The Value of Proactive Monitoring for Managed Service Providers

By Kevin Kieller

Managed Service Providers (MSPs) look to provide the highest-quality service with the lowest operational cost. This requires implementing people, products, and processes that minimize the number of incidents, respond quickly to incidents raised, improve CSAT (and/or NPS) scores, reduce churn, and maximize revenue opportunities all while managing costs.

This paper explores the value of **proactive monitoring** and **advanced diagnostics** tools for managed services providers (MSPs) who support Microsoft Teams and Teams Phone.

The developed model was based on confidential interviews with small, medium, and large MSPs, and a systematic review of published literature. In developing this model we leveraged previous work exploring the primary sources of outages and service degradation in a Teams environment.

For the purposes of this article, proactive monitoring refers to tools that simulate user interactions on an on-going basis to detect service outages or service degradations as soon as possible. Advanced diagnostic tools extend the built-in Teams reports and provide better root-cause analysis including improved end-to-end network visibility.

Key Findings for MSPs

If MSPs implement advanced diagnostic tools and proactive monitoring our research indicates it is reasonable to expect...

- **50%** reduction in labor required for incident management
- **20%** reduction in churn
- **10%** upsell opportunity
- **20%** reduction in tickets that are escalated to Microsoft (which may incur support costs)
- **5%** improvement in CSAT (customer satisfaction) or NPS (net promoter score)
- **25%** reduction in SLA penalties, if applicable

Calculating Monetary Impact

Based on MSP interviews and our research, the developed model incorporates six primary variables:

AUTHOR'S NOTE

The model allows an MSP to modify any of the default values to align more closely with their market observations and experience.

1. The number of issues that escalate to incidents (i.e. create a ticket)
2. The time it takes to resolve an incident
3. The average customer retention rate (the complement to churn rate)
4. Upsell revenue potential
5. Cost associated with escalating incidents to Microsoft (i.e. opening a ticket with Microsoft)
6. SLA penalties incurred

Each of these variables is discussed in more detail below and an explanation is given for the default values used in the model.

Number of Incidents

Proactive monitoring can reduce the number of incidents that impact and are reported by MSP customers. Proactive monitoring relies on **synthetic transactions**, which simulate user activities to test and monitor the performance and availability of Microsoft Teams services. These transactions are pre-scripted actions that mimic real user interactions.

By continuously running synthetic transactions, MSPs can detect issues before they impact users at their customers.

Synthetic transactions allow incident mitigation through two primary mechanisms:

1. Detect and correct
2. Detect and communicate

Per the chart below, we identified 11 categories of issues that created outages or service degradation. For each of the identified 11 issue categories, we estimated the percentage of issues that could be mitigated with proactive monitoring, ranging from 0% to 90% depending on the source of the issue.

In total, our model indicates that over 40% of potential issues could potentially be mitigated with proactive monitoring.

What are Synthetic Transactions?

Synthetic transactions simulate user activities to test and monitor the performance and availability of Microsoft Teams services. These transactions are pre-scripted actions that mimic real user interactions, such as:

- Joining a Teams meeting
- Sending a message
- Sharing a file
- Scheduling a meeting

By continuously running these synthetic transactions, IT teams can detect issues before they impact actual users. This proactive approach helps identify performance bottlenecks, service outages, and other problems early on.

Agents or Appliances

To execute synthetic transactions, organizations deploy agents or appliances at various locations. Sometimes these agents are referred to as "robots". These agents can be software-based or hardware devices that perform the following functions:

- Monitoring Performance: Agents simulate user activities and measure the response times and success rates of these actions.
- Collecting Data: They gather detailed metrics on network performance, application responsiveness, service quality, and service availability.
- Alerting and Reporting: When an issue is detected, agents can trigger alerts and generate reports, providing IT teams with actionable insights.

Source of outage/ degradation	Description	Availability	Disruption %	Impact scope
Core services issues	The Teams service itself is covered by three different SLAs (Dec 1, 2024) 99.9% for chat and meetings, 99.999% for PSTN calls, auto attendants, and call queues, 99.9% "good" voice quality (VoIP or PSTN)	99.99%	0.01%	Broad
Supporting service issues	Even if Teams is "up", occasionally supporting services, such as Active Directory (aka Entra) or MFA (multi-factor authentication) can prevent users from accessing Teams.	99.99%	0.01%	Broad
Hardware issues	Occasionally individual users experience hardware issues; these could be related to their laptop, headset, or external camera.	99.99%	0.01%	Individual
Software issues	More often other software running on a user's laptop cause issues with Teams, either because CPU or memory resources are overloaded or because a video device is "in use" by another application. Pending Windows updates can also cause issues.	99.95%	0.05%	Individual
Human error causing configuration issue	Typically a misconfiguration, e.g. firewall rule, expired certificate.	99.90%	0.10%	Location (or Broad)
Network issues	Remote users may experience issues with their Internet provider. Occasionally office-based networks, especially WiFi may encounter problems.	99.70%	0.30%	Varies
Security issues	Cybersecurity issue - could impact entire org; disruption for security/Comms/PR because of this incident.	99.90%	0.10%	Location (or Broad)
Loss of power	Power disruptions due to scheduled maintenance.	99.90%	0.10%	Varies
Physical infrastructure damage	Occasionally an office may be inaccessible due to construction, events, or accidents.	99.98%	0.02%	Location
Weather issues	Inability to physically access specific site. The United States has seen a 67% increase in major power outages from weather-related events since 2000. In 2023, the U.S. experienced 28 separate weather and climate disasters, resulting in $92 billion in damages.	99.90%	0.10%	Location
End-user error/ issues	Primarily productivity degradation due to user training "blindspots"; no tickets because users don't realize inefficiency.	99%	1.00%	Individual

A summary of **mitigation strategies** and the percentage of issues that could potentially be mitigated by MSPs who have implemented proactive monitoring are summarized in the chart below.

Source	Primary mitigation strategy	Secondary mitigation strategy	Issues that can be avoided with proactive monitoring
Core services issues	Detect and communicate		75%
Supporting service issues	Detect and communicate		75%
Hardware issues	React efficiently	Detect and communicate	5%
Software issues	React efficiently	Detect and communicate	5%
Human error causing configuration issue	Detect and correct	Detect and communicate	75%
Network issues	Detect and correct	Detect and communicate	90%
Security issues	Detect and communicate		50%
Loss of power	Detect and communicate		75%
Physical infrastructure damage	Detect and communicate		80%
Weather issues	Detect and communicate		90%
End-user error/issues	Training	On-going training	0%

Mitigation Strategies

When an issue is detected, a variety of mitigation strategies can be employed to reduce or eliminate the impact of the issue. Standard mitigation strategies include ...

- Detect and correct: Synthetic transactions, used as part of proactive monitoring, often alert IT to issues before they impact end users; for example, a misconfiguration issue that causes an outage that occurs before or after working hours. In this case, IT may be able to diagnose and correct the issue before the start of the next work cycle.
- Detect and communicate: Proactive monitoring may note a broad or location-specific issue. Some issues may be outside the ability for IT to correct (for instance a Microsoft Teams or supporting service issue, such as the one that happened recently, referred to as MO941162; a power failure, or a physical cable cut). In these cases, IT can communicate the outage and suggest alternatives. For example, potentially rescheduling a meeting if Teams is not available or using an alternative meeting solution (many larger organizations maintain some Zoom or Webex licenses for this exact scenario), or working from home, a coffee shop, or another company location, if an issue is impacting a specific office.

For mitigation strategies to be effective, pre-work is required. This can include training users on alternatives (for instance making sure everyone knows how to "hot spot" if their home network or an office network is impacted) and preparing communications in advance of specific types of issues (e.g. office closures due to weather, power, or physical infrastructure issues).

Individual hardware and software issues are difficult to prevent and so the approach is to react efficiently. This also involves pre-work such as stocking spare devices, components, and having a tested process to "swap" out components, or in some cases entire laptops, while preserving data and configuration settings. For some organizations this could also include having "loaner" laptops that can be used while a full replacement is being arranged.

Time to Incident Resolution

Proactive monitoring can reduce issues, but it cannot eliminate every issue or the corresponding tickets that customers open with their MSP.

Microsoft continues to improve the built-in Teams reports, however, they often provide technical detail without clearly providing actionable information.

Microsoft reports also do not provide sufficient detail outside of the Microsoft environment. For organizations using Operator Connect, direct routing, and/or session border controllers (SBCs) built-in report details are incomplete.

Advanced diagnostic tools help MSP support engineers more quickly identify the cause of and resolve incidents by providing root cause analysis and delivering more granular network details.

As a default, we modeled that a standard support engineer can close 16 tickets during an 8-hour shift. A support engineer with access to advanced diagnostic tools is assumed to be able to close 50% more tickets in an 8-hour shift (24 tickets in this modeled scenario). The specific number of tickets were chosen as a baseline value to model the impact of improved efficiency; every MSP will have their own support load model depending on the services they offer. These also represent incident response averages; some tickets will take longer, some shorter.

Incident resolution time directly impacts the number of full-time equivalent (FTE) staff required to handle a comparable volume of tickets.

Advanced Diagnostics

Proactive monitoring can reduce issues, but it cannot eliminate every issue or the corresponding tickets that users raise.

Our model considers how advanced diagnostics can reduce the time required to identify an issue's root cause and resolve a particular issue.

Microsoft continues to improve the built-in diagnostic reports, most recently deprecating the Call Quality Dashboard in favor of PowerBI Quality of Experience (QER) report templates. However, both CQD and QER reports can be data rich and information poor. They provide lots of technical details but can overwhelm all but the most skilled IT professionals.

Additionally, the Microsoft reports don't provide much detail outside the Microsoft environment. Local network and ISP details are not fully captured using the Microsoft built-in reports. For organizations using direct routing, session border control (SBC) details and carrier SIP trunk details are incomplete. For customers using Operator Connect, key carrier or network service provider details are sparse.

Advanced third-party diagnostic tools can reduce the time taken to resolve a particular incident from an average of 30 minutes to 20 minutes. Put another way, a typical MSP support engineer can handle an average of 16 tickets per 8-hour shift using the built-in Microsoft tools and an average of 24 tickets per day with an enhanced set of tools.

AUTHOR'S NOTE

The FTE calculations reflect the total FTE complement required, which includes tier 1, 2, and 3 support and supporting administrative staff. Calculations also assumes MSP provides 7x24 coverage. The model allows you to adjust the average fully-loaded FTE cost to match your situation; as a default we use a conservative fully-loaded FTE cost of US $135K/year.

Retention Rate / Reduction in Churn

The retention rate represents the proportion of customers retained during a specific period, while the churn rate represents the proportion of customers lost during the same time period. These two rates are inversely related and together account for the entirety of the customer base within that period.

Feedback and research suggest that proactive monitoring, which often allows alerting a customer of a potential issue before it impacts their users, along with faster incident resolution can improve overall customer service levels and customer satisfaction which in turn can significantly reduce churn. We believe a 20% reduction in churn is a realistic metric and use this as a default value in our model.

Upsell Opportunity

MSPs indicated that not all customers may understand what proactive monitoring is and thus may not necessarily be able to sell "proactive monitoring" as a discrete add-on, that increases ARPU (average revenue per user).

However, MSPs did indicate that delivering more responsive service, leveraging proactive monitoring, would likely lead to the opportunity to either sell existing customers additional services OR in the case where the MSP offered tiered service levels (e.g. bronze, silver, gold) could help migrate a percentage of users to a higher, more revenue generating, tier.

Using information from our MSP interviews, the model defaults to using a 10% upsell potential based on the existing annual managed services revenue.

Microsoft Support Costs

MSPs are often required to have a Microsoft Premier support contract. According to Microsoft, "Microsoft Premier Support for Partners offers complete, end-to-end managed support across the full Microsoft platform to meet your complex needs, expand your capabilities in the cloud, and collaborate more strategically with Microsoft."

This level of support does not come cheap. On average premier support cases (aka tickets escalated to Microsoft) incur costs between $550 (if pre-paid) and $650 (paid when needed) per case.

Advanced diagnostic tools can help ensure only cases that relate to Microsoft services are escalated to Microsoft. Additionally, proactive monitoring combined with proactive communications can reduce the number of customers asking for an incident escalation to Microsoft.

AUTHOR'S NOTE

MSPs who are also Operator Connect (OC) providers may have direct access to premier support through the OC requirements/certification process.

Given the above, our model defaults to projecting a 20% reduction in cases sent to Microsoft if proactive monitoring and advanced diagnosti tools are implemented.

SLA Penalties

Some MSPs provide financially backed service level agreements (SLAs) while others only offer SLOs (service level objectives) aka targets.

For MSPs who do offer SLAs, proactive monitoring and advanced issue diagnostic tools can reduce the number of incidents that incur SLA penalties.

Based on our research, our model defaults to assuming a 25% reduction in SLA penalties when more advanced tools are deployed.

Other Noted Benefits

In our discussion with MSPs, several benefits not directly incorporated into the model were mentioned:

CSAT / NPS

To gauge the success of their service delivery and the health of client relationships, MSPs rely on key performance indicators (KPIs), among which Customer Satisfaction Score (CSAT) and Net Promoter Score (NPS) are prominent.

Both metrics are vital for MSPs to understand client sentiment, identify areas for improvement, predict churn risk, and gauge overall business health.

Our analysis confirms that while publicly available data directly quantifying specific point or percentage increases in CSAT or NPS for MSPs implementing proactive Microsoft Teams monitoring and diagnostic tools is scarce, a significant body of indirect evidence points towards a strong positive correlation. Evidence suggests expecting a 5 – 10% increase in CSAT / NPS.

Vendor audits

In discussions with MSPs, it was indicated that vendors, such as Microsoft, may conduct audits of partners to ensure quality of service delivery.

Advanced diagnostic tools, the associated detailed reporting, and proactive monitoring tools were mentioned as assisting to streamline this vendor audit process and improve the overall audit results. It is reasonable to assume that these tools would similarly assist should a prospective customer wish to audit an MSP's process.

Additional Model Variables

Additional assumptions built into the model (which can be configured) include:

- MSPs can expect 1 incident per every 1,000 physical phones deployed per day
- MSPs can expect 1 incident per every 50 Microsoft Teams Rooms per day.
- An issue or outage needs to last 10 minutes to create a ticket. For instance, if a momentary "blip" occurs while trying to join a meeting, most users simply retry.
- On average only 10% of users raise a ticket that advances to the MSP when an incident/issue occurs.

Using the MSP Model

The developed model allows an MSP to customize the inputs to match their specific situation. The calculations and output are then based on our interviews and research.

The intent of this model is to help an MSP understand how proactive monitoring and better diagnostic tools would impact their business.

The images below visually illustrate some of the input variables that can be modified to align with a specific situation.

Managed Service Provider (MSP) Scale, Scope, and Current State		**Notes**
Total managed customers	10	
Total managed users	20000	
Average users per MSP customer	2000	*Calculated*
Total managed desk phones	500	Suggest 1 per 100 users; assumes many orgs moving to Teams use softphones
Total managed rooms	1000	Suggest 1 per 50 users
Managed services revenue	$ 2,500,000	Annual revenue related to Teams, Teams Phone, or M365 workload management
Average managed user revenue (annual)	$ 125.00	*Calculated*
SLA penalty costs (if applicable)	$ 20,000	Estimated per year
Current retention %	90.0%	Should be 90%
Churn	10.0%	*Calculated*
Tickets escalated to Microsoft	1%	Under premier support; enter 0 if not applicable
Cost per Microsoft ticket	$ 650	Previously $200-$300/hr; now $650 flat rate per ticket ($550/case if prepaid, min 100 cases)
Primary model assumptions		
Reduction in SLA penalties	25%	Faster diagnosis and correction of issues
Vantage DX reduction in churn	20%	% of churn reduction due to proactive monitoring and advanced diagnostics (faster issue resolution)
Upsell potential as a percentage of managed service base	10%	Either moving some users to higher level service, selling additional user service, or selling customer complimentary service
Vantage DX mitigates how many Microsoft tickets	20%	Based on better visibility of root cause for issue
Average office/location size	500	Used to determine scope of incidents that impact one location
Incident ticket assumptions		
Disruption minutes to create incident	10	
Percentage of users impacted who raise a ticket	10%	Lowered from 16% used in original model as not all tickets will be escalated to MSP
Tickets MSP support engineer can handle per work day	16	8 hour shift
Tickets MSP support engineer can handle per work day with DX	24	Identifying root cause takes less time with DX
Fully-loaded annual IT FTE cost (incl. vacation, bonus, benefits)	$135,000	
		in USD$
Issues creating Teams outages or service degradation for MSP customers		

Source	Availability	Disruption %	Impact scope	Annual Disruption minutes	Annual Incidents
Core services issues	99.99%	0.01%	Broad	26	2
Supporting service issues	99.99%	0.01%	Broad	26	2
Hardware issues	99.99%	0.01%	Individual	26	2
Software issues	99.95%	0.05%	Individual	131	13
Human error causing configuration issue	99.90%	0.10%	Location (or Broad)	263	26
Network issues	99.70%	0.30%	Varies	788	78
Security issues	99.90%	0.10%	Location (or Broad)	263	26
Loss of power	99.90%	0.10%	Varies	263	26
Physical infrastructure damage	99.98%	0.02%	Location	53	5
Weather issues	99.90%	0.10%	Location	263	26
End-user error/issues	99%	1.00%	Individual	2628	262
Total disruption percentage		1.80%	**Total hours**	**79**	

Example Results

Based on the rationale and assumptions detailed above, our MSP model projects the following outcomes for MSPs with different-sized Teams businesses.

Our model shows an MSP that generates $1 million/year revenue from 4,000 managed Teams users, would be able to reduce operational costs by $500K per year and would be able to increase revenue by $120K per year.

The model below focuses on the costs of an MSP responding to Teams-related incidents with and without proactive monitoring and advanced diagnostics (not MACDs). Churn reduction and upsell potential are based on interviews and research.

MSP with 4,000 managed Teams users, $1,000,000 annual revenue and 10% churn

	Without proactive monitoring and advance diagnostic tools	With VantageDX	
Full-time equivalent resources (FTEs) required for incident management	5.8	1.9	67% fewer FTEs
FTE cost	$ 783,000	$ 256,500	
Microsoft support ticket cost	$ 120,725	$ 96,580	Reduced by 20%
SLA penalties	$ 10,000	$ 7,500	Reduced by 25%
Potential savings due to proactive monitoring and advanced diagnostics		**$ 553,145**	
Gross incident support cost per user	$ 228.43	$ 90.15	
Incremental value			
Reduction in churn (20%)	$ -	$ 50,000	
Upsell (10% of users @$180 per user)		$ 72,000	
Potential value due to proactive monitoring and advanced diagnostics		**$ 675,145**	

An MSP with a larger managed Teams business having 20,000 users would require 50% less FTEs and could expect might expect a $2 million per year positive impact.

The model below focuses on the costs of an MSP responding to Teams-related incidents with and without proactive monitoring and advanced diagnostics (not MACDs). Churn reduction and upsell potential are based on interviews and research.

MSP with 20,000 managed Team users, $6,000,000 annual revenue and 10% churn

	Without proactive monitoring and advance diagnostic tools	With VantageDX	
Full-time equivalent resources (FTEs) required for incident management	17.0	7.8	54% fewer FTEs
FTE cost	$ 2,295,000	$ 1,053,000	
Microsoft support ticket cost	$ 352,677	$ 282,142	Reduced by 20%
SLA penalties	$ 10,000	$ 7,500	Reduced by 25%
Potential savings due to proactive monitoring and advanced diagnostics		**$ 1,315,035**	
Gross incident support cost per user	$ 132.88	$ 67.13	
Incremental value			
Reduction in churn (100%)	$ -	$ 300,000	
Upsell (10% of users @$180 per user)		$ 360,000	
Potential value due to proactive monitoring and advanced diagnostics		**$ 1,975,035**	

Based on our model, a large MSP with 50,000 managed Teams users, assuming 1,000 managed desk phones and 500 managed rooms, generating $12 million in Teams managed revenue, could look for $2.7 million in annual operational savings and $1.5 million in potential annual incremental revenue. The bulk of the operational cost savings coming from reduce FTE requirements due to providing support engineers with more advanced tools.

The model below focuses on the costs of an MSP responding to Teams-related incidents with and without proactive monitoring and advanced diagnostics (not MACDs). Churn reduction and upsell potential are based on interviews and research.

MSP with 50,000 managed Team users, $12,000,000 annual revenue and 10% churn

	Without proactive monitoring and advance diagnostic tools	With VantageDX	
Full-time equivalent resources (FTEs) required for incident management	36.9	18.1	51% fewer FTEs
FTE cost	$ 4,981,500	$ 2,443,500	
Microsoft support ticket cost	$ 766,870	$ 613,496	Reduced by 20%
SLA penalties	$ 10,000	$ 7,500	Reduced by 25%
Potential savings due to proactive monitoring and advanced diagnostics		**$ 2,693,874**	
Gross incident support cost per user	$ 115.17	$ 61.29	
Incremental value			
Reduction in churn (%)	$ -	$ 600,000	
Upsell (10% of users @$180 per user)		$ 900,000	
Potential value due to proactive monitoring and advanced diagnostics		**$ 4,193,874**	

While these representative examples are useful, the true power of the model is that allows a specific MSP to tailor the inputs in order to evaluate scenarios that match their current business reality.

Conclusion

Individual results may vary; however, based on our extensive research, and the developed model, managed service providers would be well advised to investigate the implementation of proactive monitoring and advanced diagnostic tools.

In many cases this approach has been seen to reduce operational costs while simultaneously increasing on-going revenue, by increasing upsell opportunity and reducing churn.

Support for this Research

Martello Technologies commissioned EnableUC to develop a model that estimates the monetary impact for managed service providers who deploy Vantage DX proactive monitoring and enhanced diagnostic tools.

Our research and the model development occurred without any influence from Martello and we only shared the results with Martello when completed.

We appreciate Martello's support allowing us to explore the area of proactive monitoring as it relates to managed service providers.

Further Reading

In two previous articles, we explored the benefits of proactive monitoring and advanced diagnostic tools for an individual organization:

- Part 1: Determining the Value of Proactive Monitoring
- Part 2: The Value of Proactive Monitoring

About the Author

Kevin is a globally recognized Unified Communications, Collaboration, AI, and technology thought-leader, strategist, and implementation leader. He was recently honored as the top UC Today UC All-Star.

Kevin is part analyst and part consultant, which ensures he understand both the "big picture" and the real-world realities.

He has led the development of many technology strategies for medium and large organizations and managed the deployment of hundreds of thousands of Microsoft calling and collaboration seats.

A long time ago he created an award-winning game for the Commodore 64 and ever since has been focused on using technology creatively to deliver effective value.