

TROUBLESHOOTING MICROSOFT 365 END-TO-END: TURNING INTERRUPTION INTO INSIGHT

By Nick Cavallancia, Microsoft MVP

If your organization is among the 115M daily Microsoft Teams users or generally relies on the Microsoft 365 platform, it's safe to say that anytime a performance or service delivery issue arises, the impact on productivity and profitability is material. In short, you need Microsoft 365 not just running, but *running well*.

It's important to keep both those goals in mind when troubleshooting Microsoft 365; its services should be both available and not hinder the performance of its users.

Microsoft has long held to their service level agreement (SLA), citing that Microsoft 365 will maintain at least a 99.9% uptime (measured on a monthly basis). However, that doesn't mean it's going to be up all the time (that .1% of a month still equates to approximately 45 minutes of downtime monthly). Even if it is up for 100% of a given month, there's no guarantee that the performance of Microsoft 365 will be optimal... only that it be 'available', within the terms of the SLA.

This becomes a difficult standard to base an organization's productivity on, as Microsoft 365 is multi-faceted: is it the core Microsoft 365 services, the supporting services like Azure Active Directory, perhaps some network latency within Microsoft's cloud?

To make things more complex, in many cases, it may not even be Microsoft that is the root cause of a problem. The issue can sit firmly with a particular endpoint, a client application, the endpoint's method of connectivity to the Internet, or the route taken to the Microsoft cloud.

Organizations need a means by which to troubleshoot Microsoft 365 service delivery issues in a way that first provides some level of information about the scope of the problem, but more importantly provides internal IT teams with a level of insight into what the next steps are – whether this is simply communicating the outage to the impacted users internally or remediating the problem when possible.

In this whitepaper, we'll take a look at:

- ▶ The challenge of troubleshooting Microsoft 365
- ▶ Examine the need for proactive service quality management enabled by correlating end-to-end data
- ▶ Discuss the high-level metrics and data points that are useful in providing the needed insight
- ▶ How to leverage these insights to achieve proper response and remediation.



MARTELLO INSIGHTS

Creating Actionable Insight Through User Experience and Service Monitoring

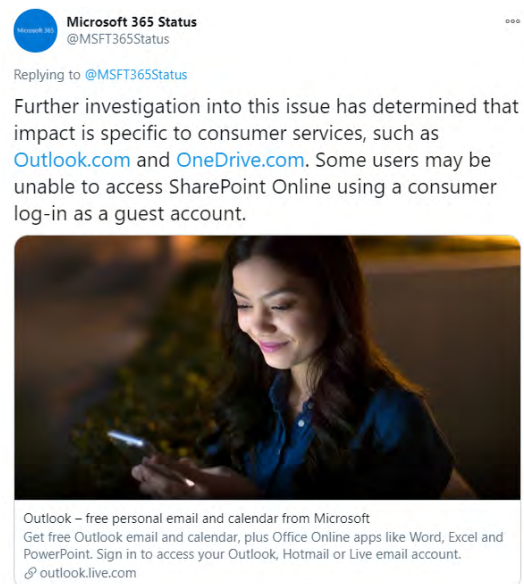
As with any service in the cloud – particularly Microsoft 365 – it's difficult to determine where along the path from user to Microsoft service lies the source of a service delivery problem. Without visibility into the entire spectrum of possible root causes – from endpoint to Microsoft cloud service – it's nearly impossible to respond and potentially remediate the issue. *Martello Gizmo* monitors the user experience, using synthetic transactions to simulate Microsoft 365 user activity, continually testing Microsoft 365 workloads to help identify drops in service quality, providing detail on scope, location, service impact, and more. *Martello iQ* collects, consolidates, correlates, and analyzes both Microsoft 365 services, as well as the internal infrastructure needed to ensure proper service delivery, providing insight into the root causes of issues from a service perspective.

MONITORING MICROSOFT 365: END-TO-END?

One of the tradeoffs of moving to the cloud is visibility; when someone else owns the service, the application, the networking stack, and/or the infrastructure, it's assumed that the organization is going to give up some visibility. But when service delivery issues arise – with Microsoft 365 or any other cloud service for that matter – the organization still looks to internal IT to diagnose and remediate the problem, regardless of the source of the issue.

Traditionally, organizations have deployed services and applications in their own datacenters, connecting them with monitoring solutions to detect the health of every component so IT knows everything is in “the green.” But today, all of that has moved to Microsoft’s datacenter, leaving IT with no direct visibility. Despite being the largest software company on the planet, even Microsoft can have service delivery issues from time to time.

To their credit, Microsoft does go to reasonable lengths to communicate outages in several ways; their own Microsoft 365 Service health status site, as well as their Microsoft 365 Status handle on Twitter. Take the example tweet, it demonstrates Microsoft’s commitment to keeping its Microsoft 365 users up to date on any service delivery issues.



Microsoft 365 Status Twitter post.

But these notification options also remind IT of the previously mentioned visibility tradeoff, as the organization waits on Microsoft to confirm an outage and relies solely on the granularity of the information provided in those notifications.

Also, keep in mind that the source of a service delivery problem may have nothing to do with Microsoft; it could be a problem with a slow personal computer, the users' home Wi-Fi, their VPN connection, a misconfigured client application or browser, or an issue stemming from routing network traffic through the corporate network before heading out to the Microsoft cloud; and there's no health status site or tweets for those kinds of issues.

In essence, internal IT is flying a bit blind and only knows there's a problem when either the user or Microsoft notifies them.

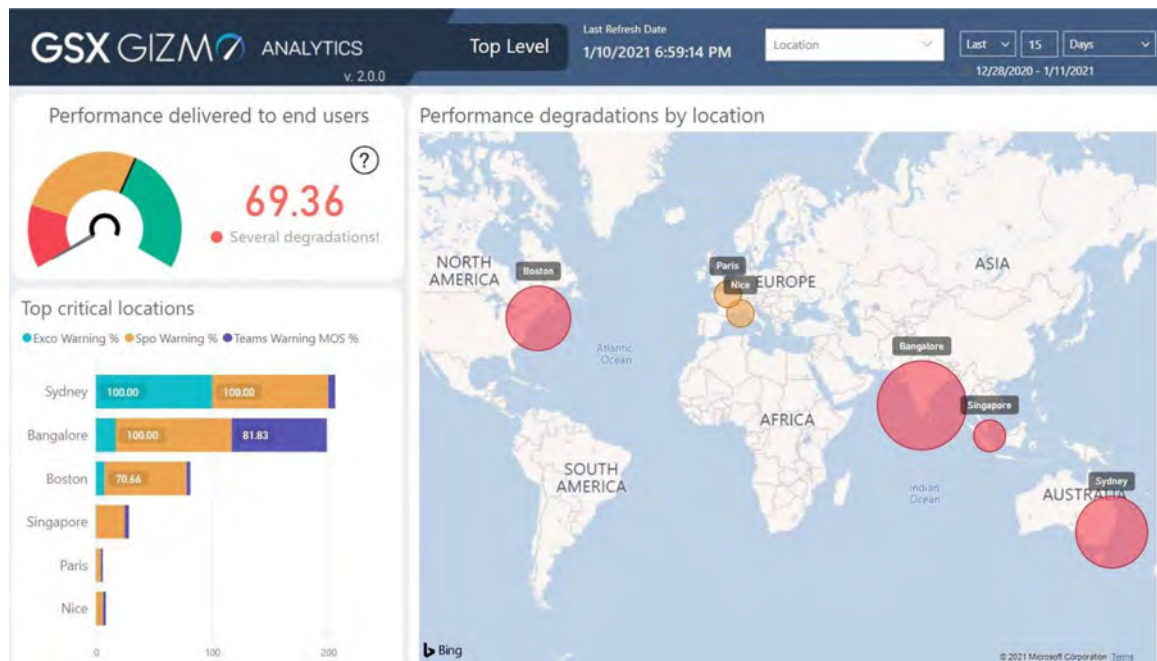



MARTELLO INSIGHTS

You Must Create Visibility When None Exists

The cloud tradeoff leaves IT in a precarious position; since Microsoft owns the stack from infrastructure to service, it's nearly impossible for organizations to gain the visibility needed. It's imperative that IT finds ways to gain visibility into everything that makes up the connection between the user's endpoint and Microsoft's services.

Martello Gizmo provides IT with visibility from the perspective of the user. By creating synthetic transactions, Gizmo emulates user transactions, interacting with the very same servers, applications, services, and data that an actual user does – providing visibility into endpoint, client, and connectivity specifics useful for response and remediation.





Instead of waiting until the user informs IT of the problem, Gizmo proactively seeks to identify when there are service delivery issues. Using a PowerBI dashboard, Gizmo can provide organizations with needed visibility into the state of their user's interactions with Microsoft 365 services, proactively yielding insight into the when, where, and who may be having (or will have) service issues.

For those organizations that heavily rely on Microsoft 365 services, this simply isn't enough; a scenario where IT finds out well after users begin feeling the repercussions of an outage is simply too late. This doesn't empower internal IT to do anything to at least understand who was impacted, what services were disrupted, and, if possible, what the root cause was.

Traditionally in larger organizations, internal IT is broken into many technology silos, each with their own team and monitoring system with limited visibility into where the problem lies and even less insight into what to do to fix the issue. What's needed is end-to-end visibility (rather than per-business application) and the ability to correlate monitoring data in a way that makes your IT teams not just aware of the problem but gives them enough proactive context and detail that it becomes actionable insight – ideally *before* users find the problem themselves.

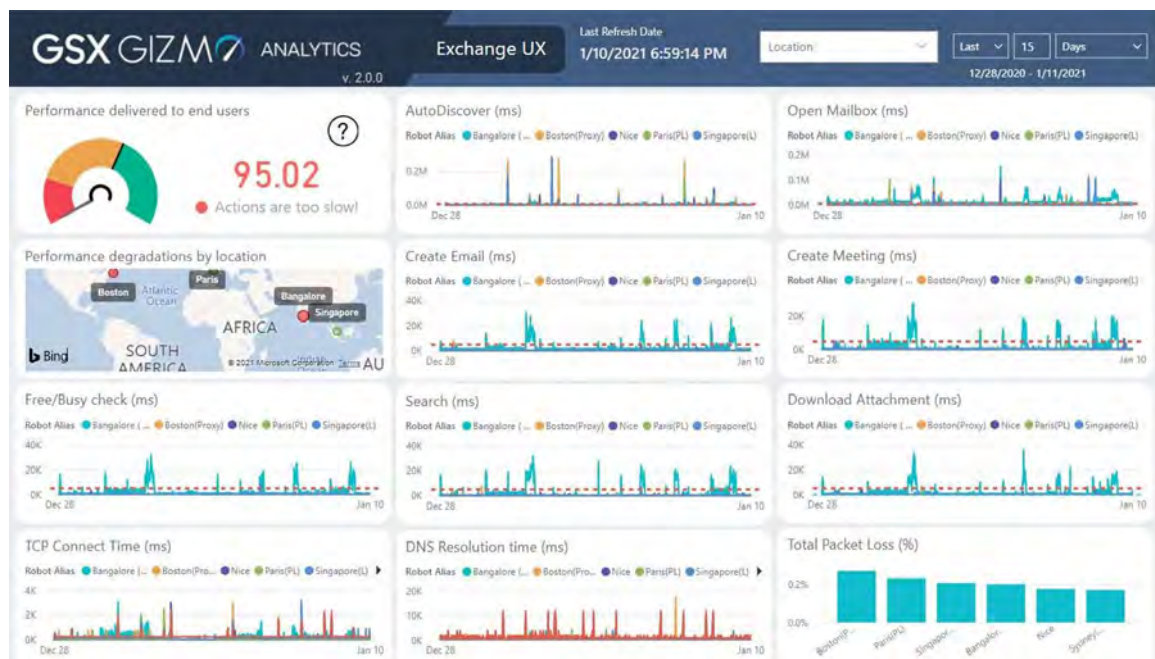


MARTELLO INSIGHTS

The Importance of Granularity

In the tweet above, Microsoft often limits the notification to a list of different services and perhaps a geographical region. That's not enough for your organization; you need to know whether your users are impacted, which ones, and is there anything you can do about it. You don't just care if SharePoint Online is up and running; you care whether your business and its users are operational.

Because Martello Gizmo mimics users' actions using the very same APIs Microsoft uses in their client applications, IT has visibility into whether there are problems with authentication, accessing a mailbox, downloading a file, create a meeting, and more.



This level of monitoring granularity allows Gizmo to identify not just when and where a problem exists, but also provides context into scope, severity, as well as what functions, client applications, and locations are impacted.

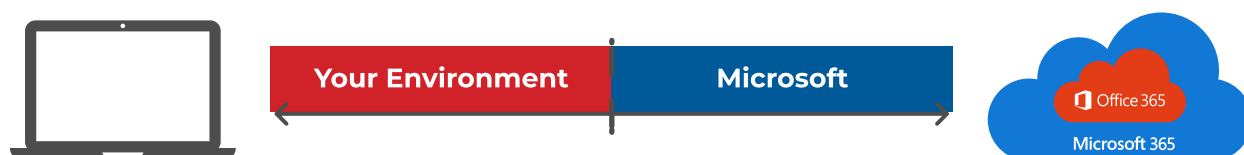
FOCUSING ON INSIGHTFUL METRICS, DATA, AND EVENTS

It's great to have the traditional dashboard “red/yellow/green” type of indicators of potential problems, but organizations today require a granular level of understanding of what their Microsoft 365 users are experiencing.

There's a significant amount of data that can be utilized (e.g., Windows endpoint logs, network traffic data, service status detail, etc.), but your focus should be the data that can yield an insightful response – whether that includes remediation or simply communication of the problem – on your part.

So, where should you place your monitoring focus to gain the needed insight?

First, keep in mind the two basic parts of the “end-to-end” spectrum between your users and the Microsoft service(s) they rely upon.



- ▶ **Your Environment** - Because it's important to consider all that goes into the user experience, it's necessary to have visibility into whether something within your environment is impacting Microsoft 365 service delivery, even if for only one user.
- ▶ **Microsoft** – Any part of the Microsoft 365 platform up and down their stack (servers, services, connectivity, bandwidth, authentication, etc.) can equally be the source of the problem.

In general, there are 6 basic sources of insightful data, listed below in a somewhat left-to-right order based on the spectrum graphic above.

- 1. Device** – For users deemed critical to the organization, understand the resource usage of their endpoint. A simple reboot could be all that's needed to rectify a perceived performance issue.
- 2. Application** – While Microsoft has taken efforts to ensure client applications are up to date, it's possible to be using an older thick client or even an older browser that may impact performance. Understanding what application is being used will aid in troubleshooting an issue.
- 3. Connectivity** – How is the user getting on the Internet? We all regularly rely on WiFi, but that doesn't mean it's the best option and could be the problem. Knowing whether a wireless or wired connection is in use is pertinent.
- 4. Routing** – Microsoft recommends having users route directly to the Microsoft cloud. Should you first route them through the corporate network via VPN, there may be slowdowns that have nothing to do with Microsoft or the user and everything to do with internal security scans, routing problems, etc. Having visibility into the route taken, as well as any services used (e.g., internal DNS, scanning solutions, etc.) along the way would be helpful.
- 5. Authentication** – Microsoft has had many authentication-specific service issues that keep users from gaining access to Office services. Knowing this is the problem is far more helpful than a user that simply says to IT "Microsoft 365 isn't working." Understanding whether authentication is successful or not (from multiple users) helps determine whether we have a Microsoft problem or a forgetful user.

- 6. Services** – You need to know which services are impacted and in which geographies. In some cases, the problem may be with a particular functionality and not an overall service outage; this level of detail could help keep users working instead of stopping work when IT says “Email isn’t available” because they aren’t aware it’s just scheduling meetings that’s not working. Ideally, you need to understand whether services are available, as well as whether expected functionality is responding normally.

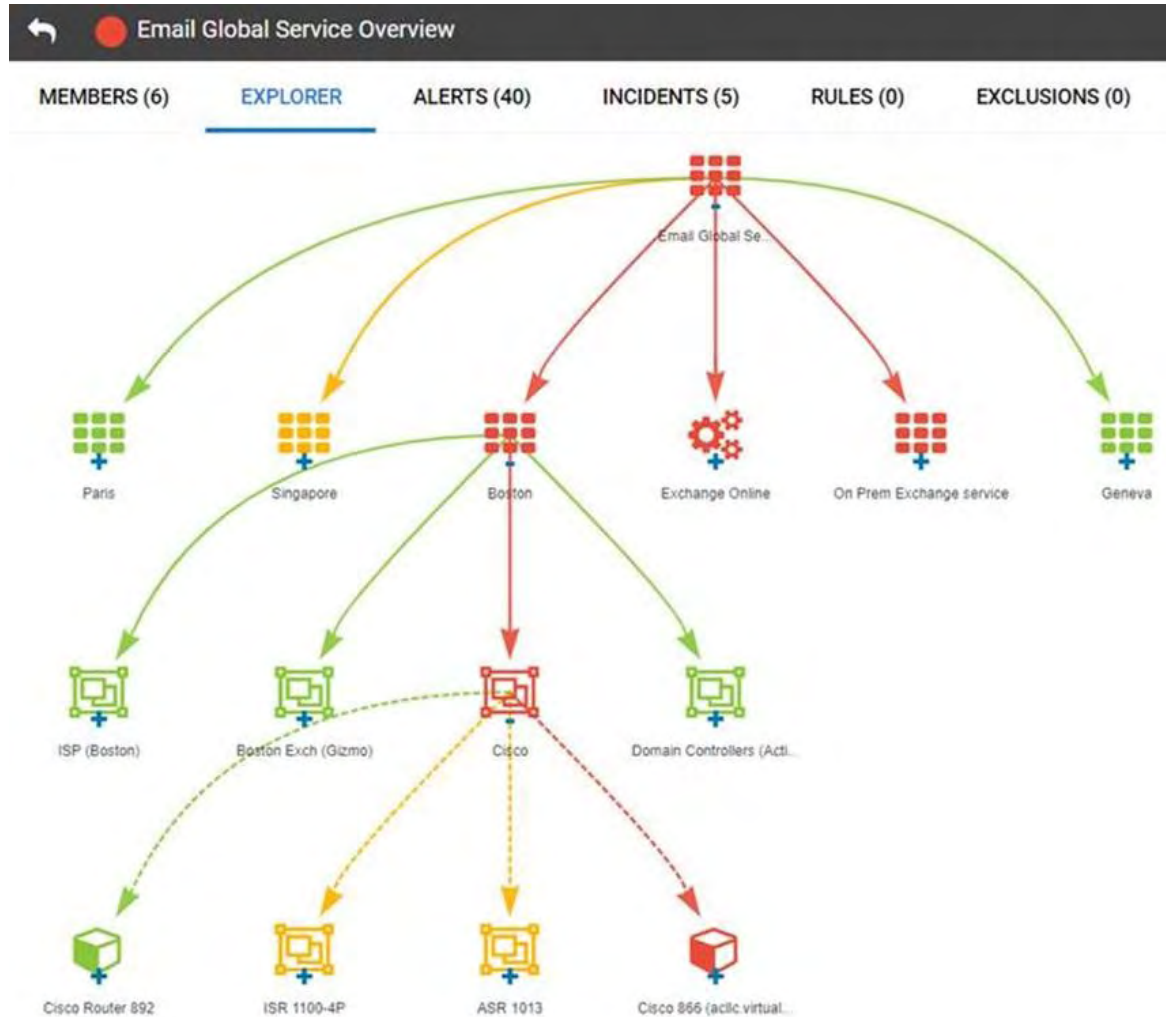


MARTELLO INSIGHTS

Thinking “as-a-Service”

When you consider the six sources above, it quickly becomes evident that your organization has varying levels of control and visibility to each. These function as separate IT silos – owned by separate teams using disparate toolsets. To properly troubleshoot issues end-to-end, it’s necessary to centrally have an overview of each silo, allowing each team to be working with the same data and have more comprehensive visibility into what’s transpiring, eliminating finger pointing and speeding up remediation time.

Martello iQ aggregates and correlates data from multiple sources (shown below), you can ensure the quality of service in a complex environment by avoiding service issue or even predict future interruption of service.



In the example above, iQ shows the end-to-end service is green in Paris and Geneva, but red in Boston. By expanding on Boston, it's possible to see which parts of the infrastructure, networking, authentication, and more are having issues, empowering the appropriate team(s) to quickly respond.

Ideally, there's a means to correlate all these monitoring sources; looking at just one facet of the spectrum only helps you understand one part of the overall user experience. It's necessary to have visibility into the entire spectrum, which requires pulling from multiple sources of data and correlating them. For example, envision a scenario where only one of your office locations is affected. If all you know is that *SharePoint Online isn't responding* for instance, you may simply believe it to be a Microsoft issue. However, if you have the correlating data that only one office is experiencing the problem – and that there are several offices in that same region of the world, you'd likely begin to look at the issue differently, realizing it may be a problem with the local office's network connectivity to the Microsoft cloud rather than with Microsoft themselves.

Having correlated data can yield a vastly different response.

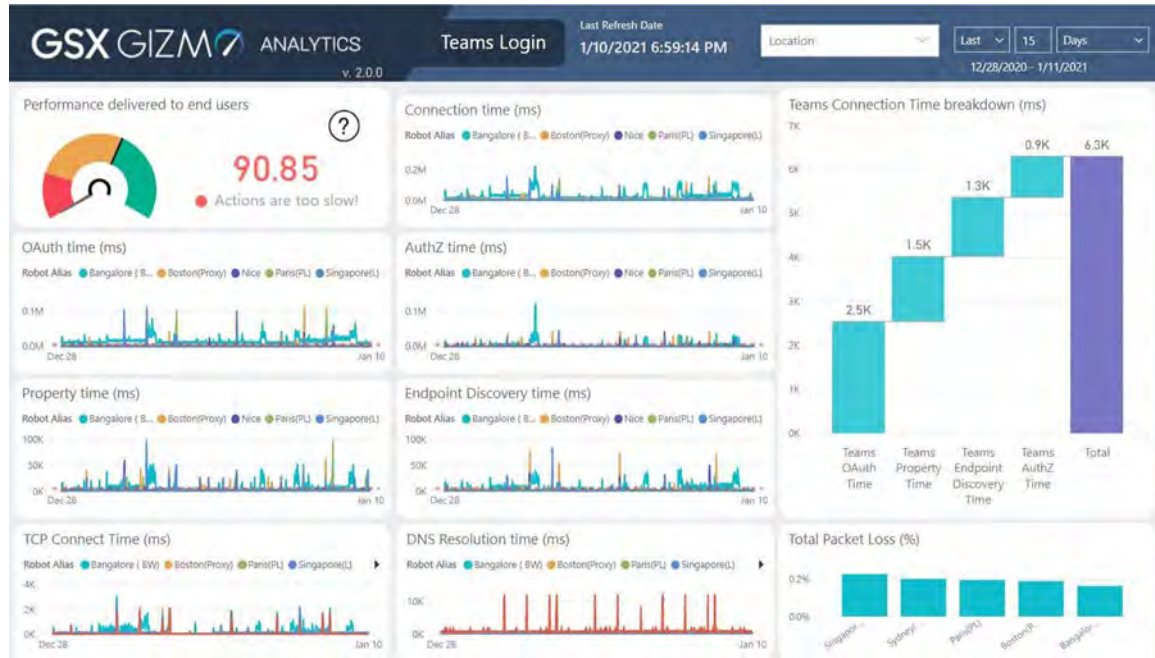


MARTELLO INSIGHTS

Should You Be Monitoring Specific Users?

There are at least a handful of key users within your organization that IT knows must stay productive. So, for the vast majority of users, the answer to the question above is no. But, keeping a watchful eye on certain users and locations may be warranted.

Martello Gizmo has the ability to synthetically mimic an individual user's experience with Microsoft 365. Take the example dashboard below, showing monitoring analytics for an organization's experience with Microsoft Teams.



In the upper left of the image above, the overall score for Teams is above 98%, which implies the organization's interaction with Teams is very good. But then when you look more closely, there are two C-level execs listed at the bottom right (the COO and CFO) that have 100% packet loss. Those two are having a very bad user experience with Teams. From the data, it's evident that this is not a global Microsoft issue (because most users are fine). Gizmo can also determine that the two users are in the same location, giving IT the notion to be looking at perhaps internal infrastructure as the culprit, or to begin looking to see if there is a problem with Teams within the region the two execs work. The more granular the monitoring via synthetic transactions, the greater ability for IT to triage service issues and address those that most require their attention first.

RESPOND TO ISSUES QUICKLY & EFFECTIVELY

Regardless of whether the source of the problem lies within your environment or Microsoft's, any monitoring you do shouldn't just be about alerting; you already have both Microsoft's status notifications and/or your users calling the service desk for that. Instead, think about how you can implement monitoring that creates actionable insight from two perspectives:

- ▶ **The User Experience** – Seeing Microsoft 365 as your users do (from the perspective of many different users using various connection methods, in different geographies, etc.) provides IT with a valuable way of demonstrating what one or more users are experiencing when interacting with Microsoft 365 – is it slow, unresponsive, or within norms? Is it one service or all of the services? etc.
- ▶ **Service-Oriented** – There's the simple "whether the service itself is running or not" aspect, but digging a bit deeper, there's the idea of grouping all the infrastructure, networking, etc. a given service (or access to a service) is reliant upon and including that into the monitoring as a subset. This allows IT to start at the 50K-foot level of "is the service green/red?" and dig deeper to assess every component that supports the access to the service to identify what's actually not functioning as expected and causing the issue.

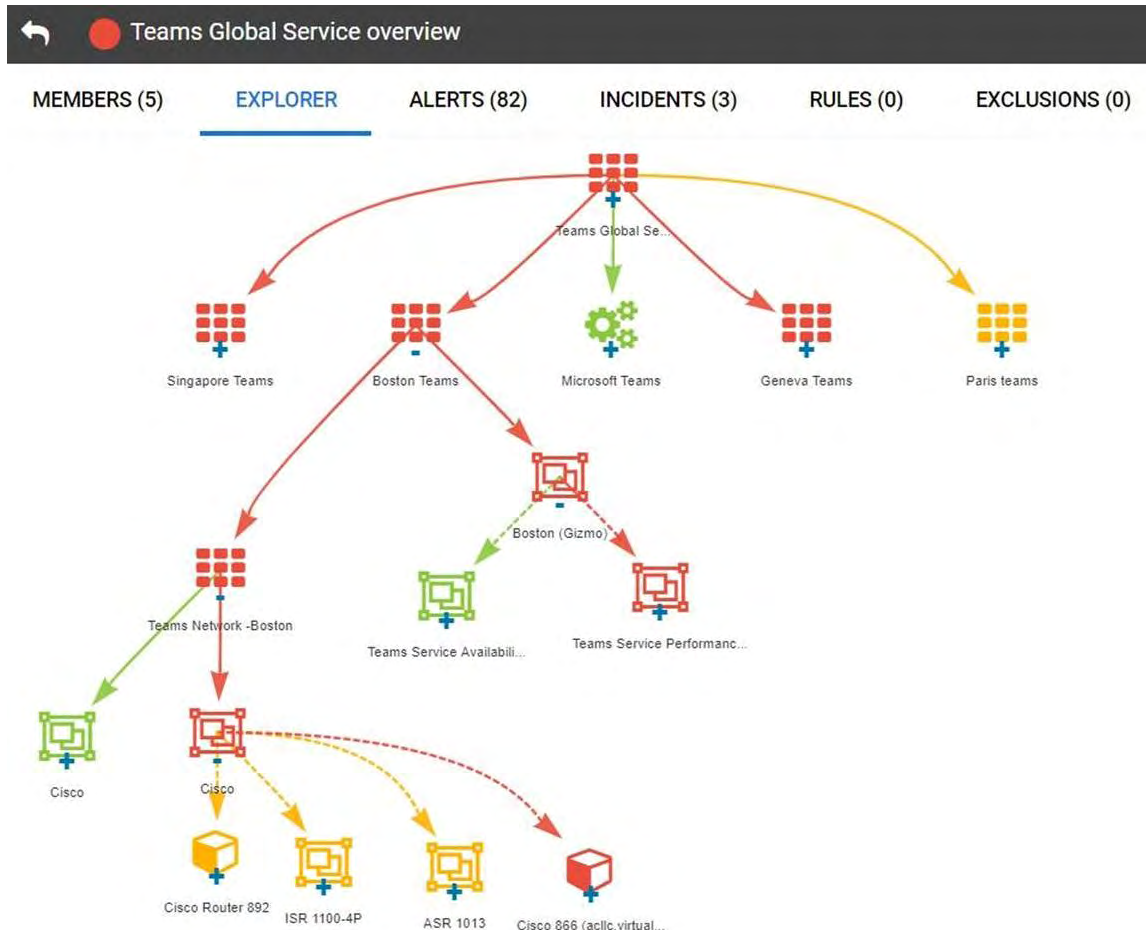


MARTELLO INSIGHTS

Why a Service-Oriented Perspective Is Important

Since the bulk of your issues are likely closer to the user, it's important to be able to quickly exclude them from the list of potential sources of a problem. User experience data from synthetic transactions will provide some insight (e.g., user DNS requests timing out), but it's also necessary to see at a high level whether everything you expect to be running to assist getting the user to interact productively with Microsoft 365 is running. For example, are the pieces of infrastructure used internally to connect a user to Microsoft 365 (e.g., the internal network components, DNS, ADFS, etc.) all up and running to support a good connection?

Martello iQ provides organizations with an ability to define what components are involved from end-to-end, including infrastructure, applications, and services that assist with connecting users to specific Microsoft 365 services. By defining everything involved in delivering a service, it becomes easy when a service isn't working properly to drill down into the supporting components and identify where the problem lies – whether it's on-prem or in the cloud.



Teams itself (top middle) is green, so the service on Microsoft’s side isn’t the problem. But the Boston office is in red, indicating a service delivery issue. Drilling down, you can quickly determine the problem is a Cisco 866 router that is the root cause and that it is already impacting other components.

This high-level service-oriented perspective is critical, as “end-to-end” is a very complex concept, requiring an ability to see every component – regardless of who owns it.

These two perspectives provide a more granular end-to-end monitoring of Microsoft 365. They empower IT to monitor critical scenarios involving specific users, locations, connectivity methods, application, or service and isolate on the problem which helps to focus the response.

If it's determined that the problem originates within your environment, having details on both the end user's experience as well as the infrastructure and services supporting the Microsoft 365 service in question can help expedite an exact remediation response. And should the problem be found to reside within Microsoft's control, your own monitoring should make your IT team proactively aware of a forthcoming problem. This ensures that they aren't simply blindsided when lots of calls come in, forced into firefighting mode, reacting to every call without first understanding the true nature of the problem.



MARTELLO INSIGHTS

What Can You Really Do If Microsoft Is the Problem?

If you determine a problem lies with Microsoft, you may wonder what good is having monitoring via synthetic transactions in place? It's a powerful thing to be able to communicate to your users or customers (as is applicable) that an outage exists, the scope of who is affected, the services that appear to be impacted, and that there's nothing the user can do. The simple act of communicating allows business teams to continue working as productively as possible – keeping users from wasting time trying to reconnect to an unavailable service, calling into the Service Desk, create tickets and create work for something IT can't rectify.

TURNING INTERRUPTION TO INSIGHT

Whether it's Microsoft 365 or any other cloud service, service interruptions should be expected. But in order for internal IT to be able to properly respond to an issue, you need to fully understand what's causing the problem, who's impacted, and why. By choosing an end-to-end monitoring approach – that includes both user experience and service-oriented monitoring – your IT team regains the lost visibility through granular details provided from synthetic transactions and service dependency details. This visibility helps IT to gain the insight necessary to determine service delivery root cause, identify impact scope, and take the necessary steps to either remediate an issue or at least minimize its impact.

ABOUT THE AUTHOR

Nick Cavalancia is a Microsoft Cloud and Datacenter MVP and has over 25 years of IT experience dealing with the architecture, implementation and training of Microsoft technologies to enterprise customers.

Nick has attained industry certifications including MCSE, MCT, MCNE, and MCNI. He has authored, co-authored and contributed to over a dozen books on Windows, Active Directory, Exchange and other Microsoft technologies and has spoken at many technical conferences on a wide variety of topics.



ABOUT MARTELLO

Martello Technologies Group Inc. (TSXV: MTLO) provides digital experience monitoring (DEM) solutions. The company's products deliver monitoring and analytics on the performance and user experience of critical cloud business applications, while giving IT teams and service providers control and visibility of their entire IT infrastructure. Martello's software products include Microsoft 365 end user experience monitoring, unified communications performance analytics, and IT service monitoring and analytics. Martello Technologies Group is a public company headquartered in Ottawa, Canada with employees in Europe, North America and the Asia Pacific region.

Learn more at www.martellotech.com

GET STARTED WITH A FREE TRIAL

SIGN UP NOW

MARTELLO