ThousandEyes
part of Cisco

eBook

Digital Experience Monitoring in 2023:

A Practical Guide for Enterprises

Introduction

From the Internet to traditional WANs, the ultimate goal of the network is to ensure seamless connectivity for all users and all locations while facilitating quality digital experiences. To this end, network teams must closely monitor performance and adjust operations where needed, all while ensuring minimal user impact. The ability to do this seamlessly while delivering optimal digital experience is dependent on three crucial factors: people, processes and technology. Moreover, in adjusting these factors for future success, network staff should be guided by insights that provide in-depth measurements that tell a complete story about the user's experience across the entire digital ecosystem.

In this guide, we will provide you with an illustration of why your traditional network operations mindset needs to change to an "evidence and escalate" model, in which NetOps teams work alongside providers to resolve issues. In doing so, we will highlight practical and focused ways for your enterprise to use Digital Experience Monitoring (DEM) to improve productivity and revenue expansion, prepare for outage situations, and prioritize needs for distributed office and hybrid workers in the coming years.

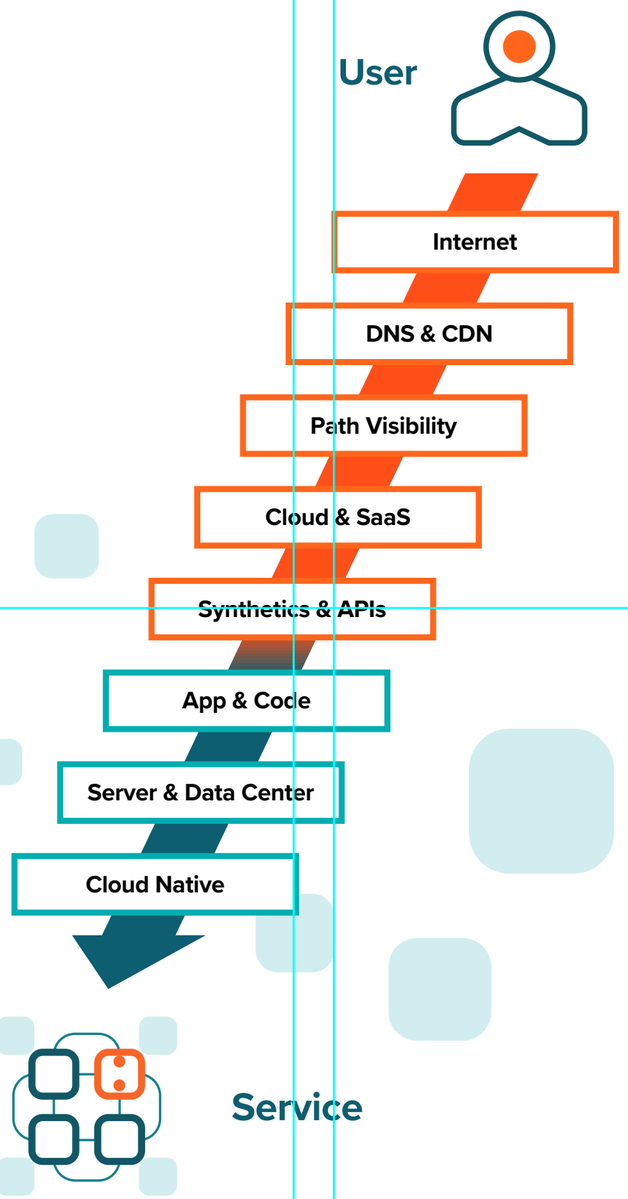
Network Teams' New Business Priority: User Experience

Network teams are moving from a narrow focus on availability and performance to a broader understanding of user experience. The reason for this transition is that networks are changing. In the past, the focus was on connecting users (most of whom were on campus) with centralized services and applications hosted in data centers. Now, there is an increasing emphasis on cloud, SaaS (software as a service), and distributed workforces. As a result, we are in a moment where the network team, to be successful, must work more collaboratively with application developers, IT, and security, as well as with business stakeholders.

Users' demand for performance is paramount in this new reality, and the most efficient way to achieve this is to reduce latency by pushing compute and services closer to them. To do this, IT must bring services near the edge of the network and increasingly outside it altogether, which is where the adoption of SaaS and third-party apps served locally rather than centrally fits in. Managing these shifts for optimal results requires a greater understanding of what users are actually doing—i.e., what they are trying to achieve—rather than just measuring how quickly they complete their transactions.

The transition to prioritizing consistent quality user experiences in any environment has already begun in large enterprises, and the pandemic has only accelerated it. "By 2024, 40% of enterprises will have extended their Digital Experience Monitoring to also include select home workers, up from less than 1% in 2020," according to Gartner.[1] And, with the increasing popularity of hybrid work and SaaS applications delivered over the Internet, it will soon become table stakes for all businesses.

[1] Gartner®, How to Monitor and Troubleshoot Remote Workers' Application Performance, Bjarne Munch, Padraig Byrne, Josh Chessman, Lisa Pierce, March 23, 2021



Dealing With Silos and the Need for a Holistic Perspective

The conversation about silos has drastically changed over the past decade. Breaking down silos between network and application teams can help you facilitate knowledge exchange and teamwork, though there are good reasons some people work better in specialized environments. The trick is balancing those two worlds so that everyone is on board and understands why we are doing what we are doing and who needs to own troubleshooting in which domain. This is easier said than done as networks grow more interdependent, applications more containerized, and business demands for increased profits, productivity, and differentiation over competitors intensifies.

Rather than continue a decades-old debate over breaking down silos, today's organizations need a holistic perspective of the end-to-end service and application delivery chain instead. One that is always in the user's context and enables IT silos to view their journey within an encompassing perspective and in terms they can all relate to and understand. The sharing of contextual data bridges the gap between NetOps and DevOps teams with information that aligns to a common goal and generates shared responsibility and accountability. You can, finally, facilitate contextual communication across silos that encourages cooperation, reduces friction, and results in better user experiences.

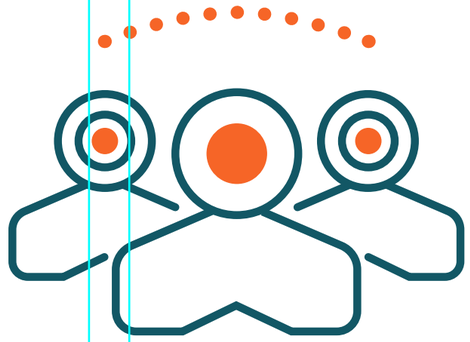
DEM and a Common Operating Language Are Key to Digital Success

To ensure that cross-silo collaboration works, we need a common operating language that can be translated from technical-speak into business-speak so that everyone can understand. Given the breadth, distribution, and different interrelationships of the Internet, networks, cloud platforms, and applications today, the only conceivable approach to finding one is Digital Experience Monitoring (DEM).

DEM focuses on monitoring user experiences to see how they are impacted by service outages or slowdowns, poor application performance, poor connectivity, and the interaction of the application relative to the delivery network. ThousandEyes is unique among DEM solutions in our ability to have a correlated view of the network (including the Internet) and application layers to produce insight into how SaaS applications are performing, and how they differ for each user and location relative to the characteristics and health of the delivery network.

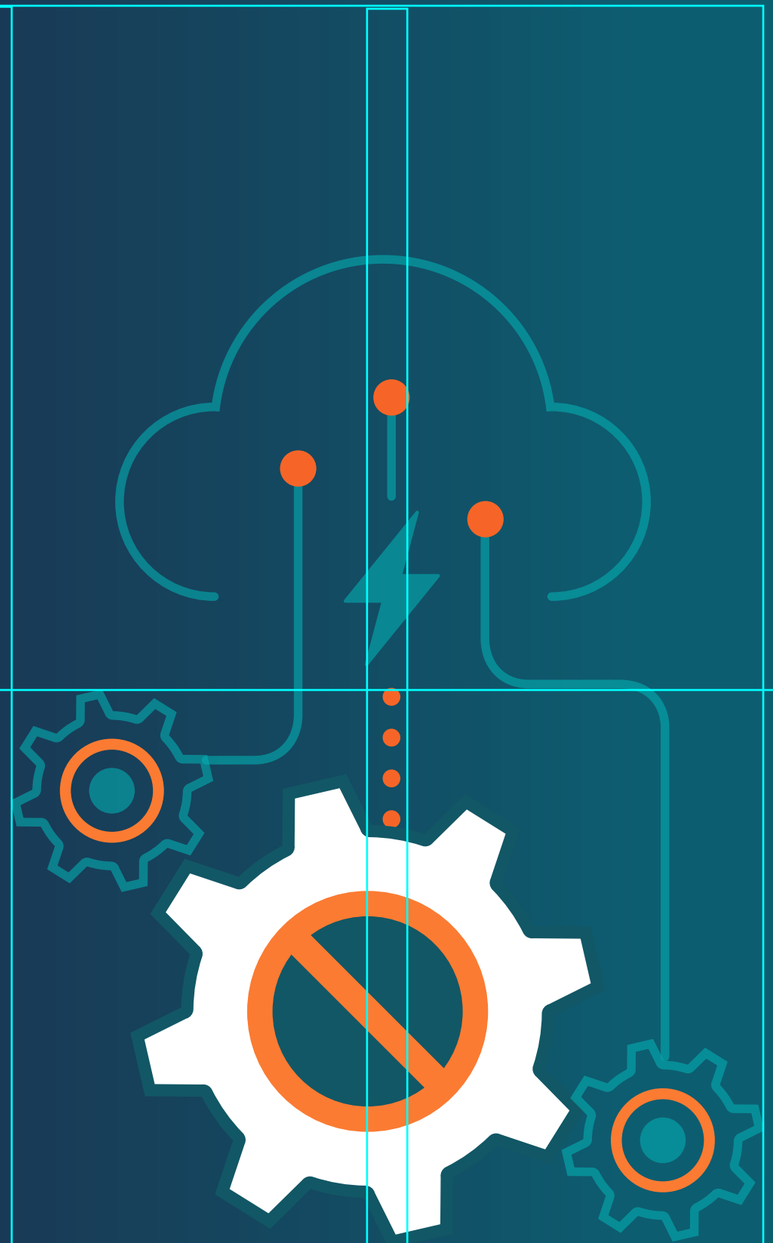
By monitoring user requests and responses across multiple channels and applications, DEM provides a common operating language that all IT teams can use to understand the user experience. A common scenario is the proverbial “finger-pointing” between network and application teams, or between an organization and an external provider when an issue arises. Each referring to their siloed monitoring tools and dashboards, each referring to different metrics, and each speaking a different language. It is obvious that these war-room scenarios waste company resources and valuable time during a user-impacting event.

Teams across silos and organizations must speak a common operating language, and leverage data that correlates application performance with underlying network performance to solve issues and outages quickly and effectively—and without the drama.



Resiliency Planning Is Critical to Outage Avoidance and Recovery

Outages happen. But many in IT still overlook creating realistic operational plans for them. A well-thought-out digital resiliency plan adds strategic value to your organization by helping to reduce or avoid unplanned downtime and limit the damage when incidents do occur. It helps ensure that the right people are involved at the right time during an incident, so they can make effective decisions as they arise. And it can safeguard investments by informing the proper stakeholders and authorities.

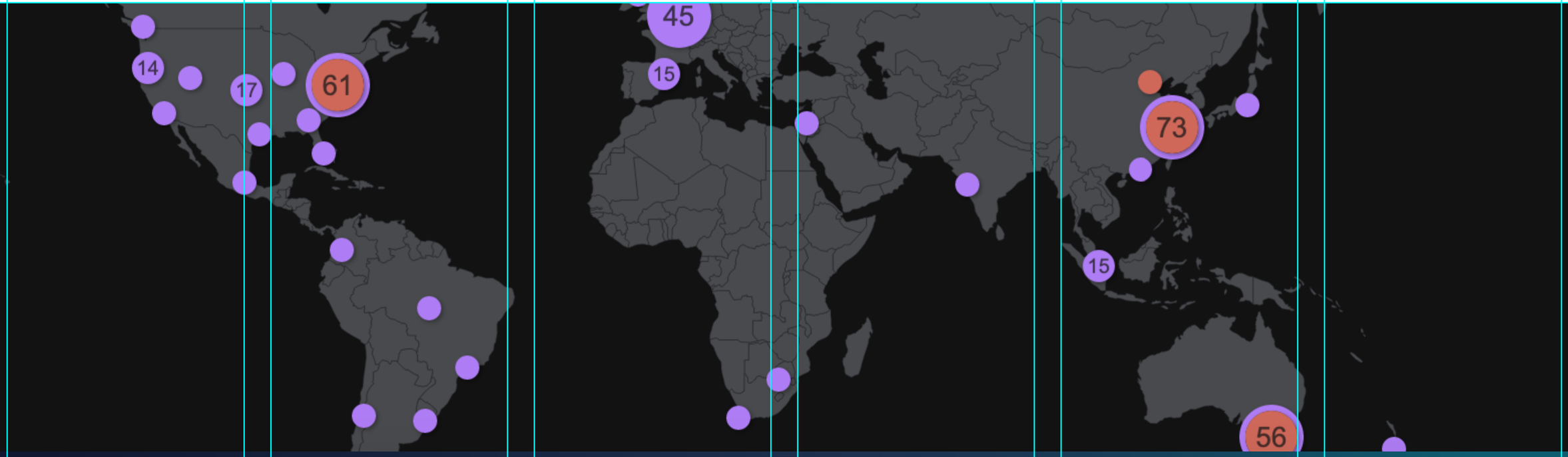


Your outage plan should answer:

- ☑ What dependencies are there? Which ones are critical to my business?
- ☑ Are you certain all dependencies are accounted for? Could there be any unknown unknowns?
- ☑ What is the impact on the business if one of those dependencies goes down?
- ☑ How is this dependency delivered to my environment? How is it delivered to those of my employees or customers?
- ☑ Does my organization have any single point(s) of failure?
- ☑ Is it worth me purchasing mitigation or redundant services?

Once you have completed your view of critical business service dependencies, you are ready for the next step: assessing how likely it is that any of these dependencies will cause an outage and plan accordingly. With ThousandEyes, you can look at historical availability and performance metrics (such as loss, latency, and jitter) to see how often a service has experienced an outage or degradation as a bellwether for its overall reliability. That may even look different for the different geographic regions your business operates in. And the more available data points you have around a given service or network, the more reliable your outage planning will be.

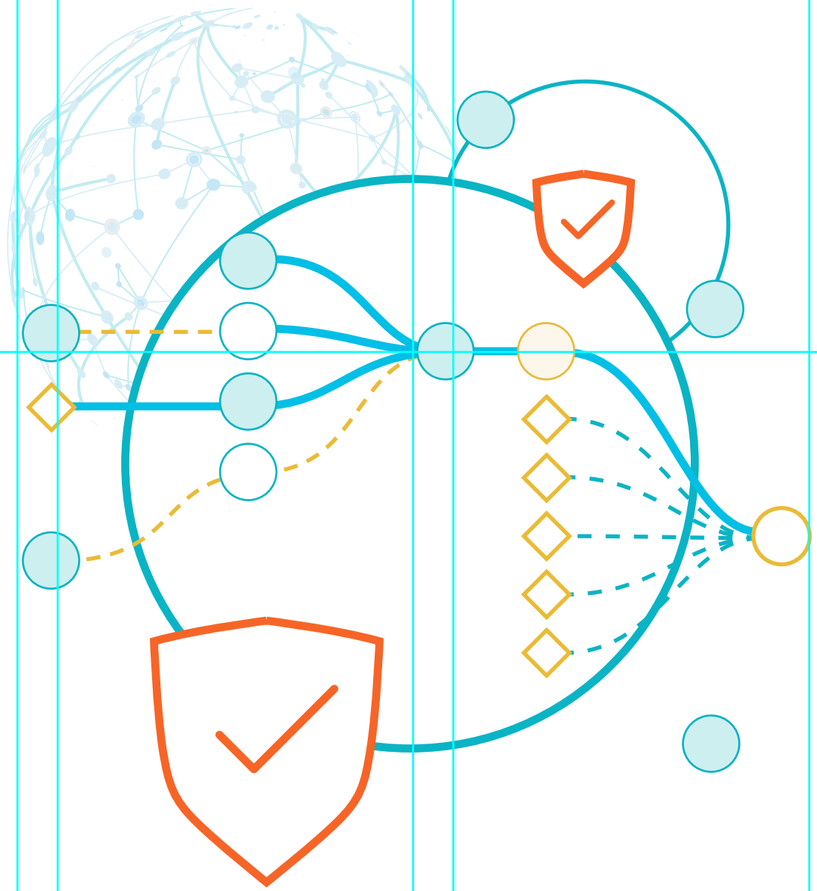
You can also use this data to compare the cost of downtime for different services and make a data-based decision on where to invest first to reduce risk. Remember, when we talk about managing your response to outages, it is important to remember that not all outages are equal. Some are even the result of planned maintenance events. What makes an outage more costly than others is the context (i.e., time of day, day of week, or scope of impact), a company's digital exposure, and ineffective resiliency planning.



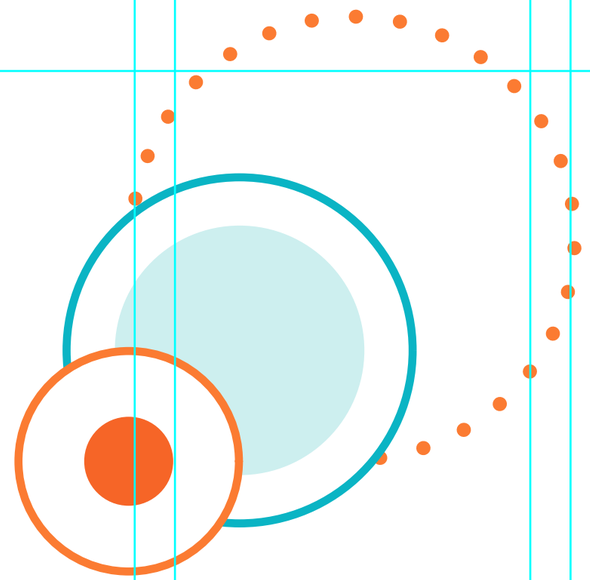
SASE, SSE Performance and Digital Dependencies

User demand for consistent and quality digital experiences has pushed security to the edge to ensure that performance is not impeded unfairly in the face of security requirements. The need for security to traverse the public Internet and third-party environments is the establishing force behind Secure Access Service Edge (SASE) and Security Service Edge (SSE). Their adoption has made Internet-aware and network-agnostic data critical for IT teams to make decisions from a governance point of view. These insights are also required to observe whether all systems are operating optimally and whether any dependencies impact your organization's environment or workers' experience.

Now that workers are everywhere, apps are in the cloud, and the Internet is effectively the new enterprise network, the question for IT managers is: how do you ensure digital experience when you no longer own the underlying transport, services, and applications that your business relies on? Moreover, how do you isolate and resolve issues when so many domains and providers are involved in delivering every digital experience?



Two common ways that organizations monitor their security and performance components are through in-built systems and third-party monitoring.

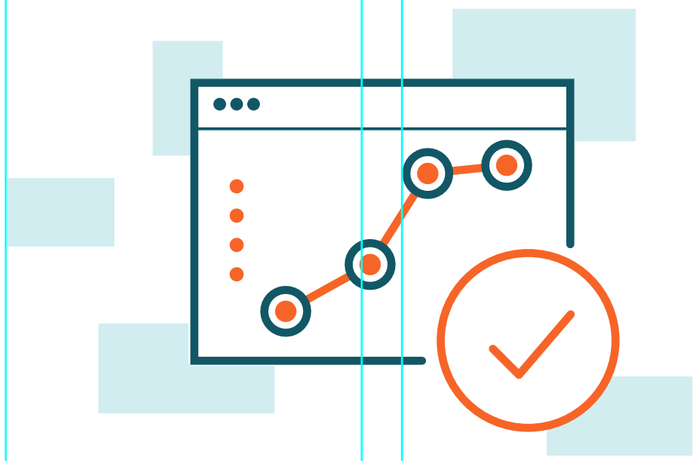


1. In-built systems have traditionally offered "good enough" insights for IT professionals to know how a change will impact their network and how to fix it. Yet, network-centric monitoring cannot provide necessary insight into the complete end-to-end environment for Internet-based ecosystems—which depend on the performance of a complex web of external services, including DNS and CDNs knitted together with BGP at various ISPs. By relying solely on a traditional monitoring approach, you may have gaps or conflicts in your information that prevent you from making the best decision for your organization.

2. Third-party monitoring fills the need for an independent, Internet-aware arbiter crucial in distributed systems like SASE and SSE. That is why DEM is a critical facet of SASE; it offers a view of all aspects, from SD-WAN (software-defined wide-area network) to SaaS to the underlying constellation of providers between them.

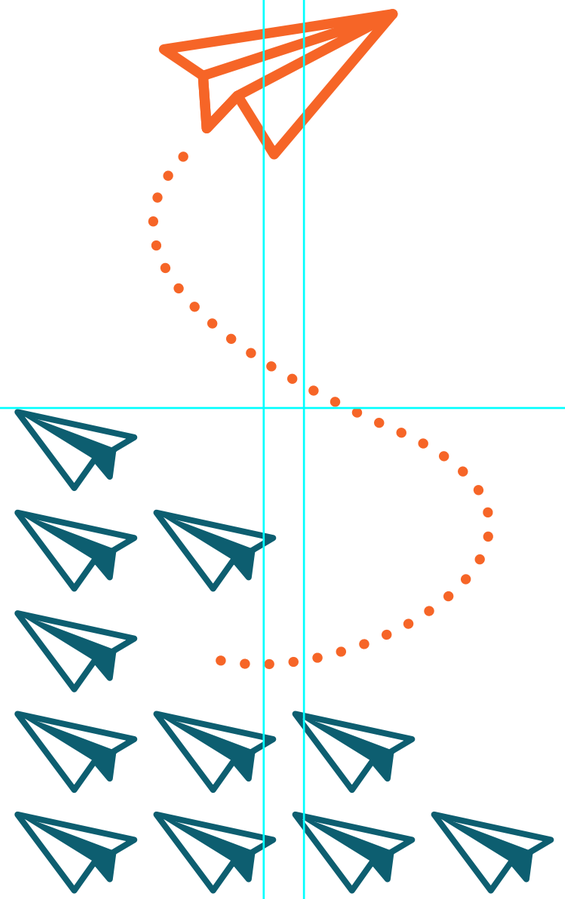
Prioritizing Monitoring Needs in the Era of Hybrid Work

The shift to hybrid work is accelerating as employees return to the office for one or more days each week. As a result, employee productivity and health are top of mind for executives and human resources leaders, who are establishing new roles and processes focused on employee wellness and technology adoption.



A happy workforce is a productive workforce, and enterprises can equip IT and corporate campuses with the right technology to facilitate performance and health equally. For example, IT can proactively extinguish end user frustration using device-layer and application performance monitoring to adjust network capacity and reallocate resources when needed. IT teams can also incorporate wellness stats from Webex to monitor meeting fatigue and technical difficulty for employees working remotely. And in the office, they can support room selection with suggestions based on connectivity insights.

The need to deliver a consistent employee experience extends from the on-campus environment to those at home. Supporting distributed workers presents its own set of challenges for IT because they do not own or control the environment or SaaS applications they depend on, which makes troubleshooting performance issues up to the digital last mile challenging. Pinpointing the cause of an issue can range from a worker's home Wi-Fi to their ISP or even the VPN connection itself. So, IT teams need complete end-to-end visibility from the end user's device, over VPN tunnels, to the apps and services they're accessing to provide the best experiences possible.



All Things Illustrate That Network Operations Needs to Change

Traditional network monitoring was designed to provide unparalleled visibility inside the four walls of your corporate perimeter. But in today's interconnected Internet-dependent enterprise network, it is no longer an adequate approach. With far too many blind spots and fundamentally inaccurate reporting, the information gained from these legacy monitoring tools is incomplete for remediating or optimizing your business today. Moreover, as the network expands beyond the edge, you can no longer rely on an inside-only perspective. It is simply not good enough.

Digital Experience Monitoring provides the insight you need to work across multiple networks, cloud providers, and the Internet. With DEM, you can optimize the user experience and prevent losing business or productivity because of poor experiences. Plus, its benefits to future-proofing your operations and preparing your organization for upcoming innovations cannot be understated.

If you are looking to harness the latest technologies to transform your enterprise, start with Digital Experience Monitoring. For more information, contact us for a demonstration.

REQUEST A DEMO TODAY

ThousandEyes
part of Cisco

www.thousandeyes.com

About ThousandEyes

ThousandEyes delivers visibility into digital experiences delivered over the Internet. The world's largest companies rely on our platform, collective intelligence and smart monitoring agents to get a real-time map of how their customers and employees reach and experience critical apps and services across traditional, SD-WAN, Internet and cloud provider networks.