AimPoint Group
high-impact marketing

WHITE PAPER

SPONSORED BY zscaler™

Delivering Fast and Secure Digital Experiences for the Modern Hybrid Workforce

Introduction

Modern workforce productivity is inextricably intertwined with high-performing technology and top-notch user experiences. Whether they're working from home, the office, or another remote location, today's employees need always-on access to business-critical applications to get their jobs done.

The hybrid revolution is just one way that today's IT ecosystems are transforming. In the past couple of years, organizations across industries have witnessed the many benefits that remote and flexible working models can bring, including higher job satisfaction rates, the ability to right-size real estate costs, and enhanced productivity. They've also increased their reliance on the cloud. Gartner estimates that global public cloud spend will reach $600 billion per year in 2023, as growing numbers of companies take advantage of the agility, flexibility, and power to innovate that comes with cloud adoption.

These changes are a boon for businesses, but they also create new challenges for network operations and service desk teams, who are under ever-greater pressure to deliver fast, secure, and highly reliable access to the applications and resources that employees depend on. As the numbers of remote and office-based workers begin to converge, service desk teams still have to support employees who are coming in to work while establishing new practices to assist those now working from home. In essence, this means the scope of their responsibilities has more than doubled. Before, they were tasked with supporting the users of a single corporate network; now, they're often responsible for thousands—or more—of remote networks (one per work-from-home employee).

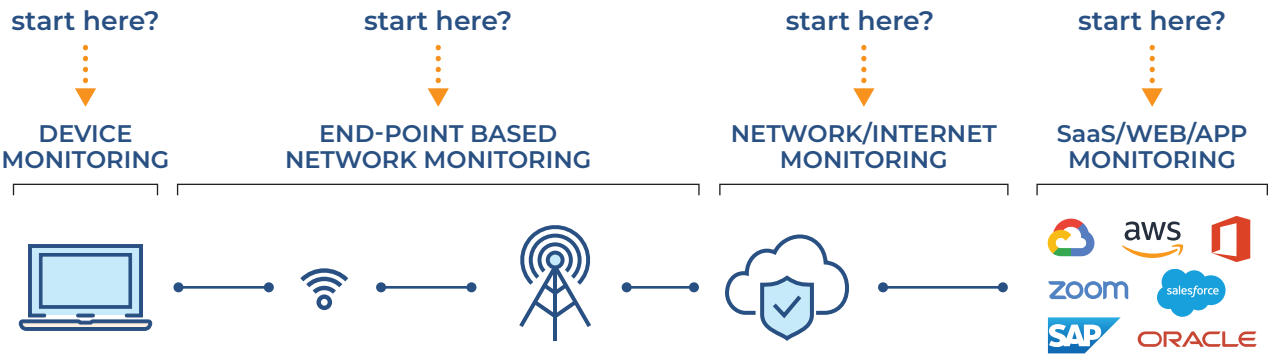
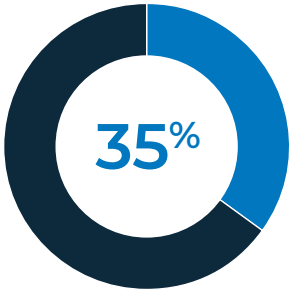


Figure 1: A hybrid workforce makes troubleshooting more complex.

Furthermore, as organizations embrace cloud applications and mobility, the internet has been transformed into the corporate backbone. This makes it far more difficult to monitor the end-to-end path from the end user's perspective. At the same time, users are increasingly dependent upon Software-as-a-Service (SaaS) apps, home WiFi networks, and internet service providers (ISPs)—along with a complex set of routing and networking links that can span the entire globe—to maintain their day-to-day productivity. Many of these systems are invisible to traditional user experience monitoring tools, which have tended to focus on individual devices, networks, or applications in a siloed manner.

This lack of visibility has been exacerbated by the shift to zero trust. As attack surfaces expand with cloud and hybrid work adoption, more and more organizations are adopting solutions like secure web gateways (SWGs), cloud access security brokers (CASBs), and virtual private networks (VPNs), in an effort to keep their environments secure. Zero trust explicitly prohibits granting access to a central, trusted network, which means that network performance monitoring tools also cannot access the network in order to assess its performance. As a result, the balancing act that's needed to keep environments secure while providing fast, reliable application access is becoming more and more difficult.

These circumstances have contributed to the growing cost and complexity of resolving tickets and diagnosing issues that impact end users. In the past two years, the volume of support tickets has increased by 35%, while the cost of servicing each of these tickets has grown by 30%. Additionally, the time it takes service desk teams to handle each ticket has grown from an average of 7.37 minutes to nearly 10 minutes—an increase of 30%.



In the past two years, the volume of support tickets has increased by 35%.

REINVENTING DIGITAL EXPERIENCE MONITORING

What's needed is a new approach to digital experience monitoring, one that leverages technology that can monitor the health of *all* the systems between end users and the applications they're accessing. This requires combined visibility into end user device issues, regional and home WiFi networks, ISPs, and target applications—all in one place that's easy for IT and service desk teams to monitor.

What's needed is a new approach to digital experience monitoring, one that leverages technology that can monitor the health of *all* the systems between end users and the applications they're accessing.

Truly effective monitoring that's supported by end-to-end visibility will make it possible to resolve issues quickly and proactively, before they ever get the chance to impact user experience. This gives employees the excellent user experiences that lie at the heart of successful work-from-anywhere initiatives, as well as secure cloud transformation. Not only are such user experiences essential for productivity, but they also prevent users from feeling tempted to bypass security controls and introduce additional risk.

As organizations begin building out their longer-term security and productivity strategies, it will be particularly important to pay close attention to tool consolidation. Not only can this reduce costs, but it enables teams tasked with troubleshooting to accomplish far more, and to do it all within a single pane-of-glass dashboard. When L1 or L2 service desk analysts can resolve more issues more quickly, there are fewer demands on specialists whose labor hours are more expensive, and better invested in higher-value projects within their core areas.

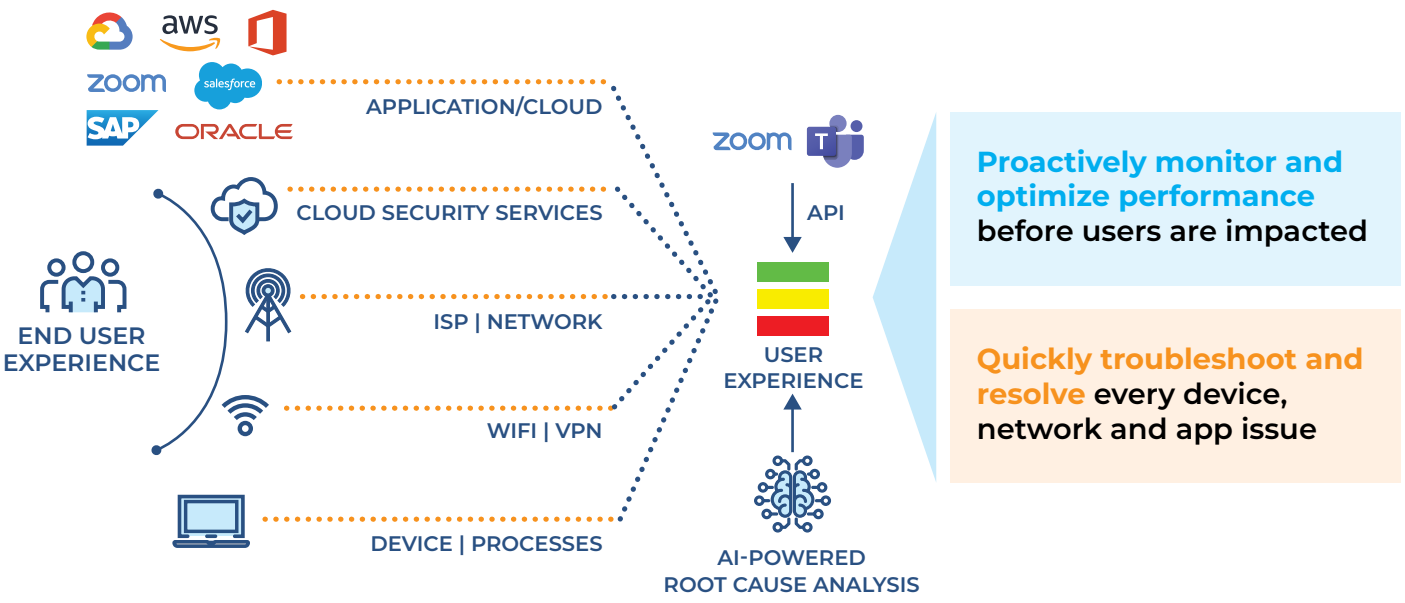


Figure 2: Unified monitoring and analysis.

Prior to the widespread adoption of hybrid work and organizations' cloud transformation, the scope of the responsibilities of network, operations, and service desk teams was relatively narrow.

	Before	After
Responsibility	Ensure excellent end user experiences while keeping users, workloads, devices, and networks secure	Ensure excellent end user experiences while keeping users, workloads, devices, and networks secure
Monitoring needs	• Corporate network • Corporate-owned devices, when connected to corporate network • Private applications running in the corporate data center	• Corporate network • Corporate-owned devices • Employee-owned devices • Thousands of home WiFi networks • ISPs • Complex network paths traversing multiple internet and backbone providers' infrastructure • Private applications running in the corporate data center • SaaS apps
Security	Castle-and-moat architectures made it so that most monitoring could be accomplished within a "trusted" network zone	Zero trust security models restrict access to a central trusted network—including by network performance monitoring tools
Need	Static visibility into network-connected devices and connectivity to the corporate data center	Continuous, dynamic, end-to-end visibility that can monitor and measure every aspect of every user's digital experience

Reducing Business Risk and Improving Employee Productivity in a Hybrid World

In the past, many organizations relied on multiple point monitoring tools that were managed by different IT teams. These tools didn't share data or context, leaving key information isolated within silos and resulting in fragmented visibility into end user experience. Monitoring tools designed for use in the data center generally cannot detect, troubleshoot, or diagnose performance issues across the internet. Conversely, application performance monitoring (APM) solutions built for SaaS environments are typically unable to provide visibility into issues within the corporate perimeter—or users' home WiFi networks.

Digital experience monitoring for the modern workforce requires a new and dynamic approach. IT teams need continuous, end-to-end visibility so that they can monitor and measure every aspect of every user's digital experience, regardless of their location or which resources they are accessing. In addition, security, network, application, and help desk teams need access to continuous monitoring capabilities that will empower them to collaborate, so that organizations can maintain robust security without compromising on user experience.

IT teams need continuous, end-to-end visibility so that they can monitor and measure every aspect of every user's digital experience, regardless of their location or which resources they are accessing.

TURN THE LIGHTS ON

Traditional network and device performance monitoring solutions are simply unable to deliver the end-to-end visibility that's needed to troubleshoot end-user performance issues across today's cloud-centric IT ecosystems that are leveraged by a geographically distributed workforce. Service desk and IT teams must be able to see what's impacting user experience even though the widespread adoption of zero trust security has made this more difficult. To achieve these ends, they'll have to monitor:

- End user device health (no matter where those devices are located)
- Home WiFi routers
- Local ISPs
- Regional, corporate, and vendor networks
- SaaS application availability and performance
- Audio, video, and content-sharing performance within videoconferencing and unified communications services
- Private application availability and performance

And the visibility that IT teams need should be granular. It should extend across all of the following three areas:

- **End user device health.** Monitoring this requires collecting detailed metrics on the device's configuration, how it's utilizing its CPU, memory, and storage, and which processes are running on it. IT teams should also be able to see if any anomalous or noteworthy events have occurred on the device.
- **Network insights.** To understand if a user's experience of latency is being caused by their device, network, ISP, or application, support teams need access to a hop-by-hop view of what's taking place across the network. They should be able to see whether packet loss is taking place or latency is occurring on any individual network segment.
- **Application monitoring.** Keeping track of application performance and service degradations requires monitoring page fetch and DNS times. This should be analyzed continuously for both private apps running in your data center or private cloud as well as for SaaS apps.

It's important to gather detailed insights about every network hop that's taken between the user device and the application. These insights should be expressed in concrete, quantitative terms. This means generating digital experience scores or other metrics that allow teams to assess the current state of end user experience and understand how it is evolving over time.

It's important to gather detailed insights about every network hop that's taken between the user device and the application.

STREAMLINE TROUBLESHOOTING, BOOST IT TEAMS' PRODUCTIVITY

When IT and service desk teams gain access to insights that enable them to quickly find and fix the root causes of network latency, user device issues, or application performance problems, they can reduce their mean time to detection (MTTD) and mean time to resolution (MTTR) while expending less effort and fewer labor hours on each ticket.

Today's application delivery chains are more complex than they've ever been in the past. IT teams must troubleshoot across a myriad of different device types, traffic paths that traverse hundreds of interconnected networks, and applications comprised of numerous loosely coupled services. This degree of complexity makes it almost impossible for support staff to analyze and identify root causes of issues within a reasonable timeframe, let alone fix them at speed. A digital experience monitoring solution that incorporates artificial intelligence (AI) and machine learning (ML) can gather, correlate, and analyze large datasets quickly, so that it can identify root causes rapidly to enable a fast IT response.

A digital experience monitoring solution that incorporates artificial intelligence (AI) and machine learning (ML) can gather, correlate, and analyze large datasets quickly.

Plus, if IT teams take advantage of a solution that consolidates security, network, and end user device monitoring capabilities in one place, they'll be able to reduce tool sprawl and the alert fatigue that often accompanies it. This all-in-one approach also leaves more room in the budget, especially if the solution's costs are shared across multiple functions or departments. Such streamlining can also reduce alert fatigue while making it possible for lean teams or less-senior support personnel to quickly and accurately triage issues. Not only does this approach simplify monitoring, but it can also deliver more complete and comprehensive capabilities than were available in yesterday's stacks of disparate point solutions.

Streamlining can also reduce alert fatigue while making it possible for lean teams or less-senior support personnel to quickly and accurately triage issues.

How the Shift to Hybrid Work Is Making Troubleshooting More Complicated

To secure networks used by large numbers of hybrid and remote workers, organizations must replace legacy castle-and-moat security architectures with more modern approaches such as a cloud-native secure service edge (SSE) that can connect users, workloads, and devices without putting them on a corporate network. Making this shift is key if they're to deploy applications securely.

However, the challenge doesn't end there. As organizations deploy more zero trust solutions—such as secure web gateways (SWGs), cloud access security brokers (CASBs), and data loss prevention (DLP) to keep their environments secure, the complex balancing act between maintaining robust security and providing fast, reliable application access becomes more difficult.

In cases where end users connect directly to SaaS apps
Traffic is not secured, leaving users vulnerable to attacks. Plus, network teams don't own the connectivity between the end user's device and the SaaS app, making troubleshooting difficult.

In cases where traffic is forwarded to a security solution for inspection prior to SaaS app connectivity
Network teams must rely on multiple, disparate tools to gain insights into end user devices and traffic. The lack of end-to-end visibility forces teams into reactive troubleshooting mode because they don't have the capabilities they need to proactivity identify and fix issues.

In cases where SaaS and private applications are secured
In addition to forwarding SaaS traffic to a security solution for inspection (as above), an additional route is added for private apps hosted on-premises or in the public cloud. This adds complexity, since network operations teams must diagnose several fragmented networks to piece together an end user's traffic to an application. It's time consuming, creates cumbersome processes, and requires expertise in correlating data across multiple monitoring solutions. Often, the end result is the existence of major blind spots, especially when traffic is encrypted.

Digital Experience Monitoring for the Modern Hybrid Workplace

As hybrid working models are adopted by growing numbers of organizations across industries and around the world, what's being asked of help desk, IT support, and network teams is changing dramatically. A modern digital experience monitoring solution can not only help them keep up, but can empower teams to get ahead of end user-impacting issues before they cause noticeable problems.

Here's how this technology can help:

A modern digital experience monitoring solution can empower teams to get ahead of end user-impacting issues before they cause noticeable problems.

USE CASE #1: DETECTING APPLICATION PERFORMANCE ISSUES CAUSED BY PROBLEMS WITH AN EMPLOYEE'S HOME WIFI NETWORK.

In the past, user support teams would often recommend that end users reboot their computers if they reported slow application performance. However, this won't fix the problem—wasting time and creating frustration—if the device isn't the root cause of the issue.

With a modern DEM solution, network operations and service desk teams can quickly pinpoint the causes of issues, even when users aren't on the corporate network. Advanced solutions can analyze telemetry data to identify potential issues within a particular timeframe, identifying which network hop is responsible for the latency. Such solutions can also identify the WiFi bandwidth that the user is connected to, as well as the signal strength over time. If the employee's teenage children are home for the day, playing games online, this could be causing the problem.

USE CASE #2: DETERMINING WHEN CONNECTIVITY FAILURES ARE CAUSED BY AN ISP OUTAGE.

ISP issues such as blackouts, brownouts, and increased latency can degrade end user experience or prevent employees from connecting to business-critical applications. The hop-by-hop path that an individual user's traffic takes from their device to the target application can be complex. Traditional network performance monitoring solutions couldn't see these issues, but a modern digital performance monitoring solution can.

An industry-leading digital experience monitoring platform can incorporate ISP insights gathered from end user telemetry (Web Probe and Cloud Path metrics) from millions of devices around the globe to detect internet outages and assess their extent and severity. It will also be able to compare the latency and packet loss between the hops that the user's traffic is taking with known ISP outages.

USE CASE#3: IDENTIFYING SERVICE DEGRADATIONS AND OUTAGES IN SAAS APPS.

Despite the complexity of the networking infrastructures that comprise the global internet, sometimes the problem is with the SaaS app that the end user is trying to access. A digital experience monitoring solution that tracks service issues around the world can quickly and reliably identify application performance problems that impact worldwide user bases. This way, IT teams can have immediate confidence that they've determined the root cause of an issue, and any tickets opened would already have resolution.

Essential Digital Experience Monitoring Capabilities for Tomorrow's Network, Operations, and Service Desk Teams

What if you no longer had to choose between security and visibility? What if you had access to dynamic, end-to-end monitoring capabilities that let you understand network and infrastructure performance from the end user's point of view?

Here are some key questions to ask yourself if you're part of a network team that's tasked with supporting a global workforce:

Key question:	Your digital experience monitoring solution should enable you to:
How quickly can I isolate regional or global network issues? If my network is experiencing high latency and packet loss, can I rapidly identify why it's happening?	Select regional groups of users to see if you can isolate network issues to a particular region or geographical location.
Can I get a hop-by-hop network view for an individual user?	Check for latency and packet loss between all network devices from the end user to the application.
Can I identify issues when GRE tunnels might be masking their root cause?	Capture end-to-end traffic from the end user's device to the private application. This will provide the insights necessary for troubleshooting.
Can I monitor private applications and traffic traveling over secured networks that are not exposed to the public internet?	Obtain continuous, dynamic, end-to-end visibility that can monitor and measure every aspect of every user's digital experience
How quickly can I identify issues when end users rely on multiple ISPs all around the world?	Check network latency and packet loss between all the hops that egress your network. Also, review status pages from individual ISPs to see whether they're reporting an outage.

A Word from Our Sponsor

HOW ZSCALER DIGITAL EXPERIENCE (ZDX) HELPS NETWORK OPERATIONS AND SERVICE DESK TEAMS MEET TODAY'S DEMANDING REQUIREMENTS

Zscaler Digital Experience (ZDX) makes it possible to provide exceptional user experiences to employees, regardless of whether they're working from home, the office, or another location. Part of the Zscaler Zero Trust Exchange, ZDX is driven by a comprehensive platform approach that empowers IT teams to monitor users and devices, connecting to any app, from anywhere in the world—all from within a single, easy-to-use, pane-of-glass dashboard. ZDX includes granular endpoint monitoring capabilities that enable user support and network teams to track device health, home WiFi signal strength, and network bandwidth for every end user. It also features active monitoring of application availability and uptime, including critical performance metrics like page fetch time and server response time. ZDX can report proxy-aware insights on every network hop taken between the user's device and the application, and it can combine all of these performance measures into an aggregated Zscaler Digital Experience Score that gives teams deep insights into the current state of end-user experience so that they can make smarter decisions.

Zscaler Digital Experience (ZDX) makes it possible to provide exceptional user experiences to employees, regardless of whether they're working from home, the office, or another location.

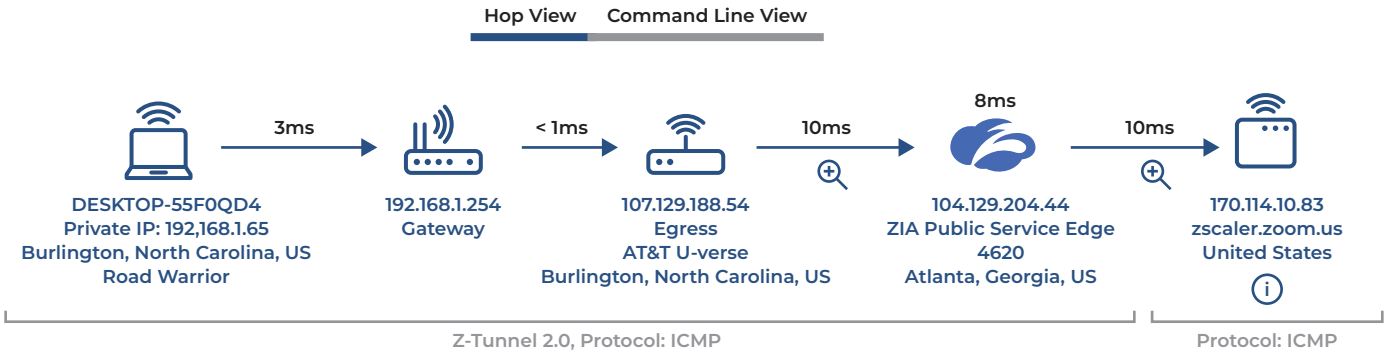


Figure 3: ZDX showing granular end-to-end performance data.

ZDX comes with unique benefits that no other digital performance monitoring solution can offer, including a rich ecosystem of API integrations with popular ITSM tools like ServiceNow to make it easy to share insights across teams and initiate remediation workflows. Zscaler also has built special partnerships with vendors like Zoom and Microsoft to optimize the performance of popular videoconferencing and collaboration software. Combined, these capabilities give Zscaler customers granular and uninterrupted visibility into the user-to-app experience. It's a solid foundation for enhanced productivity—one that's designed for the way we work today.