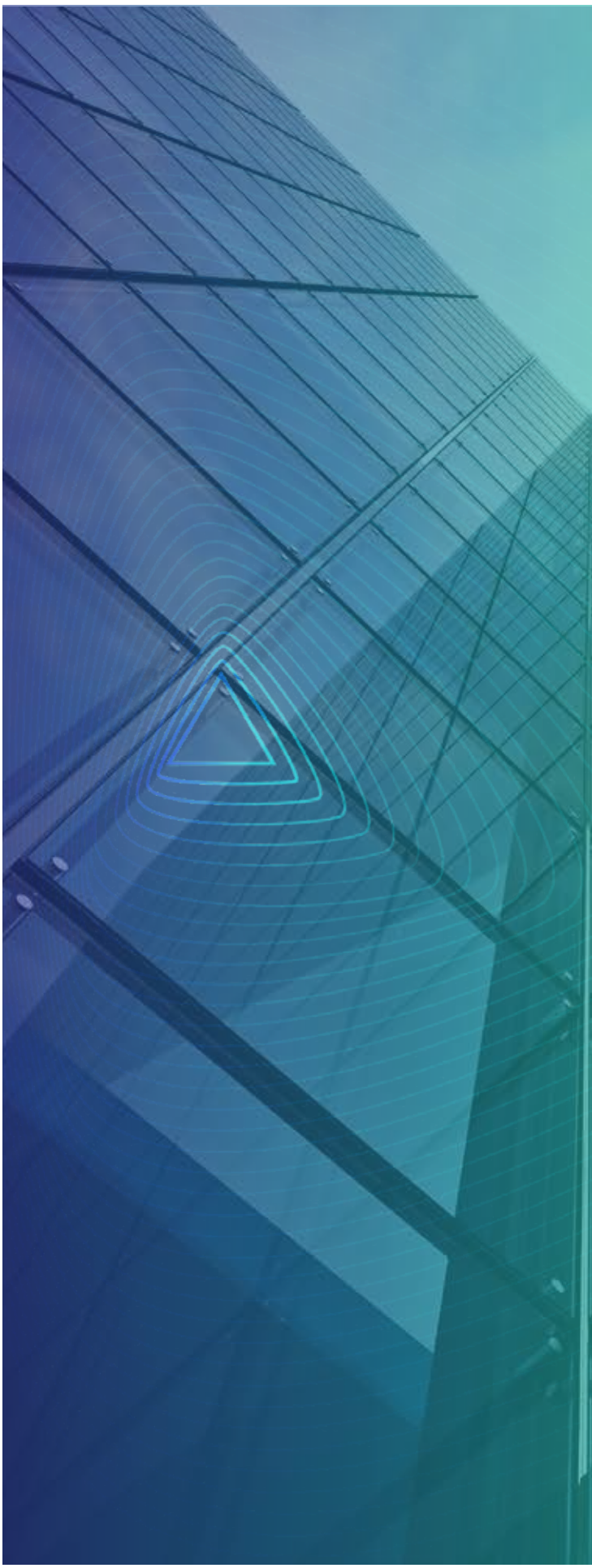
ignio AIOps fits in seamlessly between the application systems, the operations tooling and the operations teams who keep the systems up and running. Figure 3 depicts a typical operation with ignio. ignio AIOps is integrated with service management, monitoring and ITOM tools and the target systems (end points) using a diverse set of integration protocols. As a result, ignio AIOps does not need any agents to be configured on end points.

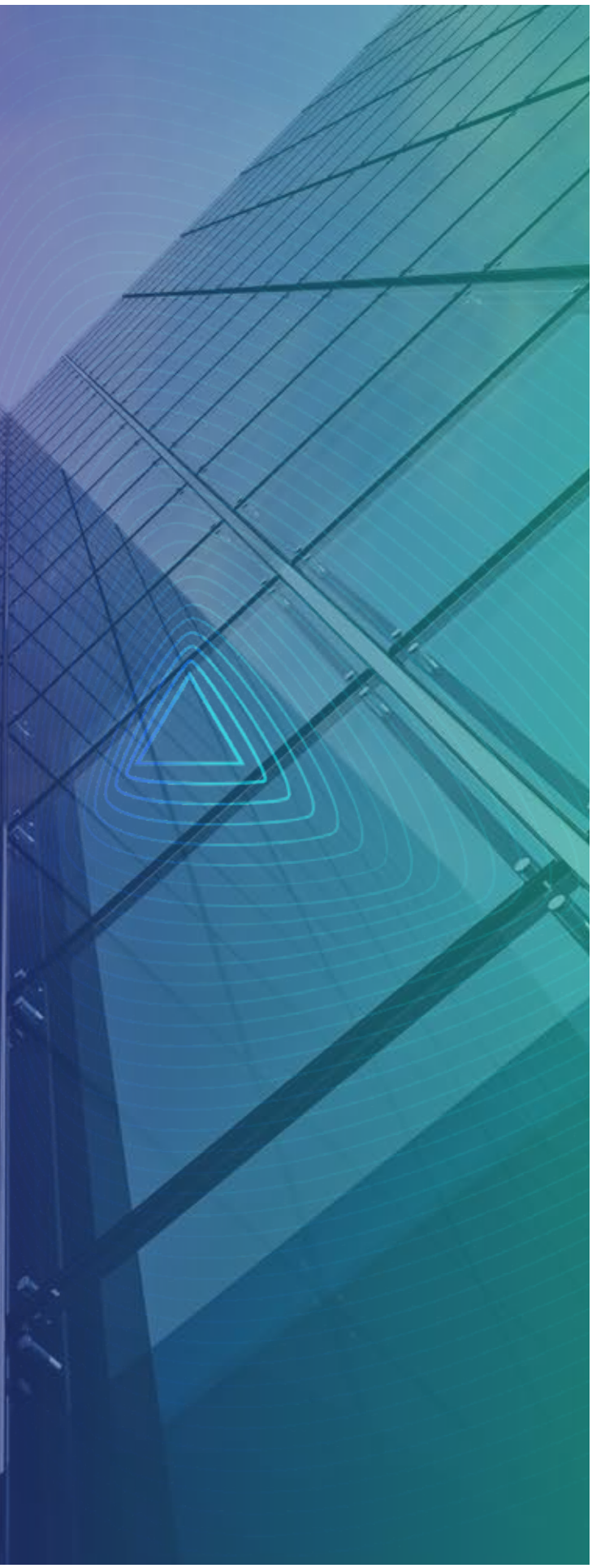
So let us now get inside ignio and see how the incident management lifecycle changes with the introduction of ignio AIOps into the environment. ignio performs incident management with a combination of three features: Learn, Resolve, and Prevent.

Learn: ignio brings deep context awareness. It constructs an end-to-end view connecting business processes to applications to infrastructure. ignio does this by assimilating data from various structured and unstructured data sources such as CMDB, alerting tools, monitoring tools, system logs, as well as, manually maintained data sources. ignio then self-learns the normal behavior of each entity by using various data mining and machine learning techniques to analyze structural and behavioral profiles.

Resolve: ignio provides a lights-out intelligent and autonomous command center.

- ignio manages alerts intelligently to generate just the right alerts at the right time. It enables this functionality using a comprehensive suite of levers. It suppresses false alerts, groups related alerts, prioritizes alerts by inferring their urgency and criticality, and predicting alerts based on observed trends and patterns.
- ignio performs intelligent diagnosis and generates recommendations. ignio on-the-fly infers the potential influencers that can cause the incident, conducts context-aware health-check, localizes the root-cause, and selects remediation action based on contextual





constraints. ignio's auto-triage and resolution is powered by model-based, case-based, and rule-based AI reasoning techniques and augments effectiveness of incident management.

- ignio performs autonomous execution of end-to-end activities. ignio comes preloaded with automation that cover autonomous execution of end-to-end activities, ranging from provision, configure, validate, update/patch, manage state, migrate, and decommission. ignio uses model-driven engineering to handle situations autonomously by constructing a procedure to perform activity on-the-fly based on the context.

Prevent: ignio assesses the "as-Is" state and produces recommendations for proactive planning and improvements.

- ignio predicts future behavior and generates ahead-of-time notifications of potential incidents.
- ignio performs risk assessments, identifying candidates of high risk, and generates recommendations for mitigation.
- ignio provides the ability to perform change-impact analysis to predict the impact of change and prescribes a strategy to adapt.

5. Conclusion

Traditional approaches to incident handling suffer from lack of visibility, unnecessary complexity, inadequate tooling, and lack of expertise in today's operations teams. As businesses demand greater stability and continue to prioritize customer experience, it is imperative that IT operations organizations stand up to these asks. AI- and ML-based technologies offer new opportunities and approaches to address the challenges associated with conventional toolsets and processes.

ignio AIOps brings in a unique combination of intelligence and automation and ability to work across the infrastructure, application and business layers. Faster, automated incident handling capabilities enable the best people in an IT operations team to focus on higher-value work, to improve the environment, not simply sustain it.