RESOLVE

Incident Response Reimagined:
A Strategic Investment for Financial Gains

Executive Summary

Quick incident response is absolutely imperative for businesses today, but 2023's rise in business demands, economic shifts, and urgency for digital transformation create too many tasks for network, security, and IT operations teams to handle.

Businesses simply cannot afford to have mission critical applications down, and many struggle to avoid downtime. Eighty-two percent of companies experienced at least one unplanned downtime incident from 2019-2022.

Downtime can come with a price tag well over a million dollars. For instance, Facebook in March 2020 encountered an unexpected, 14-hour outage that caused an estimate of $89.6 million in lost revenue. A few years prior, an outage at Atlanta-based Delta Airlines resulted in about $150 million in revenue loss.

IT plays a critical role in keeping costly downtime to a minimum, if not preventing it all together. IT incidents most often directly impact revenue, so businesses must keep applications running properly.

Resolve in a study of three customers documented the return on investment (ROI) of automating incident response activities to help others advance their automation goals.

Interviews with Resolve customers and consecutive financial analysis found the participating organizations experienced total benefits of $12,292,863 over three years and provided a framework for organizations to evaluate the potential financial impact of Resolve's Incident Response Automation solution.

Cost Reduction Labor Savings

Our study found significant cost reduction savings of $4,621,788. The study's participants tracked and reported on costs and cost reduction by task, across 10 IT service desks, as well as monitored the exact number of staff needed based on volumes.

Cost Avoidance Labor Savings

The companies included in the study, across 10 IT service desks and 1,000 agents, reached significant cost avoidance savings totaling $7,671,074.

Customer Satisfaction

Average alarm acknowledgment time fell from 1,889 minutes (31 Hours) to less than one minute, along with a notable improvement in mean time to resolution (MTTR).

Consistent Processes

The study's participants standardized their processes, which resulted in positive employee morale and enhanced customer satisfaction.

What's Really Stressing Leaders Out?

Organizations are facing extremely difficult challenges as they work to meet business needs, especially from disruptions that are unexpected. Change proves to be unpredictable, as we've seen in recent years.

Far from minor, today's technological developments have the ability to transform an entire organization.

Artificial intelligence (AI), machine learning (ML), the internet of things (IoT), Generative AI (genAI), cloud computing, 5G network protocols, and more have all exploded due to new patterns like connectivity demands, hybrid and remote work models, economic twists and turns, and decision-making best practices within businesses.

Ever-faster technological development, while innovative and opportunistic, also requires organizations to keep up with shifts and evolutions. The speed and intensity at which technological advancement accelerates creates a great sense of urgency to overcome them.

The stakes are especially high when business-threatening incidents arise. Cybersecurity issues from ransomware attacks leave no room for error, and incident response teams must be equipped to respond efficiently and effectively in an instance, in order to maintain business continuity.

The intense, potentially jeopardizing obstacle course of incident response is reflected in today's most pressing challenges, and leaders are adjusting their top priorities accordingly, not just for incident response management, but for protecting the business.

Top 10 Incident Management Challenges

Incident escalation is expensive

Incident resolution takes too much time, tarnishing the customer experience

Too much event noise causes missed alerts and operational inefficiencies

Some events have a larger impact on the business than others

Reduction of labor and costs is required, but also while managing a growing network and having fewer resources

Supporting network growth demands and product expansion, while struggling to meet existing SLAs

Decreasing customer satisfaction causes unsettling churn within the organization

Deviating, confusing incident response processes allow for poor customer satisfaction

Customer service complaints related to inconsistent incident response reduces employee morale

Managing data from multiple systems creates inefficiencies

Key Results Attributed to Automation

What happened when IT teams automated their incident response?

Today's historical, profound growth in data causes disruption in economies and business around the globe, which can shake up an IT department as challenges emerge. They're dealing with a never-before-seen telemetry of alerts, events, and other signals, and the business depends on IT to triage this alarming influx of issues. IT, no matter the size of its staff, has been struggling to manage these alerts with enough speed and accuracy. Only the most critical alerts get the team's attention, yet the others should also be looked at as symptoms of potentially an impending outage if left alone.

5 Main Benefits of Implementing Automation

1   **Data Insights**

Organizations can track incident response processes and metrics.

- How many alarms were acknowledged and how long did it take on average?
- How many trouble tickets were created and how long did the resolution take?
- How many devices and logins were needed to perform triage and diagnostic repairs?

2   **End-to-End Process Automation**

Companies can automate all feasible tasks across existing silos, leaving IT staff to handle only the value-add tasks.

3   **Acceleration of Incident Response and Resolution**

Human-guided automation, real-time incident collaboration, and the ability to fully and partially automate processes will improve MTTR.

4   **Significant and Ongoing Cost Reduction and Cost Avoidance**

Organizations can use trackable metrics to report on cost reduction and cost avoidance by task and service desk.

5   **Process Standardization**

Incident response processes are clearly documented and available across IT teams. Standardizing the process improves customer satisfaction and employee morale.

Improving MTTR with incident response automation with human-free, automatic triage of events minimizes impact on the business when issues spike, and most importantly can address problems before they impact the customer experience. Chief Information Officers (CIOs) rank financial loss as the most severe product of network outages as it slashes customer goodwill that took years to build, causes data loss, and can destroy company and brand reputation.

The need for automation is clear. Streamlining operations and boosting network resiliency to dodge downtime is critical for avoiding financial and reputational damage.

Building a Use Case: Using Realistic Data on Risk-adjusted Benefits and ROI

Background

Automating tedious tasks empowers IT teams and creates the space needed for important, vital jobs, which significantly improves efficiency, productivity, and cost savings. Research shows enterprises realize a potential return on investment (ROI) by deploying incident response automation, yet many organizations still use legacy tools and manual processes. For this part of the study two customers were interviewed with very similar use cases related to incident response.

Customer 1

14+
Service desks

1000
Service desk agents

Customer 2

1000
Service desk agents
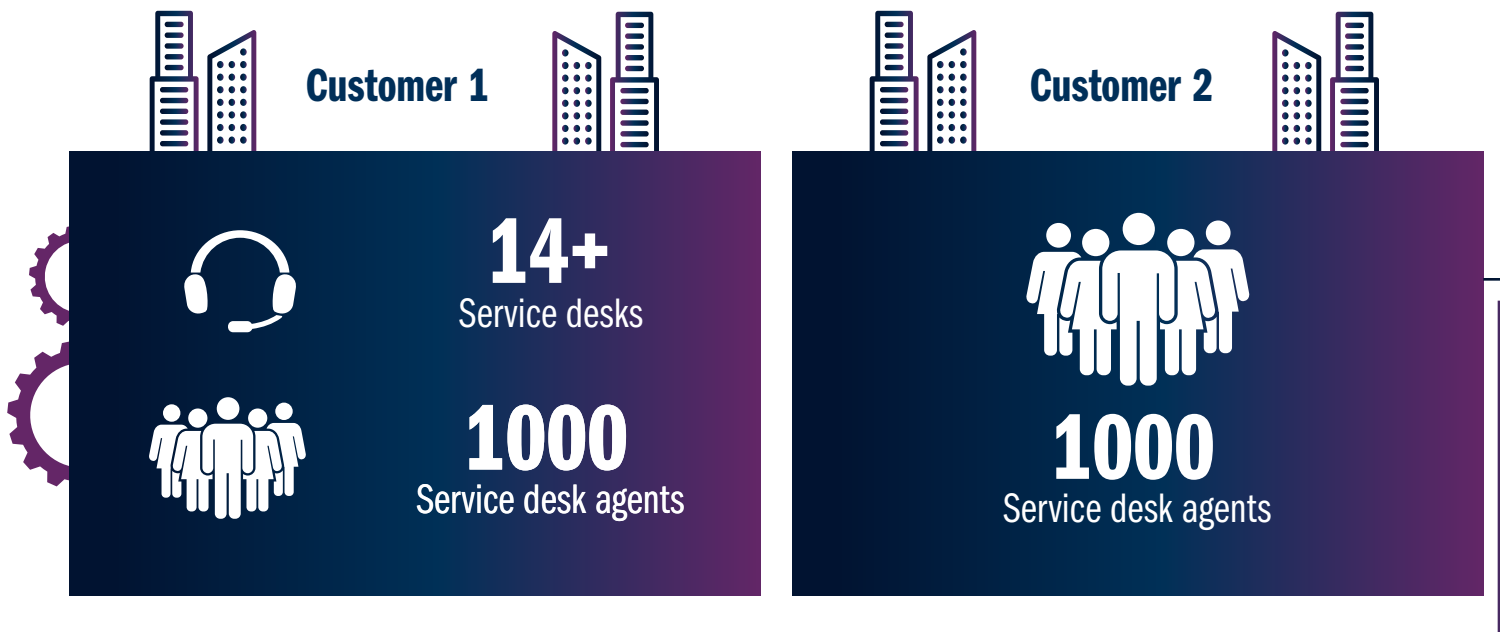
Resolve Actions was used to automate and orchestrate operations across their service desk organization of 1,000. Workflows were automated that touched their systems across observability platforms, security management, network management, knowledge management, ITSM ticketing systems, network devices, DevOps, and configuration management systems.

The service desk is responsible for more than 100 network service provider equipment vendors, including routers, switches and digital subscriber line access multiplexers (DSLAMs), and voice switches.

Our interviews with the customers found that on average, they experienced total tangible ROI from automation amounting to a present value (PV) of $12,292,863 over three years with implementation and labor costs amounting to $3,533,634, equaling a net present value (NPV) of $8,759,228 with a payback period of one month and an ROI of 248%.

Financial Analysis
Quantified Benefit and Cost Data

Total Benefits Across Two Customers					
Benefits	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Cost reduction labor savings	$728,000	$2,475,200	$2,548,000	$5,751,200	$4,621,788
Cost avoidance labor savings	$1,820,000	$2,912,000	$4,804,800	$9,536,800	$7,671,074
Total benefits (risk-adjusted)	$2,548,000	$5,387,200	$7,352,800	$15,288,000	$12,292,863

ROI
248%

Benefits PV
$12.3 million

NPV
$8.7 million

Payback
one month
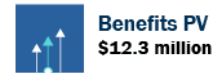
Cost Reduction Labor Savings: Metrics Remove the Guesswork

Saving costs related to labor practices is part of sound organizational operations, and sometimes, that means a reduction in headcount. While no company wants to part ways with its talent, emerging technological advancements can lead to and allow for increasing team capacity without really adding headcount.

IT professionals should dedicate their time and effort to high-value work that impacts the business instead of repeating endless simple tasks that don't move the needle.

Cost reduction labor savings stems from determining exactly how much headcount your company needs based on volumes, per tracking data on costs and costs reduction by task. Resolve's automation solution's trackable metrics takes the guesswork out of an organization's budget as it relates to number of employees, increasing efficiency, and potentially saving millions of dollars.

Cost reduction labor savings
- 38% of total benefits

$4.6 million
3 year
benefit PV

38%
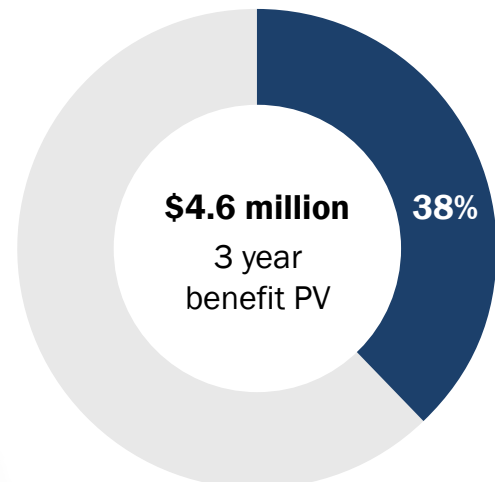
Putting Automation to Work

The customer's average alarm acknowledgement time was 1,889 minutes before any automation was put in place. It took the IT team over 31 hours to get to an alarm at the time a customer's network was down, which failed to meet the SLA's requirement of four hours.

The organization had to use process automation to comply with the SLA, rather than a piecemeal change.

Resolve Actions workflows enabled the organization to optimize the process and bring the alarm acknowledgement time down to about one minute.

The Resolve workflow performed the following tasks:

Created the trouble ticket in their ITSM tool with all the information

Logged into the troubled device to validate the alarm

Updated the diagnostic notes in the trouble ticket

Executed resolution procedures if they were defined or escalated the alarm to an agent

The customer reported cost reductions that they achieved as a direct result of process automation, which also empowered them to predict and track the exact staff size needed based on alarm volumes.

Tracking Metrics

Customer satisfaction will plummet while waiting for a web application to be restored, and the average of 31 hours doesn't come close to meeting their expectations. Customers believe web applications should be user-friendly, run smoothly, and do so continuously without flaw.

More users are in the same place at the same time due to the rise of remote work and online resources for goods and services, so web applications have to handle an increasingly larger crowd. Automation, in addition to scaling properly, makes incident response faster and more effective by reducing wait times.

Financial Analysis

The customer's average alarm acknowledgement time was 1,889 minutes before any automation was put in place. It took the IT team over 31 hours to get to an alarm at the time a customer's network was down, which failed to meet the SLA's requirement of four hours.

The organization had to use process automation to comply with the SLA, rather than a piecemeal change.

Resolve Actions workflows enabled the organization to optimize the process and bring the alarm acknowledgement time down to about one minute. The Resolve workflow performed the following tasks:

Cost reduction labor savings	A1 * A2	$910,000	$3,094,200	$3,185,000
Risk adjustment	↓20%			
Cost reduction labor savings (risk-adjusted)		$728,000	$2,475,200	$2,548,000

Assumptions:
- An industry average fully loaded cost of $91,000 for the service desk staff
- 20 percent risk adjustment to account for attrition of redundant headcount, resulting in delays in achieving the savings

Tracking metrics allowed the study's organizations to confidently reduce headcount over three years. In the third year, they saved an average of $2,548,000 (after risk adjustment) by lowering their staff size by 35.

Average savings of $2,548,000

Cost Avoidance Labor Savings: Incident Response Down by 27 Hours

Workloads in IT departments are increasingly heavy as alert volumes continue to climb and customer expectations become harder to meet. Required to do more with less, IT teams must adjust for higher work volumes, but keep headcount the same, if not lower it.

Unable to complete the work at hand manually, IT can use incident response automation to relieve pressure and lighten the load. IT teams can then have the bandwidth to better handle costly tasks, as well as execute work that aligns with business goals.

Cost avoidance labor savings - 63% of total benefits

63%

$7.7 million
3 year
benefit PV
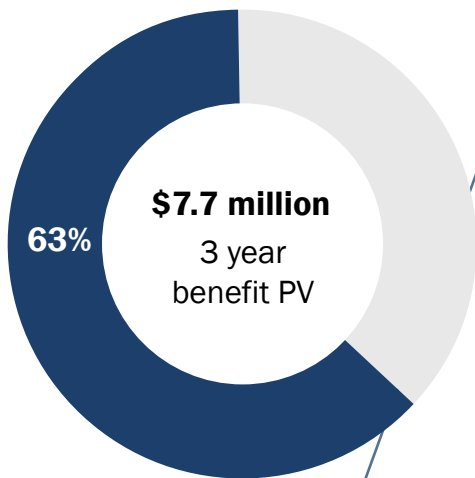
Tracking Metrics

As with Cost Reduction Labor Savings, automation reduced incident response time by 27 hours.

Resolve's automation, in the study, unlocked support for all-new networks and the steep volume of alerts it received. It contributed to a significant drop in MTTR, exceeding the acknowledgment time goal of four hours and coming in at one minute.

There was an additional headcount reduction measured, as in the third year, with an Ongoing Full-time Employee (FTE) Avoidance of 66 and an Ongoing FTE Cost Avoidance Savings of $4,804,000 was recorded (after risk adjustment).

Before automation, as the study indicated, IT service desk professionals spent an average of six minutes manually gathering data from a broad spectrum of infrastructure services to diagnose customer issues. Implementing automation allowed the same task to take far less time, with an average of only four seconds. It meant customers didn't have to wait nearly as long, and IT teams could produce more work in less time.

Putting Automation to Work

A high volume of alters was purposefully set up to help agents catch a problem before it turned into an outage. Too much for the team to handle, this pre-diagnosis step dramatically increased customer wait times.. Service desk staff were spending an average of six minutes manually gathering data from a broad spectrum of infrastructure services to diagnose customer issues.

The need to do more with the resources on-hand drove them to automation. The customer deployed Resolve Actions to support the new networks and the sheer volume of alarms. The Resolve workflow solution automatically gathered the required data based on the alarm in a remarkably low four seconds, reducing customer wait times and increasing technician productivity.

Financial Analysis

Cost avoidance labor savings	B3	$2,275,000	$3,640,200	$6,006,000
Risk adjustment	↓20%			
Cost avoidance labor savings (risk-adjusted)		$1,820,000	$2,912,200	$4,804,000

Assumptions (constant):
- An industry average fully loaded cost of $91,000 for the service desk staff
- 20 percent risk adjustment to account for attrition of redundant headcount, resulting in delays in achieving the savings

The participating organizations used tracking metrics to reduce headcount over three years. In the third year, they saved an average of $4,804,800 (after risk adjustment) by lowering their staff size by 35.

Components of Incident Response That Were Automated

Acknowledging an alarm

ITSM ticket creation with all the right details

Alarm validation by confirming the device state

Diagnostics and data collection from all related services

Ticket enrichment to keep the ITSM most current with all findings

Auto-remediation of issues by executing the resolution procedures

Escalation to an IT team or SME with all the required information where auto-remediation cannot be applied

Flexibility for the Future

Automation opportunities and uses can unfold at times and for reasons unique to an organization and its future.

Flexibility and investing in additional capacities or capabilities that could lead to business benefits gives a green light to organizations to engage in future initiatives. Some companies value flexibility more than others, and the measure of its value also varies.

An organization can implement automation, and later down the road, need to capitalize on new automation use cases as they present themselves. In this case, for example, a user calls into the service desk for help, but there's a significant knowledge gap between the reason for the call and how the technician interprets it.

Automation provides a single pane of glass that unifies and presents data from across many integrated systems, including:

- Service management
- Event management
- System/network management
- Configuration management
- Network devices
- Knowledge management
- Ticketing systems
- Trouble ticket dispatch
- Change management

Technicians gain the ability to better identify the problem and work with the user to resolve the solution.
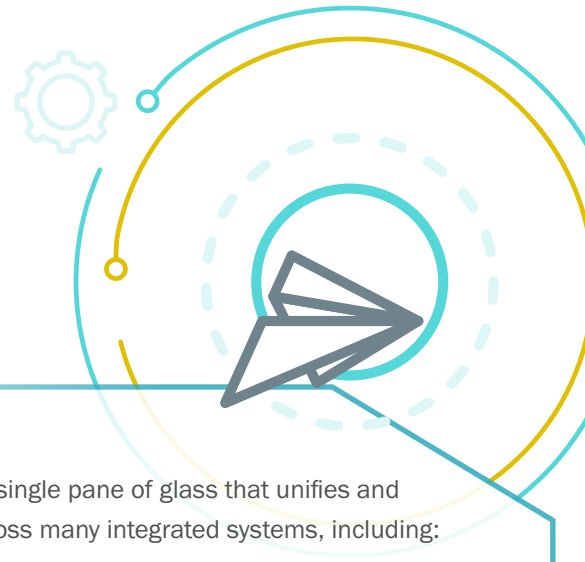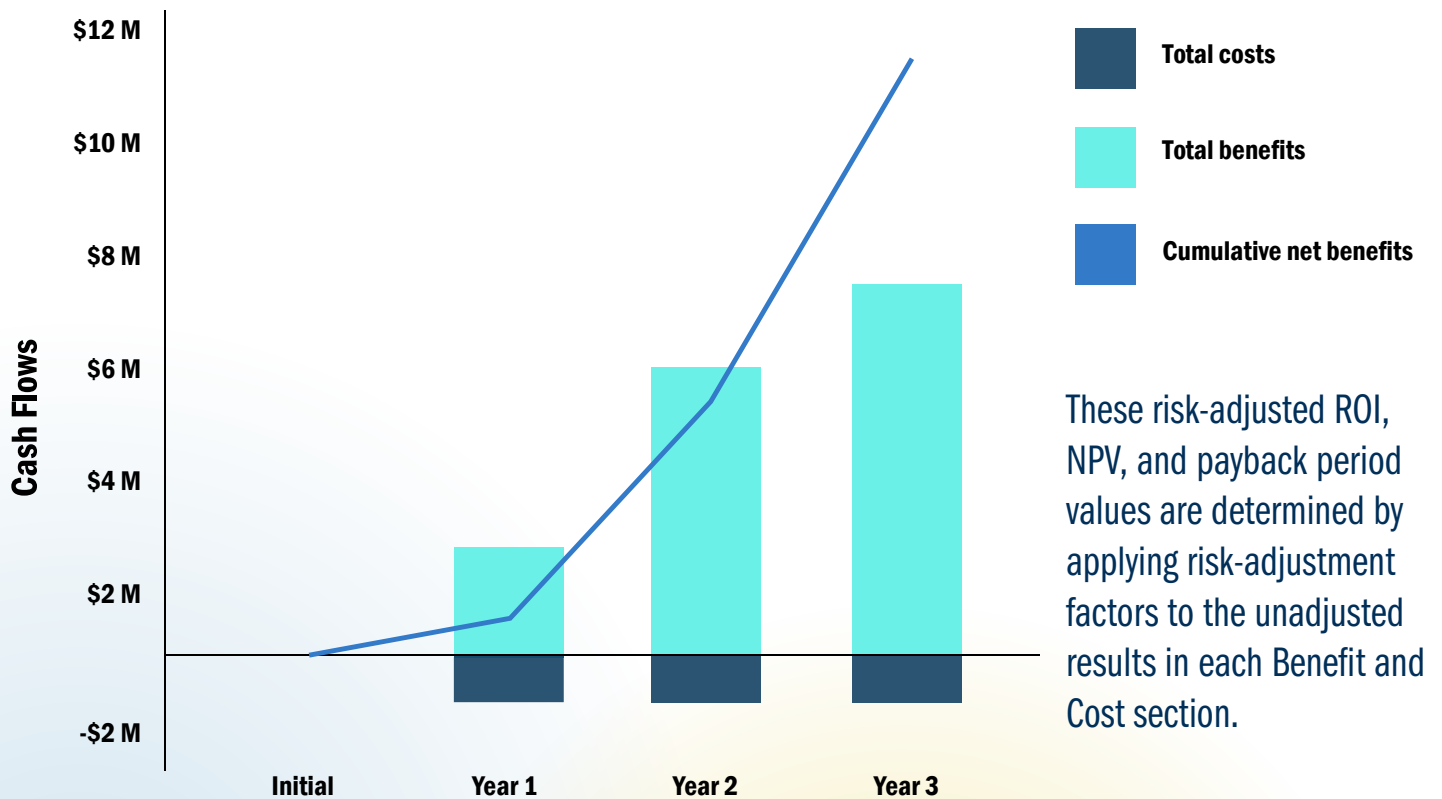
Financial Summary

The risk-adjusted cash flow rose steadily over the three-year study, starting with a first-year increase of $1,410,552, and reaching a total amount of $4,527,456 after the third year. The cumulative net benefits also climbed, from an initial amount of $25,800 to a solid $11,030,544. Over three years, ROI climbed by 248 percent. This data presents a compelling, confident business case for automation investment.

Chief Financial Officers (CFOs) are focused on the current unpredictable landscape and economic uncertainty, and they expect IT to drive efficiency and productivity, but to do so while cutting labor costs. Automation is the foundation—and catalyst—of driving business success despite a downturn in the economy. Getting buy-in from CFOs for investment in automation presents a great challenge, but it can be easy to start by communicating metrics like ROI, internal rate of return (IRR) and payback, as well as the ways automation aligns with, and directly impacts, business goals and outcomes.

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS-ORGANIZATION

Cash Flow Chart (Risk-Adjusted)

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Six Ways Resolve's Incident Response Automation Brings Incidents to Resolutions Quickly

Interactive process guidance

Guided incident resolution with step-by-step instructions, decision trees, and automations

Incident resolution dashboard

Summary results of automated tests and diagnostics with easy-to-follow troubleshooting actions

Analytics and process improvement

Reporting and analytics integrated with social collaboration for proactive process improvement

Human-guided Automation

Automation actions performed incrementally as part of an interactive resolution guidance process

End-to-end Resolution Automation

Automated diagnostics and resolution of incident without operator interaction

Incident ecosystem connectivity

Integrated solution connecting all systems, devices, and applications, accelerating incident resolution

What lies ahead for automation as it relates to incident response and its financial impact?

Incident management in the foreseeable future will become more critical in supporting network operations centers (NOCs) as they endure increasing complexity. As new and emerging technologies make their debuts, data volumes follow suit. NOC advancement will be key in scaling to manage massive amounts of additional data, and incident response automation will be critical to optimize network performance and protect it from business-critical threats over time.

Incident response automation will add the important functionality that NOCs will need to offer, as they'll have to adapt to change quickly and smoothly to ensure value and ROI for the business. For example, as businesses continue their progression toward cloud-based services and gain cost savings along the way, network management must echo with agility, speed, and powerful, ever-evolving best practices, such as network monitoring, validating alarms, and executing remediation processes.

Optimizing resources and improving network performance will gain new abilities from automation, like analyzing network data with exceptional speed to quickly identify trends, enabling businesses to apply the proper resources for increased efficiency and improved performance. Automation contributes to stellar customer experiences and maintains competitiveness as a key marketplace differentiator.

Conclusion

The data is clear: Incident response automation empowers IT teams and leads to greater cost savings, improved customer satisfaction, and higher ROI.

Enterprises are realizing a greater ROI by implementing incident response automation and enabling it to perform the mundane, repetitive tasks that burden IT teams and cause inefficiencies across the entire organization. Many organizations continue to rely on manual processes and legacy software, but business demands today are proving that automation deserves a key spot on the incident response roster. Human IT staff, even those of the largest teams, are no longer able to meet expectations on their own.

Incident response automation manages alerts and alarms efficiently and quickly — without error — to address and solve problems. It fuels productivity of IT teams, allowing them to spend valuable time on substantial processes that support the business goals, like ROI, and prepare the organization for future success.

Ready to start automating incident response in your NOC?

Request a demo