

The Numbers Don't Lie:

Fast Coordinated Incident Response Is More Critical Than Ever

With the volume and variety of critical IT events growing every day, shortening incident response time is the new business imperative. After all, the longer a company takes to address an IT issue, the more severe the impact on the organization, its customers, and its users, among others.

But there's good news: New-generation incident response automation can help mitigate the risk—and reduce the impact on business operations, revenues, and your brand reputation.

The Odds Are Against You



Getting struck by lightning?

1 in 960,000



Dating a millionaire?

1 in 220



Experiencing a databreach?

1 in 4

Source: 2017 Ponemon Institute

Cost of Downtime



\$8,900
per minute

Source: 2016 Ponemon Institute

Average Time to Respond



25 to 39
minutes

Average Number of IT Incidents* Annually



85%

— at least one
major IT incident
in the last year

Source: IDG Research

Cost per Incident

(Reflects time to assemble a response team)

\$222,500 to **\$347,100**



Why a Speedy Response Is Essential

Consider the added costs of:

- ⚠️ Additional downtime before response team begins addressing incident increases impact
- ⚠️ Reduced non-IT employee productivity
- ⚠️ Loss of revenue, of customers
- ⚠️ Damage to brand reputation



Automation to the Rescue

A best-in-class incident response solution can:

- ✔️ Integrate with all ITOM, SIEM, ITAM, and DevOps tools
- ✔️ Automatically assess the IT event's severity
- ✔️ Activate the appropriate response plan
- ✔️ Automatically identify and contact the on-call response team
- ✔️ Communicate that the response team has been activated
- ✔️ Send synchronous, multimodal, contextual, targeted notifications
- ✔️ Send geographically specific communications, using local caller IDs
- ✔️ Escalate communication if response team members don't respond
- ✔️ Provide tools for quick and seamless collaboration (such as one-click conference calls and ChatOps)
- ✔️ Help confirm and coordinate who will work on what, based on available personnel and skills
- ✔️ Automate workflows that remediate known issues
- ✔️ Ensure a more predictable, consistent response process across the organization
- ✔️ Streamline communication with non-IT staff and key stakeholders
- ✔️ Proactively notify potentially affected business users
- ✔️ Improve information capture for postincident debriefing, compliance audits, and future event responses