SOLUTION BUILDERS®

A SOLUTION BUILDERS WHITEPAPER
2026 EDITION

A WHITEPAPER FOR IT DIRECTORS AND OPERATIONS LEADERS

The IT Director's Guide to Supporting Multiple Locations.

Architecture, connectivity, and support models that scale cleanly past your second site.

INSIDE THE WHITEPAPER

01 Architecture
02 Connectivity
03 Support models

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

30+	Top 1%	98%
YEARS	OF MSPS	CSAT

WHAT'S INSIDE

The second site is where IT models break.

One office is easy to run by hand. Two offices is where the shortcuts stop working: the server closet becomes two, the help desk becomes a travel schedule and the network becomes a tangle of point solutions. This whitepaper lays out the three decisions that let IT scale to five, ten or fifty sites without multiplying the work.

01 **Design for many sites, not one site many times.**
Why copying your headquarters to every location fails, and the identity first, cloud centric pattern that scales instead.
PAGE 03

02 **Connect every site like it is the only site.**
Why MPLS era thinking fails cloud first businesses, how SD-WAN turns cheap circuits into a resilient fabric and how to design failover nobody notices.
PAGE 06

03 **Support fifty sites with the team you have.**
Centralized help desk, smart hands, local champions and the co managed model. How to tier support so every site gets what it needs without a technician in every building.
PAGE 09

WHO IT IS FOR
IT directors, IT managers and operations leaders at companies opening a second site, or already juggling several.

HOW TO USE IT
Three chapters, three decisions: how you build sites, how you connect them and how you support them. Each ends with sources.

READING TIME
About 20 minutes. The readiness scorecard in chapter 03 is built to take into your next planning meeting.

01

Design for many sites, not one site many times.

Most multi-site problems start on day one of the second site, when someone copies the headquarters design: a server, a file share, local accounts and a firewall somebody configured by hand. The pattern that scales is the opposite. Decide once, centrally, and make every site a copy of that decision.

1
identity directory, one policy set, one image for every site

0
servers a new site needs when identity, files and apps are in the cloud

2
hours of lead time to stand up a standardized "site in a box" network kit

80%
of multi-site support tickets trace to inconsistency between sites, Solution Builders client data

Identity first, cloud centric, standardized to the port.

Three principles do most of the work. Identity lives in one place and follows the user. Data and applications live in the cloud or in one well connected core, never in a closet. And every site is built from the same kit, the same configuration templates and the same naming scheme.

01 **One identity for everyone**

A single directory (Entra ID for most organizations) with MFA and conditional access. A user hired in one site can sit down in any other and work. No local accounts, no per site domains.

02 **Data in the core, not the closet**

Files in SharePoint or a central file service, line of business apps hosted centrally or as SaaS. Local caches are fine. Local masters are how data gets lost and backups get skipped.

03 **Site in a box**

A standard kit per site size: firewall, switch stack, access points, printer and a cellular backup. Pre configured from templates so a new site is a shipping label, not a project.

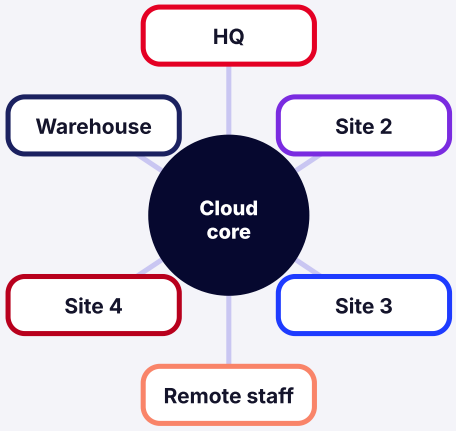
04 **Configuration as a template**

Every firewall rule, VLAN and Wi-Fi network defined once and pushed from a cloud console. A change to the standard reaches every site the same afternoon.

05 **Zones that travel**

The same network zones at every site: staff, guest, devices, building systems, vendor. Security policy is written once because the zones are identical everywhere.

Sites connect to a core, not to each other



The test for any site design

Could you open a new location next month by shipping a box and emailing a login? If the answer involves a server, a site visit from your best engineer and a week of configuration, the design does not scale.

> **Standardization is not about limiting sites. It is about making the hundredth site as boring as the second.**
>
> SOLUTION BUILDERS INFRASTRUCTURE PRACTICE

Three site sizes, three kits, one standard.

Not every site needs the same hardware, but every site needs the same design. Most organizations land on three tiers, and the tier decides the kit, the connectivity and the support model for that location.

Site tiers

TIER	TYPICAL PROFILE	NETWORK KIT	CONNECTIVITY	LOCAL IT PRESENCE
Tier 1 · Core	HQ or primary plant, 75+ users, critical systems	Redundant firewalls, core and access switches, dense Wi-Fi	Two diverse circuits plus cellular	On site engineer or co managed team
Tier 2 · Branch	15 to 75 users, office or production	Single firewall, switch stack, Wi-Fi 6E	Primary circuit plus broadband or cellular	Remote support, scheduled visits, local champion
Tier 3 · Micro	Under 15 users, retail, clinic, depot	Integrated firewall and Wi-Fi, small switch	Broadband plus cellular failover	Fully remote, smart hands on call

Standards every site inherits

- Naming convention for sites, devices and networks, documented and enforced by template.
- Identical VLAN and zone design, with the same policy between zones everywhere.
- Cloud managed firewall, switching and Wi-Fi so configuration and monitoring are central.
- Printing, conferencing and endpoint images chosen once for all sites.
- A spares kit per tier, staged regionally, so a failed switch is a swap, not an outage.

3

tiers cover almost every real world site

1

console for every firewall, switch and access point

What to centralize and what to leave local

Centralize identity, data, security policy, monitoring and purchasing. Leave local what physics requires: printing, badge readers, production equipment and the one person who knows where the network closet key is.

Sources: Microsoft Entra ID and Zero Trust deployment guidance; CISA Cross Sector Cybersecurity Performance Goals; Solution Builders multi-site client data (tier model and ticket analysis).

02

Connect every site like it is the only site.

Connectivity used to mean a private circuit from every site back to headquarters, because that is where the servers were. Now the servers are in the cloud, the users are everywhere and the headquarters is just another site. The network has to follow that reality.

2
independent paths per site is the minimum for business continuity

< 1 sec
failover time a well designed SD-WAN fabric delivers between paths

30 to 50%
typical WAN cost reduction replacing MPLS with SD-WAN over broadband, illustrative planning range

100%
of traffic that should be encrypted between sites, no exceptions

From private circuits to a software defined fabric.

SD-WAN sits on top of whatever circuits a site can get, fiber, cable, fixed wireless or cellular, and treats them as one pool. It measures every path, steers each application to the best one and fails over in under a second when a path degrades.

THE OLD MODEL

MPLS hub and spoke

- Every site backhauls to HQ, then out to the cloud. Latency and cost on every packet.
- Circuits take 60 to 120 days to deliver and come with long contracts.
- Failover is manual or slow, and often untested. Adding a site is a project.

THE MODERN MODEL

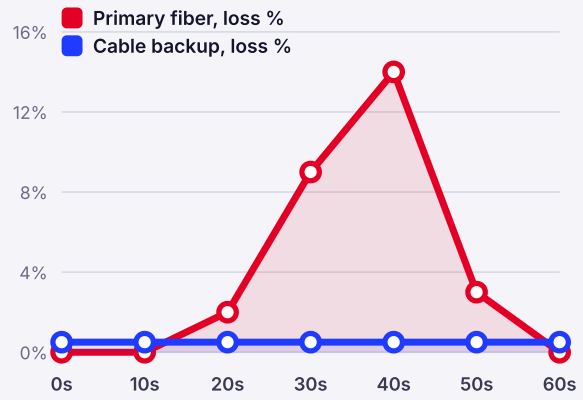
SD-WAN over any circuit

- Local internet breakout to Microsoft 365 and SaaS, direct from each site.
- Any circuit, delivered in days, mixed by cost and quality.
- Automatic sub second failover, and a new site is a shipped appliance.

How application aware routing works

- **Identify the application** in the first packets, so voice, video, ERP and backups are treated differently.
- **Measure every path** for latency, loss and jitter many times a second.
- **Steer in real time**, moving a video call to the cleaner path mid call without a drop.
- **Prioritize** what the business depends on when bandwidth gets tight.

Path quality during a circuit problem



Illustrative. At 20 seconds the fabric steers voice and video to the backup path and returns them when the fiber recovers.

Design rule

Every site gets two paths from two providers on two physical media: fiber plus cable, cable plus cellular. One provider with two circuits still fails together.

Failover nobody notices, security everybody gets.

Resilience is designed, then tested. Security is built into the fabric rather than bolted on at headquarters, because traffic no longer flows through headquarters.

Designing automatic failover

1

Two paths, two media, two providers

Diversity is the whole point. Confirm the circuits do not share a pole, a conduit or an upstream carrier.

2

Local breakout with cloud security

Send Microsoft 365 and SaaS traffic directly to the internet from each site, inspected by a cloud security service, so the backup path is not overwhelmed by backhaul.

3

Power and hardware too

A UPS on the network stack, a cellular appliance on battery and a cold spare at the site or within two hours of it.

4

Test it on purpose

Pull the primary circuit during business hours once a quarter. If anyone notices, fix the design.

Security built into the fabric

LAYER	WHAT IT DOES
Encrypted tunnels	Every site to site and site to cloud path encrypted by default
Zero trust access	Users and devices verified per application instead of trusted by network location
Cloud firewall and web filtering	The same inspection and policy at a micro site as at headquarters
Segmentation	Identical zones at every site, enforced centrally
Central visibility	One console for every path, policy and alert across all sites

4

quarterly failover tests per site, scheduled and logged

1

policy set enforced identically at every site

> **If your backup circuit has never carried production traffic, you do not have a backup circuit. You have an invoice.**
>
> SOLUTION BUILDERS NETWORK PRACTICE

Sources: Gartner, Market Guide for SD-WAN and SASE research; Microsoft 365 network connectivity principles; CISA Zero Trust Maturity Model 2.0. Cost ranges are planning estimates from Solution Builders client engagements.

SOLUTION BUILDERS®

03

Support fifty sites with the team you have.

The question every IT director asks at site five is the same: do I hire someone for each location? Almost always the answer is no. The sites need a model, not a headcount. Here is the one that holds up.

1
central help desk, one ticket system, one knowledge base for every site

90%+
of multi-site tickets resolvable remotely with the right tooling, Solution Builders client data

4 hrs
a reasonable on site response target for Tier 1 and 2 sites with staged spares

24/7
security monitoring, because a micro site at midnight is still your network

Central brain, local hands.

Put the expertise in one place and the hands everywhere. A central team owns the help desk, engineering, security and projects. Each site has a trained local champion for the physical world, and a smart hands partner for anything heavier.

Three ways to staff multi-site support

MODEL	HOW IT WORKS	STRENGTHS	BREAKS WHEN
Generalist per site	One IT person at each location	Fast on site response	Sites exceed five, skills vary, nights and weekends uncovered
Central team plus travel	HQ team covers all sites, drives or flies	Consistent standards	Travel eats the week, remote sites wait days
Central brain, local hands	Central or co managed team, local champions, smart hands partner	Scales to any site count, 24/7 coverage, every specialty	Standards are not enforced or tooling is weak

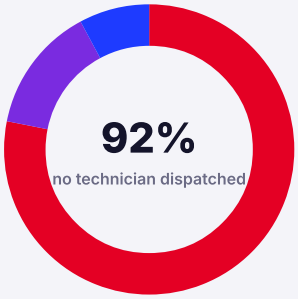
What the local champion actually does

- **Eyes and hands.** Reseats a cable, reads a light, swaps a staged spare while the central team drives the fix.
- **First call for the site.** Knows how to open a ticket well and who to call when the building loses power.
- **Not an IT job.** An office manager or shift lead with two hours of training and a laminated card.

Where co managed IT fits

Many IT directors keep strategy, applications and the core sites in house and bring in a partner for the help desk, 24/7 security and the long tail of branch support. The internal team stays in control and stops being the travel department.

How tickets resolve in a mature multi-site model



Resolved remotely	78%
Local champion assist	14%
On site visit	8%

Solution Builders multi-site client data, rounded.

Score your sites before the next one opens.

Twelve questions across the three decisions in this whitepaper. Score each one from 0 (not started) to 2 (done and documented). Most organizations opening a second or third site land between 8 and 14.

Architecture

- [ ] One identity directory with MFA for every site and user.
- [ ] No site holds the master copy of business data.
- [ ] A documented kit and template per site tier.
- [ ] Identical network zones and naming at every site.

Connectivity

- [ ] Two paths, two media, two providers at every site.
- [ ] Local internet breakout with cloud security inspection.
- [ ] Failover tested in business hours this quarter.
- [ ] One console shows every site, path and alert.

Support

- [ ] One help desk, one ticket system, one knowledge base.
- [ ] A trained local champion and staged spares per site.
- [ ] 24/7 security monitoring covering every site.
- [ ] An on site response target per tier, met and measured.

Your multi-site readiness score

_____ / 24

Add your points across all twelve questions and write the total here.

What your score means

SCORE	WHERE YOU STAND
0 to 8	Each new site adds risk and workload. Start with identity and connectivity.
9 to 16	Workable today, fragile at scale. Standardize the kit and the support model.
17 to 24	Ready to grow. The next site is a shipping label and a login.

Bring this to planning

Score it with your leadership team before the next lease is signed. The cheapest time to fix a multi-site design is before the site exists.

Sources: Solution Builders multi-site client data; HDI Support Center Practices and Salary Report (remote resolution benchmarks); CISA Cross Sector Cybersecurity Performance Goals.

Multi-site IT, run as one environment.

Solution Builders has supported multi-location businesses across Minnesota and beyond since 1995, from two office firms to manufacturers with plants in several states. Our approach follows the RISE framework and is delivered by 50+ engineers with a 24/7 security operations center.

R

Resilient

Cloud centric architecture, redundant connectivity and tested recovery at every site.

I

Integrated

One identity, one network standard and one support model across all locations.

S

Secure

Zero trust access, encrypted fabric and 24/7 monitoring for every site, large or small.

E

Evolving

A roadmap that adds automation, AI and new sites without adding chaos.

01

Multi-Site Readiness Snapshot

A 30 minute conversation about your sites, your growth plan and where the current model will break.

FREE · 30 MINUTES

02

Multi-Site Architecture Assessment

Two weeks across architecture, connectivity and support, ending with a tiered design and a cost model.

FIXED FEE · 2 WEEKS

03

Managed Multi-Site Program

Help desk, SD-WAN, security operations and site rollouts, with your team keeping the strategy.

MONTHLY · ONGOING

Opening another site? Start with the design.

Book a free Multi-Site Readiness Snapshot with a Solution Builders solution architect and find out what your next location should look like.

Book my readiness snapshot

THE SHORT VERSION

Three things to remember.

If this whitepaper gets one reading, keep these three ideas. They separate companies that grow by adding sites from companies that grow by adding problems.

01 **Decide once, deploy everywhere.**

One identity, one kit per tier, one set of templates. The hundredth site should be as boring as the second.

02 **Two paths, two media, two providers.**

Resilient connectivity is designed and then tested in business hours. An untested backup circuit is an invoice.

03 **Central brain, local hands.**

A central or co managed team with local champions and staged spares scales to any number of sites. Headcount per site does not.

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.