ThousandEyes

eBook

Network Intelligence for the Modern Enterprise WAN

Visibility for Internet-Centric, Hybrid and Software-Defined WANs

The Rise of the Modern Enterprise WAN

The modern enterprise WAN has emerged as a cloud-oriented and Internet-centric architecture. This represents a dramatic evolution away from traditional MPLS-based private WANs that were appropriate for the pre-cloud, pre-digital business, and pre-digital transformation era. Traditional WANs assumed that Internet communications were the exception rather than the rule. The rapid shift to SaaS and cloud-based technologies—consuming 75% of IT infrastructure and software spending by 2019 according to IDC[1]—means that for most enterprises this WAN evolution is accelerating.

The Modern WAN is Internet-Centric

The shift of IT spending to the cloud means that the days when privately managed links handled the preponderance of WAN communication streams are over. Several factors are moving both overall traffic and the matrix of connectivity from privately managed links to the Internet:

Digital Business

Customers connecting to front-door websites, e-commerce sites and external-facing web and mobile apps over the Internet are becoming more central to every business. According to Gartner, “CIOs expect 37% of their sales to be attributed to digital sales by YE20, which is an increase of 147% during a five-year span. By YE20, they also anticipate that 78% of business processes will be affected by digital business opportunities and threats. This represents an 85% increase over a five-year period.”[2]

Digital Transformation

Digital transformation of business processes means that even on-premises data center applications are bristling with SaaS-bound, Internet-connected web APIs. Retail PoS systems call SaaS-based payment gateways and omni-channel order management. Transportation, utility and telecom ERP systems integrate with SaaS-based fleet management. Distribution ERP systems call warehouse management SaaS. Soft drink bottler CRM systems call messaging APIs to execute vending machine service dispatches. Electronic Healthcare Record (EHR) systems call SaaS-based medical coding apps, while healthcare patient-facing websites connect to SaaS-based diabetes self-management portals.

According to IDC, digital transformation is “at an inflection point. Over the next three to four years, digital transformation efforts will no longer be ‘projects,’ ‘initiatives,’ or ‘special business units’ for most enterprises. They will become the core of what industry leaders do and how they operate.”[3]

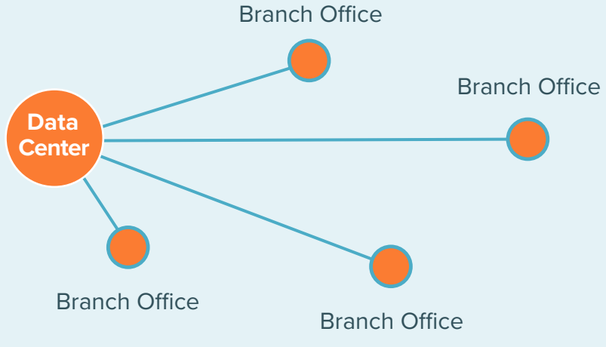
Hybrid Cloud Infrastructure

Most enterprises are and will stay in a hybrid cloud mode for quite some time. IaaS adoption is increasing sharply, but investment in private data centers and private hosted clouds continues to grow, albeit at a lower rate. This guarantees that intra-cloud and inter-cloud Internet communications will remain and grow over time.

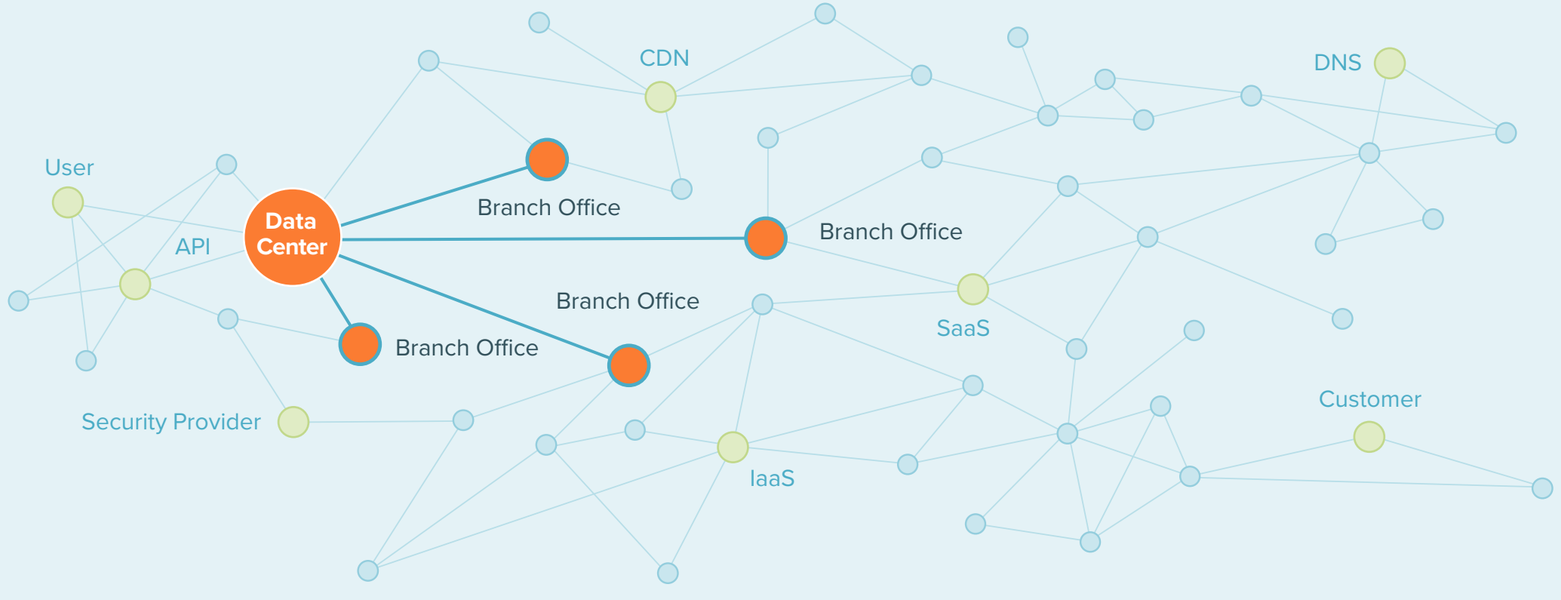
SaaS Mainstreaming

A majority of businesses have now adopted SaaS for at least one critical application, which means that a large and increasing percentage of branch traffic goes to SaaS-like Microsoft Office365, Google Suite, Salesforce.com, Workday and Box. As a result, according to Gartner, “by 2020, more than 60% of enterprises will have deployed direct internet access in their branch offices (which is an increase from fewer than 30% in 2016).”[4]

> CIOs expect 37% of their sales to be attributed to digital sales by YE20.



Traditional Enterprise WAN



Internet-Centric Modern Enterprise WAN

Increased Remote and Mobile Workers

Workers are no longer in offices—they are working from home, cafes, hotels, and customer sites. All of their communications are Internet-based in one way or another.

IoT

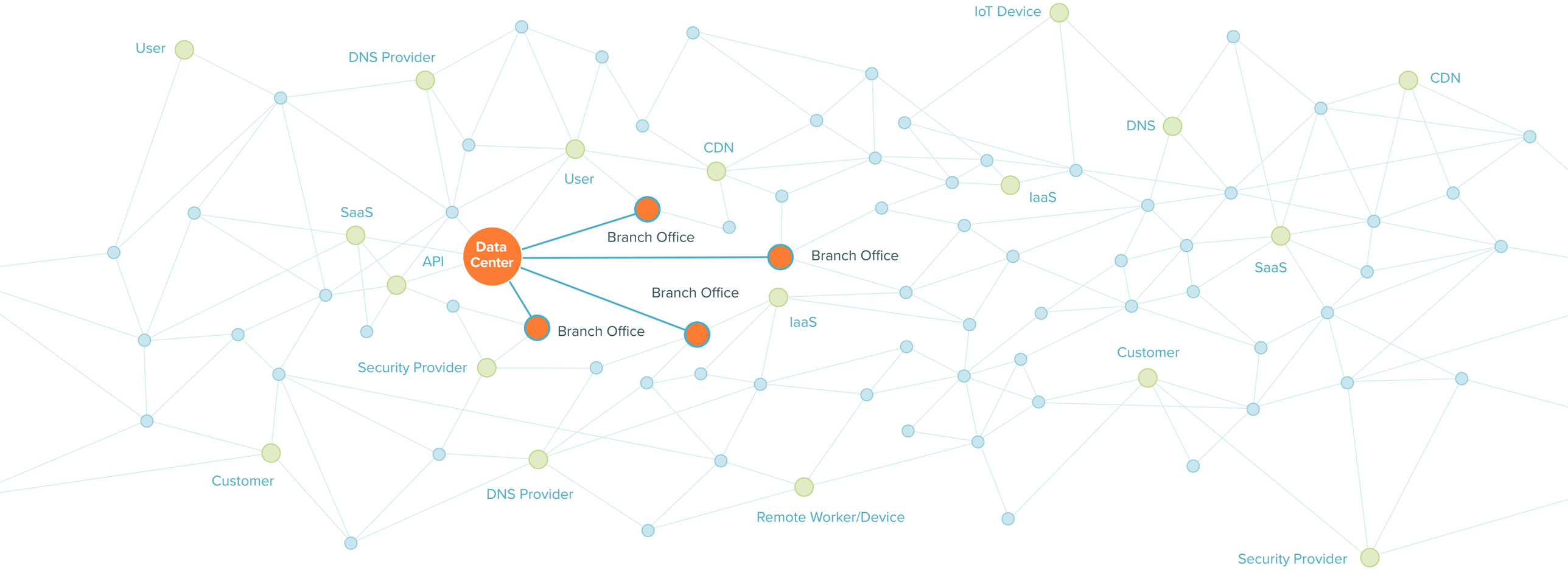
Internet-enabled devices are embedded in an increasing number of customer and employee business processes. Much of the communication from these devices goes directly to IaaS or SaaS applications.

Always-on Infrastructure Providers

The shift to Internet traffic has moved more than servers and storage into the cloud. Modern enterprises rely on DNS, CDN, and security providers to ensure customers and partners can reach and have a good experience with their websites. DDoS protection and web application firewalls have evolved from appliances to always-on services—turning security providers into an integral part of network connectivity. Attacks, Internet disruptions, internal outages, or performance slowdowns at any of these providers can cause significant business continuity impacts.

The Modern WAN Communications Matrix

The result is a new enterprise communications matrix that skews heavily to Internet-based connectivity—much of which happens completely apart from any enterprise site or infrastructure.



Hybrid WAN vs. SD-WAN

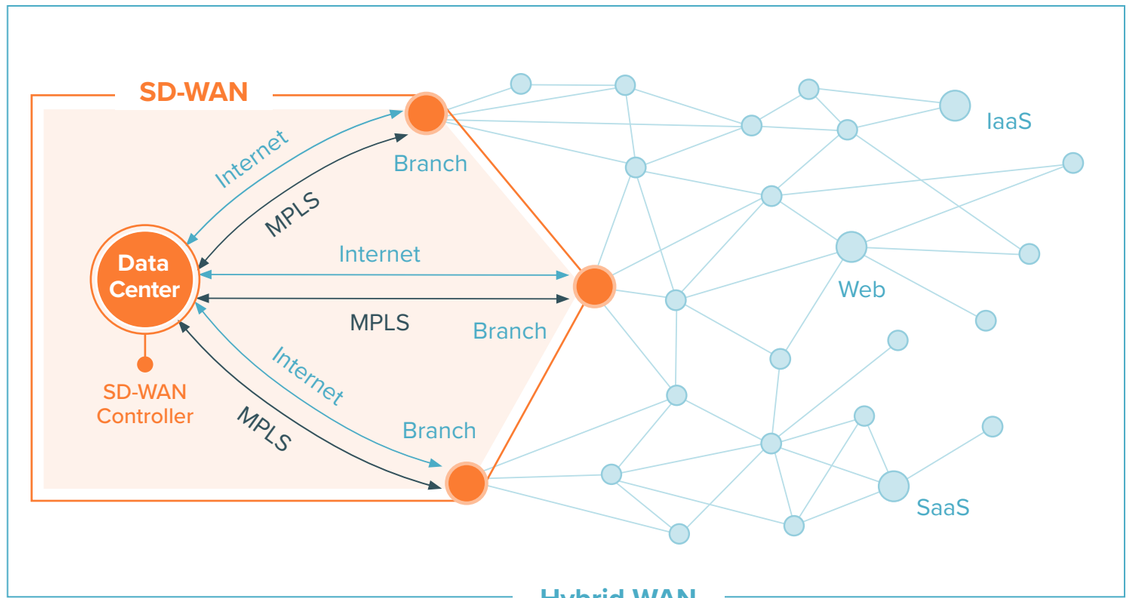
Hybrid WAN describes a logical WAN evolution in response to the Direct Internet Access (DIA) shift, where private MPLS connectivity is paired with DIA to SaaS and IaaS, often with Internet-based encrypted VPN tunnels as additional private connectivity to the data center. Dynamic Multipoint VPNs (DM-VPNs) extend the functionality of those encrypted Internet transit tunnels by allowing branch (spoke) sites to request direct tunnel access from the VPN hub concentrator to other spoke sites, allowing for more flexible, meshed communications.

One of the challenges of hybrid WANs was that for purposes of private connectivity, there was no centralized way to control which type of communication went over the more expensive MPLS links versus the more cost-effective Internet-based tunnels. SD-WAN introduces a SDN controller-based architecture for optimizing both the cost and performance of traffic routing across these two types of links. SD-WAN has succeeded where many other forms of SDN have not because the hub and spoke nature of branch to data center connectivity is relatively simple. This allows SDN controllers to implement business priority-based routing policies based on an expanded set of metrics including relative performance of apps across Internet tunnels versus MPLS links.

SD-WAN architecture is going mainstream. Gartner states, "We estimate there are over 5,000 paying SD-WAN customers, with more than 3,000 production SD-WAN deployments, covering more than 100,000 total branches."[5]

However, the rise of SD-WANs doesn't negate the larger shift towards the Internet. The scope of SD-WANs is primarily around connectivity (via MPLS or encrypted tunnels) from branches to the data center. SD-WANs themselves increase dependence on Internet connectivity. Many early adopters have discovered major operational challenges in the unpredictability of underlying Internet communications.

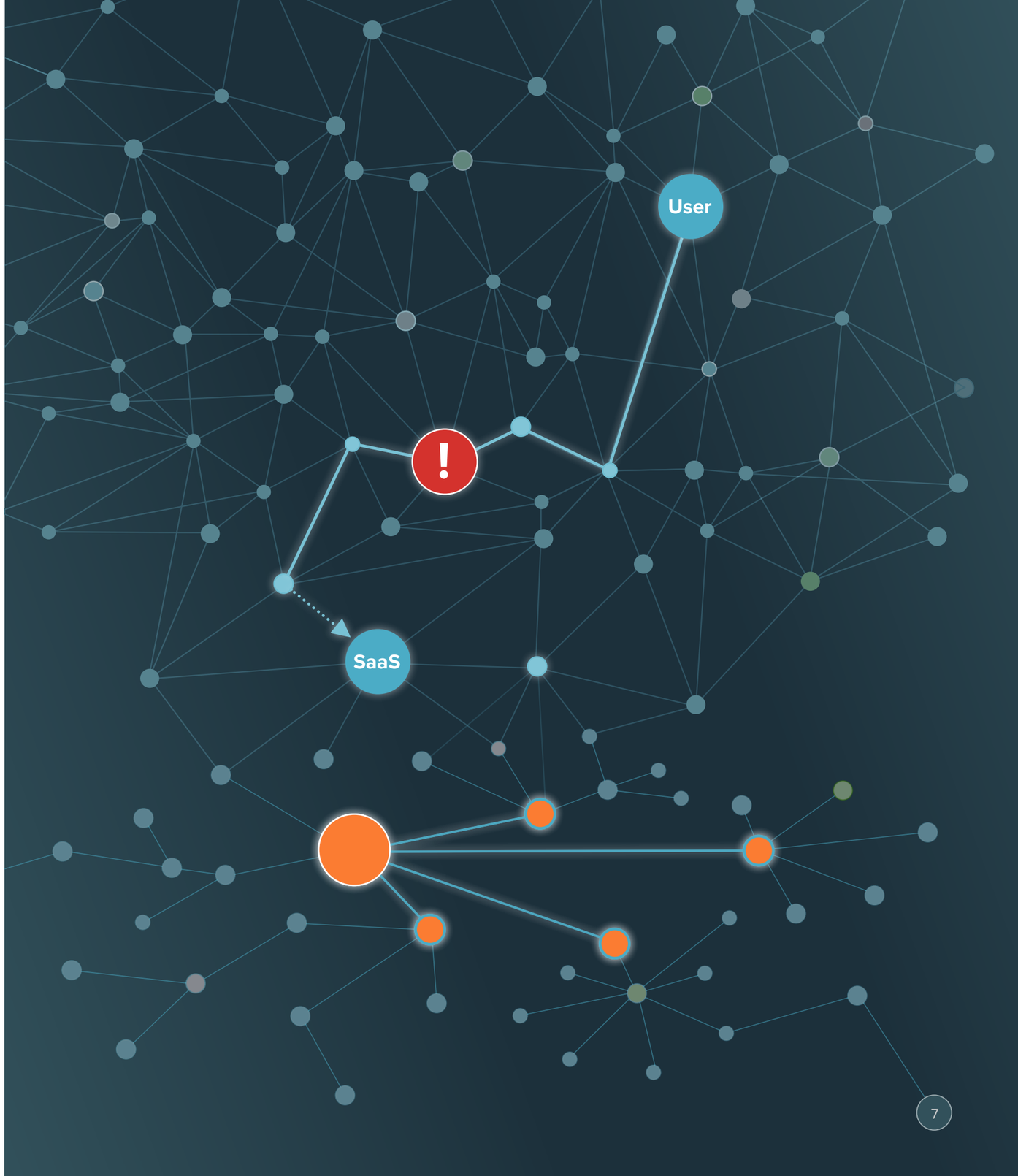
Whether hybrid or SD-WAN, enterprises are turning away from MPLS to Internet connectivity. According to Gartner, "up to 20% of global enterprises will completely replace their MPLS with internet before year-end 2022, up from less than 5% today."[6]



> Up to 20% of global enterprises will completely replace their MPLS with internet before year-end 2022, up from less than 5% today.

IT Owns Every Connected Experience

In the modern WAN, IT's role is expanding beyond building and maintaining infrastructure to include cloud governance. The scope of WAN governance in the cloud era can't be underestimated, since any communication path that delivers important applications is consequential to the business. It doesn't matter if the app is internally consumed or external facing; or if the communication paths move across privately managed links or the Internet. Nor does it matter whether a "user" is a person, an API or Internet-enabled thing; or if the app is internally hosted, runs on Infrastructure as a Service (IaaS) or is Software as a Service (SaaS). In terms of delivering performance, continuity and experience, IT leaders own the outcome from every user to every app across every network.

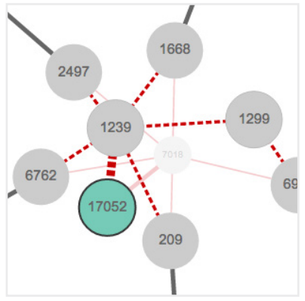


New Visibility Needed for Modern WANs

A major challenge for IT in the modern WAN era is that baseline network performance assumptions, traditional monitoring techniques and siloed data sets have lost validity. Furthermore, IT teams need independent and relevant data to keep a growing fleet of Internet-based vendors and partners accountable for performance and availability.

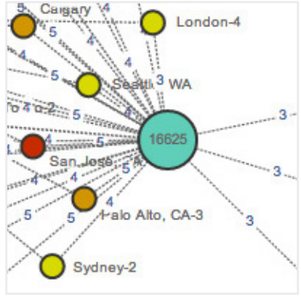
Recalibrating to the New Normal

Rolling out private data center applications that send traffic to branches over an MPLS WAN in place for a decade meant that the network's baseline performance was known—a norm. By contrast, Internet-based connectivity is a "new normal" that is unpredictable, especially for enterprises with global scope. This means that performance measurement must start before major cloud migration or SaaS rollouts occur. Moving performance measurement "to the left" in cloud migration timelines helps establish baselines, proactively identify bottlenecks, minimize project risk, and establish the basis for operational monitoring, troubleshooting and reporting.



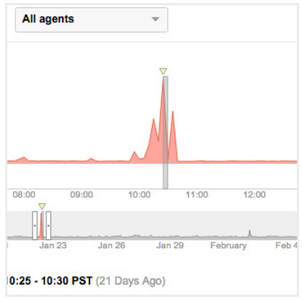
Active vs. Passive Monitoring

Traditional WAN performance monitoring techniques rely primarily on passive data collected from network infrastructure devices such as routers and switches. However, since so much cloud communication relies on networks that IT teams don't own and infrastructure that they can't access, passive data is simply no longer available in much of the extended WAN. This means that active monitoring that utilizes synthetic transactions to create performance data sets must assume a more prominent role in modern WAN visibility.



Integrated Performance Views from Every Perspective

Traditional network monitoring is siloed, focusing on network-only phenomena, requiring time-consuming expert intervention to assess user experience. Given the expansion of IT's scope of governance, it is critical that IT teams possess instant insights into precisely how the network is supporting or impacting application performance and digital experience. Since the new communications matrix includes so many legs that originate in the cloud or at Internet access endpoints outside of enterprise locations, that insight must be available from the perspective of users wherever they are.



Data-Driven Provider Accountability

With critical dependencies on cloud and infrastructure providers proliferating, IT teams need to exercise detailed governance of these vendors. Without precise, independent data to keep providers accountable, service escalations are at best a negotiation process, auditing is difficult if not impossible and IT teams lack the ability to enforce SLAs or achieve smarter contracts.

Network Intelligence

Network Intelligence refers to the data, technology, algorithms and techniques used to collect, analyze and visualize network information for the globally connected, digital world. The purpose of Network Intelligence is to optimize digital experiences everywhere, by understanding global network topologies, dependencies and behavior, and to support better IT decision making.

ThousandEyes is the Network Intelligence market leader, chosen by hundreds of enterprises and dozens of Fortune 500 and Global 2000 companies to solve visibility problems for modern WANs.

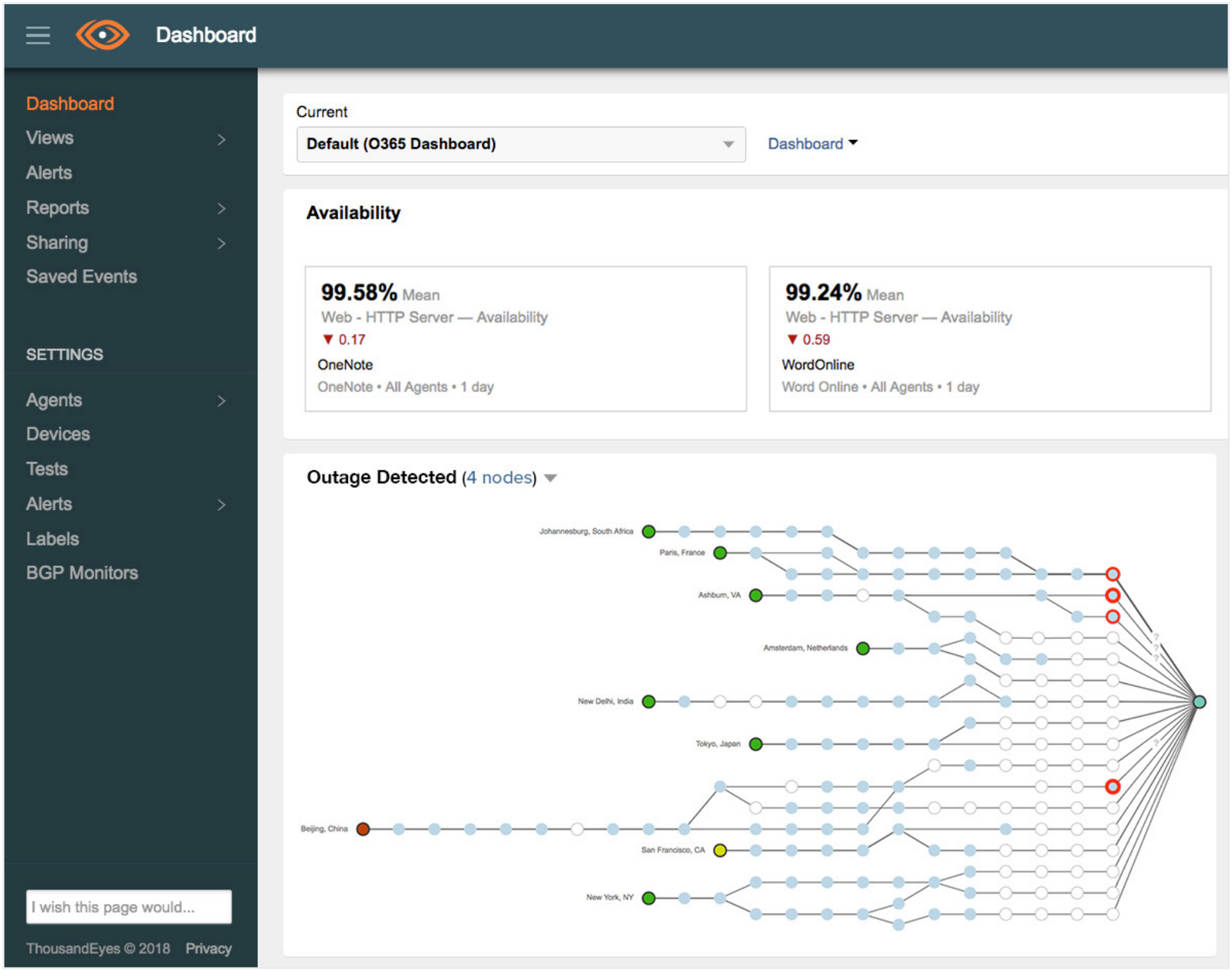
ThousandEyes Solution

ThousandEyes Network Intelligence platform updates network monitoring to better suit the needs of today's WAN. ThousandEyes delivers visibility for modern WANs by monitoring every network segment and application your enterprise relies on. Enterprise Agents are software appliances deployed in data centers and branch offices that continuously probe IaaS and SaaS apps and the underlying network at regular intervals to determine the health of the WAN. Enterprise Agents also collect and integrate detailed views of the status and performance of on-premises network devices. Cloud Agents in over 150 global cities provide app and network visibility to external-facing web properties, external-facing apps and cloud providers from a cloud and Internet-based perspective. Endpoint Agents deploy on employee devices to cover the perspective of remote and mobile workers.

ThousandEyes monitoring links 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. Monitoring can track the performance of critical DNS, DDoS and security providers from a variety of agent location vantage points.

Data gathered through active monitoring is algorithmically processed and represented in intuitive visualizations and correlated across application, network and routing layers.

ThousandEyes makes sharing detailed data and visualizations across teams and organizations easy, for more effective collaboration, service escalation and accountability with cloud providers.



Summary

The transformation of the enterprise WAN means that business now depends on Internet-centric connectivity and user experience. ThousandEyes Network Intelligence empowers IT teams to see, understand and improve connected experiences everywhere. To see the power of Network Intelligence for yourself, start a free trial or request a demonstration at www.thousandeyes.com

ThousandEyes

201 Mission Street, Suite 1700
San Francisco, CA 94105
(415) 513-4526

www.thousandeyes.com

References

1. IDC “FutureScape: Worldwide IT Industry 2017 Predictions.”
2. Gartner “2017 Strategic Roadmap for Networking,” Danilo Ciscato, Mark Fabbi and Lisa Pierce, February 2017.
3. IDC “FutureScape: Worldwide IT Industry 2017 Predictions.”
4. Gartner “2017 Strategic Roadmap for Networking,” Danilo Ciscato, Mark Fabbi and Lisa Pierce, February 2017.
5. Gartner “Hype Cycle for Enterprise Networking and Communications 2017,” Danellie Young, Bjarne Munch, July 2017.
6. Gartner “How to Architect Your Internet Services for Best Performance,” Bjarne Munch and Danellie Young, March 2017.

About ThousandEyes

ThousandEyes is a Network Intelligence platform that delivers visibility into every network your organization relies on, enabling you to resolve issues faster, improve application delivery and run your business smoothly.