2020 and beyond: IT Ops facing change, disruption and the unknown

More dependent than ever on smooth-running IT operations, organizations of all sizes and from every industry face daunting challenges in providing uninterrupted, high-quality services. Solutions leveraging artificial intelligence/machine learning can help by simplifying and automating different aspects of IT incident detection, investigation, and resolution.

Life was already getting dicey for IT Operations teams, with increasingly complex, noisy, and constantly changing IT environments. Most of the digitally dependent companies employing them couldn't hope to execute even basic business functions—much less compete successfully—without 24 x 7 access to powerful, distributed, and increasingly complex IT infrastructures.

Then came COVID-19.

Virtually overnight, many employees, including IT staff, were suddenly forced to work from home as the world went online and the demand for digital services skyrocketed. As if dealing with this new demand wasn't enough, the vast workplace migration upended many existing IT processes.

For IT professionals, the work-from-home edicts posed a number of challenges. For example, network operations center staffers who were accustomed to sitting in rooms equipped with a variety of monitors now had to track and manage all of their critical infrastructure from a single laptop screen at home.

The sudden and open-ended demands caused by COVID-19 confirmed what many of these professionals had already determined: To have any hope of meeting their growing list of needs and demands, IT Ops requires rapid infusions of artificial intelligence (AI)–enabled and automated technologies.

Even before the pandemic struck, IT Ops teams were inundated with a deluge of infrastructure alerts. Manually sifting through thousands of alerts to identify and address the handful that posed real threats had become next to impossible for many teams. That's why many were already exploring ways in which AI and machine learning (ML) could drive AI-enabled IT operations (AIOps) and help them do more with less.

A survey conducted by IDG Research in the early days of the pandemic explored the IT Ops challenges that companies are now facing. Among other topics, the survey gauged the benefits that AIOps can deliver to IT Ops teams and their organizations.

The Limitations of Legacy IT Monitoring Tools

To keep tabs on their complex IT environments and keep them and their organizations humming, IT Ops teams have deployed a wide variety of monitoring tools. The problem: Each of these tools tracks just a subset of the overall IT infrastructure, and, collectively, they generate far too many alerts for IT Ops personnel to manage.

The tools' siloed, disparate nature makes the detection and analysis of issues and outages extremely difficult for IT Ops teams. Team members can often spend hours on unproductive bridge calls and forensic efforts trying to identify and resolve problems, all while expensive resources are taken offline.

To address these challenges, growing numbers of organizations are turning to AIOps, which incorporates AI/ML technologies into IT Ops tools for detecting and analyzing incidents as well as automating parts of incident investigation and remediation. AIOps-enabled tools can automatically sort through and consolidate the blizzard of alerts and, increasingly, identify the root causes of problems and help IT Ops teams quickly address them.

Complex IT Environments Generate a Tsunami of Alerts

IDG Research surveyed 100 IT professionals with manager titles or above who had IT Ops, networking, or engineering-related roles. The respondents worked in more than a dozen industry sectors, and nearly three-quarters (73%) of them were involved in IT incident investigation, remediation, and/or management.

IT infrastructure among the surveyed organizations was broadly distributed, with 60% having on-premises IT infrastructure, 57% public-cloud-based infrastructure, and 47% private-cloud-based infrastructure, plus 24% using commercial data centers such as Rackspace. One-third had both on-premises and public-cloud-based infrastructure.

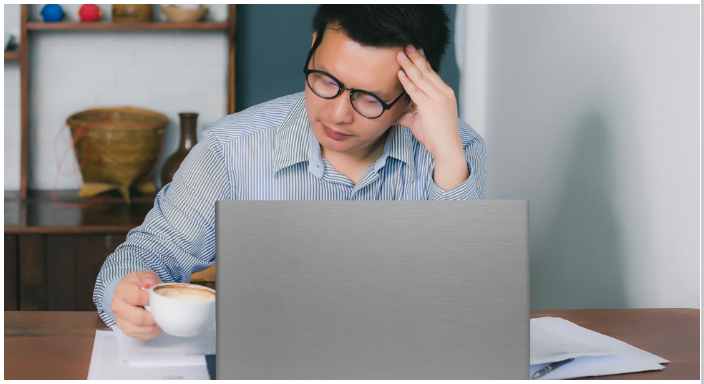
Almost all of the companies had multiple IT teams in place to support the range of IT and business services deployed. On average, the respondents had 12 distinct IT teams, with 36% having 16 or more.

Collectively, these teams used a variety of tools, such as application performance monitoring tools, IT infrastructure monitoring tools, network monitoring tools, and log monitoring tools. The average respondent organization was using 20 different monitoring tools, with 16% of the organizations using more than 50 such tools.

On average, for each of the organizations surveyed, these constellations of monitoring tools were generating more than 14,300 alerts per day . Two-thirds (65%) of the survey respondents said the frequency of alerts had increased during the prior 12 months.

Just under half (44%) of the alerts received were caused by infrastructure or software changes, making such changes far and away the leading alert source in modern IT environments. Regardless of the cause, major incidents proved difficult to investigate and resolve, requiring 12 hours, on average, for IT Ops teams to determine their root causes.

The key takeaway: Complex and ever-changing IT environments require many different tools. These disparate tools generate massive numbers of siloed alerts that must somehow be consolidated, assessed, and resolved.



Alert Overload Strains Staff, Undermines Business Objectives

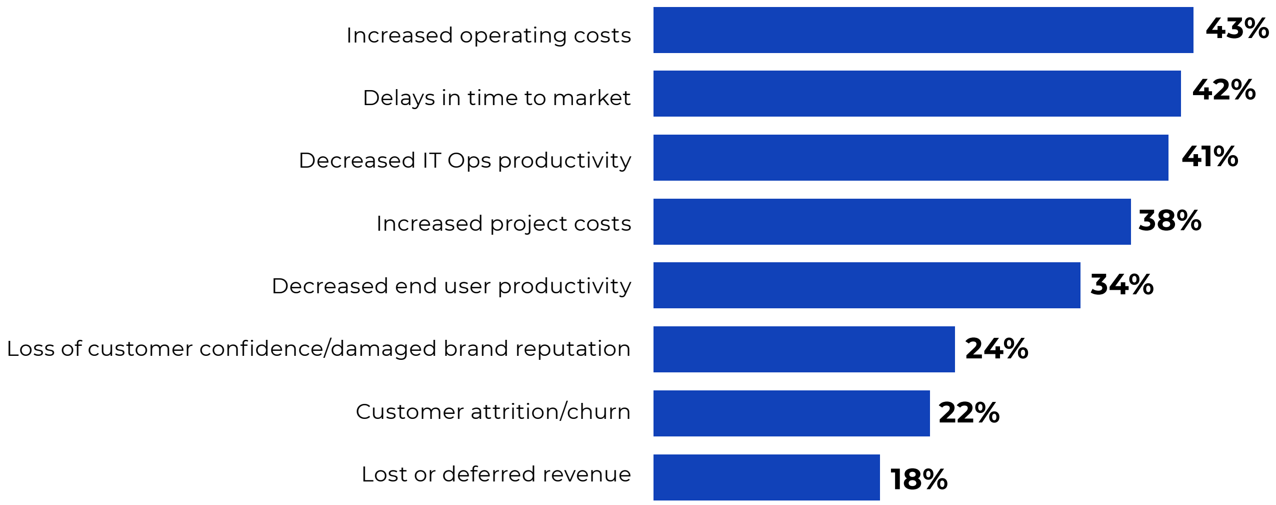
IT pros encounter numerous problems when trying to detect and resolve incidents before they impact employees, customers, and others. The top-ranked challenge, cited by 47% of the respondents, was coordinating IT incident or outage detection, analysis, and response across siloed IT teams. Nearly as many (45%) said that it was difficult to identify needs and to bring the appropriate IT Ops skill sets to bear on any given problem.

Other common challenges included a lack of context for alerts (37%), data/noise overload (36%), and lack of visibility into infrastructure topology (30%).

Predictably, these IT challenges—driven by siloed teams and disparate tools—hinder operational visibility and context. That, in turn, translates into significant business impacts. As shown in Figure 1, increased operating costs and longer time to market topped the list of eight identified business consequences.

IT incident management challenges impact the business in multiple ways including *increased costs, delays in time to market*, and *decreased productivity within IT ops.*

Figure 1: Business Impact of IT Incident Management Challenges



57%

of **those in a DevOps/Engineering function** most often cite **delays in time to market** as the top business impact.

A Patchwork Incident Management Scene, Complicated by COVID

As noted, many legacy monitoring and management tools have limitations that hamper their effectiveness. When asked about the capabilities of their deployed tools, the respondents gave mixed assessments. In only one area—providing an efficient means of communication/collaboration within IT Ops teams—did more than half of the respondents say their tools enabled the needed functionality “to a great extent” (see Figure 2).

The emergence of COVID-19 has added to the challenges faced by hard-pressed IT Ops teams. When asked how the pandemic has impacted their organizations, 42% of the respondents said they have had “to a great extent” needed to make changes to many of their IT processes to support the new flood of remote workers. Most of the remaining respondents (40%) said they have had to make such changes “to some extent.”

In short, the COVID-19 pandemic has largely removed any remaining doubts: IT Ops needs to transform—and transform now.

While more than half indicate current IT monitoring and incident management toolsets enable *team communication/collaboration* to a great extent, it appears to be more challenging to enable *IT incident correlation* or *researching incident history/context.*

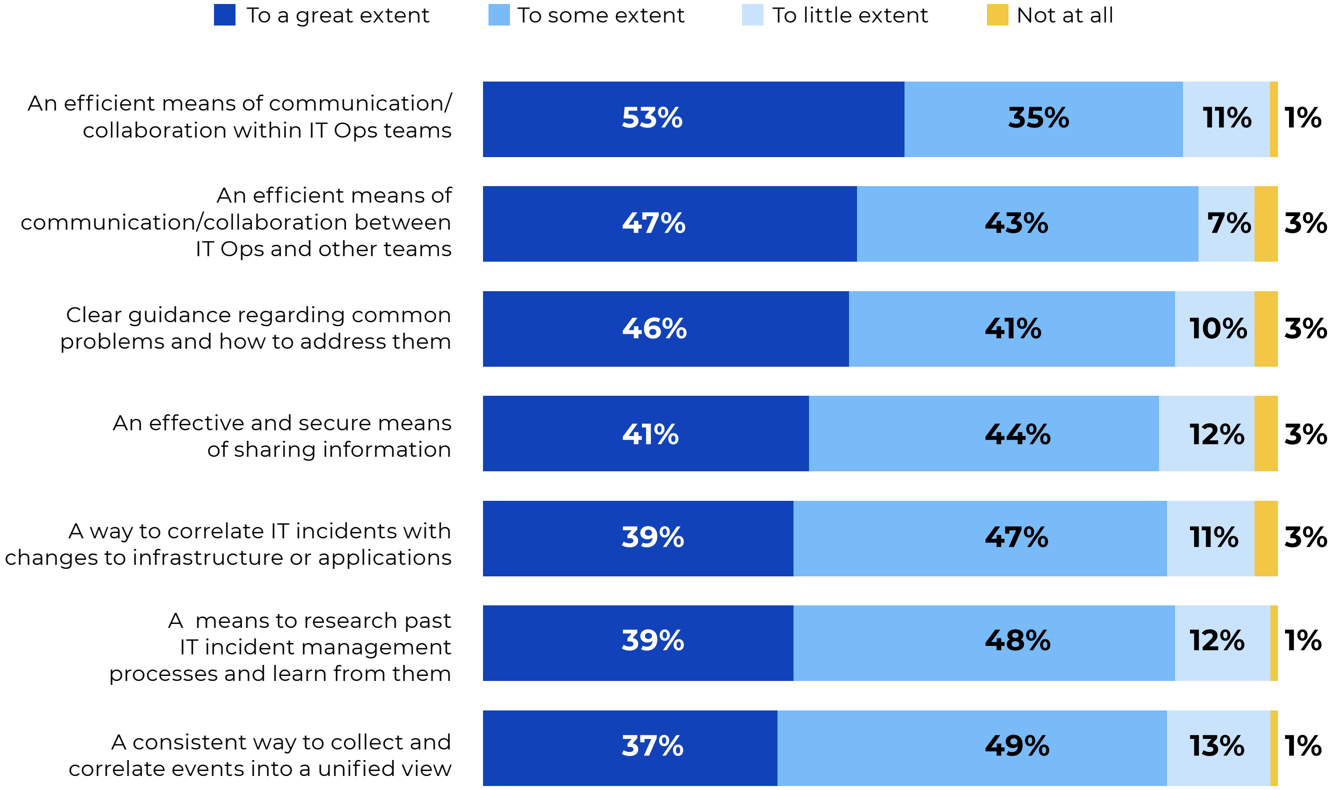


Figure 2: Capabilities of Current IT Monitoring and Incident Management Toolsets

Sponsored Content

Investing in Automation and AIOps

Given the many demands they face, it isn't surprising that nearly 80% of those surveyed expected their budgets for IT Ops to increase either slightly or significantly in the coming year. As shown in Figure 3, the top area of anticipated IT investments, cited by nearly two-thirds of the respondents, was improving the level of automation for IT incident management.

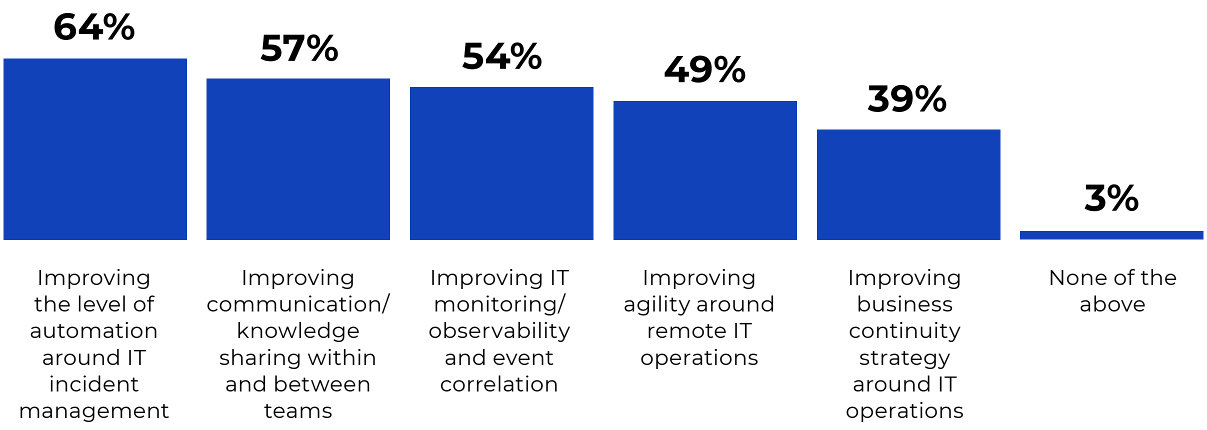
Fortunately, many of the identified needs can be fully or partially addressed by AIOps investments and solutions. Among those surveyed, 20% already had AIOps solutions in place and another 24% were actively considering such solutions.

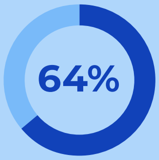
Among those already using or considering AIOps, the solutions aligned well with the planned areas of IT investment shown in Figure 3. For example, 70% of these respondents said these solutions were being, or would be, used to enhance IT incident response.

Even those respondents at organizations not yet considering or using AIOps solutions thought they could deliver a range of benefits. More than half of this subset, for example, said that AIOps, if deployed, could help them route incidents to the right teams and also automate incident resolution and remediation.

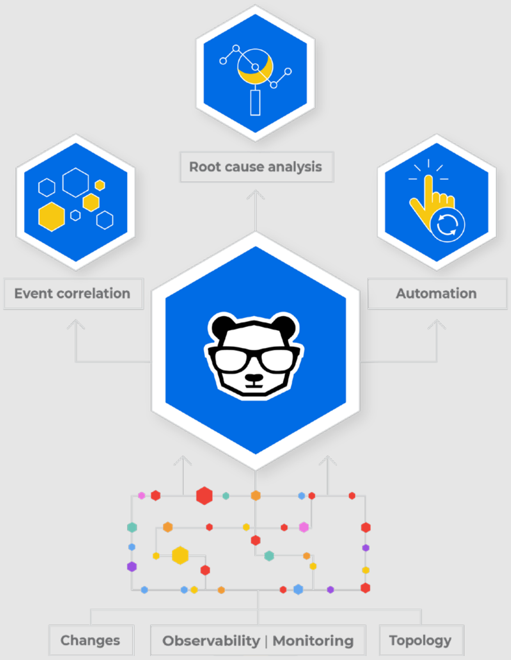
More than half of respondents expect increased IT investment over the next 12 months in *automating IT incident management, increasing communication/knowledge sharing,* and improving *IT monitoring and event correlation.*

Figure 3: Areas of Expected IT Investment





Improving communication/knowledge sharing, within and between teams is the top area of expected increased investment among those **involved in IT incident investigation, remediation, and/or management.**



Conclusion and Call to Action

BigPanda was founded specifically to help IT Ops, NOC, and DevOps teams handle more incidents than before, and faster than before, by taking advantage of its AI/ML-powered solutions—across different aspects of the incident management lifecycle: detection, investigation, workflow automation, and resolution.

The company's Open Integration Hub offers a broad set of ready-to-use connectors for a variety of monitoring, change, topology, and collaboration tools, enabling IT Ops teams to easily add BigPanda to their existing IT Ops tool stack. They can make this addition without forcing a "rip and replace" of their existing tools, without breaking their existing workflows, and without forcing them to drastically change their processes.

Once alerts are ingested from various enterprise monitoring tools (including legacy, homegrown, custom, and modern commercial tools), Open Integration Hub enriches them with contextual data gleaned from configuration management databases (CMDBs) and other sources of topology data.

BigPanda's Open Box Machine Learning uses a collection of ML algorithms to process and correlate all the collected and enriched IT alerts in real time, factoring in topology, context, and other relevant information. In addition to reducing noise by 95% or more, BigPanda's solution can detect incidents and surface the probable root cause of those incidents in real time.

BigPanda's platform simplifies, accelerates, and automates many of the most onerous manual detection, investigation, and remediation functions. For maxed-out IT Ops teams and their organizations, the solutions can reduce operating costs, improve application performance and availability, and accelerate business velocity.

For more information about how BigPanda and its AIOps solutions can help your organization better identify and resolve IT infrastructure incidents, go to

www.bigpanda.io