CATO NETWORKS

US SIGNAL®

The Dark Side of SD-WAN

Organizations around the globe continue to invest in SD-WAN to optimize their edge network connectivity, enhance user and application experiences, enable increased operational efficiency, and save money.

IDC Analyze the Future

2023 IDC MarketScape on Worldwide SD-WAN Infrastructure

47%

of businesses have migrated to SD-WAN and another 48% say they'll deploy the technology some time in the next two months.

Realizing the Full Potential of SD-WAN, An IDC White Paper sponsored by GTT

90%

among survey respondents organizations are actively researching SD-WAN.

2019 SD-WAN Market Trends Survey

CATO NETWORKS

US SIGNAL®

Such high adoption rates come as no surprise given the wide range of benefits the technology offers. (See **The Ultimate List of SD-WAN Benefits**.) Organizations look to SD-WAN for a variety of reasons—to augment or eliminate MPLS, to get better cloud application performance, to reduce WAN costs, to get better business agility, all of which are benefits today's businesses are looking for.

While there's certainly a glow on the upsides of SD-WAN, there's also a "dark side" that companies need to consider as they buy into the technology. For example, companies looking to replace their traditional WAN's end-to-end MPLS circuits with less expensive transport options must consider how to design reliability and high availability into both the middle mile and the last mile of their SD-WAN. There are trade-offs everywhere.

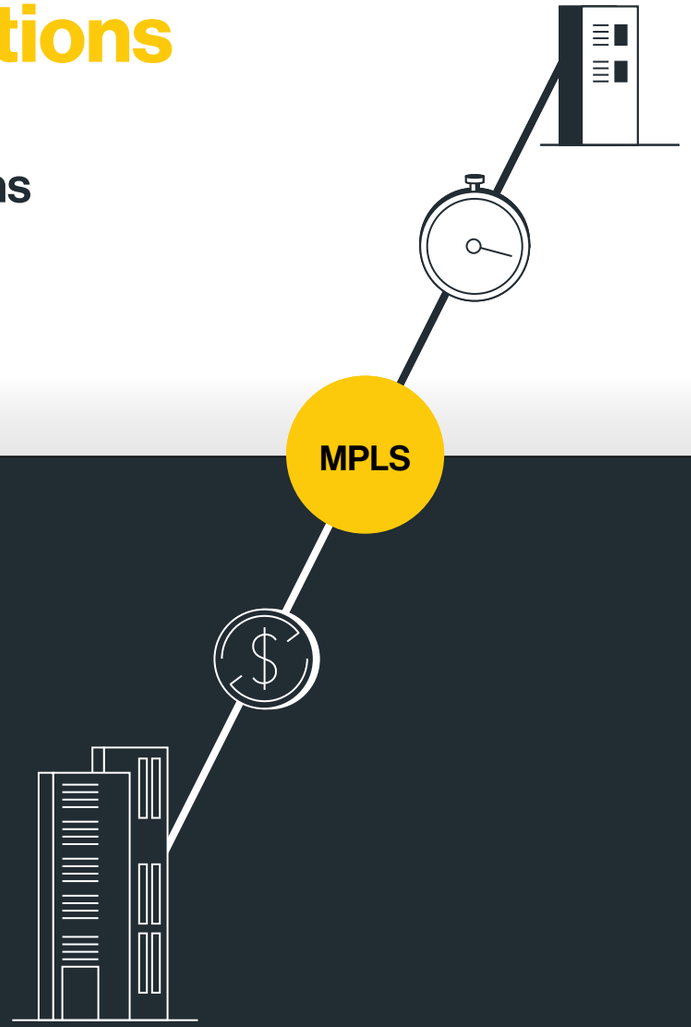
This article shines a light on the side of SD-WAN.

CATO NETWORKS

US SIGNAL®

Last Mile Considerations

Trading MPLS for Diversity of Options

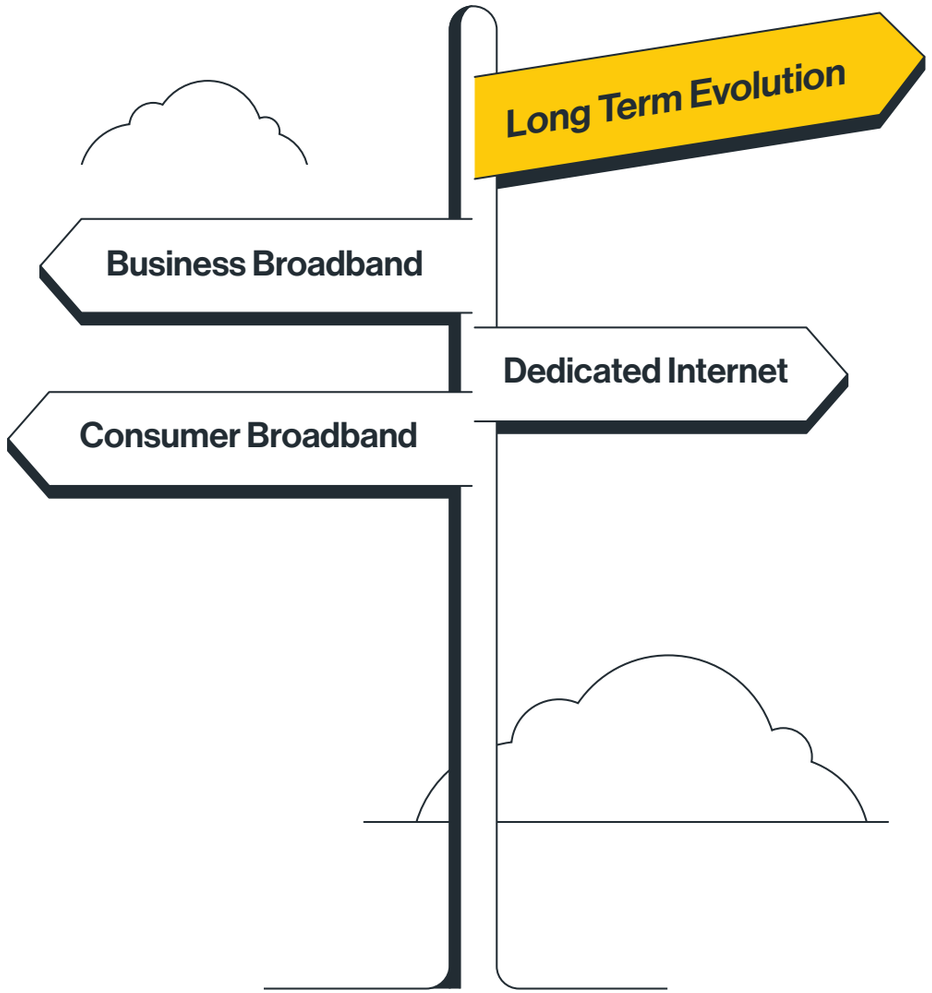


As a premium product, MPLS provides high availability, is backed by SLAs, and is fully managed by the provider. All the capacity is dedicated to just one enterprise.

But it lacks in flexibility and cost-efficiency—two of the prime drivers for replacing MPLS with SD-WAN. With SD-WAN, companies can select the optimum last-mile service for each location, connecting their sites MPLS as well as affordable last-mile services using fiber, broadband, or 4G/LTE.

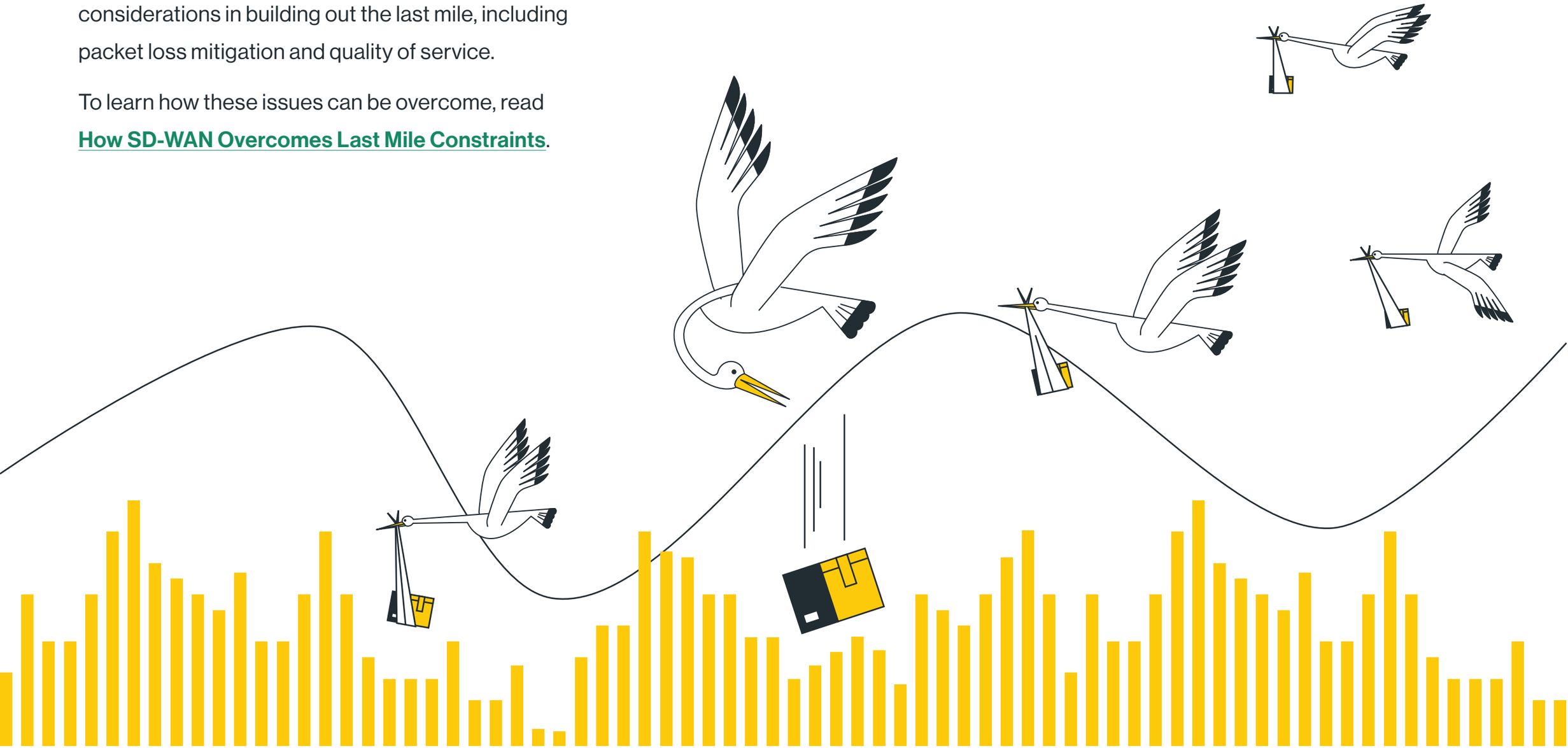
There are trade-offs to consider in terms of dedicated capacity and availability in the last mile types such as dedicated Internet, business broadband, consumer broadband, and LTE. Having these choices is important because the relative cost of these options enables tailoring last mile connectivity to the needs of a particular business location instead of buying the premium service everywhere the business operates. It gives more flexibility and enables business agility. However, having just a single Internet connection might be too unstable for the business in terms of availability. This requires careful consideration of how to build reliability into the chosen connections.

Something like LTE isn't a traditional transport in the sense that it may not be used all the time, but it does provide an extremely powerful failover in case there is physical infrastructure damage (think backhoe cutting a major Internet circuit). A combination of Internet wired last mile with wireless can achieve an availability level actually exceeding MPLS.



While flexibility is great, there are other important considerations in building out the last mile, including packet loss mitigation and quality of service.

To learn how these issues can be overcome, read **How SD-WAN Overcomes Last Mile Constraints**.



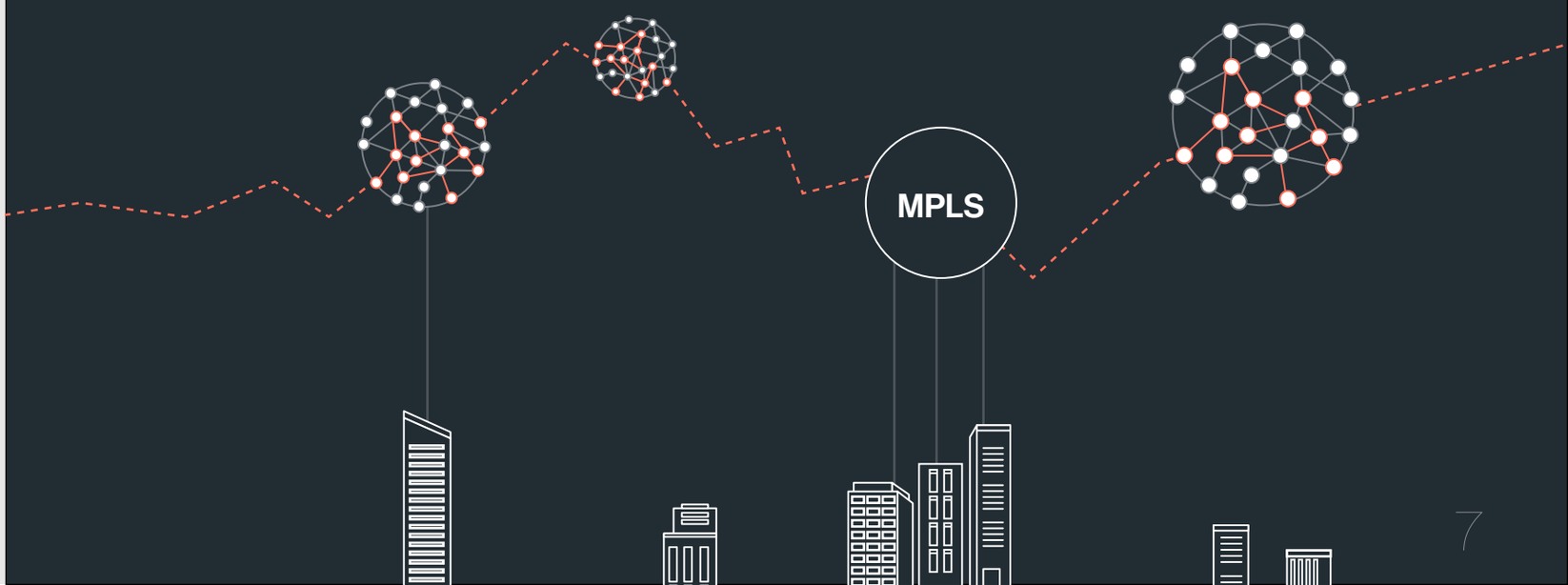
Middle Mile Considerations

Compensating for an Unpredictable

Organizations that want to replace or reduce reliance on MPLS have to think about how to design the middle mile such that it delivers the same predictability and the same stability that they had with MPLS in order to ensure good user experience. While the Internet seems to be the obvious choice, it's an unpredictable transport platform.

The reason for the problems in the Internet middle mile are well known. Routers are built for fast traffic processing and are therefore stateless. Control plane intelligence is limited as there's little communication between the control and data planes. As such, routing decisions are not based on application requirements or the current network levels of packet loss, latency, or congestion for each route. Shortest path selection is abused: Service providers' commercial relationships often work against the end user interest in best path selection. In short, the Internet moves traffic forward based on what's best for the providers, not the users or their applications.

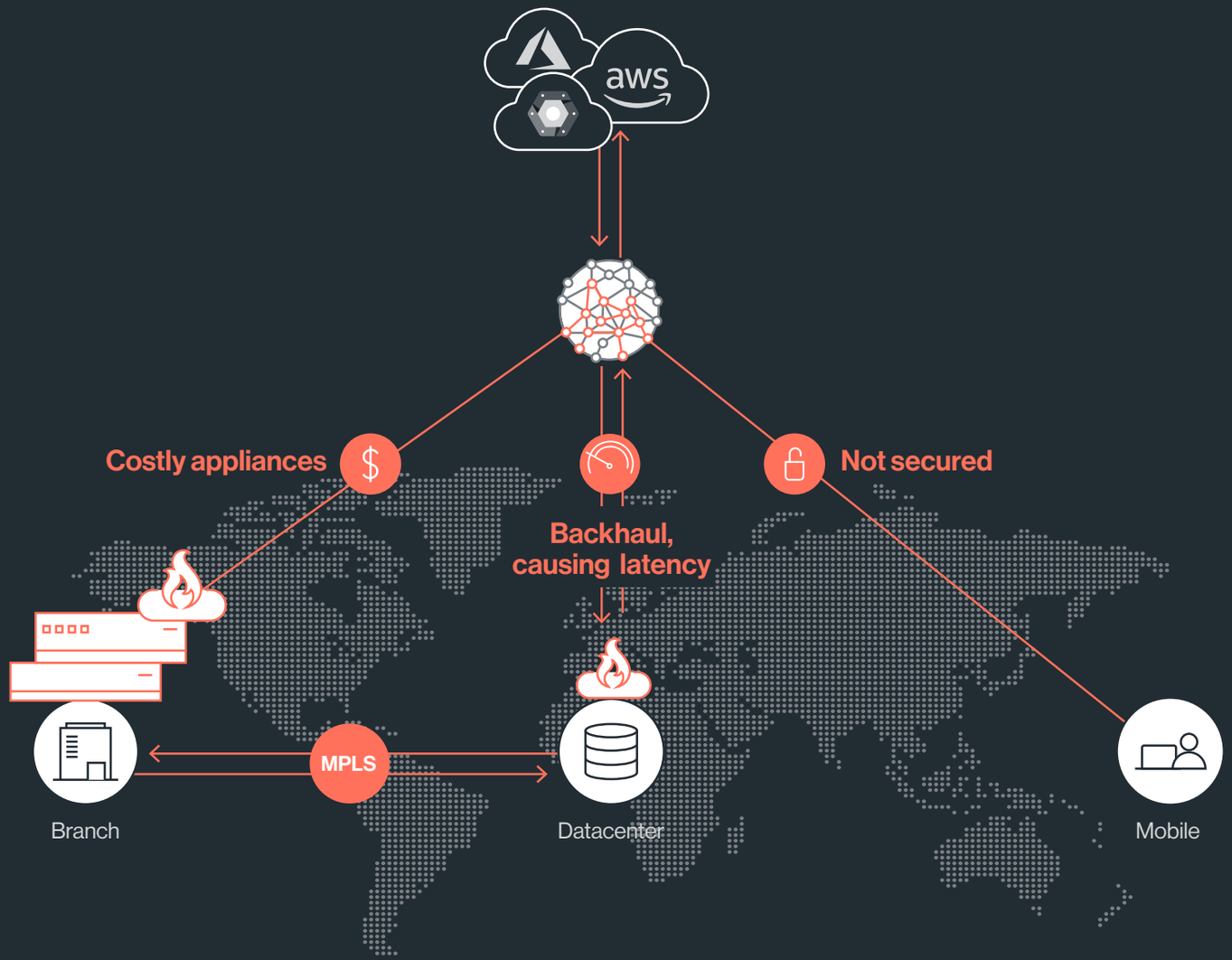
MPLS continues to be an option for the middle mile, but that defeats the principles of agility and cost reduction. What's needed is an alternative that is designed to deliver a globally consistent experience while controlling the cost of that global platform. Read more on **How to Get Reliable Global Connectivity at an Affordable Price**.



Security Considerations

Security poses many questions when it comes to SD-WAN. Often, companies are forced to backhaul traffic from their branch locations to their datacenter in order to maintain a uniform security policy—a practice that's not compatible with today's distributed networks.

There are several options for doing direct Internet access (DIA).



CATO NETWORKS

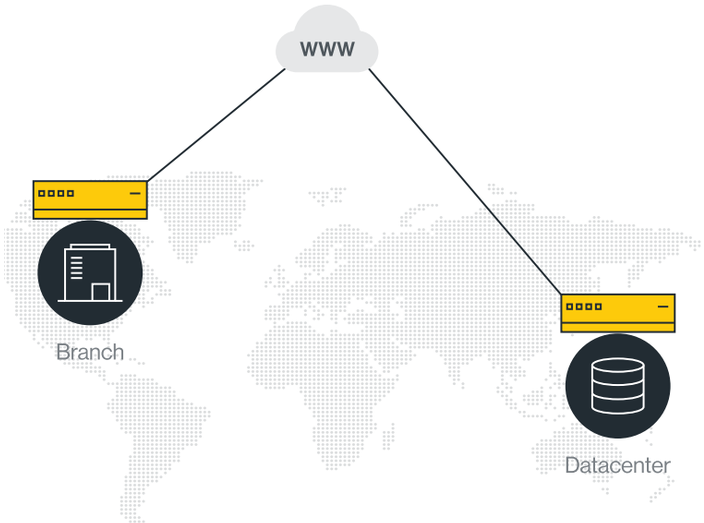
US SIGNAL®

Security Considerations

How Much Threat Prevention Do You Need?

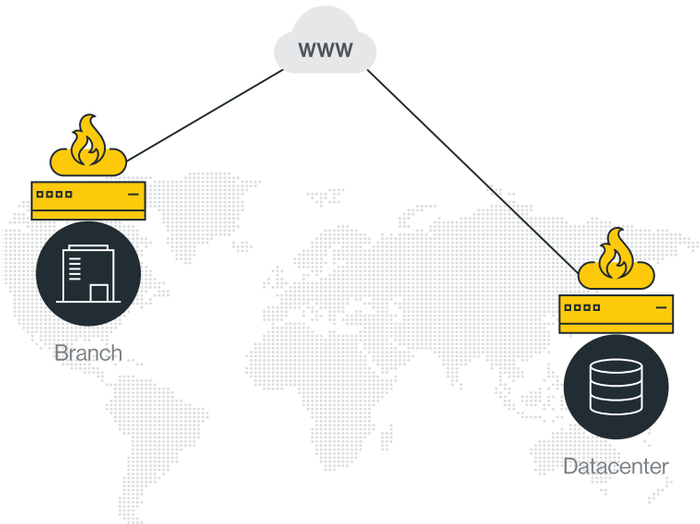
1 None

Use the basic firewall within the SD-WAN appliance—and we do mean basic. This firewall doesn't inspect user traffic, which means if a user accesses a malicious site or downloads malware, the firewall would be blind to these threats. Most organizations can't afford that level of risk.



2 UTM

Typically a unified threat management (UTM) device from a company that sells network security. This does provide traffic inspection and often some level of threat prevention, but it also means appliance proliferation. If a company has 50 locations, that means buying, deploying and managing 50 security appliances. Most companies don't like this approach due to cost and complexity.



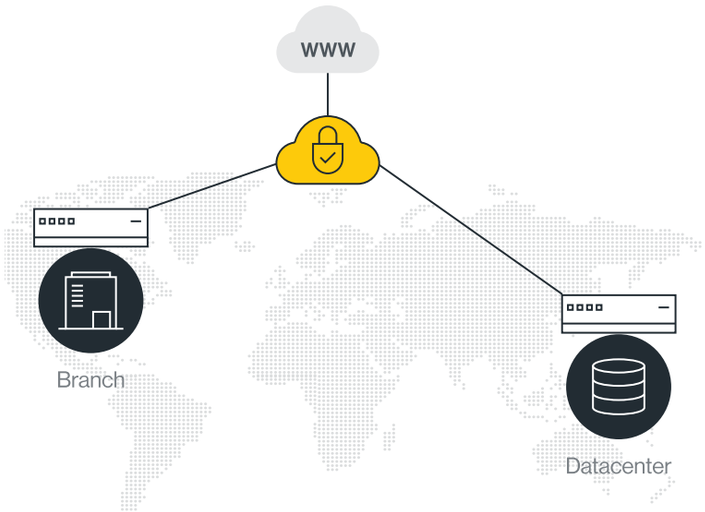
Security Considerations

How Much Threat Prevention Do You Need?

3

Cloud-based security

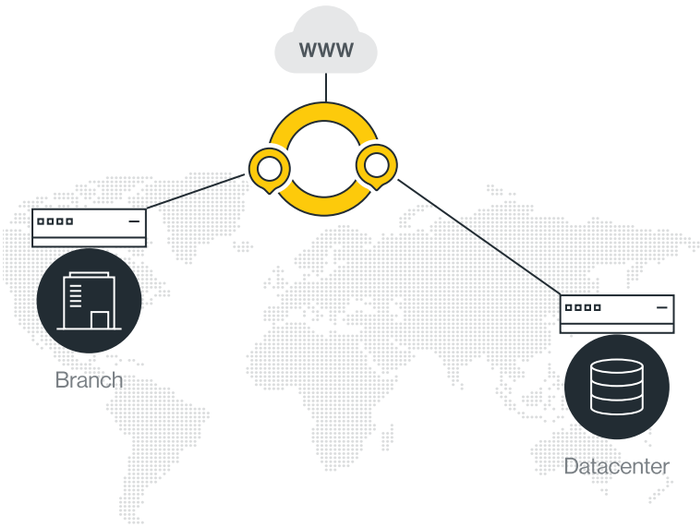
A third approach is to connect all these branches to some form of cloud-based security technology. This eliminates the firewalls at every location, but there are still multiple products to deal with. There's the firewall in the datacenter, the SD-WAN at the edge, and the cloud-based security—each with its own management interface and policies. This, too, adds complexity and cost.



4

Converged cloud-based network and security

And finally, there is the **convergence of cloud-based network and security**. It's a single platform that provides SD-WAN at the edge and the security in the middle. Gartner calls this approach **Secure Access Service Edge (SASE)**. It's one place to manage all the policies, see all the analytics, and understand all the events.



CATO NETWORKS

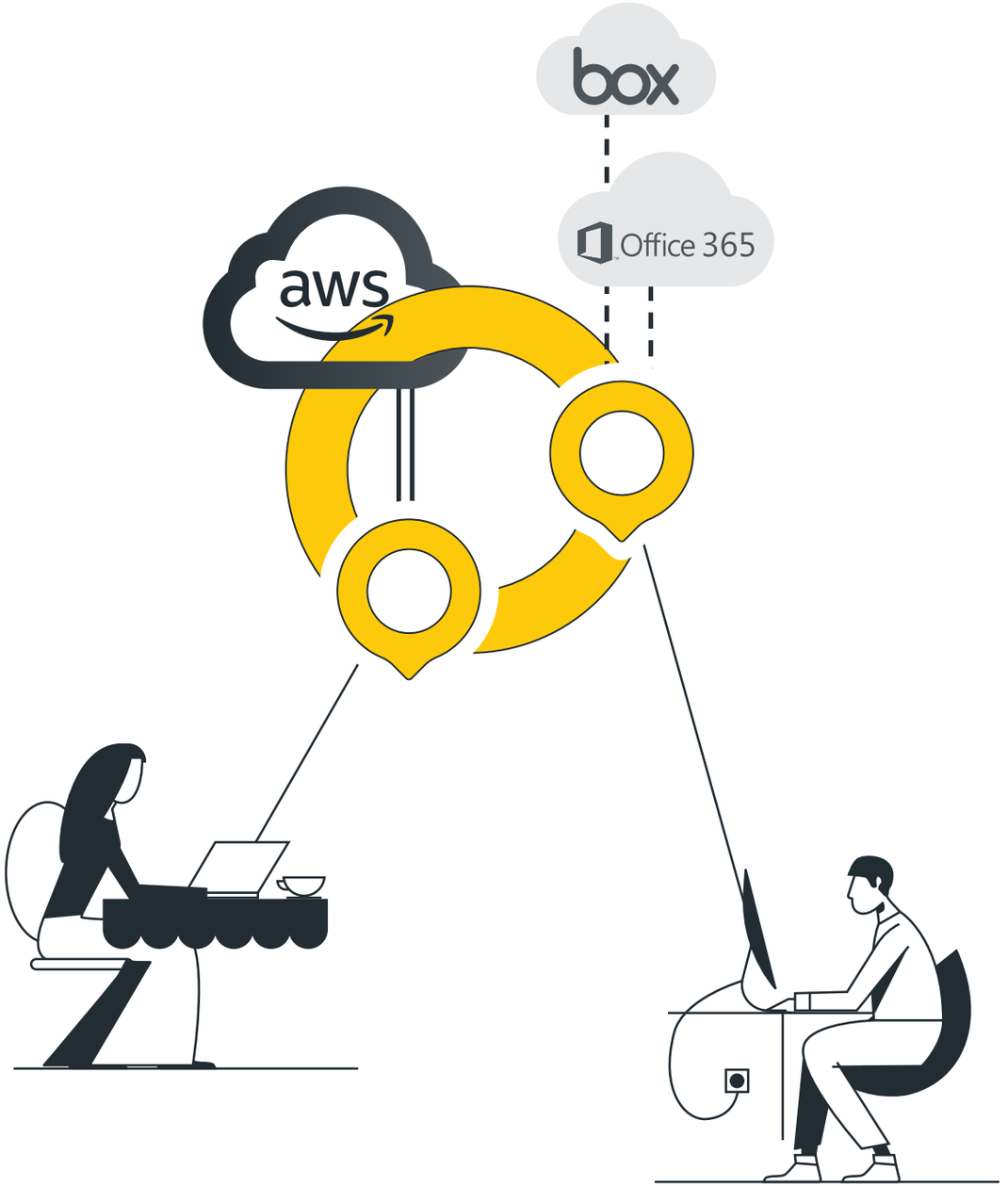
US SIGNAL®

Cloud Access Optimization

When thinking of replacing MPLS as the middle-mile transport, cloud access is of particular importance. Companies have datacenters, branches and users and they all want access to cloud datacenters and cloud applications. It's difficult to predict where the cloud instances are and they may be very far away from the business location. Using the public Internet to get there is risky in terms of performance and reliability.

One option for optimizing cloud access is to use premium connectivity from the providers, like AWS Direct Connect or Azure ExpressRoute.

Other solutions would be to use cloud networks that get closer to these datacenters by egressing the traffic from any of the enterprise's edges as close as possible to the target cloud instance.



Network Monitoring

Another dimension of SD-WAN is network monitoring, especially when there are multiple last-mile ISPs. Somebody has to monitor the network, understand that there is a problem, open the tickets with the relevant ISP, and then work with that ISP until the issue is resolved.

Something to consider here is some form of 24/7 support, whether it comes from the different service providers or it's hosted internally. We find that many organizations choose to rely on external providers in order to achieve 24/7 monitoring.

CATO NETWORKS US SIGNAL®

Managing the SD-WAN

There are several considerations when it comes to managing the SD-WAN. A broad consideration is how to transition from a network that had a single provider or one primary MPLS provider and secondary Internet providers, to a network that has multiple providers. This requires thinking about how to contract with ISPs in every location, and how to manage those contracts. Some companies choose to manage this effort themselves, while other choose an aggregator.

And then there is management of the network itself. The legacy network basically allowed for do-it-yourself (DIY) and fully managed models. With DIY, the enterprise organization – typically a large one staffed for the task – did the deployment, integration and management. With a fully managed model, the carrier took responsibility for everything and the business could only submit tickets to enact changes.

Conclusion

The era of the legacy network is coming to a close. A WAN centered around an on-premise datacenter, with all traffic running through that datacenter for access to applications and security, just can't support the growing use of cloud-based applications and mobile users.

SD-WAN addresses many of today's networking needs, but it's not without some serious considerations in "the dark side of SD-WAN."

Eliminating the Dark Side of SD-WAN with the world's first SASE platform

Cato saves companies from SD-WAN's "dark side" with the world's first secure access service edge (SASE, pronounced "sassy") platform. Following the principles set by Gartner's SASE framework, Cato provides global, cloud-native, and software -defined architecture to deliver an adaptive and secure network that evolves at the pace of your business.

US Signal, a leading provider of network connectivity and data center services, partners with Cato Networks, the provider of the world's leading SASE platform, to offer the SASE Cloud throughout North America.

The SASE Cloud connects data centers, branches, mobile users, and cloud resources into a global, optimized and secure managed SD-WAN service. All WAN and internet traffic is protected by a comprehensive suite of security services, updated and managed by dedicated security experts.

Replacing MPLS and multiple networking and security point solutions with the SASE Cloud forms an agile, efficient network that can meet today's and tomorrow's business requirements.

US Signal / Cato Cloud

Global Private Backbone

Edge SD-WAN

Security as a Service

Cloud Datacenter Integration

Cloud Application Acceleration

Mobile Access Optimization

Managed Services

Managed Threat Detection and Response (MDR)

Intelligent Last-Mile Management

Hands-Free Management

Site Deployment