March 27, 2019

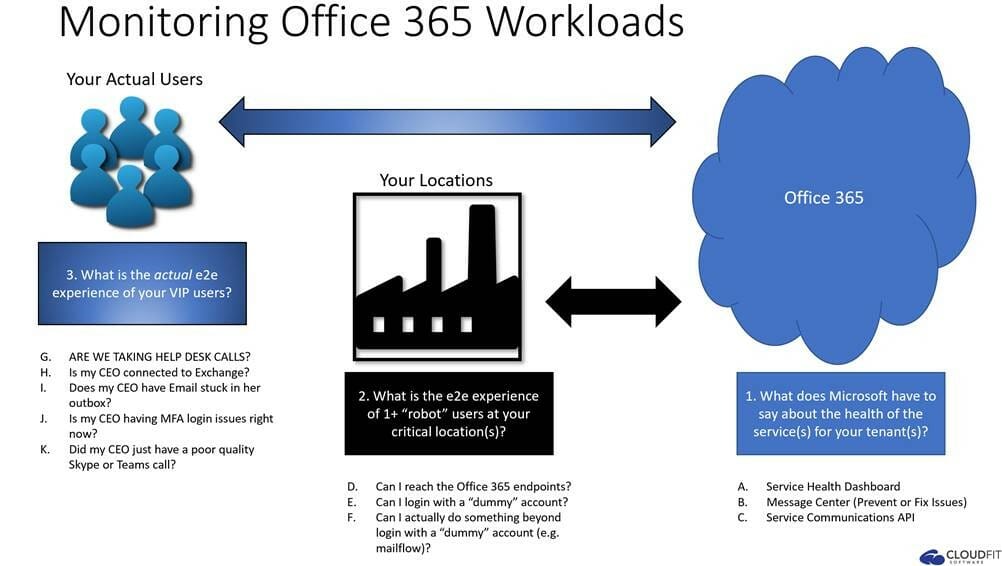
**Here’s What You Need to Know About Monitoring to be Successful with Office 365**

The question of how to monitor Office 365 workloads like Exchange Online, SharePoint Online, Microsoft Teams, Skype for Business and other workloads is one that most customers of Office 365 have asked, or will ask, at some point in time.  Enterprise customers have enterprise expectations for monitoring, situational awareness and performance achievement reporting.  Small businesses all have at least one person who plays the IT Admin role who wants to know that there is impact before the boss calls.  We get asked this question constantly, so we decided to write an article to simplify it.

*The first thing to know* about monitoring Office 365 is that nobody can monitor Office 365 as well as the Office 365 product group.  Who knows a car better than the builder of the car?  Nobody.  Who knows Office 365 better than the people who built Office 365?  Nobody.  Obviously, nobody knows how to monitor Office 365 better than the people who built it.  Further, nobody is incented to monitor Office 365 more than the people whose business it is to make sure Office 365 is available.  No matter what a monitoring-tool-sales-guy tells you, nobody will monitor Office 365 better than the Office 365 Product Group.  Given that fact, your **first step** to monitoring Office 365 is to consume the information that Microsoft provides about the health of Office 365 for your tenant(s) through the Office 365 Service Health Dashboard and through the Office 365 Service Communications API.

Office 365 is an amazing grouping of services that are transforming how the world collaborates.  Let’s take a step back and discuss a service that we all use outside of IT.  We all use electricity.  If you are reading this article, you have access to electricity.  The power company generates and delivers the power to your home.  Once the power connects to your home, all bets are off.  Thankfully, with electricity, there are commoditized standards.  In the US, electrical sockets are all the same.  In the UK, the sockets are different than in the US, but they are the same.  There are standards, and those standards are even enforced by building inspectors.  For Office 365, the service is great, but Microsoft does not bring the service to your doorstep.  You have to use someone else’s plumbing (your ISV, who in turn depends on many other providers to deliver connectivity) to get to Office 365 from your doorstep.  And once in your environment, there are countless options for networks and network configurations.  There are countless options for user devices, including BYOD.  There are countless options for configurations, including network drivers, on each device itself.  The electrical company knows if their service is impacted, but they are not providing a monitoring service to let you know if your refrigerator is broken inside of your boundary.  Office 365 knows if their service is impacted, but they are not providing a monitoring service to text you to let you know that your CEO has mail stuck in her outbox, and they aren’t going to pop an alert in your NOC’s existing single pane of glass to let you know that the quarterly all-hands call is having choppy audio.

With all of that out of the way, *the second thing to know* about monitoring Office 365 is that while nobody will monitor Office 365 as well as their Product Group, their monitoring does not provide the entire, end-to-end story for your user experience.  There are two additional steps to monitoring Office 365 for your users.  The **second step** is to monitor the health of the end-to-end service from your most critical locations.  The approach there is to have synthetic transactions that imitate user behavior running on a schedule from machines in each critical location.  You can write your own simple scripts for that purpose, or you can buy or rent synthetics from a 3rd party.  Synthetics aren’t rocket science, so do not get caught up in fancy dashboards.  The key thing here is whether simple user activities like logging in are working from your critical locations.  Remember that the goal here is not really to monitor Office 365, but rather to monitor your ability to use Office 365 in your critical locations because of all of the complexity between your doorstep and Office 365.  The **third step** is to monitor the actual user experience of your most important users.  Knowing that a synthetic transaction just recorded a successful call for a fake Skype for Business voice call if your CEO just dropped a call in the middle of an important conversation.  You need to know that the CEO just dropped that call so you can go do damage control proactively.



That comment about damage control is really the most important piece.  In reality, nobody wants to monitor.  Monitoring is just extra cost.  Nobody wants to buy another monitoring tool.  Nobody wants to pay for a monitoring tool in the cloud.  Monitoring is cost.  Nobody needs monitoring.  Everyone needs damage control.  Everyone needs to know that Building 23 is having sporadic Email login issues.  Everyone needs to know that the head sales person has email stuck in her outbox.  Everyone needs to know that the company’s main intranet site that runs on top of SharePoint online is down.  The key word there is “know”.  Everyone needs to know.  Tools and dashboards only provide part of the story.

That leads us to the final point.  *The third thing to know*about monitoring Office 365 is that it is about the outcomes.  There are an infinite number of possible inputs—Office 365’s view on your tenant’s health, a synthetic view of end-to-end health at your critical locations, a real-time pulse of your most important users’ experience, your help desk call volumes, your network flow data, what social media has to say about Office 365’s health, and so on.  Someone needs to make sense of all of that data.  They need to make sense of that data in light of your business rules.  For example, do you want a page on a Saturday morning at 4am if Building 34 is offline, or would you rather not get that page at all unless Building 34 is still offline at 6am Monday morning? Would you want a ticket cut in your ticketing system for that Building 34 issue no matter when it happened? Would you also want a phone call to your help desk to give them a heads up about the outage in building 34?  What about building 35? Is it the same protocol or different? What if both buildings go offline? Do you want the same people paged if Microsoft has acknowledged the issue?  The outcomes are the phone calls, the emails, the alerts, the tickets and all of that at the right time. Who is going to be accountable for that?

In all of our experience building and running Office 365 while we were at Microsoft, and in all of our experience with customers consulting with them about how to monitor Office 365 while we were at Microsoft, we only heard one true question about monitoring Office 365: who is going to take accountability to let me know when my users are impacted and to never bother me when they aren’t impacted? Underneath every question about how to monitor Office 365 is a customer who simply wants the outcomes. Nobody wants monitoring. Everyone wants outcomes.

Who is CloudFit Software?  We are the people who take accountability for those outcomes.

Filed Under: [Monitoring](https://www.cloudfitsoftware.com/category/monitoring/)