ThousandEyes

Thrive in a Connected World™

eBook

There’s a Cloud-Sized Hole in Your Monitoring Stack

Digital Experience Monitoring for Your Cloud Ecosystem

The Great Cloud Migration

Every business is now a digital business and user experience is the currency of success in a digitized world. Organizations are digitally transforming customer interactions, business processes and employee collaboration. Digital transformation typically takes the form of highly visible and cost-intensive initiatives that range from modernizing the workplace by heavily engaging in SaaS, to adopting SD-WAN architectures for optimizing operating cost and performance, to placing bets on IaaS providers to host applications. Frequently grouped under the “Cloud First” umbrella, these strategic initiatives are meant to drive faster time to market, increase agility and deliver superior user experience for both customers and employees. However, these shifts come with their fair share of technical and operational risks. In the world of the cloud, as IT business leaders are ultimately responsible for delivering superior digital experiences, how do you balance the risk-to-reward ratio?

The Cloud Ecosystem—A Deluge of Dependencies

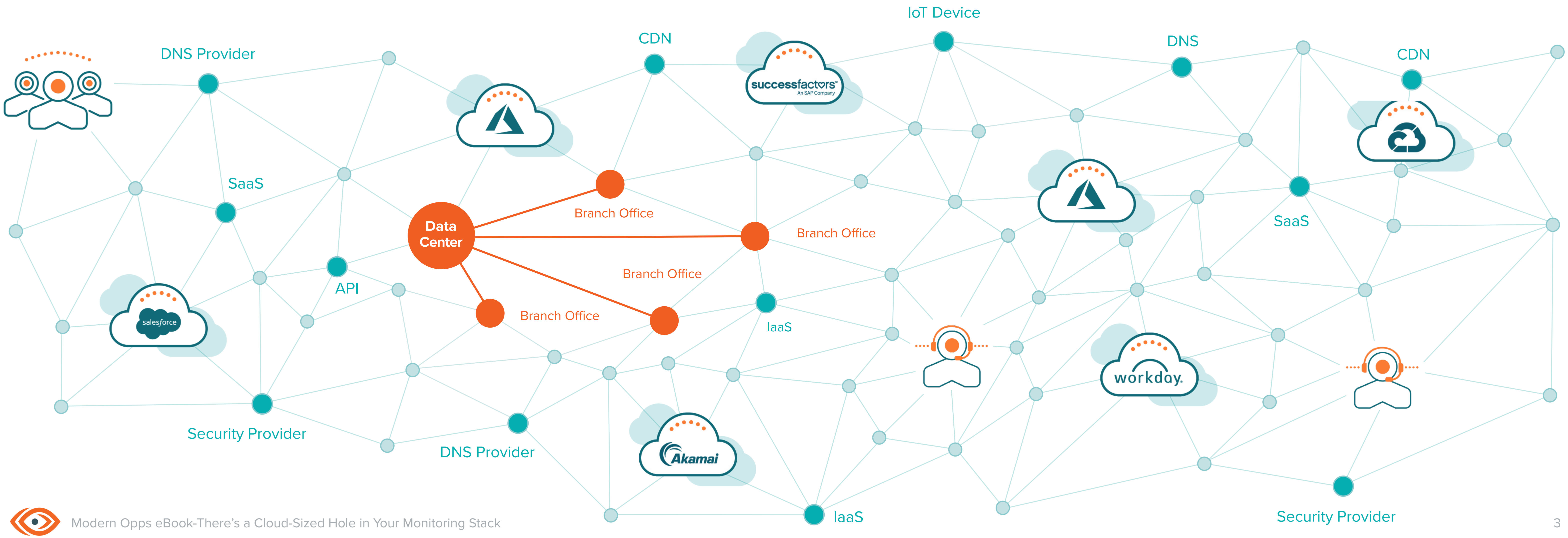
The "cloud" is collective and interdependent in its composition. Digital experiences riding on "Cloud First" initiatives are increasingly built and delivered via a complex, interconnected ecosystem of software, services, infrastructure, networks, and service providers that are external and Internet-based. The importance of this external ecosystem to deliver digital experience manifests in a massive shift of IT spend from traditional data center infrastructure and on-premises applications to IaaS environments and SaaS applications.

Applications are no longer monolithically hosted in on-premise data centers, but micro-serviced and shipped to the cloud, public and private alike. The pursuit of best-of-breed options steers enterprises on a multi-cloud journey, where services extend across many cloud providers. Web service APIs, the stuff that distributed modern applications are made of, are proliferating and becoming the forefront of digital experiences.

Establishing a customer-facing presence means unconstrained 24/7 availability across the globe with no compromise on speed. Enterprises striving to attain those attributes heavily rely on Content Delivery Networks (CDNs), to cache and distribute content. The reliance on the hierarchical Domain Name System (DNS), yet another dependency for digital presence, is often taken lightly and most times even forgotten, until a large-scale outage like a DDoS on Dyn brings it to the limelight.

Delivering a digital service or accessing a SaaS application is also highly reliant on the underlying infrastructure that connects the service to its users, aka the Internet. The Internet is unlike centrally controlled and slow-changing traditional infrastructures. Made up of hundreds of Internet Service Providers (ISPs), it is more like a living organism that is continuously and rapidly evolving in response to a variety of stimuli.

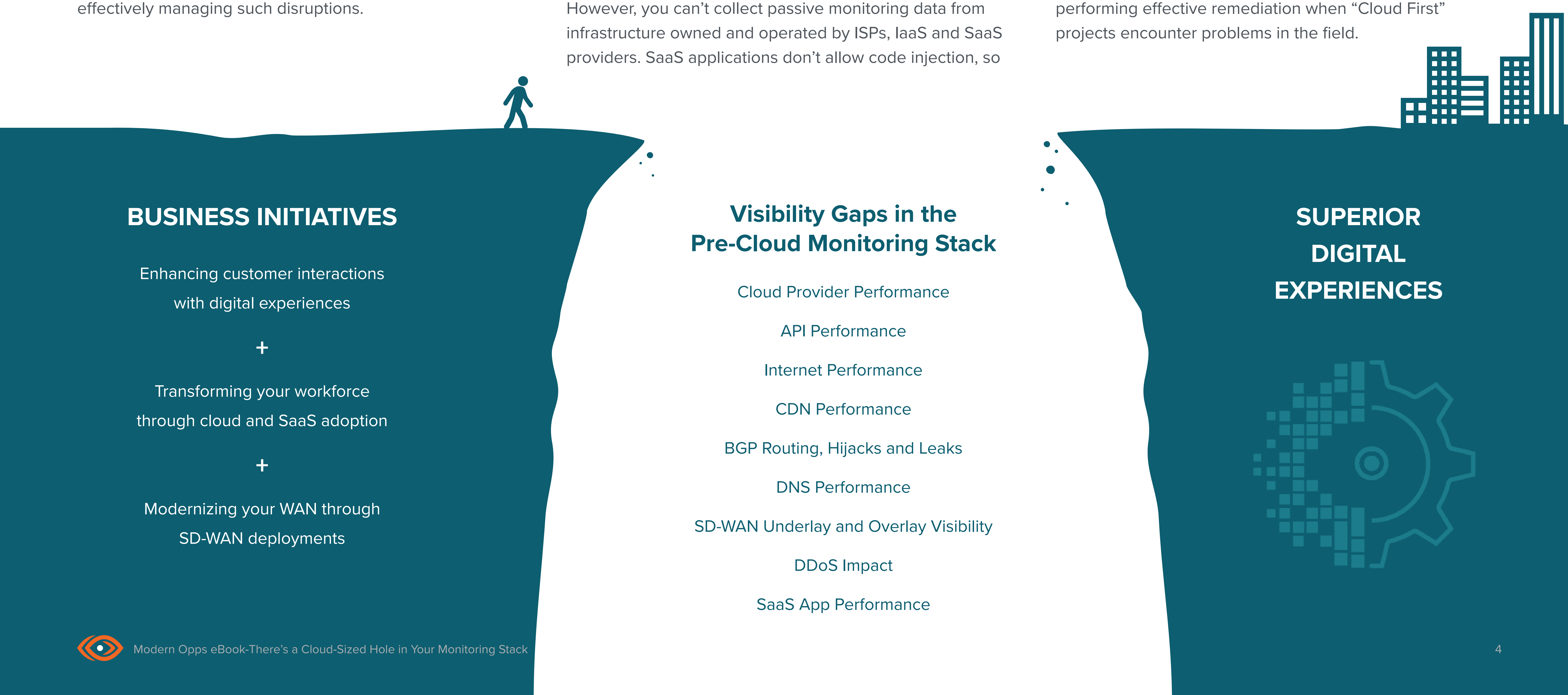
Enterprise IT teams are tasked with delivering optimal digital experiences but the building blocks of that delivery chain are not directly owned by them, resulting in an inverse relationship between control and accountability in the cloud.



The Cloud Fractures Visibility

With business-critical digital experiences dependent on so many external factors, any disruption in that interconnected web of dependencies has a ripple effect and the potential to disrupt service. Unfortunately, the nature of the cloud ecosystem compounded by an inherent lack of ownership engenders a visibility gap that handicaps IT teams from effectively managing such disruptions.

Most large IT organizations already possess a portfolio of network and application monitoring. However, these tools are typically built for pre-cloud scenarios. Traditional IT monitoring stacks rely on passive data collection from network infrastructure devices such as switches and routers, via SNMP, packet capture, sFlow and NetFlow. However, you can't collect passive monitoring data from infrastructure owned and operated by ISPs, IaaS and SaaS providers. SaaS applications don't allow code injection, so many application performance management techniques, such as Real User Monitoring (RUM), aren't applicable. Not only does the ill-suitedness of traditional monitoring to cloud scenarios prevent project teams from proactively baselining performance to check upfront assumptions, but the lack of actionable data also hinders you from performing effective remediation when "Cloud First" projects encounter problems in the field.



BUSINESS INITIATIVES

Enhancing customer interactions with digital experiences

+

Transforming your workforce through cloud and SaaS adoption

+

Modernizing your WAN through SD-WAN deployments

Visibility Gaps in the Pre-Cloud Monitoring Stack

Cloud Provider Performance

API Performance

Internet Performance

CDN Performance

BGP Routing, Hijacks and Leaks

DNS Performance

SD-WAN Underlay and Overlay Visibility

DDoS Impact

SaaS App Performance

SUPERIOR DIGITAL EXPERIENCES

The Perils of Lost Visibility

Often, enterprises only become aware of the risks associated with lack of cloud visibility when they are well into their cloud journey. Yet there are significant operational and security areas where risks emerge and can turn into business impacts unless IT teams have sufficient visibility to counter them.

ITOps Process Risks

When you directly own and operate IT assets, the troubleshooting domain that ITOps teams have to work with is relatively contained and, once a root cause is determined, someone on the team can fix it. That “find and fix” process doesn’t work so cleanly in the cloud. The troubleshooting domain expands to include potentially thousands of Internet networks and multiple cloud and service providers, so just tracking the source of the problem to a particular network or provider is exponentially harder. Furthermore, once you identify a root cause, you have to have enough evidence to get your service provider to accept an escalation process from your team and fix the problem for you. If you’re not ready for this reality, then your Mean Time to Resolution (MTTR) for cloud issues may rise uncontrollably, and your service desk costs may explode due to unclosed trouble tickets.

Security Risks

While the Internet might seem like a harmless conduit for digital experience delivery, the reality is that it is an interconnected web of over 60,000 Autonomous Systems communicating over a trust-based protocol called Border Gateway Protocol (BGP) and is extremely vulnerable at its very core. As a publicly shared network, delivery is best effort. Moreover, since the Internet has no centralized governance, its proper functioning rests on implied trust, which can be easily broken. For instance, an innocent BGP routing misconfiguration halfway around the world could steer all your business traffic to a completely mistaken destination, like the Google Route Leak. Alternatively, hackers with malicious intent could abuse both DNS and BGP to hijack your IP address domain and steal both data and money, like the cryptocurrency heist in 2018. Add 400,000 recorded DDoS attacks per month and growing, the potential for your service to be disrupted by any one of these attacks becomes a probability game.

Business Impact

Ultimately, digital experience is all about providing uninterrupted and supersonic access to services to customers and employees. The average cost of a single enterprise service outage in the United States is estimated to be roughly $400,000. Furthermore, any disruption in that service line may not only impact revenue but also the brand and other key aspects of the business.

Business Impact of Insufficient Cloud Visibility

- Costly and prolonged outages and failures
- Wasted IT resources
- Loss of innovation with top technical talent consumed by troubleshooting
- Lost employee productivity
- Lost revenue and higher customer churn
- Brand and reputation impact, lower NPS
- Strained and ineffective vendor relationships
- Loss of provider accountability and SLA enforcement
- Costly rollbacks of failed cloud and WAN migration projects

Evolving the Modern IT Monitoring Stack

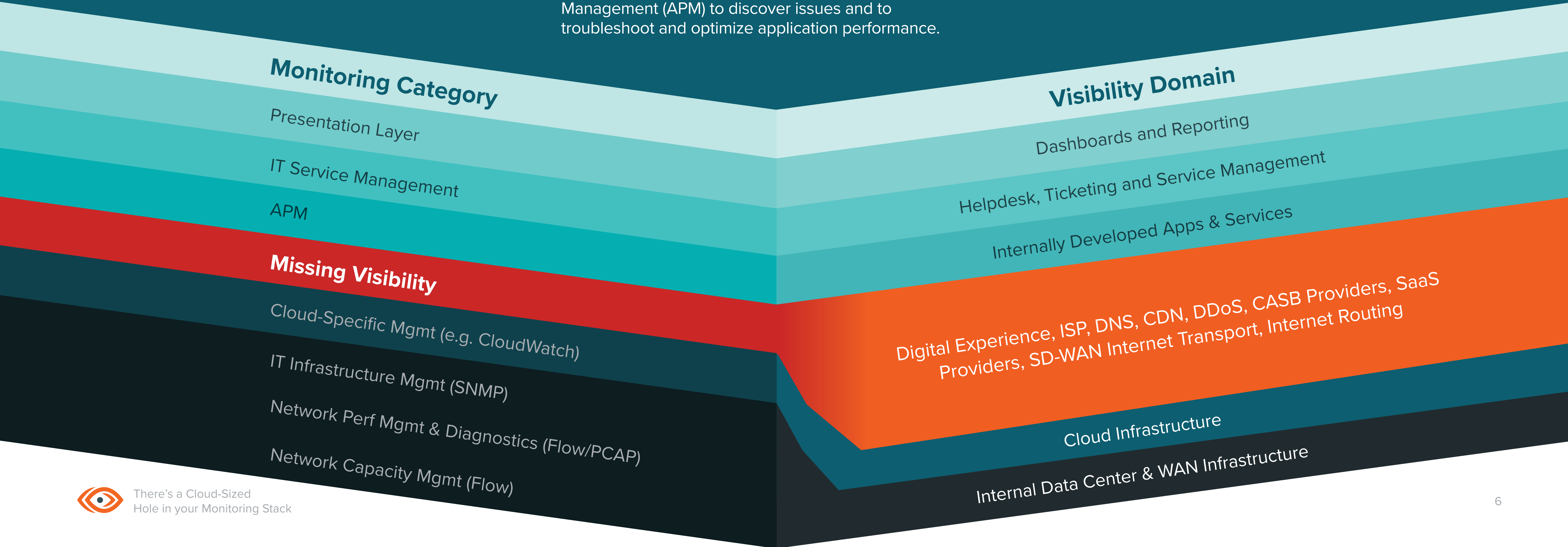
Establishing cloud visibility requires taking a holistic approach on two fronts—refabricating the IT monitoring stack to gain visibility beyond traditional enterprise domains and restructuring IT operations processes to take you through cloud migrations successfully. Redesigning the visibility framework is not so much about replacing conventional monitoring techniques, but refactoring your investments to address the significant new challenges and risks in the cloud so that you can effectively capitalize on all the cloud has to offer your organization both technically and from a business agility perspective. Shifting ITOps processes to be proactive, facilitating ITOps teams to adopt an "evidence and escalate" model and creating a methodology that is transparent within and beyond your organization is critical for delivering superior digital experiences.

Cloud-specific monitoring tools are an important addition in the new monitoring stack. Cloud vendors cater to this by providing access to flow logs and packet analysis, plus visibility into resource utilization and operational health of your cloud services. While native cloud monitoring tools help bridge the gap created by the new ecosystem, they do not address external factors that impact cloud performance. Recent research by EMA reveals that 92% of operations teams continue to face monitoring challenges when relying only on cloud-native monitoring tools.

Monitoring the performance of cloud-based architectures with native cloud monitoring is only one piece of the puzzle, as digital experience is also beholden to application performance. Enterprise DevOps teams have historically relied on Application Performance Management (APM) to discover issues and to troubleshoot and optimize application performance.

However, as applications become increasingly atomized and distributed, a greater proportion of applications are composed of third-party API services that aren't under your control, and your reliance on the Internet becomes increasingly mission-critical. This is where traditional APM tools fall short, particularly in their ability to provide insight into digital experience factors that fall outside of your management domain.

Effective digital experience delivery requires a whole new category of monitoring that focuses on the end-to-end cloud ecosystem, Internet and external provider dependencies. With the Internet becoming a core component of the delivery infrastructure in cloud environments, this means monitoring specific to critical Internet services like BGP routing, CDNs and DNS is essential, along with ways to gain insight into all the dependencies across ISP and cloud provider networks that carry digital experience traffic.



Monitoring Category

Presentation Layer

IT Service Management

APM

Missing Visibility

Cloud-Specific Mgmt (e.g. CloudWatch)

IT Infrastructure Mgmt (SNMP)

Network Perf Mgmt & Diagnostics (Flow/PCAP)

Network Capacity Mgmt (Flow)

Visibility Domain

Dashboards and Reporting

Helpdesk, Ticketing and Service Management

Internally Developed Apps & Services

Digital Experience, ISP, DNS, CDN, DDoS, CASB Providers, SaaS Providers, SD-WAN Internet Transport, Internet Routing

Cloud Infrastructure

Internal Data Center & WAN Infrastructure

Complementing APM and Cloud Monitoring with ThousandEyes

ThousandEyes Digital Experience Intelligence platform modernizes performance monitoring for cloud-based architectures by delivering unprecedented visibility into networks and infrastructure you don’t own, as well as the ones you do. This means that the Internet, cloud provider networks, the extended eco-system and user-level performance (regardless of location) are all visible, so you can manage every network like it’s your own.

ThousandEyes complements your APM tools and enables you to see real-time application, service, and network performance from external vantage points around the world. ThousandEyes fills the visibility gaps left by APM in your application and user experience by providing deep insights into the availability and performance of all of your external dependencies, as well as simulating the experience of your users.

By leveraging both within your stack, you can:

Gain real-time visibility and application performance insights

Pinpoint issues across your entire data center environment, VPCs and full application stack

Consolidate your monitoring tools to speed understanding of critical issues

See end to end across both all your applications and the implications of network performance to user experience

Identify and fix issues before your customers are impacted

Improve your user experience at every level

Whether or not your organization leverages APM solutions for internally owned applications, ThousandEyes can provide the deep insight your IT teams need to understand how your cloud external factors impact application health and user experience.

Don’t Let Digital Experience Fall Into the Cloud Black Hole

ThousandEyes’ fleet of smart, software-based monitoring agents located in over 180 global cities provides app and network visibility into your cloud-hosted services from a customer and market perspective. These Cloud Agents are available in over 74 regions of AWS, Azure, GCP and Alibaba cloud and offer rich visibility into every thread of communication from data centers, between public cloud region instances, and external SaaS and API endpoints. Enterprise Agents are software appliances deployed in data centers and branch locations that continuously test IaaS and SaaS apps and underlying network communications at regular intervals to determine their health.

Bridge the visibility gap in the cloud with ThousandEyes monitoring by linking app performance to the end-to-end network path, from users wherever they’re located, across internal or Internet links, to data center, IaaS and SaaS applications. ThousandEyes can track the performance of critical external dependencies such as DNS, CDNs, BGP routing, DDoS and security providers. ThousandEyes makes sharing detailed data, visualizations and service-level dashboards across teams and organizations easy, for more effective collaboration, escalation and accountability with cloud providers.

Conclusion

Cloud success requires more than moving IT investments to SaaS and IaaS. Evolving operational visibility and processes is imperative. Digital Experience Intelligence empowers IT teams to move from a reactive to a proactive stance based on sound planning, effective problem solving and confident provider governance. Ultimately, mature cloud operations allows IT teams to offer their users and stakeholders a clear path to business success in the cloud.

ThousandEyes

201 Mission Street, Suite 1700
San Francisco, CA 94105
(415) 231-5674

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.