

Break-Fix vs Managed IT Models

Why A Proactive Approach is Always Superior

approach on a by-problem basis, or take a proactive approach to solving issues? We call these two models: Break-Fix, and Managed IT.

It can be difficult to identify the proper IT strategy for your organization. Is it easier to adopt a reactive

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.

Although a Break-Fix model offers simplicity, it's becoming an approach of the past as it

Why Does a Break-Fix Model Fail?

creates a variety of challenges, including:

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.



Downtime is a killer for any business. A Break-Fix model in

Increased Downtime:

#2

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.1

Security Challenges:

#3

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





1. Unpredictability 2. Relies heavily on staff time and effort 3. Fixes immediate problem, not the root cause

The Top 5 Reasons that

Break-Fix Fails

- 4. Variable downtime due to unforeseen issues
- 5. Focus is on incoming issues rather than overall strategy

#1 **Better Cost Management:**

Why is a Managed IT Model Superior?

Reducing cost is one thing, but eliminating variability in cost is just

#3

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

as important. With annual subscriptions at a consistent price, a

#2 **Better for Your Business**



An Managed IT model provides continuous visibility into the root

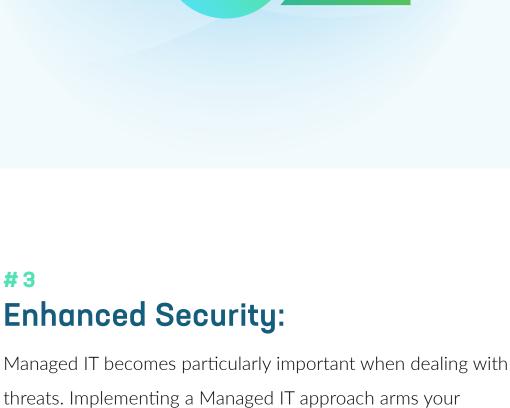
causes of issues facing your endpoints and automated responses

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

to deal with and prevent those issues. Prevention makes life



all within a single solution. These features include patch

alerts, advanced scripting, and asset management.

management (Windows and Application updates), antivirus,

65% of cyber-attacks are aimed at small and medium-sized

businesses, and half of those companies go out of business

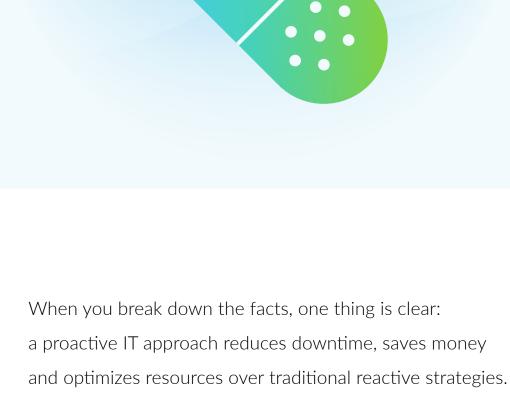
two-factor authentication, encryption, proactive and self-healing

in 6 months⁵

82% of MSPs⁴

and Employees:

company with proactive security features and enhanced visibility



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

5. Automate routine tasks and set proactive and self-healing alerts

4. Prevent downtime before it happens

LogMeIn Central can help you: • **Monitor** – Gain better visibility & have a single pane of glass

reporting & proactive alerts Manage – Automate manual tasks and bring productivity to

view into all of your company's endpoints with advanced

- the next level with automated task management and self-healing alerts
- Access Remotely access any endpoint from anywhere with one-click access from any desktop, laptop, tablet or

by Bitdefender

mobile device

• **Secure** – Take control and mitigate risk of cyber threats with patch management and LogMeln Antivirus powered

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

Request a demo.

3. Channel Insider for CompTIA. "Do Managed Services Really Save Money?" 2018 4. Otelco. "Break-Fix vs. Managed Services" 2018

1. ITIC. "2019 Global Server Hardware, Server OS Reliability Survey" 2019 2. Accenture. "The Cost of Cybercrime" 2019

©2020 LogMeIn, Inc. All rights reserved.

