2019 REPORT

LogicMonitor

IT Outage Impact Study

A global analysis of IT downtime and its impact on businesses

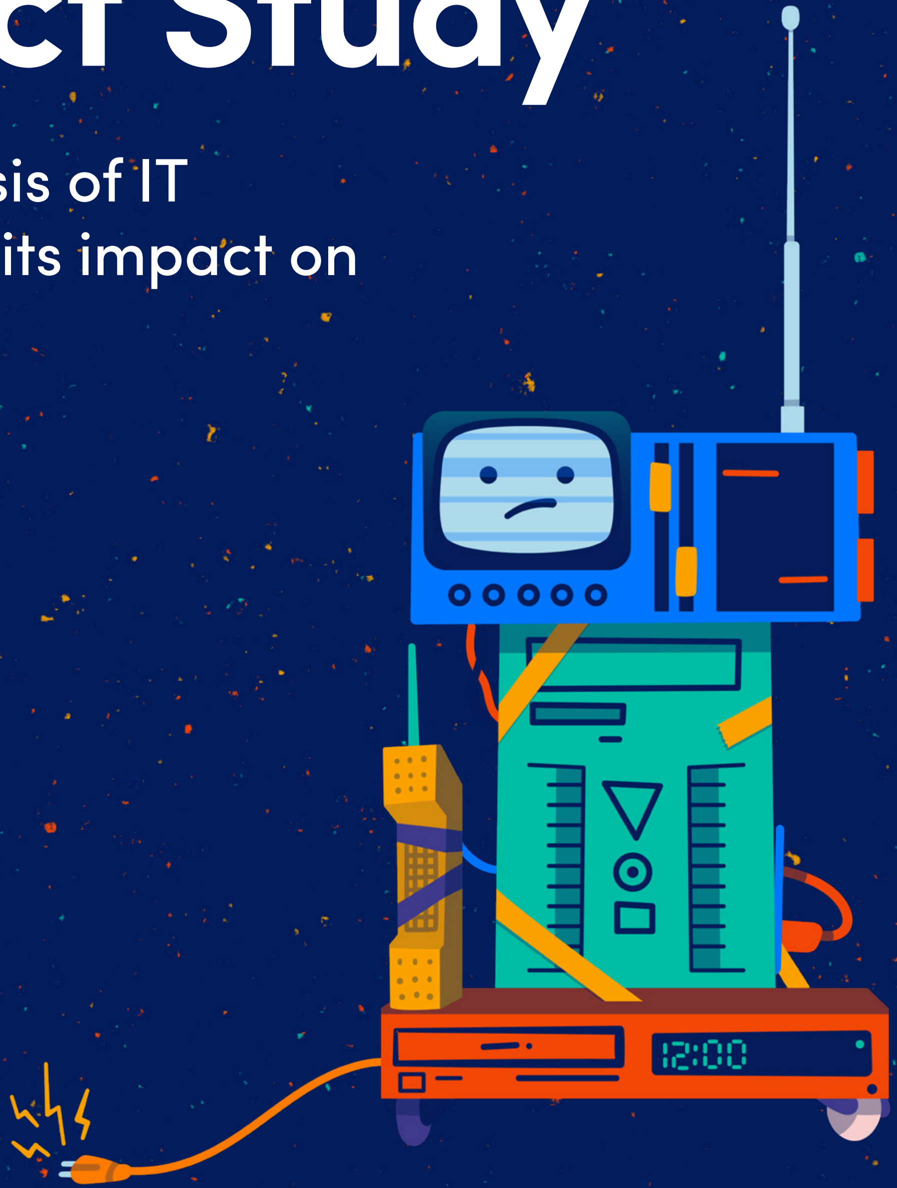
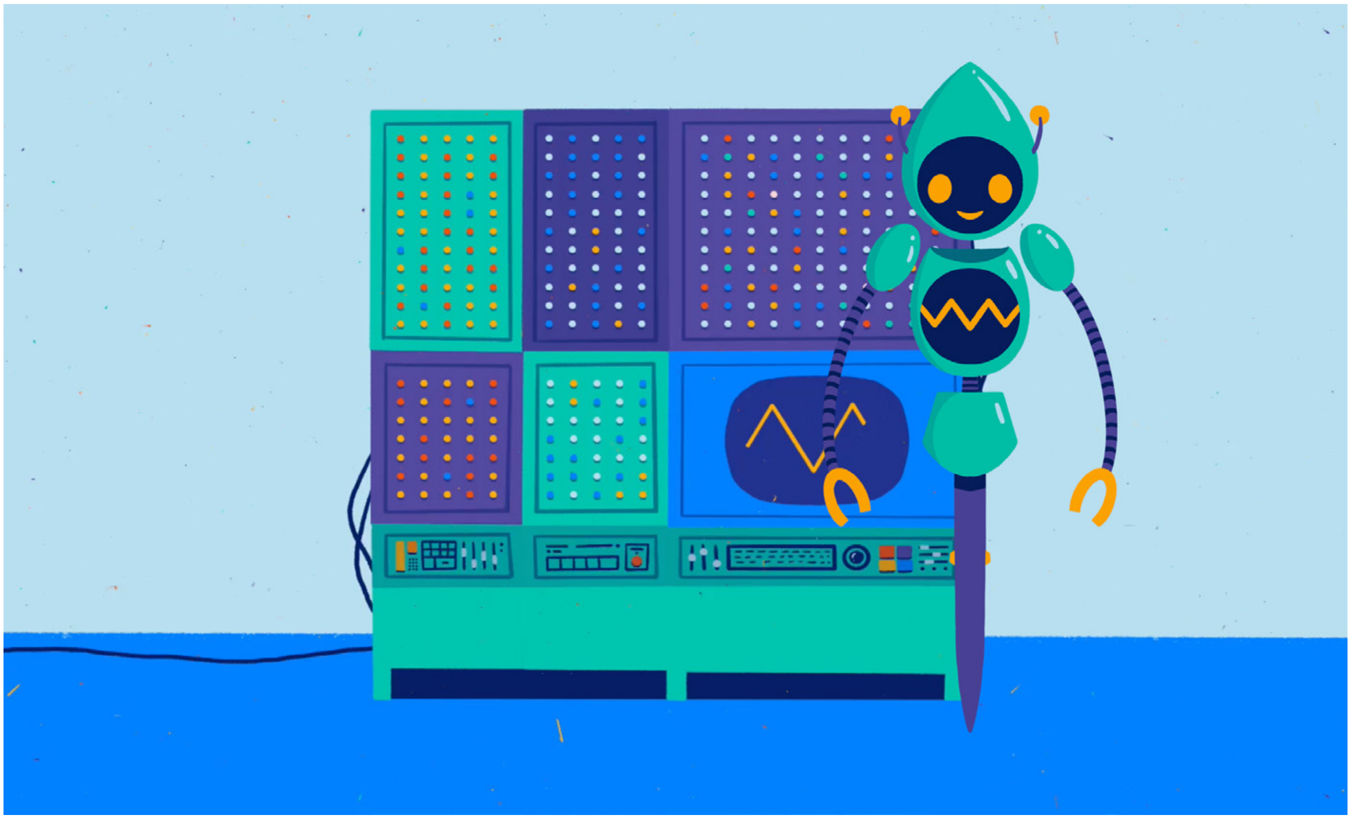


Table of Contents



Digital transformation is nothing less than a revolution in how businesses interact with customers. Access to information is changing the world in important, impactful ways.

Mobile computing is pushing the boundaries of where and how we can connect into every corner of our world. Cloud computing means that virtually everything we need is just a click away. But none of this—connection, interaction, computing—is possible unless the underlying technology is working.

Availability has become our most valuable commodity. And unfortunately, high-profile availability and technology outages occur at an alarming rate. No company is immune —Target, Macy's, British Airways, Lowe's, Facebook and Twitter have all struggled through embarrassing and expensive outages in recent years—and the costs go far beyond the bottom line.

To dig deeper into what causes downtime, LogicMonitor, the leading performance monitoring platform for Enterprise IT, commissioned a survey to explore the two biggest threats to availability: IT outages and brownouts.

With this survey, LogicMonitor sought to understand not only what IT outages and brownouts are, but also what causes them, whether or not they are preventable, and how organizations are combating these costly issues.

Study Methodology

In 2019, LogicMonitor commissioned an independent research firm to survey 300 IT decision makers at organizations with 2,500 or more employees. The organizations were distributed across a variety of industries and geographic regions. The goal of the research was to better understand how availability and downtime impact not only IT teams, but also businesses as a whole.

Respondents by Region:

- United States and Canada: **100**
- United Kingdom: **100**
- Australia and New Zealand: **100**

Size of Organizations by Number of Employees:

- 2,500-4,999 Employees: **30%** (n = 92)
- 5,000-9,999 Employees: **34%** (n = 101)
- 10,000+ Employees: **36%** (n = 107)

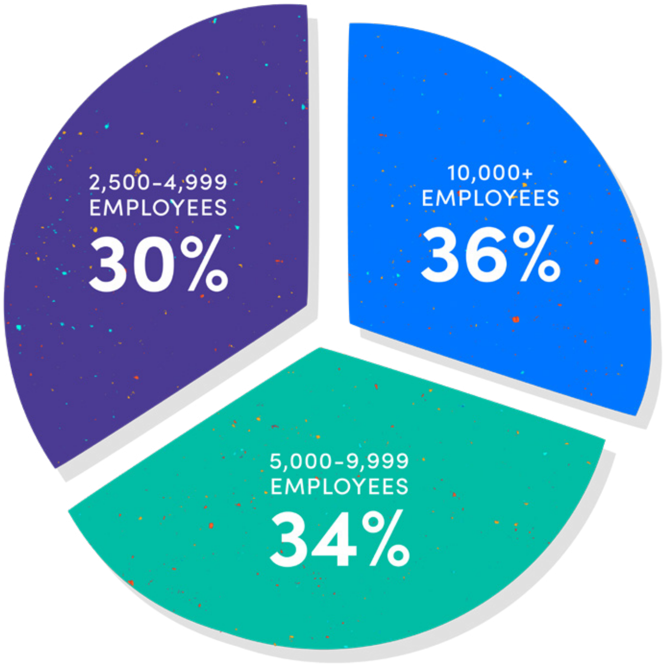
Respondent Seniority:

- IT Executive Management (CIO, CISO, VP): **64%** (n = 193)
- IT Management (Director): **36%** (n = 107)

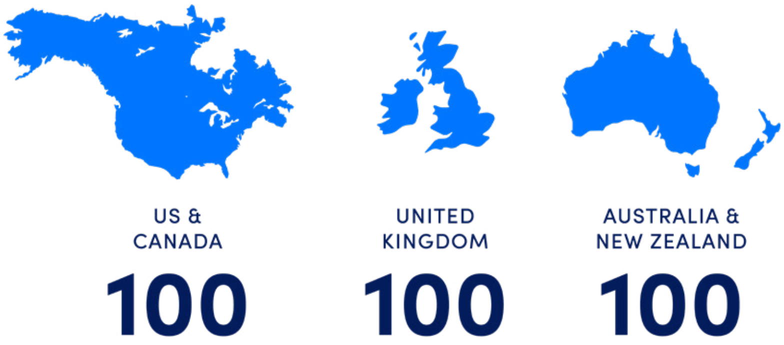
Respondents by Industry Vertical:

- Technology: **85**
- Manufacturing: **49**
- eCommerce/Retail: **41**
- Financial Services: **35**
- Healthcare/Insurance: **26**
- Education: **12**
- Transportation/Travel: **12**
- Communications/Media: **11**
- Energy/Utilities: **10**
- Other: **9**
- Business Services: **5**
- Government: **5**

Respondents by Company Size



Respondents by Region



Key Findings

The following pages detail the key findings of LogicMonitor's 2019 IT Outage Impact Study, summarized here:

- **96%** of global IT decision makers surveyed had experienced at least one outage in the past 3 years.
- According to global IT decision makers, **51%** of outages are avoidable.
- Global IT decision makers also said **53%** of brownouts are avoidable.
- **53%** of global IT decision makers think it's likely their company will experience a brownout or outage so severe that it makes national media headlines.
- The same percentage (**53%**) of global IT decision makers think it's likely their company will experience a brownout or outage so severe that someone loses their job as a result.
- Companies that have frequent outages and brownouts experience up to **16x higher costs** than companies who have fewer instances of downtime.

KEY FINDING

Availability Matters

Availability, the state when an organization's IT infrastructure is functioning properly, is critical when it comes to operating a successful business. **If the services or systems that a business provides suddenly become unavailable, that is referred to as an outage. If the services or systems remain available but slow down significantly, that is referred to as a brownout.**

When asked what keeps them awake at night, the top answers for global IT decision makers were performance and availability. **80% of respondents indicated that performance and availability were important issues.** In fact, availability was more important than security or cost to the senior IT managers surveyed.

> **"We see brownouts with regards to long log-in times. I.e., instead of taking 10 to 15 seconds to log in to a full virtualized desktop, it might extend out to 70 or 80 seconds. You then have poor experience or a slow and lagging desktop experience."**
>
> - DATA ANALYST AT AN IT CONSULTING COMPANY

Top 4 Issues Keeping IT Decision Makers Awake at Night

1. Performance
2. Availability
3. Security
4. Cost-effectiveness

(n=300)

KEY FINDING

Downtime is Rampant

The data indicates that IT departments are highly concerned about availability and performance. But does this ongoing concern drive companies to excellence, or is it a sign that companies are struggling to maintain performance and availability? The evidence unfortunately points to the latter conclusion.

Can outages be avoided?

According to the IT decision makers surveyed, **51% of outages and 53% of brownouts are avoidable**. These percentages remained relatively constant regardless of industry, respondent seniority, region or company size. However, this also means that **global IT decision makers feel that 49% of outages and 47% of brownouts are unavoidable.**

How frequently do brownouts and outages occur?

Outages and brownouts are surprisingly prevalent. In fact, **96% of organizations surveyed experienced at least one outage in the past three years, and 95% of organizations experienced at least one brownout in the past three years**. Australia and New Zealand reported experiencing outages the most frequently out of all regions surveyed.

51%

OF OUTAGES ARE AVOIDABLE

53%

OF BROWNOUTS ARE AVOIDABLE

> **“A lot [of outages] are avoidable. If you’re not paying for storage, or maybe you’re slow-rolling your signature on a change order to increase storage on a SQL server, and you run out of a space—that’s avoidable.”**
>
> - SYSTEMS INTEGRATION ENGINEER FOR A SERVICE PROVIDER

How many **brownouts** has your organization seen in the past three years?

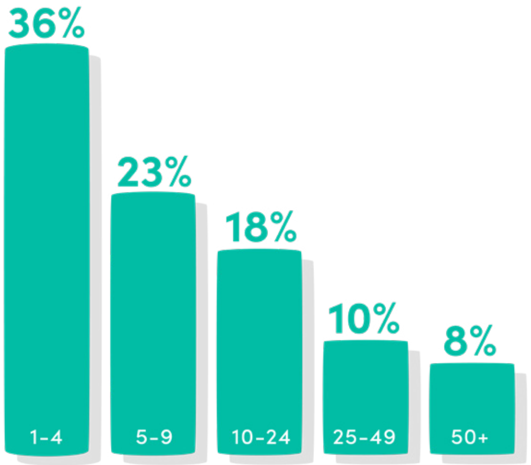


Figure 1. Among global organizations, frequency of brownouts varies significantly (n = 300)

How many **outages** has your organization seen in the past three years?

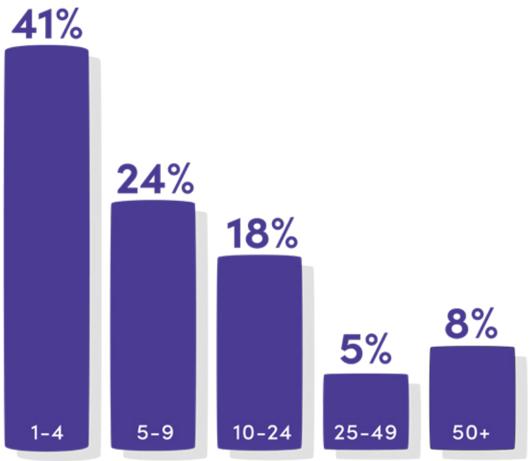


Figure 2. Among global organizations, frequency of outages varies significantly (n = 300)

In the U.S. and Canada:

- **47%** have experienced 5 or more outages over the last 3 years.
- **53%** of U.S. and Canada-based IT decision makers have experienced 4 or fewer outages over the last 3 years.

In the United Kingdom:

- **51%** have experienced 5 or more outages over the last 3 years.
- **49%** of UK-based IT decision makers have experienced 4 or fewer outages over the last 3 years.

In Australia & New Zealand:

- A whopping **69%** have experienced 5 or more outages over the last 3 years.
- Just **31%** of Australia and New Zealand-based IT decision makers have experienced 4 or fewer outages over the last 3 years.

The industry in which the company operates also seems to be related to the frequency of outages and brownouts. Financial and technology organizations experienced outages and brownouts most frequently during a three-year period, followed by retail and manufacturing:

- **41%** of respondents from financial organizations stated that they experienced **10 or more outages** over the past 3 years (n = 35).
- **37%** of respondents from technology organizations stated that they experienced **10 or more outages** over the past 3 years (n = 85).
- **34%** of respondents from retail organizations stated that they experienced **10 or more outages** over the past 3 years (n = 41).
- **28%** of respondents from manufacturing organizations stated that they experienced **10 or more outages** over the past 3 years (n = 49).

Are organizations worried about negative consequences from downtime?

IT decision makers are pessimistic about their ability to avoid outages and brownouts. The majority of survey respondents worry about the negative repercussions of downtime, with **53% of global respondents saying it's likely they will experience a brownout or outage so severe that it makes national media**. When those downtime instances do occur, these respondents fully expect someone to lose his or her job. When comparing levels of concern across regions, industry and respondent seniority, however, the data reveals stark differences.

Concerns by Region

In the UK, only **38%** of respondents say it's likely they will experience a major brownout or outage so severe it makes the media. And only **35%** of UK respondents believe someone might lose his or her job as a result of this downtime.

That number increases among U.S. and Canada-based respondents, with **50%** saying it's likely they will experience a major brownout or outage being so severe it makes the media. **52%** of U.S. and Canada-based respondents believe they will experience a major brownout or outage so severe that someone loses his or her job as a result.

In Australia and New Zealand, **63%** of respondents say they are likely to experience a major brownout or outage so severe it makes the media. **63%** of Australia and New Zealand respondents also worry someone might lose his or her job as a result of downtime.

Concerns by Industry

Fears about outages or brownouts showing up in the media also vary according to which industry the respondent works within. **68% of respondents working within the retail sector (n = 41)** felt they would experience a brownout or outage so severe that it would make national media coverage. 68% felt that someone could lose his or her job as a result of a brownout or outage.

- **67% of respondents working within the manufacturing sector (n = 49)** felt they would experience a brownout or outage so severe that it would make major media coverage. 69% felt that someone could lose his or her job as a result of a brownout or outage.
- **43% of respondents working within the financial sector (n = 35)** felt they would experience a brownout or outage so severe that it would make major media coverage, although 52% felt that someone could lose his or her job as a result of a brownout or outage.
- **Only 30% of respondents working within the technology sector (n = 85)** felt they would experience a brownout or outage so severe that it would make major media coverage. Still, 47% felt that someone could lose his or her job as a result of a brownout or outage.

> **"One of our clients is a radiology company, and they need to be up 24/7. If they have more than an hour of downtime a year, probably less than that, that's a serious issue. These guys can never go down, for legal reasons."**
>
> – SERVICE DESK SUPPORT ENGINEER FOR A SOLUTION PROVIDER

Concerns by Job Title

Seniority also impacted views around the likelihood of major media outlets picking up stories about brownouts or outages. **62%** of the 193 respondents who identified as being IT Executive Management (CIO, CISO, VP) felt that it is likely that their company will experience a brownout or outage so severe that it makes the major media, while only **38%** of the 107 respondents at the IT Management (Director level) felt the same.

KEY FINDING

Downtime is Expensive

It is no wonder that IT professionals are so concerned about availability. Downtime is expensive, and it also impacts the business as a whole. The following list shows the top business impacts of downtime, as described by global IT decision makers.

Business Impacts of Downtime

- Lost revenue
- Compliance failure
- Damage to the brand
- Lowered stock price
- Mitigation costs
- Lost productivity
- Costs to mitigate and recover from a brownout
- Career negatively impacted
- Business failed

Companies that have frequent outages and brownouts experience up to **16x higher costs** than companies who have fewer instances of downtime. Furthermore, companies with frequent downtime require **nearly 2x the number of team members** to troubleshoot problems, even when the system they are troubleshooting has monitoring software already assigned to it. Troubleshooting also takes an average of **2x as long** for those companies.

Globally, on average, the costliest outage-related issues are:

- Lost revenue
- Compliance failure

And the costliest brownout-related issues:

- Lost revenue
- Lost productivity

> **"We support a few finance clients that deal with micro transactions against the open market, so an outage or even a loss of connectivity to the stock exchange can quickly equate to lost dollars, and they hold us accountable for that."**
>
> – DEVOPS ENGINEER FOR A TECHNOLOGY INTEGRATION AND MANAGEMENT COMPANY

For companies with **frequent outages and brownouts:**

16x
HIGHER COSTS

NEARLY
2x
MORE TEAM MEMBERS TO TROUBLESHOOT PROBLEMS

2x
AS LONG TO TROUBLESHOOT PROBLEMS

KEY FINDING

Causes of Downtime

Why are companies around the world so ineffective at avoiding downtime? After all, the study data shows that IT decision makers are focused on and aware of the risks of outages. IT departments also understand the overall costs of downtime to the business. And it is clear that more than half of downtime can be avoided. So, what exactly is the problem?

According to survey respondents, the most common culprits of downtime vary. Figure 5 shows the top causes of downtime, according to IT decision makers in each region. **Respondents noted the lead contributors to downtime are network failure and usage spikes/surges.**

What becomes clear from the data as well, however, is that **human error** is often a contributing factor to downtime. This is where AIOps and intelligent monitoring tools can help, and where the IT industry is shifting as companies look to future-proof their monitoring.

"We've seen outages based on people not following their own change control because they thought, 'It was just a simple change, so nobody needed to worry about it.' We've had to recover from quite a few outages from that," said a principal engineer at an IT services engineering firm.

According to the 300 global respondents, the **top two missed opportunities when it comes to preventing downtime are:**

- **Passing a capacity threshold:** Failing to notice when usage is trending towards a danger level. For example, this might be more traffic than the network can efficiently handle, or a primary storage share running out of space.
- **Failure of hardware/software:** Failing to notice that critical hardware/software performance is trending downward.

Most Common Causes of Downtime

	Global (n=300)	US + Canada (n=100)	UK (n=100)	Australia + New Zealand (n=100)
#1 Cause	Network failure	Human error	Network failure	Network failure
#2 Cause	Usage spikes/surges	Usage spikes/surges	Software malfunction	Usage spikes/surges
#3 Cause	Human error	Infrastructure hardware failure	Usage spikes/surges	Human error
#4 Cause	Software malfunction	Loss of electrical power	Third-party provider outages	Software malfunction
#5 Cause	Infrastructure hardware failure	Network failure	Human error	Storage failure
#6 Cause	Third-party provider outages	Software malfunction	Configuration error	Unknown cause

Figure 5. The most common causes of downtime, as identified by regional survey respondents

LM's Recommendations: How to Avoid Outages

LogicMonitor expands what's possible for businesses by advancing the technology behind them. Through monitoring, LogicMonitor customers gain the ability to focus less on problem-solving for events such as an outage or brownout, and more on optimization and innovation. Want to do the same? Here are five ways to get started:

- **Embrace comprehensive monitoring**. Find and implement a platform that comprehensively monitors infrastructures, allowing you to view your IT systems through a single pane of glass. Consider extensibility during the selection process to ensure the platform integrates with all of your technologies.
- **Identify and address gaps in your systems**. Build a high level of redundancy into your monitoring to prevent outages from occurring. Focus on eliminating single points of failure that might cause a system to go down.
- **Act on trends in your monitoring data**. Make sure you have a solution in place that gives you early visibility into trends that could signify trouble ahead. Use data forecasting to proactively identify future failures and prevent an outage before it impacts your business.
- **Create an outage response plan**. Hopefully you'll never have to use it, but it's critical to have a defined process for handling outages, from escalation and remediation to communication and root cause analysis. Set a plan on who to involve—and when—to ensure your organization can respond quickly if an outage does occur.
- **Scale your monitoring**. Whether you're adopting new technologies or moving your infrastructure to the cloud, make sure that the monitoring solution your company uses is able to keep up. Select a scalable platform that will help take your business to the next level while still maintaining visibility into your systems.

Want to learn how other IT decision makers are preventing, detecting and mitigating outages and IT issues? LogicMonitor will be releasing a second comprehensive report in Q4 2019 detailing techniques used by IT decision makers to prevent, detect and mitigate outages.

Learn more about LogicMonitor

About LogicMonitor®

Monitoring is an essential technology that can unlock new pathways to growth. At LogicMonitor®, we expand what's possible for businesses by advancing the technology behind them. LogicMonitor seamlessly monitors infrastructures, empowering companies to focus less on problem solving and more on evolution. We help customers turn on a complete view in minutes, turn the dial from optimization to innovation and turn the corner from sight to vision. Join us in shaping the information revolution by visiting LogicMonitor.com.

LogicMonitor