A Guide to Intelligent Operations
Digital Requires a New Level of Insight and Control

Digital strategies have caused business executives to intensify their scrutiny of how technology affects bottom line performance. With a growing emphasis on differentiating the customer experience in highly competitive markets, these executives want to understand how their IT systems affect everything from brand perception to customer acquisition and loyalty.
Meanwhile, those same demanding business leaders lack appreciation and patience for the complexity of today’s digital technology environment. While applications and user experiences are simpler and more intuitive, the backend processing, application interdependencies, and underlying infrastructure are more complex than ever, even in light of the benefits of abstraction, virtualization, and cloud computing (see Figure 1.)

While CIOs have long been expected to improve stability and uptime - and done a pretty good job of it - the stakes are much higher in a digital context, where customer switching costs are at all-time lows. Drastically cutting the time to detect and then fix issues is now a strategic mandate. Unfortunately, many enterprise IT departments still can’t satisfy these demands.
The Challenge of Monitoring Today’s Digital Environment

FIGURE 1
Today’s Monitoring Environment is Fragmented and Ineffective

Some of what’s holding back CIOs is the complexity of the environments they inherited, both in terms of the technology to manage and the organizations tasked with doing so. An offshoot of both is that there are now so many tools in place to monitor IT across infrastructure, applications, and digital experiences – too many, in fact.

Add in their close cousins of automation tools and workflow for incident response and remediation, and the problem is exacerbated. According to research of infrastructure and operations executives at AHEAD clients, tool proliferation is a top concern.
Hybrid IT environments ratchet up the complexity
Public cloud and hybrid infrastructures create a fragmented environment that many legacy monitoring tools can’t handle. Everything-as-a-Service delivery models strain the capabilities of traditional monitoring tools, while newer virtualization and abstraction concepts like containers create more questions than answers.

Isolated roles and responsibilities lead to expensive war rooms
Today’s monitoring is spread across siloed teams and tools. When something goes wrong, we might hear from one corner, “Well, it’s not a server problem.” As a result, when a major performance issue occurs, large organizations scramble to set up War Rooms or SWAT Teams with, in some cases, hundreds of members dialing in from across the globe to troubleshoot en masse.

Fractured tools hinder root cause analysis
It may be easy to pinpoint a glaring “red status” issue related to a single network node, but more often what creates an outage or poor user experience involves a web of smaller problems across, for instance, a network device, a server, and a particular database. These connected “yellow status” issues often go undetected or lost in waves of alerts (See Figure 2.)
FIGURE 2
Uncovering Smaller Interconnected Issues is More Valuable and More Difficult
Intelligent Operations Delivers Actionable Insights and a Unified View

The growing urgency to improve technology performance across an increasingly complex environment requires a new approach. While terms like AIOps capture the headlines, some major prerequisites must be met first:

➢ To first deliver a unified view of performance across all IT domains,

➢ To define performance in business terms clearly understood by leadership, and

➢ To close the loop not just with fast remediation but by incorporating learnings back into your architecture and processes.

We call this collective approach, Intelligent Operations, one of five pillars of the AHEAD Digital Delivery Platform. A successful Intelligent Operations strategy consists of four main areas (See Figure 3.)
FIGURE 3
Framework for Intelligent Operations

- Application Performance Monitoring
- Infrastructure Monitoring
- Log Analytics
- Event Management
Infrastructure Monitoring

Using these technologies, infrastructure and operations leaders can collate availability and resource utilization metrics across an increasingly dynamic infrastructure environment, including servers, network, storage; and across public and private cloud infrastructure. Increasingly important in this area, is the need to monitor the costs, compliance, and security of public cloud usage.
Application Performance Monitoring

To ensure that customer-facing applications and business services meet performance standards and provide a quality user experience, tools like AppDynamics offer basic analytics and application discovery, tracing, and diagnostics. The overlap with the other aspects of Intelligent Operations means that the capability also exists to centralize tools and assess server, network, and overall infrastructure metrics in the context of an application.
Log Analytics

Where infrastructure monitoring pulls performance data from infrastructure devices, log analytics collects all of the logs written by an application or a server, analyzes them for event correlation, and attempts to separate signal from noise. This part of the Intelligent Operations story also represents a key integration point to another digital transformation imperative - Integrated Security - using SIEM tools like Splunk to assess and alert to security-related incidents.
Event Management

Typically residing in platforms like ServiceNow, event management also plays a critical role in separating alert noise from signal, but equally important, handles the triggering of IT processes and automated remediation steps in order to reduce mean-time-to-repair (MTTR.) The platform also increases value from existing tools by consolidating events from disparate monitoring tools; an area of overlap with certain Log Analytics products.
A Closer Look at Application Performance Monitoring

Each of the four chapters in an Intelligent Operations strategy not only interconnects with the other three, it’s a journey in its own right. Take Application Performance Monitoring (APM), for example.

Previously, infrastructure leaders would analyze metrics like disk I/O, CPU memory, and storage utilization, and try to use that data to approximate how an application was performing. If usage across certain devices was higher than a certain threshold, the monitoring team would assume an adverse business impact on related applications, and resources would then be deployed to fix the issue.

APM represents an evolution from monitoring resource utilization of the underlying environment to true instrumentation of business services and applications focused on the end user experience, just one of many evolutions in monitoring (See Figure 4.)
FIGURE 4
From the Old to the New in APM

OLD: FOCUSED ON RESOURCE UTILIZATION

- Monitor The Underlying Environment
- Monitor Application Usage Of Key Resources
- Build An Understanding Of What’s “Normal”
- Monitor Availability Of The Environment
- Alert When Resource Usage Is Above Normal
- Get Everyone Across It Into A War Room

NEW: FOCUSED ON USER EXPERIENCE

- Instrumentation Of Business Services And Applications
- Monitor Response Time Of Production Apps To Others
- Understand User Behavior Within The Application
- Identify Users Of Critical Business Functions
- Focus On Performance Received And Achieved
- Map Interdependencies Between Apps And Services

OLD: FOCUSED ON RESOURCE UTILIZATION

NEW: FOCUSED ON USER EXPERIENCE
FIGURE 5
Integration Required for Intelligent Operations for a Large Enterprise
Figure 5 Detail

1-4
Component and application level performance metrics and information are acquired at this level.

5
Event / alert information is sent into BigPanda, which uses Open Box Machine Learning to correlate events and alerts, getting rid of redundant / extraneous alerts and only sending forward alerts that are important and actionable.

6
Information, metrics, and logs are sent to Splunk, which correlates and reports on the data, allowing a graphical understanding of how the components interact, allowing for a deeper understanding of business transactions... capacity planning... infrastructure components in context of business transactions and user impact

7
ServiceNow acts as the central workflow engine, working on events, tickets, manual and automated remediation, auditing

8 & 9
This is the automation / IaC layer, that takes automatic remediation requests from ServiceNow, builds the correct configuration if necessary, and implements the remediation, be it adding servers to applications, adding network bandwidth, restarting services, or other activities and runbooks.

10
This is the platform that runs your business and applications.
As things are changed in 18 by 14, there is a feedback look that runs back through 14 to 12 to close the loop, ensure the issue is corrected by checking current status of 1,2,3,4, closing tickets and creating an audit trail.
FIGURE 6
A Maturity Model for Intelligent Operations

As with all of our Digital Delivery Platform imperatives, AHEAD created a 5-stage maturity model to help guide your Intelligent Operations journey and monitor your progress. Consider this a high-level roadmap.
STAGE 0

Reactive: Troubleshooting

The organization’s monitoring strategy is non-existent or at best, fragmented across siloed teams and disconnected technologies. As a result, monitoring and operations are reactive in nature, where the most immediate need is priority du jour. Visibility into performance is low or not actionable.
The organization has a handle on its various monitoring tools, and as a result, some improved visibility. Therefore, they’re in a foundational starting point for creating a plan for going the Intelligent Operations route. The overall environment is still fragmented, but at least somewhat understood.
The organization looks proactively at application and infrastructure performance but is still more focused on resource usage as a proxy of application performance, more than end user experience. The foundation for Intelligent Operations planning has taken another step forward.
STAGE 3

Optimized: Application Performance Management

The organization is proactive now with all phases of monitoring, able to spot and mitigate issues prior to impact. They now understand the root cause of end user experience issues and business service issues. Process maps have been defined to speed detection through remediation.
STAGE 4

Intelligent: Automation

Runbooks are in place to remediate issues with less manual intervention. A full Intelligent Operations architecture is in place, with the ability to detect and diagnose smaller, interconnected “yellow status” issues spread across applications and infrastructure, including robust SIEM capabilities.
Expected Business Outcomes from an Intelligent Operations Strategy

Hold yourself, your team, and your technology partners accountable to the following business outcomes associated with an Intelligent Operations journey.

- Higher System Uptime and Availability
- Reduced Mean-time-to-Detect (MTTD)
- Reduced Mean-time-to-Repair (MTTR)
- Elimination of Overhead Initiatives, Such as War Rooms
- Longer Time on Page or In Application
- Higher Return Rates / Purchases
- Higher Customer Satisfaction
- Improved Internal End User Productivity
- Headcount Reduction from Automated Monitoring and Remediation
FIGURE 7

Continuum of Analytics Applied to IT

- Monitoring
- Intelligent Operations
- AIOps

- Descriptive
- Diagnostic
- Predictive
- Prescriptive
Questions to Ask Yourself to Establish a Baseline

› Can you identify your business-critical applications, transactions, and services?
› Are they being adequately monitored?
› What pain points are you experiencing in delivery of services to your business?
› Do you have blind spots in system performance and delivery?
› Are your capacity management efforts effective? Are they reactive or proactive?
› Are you able to articulate an enterprise monitoring strategy or direction?
› Do you have siloed teams with their own monitoring tools?
› Are you experiencing false positives or missing critical events?
› How are event management, workflow, and remediation addressed today?
› What automated remediation capabilities do you have today?
Our Expertise Sets Us Apart. Our Passion Puts Us AHEAD.

ACTIVITY 1

Intelligent Ops Visioning Workshop

In this executive one-day workshop, we report out our assessment of your current monitoring environment, processes, KPIs, and architecture, discuss the various stages of maturity applied to your context, then facilitate a new course along the Intelligent Operations maturity continuum.
ACTIVITY 2

Application Performance Monitoring Foundation

APM is often an ideal starting point for an Intelligent Operations journey, because of how customers demand simplified user experiences from across applications that are increasingly dispersed and interdependent. The AHEAD APM Foundation engagement delivers the following:

- Identifies the applications, transactions, infrastructure metrics, business metrics, KPIs, logging, and other information that is critical to understanding the health of applications across your enterprise.

- Identifies where the above data can be acquired, identifying the correct tools to collect, store, and correlate and analyze the data, including rationalization of current tools to understand the gaps and overlaps.

- Identifies what is normal and when deviations or anomalies happen, and who is responsible for taking action on events, leading to a robust playbook / knowledge base for taking action, including automated remediation where appropriate.
ACTIVITY 3

Monitoring Tool Rationalization

Gartner lists 37 different vendors or open source projects in the IT infrastructure monitoring category alone, and that doesn’t include APM or public cloud monitoring and optimization services like AHEAD CoPilot®. With these vendors incorporating additional features every month, our clients see a lot of functional overlap in tools that they already possess. AHEAD will evaluate your tooling to look for areas to get more efficient in your current coverage, as well as set you up for the longer-term Intelligent Operations journey.
ACTIVITY 4

CoPilot Cloud Optimization and Governance

The public cloud presents unique challenges when it comes to ongoing assistance and visibility into usage, billing, and security. CoPilot is a subscription-based offering combining tooling and insights with ongoing remediation and configuration services, all designed to optimize cloud environments.

- Maintain cloud control with security and compliance
- Get assistance with configuration and deployments
- Gain visibility and continually optimize cloud usage
Intelligent Operations is one of five imperatives that comprise the AHEAD Digital Delivery Platform.

The other imperatives are:

- Relentless Automation
- Integrated Security
- Scaled DevOps
- Enterprise Cloud