SOLUTION BUILDERS®

CLIENT CASE STUDY
PROFESSIONAL SERVICES · 42 USERS

CASE STUDY · PROFESSIONAL SERVICES · 42 USERS

# Defeated a ransomware attack with zero data loss, and zero ransom paid.

An accounting firm was hit on a Friday evening, the hour attackers love most. Because managed backups, XDR protection and an MDR backed security operations center were already in place, the attack was contained in 22 minutes and Monday morning looked exactly like any other Monday.

**22 min**
from first alert to confirmed containment

**$0**
ransom paid, no negotiation needed

**100%**
of data recovered, nothing leaked

## AT A GLANCE

**INDUSTRY**
Accounting and advisory

**SIZE**
42 users, 1 office, hybrid staff

**SERVICES**
Managed security, backup, Microsoft 365

**ATTACK WINDOW**
Friday, 6:41 p.m., tax season

Published by Solution Builders · Bloomington, Minnesota · www.solutionbuilders.com Client details anonymized at the client's request

# Friday at 6:41 p.m., somebody clicked.

A senior associate opened an invoice attachment that looked like it came from a long time client. It installed a loader designed to hand control to a ransomware crew. In a firm with no monitoring, the next sound would have been Monday morning phone calls. Here, the next sound was an alert.

THE SETUP

## Why Friday evening matters.

Ransomware crews time their detonations for nights and weekends, when internal IT has gone home and nobody is watching the console. A Friday in tax season was the perfect window: maximum pressure to pay, minimum people on hand.

The firm had engaged Solution Builders eighteen months earlier for managed security after a cyber insurance renewal demanded MFA, endpoint detection and tested backups. Those controls were about to earn their keep.

ENTRY POINT

**Phishing email with a weaponized invoice**

TARGET

**File server and client document library**

CONTROLS IN PLACE

**MFA, managed XDR, 24/7 MDR, immutable backup**

INSURANCE

**Policy renewed on the strength of these controls**

### The first hour

**6:41 P.M.**

**Loader executes**

The attachment runs a script that tries to disable antivirus and reach out to a command server.

**6:43 P.M.**

**XDR flags behavior**

Process behavior, not a known signature, trips a high severity alert. The device is automatically isolated.

**6:49 P.M.**

**Analyst engages**

A SOC analyst confirms the pattern, revokes the user's sessions, resets credentials and hunts for lateral movement.

**7:03 P.M.**

**Contained**

No other device touched. Encryption attempt on two shared folders stopped at 1.4 percent. Firm leadership briefed by phone.

**SATURDAY**

**Restored and verified**

Affected folders rolled back from the immutable snapshot, device rebuilt, email rules checked, incident report delivered.

### What the attackers expected versus what they got

They expected an empty office, a flat network and backups they could delete first. They got an isolated laptop, a live analyst and a backup copy nobody could touch. The 22 minutes were not luck. They were the product of eighteen months of preparation.

# Monday looked like any other Monday.

Partners spent the weekend worrying about client data and about paying a ransom during tax season. By Saturday afternoon both worries were gone. Here is what the numbers looked like compared with a typical ransomware event.

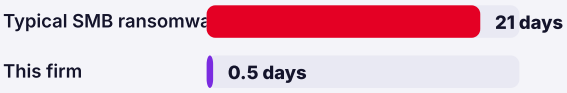
**22 min**
to containment

**$0**
ransom paid

**100%**
data recovered

**0**
client notifications required

**Days of disruption: typical event versus this firm**




Typical figure reflects commonly reported downtime of about three weeks for SMB ransomware incidents (Coveware and Sophos reporting). Illustrative comparison.

> **I got a phone call at 7 p.m. telling me we had been attacked and that it was already over. I did not know that was possible.**
>
> MANAGING PARTNER, ACCOUNTING FIRM CLIENT

## Why the outcome was different

| CONTROL | ROLE IN THE INCIDENT |
|---|---|
| **Managed XDR** | Detected behavior in 2 minutes and isolated the device automatically |
| **24/7 MDR SOC** | A human analyst engaged within 8 minutes, on a Friday night |
| **Immutable backup** | Snapshot could not be encrypted or deleted, restore took one afternoon |
| **MFA and conditional access** | Stolen credentials could not be reused from outside |
| **Email protection** | Blocked the attacker's follow up messages to other staff |

**1.4%**
of one shared folder encrypted before isolation

**18**
months since the security program began

### The insurance angle

Because the incident was contained with documented evidence, the firm filed no claim, kept its premium and used the incident report at renewal as proof of a working program.

Timeline and figures reflect the Solution Builders incident report for this engagement. Client details anonymized at the client's request.

# Managed security, built on the RISE framework.

Solution Builders has protected Minnesota professional services firms since 1995. This outcome came from the same framework we bring to every client: resilient recovery, integrated controls, 24/7 security and a program that keeps evolving with the threats.

**R**

**Resilient**

Immutable, replicated backups with restore tests every quarter, so recovery is a procedure, not a prayer.

**I**

**Integrated**

Identity, email, endpoint and backup working as one managed platform.

**S**

**Secure**

Managed XDR with a 24/7 security operations center that has authority to act.

**E**

**Evolving**

Quarterly reviews that add new controls as attackers change tactics.

**01**

### Security Readiness Snapshot

A 30 minute conversation about your firm, your controls and the gaps an attacker would find first.

FREE · 30 MINUTES

**02**

### Cyber Resilience Assessment

Two weeks covering identity, endpoints, email, network and recovery, with a scored report.

FIXED FEE · 2 WEEKS

**03**

### Managed Security Program

24/7 detection and response, hardening, backup testing and training, run for you.

MONTHLY · ONGOING

## Could your firm survive a Friday night like this one?

Book a free Security Readiness Snapshot with a Solution Builders solution architect and find out before an attacker does.

**Book my readiness snapshot**