How to Mitigate the Impact of Microsoft 365 Downtime

Published 20 October 2021 - ID G00758705 - 34 min read
By Analyst(s): Guy Creese, Larry Cannell
Initiatives: Collaboration and End-User Technologies for Technical Professionals

Despite Microsoft 365’s 99.9% uptime SLA, the service can and does go down. This research describes the eight actions that application technical professionals can take to mitigate those downtime impacts.

Overview

Key Findings

■ Since 2018, major services within Microsoft 365 — Azure Active Directory (Azure AD), multifactor authentication, Exchange, SharePoint, OneDrive and Microsoft Teams — have gone down for several hours at a time, with one outage lasting as long as 15 hours.

■ Microsoft’s published uptime metric is for the Microsoft 365 service as a whole or a geographic region. It does not specifically reflect the uptime for your tenant and its users.

■ What organizations can do to mitigate the downtime impact varies widely across services. For Planner, IT can do nothing; for OneDrive for Business, users can access synced files stored locally; for Exchange Online, IT can use an email continuity solution to keep email running.

■ Employees often resort to using consumer tools as a workaround when Microsoft 365 is down, thereby putting corporate data at risk.

Recommendations

Application technical professionals responsible for collaboration and end-user technologies should do the following when working to mitigate Microsoft 365 downtime:
When Microsoft 365 goes down, it can cause major havoc in the organization. Depending on which service is down, organizations can't log on to Microsoft 365, send or receive email, access some of their files, or hold online meetings. To add insult to injury, Microsoft is sometimes tardy about telling IT about the system failure. For real-time communications services such as Microsoft Teams, users typically start complaining about the system being down 15 minutes before the official Microsoft notification. Tired of being caught out by irate employees who can't get their work done, IT departments ask Gartner, “How can we quickly know of and mitigate Microsoft 365 downtime?”

There are eight concrete actions that an organization can take to mitigate Microsoft 365 downtime. The first five steps require internal process changes; the remaining three steps require purchasing third-party tools.
For eight services, third-party tools and/or native Microsoft 365 capabilities make it possible to use a portion of the service or continue to access at least some of its data while the service is “down.” These eight services are: Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams, Power Apps, Power BI, Viva Learning (not yet generally available) and Viva Topics (see Figure 1).

**Figure 1: Eight Services Can Still Be Partially Used When “Down”**

<table>
<thead>
<tr>
<th>Third-Party Tools</th>
<th>Native Microsoft 365 Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Online</td>
<td>Azure AD MFA</td>
</tr>
<tr>
<td>SharePoint Online</td>
<td>Microsoft Teams</td>
</tr>
<tr>
<td>OneDrive for Business</td>
<td>Viva Learning</td>
</tr>
<tr>
<td></td>
<td>SharePoint Online</td>
</tr>
<tr>
<td></td>
<td>Power Apps</td>
</tr>
<tr>
<td></td>
<td>Viva Topics</td>
</tr>
<tr>
<td></td>
<td>OneDrive for Business</td>
</tr>
<tr>
<td></td>
<td>Power BI</td>
</tr>
</tbody>
</table>

Unfortunately, for most Microsoft 365 services, you must wait for the service to come back up to use the service or access its data. This is true for Azure AD, Microsoft 365 Groups, Power Automate, Power BI, Planner, Project Online, Bookings, Shifts, Viva Connections, Viva Insights, Forms, Sway and Yammer.

This research gives you the actionable advice upfront. It starts with laying out the mitigation options. After that, it discusses two related subjects:

- What are the known causes for the system going down?
- What is the Microsoft 365 SLA, and how does Microsoft calculate its uptime metric?
This report also includes a downloadable document: “Customizable Template for End-User Actions to Take When Microsoft 365 Goes Down.” This template will help IT create a document that tells employees what to do when a specific Microsoft 365 service goes down. For each major Microsoft 365 service, this document describes the impact of the service going down and potential workarounds. In some cases, it tells users to avoid using substitute services as workarounds, as these will put corporate data at risk.

**Download the companion Tool: Customizable Template for End-User Actions to Take When Microsoft 365 Goes Down**

**The Eight Mitigation Options**

The Merriam-Webster dictionary defines “mitigation” as: “The process or result of making something less severe, dangerous, painful, harsh, or damaging.” The important point here is that mitigation does not completely fix an issue — it merely softens the impact. And anything that offers an improvement over the status quo is fair game. Learning about a downtime issue sooner is a form of mitigation, as is gaining a more accurate understanding of the issue. Mitigating Microsoft 365 downtime is often a smattering of small wins, rather than a collection of big wins.

There are eight ways an organization can mitigate Microsoft 365 downtime, split into two main categories: through internal process changes and by purchasing third-party tools (see Figure 2).
### The Eight Mitigation Options for Microsoft 365 Downtime

#### No License Costs

1. Calculate uptime metrics for your tenant using two definitions: Microsoft's and yours.
2. Use Microsoft’s three notification methods beyond the Service Health Dashboard.
3. Monitor non-Microsoft sources to get faster notifications.
4. For identity, follow Microsoft’s guidance on making it more resilient, and turn off MFA while it is down.
5. Tell users what to do (and not do) during Microsoft 365 downtime.

#### Additional License Costs

6. Implement a Microsoft 365 performance monitoring solution.
7. Implement an email continuity solution.
8. Implement a third-party backup solution.

---

**Internal process changes**, which require time and effort but do not incur additional license costs, are:

- Calculate uptime metrics for your tenant using two definitions: Microsoft’s and yours.
- Use Microsoft’s three notification methods beyond the service health dashboard.
- Monitor non-Microsoft sources to get faster notifications.
- For identity, follow Microsoft’s guidance on making it more resilient, and turn off multifactor authentication (MFA) while it is down.
- Tell users what to do (and not do) during Microsoft 365 downtime.

**Third-party tools**, which come with additional license costs, are:

- Implement a Microsoft 365 performance monitoring solution.
1. Calculate Uptime Metrics for Your Tenant Using Two Definitions: Microsoft’s and Yours

Microsoft calculates Microsoft 365’s uptime metric on a quarterly basis for (1) the service in general and (2) for specific regions, such as Europe. It displays the general uptime metrics for the past several years on the Microsoft webpage, Service Health and Continuity. However, this metric is for the service overall; Microsoft does not calculate a metric for individual tenants. Consequently, your uptime could be above or below the general metric. For example, during a 30-day month, if Microsoft Teams had one hour of downtime for half of its users, the monthly uptime percentage would be 99.93%. If your organization wasn’t impacted by that outage, the uptime percentage for your tenant would be 100%. Alternatively, if all of your users were impacted by that outage, the uptime percentage for your tenant would be 99.86% — below Microsoft’s 99.9% SLA threshold (see Figure 3).

**Figure 3: The Microsoft Uptime Metric Does Not Reflect Actual Tenant Experience**

*The Microsoft Uptime Metric Does Not Reflect Actual Tenant Experience*
Because Microsoft’s generic metric cannot accurately reflect a specific tenant’s uptime, Gartner recommends that Microsoft 365 customers calculate their own uptime percentages. To do so, you will need to track (1) the total number of active users in your tenant and (2) the number of impacted users and how long they were down. As a starting point for the second step, look at the history page on your service health dashboard (SHD). This will list service incidents over the last 30 days. Then, survey users, asking them if they were impacted by these incidents and for how long. A faster and more accurate way to do this is to leverage the data provided by a Microsoft 365 performance monitoring solution.

Calculate downtime in two ways:

- **Use Microsoft’s downtime definitions:** Use Microsoft’s definitions of downtime laid out in the Microsoft document, Service Level Agreement for Microsoft Online Services (WW), available at the Microsoft webpage, Service Level Agreements (SLA) for Online Services.

- **Use the organization’s downtime definitions:** Microsoft’s definitions do not always map to the organization’s perception of downtime. Take Exchange Online as an example:
  
  - **User downtime not acknowledged by Microsoft.** Microsoft says Exchange Online downtime is any period of time when users are unable to send or receive email with Outlook on the web. However, most organizations would say the service is down when users are unable to send or receive email via the rich Outlook client.

  - **Administrator downtime not acknowledged by Microsoft.** Microsoft will issue service notifications about Exchange Online administration. For example, on 29 June 2020, Microsoft issued the warning, “Some admins can't leverage some features in Exchange admin center.” However, Microsoft does not count that service impairment as downtime.

Therefore, the corporate definition of Exchange Online downtime could be as follows. Exchange Online downtime is any period of time when (1) users are unable to send or receive email with either Outlook on the web or the Outlook client or (2) administrators are unable to administer the service.
Using your own downtime definitions will give you an organization-centric metric that is not dependent on Microsoft’s vendor-centric viewpoint. There are two benefits for doing this additional work:

- **It supplies data to your procurement department for negotiating with Microsoft.** Factual data that shows your tenant experienced more downtime than Microsoft’s official number will make it easier for your procurement department to extract concessions from Microsoft during contract negotiations.

- **It gives upper management data that accurately reflects the corporate experience.** By creating your own metrics, you will be giving upper management an accurate view of Microsoft 365 downtime in your tenant. You will be able to show how Microsoft’s definition of downtime and your definition of downtime can alter the downtime statistics.

2. **Use Microsoft’s Three Notification Methods Beyond the Service Health Dashboard**

All Microsoft 365 customers know they can monitor service interruption via the service health dashboard within the Microsoft 365 admin console. This is available only to system administrators; end users without admin privileges cannot view it.

Happily, the functionality of the SHD continues to evolve. As of October 2021, Microsoft is previewing more detailed Exchange Online monitoring for large customers. This SHD feature monitors Exchange Online metrics (such as basic authentication, mail delivery and app connectivity) for the past 30 minutes, and then displays how that amount of activity has changed over the last seven days (e.g., +32% or -6%). It can also tell the viewer whether the issue is occurring within Microsoft’s infrastructure, third-party infrastructure or the customer’s infrastructure. In short, this new feature offers a depth of detail that was previously missing from the SHD. Microsoft states that it plans to expand this more detailed reporting capability to other services in the future. For further information on this feature, see the Microsoft webpage, [Exchange Online monitoring for Microsoft 365](https://docs.microsoft.com/en-us/Exchange/exchange-online-monitoring).

If the SHD is unavailable, the backup notification site is [Microsoft 365 Service health status](https://docs.microsoft.com/en-us/teams/service-health-status).

However, Microsoft’s alternative notification methods aren’t always as well-known to customers:
If you aren’t using them already, use the mobile app and monitor Microsoft’s Twitter account to increase the chances of receiving updates when not sitting in front of the service health dashboard. Use the APIs to funnel service health information to end users and help desk applications.

3. Monitor Non-Microsoft Sources to Get Faster Notifications

When a Microsoft 365 service goes down at a Microsoft data center, alarms go off. Microsoft employees diagnose the problem and its impact, and then write up the notification notice. That’s why Microsoft’s notifications often lag the service failure by 15 minutes or so.

To shrink the notification time, monitor social media so you can instantly see people asking, “Hey, is this service down?” People are frequently specific about what’s still working for them and what isn’t, which can give context to Microsoft’s official announcement. Unfortunately, there is no universally recognized hashtag for reporting Microsoft 365 downtime. Searching for the product name and then “down” sometimes works (e.g., #teamsdown). The best strategy here is to notice who often posts early about Microsoft 365 downtime and then follow them.
Another option is to follow the site Downdetector, which monitors Twitter and outage reports submitted to it. Using sentiment analysis and historical data, it then decides a service's current status: has no problems, possible problems or problems. It offers status webpages for popular Microsoft 365 services such as Exchange Online, SharePoint Online and Microsoft Teams. Besides the above webpages on its publicly accessible website, Downdetector offers an enterprise service called Downdetector Enterprise.

4. For Identity, Follow Microsoft’s Guidance on Making It More Resilient and Turn Off MFA While It Is Down

There are two changes organizations can make to mitigate the impact of Microsoft 365’s identity mechanisms going down. The first change is to follow Microsoft's guidance on how to architect Azure AD identity and access management infrastructure so that it’s more resilient. The recommended six steps are listed on Microsoft's webpage, Build Resilience in Your Identity and Access Management Infrastructure. This change requires modifying system settings before an outage.

The second change is to implement a potential workaround during a multifactor authentication outage. The issue is that if MFA is down, then users required to use MFA can’t login to Microsoft 365. The workaround is to temporarily turn off MFA for the duration of the outage. To do this, organizations should maintain two break-glass Global Administrator accounts with very long, random, frequently rotated passwords unencumbered by MFA — or use third-party MFA-enabled privileged access management (PAM) tools. Using such an account, a Global Administrator can disable MFA or policies that require MFA. Azure AD doesn’t support temporary removal of MFA, so administrators must perform this action “manually” by capturing their current configurations, policies and/or enrollment information, making the change and then immediately rolling it back after the incident is over.

Note that security-defaults-based MFA requires all users in a tenant to be enrolled in MFA. This means that all administrators will be locked out if the MFA service is down. Organizations that use security defaults will need to wait out the downtime event. The exception will be users that remember their MFA on a trusted device and recently authenticated using MFA from that device.

5. Tell Users What to Do (and Not Do) During Microsoft 365 Downtime
Microsoft 365 going down is unsettling for users. Rather than letting users flail around, guessing at what they should now do, the organization needs to give them clear guidance on what to do and what not to do if a Microsoft 365 service goes down. This will help the users be productive when they can, and prevent them from inadvertently putting the organization at risk.

**Telling Users What to Do**

For eight Microsoft 365 services, some native functionality remains or the data remains accessible in some way even if the service is down (see Table 1). For example, even if the OneDrive for Business service is down, files synced down to the desktop are still accessible to the end user. For three services — Exchange Online, SharePoint Online and OneDrive for Business — the downtime damage can be mitigated by purchasing a third-party tool.
Table 1: The Workarounds for a Microsoft 365 Service Going Down  
(Enlarged table in Appendix)

<table>
<thead>
<tr>
<th>If this service goes down …</th>
<th>The workaround is supplied by …</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure AD MFA</td>
<td>Native Microsoft 365 capabilities</td>
<td>Use an MFA-unencumbered break-glass Global Admin account or a PAM tool to temporarily turn off MFA while it is down.</td>
</tr>
<tr>
<td>Exchange Online</td>
<td>A third-party tool</td>
<td>Use an email continuity service to allow users to continue to receive and send email. However, as noted, this typically will not fix email delivery for the integrated applications.</td>
</tr>
<tr>
<td>SharePoint Online/ OneDrive for Business</td>
<td>Native Microsoft 365 capabilities, a third-party tool</td>
<td>Files synced to endpoints (e.g., desktop, laptop, tablet) via OneDrive will still be accessible. To access copies of all files stored in SharePoint and OneDrive, use a third-party backup service.</td>
</tr>
<tr>
<td>Microsoft Teams</td>
<td>Native Microsoft 365 capabilities</td>
<td>Users can access their Teams files via the SharePoint Online and OneDrive for Business interfaces if they know where they’re stored.</td>
</tr>
<tr>
<td>Power Apps</td>
<td>Native Microsoft 365 capabilities</td>
<td>Users can still use the Power Apps mobile app in offline mode.</td>
</tr>
<tr>
<td>Power BI</td>
<td>Native Microsoft 365 capabilities</td>
<td>Employees will be able to use the Power BI desktop or Power BI Report Builder to create dashboards or reports as long as the underlying data sources are still accessible.</td>
</tr>
<tr>
<td>Viva Learning</td>
<td>Native Microsoft 365 capabilities</td>
<td>Users can search the individual courseware platforms, such as LinkedIn Learning and Microsoft Learn.</td>
</tr>
<tr>
<td>Viva Topics</td>
<td>Native Microsoft 365 capabilities</td>
<td>Current topic cards will remain visible.</td>
</tr>
</tbody>
</table>

Source: Gartner (October 2021)

Write a memo to tell your end users of the workarounds available to them. Make sure this is in a format accessible to them even if Microsoft 365 goes down. For example, you may decide to post it as a webpage on your corporate intranet or send it out as a memo via email. Urge users to print it out so they can still read it if the corporate intranet goes down or they can no longer get to their email Inbox.

Use the downloadable template to get a head start on your “Actions to Take When Microsoft 365 Goes Down” memo to users.
For each service, explain in a clear, step-by-step fashion what users can do to get access to the service or data. Below is a sample explanation of what users should do if Microsoft Teams goes down.

**Impact:** If the Teams service goes down, you will not be able to have conversations, chats or videoconferences within Teams or access files via the Teams interface. However, you will be able to access Teams files stored in SharePoint Online and OneDrive for Business.

**Workarounds:**

- **Peer-to-Peer Voice:** Call users on a separate fixed line or mobile phone, in place of voice calls on Teams.

- **Chats/Conversations:** Use email in place of chats and conversations.

- **Videoconferences:** None.

- **Files:** You can still access group-owned files in Teams by going to the following location: https://<tenant-name>.sharepoint.com/sites/<Team-name>/Shared%20Documents/<channel-name>. You can access privately owned Teams files within the Microsoft Teams Chat Files folder in your OneDrive folder. This assumes that the files have been synced down to your device. Since we use Files on Demand, that may not always be the case. Within the OneDrive folder, if the files are shown with a cloud icon, they are stored in the cloud and currently inaccessible. However, if the files are shown with a green check mark within a green circle, they are local and can be accessed.

- **Teams Phone System:** Call from a mobile phone or use Teams peer-to-peer voice (if not affected).

The above example is for Microsoft Teams. The downloadable template affiliated with this report suggests wording for Teams and 22 other Microsoft 365 services. Use the template to get a jump-start on your memo telling users what to do when Microsoft 365 goes down.

**Telling Users What Not to Do**

End users, under pressure to get their work done, will resort to using alternate solutions — often consumer solutions — when Microsoft 365 goes down. The conversations are along the lines of:
The issue is that such ad hoc workarounds may put your organization at risk. Corporate files and communications are now being stored in nonenterprise systems. These systems cannot be monitored by corporate data loss prevention policies, backed up to a third-party service, subjected to the corporate retention or records management policies, or interrogated via the corporate e-discovery tool. If your legal counsel deems several hours of “outside the enterprise” collaboration too risky in terms of security, record keeping and e-discovery, then explicitly tell your employees not to use unsanctioned workarounds when Microsoft 365 is down.

With this in mind, you may want to add the following paragraph to the sample explanation above.

**Actions Not to Take:** If Teams is down, do not attempt to have conversations, chats or videoconferences on noncompany systems. For example, do not have a videoconference on Zoom in place of a videoconference on Teams. It will be tempting to do, as you will want to continue to get your work done. However, if you do this, you will be storing corporate data on noncompany systems, which means we cannot monitor it, delete it or search it for e-discovery purposes. Our company policy explicitly prohibits employees from using nonsanctioned systems for company business. There are no exceptions. If you have a question about this policy, contact our chief information security officer. If the system outage prevents you from completing a task on time, explain that to your manager. You will not be disciplined for following organizational guidelines on system usage.

Alternatively, to protect corporate data, you could purchase a non-Microsoft solution to serve as an alternative when Microsoft 365 is down. For example, you could buy a corporate license for Zoom to use only when Microsoft Teams is down. Most organizations shy away from this option due to the expense, as most of these services charge per user, whether the service is used or not.
6. Implement a Microsoft 365 Performance Monitoring Solution

Third parties offer solutions specifically designed to monitor Microsoft 365 performance and downtime. These are called Microsoft 365 performance monitoring solutions. These packages will warn of issues sooner than Microsoft will. They will give you a better understanding of which regions/offices are affected than Microsoft’s vague pronouncements. Finally, they will help you calculate an objective measure of your downtime.

These solutions can do this because they use synthetic transactions at endpoints to mimic user behavior. They send emails and watch how long it takes the email to arrive. They visit a SharePoint webpage and see how long it takes to load. When these transactions slow or fail, they will instantly notify you. Because they’re often running synthetic transactions from around the world, they can tell you that Exchange Online is down in the U.S. but up in Europe, for example.

Four vendors who specifically monitor Microsoft 365 performance are ENow, Exoprise, Martello Technologies (previously GSX), and Cisco- ThousandEyes. For a feature comparison of those four solutions, see Solution Comparison for Microsoft Office 365 Monitoring Solutions. However, any form of synthetic monitoring will be useful. For further information on synthetic monitoring in general and vendors that offer that capability, see Use Monitoring for SaaS Despite Its Limitations and Use Synthetic Monitoring to Enhance User Experience for Hosted and SaaS Applications.

7. Implement an Email Continuity Solution

If Exchange Online goes down, users cannot receive or send email, either from Outlook or Outlook on the web. However, third-party solutions called “email continuity solutions” can get around this limitation. When organizations purchase such a solution, they route their Exchange Online email through the vendor’s email server. This allows the vendor to have an ongoing copy of that organization’s email history. When Exchange Online goes down, the incoming email continues to be routed to the vendor’s email server. The organization then points to the vendor’s email server and uses it to receive and send email while Exchange Online is down.

Three vendors that offer such a service are:

- **Barracuda**: Barracuda Email Continuity routes email through the Barracuda Email Security Service. Users can send and receive emails when Exchange Online is down via a Barracuda-browser-based application.
8. Implement a Third-Party Backup Solution

A third-party backup solution will ensure users have access to recent copies of files when Microsoft 365 goes down. This will allow the enterprise to access copies of files stored in services such as Exchange Online, SharePoint Online, OneDrive for Business, Microsoft Teams and Microsoft Stream.

To use SharePoint as an example, if the enterprise uses a third-party backup solution, users will be able to use the solution to access copies of all SharePoint files while SharePoint Online is down. This is in contrast to the native capabilities of Microsoft 365, which allow continued access to a much smaller subset: those SharePoint files synced down to endpoints via OneDrive for Business. Unfortunately, third-party backup cannot completely make up for SharePoint Online being down. For example, users will still be unable to access or update SharePoint Online sites.

Vendors that offer third-party backup solutions include Acronis, AvePoint, Barracuda, CloudAlly, Cohesity, Commvault, Datto-Backupify, Druva, Keepit, Metallic, Mimecast, Rubrik, Spanning Cloud Apps and Veeam. For further information of why you should backup data stored in Microsoft 365, see When to Leverage Third-Party Solutions to Back Up Office 365.

What Are the Known Causes for the System Going Down?

There have been various causes for Microsoft 365 going down in the past. Additional ones may occur in the future, but the documented causes include:

- **Natural disaster:** Lightning strikes at times take out Microsoft data centers. This happened a number of years ago in Dublin, Ireland (both Google Workspace and Microsoft 365 were impacted). On 4 September 2018, a lightning strike near a San Antonio, Texas, data center caused part of the data center’s cooling system to fail. This, in turn, caused Exchange Online, Power BI, SharePoint Online, Teams and Intune to be impacted for approximately 11 hours. ²
Calculation Details: The SLA and the Uptime Calculation

This section describes Microsoft 365’s service-level agreement (SLA), corresponding service credits, Microsoft’s downtime definitions and how the monthly uptime percentage is calculated.

The Microsoft 365 SLA

Microsoft states that the general uptime SLA for Microsoft 365 is 99.9%. This calculates out to a guarantee that the service won’t go down for all users more than 8.8 hours per year or 43 minutes in a 30-day month. Furthermore, this metric is not cumulative. Microsoft recalculates the uptime metric for each calendar month.

- **Azure AD**: This is a single point of failure. If Azure AD goes down, customers cannot log in to the service. Users already logged in can continue to use the service, due to a time-to-live setting. This happened on 6 April 2018 (more than 14 hours), 28 September 2020 (six hours) and 15 March 2021 (two hours). ³

- **Multifactor authentication**: This is a single point of failure. If MFA goes down, users required to use MFA cannot log in to the service. Users already logged in via MFA can continue to use the service. On 19 November 2018, MFA was down for 15 hours. ⁴

- **Domain name service (DNS) updates**: This is not the DNS service in general, but, rather, Microsoft’s updating of its own DNS pointers. This is a single point of failure. A Microsoft DNS misconfiguration occurred on 2 May 2019. This brought down SharePoint Online, OneDrive for Business and Dynamics 365 for an hour. ⁵

- **Bad network infrastructure or misconfiguration**: This seems to be the biggest cause of Microsoft 365 downtime. Bad network infrastructure or misconfiguration brought Microsoft 365 down on 19 November 2019, 7 October 2020, 15 January 2021, 17 February 2021 and 25 February 2021. ⁶

- **Software updates**: A software update impacted Exchange Online, Outlook.com, Office.com, Power Platform, Dynamics 365 and Microsoft Teams on 1 October 2020. ⁷

- **Certificate nonrenewal**: Microsoft’s failure to renew an authentication certificate led to Microsoft Teams being down for three hours on 3 February 2021. ⁸
It’s the “all users” portion of the calculation that customers often do not take into account, which leads to a misunderstanding of the SLA. For example, a customer may say, “Teams was down for three hours for all of our users last month. So why didn't the Microsoft 365 uptime metric dip below 99.9% last month?” There are several reasons for this. First, Teams is not the only Microsoft 365 service, so its downtime was diluted by all the other services that stayed up. Second, Teams was probably not down across the world, but only in a specific region, so the majority of Teams users were not impacted. So, while the three hours of Teams downtime was significant for that organization, for Microsoft’s overall operation — running more than 20 Microsoft 365 services around the world — it had a relatively small impact.

Azure AD is the exception to the 99.9% SLA. In April 2021, Microsoft increased its uptime guarantee for Azure AD from 99.9% to 99.99%; that calculates out to a downtime for all users of less than 26 minutes in a year or four minutes in a 30-day month.

On a quarterly basis, Microsoft calculates the Microsoft 365 uptime percentage for the service in general, as well as for regions of the world. The recent worldwide numbers are listed on the Microsoft webpage, Service Health and Continuity.

**Microsoft 365 Service Credits**

The sole customer remedy for excessive downtime is Microsoft 365 service credits. Microsoft offers service credits on a monthly basis. This has the impact of compartmentalizing the payouts. For example, if a service goes down for nine hours in a single day, that violates Microsoft's 99.9% SLA for the month (no more than 43 minutes of downtime). Calculating it out, it's also higher than 12 consecutive months of permissible downtime (no more than 8.8 hours per year). However, Microsoft will offer service credits for that incident only for that month.

Furthermore, the credits are not automatic. The SLA for Microsoft Online Services states, “In order for Microsoft to consider a claim, you must submit the claim to customer support at Microsoft Corporation including all information necessary for Microsoft to validate the claim, including but not limited to: (i) a detailed description of the Incident; (ii) information regarding the time and duration of the Downtime; (iii) the number and location(s) of affected users (if applicable); and (iv) descriptions of your attempts to resolve the Incident at the time of occurrence.” For further information on the service credit process and the timeline for submitting a claim, see the Microsoft document, “Service Level Agreement for Microsoft Online Services (WW),” available at the Microsoft webpage, Service Level Agreements (SLA) for Online Services.
Microsoft's definition of a product’s downtime may not map to your organization's definition.

The downtime definition for each service is listed within Microsoft’s “Service Level Agreement for Microsoft Online Services (WW).” It’s worth understanding each of these definitions in detail, because Microsoft's definition of a product's downtime may not map to your organization's definition. Therefore, you can have users reporting that a service is down but Microsoft saying it isn't.

Two examples are:

- **Exchange Online**: Microsoft’s definition is, “Any period of time when users are unable to send or receive email with Outlook Web Access [now actually named Outlook on the web].” Therefore, if employees using Outlook cannot access Exchange Online (due to a communications failure between Outlook and Exchange Online), Microsoft does not consider that downtime in Exchange Online.

- **Microsoft Teams**: Microsoft’s definition is, “Any period of time when end users are unable to see presence status, conduct instant messaging conversations or initiate online meetings.” Therefore, if files stored in Teams are inaccessible (because SharePoint Online is down), Microsoft does not consider that downtime in Teams.

**Monthly Uptime Percentage**

Microsoft’s uptime percentage calculation: User minutes - downtime minutes/user minutes x 100
Unlike the downtime definitions, which differ by service, the monthly uptime percentage calculation is universal — it does not differ between services. That calculation is: User Minutes minus Downtime Minutes divided by User Minutes times 100. To take a simple example, let’s say 10,000 users are running Microsoft Teams during a 30-day month, and Teams went down for an hour for 5,000 of those users. In that case, the calculation would be:

- **User Minutes**: 1,440 minutes in a day times 30 days (43,200) times 10,000 users = 432 million minutes.
- **Downtime Minutes**: 60 minutes of downtime times 5,000 users = 300,000 minutes.
- **User Minutes minus Downtime Minutes**: 431,700,000 minutes.
- **User Minutes minus Downtime Minutes divided by User Minutes times 100**: 431,700,000 divided by 432,000,000 times 100 = 99.93% uptime.

It turns out that Microsoft’s calculation of downtime minutes — how many users were impacted, for how long — is more of an art than a science. Microsoft uses a combination of service log data, synthetic transaction data and historical/trend data to calculate how many users were impacted by a downtime incident and for how long. Given the huge scale of these operations, this lets-triangulate-the-number strategy is to be expected. However, it’s important to note that it’s not exact.

**Recommendations**

While the first three recommendations listed below take time to implement, they incur no additional licensing costs, so implement them first before deciding whether to purchase third-party tools.

**Harden the Downtime Notification Process**

Examine your general downtime notification process and work to improve it. Questions to ask are:

- How do we notify users if a service is down? This includes not only employees, but also impacted customers and partners.
- Who decides if a notification is necessary, and what are the logistics of sending out the notification?
- What do we do if a notification channel is down (e.g., email)?
Implement IT Process Changes That Don't Require Purchasing Third-Party Tools

These changes will give you process improvements that don't require significant investment:

- **Calculate the Microsoft 365 uptime metrics for your tenant:** Calculate the uptime metrics for your tenant — using (1) Microsoft’s downtime definitions and (2) your own downtime definitions — to get an accurate picture of what your organization experiences.

- **Use Microsoft’s mobile admin app, its @MSFT365Status Twitter account and the Office 365 Service Communications API:** The first two mechanisms will allow you to get notifications no matter where you are. The third will help you disperse Microsoft 365 downtime information to other systems and end users.

- **Monitor Downdetector and social media sites:** Monitoring these third-party channels will give you notifications of Microsoft 365 downtime before Microsoft does.

- **Prepare to suspend MFA:** Put a process in place to temporarily turn off MFA while it is down.

Tell Users What to Do — and Not Do — During Microsoft 365 Downtime

The Microsoft 365 Governance Committee should give guidance on what users should do when a specific service goes down. For example, is it acceptable for employees to use the consumer Zoom service when Microsoft Teams is down? Or would that put corporate data at risk and be prohibited?

When that guidance has been decided, use the downloadable Gartner customizable template to formulate those directions and then issue them to employees in a form they can refer to when Microsoft 365 services are down.
Implement Third-Party Tools to Further Mitigate the Impact of Microsoft 365 Downtime

If the impact of major Microsoft 365 services going down is severe, then investigate purchasing and implementing third-party tools:

- **Microsoft 365 performance monitoring solutions** will generate faster notifications and more detailed information about downtime issues than you can get from Microsoft.
- **Email continuity solutions** will allow you to continue to send and receive email when Exchange Online is down.
- **Backup solutions** will give users access to copies of files when SharePoint Online and OneDrive for Business are down.

**Conclusion**

Microsoft 365 customers often feel helpless when a Microsoft 365 service goes down. Use this research to take control of the situation. Through a combination of improved processes and third-party tools, you can get quicker downtime notifications, gain a more detailed understanding of the problem and continue to use email and access files when Exchange and SharePoint are down. In addition, you will be able to give clear instructions to users on what to do and not do when a service goes down, thereby ensuring that they remain productive while not putting the organization at risk.

**Evidence**

1. Mitigation, Merriam-Webster.

2. Microsoft South Central U.S. Datacenter Outage Takes Down a Number of Cloud Services, ZDNet.


4. Office 365, Azure users are locked out after a global multifactor authentication outage, TechCrunch; Microsoft’s Office 365 Outage Is a Big Backwards Step for Security, WIRED.
SharePoint, Azure, Office 365, Teams Suffer Outage Thursday Afternoon, Redmond Magazine; Microsoft Azure Recovering From Major Networking-Related Outage That Took Out Office 365, Xbox Live, and Other Services, GeekWire.

Update: Microsoft Teams and Other Office 365 Services Back Online After Untimely Outage, GeekWire; Microsoft Blames Networking Build for 365 Outage, CRN; Microsoft Services Including Office 365, Skype Hit With Global Outage, Now Restored, RepublicWorld.com; ‘Very Frustrating’: Microsoft Office 365 Outage Hits U.S. Again, CRN; Office 365 Monitoring: Microsoft 365 Outage January 15, 2021, ENow; Is Microsoft Teams Down for You? WAVY.com; Microsoft 365 Status on Twitter, Microsoft.

Microsoft Outlook Email Outage Hits Users Worldwide, daijiworld.com.

Microsoft Teams Goes Down After Microsoft Forgot to Renew a Certificate, The Verge.

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

When to Leverage Third-Party Solutions to Back Up Office 365
Solution Comparison for Microsoft Office 365 Monitoring Solutions
Use Synthetic Monitoring to Enhance User Experience for Hosted and SaaS Applications
Use Monitoring for SaaS Despite Its Limitations
### Table 1: The Workarounds for a Microsoft 365 Service Going Down

<table>
<thead>
<tr>
<th>If this service goes down ...</th>
<th>The workaround is supplied by ...</th>
<th>Workaround</th>
</tr>
</thead>
<tbody>
<tr>
<td>Azure AD MFA</td>
<td>Native Microsoft 365 capabilities</td>
<td>Use an MFA-unencumbered break-glass Global Admin account or a PAM tool to temporarily turn off MFA while it is down.</td>
</tr>
<tr>
<td>Exchange Online</td>
<td>A third-party tool</td>
<td>Use an email continuity service to allow users to continue to receive and send email. However, as noted, this typically will not fix email delivery for the integrated applications.</td>
</tr>
<tr>
<td>SharePoint Online/ OneDrive for Business</td>
<td>Native Microsoft 365 capabilities; a third-party tool</td>
<td>Files synced to endpoints (e.g., desktop, laptop, tablet) via OneDrive will still be accessible. To access copies of all files stored in SharePoint and OneDrive, use a third-party backup service.</td>
</tr>
<tr>
<td>Microsoft Teams</td>
<td>Native Microsoft 365 capabilities</td>
<td>Users can access their Teams files via the SharePoint Online and OneDrive for Business interfaces if they know where they're stored.</td>
</tr>
<tr>
<td>Power Apps</td>
<td>Native Microsoft 365 capabilities</td>
<td>Users can still use the Power Apps mobile app in offline mode.</td>
</tr>
<tr>
<td>Power BI</td>
<td>Native Microsoft 365 capabilities</td>
<td>Employees will be able to use the Power BI desktop or Power BI Report Builder to create dashboards or reports as long as the underlying data sources are still accessible.</td>
</tr>
<tr>
<td>Viva Learning</td>
<td>Native Microsoft 365 capabilities</td>
<td>Users can search the individual courseware platforms, such as <a href="https://www.linkedin.com/learning">LinkedIn Learning</a> and <a href="https://learn.microsoft.com">Microsoft Learn</a>.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------</td>
</tr>
<tr>
<td>Viva Topics</td>
<td>Native Microsoft 365 capabilities</td>
<td>Current topic cards will remain visible.</td>
</tr>
</tbody>
</table>

Source: Gartner (October 2021)