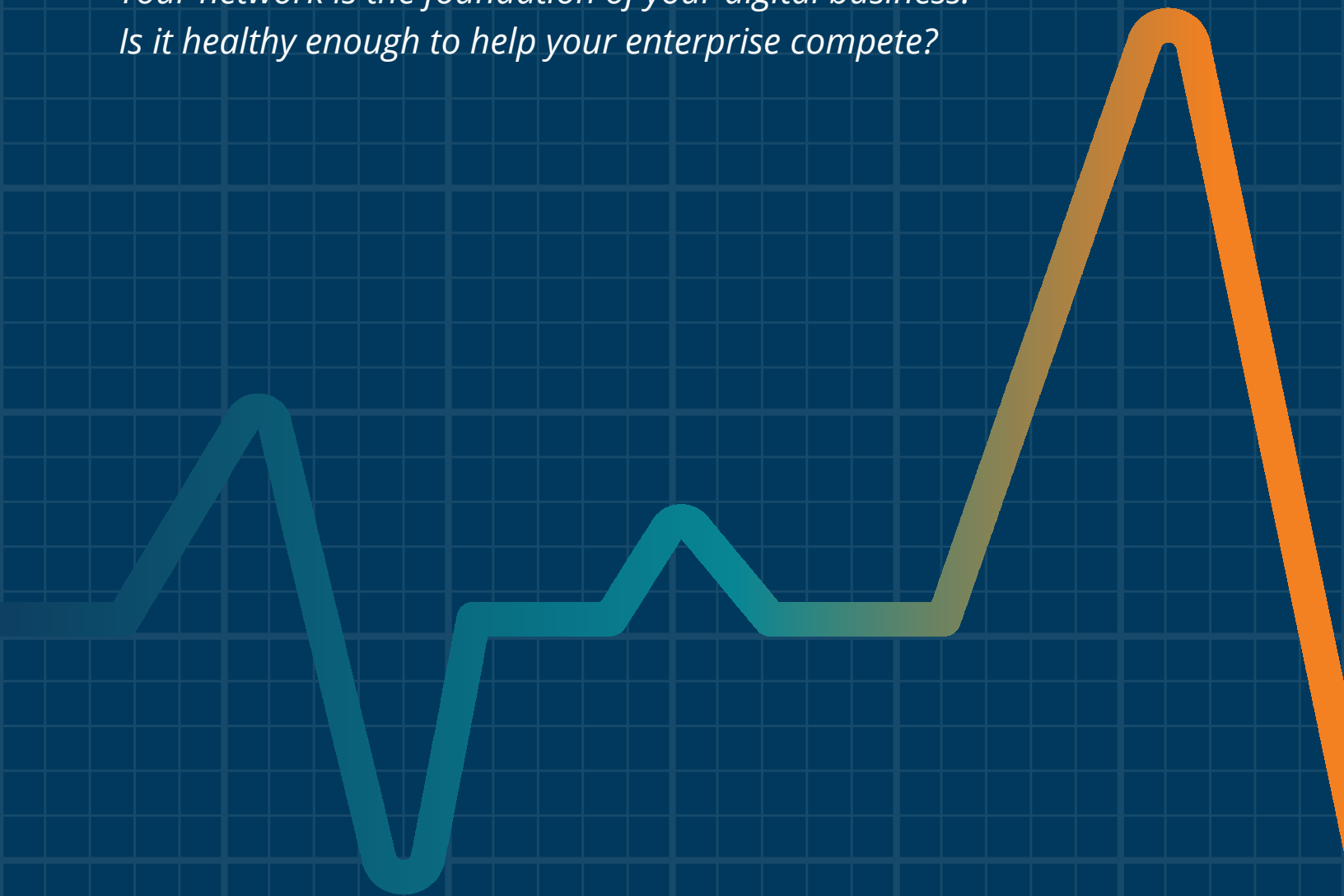




# Healthy network. Hearty enterprise.

*Your network is the foundation of your digital business.  
Is it healthy enough to help your enterprise compete?*





# At Zayo, we evaluate network health across two important aspects:



## Structure: healthy body

Is the design, connectivity, and diversity of your network — the fundamental arterial system through which your digital business flows — flexible, scalable, stable, and secure?



## Management: healthy habits

Are you monitoring your network's vitals on a continual basis? Healthy networks are observed across multiple signals, from circuits and switches to applications and beyond, to anticipate and proactively — even automatically — address issues.



# Diving in

## Structure: the steps to building it right

- Flexible design and connectivity solutions →
- Hybrid networks for the multi-cloud world →
- Diversity for resiliency and flexibility →

## Management: the steps to keeping it healthy

- Network monitoring keeps the pulse →
- Network observability to stay ahead →
- Automation solves problems before they cause issues →

## A holistic view: prevention to stay healthy

- Security from edge to core to cloud →
- Strategy for growth and scale →



# Structure

## Flexible design and connectivity choices for success

Are you still using only MPLS to move big data sets, or have you started incorporating edge networking to connect branches and sites? Whether you need the security and reliability of MPLS or the flexibility and efficiency of SD-WAN — or most likely both — a healthy network employs a range of connectivity solutions that fit the needs of the business today — and can help it grow into tomorrow.

Keeping your staff, your customers, and your stakeholders all happy means developing a range of flexible networking options. Knowing which technology to turn to depends upon how your organization's data flows, and frankly, upon your DNA.

"There's an assumption that everyone is moving to the cloud, yet many IT orgs are pulling back, finding that being able to control their own data centers gives them greater reliability and predictability and saves them the expense of ingress and egress fees," says Alissa Clousing, Vice President of Product Management at Zayo. "Unforeseen events like the pandemic have taught us that being able to move workloads from the core to the cloud — while taking advantage of the edge — is critical."

### USE MPLS IN THE CORE WHEN YOU NEED:

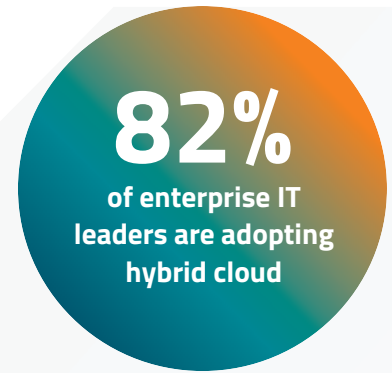
- Dedicated, private connections
- Highest reliability
- Most mature, widely adopted technology
- Traffic prioritization

### USE SD-WAN AT THE EDGE WHEN YOU NEED:

- Fast configuration and deployment
- Lower-cost underlay infrastructure
- High flexibility and control
- Application-level management

## Hybrid connectivity for multi-cloud

Cisco reports that 82% of IT leaders are adopting the hybrid cloud, meaning increasingly, enterprise IT needs to connect a combination of various third-party cloud service providers with their own data centers. A multi-cloud approach that requires a range of connectivity types to ensure that it's all networked securely together. Healthy networks have clouds that are networked together with reliable, low-latency, and cost-effective connections.



### If this sounds like you:

*"We are looking to increase our adoption of the cloud to support our corporate growth. In addition to greater choice, we need to ensure that our data stored in different cloud environments, including our own private cloud, can interact efficiently and securely."*

### Then we prescribe:

First, a private, secure connection to multiple cloud providers will improve performance and cost over a public connection. Then, build private, virtual, protected, and high-performance connectivity between cloud environments. Enterprise data is increasingly being stored across multiple cloud infrastructures. This network structure allows for direct interaction for applications, delivering optimal customer experiences and indirect cost savings.



## Diversity = reliability + resilience

In order to be resilient and reliable from the core to the edge, your network should be built on diverse routes and structured with failover in mind. And diversity means more than just physical routes and redundant equipment: it's having diversity of technology, from Ethernet to wavelengths to the intelligence of SD-WAN.

Design as much diversity into your network structure as you feel you need to bounce back from common outages. That could include card diversity to protect against card failures, PoP and geographic diversity to protect against regional or localized incidents like power outages or disasters, or path diversity to protect against fiber cuts.

Technology diversity mixes multiple transport mechanisms like waves or dark fiber to provide diversity of underlying network topology. This protects against software related or logical configuration issues in one single technology platform.



*Zayo has expansive, deep, and diverse fiber networks in North America and Europe, including long-haul and dense metro routes.*

[LEARN MORE ABOUT ZAYO'S NETWORK >>](#)



*Zayo offers SD-WAN solutions to optimize application throughput and migration to the cloud.*

[LEARN ABOUT MANAGED EDGE >>](#)



### If this sounds like you:

*"We need to keep our business running, stay compliant with regulations and policies, and create efficiencies in our system backup and data replication. For us, security, high capacity, latency, and encryption are all key elements of optimizing disaster recovery."*

### Then we prescribe:

A bespoke design with fully diverse routes for your core disaster recovery and storage area network. Zayo has 141,000 metro, long haul, and subsea route miles connecting the majority of data centers. With thousands of neutral data centers and 44,000 buildings connected globally, we provide robust designs and SLAs for your core and replication network.

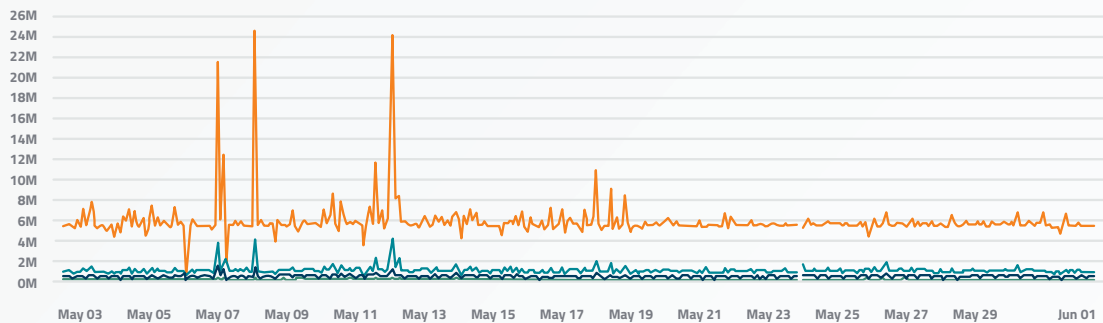


# Management

## Monitor the pulse of your network

When you collect and report on a variety of data about your network's performance — routers, switches, firewalls, load balancers, and endpoints — you should be able to correlate the data points to understand a drop in performance. Monitoring usage is an important metric to ensure you never see red (i.e. reach your bandwidth limit).

### EXAMPLE OF NETWORK PERFORMANCE OVER 30 DAYS



— Avg In: 645.29B — Avg Out: 312.54B — Max In: 24.59M — Max Out: 4.36M

## Observability translates to prevention

Strive for total **network observability** — a single-pane view of separate network data, down to the application and business service level. Observability provides the intelligence to identify root causes of anomalies and malfunctions anywhere on your network, allowing you to get ahead of potential issues, so you can predict outcomes and prevent slow-downs and outages before they happen.

“Imagine being able to see continuous health information about your network: get information from multiple devices and systems, understand dependencies, separate signal from noise, and act on that data,” says Ed Loveless, Director of Edge Product Management at Zayo.



### **Visibility and control at the edge**

*Zayo's Edge Networking Solutions portfolio includes our zInsights Portal, a comprehensive view of multiple platforms, domains, and silos to provide our customers with visibility and control of network health and performance.*

[WALK THROUGH ZAYO'S ZINSIGHTS PORTAL »](#)

## Let's compare:

### MONITORING



Collect and display data from different systems



Show performance metrics and usage data



Alert/troubleshoot potential issues

### OBSERVABILITY



Collect and display data across systems



Uses AI to determine which signals matter



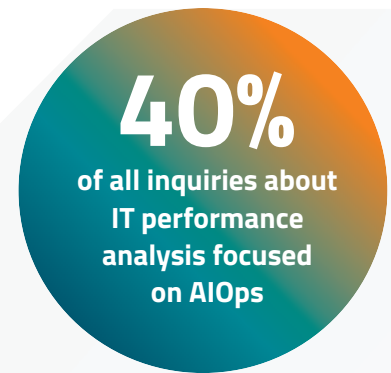
Detect and solve root cause



## Automation provides scale and speed

Expect automation to play a growing role in how a healthy network can meet bandwidth demand. When packet delivery is automated, the buying and installation process can be nearly immediate.

AIOps is growing in importance — last year Gartner reported that AIOps formed part of the conversation in 40% of all inquiries with their clients on IT performance analysis. The emergence of AIOps means that when an issue with the network is detected, the necessary tooling or processes can be automatically deployed to better understand and even attempt to resolve the issue. Again, network observability is key: the integrated view of every aspect of the network collects the data necessary for AIOps to properly grasp what happened. “An AIOps approach drastically reduces operational workload and improves incident outcomes, enabling a true end-to-end solution that’s essential for optimizing digital experiences,” Loveless says.



### If this sounds like you:

*“We have multiple offices across the United States, and a complicated data infrastructure — including a business-critical UCaaS phone system — that is causing network reliability, bandwidth, and cost challenges.”*

### Then we prescribe:

Replace the majority of your complicated stack with a single SD-WAN appliance to simplify and streamline your network edge. By simplifying your network, your UCaaS solution can operate at peak performance. We also suggest supplementing your MPLS and broadband with an LTE connection for lower-cost reliability and stability in the network and integrating your data centers using both MPLS and Internet. With SD-

WAN running on top of your less expensive network connections, you’ll find that your network performs better than it did when you were paying for a more expensive infrastructure.

Even better: SD-WAN offers application-level visibility. With AI capabilities built into the edge ticketing and management systems, your IT team will understand at a glance where it needs to spend its time. Observability eliminates the “noise” in your network, stops your IT team from firefighting, and lets you concentrate on your business again.



# A holistic view



## Secure from edge to core to cloud

Network-based security protects against network threats, for example, DDoS attacks, which cost businesses an average of \$200,000 per attack. The **best DDoS protection** stops DDoS attack traffic before it reaches your network and impacts your business.

Site-based security is vital for mitigating in-bound threats and providing inline filtering. To protect the network at the edge, adopt a user-based, “trust no one” security approach. Technologies like **SASE** and **Zero Trust** follow each user, no matter their location or what device they’re using to access the network.



## Building for the future

Planning ahead for capacity demands requires both a network growth strategy and a just-in-time approach to add capacity when and where you need it. A healthy network is one that can scale both strategically and on demand.



**Armed with an understanding of how to think about network health, are you ready to get your own diagnosis?**

Take our 3-minute network health check to get your score.

**GET ASSESSED →**

## **About Zayo**

For more than 15 years, Zayo has empowered some of the world's largest and most innovative companies to connect what's next for their business. Zayo's future-ready network spans over 16.8 million fiber miles and 141,000 route miles. Zayo's tailored connectivity and edge solutions enable carriers, cloud providers, data centers, schools, and enterprises to deliver exceptional experiences, from core to cloud to edge. Discover how Zayo connects what's next at [www.zayo.com](http://www.zayo.com) and follow us on [LinkedIn](#) and [Twitter](#).