

Break-Fix vs Managed IT Models

Why A Proactive Approach is Always Superior

It can be difficult to identify the proper IT strategy for your organization. Is it easier to adopt a reactive approach on a by-problem basis, or take a proactive approach to solving issues? We call these two models: Break-Fix, and Managed IT.

Break-Fix Model: A reactive approach which operates only when there's an issue. Exact features and functionality depend on the IT team's collective expertise

Managed IT: A proactive approach where endpoints are constantly managed, and concerns are resolved before they become problems. Implementing a Managed IT approach enables IT professionals to proactively monitor, manage, secure, and access their endpoint infrastructure from anywhere.

Why Does a Break-Fix Model Fail?

Although a Break-Fix model offers simplicity, it's becoming an approach of the past as it creates a variety of challenges, including:

#1 Unpredictable Costs and Issues:

A Break-Fix model relies on intermittent and unscheduled consultations, making it impossible to budget for unseen issues. Variability in costs due to fluctuating demand can lead to resource constraints that hamper business growth.



#2 Increased Downtime:

Downtime is a killer for any business. A Break-Fix model in particular can result in massive amounts of downtime as a problem gets resolved. Instead of proactively identifying the root cause of the issue, Break-Fix teams focus on the issue at hand after it has already occurred.

It has been reported that even one hour of downtime can result in costs \$100,000 for a small to midsize business. For large enterprises, a single hour of downtime can cost \$1 million to over \$5 million.



#3 Security Challenges:

Break-Fix models do not offer active network monitoring options but instead solves security issues on a one-off basis after they have already occurred. This reactive strategy leaves your endpoints vulnerable and at risk to cyber-threats.

Average cost of a malware attack: \$2.6 million²

Average cost of a ransomware attack: \$645,000²

Average cost of phishing or social engineering: \$1.4 million²

Average cost of web-based attacks: \$2.75 million²



The Top 5 Reasons that Break-Fix Fails

1. Unpredictability
2. Relies heavily on staff time and effort
3. Fixes immediate problem, not the root cause
4. Variable downtime due to unforeseen issues
5. Focus is on incoming issues rather than overall strategy

Why is a Managed IT Model Superior?

#1 Better Cost Management:

Reducing cost is one thing, but eliminating variability in cost is just as important. With annual subscriptions at a consistent price, a Managed IT solution can help you stabilize your IT costs and provide insight into your recurring expenses.

46% of organizations that utilize a Managed Services Provider (MSP) say they have reduced annual IT budgets by at least 25% as a result of adopting managed services. And 13% of those respondents estimated their savings at 50% or more³



#2 Better for Your Business and Employees:

An Managed IT model provides continuous visibility into the root causes of issues facing your endpoints and automated responses to deal with and prevent those issues. Prevention makes life much easier: it conserves resources and reduces employee strain.

According to information gathered by Clutch, 59% of IT providers have moved from a Break-Fix model to Managed IT, along with 82% of MSPs⁴



#3 Enhanced Security:

Managed IT becomes particularly important when dealing with threats. Implementing a Managed IT approach arms your company with proactive security features and enhanced visibility all within a single solution. These features include patch management (Windows and Application updates), antivirus, two-factor authentication, encryption, proactive and self-healing alerts, advanced scripting, and asset management.

65% of cyber-attacks are aimed at small and medium-sized businesses, and half of those companies go out of business in 6 months⁵



The Top 5 Ways Managed IT Helps your Business

1. Anticipate, protect against and eliminate cyber threats
2. Stay on top of patches, updates and system changes
3. Reduce variability in cost
4. Prevent downtime before it happens
5. Automate routine tasks and set proactive and self-healing alerts

When you break down the facts, one thing is clear: a proactive IT approach reduces downtime, saves money and optimizes resources over traditional reactive strategies.

LogMeIn Central can help you:

- **Monitor** – Gain better visibility & have a single pane of glass view into all of your company's endpoints with advanced reporting & proactive alerts
- **Manage** – Automate manual tasks and bring productivity to the next level with automated task management and self-healing alerts
- **Secure** – Take control and mitigate risk of cyber threats with patch management and LogMeIn Antivirus powered by Bitdefender
- **Access** – Remotely access any endpoint from anywhere with one-click access from any desktop, laptop, tablet or mobile device



Implement a proactive Managed IT model and solve concerns before they become problems with LogMeIn Central.

[Request a demo.](#)