SOLUTION BUILDERS®

A SOLUTION BUILDERS PLAYBOOK
2026 EDITION

A PLAYBOOK FOR SMALL AND MIDSIZED BUSINESSES

The SMB Cyber Resilience Playbook.

Five layers, three acronyms decoded, a 30 day hardening plan and the questions that separate a security vendor from a security partner.

INSIDE THE PLAYBOOK

01 The five layers

02 XDR vs ITDR vs MDR

03 30 day hardening checklist

04 Choosing a security partner

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

30+ YEARS

Top 1% OF MSPS

98% CSAT

WHAT'S INSIDE

Built for companies that cannot afford a bad week.

Attackers stopped caring about company size years ago. What they care about is whether anyone is watching. This playbook shows you how to be the company that is watching, without a Fortune 500 budget or a 40 person security team.

01 **The 5 layers every SMB defense needs.**
Identity, endpoints, email, network and recovery. Why one great tool never saves you, and what good enough looks like at each layer.
PAGE 03

02 **XDR vs. ITDR vs. MDR, decoded.**
Three acronyms that get sold interchangeably and are not. What each one watches, what each one misses and which combination an SMB actually needs.
PAGE 06

03 **A 30 day hardening checklist you can run today.**
Four one week sprints that close the gaps attackers use most. Most steps need no new licenses, only decisions and a calendar.
PAGE 09

04 **What to look for in a security partner.**
Twelve questions, a scorecard and the red flags. How to tell a partner who will stand next to you during an incident from a vendor who will send an invoice after it.
PAGE 12

WHO IT IS FOR
Owners, COOs, finance leaders and IT managers at companies with 25 to 500 people who want a defense that holds.

HOW TO USE IT
Read the chapter you need. Each one ends with sources you can take to your leadership team or your board.

READING TIME
About 25 minutes cover to cover. The 30 day checklist in chapter 03 is built to print and pin up.

SOLUTION BUILDERS®

01

The 5 layers every SMB defense needs.

Resilience is not a product. It is five layers that each catch what the others miss. Most small and midsized companies have bought one or two of them and assume they are covered. This chapter shows the whole stack and where the gaps usually are.

68%
of breaches involve a human element such as a phished login or a mistake

$4.88M
global average cost of a data breach in 2024

258
days on average to identify and contain a breach

99%+
of account compromise attacks are blocked by multifactor authentication

Five layers, one goal: no single point of failure.

Each layer assumes the one before it will eventually fail. That assumption is the whole idea. A phishing email that gets past the filter still has to beat multifactor authentication, then endpoint detection, then network segmentation, then a backup that cannot be encrypted.

01 **Identity**

Multifactor authentication everywhere, conditional access and a clean, reviewed list of who has admin rights. Identity is the new perimeter because most attacks simply log in.

02 **Endpoints**

Managed detection on every laptop, desktop and server, automatic patching and full disk encryption. The device is where ransomware actually runs.

03 **Email and collaboration**

Advanced phishing protection, link and attachment detonation, and controls on external sharing in Microsoft 365 or Google Workspace.

04 **Network and cloud**

Segmented networks, a modern firewall, secure remote access instead of open VPN ports, and hardened cloud tenant settings.

05 **Data and recovery**

Immutable, tested backups of servers, cloud workloads and Microsoft 365. Recovery is the layer that turns a breach into a bad day instead of a bad year.

Every layer protects the center



The test that matters

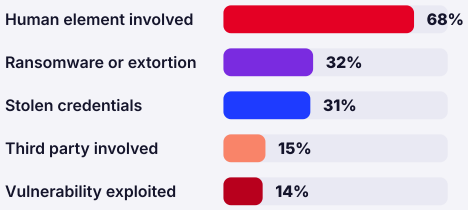
Pick any single control and imagine it failed today. If the answer is "then we are done," you have found the layer to fix first.

> **The companies that recover fastest are not the ones with the most tools. They are the ones with no single point of failure.**
>
> SOLUTION BUILDERS SECURITY PRACTICE

Most attacks do not break in. They log in.

The data is consistent year after year. Stolen credentials, phishing and unpatched systems account for most intrusions. Exotic zero day exploits make the news, but ordinary hygiene gaps make the breach reports.

What shows up in real breaches



Share of analyzed breaches. Categories overlap, so they do not total 100. Source: Verizon 2024 Data Breach Investigations Report.

< 60 sec

median time for a user to fall for a phishing email

180%

year over year growth in breaches that started with an exploited vulnerability

Minimum versus mature, by layer

LAYER	MINIMUM	MATURE
Identity	MFA on email and VPN	Phishing resistant MFA, conditional access, quarterly access reviews
Endpoints	Antivirus, manual patching	Managed XDR, automated patching, encryption, 24/7 response
Email	Built in spam filter	Advanced phishing protection, impersonation rules, user reporting
Network	Firewall, flat network	Segmentation, secure remote access, continuous monitoring
Recovery	Nightly backup, never tested	Immutable copies, M365 backup, quarterly restore drills, documented RTO and RPO

Start with identity and recovery

If budget forces a choice, fund the first and last layers first. Identity stops most attacks from starting. Recovery guarantees the business survives the ones that get through.

Sources: Verizon 2024 Data Breach Investigations Report; IBM Cost of a Data Breach Report 2024; Microsoft Digital Defense Report 2023 (MFA effectiveness).

SOLUTION BUILDERS®

02

XDR vs. ITDR vs. MDR, decoded.

Vendors have turned detection into alphabet soup. Underneath the acronyms there is one question that matters: when an attacker gets in, who notices, how fast, and who acts at 2 a.m. on a Saturday? This chapter answers it in plain language.

10
days median time attackers spend inside before being detected

$2.73M
average cost to recover from a ransomware attack, before any ransom

94%
of ransomware victims saw attackers try to compromise their backups

168
hours a week attackers work. Your detection has to cover all of them.

Three acronyms, one job: catch the attacker before the damage.

XDR and ITDR are capabilities. MDR is a service that runs capabilities for you. Understanding that one distinction clears up most of the confusion in security proposals.

	WHAT IT WATCHES	WHAT IT CATCHES	WHO RUNS IT
EDR	Laptops, desktops, servers	Malware, ransomware behavior, suspicious processes	Your IT team or an MSP
XDR	Endpoints plus email, identity, cloud and network signals	Attacks that hop between systems and would look harmless in any single tool	Your IT team or an MSP
ITDR	Logins, tokens, privileges, Active Directory and Entra ID	Credential theft, token replay, impossible travel, privilege abuse	Your IT team or an MSP
MDR	Whatever XDR and ITDR produce, 24 hours a day	The same threats, but a human analyst investigates and responds in minutes	A security operations center on your behalf

How to read a proposal

- **"We include XDR"** means you get the tooling. Ask who watches the console at night.
- **"We include MDR"** means people respond. Ask about response times and whether they can isolate a device without calling you first.
- **"We cover identity"** should mean ITDR style monitoring of Microsoft 365 and Entra ID, not just MFA.

The SMB answer

Most companies with 25 to 500 people land on the same combination: XDR on every device, identity monitoring on Microsoft 365, and an MDR service so a human responds around the clock. Buying the tools without the service is the most common and most expensive mistake.

Where detection signals come from



Endpoints	42%
Identity and email	33%
Cloud and network	25%

Illustrative mix in a typical managed SMB environment.

What the stack looks like when it is working.

Here is a real pattern from a 42 person professional services firm. One employee entered their password into a convincing fake Microsoft login page. What happened next is the difference between a tooling purchase and a managed program.

00:00

Credential phished

The user signs in to a lookalike page. The attacker now holds a valid password and a session token.

00:02

ITDR flags the login

A sign in from an unfamiliar device and location, seconds after a normal one, trips an identity alert.

00:04

XDR correlates

A new mailbox rule that hides replies appears. On its own it looks harmless. Correlated with the login, it is an attack pattern.

00:09

MDR analyst acts

Sessions are revoked, the password is reset, the rule is deleted and the device is isolated for review.

00:22

Contained

Scope confirmed. No data left the tenant. The user is back to work within the hour.

22 min
from first alert to confirmed containment

$0
ransom paid, no data lost

100%
of systems recovered the same day

TOOLS ONLY

What usually happens

- Alerts pile up in a console nobody opens after 5 p.m.
- The mailbox rule and the odd login are never connected.
- Response depends on who happens to be available.
- Detection is measured in days, and so is the damage.

MANAGED PROGRAM

What should happen

- A human triages every real alert within minutes, 24/7.
- Identity, email and endpoint signals are correlated automatically.
- Analysts have standing authority to isolate and revoke.
- You get a written incident summary the same day.

Sources: Mandiant M-Trends 2024 (median dwell time); Sophos, The State of Ransomware 2024 and The Impact of Compromised Backups on Ransomware Outcomes 2024. Case timeline from a Solution Builders client engagement, 42 users, professional services.

SOLUTION BUILDERS®

03

A 30 day hardening checklist you can run today.

You do not need a six month project to get measurably safer. You need four focused weeks, a named owner for each item and the discipline to finish. This checklist is ordered by impact, so even stopping at week two leaves you far better off than you started.

4
one week sprints: identity, endpoints, email and data, recovery and people

0
new licenses required for most of the week one and week two items

14%
of breaches now begin with an unpatched, exploitable vulnerability

3, 2, 1
three copies of your data, on two kinds of media, with one offsite and immutable

Lock the doors first: identity and endpoints.

The first two weeks remove the easiest ways in. Every item below is something your IT team or partner can do with the Microsoft 365 and endpoint tools you most likely already pay for.

WEEK 1

Identity

MFA everywhere, admin cleanup, legacy protocols off

WEEK 2

Endpoints

Patch, encrypt, detect, remove local admin

WEEK 3

Email and data

Phishing defenses, sharing controls, DNS protection

WEEK 4

Recovery and people

Immutable backups, restore test, tabletop, training

Week 1: Identity

- Enforce MFA for every user, every app, including email, VPN and remote desktop. No exceptions for executives.
- Review every account with admin rights. Separate daily use accounts from admin accounts.
- Disable legacy authentication protocols (POP, IMAP, SMTP basic auth) that bypass MFA.
- Turn on conditional access: block sign ins from countries you do not do business in.
- Remove accounts for anyone who has left. Check shared mailboxes and service accounts too.
- Enable sign in risk alerts and route them to a person who will act on them.

Week 2: Endpoints

- Confirm every device is enrolled in management and reporting in. Unknown devices get blocked.
- Patch operating systems and the big four: browsers, Office, PDF readers and remote access tools.
- Turn on full disk encryption (BitLocker or FileVault) and escrow the recovery keys.
- Deploy managed detection and response on every endpoint, servers included.
- Remove local administrator rights from standard users.
- Block USB mass storage unless a documented exception exists.

Then make a breach survivable.

Weeks three and four assume something still gets through. Email is where it starts and recovery is where it ends, so these two weeks decide whether an incident costs you an afternoon or a quarter.

Week 3: Email and data

- Enable advanced phishing and impersonation protection, with link rewriting and attachment detonation.
- Publish SPF, DKIM and DMARC for your domain so nobody can convincingly send as you.
- Add a one click "report phishing" button and tell people to use it.
- Restrict anonymous external sharing links in Microsoft 365 or Google Workspace.
- Turn on DNS filtering on every device, in and out of the office.
- Label and locate your crown jewel data: finance, HR, customer files, source code.

Week 4: Recovery and people

- Back up servers, cloud workloads and Microsoft 365 to an immutable copy attackers cannot delete.
- Restore one server and one mailbox end to end. Time it. Write the time down.
- Agree on RTO and RPO targets for each critical system with the business, not just IT.
- Run a 60 minute tabletop exercise: "Payroll is encrypted on Friday at 4 p.m. Now what?"
- Deliver short, monthly security awareness training and a quarterly phishing simulation.
- Print the incident contact list. Keep a copy that does not depend on your network.

_____ / 24

Score yourself

Count the items you have fully completed across all four weeks and write the number here.

What your score means

ITEMS DONE	WHERE YOU STAND
0 to 8	Exposed. Prioritize week one immediately.
9 to 16	Typical. Attackers would still find a way in, and recovery is uncertain.
17 to 24	Resilient. Now add 24/7 detection and response and keep testing.

Make it stick

Assign every item an owner and a date. Review the list at your next leadership meeting. Security that lives only in the IT department does not survive contact with a busy quarter.

Sources: Verizon 2024 Data Breach Investigations Report (vulnerability exploitation as initial access); CISA Cross Sector Cybersecurity Performance Goals; Microsoft 365 security baseline guidance.

SOLUTION BUILDERS®

04

What to look for in a security partner.

At some point every growing company decides it cannot do this alone. The decision that follows, who to trust, matters more than any product choice. Here is how to evaluate the people who will be holding your keys.

15%
of breaches involved a third party such as a vendor or partner

12
questions that reveal whether a provider actually operates security or resells it

3
tiers of provider: break fix shop, managed IT, managed security

30 min
is all a credible partner needs to give you an honest readiness snapshot

Twelve questions that separate a vendor from a partner.

Ask every one of these before you sign. A real partner will have crisp answers and documents to back them up. A reseller will change the subject.

01 **Who watches alerts at 2 a.m.?**
You want a staffed security operations center, not an after hours pager.

02 **What is your median response time?**
Minutes to triage and under an hour to contain is the bar.

03 **Can you show me your own audit?**
SOC 2 Type II or equivalent, current, with the report available under NDA.

04 **How do you protect your access to us?**
MFA, privileged access management and logging on every technician account.

05 **What happens during an incident?**
Ask for the runbook, the escalation path and who talks to your insurer.

06 **How do you test our backups?**
Scheduled restore tests with results you can see, not a green checkmark.

07 **Who owns our data and credentials?**
You do, in writing, with documented offboarding if you ever leave.

08 **How do you report to leadership?**
A monthly or quarterly review in business language, with a risk register.

09 **What do you not do?**
Honest providers name their limits and their partners for the rest.

10 **Can we talk to three clients our size?**
Then actually call them and ask about their worst day.

11 **How do you handle compliance?**
Mapped controls and evidence collection for frameworks like HIPAA, PCI DSS and CMMC.

12 **What does the first 90 days look like?**
Expect an assessment, a prioritized plan and quick wins in the first month.

Compare proposals side by side, not price by price.

Weight what matters to your business, score each proposal honestly and let the math make the call. The cheapest option is rarely cheapest after the first incident.

Partner scorecard

CRITERION	WEIGHT	WHAT A 5 LOOKS LIKE
24/7 detection and response	25%	Staffed SOC, isolation authority, documented response times
Identity and M365 expertise	15%	Conditional access, ITDR, tenant hardening as standard
Backup and recovery proof	15%	Immutable copies, quarterly restore tests with reports
Their own security posture	15%	SOC 2 Type II, PAM, background checked staff
Compliance support	10%	Control mapping and evidence for your frameworks
Reporting and references	20%	Quarterly reviews, risk register, clients your size who will take your call

Where providers tend to land



Illustrative positioning. Managed IT with integrated detection and response is the sweet spot for most SMBs.

> **Hire the partner you would want on the phone at 2 a.m., not the one with the nicest slide deck.**
>
> SOLUTION BUILDERS SECURITY PRACTICE

RED FLAGS

Walk away when you hear

- "Our tools handle it automatically."
- No SOC 2 or equivalent audit of their own.
- Response time is "best effort."

GREEN FLAGS

Lean in when you see

- A named security lead for your account.
- Restore test reports before you asked.
- They tell you something you did not want to hear in the first meeting.

Sources: Verizon 2024 Data Breach Investigations Report (third party involvement); AICPA SOC 2 Trust Services Criteria; Solution Builders client onboarding data.

Security that is managed, not just installed.

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

R

Resilient

Immutable backups and tested recovery, so an incident never becomes an outage.

I

Integrated

Security built into your infrastructure and Microsoft 365, not bolted on.

S

Secure

Managed XDR, identity monitoring and 24/7 response, plus compliance support.

E

Evolving

Safe AI adoption with data governance and Copilot readiness built in.

01

Security Readiness Snapshot

A 30 minute conversation. You get a candid read on your five layers and the three things to fix first.

FREE · 30 MINUTES

02

Cyber Resilience Assessment

Two weeks covering all five layers, with a scored report and a prioritized 90 day plan.

FIXED FEE · 2 WEEKS

03

Managed Security Program

Everything in this playbook, run for you: 24/7 detection and response, hardening, backup testing and training.

MONTHLY · ONGOING

Find out where you stand in 30 minutes.

Book a free Security Readiness Snapshot with a Solution Builders solution architect. No pitch, just a clear read on your defenses.

Book my readiness snapshot

THE SHORT VERSION

Three things to remember.

If this playbook disappears into a drawer, keep these three ideas. They are the difference between companies that have incidents and companies that have outages.

01 **Resilience is five layers, not one tool.**

Identity, endpoints, email, network and recovery. Fund identity and recovery first if you must choose.

02 **Detection without response is a dashboard.**

XDR and ITDR find the attacker. MDR is the human who acts at 2 a.m. Buy the outcome, not the acronym.

03 **Thirty days changes everything.**

Four one week sprints close the gaps attackers use most. Name an owner for every item and start Monday.

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.