SOLUTION BUILDERS®

A SOLUTION BUILDERS PLAYBOOK
2026 EDITION

A PLAYBOOK FOR MULTI-SITE AND REMOTE FIRST BUSINESSES

The Modern Network Playbook.

MPLS versus SD-WAN decoded, how application aware routing keeps calls clear, a failover design that works at 2 a.m., and security built into the network itself.

INSIDE THE PLAYBOOK

01 MPLS vs SD-WAN

02 Application aware routing

03 Automatic failover

04 Security in the network

Published by Solution Builders
Bloomington, Minnesota · www.solutionbuilders.com

30+ YEARS

Top 1% OF MSPS

98% CSAT

WHAT'S INSIDE

Built for companies whose work no longer lives in one building.

Your applications moved to the cloud. Your people moved home, to branch offices and to job sites. Your network is still wired for a headquarters that everything used to flow through. This playbook shows how to replace that wide area network with one fast, resilient, secure fabric.

01 **MPLS vs. SD-WAN, decoded.**
What MPLS gave you, what it costs you now, and how SD-WAN turns fiber, broadband and LTE into one managed fabric without giving up reliability.
PAGE 03

02 **How application aware routing works.**
The mechanics behind the magic: how the network recognizes a Teams call, measures every path, and moves the call before anyone hears a glitch.
PAGE 06

03 **Designing for automatic failover.**
Why "we have two internet connections" is not a failover plan, the five ways redundant networks still go down, and a design you can draw on a napkin.
PAGE 09

04 **Building security into the network.**
Why the branch firewall and the full tunnel VPN are the weak spots now, and how SASE, zero trust access and segmentation put security in the path itself.
PAGE 12

WHO IT IS FOR
Owners, operations leaders, finance leaders and IT managers at companies with two or more locations, or a workforce that rarely sits in one.

HOW TO USE IT
Start with the chapter that matches your pain: cost, call quality, outages or security. Each ends with sources you can share with leadership.

READING TIME
About 25 minutes cover to cover. The failover checklist in chapter 03 is built to hand to whoever designs your next site.

SOLUTION BUILDERS®

01

MPLS vs. SD-WAN, decoded.

For twenty years MPLS was the safe answer for connecting offices. It is still reliable. It is also expensive, slow to change and blind to the cloud, which is where your applications went. This chapter explains what SD-WAN replaces, what it does not, and how to decide.

54%
of significant outages cost more than $100,000, and 16% cost over $1 million

#1
cause of IT service downtime over the last three years: network related problems

89%
of organizations now run a multi cloud strategy, so traffic no longer flows to one data center

38%
infrastructure cost cut by a 60 user, multi-location architecture firm that went cloud native

MPLS connects offices. SD-WAN connects your business.

MPLS is a private circuit from one carrier, priced by the megabit and built to haul everything back to headquarters. SD-WAN is software on top of any circuits you choose. It measures them constantly and sends each application down the best one.

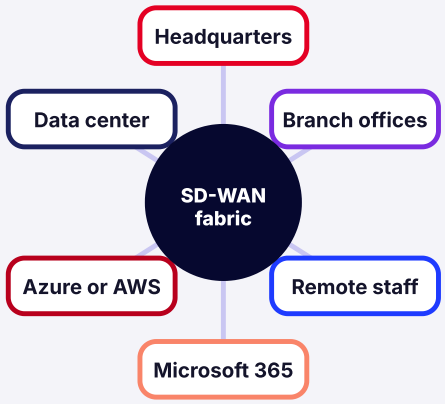
Side by side

	MPLS	SD-WAN
Transport	One carrier, private circuit	Any mix: fiber, cable, LTE, 5G, even old MPLS
Cost per megabit	**Premium, fixed term contract**	**Commodity bandwidth, month to month**
Time to add a site	**60 to 120 days, carrier dependent**	**Days. Ship a device, plug in broadband**
Path to Microsoft 365	**Backhauled through headquarters**	**Direct from every site, with security applied**
Failover	**Manual or minutes**	**Automatic, under a second**
Visibility	**A monthly carrier report**	**Per application, per path, in real time**

What SD-WAN does not do

- **It does not make bad circuits good.** It routes around them. Two weak links are still two weak links.
- **It does not replace security.** It carries it. Chapter 04 covers what has to ride along.
- **It does not require ripping out MPLS on day one.** Most firms run both for a quarter, then let the contract lapse.

Every site and every cloud, one fabric



Why the cloud broke MPLS

MPLS was designed when applications lived in your server room. Today a branch user opening Teams on MPLS travels to headquarters, out to Microsoft, and back the same way. SD-WAN sends that traffic straight out the local door, inspected.

> **The question is no longer whether to leave MPLS. It is what you keep paying for while you decide.**
>
> SOLUTION BUILDERS NETWORK PRACTICE

The real cost of MPLS is not the invoice. It is the wait.

The per megabit premium is easy to see on the bill. Harder to see is the new office that ran on hotspots for three months, the acquisition that waited a quarter for a circuit, and the calls that cross the state twice to reach the next town.

WEEKS 1 TO 2

Discover

Inventory circuits, contracts, sites, applications and real traffic.

WEEKS 3 TO 4

Design

Pick transports per site, write application policies, size the edges.

WEEKS 5 TO 6

Pilot

Two sites run SD-WAN beside MPLS. Measure calls, failover, experience.

WEEKS 7 TO 10

Roll out

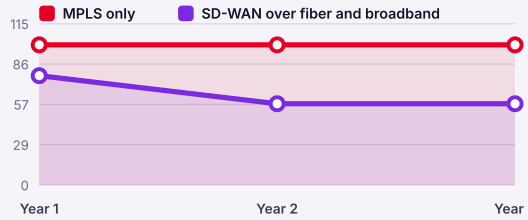
A site or two per day. Local breakout turns on as each one cuts over.

WEEKS 11 TO 12

Retire

MPLS circuits come off as contracts allow. Savings start that month.

Three year wide area network cost, 8 sites



Indexed, MPLS year one = 100. Year one includes edge devices and migration. Illustrative planning assumption, not a quote.

3x

remote productivity at a multi-location architecture firm, cloud native

0

on premises servers left at that firm today

Keep, blend or replace

YOUR SITUATION	OUR USUAL ADVICE
MPLS contract ends within 12 months	Replace. Design now, cut over as it lapses
Multi year MPLS term remaining	Blend. Add SD-WAN on top, shed MPLS later
Plant or clinic with latency sensitive gear	Blend. Keep the private circuit where it is proven
Sites running on hotspots or consumer gear	Replace. Nothing to protect, only to fix

Bring the CFO a different number

Do not pitch SD-WAN as cheaper bandwidth. Pitch the end of carrier lead times, a network that reaches any new site in days, and the first honest view of your traffic.

Sources: Uptime Institute Annual Outage Analysis 2023 (outage cost) and 2022 (network related causes); Flexera State of the Cloud Report 2024 (multi cloud adoption). Client outcomes from a Solution Builders engagement, 60 users, multi-location architecture firm. Cost chart is an illustrative planning model.

02

How application aware routing works.

Old networks treat every packet the same and send it down one path until that path dies. Application aware routing knows a payroll upload from a video call, measures every circuit every second, and steers each application in real time. Here is how it works and how to set the rules.

150 ms
one way delay ceiling for a voice call to sound natural, per ITU recommendation G.114

1%
packet loss is enough to drop words from calls and freeze video

30 ms
jitter ceiling before real time audio starts to break up

4
things every path is measured on, constantly: latency, loss, jitter and availability

Identify the app, measure every path, steer in real time.

Four things happen to every new session that crosses an SD-WAN edge, in a few milliseconds. Understanding them is what lets you set policies in business terms instead of router syntax.

1

Identify

The edge recognizes the application by its signature, not its port. Teams is Teams, not "encrypted web traffic." Thousands of apps are known out of the box.

2

Measure

Tiny probe packets cross every circuit continuously, scoring each one for latency, loss, jitter and availability.

3

Decide

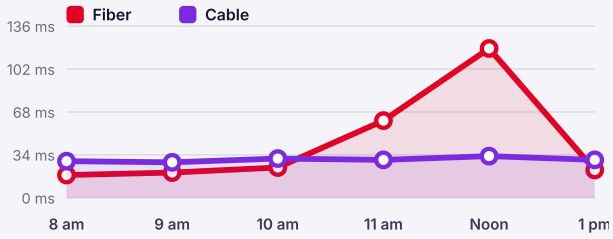
Each application class has a policy: what quality it needs, which paths it may use, what it gets when things degrade.

4

Steer

The session lands on the best qualifying path. If that path slips below threshold, it moves, mid call, without a drop.

Latency on two circuits during one morning



Illustrative. At 10:30 a carrier issue degrades the fiber circuit. Voice and video move to cable automatically and move back when fiber recovers.

What a user experiences

Nothing. That is the point. The call that would have turned into robot voice on a single circuit stays clear. The only evidence is a line in the dashboard showing 40 minutes on the secondary path.

1 sec

typical probe interval on every circuit, all day long

40 min

on the cable circuit above, with nobody noticing

> **Old networks fail over when a cable dies. Modern ones fail over when a call starts to sound bad.**
>
> SOLUTION BUILDERS NETWORK PRACTICE

Not every packet earns the fast lane.

The payoff of application awareness is a policy you can read out loud at a leadership meeting. Five classes cover almost every company we see. Write them down, agree on them, and the network enforces them at every site.

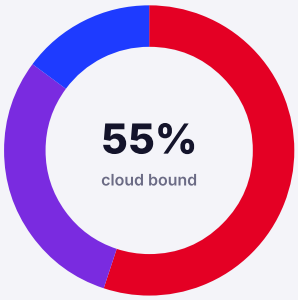
A policy your CFO can read

CLASS	EXAMPLES	POLICY
Voice and video	Teams, Zoom, desk phones	Lowest latency path, protected bandwidth, moves first when quality drops
Core business apps	Microsoft 365, ERP, CRM, EHR	Best available path, failover in under a second
Bulk transfer	Backups, updates, replication	Cheapest path, rate limited during business hours
Guest and personal	Streaming, personal phones	Separate segment, capped, never on the private path
Management and security	Monitoring, EDR, logging	Guaranteed small slice on every path, always

The rule that saves the most calls

Reserve bandwidth for voice and video before anything else gets a byte. A single Windows update at the wrong moment has ruined more sales calls than any carrier outage.

Where branch traffic goes today



- SaaS and cloud 55%
- General internet 30%
- Your data center 15%

Illustrative mix for a typical multi-site business. Backhauling all of it to headquarters is the hidden cost of a legacy WAN.

Three policy mistakes we see

- **Everything is priority one.** Then nothing is. Keep voice and video alone at the top.
- **Backups run during lunch.** Rate limit them or schedule them, or they will eat the afternoon.
- **Guest Wi-Fi shares the staff segment.** Separate it today. It takes an hour.

Sources: ITU recommendation G.114 (one way delay for voice); Cisco quality of service design guidance (loss under 1%, jitter under 30 ms for real time traffic); Solution Builders network design practice. Traffic mix and latency chart are illustrative.

03

Designing for automatic failover.

Every multi-site business has a story about the day the internet died and the phones went with it. Most of them had a backup circuit. It was in the same conduit, from the same carrier, plugged into the same router, and nobody had tested it. This chapter is about making the backup real.

$300K+

cost of one hour of downtime, reported by over 90% of mid size and large enterprises

< 1 sec

failover target for voice and video, versus minutes with traditional routing

2

carriers on two physical paths is the minimum. Two circuits from one carrier is one circuit

100+

hours of monthly downtime eliminated for an 85 user manufacturer within 90 days

Redundancy is not two cables into the same hole.

Networks rarely fail in interesting ways. They fail in the same five ways, over and over. Each one has a design answer that costs far less than the outage it prevents.

Five ways "redundant" networks still go down

01 Same conduit

Two circuits from two carriers, one trench into the building. A backhoe takes both. Ask for diverse entry or add wireless.

02 Same carrier underneath

Your second provider resells the first one's last mile. Ask who owns the fiber, not who bills you.

03 Single edge device

Two circuits into one router or firewall. When it reboots, so does the site. Pair devices wherever downtime is not an option.

04 No power plan

The modem is not on the UPS, or the UPS died two years ago. Put everything in the path on protected power and test it quarterly.

05 Failover never tested

Configured in 2021, changed six times since. Pull the primary cable twice a year, on purpose, during business hours.

Symptom and design answer

WHAT YOU SEE	DESIGN ANSWER
Both circuits down at once	Diverse physical paths, plus LTE or 5G
Calls drop at every failover	Sub second steering, not router level failover
Site goes down when the firewall updates	Paired edge devices, rolling updates
HQ outage takes every branch down	Local internet breakout at each site
Nobody knew for 40 minutes	Human monitoring, 24/7, that calls you

Ask the backhoe question

For every site, ask: if a backhoe cuts the fiber on the street, what still works? If the answer involves someone driving over with a hotspot, you have one circuit.

60%

fewer support tickets at that 85 user manufacturer once the network stopped flapping

2x

per year is how often a failover path should be tested on purpose

1

line item, not a plan: a backup circuit nobody has ever unplugged

A failover design you can draw on a napkin.

Here is what should happen in the first minute after a fiber cut at a well designed site, and the checklist that makes it happen. Nothing on this page requires exotic hardware. It requires decisions made before the cut, not after.

0 SEC

Loss detected

Probes on the fiber path stop returning. The edge marks it down.

< 1 SEC

Calls steered

Live Teams calls and desk phones move to cable or LTE. No drop.

5 SEC

Everything moved

Core apps and bulk traffic follow. Users notice nothing, or a pause.

1 MIN

Humans alerted

The operations center sees the event and opens a carrier ticket.

RESTORED

Automatic fail back

Fiber returns. After a clean quality window, traffic moves back.

Failover design checklist

- [x] Two carriers, two physical entries, verified by asking who owns the last mile.
- [x] Cellular (LTE or 5G) as a third path at every site that takes phone calls.
- [x] Paired edge devices at headquarters and at any site with more than 25 people.
- [x] Local internet breakout at every site, so no branch depends on headquarters being up.
- [x] Everything in the path on protected power: modems, edges, switches, phones.
- [x] A documented failover test, run twice a year, with results sent to leadership.

Transport mix by site type

SITE	PRIMARY	BACKUP	THIRD
Headquarters	Dedicated fiber	Second carrier fiber	LTE or 5G
Branch office	Fiber or cable	LTE or 5G	Optional
Plant or warehouse	Fiber	Fixed wireless	LTE or 5G
Home office	Home broadband	Phone hotspot	None

< 1 sec

from loss detected to calls moved, the number to put in the contract

3

paths at any site that takes customer calls: wired, wired, wireless

Local internet breakout

Each site reaches Microsoft 365 and the internet through its own door, with the same security policy at the edge. A headquarters outage stays a headquarters problem.

Sources: ITIC 2024 Hourly Cost of Downtime Survey; Solution Builders client engagement, 85 user manufacturer (downtime and ticket reduction); Solution Builders network design practice. Failover timings are design targets for a correctly built site.

04

Building security into the network.

The old model put a firewall at the edge of each office and a VPN in front of remote staff. Attackers noticed. Today the fastest growing way into a company is an exploited edge device. This chapter shows how a modern network carries its own security, with one policy applied everywhere.

180%
growth in breaches that began with an exploited vulnerability, year over year

38%
of intrusions investigated by Mandiant started with an exploit, the top initial access vector

2019
the year Gartner coined SASE: networking and security delivered together as a cloud service

0
implicit trust in a zero trust network. Every user and device proves itself, every session

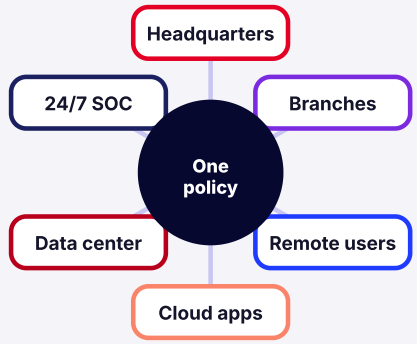
Security belongs in the path, not at the perimeter.

Five layers turn a wide area network into part of your defense. Each replaces something you are probably still running. Together the industry calls them SASE, secure access service edge: one policy, every site, every user.

The five security layers of a modern network

LAYER	WHAT IT DOES	WHAT IT REPLACES
Encrypted overlay	IPsec tunnels between every site and cloud, keys rotated for you	Trusting the carrier
Segmentation	Guest, IoT, plant gear, finance and servers kept apart	One flat network
Zero trust network access	Access per application, tied to identity and device health	The full tunnel VPN
Firewall as a service	Cloud inspection, one policy for every site and remote user	A firewall per office
Central policy and logging	One console for every edge, every event sent to the SOC	Per device configs

Every edge enforces the same rules



Why the VPN has to go

A VPN appliance is a door on the internet with a password. Whoever holds that password is inside. Zero trust access opens one app at a time and checks the device first.

PERIMETER MODEL

How most networks still work

- A firewall at each office, each configured a little differently.
- Remote staff on a full tunnel VPN with access to everything.
- Cameras and printers on the same flat network as finance.

BUILT IN MODEL

How a modern network works

- One policy, pushed to every edge and every remote device.
- Access per application, tied to the person and their device.
- Segments that keep a hacked camera from reaching a server.

Four moves that make the network part of your defense.

You do not need to do all of this at once. Do it in this order. Each move stands on its own, pays off immediately, and makes the next one easier.

1

Segment first

Separate guest, IoT, plant equipment and servers from staff devices. It is mostly configuration, it takes days, and it limits every breach that follows.

2

Retire the VPN

Move remote staff to zero trust access, application by application. Start with email and the ERP. Decommission the appliance when the last app moves.

3

Move inspection to the cloud

Firewall, web filtering and data loss prevention as a service, so a user in a coffee shop gets the same protection as one at headquarters.

4

Feed the SOC

Every edge, every segment, every denied connection logs to the security operations center. The network becomes a sensor, not just a pipe.

Where to start



Illustrative. The top left quadrant is a week of work. The top right is where the VPN finally dies.

> **The best firewall is a network where a stolen laptop password gets an attacker exactly one application, and a very loud alert.**
>
> SOLUTION BUILDERS SECURITY PRACTICE

Network security checklist

- [x] Every site to site and site to cloud path is encrypted, with no exceptions for "internal" links.
- [x] Guest, IoT, cameras and plant equipment cannot reach servers or staff devices.
- [x] Remote access is per application and checks device health before connecting.
- [x] Web filtering and DNS protection follow the user, in and out of the office.
- [x] Edge device firmware is patched within 14 days of a critical advisory.
- [x] Network logs flow to a security operations center staffed around the clock.

Sources: Verizon 2024 Data Breach Investigations Report (vulnerability exploitation growth); Mandiant M-Trends 2024 (initial infection vectors); Gartner, The Future of Network Security Is in the Cloud, 2019 (SASE); NIST SP 800-207, Zero Trust Architecture. Matrix is illustrative.

A network that is managed, not just installed.

Solution Builders has connected Minnesota businesses since 1995. Our SD-WAN practice is built on the RISE framework, delivered by 50+ engineers and watched by a 24/7 security operations center.

R

Resilient

Multi path sites with automatic failover, so a cut cable never becomes a lost day.

I

Integrated

One fabric across offices, remote staff, Microsoft 365 and your cloud platforms.

S

Secure

Zero trust access, segmentation and cloud inspection, monitored around the clock.

E

Evolving

A network that already has the bandwidth, policy and visibility your AI tools will need.

01

Network Readiness Snapshot

A 30 minute conversation about your sites, circuits and contracts. You leave with a candid read and the three things to fix first.

FREE · 30 MINUTES

02

SD-WAN Design and Pilot

Discovery across every site, a transport and policy design, and a two site pilot measured against your current network.

FIXED FEE · 4 WEEKS

03

Managed Network Service

Everything in this playbook, run for you: circuits, edges, policy, failover testing, security and 24/7 monitoring.

MONTHLY · ONGOING

Find out what your network is costing you in 30 minutes.

Book a free Network Readiness Snapshot with a Solution Builders solution architect. No pitch, just a clear read on your sites, circuits and risk.

Book my network snapshot

THE SHORT VERSION

Three things to remember.

If this playbook disappears into a drawer, keep these three ideas. They are the difference between a network that follows your business and one that holds it back.

01 **MPLS is a product. SD-WAN is a strategy.**

Any circuit, any site, one policy. The savings are real, but the speed to open a site and see your traffic is the point.

02 **Route by application, not by cable.**

Measure every path constantly and move voice and video before anyone hears it. Write the policy in business terms.

03 **Redundancy is tested or it is imaginary.**

Two carriers, two paths, local breakout, protected power, and a plug pulled on purpose twice a year.

SOLUTION BUILDERS®

START THE CONVERSATION

www.solutionbuilders.com

(952) 854-8188 · 1550 American Blvd East, Suite 900, Bloomington, MN 55425
Your technology partner since 1995

Book a free assessment

© 2026 Solution Builders, Inc. All rights reserved. Product names and marks are the property of their respective owners. Figures marked illustrative are planning estimates, not guarantees.