DO YOU NEED OFFICE 365 MONITORING?

PAUL ROBICHAUX ▪ JAY GUNDOTRA ▪ MICHAEL VAN HORENBEECK

ENOW

Paul Robichaux

15 Year Microsoft MVP

Paul Robichaux has over 30 years' experience with software development, messaging, collaboration, and communication tools. He has worked as an Office 365 architect, helping enterprise customers deploy Microsoft's collaboration suite. He serves as a Senior Editor for Windows IT Pro magazine and has written more than a dozen books on Windows, Exchange and Office 365. Microsoft has named Paul as a Microsoft Valuable Professional (MVP) for 15 consecutive years.

Jay Gundotra

Founder and CEO, ENow | [MCP, MCT, MCSE, CompTIA]

Jay Gundotra is the technical founder and CEO of ENow, a leader in the Microsoft systems management space. With over 20 years of experience in Unified Communications and Network computing, he has led ENow to deliver effective monitoring and analytics software to customers in over 130 countries, including enterprise companies like Wendy's, Experian, and Dentsu Aegis Network. ENow Software's products have won over 23 technical awards since 2008 is a 3 time recipient of the Inc 5000 award and last year was named to Deloitte's exclusive Fast 500 fastest growing technology companies.

Michael Van Horenbeeck

Solution Architect | MVP | MCSM, VH Consulting & Training

Michael is a Microsoft Certified Solutions Master (MCSM) and Office Servers & Services MVP. As an independent consultant, he has helped customers all over the world to design, implement, secure, and migrate to Exchange and Office 365. Michael is also a published author, and has co-authored several books, including the coveted 'Office 365 for IT Pros' e-book along with Tony Redmond and Paul Cunningham.

Office 365 is a major success story for Microsoft. Although Microsoft still does not disclose exact numbers of active users or Office 365-specific revenue, in the October 2017 earnings call Microsoft executives reported that Office 365 now has more than 120 million active monthly users. In addition, Microsoft reached its target of $20 billion of cloud-related revenue (including revenue from Azure, Dynamics, Office 365, and Enterprise Mobility + Security) about two months before their target date. The majority of the organizations using Office 365 are small to medium businesses that span a variety of market segments. However, a significant portion of Office 365 customers are from enterprise: Almost every Fortune 500 company also leverages Office 365 in some shape, way, or form, with an increasing number moving their key workloads to it.

Microsoft's arguments in favor of Office 365 fall into a few well-defined categories:

More for less

Microsoft claims that the subscription cost for Office 365 is lower than the cost required for most organizations to provide their own on-premises services, and that any cost differential is more than balanced by the broad portfolio of services and capabilities included in Office 365 enterprise plans.

On-premises simplification

Moving email, communications, and collaboration work to the cloud means that Office 365 customers can dramatically reduce the amount of on- premises infrastructure they have to keep in place. This reduction leads to immediate direct cost savings; Microsoft has had success marketing this simplification as a way to rebalance IT spending by freeing up money dedicated to on-premises work for other uses.

Unique features

By introducing compelling new features such as Microsoft Teams, Delve, and MyAnalytics, Microsoft is trying to entice customers by offering capabilities that aren't available on-premises. Although this stance has aggravated some customers, it gives Microsoft a strong argument to make to customers who have resisted migrating to the cloud.

Peer pressure

Microsoft's strategy has been to "land and expand"—get bellwether customers in a particular territory or industry, then use their experience to induce other similar customers to move. Coupled with a muscular marketing effort, this strategy has definitely paid dividends.

That's not to say that the success of Office 365 is due only to these factors. The fact that Office 365 has been so successful across such a wide range of customers is also due to the technical and operational excellence of the products. The value proposition Microsoft has established for hybrid operations is a big part of this excellence. Hybrid configurations ease the on-boarding process, making the (technical) decision to migrate to Office 365 a lot easier –especially for large and complex environments. However, as customers start their individual journeys to Office 365, there are some weak spots in the portfolio of monitoring and management tools that the service offers, and it's important to know and understand what these are in order to make your own experience as smooth as possible.

Monitoring challenges in Office 365

Traditional monitoring solutions focus almost entirely on the infrastructure supporting a specific service or application. While this approach proves relatively successful in a pure on-premises scenario, it is much less effective with cloud-based services. In an on-premises scenario, you typically have a full understanding of what each piece of the infrastructure is responsible for, what the relation is between components, and what "normal" behavior looks like for each component. When one component breaks or underperforms, you know what the impact will be on other components and, ultimately, the service or application depending on it. In addition, your on-premises environment is probably mature and stable, as you have been able to monitor and fix issues with it over time to increase its performance, stability, and reliability.

Cloud-based systems are very different. First, you do not have visibility into the supporting infrastructure, let alone an understanding of how components relate to one another. As such, even if you would have access to all the metrics of the infrastructure, the information wouldn't be useful. As one example, consider the servers that Microsoft uses to implement the Office Graph- powered features such as Delve—outsiders have no way to know how many or what kind of servers are handling that work, what they're doing, or what a normal performance baseline looks like.

Second, the massive scale of services like Office 365, plus the way users are distributed across several datacenters and hundreds of thousands of servers, make it nearly impossible to maintain the same monitoring paradigm. Within a sea of information, you can't correlate what information is relevant to you and what isn't, in part because you don't have complete information about all the components and in part because of the scale and complexity of the environment. This problem is worsened by the fact that the cloud service provider has little information about your network.

Because of the fundamental differences between how an on-premises application or a cloud-based system are managed, an entirely new monitoring approach is required. This approach must focus on the service and the tasks one executes through it and capture the true user experience. For example, in Exchange Online, one of the core tasks is the ability to send and receive email. Even if you knew what the queue length for a specific server is, that one data point would not tell you anything useful about your own experience using the service. However, if you proactively test the ability to send/receive email, you effectively measure the end-user's experience by doing so. The ultimate measure of any cloud-based service is whether or not the user can use the service to accomplish some task and

what performance and error conditions they encounter, if any, while doing so. This is information that Microsoft doesn't expose to users or administrators.

The best way to measure the end-user experience is to perform synthetic transactions. Synthetic transactions programmatically mimic end-user interactions with the service and typically focus on the most common actions a user executes. By faithfully performing the same operations that a "real" client such as Outlook 2016 or Skype for Business 2015 would perform, these transactions give you an end-to-end view of the service, including DNS and network operations, logon, and sending and receiving data. The results of the transactions, including success or failure, measures of latency and performance, and historical trends allow you to quickly identify issues with the service, with hybrid components that you maintain to support the service, or with connectivity between the user's location and the service.

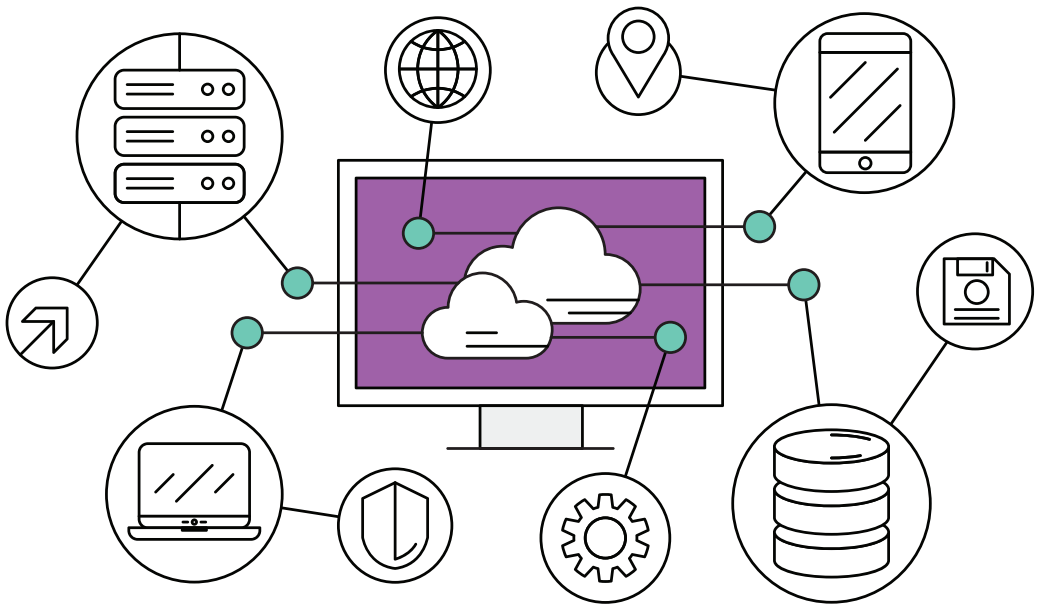
Although synthetic transactions can provide a lot of information about a specific action, such as whether the action was successful and how long it took to perform a certain task, the behavior of a transaction alone does not necessarily tell you what component caused a specific problem or where an issue occurred. For this, synthetic transactions must be complemented with the necessary

application logic and additional tests allowing the monitoring solution to correlate events, ultimately enabling it to provide you with detailed insights into the cause and location of the problem.

Hybrid configurations prove particularly problematic in terms of monitoring. Just like how you don't have any visibility to the infrastructure of a service provider, the same is true the other way around—Microsoft has no idea if or when there are problems affecting your on-premises servers. However, in some scenarios on-premises components are crucial to the operations of the cloud- based service. Great examples of this are directory synchronization and Active Directory Federation Services servers. When an organization decides to use these services, additional components are deployed on-premises and become the customer's responsibility. This responsibility is magnified by the fact that, in many hybrid environments, the AD FS and dirsync servers are new to the environment and not managed to the same standard, or with the same skill, as the existing mature on-premises systems. If one of these services fail, the consequences to the service can be substantial. For example, when the AD FS infrastructure becomes unavailable, no users will be able to log on to any Office 365 service. While an end user will perceive this as an Office 365 outage, this particular scenario falls solely within the responsibility of the customer to detect and solve.

Cloud-based systems, such as Office 365, enable organizations and users to work from virtually anywhere. Because of this, monitoring a service from a single location, typically the organization's datacenter, no longer represents how applications are used in the real world. As users roam between various locations, and connect from both within or outside the boundaries of the corporate network, it is important for an organization to understand if service issues are confined to a single location or if an outage is affecting its operations at a larger scale –potentially even service-wide.

.



Microsoft's monitoring approach

Microsoft performs a large number of monitoring tests on the Office 365 service; they have to, given the scale and reach of the services. However, these tests don't necessarily produce results that are useful to tenant administrators.

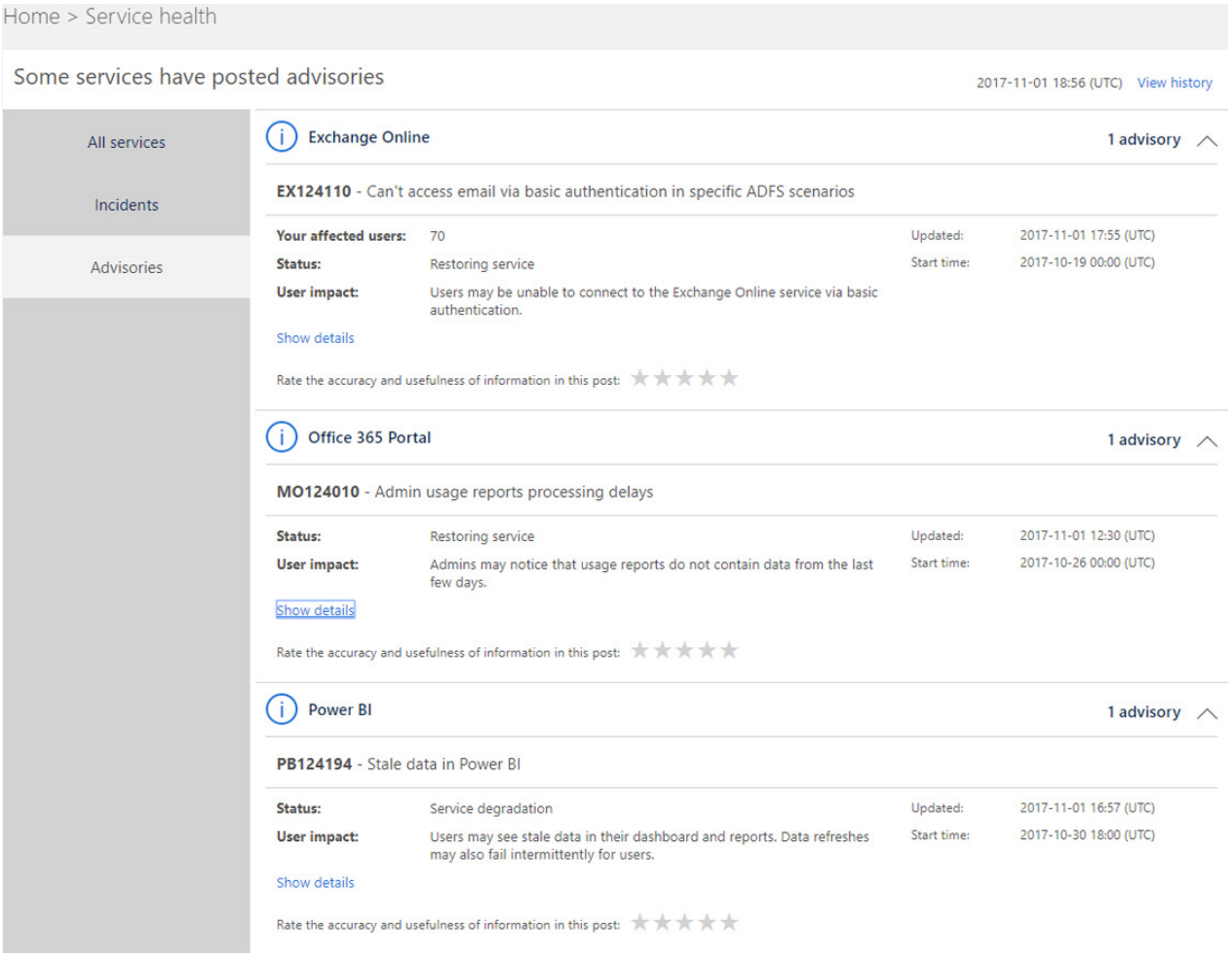


Figure 1 *An example of the Service Health Dashboard showing issues that do not actually affect the tenant for which it appears.*

Today, Microsoft exposes health information about Office 365 services through the Service Health Dashboard (SHD). The information that is provided through the dashboard, or the underlying Service Health API, is only of limited use as it focuses primarily on the overall service health instead of tenant-specific or user-specific problems. Because of the massive scale of Office 365, the dashboard almost always reports some type of issue in one of its services as, logically, there is always something going on somewhere. A warning in the dashboard does not necessarily mean that your tenant is affected or that some of your users are experiencing problems. Often, service issues are accompanied with vague descriptions of who might be affected, leaving the customer wondering if an issue impacts them or not. This creates a new challenge for the administrator as they are left with the question of whether an issue is relevant and, if it is, to what extent.

The SHD also does not send automated alert notifications. One must purposefully logon to the SHD or query the data through the API in order to view the latest health information. In the past, some issues in Office 365 were directly related to an outage in Azure Active Directory which prevented access to the SHD. For instance, in the July 2015 outage, users in North America were unable to authenticate to Office 365 because of a bad update to Azure Active Directory. This also creates a Catch-22 situations for the Service Health Dashboard: the inability to authenticate to Azure AD also prevented users from getting up-to-date Service Health Information. What good is a health dashboard if you risk being locked out of it?

The SHD only displays outage information when Microsoft decides to formally report an incident. In an October 2017 Azure Storage outage, nearly eight hours elapsed between the first outage indications and an outage announcement in the Azure service health dashboard. During that time, customers were left to wonder whether there was an outage and, if so, whether it was going to affect them.

There's another serious issue: whatever monitoring solutions Microsoft provides for cloud services, you still have to monitor your directory synchronization and federation health. Microsoft has released Azure AD Connect Health, which allows you to monitor specific aspects of your Directory Synchronization solution, but it is not integrated with Office 365, requires separate Azure AD Premium licenses, and lives in a different portal than the Service Health Dashboard. The limitations in Microsoft's Operations Management Suite (OMS) and Azure AD Connect mean that you must turn to alternative solutions to monitor other aspects of your environment that could directly or indirectly affect the operations of the service. This is particularly important so that an administrator can figure out what causes an outage. It allows an organization to respond appropriately to detected issues. The ability to detect where an outage stems from crucially important as it ultimately allows you to drive down the Mean-Time-To-Resolution (MTTR) of reported issues. For instance, this would be the case where your AD FS servers become unresponsive. Because these servers are your responsibility, you can

respond by fixing the issue yourself. Because you also monitor the on-premises components, you can reliably detect cloud-outages, when they happen – even though large-scale issues are far and few in between. The way you handle an outage is obviously different when the issue occurs within Microsoft's datacenters. In such case, all you can really do is open a support ticket so that Microsoft is aware of the issues and can keep you in the loop while they solve the problem on their end.

How Mailscape 365's better monitoring helps you

The old way of monitoring on-premises servers simply doesn't work in the cloud. You can't install monitors within Office 365 datacenters to tell you what's going on there. Instead, monitoring solutions have to use a variety of mechanisms to achieve broad coverage and be able to assess the quality of service available to end users. Synthetic transactions are useful in measuring how a workload behaves from the perspective of an end user. In addition to measuring application responsiveness to end user requests, monitoring solutions can use probes to test whether Office 365 components are online and are able to respond to end user requests to log on or conduct transactions. For maximum effectiveness, these probes should use a mix of passive monitoring and synthetic transactions to accurately report what the end user experience is from a variety of locations. Finally, Microsoft makes service health and monitoring data available for tenants through APIs so that the data used for Office 365 service dashboards can be harvested and interpreted in light of other information to provide the fullest possible picture of what's happening across on-premises, hybrid, and cloud operations.

The best monitoring solutions don't depend on a single source of data to make assessments. Logically, the more information that is available, the clearer the picture and the better a decision can be made about what to do should an outage occur. In addition, monitoring solutions that extract data on an ongoing basis are able to report availability and outage trends on an historical basis over a monthly, quarterly, yearly, and long-term basis. Analysis of this data can identify any weaknesses that might exist in a configuration and allow administrators to rectify issues before they become a real problem.

Knowing immediately when a problem exists, where the fault lies, and why the issue has occurred, especially in some of the more complex components involved in hybrid connectivity and mail transport, makes sure that any outages are detected and solved as quickly as possible.

Mailscape 365 provides that visibility into issues that develop within Office 365 so that mail keeps flowing and users remain productive. Figure 2 shows a timeline of major Office 365 outages, all of which Mailscape 365 had the ability to detect:

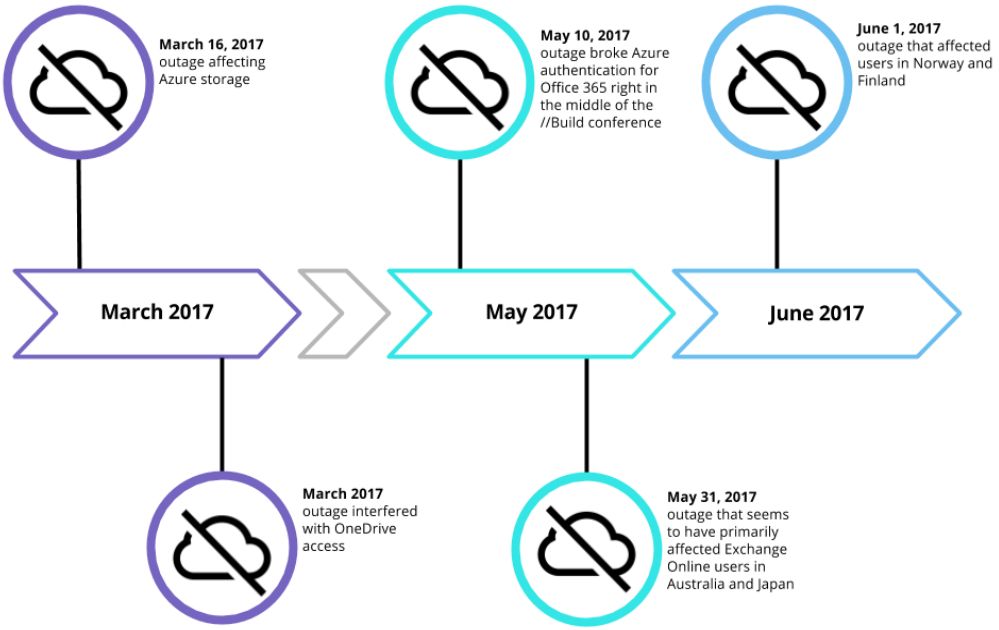


Figure 2 *Timeline showing major outages in Office 365*

- **A March 16, 2017** outage that affected Azure storage—this one bit us pretty hard at ENow because we use Azure so heavily.
- **A March 2017** outage that interfered with OneDrive access.
- **A May 10, 2017** outage that broke Azure authentication for Office 365 right in the middle of the //Build conference.
- **A May 31, 2017** outage that seems to have primarily affected Exchange Online users in Australia and Japan.
- **A June 1, 2017** outage that affected users in Norway and Finland.

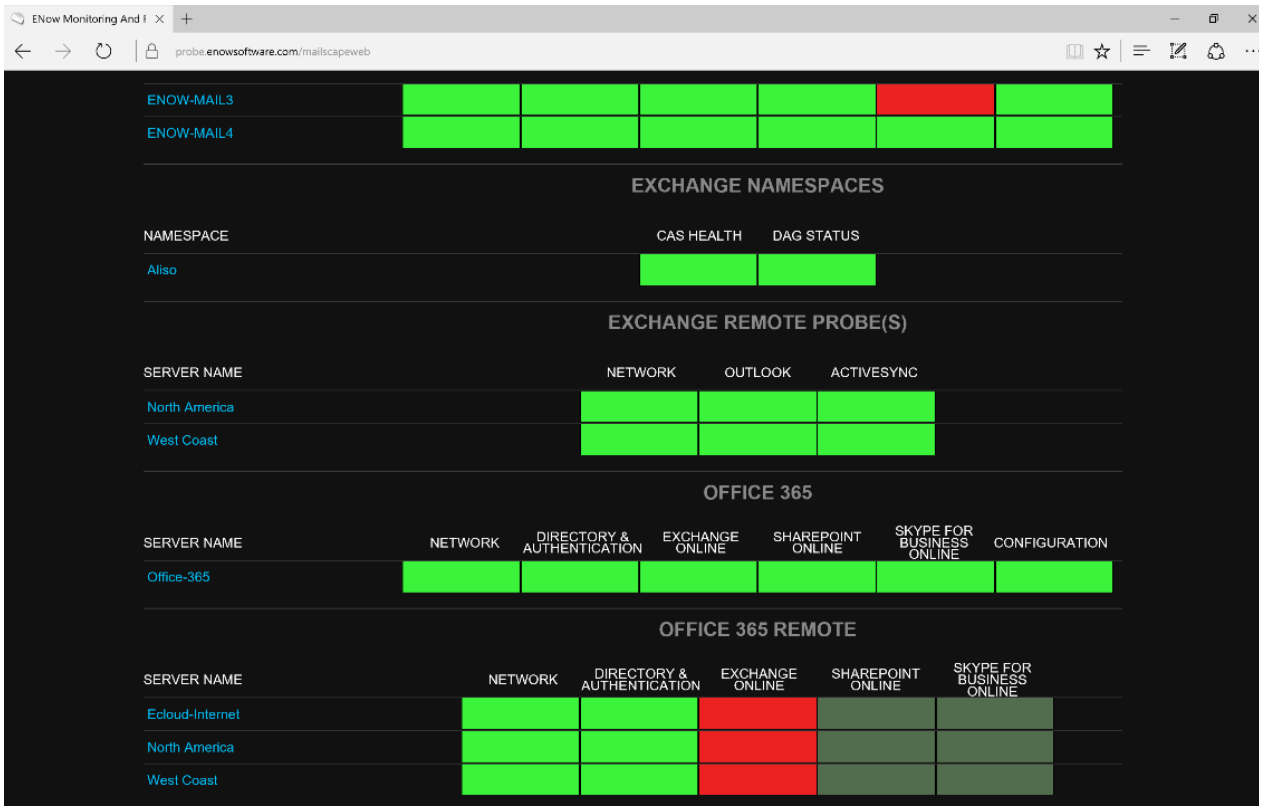


Figure 3 *the Mailscape 365 dashboard gives you an easily glanceable summary of service health and quality*

Mailscape 365 gives you a single consolidated view.

Because Mailscape 365 monitors Office 365 and your on-premises hybrid services, It provides a single easy-to-use overall view of everything that you need to check. You don't need separate tools to monitor on-premises servers, hybrid components, and Office 365. Everything is integrated and monitored as one system. The display is ideal for displaying on a large monitor in a network operations center or in a background window, where a quick glance tells you everything you need to know about the health of your environments.

Mailscape 365 eases your transition to Office 365.

Administrators use Mailscape 365 to accelerate the setup and configuration of their hybrid deployments. If your enterprise intends to use a hybrid environment, some new components are required that didn't exist in an on-premises deployment. The initial challenge is to deploy these components properly. Mailscape 365 eases that process by giving you detailed reports on the current state of your environment (including reports that identify potential pitfalls such as users whose UPNs don't match their primary SMTP address). The challenge then moves to steady operations

and monitoring. Mailscape 365 makes this process simple. Our solution automatically conducts an ongoing series of tests to ensure that all networking components including mail flow, Active Directory Federation Services, and directory synchronization are working properly. This gives administrators confidence in their configuration and saves hours of troubleshooting time when outages happen.

Mailscape 365 monitors hybrid components.

Preserving a solid end user experience is critical to the success of any deployment, including Office 365. Cloud platforms are enormously flexible and powerful, but incidents do occur from time to time. Mailscape 365 enables you to monitor your entire hybrid environment in real time so that you know what kind of performance end users experience at any time. This knowledge provides administrators with confidence that everything is working as it should be to deliver the intended experience to end users, eliminating some of the fear associated with moving to the cloud.

Mailscape 365 gives you early warning of problems.

Mailscape 365's monitoring provides early warnings of outages in any of the components within the infrastructure, including Office 365. It is obviously much better when administrators know that something has gone wrong and have taken steps to rectify the issue before end users notice that they can't get work done. Even if the problem cannot be immediately addressed because it is within Office 365, a support call can be logged with Microsoft and a mitigation plan can be put in place to advise end users what they can do to remain productive. For instance, if Exchange Online is unavailable, you can tell users that clients such as Outlook Web App and mobile devices won't be able to do much work with email and that they might be better switching to Outlook. If SharePoint Online is unavailable, users can be told to work with local copies of documents until online access is restored. Being able to proactively coach and guide end users during outage situations is a much better position to be in than having to scramble to understand what's going on and then rushing to react.

Mailscape 365 gives you end-user experience monitoring.

Mailscape 365 runs its suite of monitoring tests both from the server where it's installed and from an Internet service, giving you valuable perspective on the source of connectivity and functionality issues. In addition, you can optionally add Mailscape 365 Remote Probes that run monitoring tests from locations you specify. Remote Probes let you monitor service quality and performance from the locations where your users work so you always have up-to-date data about service quality in those locations. Monitoring the experience that individual end users have when using the service is critical to identifying and localizing problems. By deploying Remote Probes where your users are, you get complete visibility into performance and service quality at each individual location so that you always know where problems are occurring and who's affected.

Conclusion

Microsoft is investing huge amounts of money in growing the reach of Office 365. They're adding new services and capabilities, expanding into new regions, and ramping up their marketing efforts to capture more (and larger!) customers. Along with all these activities, they are continuing to slowly enhance their included monitoring tools. However, the nature of cloud services means that customers will never get the complete visibility they need from Microsoft's own tools; there are some components, such as hybrid services, that must be monitored from the customer side. In addition, customer-centered monitoring of service availability and quality is critical to detecting and resolving problems no matter their origin.

ENow's Mailscape 365 is the market leader in Office 365 monitoring and reporting because it combines synthetic transaction-based monitoring with Microsoft's own monitoring APIs to give you a clear, actionable picture of the state of your cloud services. Its unique combination of reporting and monitoring functionality has led the Gartner Group to recently recommend Mailscape 365 in their "Monitoring the Move to Exchange Online" research note.