CATO NETWORKS

BYTES

The ROI of Doing Nothing

Don’t Mess with What Works, Right?

The old saying, “If it ain’t broke don’t fix it,” applies to a lot of things in life, but certainly not to IT networks and security in the age of digital transformation.

It took time to get your network fully operational. Users seem happy and productive, with no disasters, and you’ve even managed to stay on budget and in compliance lately without a tremendous amount of effort. Why change anything?

In today’s business climate, standing still is the kiss of death.

No business can do so for long and stay competitive in this era of constant digital change. Even in mature industries, change is necessary, whether organizations are looking to slash production costs to improve profit margins, adopt new methods and technologies for improving customer success, or discover new markets to enter.

IT must be prepared for that change. Cloud migration, work from home (WFH), new security threats — legacy networks can accommodate these and other dynamics to a point. But at some time, even the best technology becomes irrelevant. As a technology owner, IT needs to ride the technology waves, skipping from wave to wave at the right time.

When is the right time for you to make the leap.

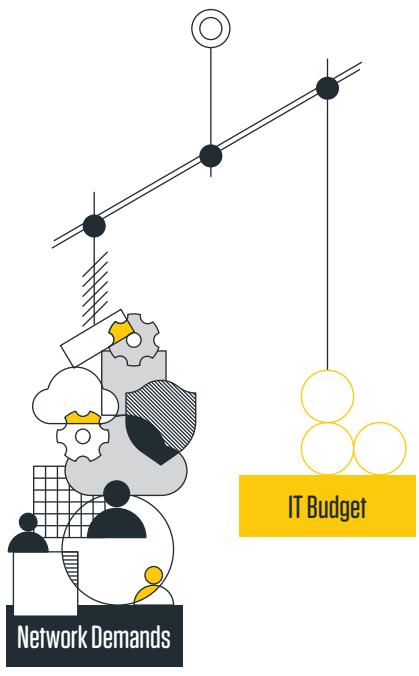
We’ll show how thinking strategically but implementing tactically will allow you to put into place a network and security architecture today that futureproofs you for tomorrow. ROI calculations and peer experiences are provided as an appendix to illustrate that adoption strategy.

Let’s take a closer look.

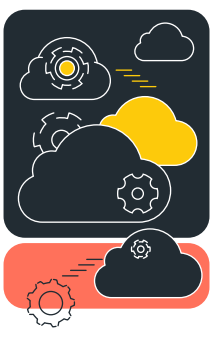
What You Know

New Demands Will Be Placed on Your Network

Your network is bound to face new challenges. Even if an earthquake doesn't strike, COVID-19 doesn't resurge, or there isn't some other major disaster, business and IT never stay the same. There will always be new needs that you must be prepared to fulfill on your current budget.

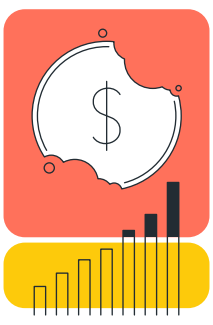


Here are some of the challenges your peers are already facing:



More Applications Will Migrate to the Cloud

Over the next year, your team will most likely provision access to more infrastructure and applications in the cloud. You'll need a way to monitor and manage that access and find a way to confront "Shadow IT." Across legacy networks, cloud provisioning and monitoring are challenging, lacking native cloud connectivity and the means for enforcing policy on cloud services.

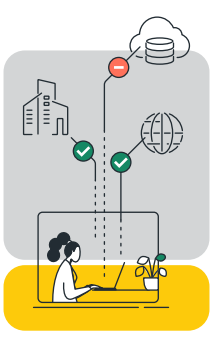


MPLS Bandwidth Costs Will Continue to Consume Your Budget

MPLS costs continue to eat up to a large portion of IT spend and will only grow in the future as applications generate more traffic and users use more video and other data-hogging media. MPLS was also never designed to deliver the direct-to-cloud performance needed by SaaS applications.

Widespread WFH is Here to Stay, and that's Harder on the Network and IT

Long after Covid-19 passes as a significant threat, people will continue to spend more time working at home and on the road than they did before. Providing the same performance, security, and user experience to home and mobile users is always challenging for IT. Supporting home and mobile users puts a more significant burden on IT than supporting users at the office.



A New Workforce Brings New Security Challenges

Organizations must also provide users working outside of the office and new kinds of users, such as consultants and contractors, with network access. At the same time, Ransomware and other network-based security threats are on the rise. Best practice today calls for restricting user access not only to the necessary applications and resources but varying access based on real-time parameters, such as location and device type. How will you deliver that kind of protection with your legacy network?

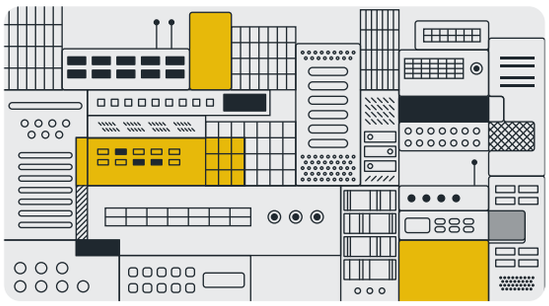
Rapid Expansion Globally and into New Regions Organically and Through M&A

If you're a typical growing organization, you can expect to open offices in new geographical regions and perhaps new countries and continents over the next few years. With major expansions and mergers and acquisitions, the pressure is on to integrate new locations and employees as quickly as possible. Regardless, how will you quickly open new locations when months are needed to deliver MPLS circuits and offices often sit in locations where MPLS access isn't even feasible?

New Demands Mean More Than Purchasing New Technologies

With each of these new demands comes organizational issues:

Hardware Appliances Constrain Growing Needs



You're going to have more users, which means you'll need more bandwidth to more sites. How will your network accommodate those changes? Eventually, network and security hardware appliances will reach the limit of users they can support, requiring expensive appliance upgrades and replacements.

Human Cost

Your organization will need the skills, time, and resources to secure and manage all of the new applications and services you'll be deploying in the next few years. That means either training staff to deepen its grasp on the new use cases it's responsible for, hiring new staff who already have that knowledge, or offloading these tasks to a third-party provider. Either way, it most likely means new budget expenditures.

The Telco Headache

The major carriers have never been easy to work with, and the headaches they cause are not likely to go away soon. The delays in opening and closing support tickets, the opaque nature of these massive organizations, and the general frustrations of getting someone there to take responsibility are likely to continue. Your frustrations will likely mount as you try to get feature requests fulfilled by telcos that resell rather than design and own the software and hardware.

What You Don't Know

The Time to Reach our ROI

You know all these things and the costs they incur. You still don't know the cost of moving away from MPLS and legacy networks in time, headcount, and resources; the best time to make that move; and how long it'll take to recoup those costs.

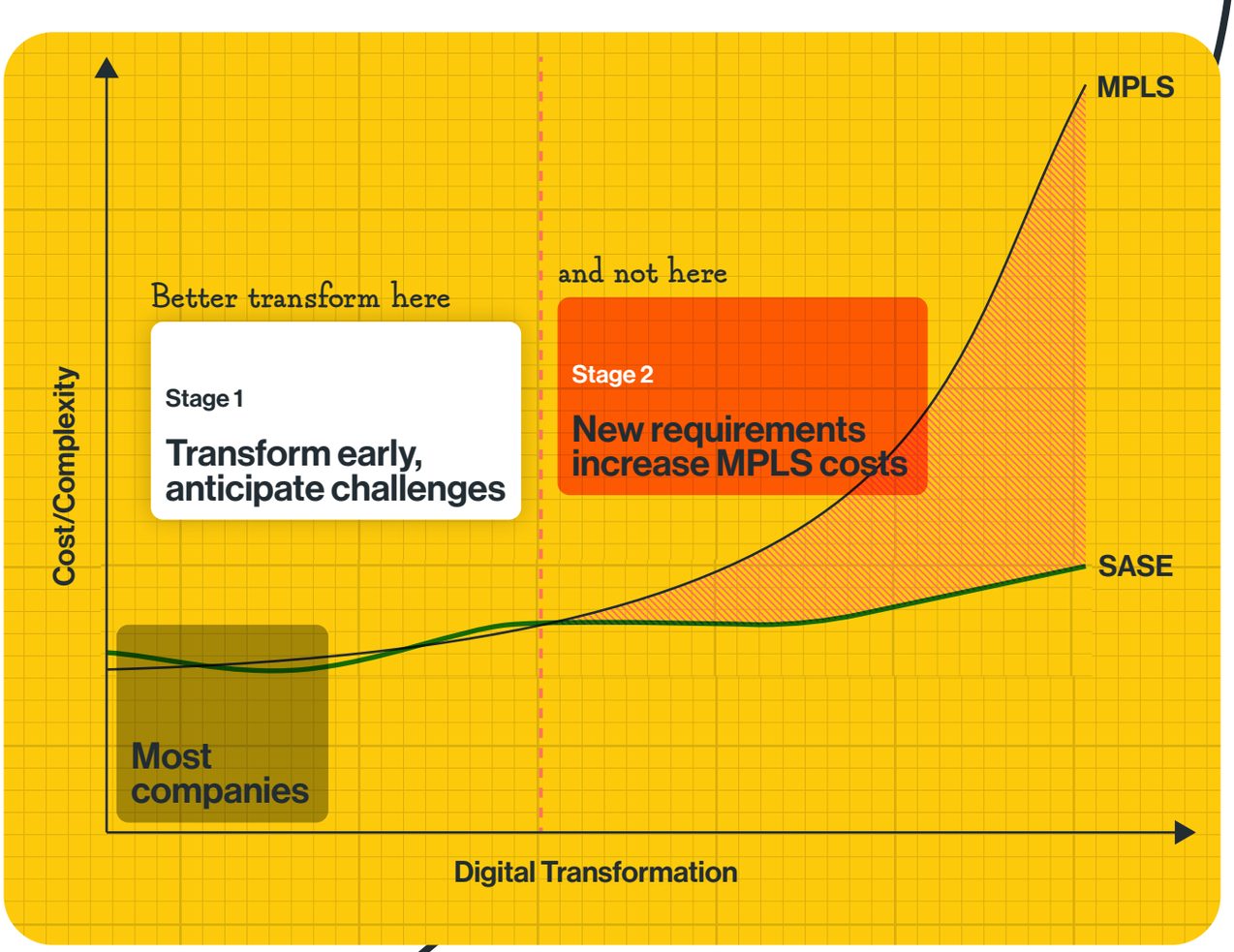
The Answer

Meet the Needs of Today and Those of Tomorrow

The answer is to put a strategy that enables you to address future challenges gracefully, without having to incur significant investment or headache.

Over time, legacy networks, such as MPLS, become more complex and costly to maintain as new challenges emerge.

MPLS bandwidth costs continue to consume a significant part of the budget. Deploying, managing, and securing MPLS can grow over time as you add new locations and workers. And MPLS is not a solution for serving cloud applications, connecting offices in international locations where it's either not available or too expensive, and certainly not for mobile and home user connectivity.



Most organizations lie in stage 1 of this graph, where MPLS costs consume a large but manageable portion of the IT budget. In this stage, a network transformation as your MPLS contracts expire requires much effort and might cost the same or more than you pay now. If this is true for you, you may feel you're in a peaceful state of equilibrium and don't need to act yet.

But what comes next? In stage 2, as requirements evolve with new locations, applications, and cloud services, your architecture will move to the right side of the graph. Your need for more staffing, resources, and time to manage the complexity of your network and security will accelerate. With every new solution comes the additional costs of evaluating, deploying, integrating, and managing that solution.

Why Act Now and Not Wait?

The worst thing to do is wait for stage 2 to make your network transition. Why?

Once you reach Stage 2, the time, money, and resources you spend coping with the complexity of your legacy solutions will constrain the time, money, and resources you have for addressing pressing new challenges. Make your transition during Stage 1, and the lack of constraints will ensure that your success and ROI will be faster and more dramatic.

For example, one study by Nemertes into an enterprise with a ~325 site network found that the company should realize $1M or more in hard-dollar savings every year starting the second year (and just under $1M in the initial, partial year). "They are adding Internet at each site — a doubling of bandwidth, typically — to accommodate growth, especially in use of cloud, and to provide redundancy, since 79% of sites have only one WAN link, currently," explains John Burke, Chief Technology Officer at Nemertes.

Imagine the problems that could be solved today if those funds could be diverted to digital transformation challenges.

It's about more than just costs, however. It's also about planning. The time to implement and plan digital transformation is when things are going well, not when you're busy putting out fires. With peace of mind, you can think through the issues more carefully and thoroughly and devise a strategy that meets today's needs and tomorrow's requirements.

How to Avoid Becoming a Stage 2 Company

The fact is whether it's for reasons of costs or agility, legacy networks are incompatible with the traffic requirements of digital transformation.

Avoiding becoming a Stage 2 company means implementing a strategy today that will prepare your network for digital transformation and make all the mentioned problems disappear, regardless if you're experiencing them now, or during the next MPLS cycle.

The question is, how do you do that?

"Current network security architectures were designed with the enterprise data center as the focal point for access needs. Digital business has driven new IT architectures like cloud and edge computing and work-from-anywhere initiatives, which have, in turn, inverted access requirements, with more users, devices, applications, services and data located outside of an enterprise than inside. The COVID-19 pandemic accelerated these trends."

Gartner®

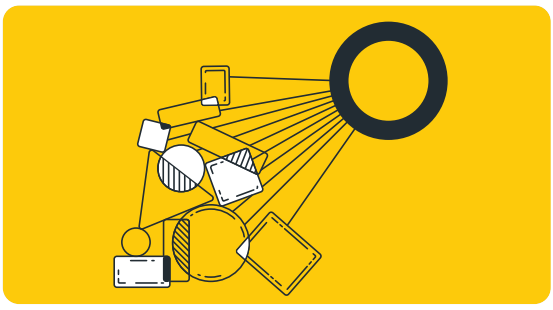
Leverage the Cloud to Meet the Needs of the Cloud

The industry has rallied around Gartner's SASE architecture as the best solution to meet the challenges introduced by the cloud, mobility, and other dynamic shifting network traffic. Why?

SASE is a cloud-native architecture that provides all enterprise users worldwide with secure access

Whether they are on the road, at the office, in Japan, or Spain—with fast, secure access to any enterprise resource, including cloud applications and the Internet.

SASE architectures come with a broad range of capabilities



Fast access, NGFW, IPS, MDR, and more. All capabilities can be enabled at once or gradually in stages where and when customers require them. All you have to do is activate each one on your dashboard.

SASE is infinitely elastic and can scale effortlessly to meet your organization's needs and requirements as they grow

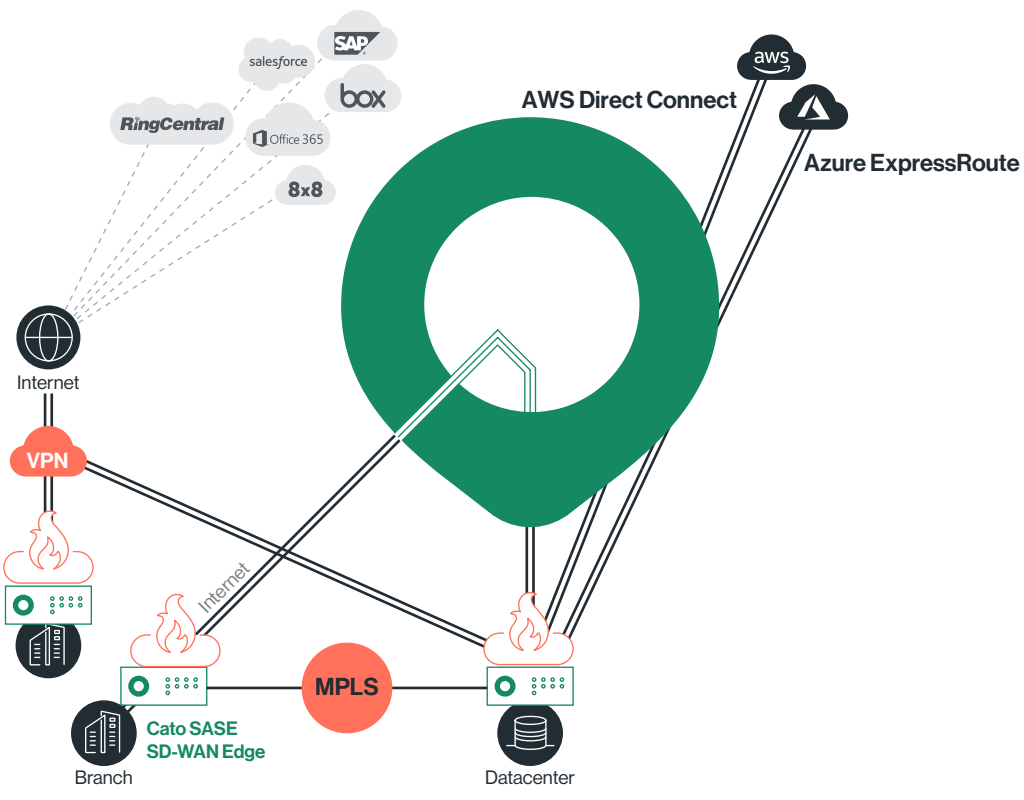
You no longer have to worry about the rigid scaling constraints of individual appliances and the pain of configuring, procuring, and paying for expensive appliance upgrades. The SASE cloud software automatically delivers the compute power needed to meet your requirements.

SASE Adoption: Think Strategically but Act Gradually

While SASE represents a shift in IT strategy, SASE implementation does not. SASE adopters find they can start gradually with SASE, incrementally growing their SASE deployment as contracts expire or new demands arise. Many can terminate MPLS contracts early to enjoy the full benefits of a SASE architecture sooner. Regardless, most enterprises end up future-proofing their networks today even while on their existing services.

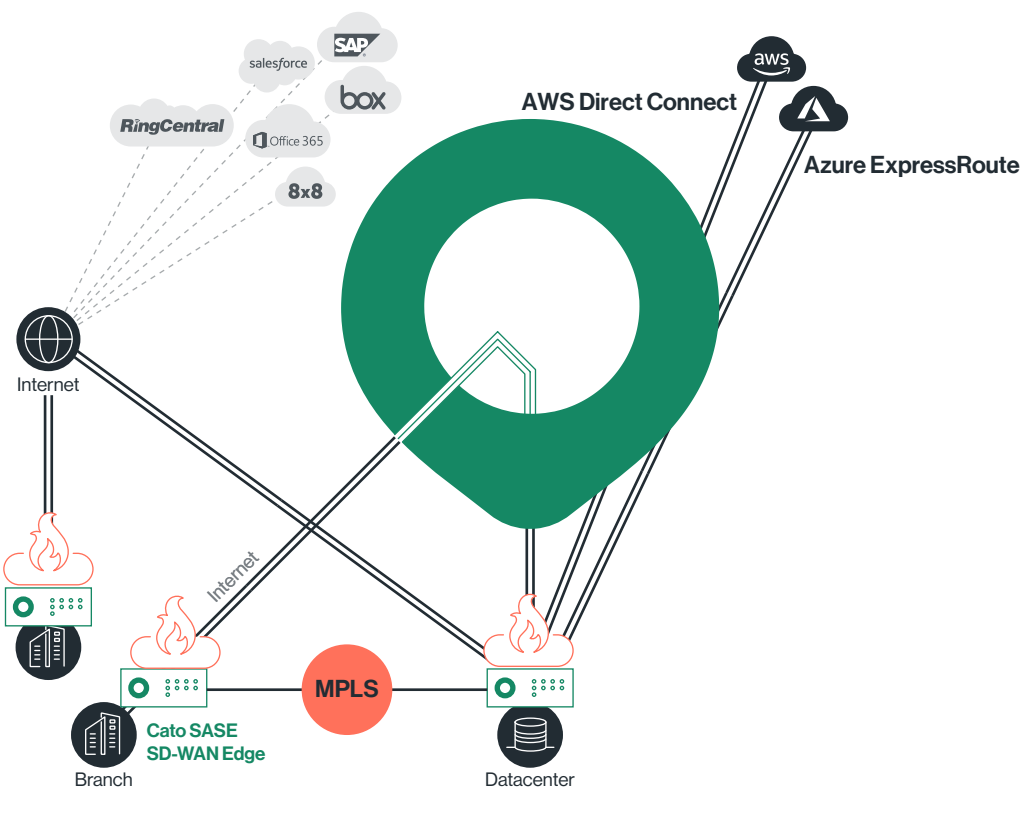
Step 1

No change. Deploy SASE SD-WAN devices solely to connect select sites to MPLS and the Internet. Applications will continue to move over MPLS. There is no alteration to the rest of the network or other resources



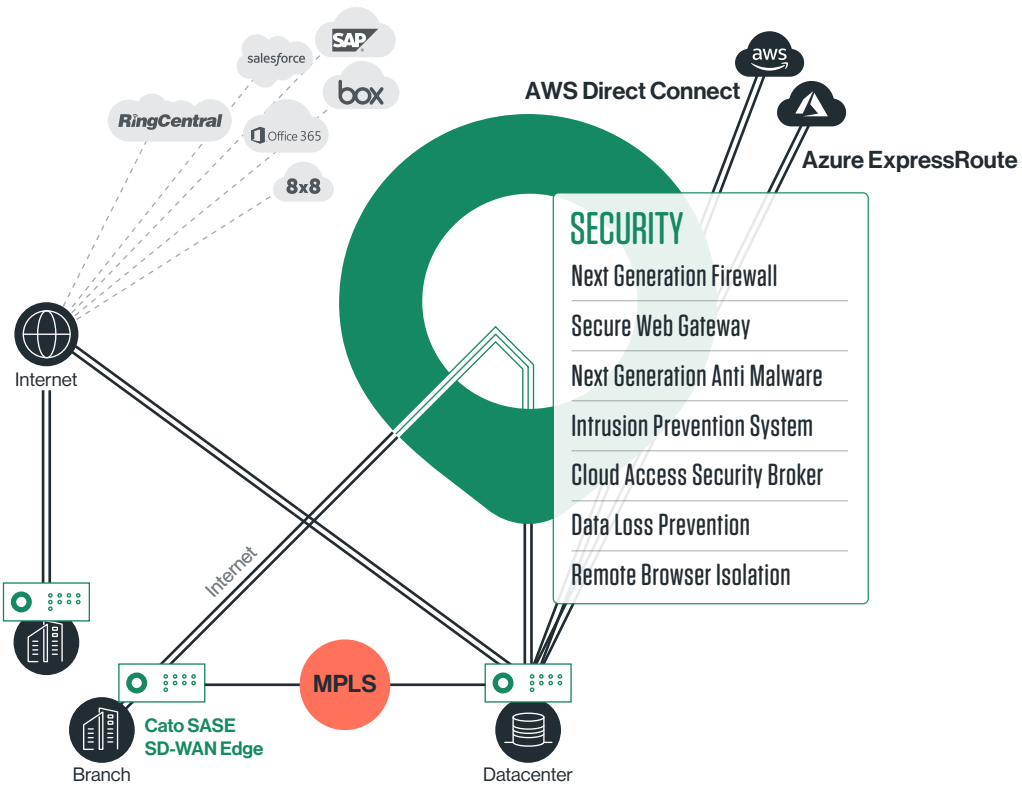
Step 2

Deploy SASE gradually to locations where MPLS is not available or is too expensive to be feasible in order to improve connectivity to WAN applications.



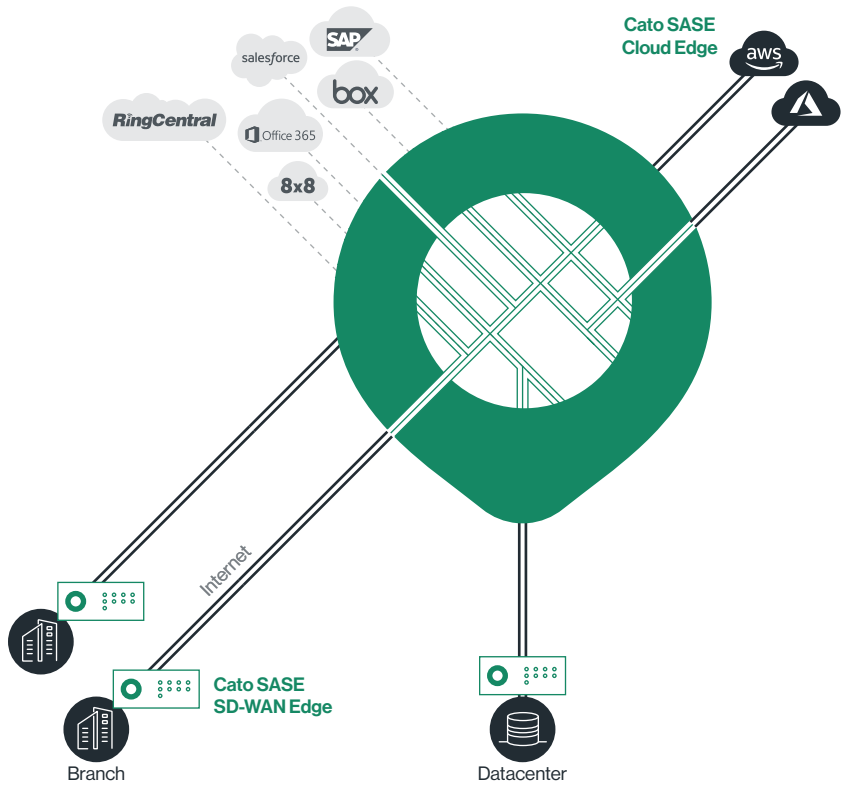
Step 3

Deploy SASE security functions such as NGFW, secure Web gateway, IPS, and anti-malware gradually as your existing appliances meet their end of life or scalability constraints, or to provide easy and effective edge security to new branch offices



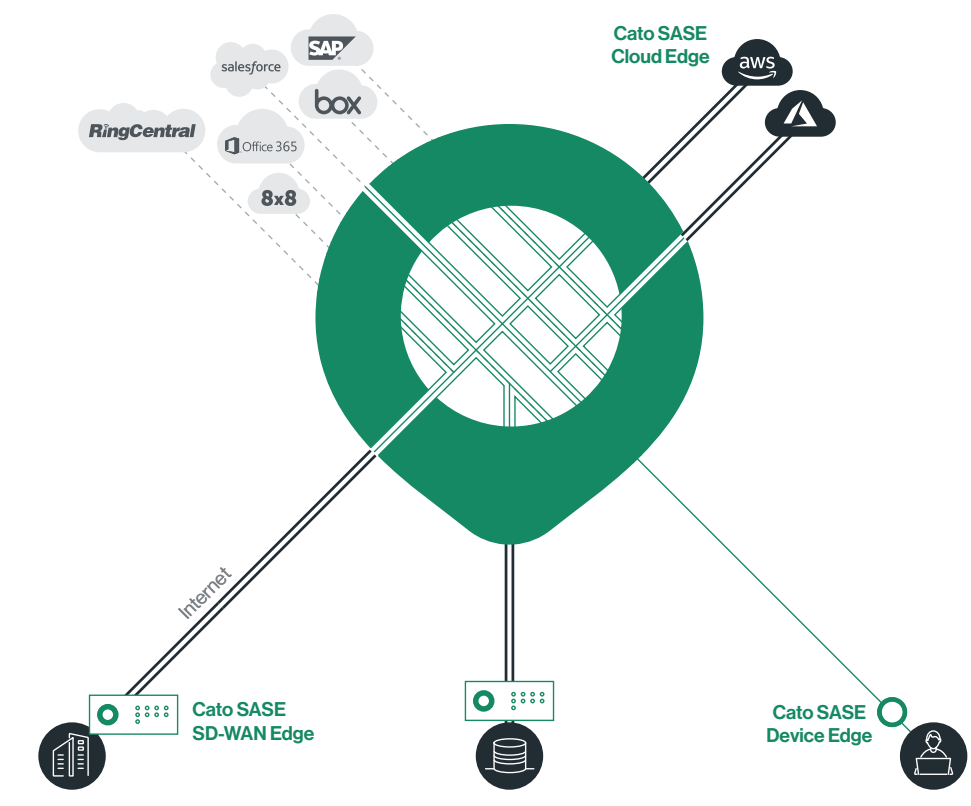
Step 4

Deploy SASE for optimized network access to cloud datacenters. SaaS applications can benefit from advanced routing rules that ensure traffic travels continuously across an optimized network, rather than the less reliable Internet. In some cases SASE PoPs are located within cloud datacenters for LAN like connectivity from the SASE to the cloud.



Step 5

Bring mobile and work from home users into the SASE cloud for optimized performance and secure access, eliminating all those VPN services, server purchases, and upgrades.



Bringing new locations gradually into the SASE is quick and effortless.

Bringing new locations gradually into the SASE is quick and effortless.

“We can set up new sites and VPN users in minutes or hours, and Cato’s agility is helping us adjust the network, bandwidth, and traffic prioritization easily as we migrate step-by-step to the cloud.”

Tobias Rölz, Executive Vice President, Market and Digital Services for Komax

Conclusion
Don't Fail to Act in Time

The important thing is to start planning your WAN transformation strategy, whether via testing, a partial installation, or a complete transition. If you don't start now:

1/ You'll continue to suffer the high cost of MPLS and operational costs of managing an army of siloed standalone appliances and external services

2/ Your costs will skyrocket as your MPLS network gets more complex and unwieldy

3/ High MPLS costs will constrain the resources and budget you have to make your network and digital transformation a success

4/ IT support will continue to suffer as network and security complexity increase

5/ You'll struggle to find the network agility to meet digital transformation requirements and achieve successful business outcomes

6/ The ROI of your network transition and digital transformation will be both lower and slower

MPLS COST

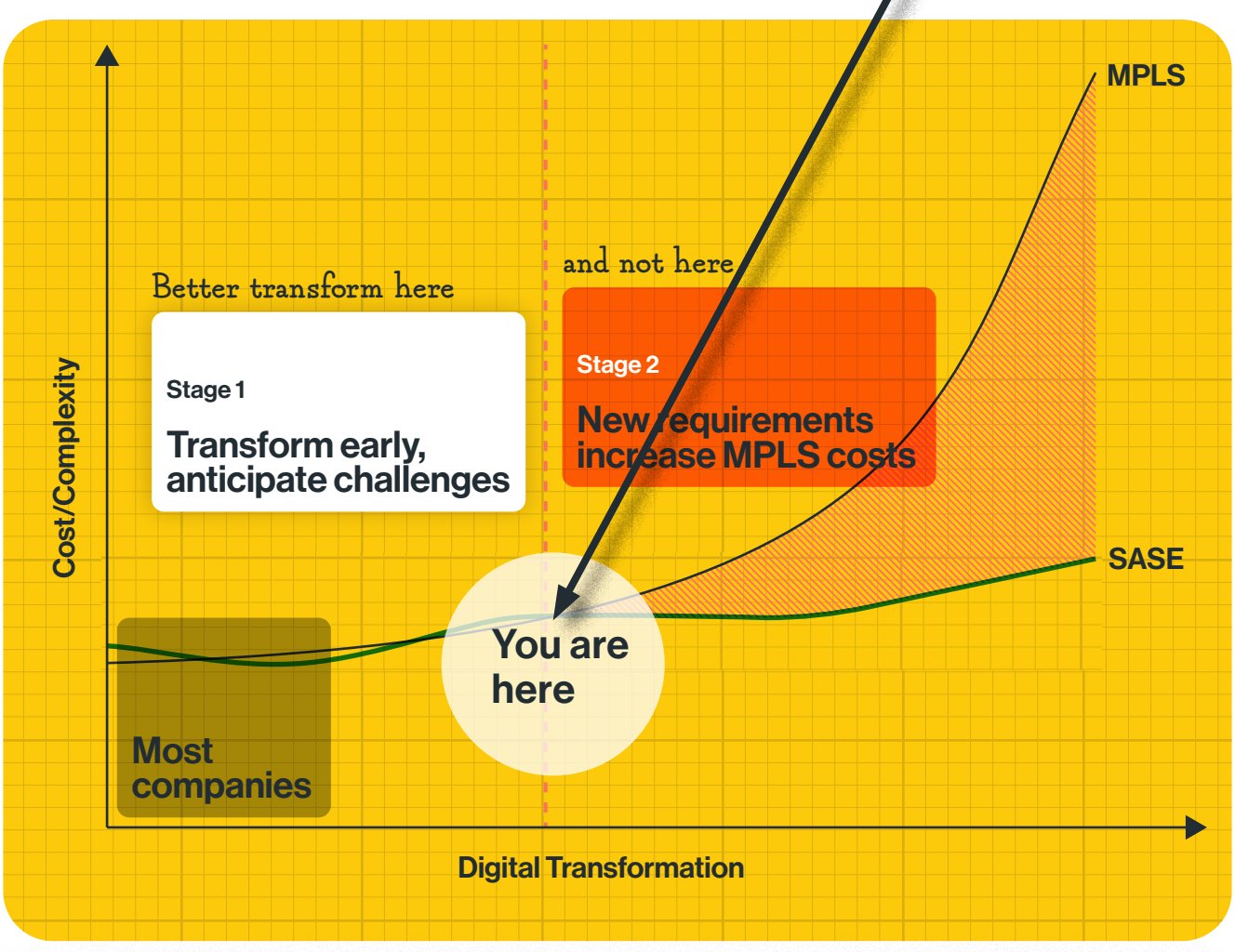
ROI

SASE ROI
How Do IT Leaders Justify the SASE Transition?

Justifying your SASE transition is about demonstrating dramatic reductions in complexity and cost. These savings eliminate expenditures on multiple services, network and security appliances, and related management costs.

For example, Figure 3 shows the cost of a WAN and security setup for a Cato customer before deploying Cato. The company had with offices running MPLS and VPN connections for users, locations, and cloud connectivity. Figure 4 shows how a simpler Secure Access Service Edge (SASE) solution slashed complexity down to two components—SASE and reverse proxy—for an annual cost of $490,000. Cato replaced the WAN connectivity and optimization, NGFW, IPS, secure Web gateway, MDR, and antimalware in the cloud for each location and client. It also replaces all those VPN services with a single Zero Trust Network Access (ZTNA) solution providing secure access to applications for remote mobile and home users worldwide, including China, and direct optimized access to applications in the cloud.

	Figure 3 Configuration and setup	Figure 4 Suggested solution
Service Cost Per Year		
Local physical firewalls license in high availability architecture in HQ offices	$50,000	Included in SASE
Reverse Proxy solution for publishing internal websites and services with a Single Sign On (SSO) system	$90,000	$90,000
VPN Solution for RnD teams for connection to AWS production environment	$50,000	Included in SASE
VPN Solution for China employees for connection to services	$25,000	Included in SASE
VPN solution for support, CSM and QA teams for connection with non-company IPs	$20,000	Included in SASE
Install MPLS/Direct Internet Access lines from offices to Center location (Allow connectivity for global services) $2,000 for each site	$240,000	Included in SASE
Secure Access Servise Edge (SASE) cloud Cato Service Fee		$400,000
Subtotal	$475,000	$490,000
Hardware Cost Per Year		
Local physical load balancing hardware for WAN optimization $40,000 + $20,000 for license and management per site	$60,000	Included in SASE
Three-year upgrade for firewalls worldwide to newer hardware and configured for high availability	$30,000	Included in SASE
Subtotal	$90,000	$0
Total	$565,000	$490,000



Similarly, Haulotte, a global manufacturer of lifting equipment with six plants and 30 locations across Western Europe, North America, South America, Africa, and the Asia Pacific, cut its network and security costs in half by switching from MPLS to a Cato SASE. During the Covid-19 crisis, it was also able to use the Cato SASE platform to transition 300 staff members to work from home in less than a day.

> **“We just dispatch the Cato Socket with a page of instructions to each location. Our local contact installs it at the site and then we take over remotely to finish the job. It’s truly plug-and-play.”**
>
> Haulotte Group CIO Thomas Chejfec

Useful SASE Links

The Total Economic Impact™ of Cato Networks

Forrester Consulting conducted a TEI study of Cato Networks for evaluating the impact and ROI of Cato's SASE cloud.

How to Terminate your MPLS Contract Early

Practical advice for interpreting your MPLS contract and transitioning from MPLS to SASE today, even if you're still under contract with your MPLS provider.

SASE RFP Template

A list and description of criteria you can include in your RFP to assess if a vendor provides a true SASE platform and meet your business, project, and budget requirements.

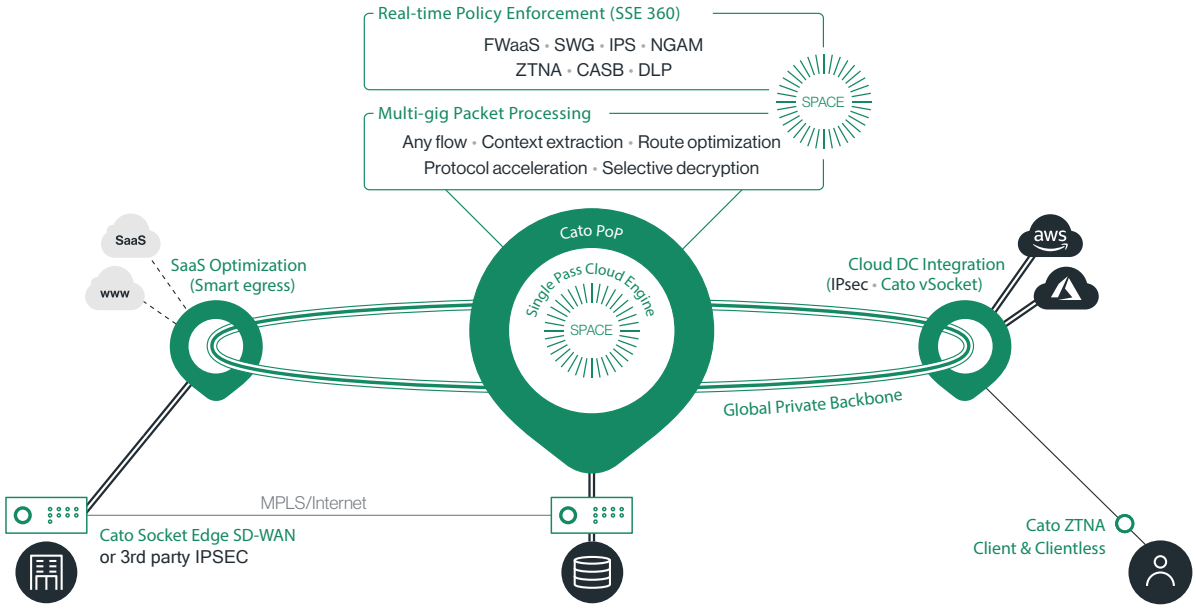
Your First 100 days of a CIO

5 Steps to Success Specific steps you should take in your first hundred days as CIO to make your mark, boost digital transformation, and more, rather than chasing your tail and putting out fires.

About Cato Networks

Cato provides the world's leading single-vendor SASE platform, converging Cato SD-WAN and a cloud-native security service edge, Cato SSE 360, into a global cloud service. Cato SASE Clou`d optimizes and secures application access for all users and locations everywhere. Using Cato, customers easily replace costly and rigid legacy MPLS with modern network architecture based on SD-WAN, secure and optimize a hybrid workforce working from anywhere, and enable seamless cloud migration. Cato enforces granular access policies, protects users against threats, and prevents sensitive data loss, all easily managed from a single pane of glass. With Cato your business is ready for whatever's next.

Cato SASE Cloud with SSE 360



Cato SASE Cloud

- SSE 360
- Secure Remote Access
- Edge SD-WAN
- Global Private Backbone
- Multi-cloud / Hybrid-cloud
- SaaS Optimization
- Cato Management Application

Use Cases

- MPLS Migration to SD-WAN
- Secure Remote Access
- Secure Branch Internet Access
- Optimized Global Connectivity
- Secure Hybrid-cloud and Multi-cloud
- Work From Home

Cato. Ready for Whatever's Next.

SASE, SSE, ZTNA, SD-WAN: Your journey, your way.