



**HEAD NERDS**

Playbook

# Turning Business Resilience into Revenue: How MSPs Can Help Organizations Adapt and Thrive



# Introduction

In today's volatile business landscape, small and medium-sized businesses (SMBs) face constant threats—from cyberattacks to natural disasters—that can disrupt operations. As a managed service provider (MSP), you have a unique opportunity to become more than just an IT support vendor. By focusing on the concept of business resilience as a sales strategy, you position your MSP as a strategic partner who keeps clients' businesses running no matter what.

This playbook is a companion guide to the masterclass **"Turning Resilience into Revenue: How MSPs Can Help SMBs Adapt and Thrive."** It translates the presentation into a structured, narrative guide with actionable steps, checklists, and frameworks to help you sell the concept of business resilience and win new SMB clients. You can use this as reference to design, price, and sell your own business resilience offering.

## Core idea: Sell outcomes, not products

SMB owners don't wake up excited about acronyms like EDR or MDR. The masterclass and this companion guide are not about how to sell technical security products like backup, EDR, or MDR.

Rather, these are about helping MSPs:

- ▲ Shift from **technology selling** to **outcome selling**
- ▲ Package tools into a **resilience program** that business owners understand
- ▲ Reduce customer risk and MSP liability
- ▲ Turn uncertainty into **higher value, stickier recurring revenue**

At its core, business resilience is about one promise: even when something goes wrong, the business will continue—or recover quickly enough to survive.

This playbook will show you how to reframe your cybersecurity and backup services into an "outcome-based" offering—referred to as a **ResilienceReady Program**—that will deliver peace of mind and tangible business results. By shifting your pitch from technical features to business outcomes, you'll differentiate your MSP, justify higher pricing, and, ultimately, generate more revenue per client.

## What you'll find in this playbook:

We'll start with a real-world cautionary tale illustrating the cost of poor resilience. Then, we'll introduce the **three-step ResilienceReady framework (before, during, and after an attack)** and break down its components: **Endpoint Resilience, Security Resilience, and Data Resilience**. You'll get guidance on building and packaging this program, pricing the program (using outcome-based pricing and a sample model), **handling sales objections** (like "it's too expensive") by reframing the discussion to risk and value, and **positioning the program as your MSP's competitive differentiator** (and even as an affirmative defense for you).

I encourage you to use this playbook as a practical sales and marketing tool to train your team, refine your sales approach, and fuel your success. By focusing on resilience outcomes, you will engage prospects on what truly matters to their business and turn uncertainty into a profitable new revenue stream for your MSP.

Happy selling!



### Stefanie Hammond

Head Nerd – MSP Growth

N-able Solutions

[stefanie.hammond@n-able.com](mailto:stefanie.hammond@n-able.com)

# The high cost of not being resilient: A cautionary tale

Nothing conveys the importance of resilience better than a real incident. Consider the [story of a small healthcare clinic](#) hit by a ransomware attack in August 2024.

**The attack:** One morning, the clinic's staff found themselves **locked out of all essential systems**. Hackers had encrypted the electronic health records and left a ransom note. The clinic's owner refused to pay the ransom and decided to rebuild the patient records manually from scratch.

**Partial recovery at a huge cost:** Despite heroic efforts and with the help of patients (who had kept some of their records), about **80% of the data was recovered, but 20% was permanently lost**. This "recovery" came at an enormous cost. The clinic's operations were slowed considerably during the rebuild, as staff had to reassemble thousands of records by hand, and financial damages exceeded six figures, far beyond what their limited \$50,000 cyber insurance could cover.

**Why this story matters:** This was not just a cyberattack. This was a **business resilience failure**. While the article didn't mention this specifically, the outcome suggests that the clinic's IT consultant had not implemented the basic business continuity and security best practices, such as offline or immutable backups, redundant systems, incident response plan, and communication workflows. Compounding this was inadequate cyber insurance and overall poor cyber hygiene. In short, there was **no business resilience strategy**. The result was months of downtime, operational paralysis, hundreds of thousands in losses, and a business that is "still struggling to stay afloat today."

**The lesson for MSPs: Prevention alone is NOT resilience.** Ask yourself, "How easily could one of my clients end up like this small healthcare clinic?" If you are only providing basic IT support without a broader continuity and recovery plan in place, an incident can quickly become an existential threat for your client.

True business resilience requires three elements:

- 1 Preparedness **before** an incident
- 2 Rapid response **during** an incident
- 3 Reliable recovery **after** an incident

An MSP who had sold a proper business resilience program, including preventive cybersecurity, secure backups, and incident response planning, could have helped save this clinic. The downtime and damage could have been minimized or avoided entirely. This story shows that selling "just IT services" is no longer enough. SMBs need partners who can help safeguard their whole business.

## Why business resilience **SHOULD** matter to business owners

Most SMB owners are deeply exposed to risk, are highly reactive, severely underestimate downtime costs, and spend very little time on any long-term strategy.

Common unspoken fears center on:

- ▲ “What if our systems go down midday?”
- ▲ “What if we fail an audit?”
- ▲ “What if ransomware shuts us down?”

Cybersecurity has evolved from an IT issue to an urgent matter of business survival. SMBs that lack a business resilience plan risk complete shutdown when (not if) a major incident occurs. One serious incident can be an extinction event for them, especially in regulated industries.

As an MSP, you have the responsibility and opportunity to prevent your customers from becoming the next big headline by implementing robust business continuity and resilience measures that can protect their livelihood.

Use this cautionary tale in your sales conversations. It vividly illustrates the business impact of poor resilience—something owners can relate to. When prospects say, “We’re too small to be a target,” remind them that attackers don’t discriminate: even a small clinic can be crippled by ransomware.

By contrast, with a solid resilience program in place, that story could have had a very different—and far better—ending.

**This sets the stage for introducing your solution: the [ResilienceReady Program](#).**

## What is business resilience?

**Business resilience is an organization’s ability to:**

- ▲ Anticipate disruption
- ▲ Prepare for disruption
- ▲ Respond quickly
- ▲ Recover reliably
- ▲ Adapt and continue operating

**It applies to:**

- ▲ Cyber incidents
- ▲ Hardware failures
- ▲ Human error
- ▲ Regulatory events
- ▲ Natural disasters

## Why business resilience matters

**\$50k-200K**

for smaller companies (10-49 employees)

<https://databreachcost.com/small-business>

**Downtime Cost Surge**

**+60%**

Increase in unplanned downtime costs for small business in recent years

<https://envision-consulting.com/true-cost-of-it-downtime/>

**Strategy Time Neglected**

**85%**

SMB leadership teams spending under 1 hour per month on strategic planning

These [statistics](#) underscore why **business resilience** is so crucial for SMBs. Downtime and attacks carry huge costs that many SMBs underestimate, and most are not devoting time to plan for “what if” scenarios.

As an MSP, you can fill this gap by introducing a comprehensive resilience program that protects your clients’ livelihoods.

## The shift: From selling technology products to selling outcomes

Before diving into the ResilienceReady Program framework, it's critical to adopt the right sales mindset that focuses on selling outcomes instead of selling just products or technical features. This aligns your offering with what SMB decision-makers truly care about: protecting their business.

MSPs often ask if I can help train their team on how to sell EDR, MDR, backup, monitoring, and similar tools. But that's the wrong question, as business owners don't buy toolsets.

They buy:

- ▲ Peace of mind
- ▲ Employee productivity
- ▲ Reduced risk
- ▲ Reputation enhancements
- ▲ Confidence that their business will survive a major downtime incident

Instead of focusing on technical feature sets and products they can install, MSPs should focus on what the business gains.

**Example:**

**Traditional MSP pitch (what not to do):** “We offer next-gen EDR, advanced backup solutions, and managed SIEM services.”

This pitches products and jargon. Many business owners will tune out or compare your line-item prices to cheaper alternatives.

**Outcome-based pitch (what to do):** “We help ensure that one clicked phishing email doesn’t shut your operations down for a week, you can recover any of your critical, confidential data in minutes instead of days, and you can sleep soundly knowing a 24/7 security team is watching over your network keeping unwanted attackers out.”

The result? Continuity, rapid recovery, and peace of mind.

Notice the difference?

In the second approach, we didn’t even mention the names of the tools (EDR, backup, MDR)—we sold the outcome each tool delivers.

We spoke to the owner’s emotions and business priorities: keeping their doors open, avoiding loss, and protecting their reputation.

**Why this matters:** Business owners care about payroll, customers, revenue, and survival, not the mechanics of IT. By translating tech into business value, you speak their language.

## The ResilienceReady Program: Framed as an outcome

Throughout this playbook, as we describe the components of the **ResilienceReady Program**, remember to frame each one in terms of the outcome or risk it mitigates:

- ▲ When discussing preventive measures (like patching or training), emphasize avoiding costly incidents and downtime
- ▲ When discussing detection and response (EDR, SOC monitoring), emphasize stopping attacks early to prevent damage
- ▲ When discussing backup and disaster recovery, emphasize quick recovery and keeping the business running no matter what

In other words, you are not selling “backup software.” You are selling **guaranteed business continuity**. You’re not selling “EDR licenses,” but **assurance that a single malware incident won’t derail the company**.

## Outcome-based selling changes everything.

When you sell outcomes instead of tools, you will experience several immediate benefits:

- ▲ **Sales conversations become simpler.** You talk about business challenges and solutions, not technical specs, so owners engage more easily.
- ▲ **Services become more valuable.** Solutions to business problems are worth more than individual tools. Clients see a comprehensive program like ResilienceReady as a value-add, not an upsell.
- ▲ **Pricing becomes easier to justify.** It’s hard to argue when a customer says, “I won’t pay for another security widget,” but gets easier to justify the added expense when it is reframed in the context of improved operational resilience and risk reduction. Clients will pay more for outcomes that protect their revenue and customers.
- ▲ **Competitive advantage:** Most MSPs still push products. By selling outcomes, you differentiate on value, not price. MSPs who sell technology compete on price, but those who sell outcomes compete on value—and value always wins.
- ▲ **Margins increase.** There is only so much markup that can be applied to a singular toolset. But when tools are bundled into a comprehensive package like a **ResilienceReady Program**, you can incorporate higher margins, resulting in a much larger average contract value (ACV) than previously generated.

**You are not selling how protection happens. You are selling what life can/will look like after something goes terribly wrong.**

By the end of your pitch, the client should clearly visualize the result: “Even if something happens, my business keeps going—that’s what I’m buying.”

For MSPs, this means evolving from an “IT fixer” into a **strategic business partner**.

And that’s exactly what the **ResilienceReady Program** delivers.

Additional examples to reinforce outcomes-based messaging:

- ▲ Instead of “**We manage your firewalls and monitor threats,**” say, “**We protect your business from cyberattacks, so you can avoid costly downtime or data loss.**”
- ▲ Instead of “**We provide disaster recovery services,**” say, “**Even if the worst happens, we’ll have you back up and running with minimal disruption.**”

## The ResilienceReady Program: Framework overview

The **ResilienceReady Program** is a three-pillar framework aligned to the lifecycle of a downtime incident. It’s an end-to-end resilience strategy you can offer to clients, structured around the three phases of any incident: before, during, and after. It provides a holistic approach to anticipating threats, responding to incidents, and recovering rapidly, so the client’s business stays resilient through adversity.

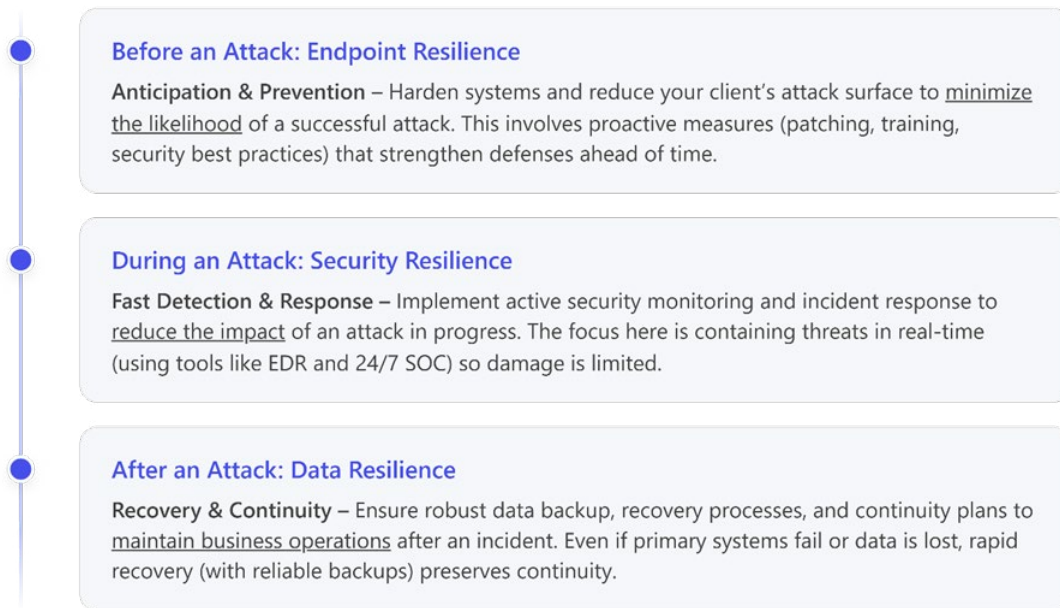


Think of it this way:

- ▲ **Endpoint Resilience – Before an attack**  
Preventive and anticipatory measures designed to minimize exposure and the risk of incidents occurring, resulting in fewer incidents happening
- ▲ **Security Resilience – During an attack**  
Reactive measures designed to detect and contain threats in real time to reduce the impact, resulting in less damage and minimal downtime
- ▲ **Data Resilience – After an attack**  
Recovery efforts to restore data and operations quickly to maintain continuity, resulting in minimal business interruption overall

This unified ResilienceReady strategy shifts the focus from merely trying to prevent all incidents (an impossible goal) to building the capacity to withstand and bounce back when incidents happen. Together, they cover the full lifecycle of a threat. It recognizes that breaches and outages are inevitable (“when, not if”) and what matters is how prepared the business is to handle them. By addressing all three pillars, you’re promising clients that no matter what stage a threat hits them, you have measures in place to safeguard their business.

Below is the high-level framework:



Let’s break down each component in detail, including actionable steps, tools/services to include, and the outcomes they deliver.

## Pillar 1: Endpoint Resilience – BEFORE the attack

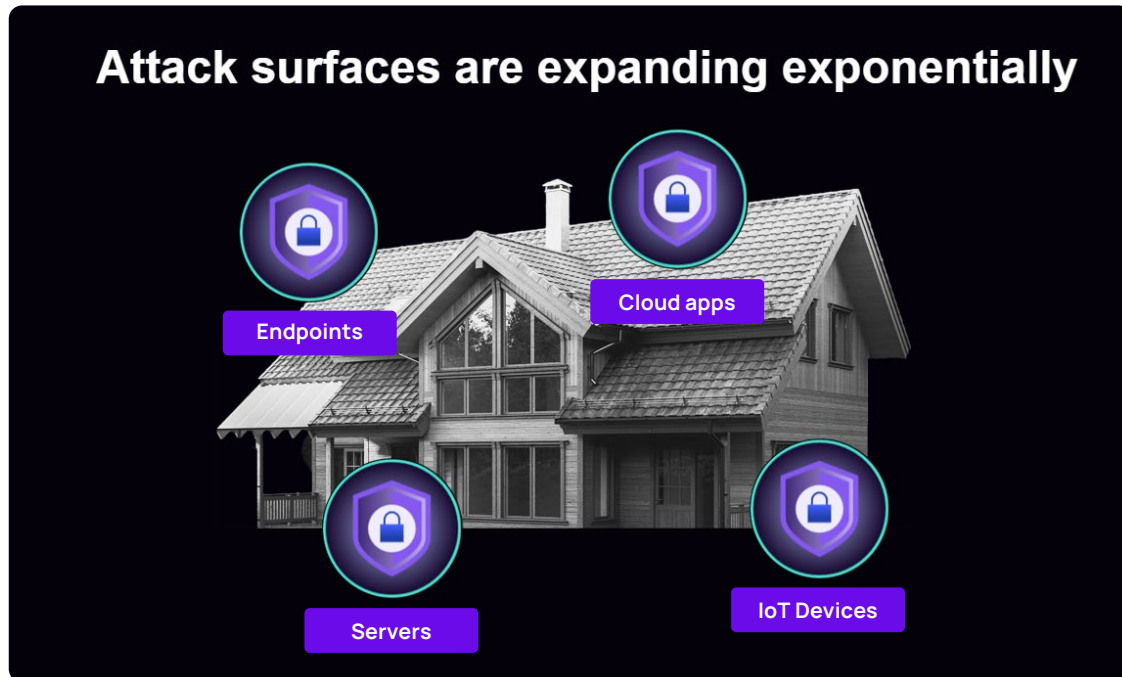
**Goal:** Prevent incidents from occurring by minimizing the attack surface and hardening endpoints.

Endpoints are where business happens and where most breaches begin, so Endpoint Resilience is all about preparation and proactive defenses to minimize the attack surface before anything goes wrong.

The attack surface includes:

- ▲ Endpoints
- ▲ Servers
- ▲ Cloud apps
- ▲ Identities
- ▲ Networks
- ▲ IoT devices

Think of it like a home, where every device, application, and account is like a door, window, or vent—each a potential access point for a thief.



The Endpoint Resilience Pillar is where you implement a set of preventative security measures and best practices to reduce the number of entry points into your customer's business by closing unnecessary doors and windows, and strengthening their defenses by adding locks to the ones you need to make the client's systems as fortified as possible.

### Key components of Endpoint Resilience



- ▲ **Full asset inventory:** Identify every device, user account, application, and data repository in the client's environment. You can't protect what you don't know exists. Use your RMM tools (e.g., [N-able™ N-central](#) or similar) to discover on-premise and cloud assets, and perform an initial risk assessment. Classify critical systems and data: which business processes are mission-critical? Which data is sensitive? This assessment guides all other measures.
- ▲ **Secure configuration and system hardening:** Establish baseline secure configurations for servers, PCs, network gear, and cloud services. This means eliminating default passwords and unwanted services, enforcing least privilege, disabling or uninstalling unused software, and turning on security features (like OS firewalls and BitLocker disk encryption on laptops). Lock down endpoints to reduce attack pathways. Then, implement monitoring to catch configuration drift to ensure systems don't slip back into insecure settings.
- ▲ **Vulnerability scanning and patching management (continuous):** Set up [regular vulnerability scans](#) (at least monthly, if not weekly) on all systems to find missing patches or misconfigurations. Enforce a strict [patch management program](#): apply OS and software patches promptly, including third-party apps and firmware updates. Many attacks (including ransomware) exploit known vulnerabilities that patches exist for—timely patching prevents that. For any legacy systems that can't be patched or replaced, implement compensating controls (isolate them on the network, restrict access, etc.). Goal: no critical vulnerabilities left unaddressed in the environment.
- ▲ **Network perimeter security:** Deploy and manage strong network defenses. This includes business-grade firewalls with IDS/IPS capabilities at all sites. Ensure network segmentation where appropriate (e.g., isolate guest Wi-Fi, IoT devices, etc.). Use email security gateways/spam filtering (like [N-able™ Mail Assure](#) or equivalent) to block phishing and malware emails before they hit user inboxes. Use [web security/DNS filtering](#) to prevent users from visiting malicious websites that could deliver malware. Together, these tools reduce the chances of a user inadvertently letting an attacker in.



- ▲ **Endpoint protection and device security:** While advanced threats require [EDR](#) (discussed in Security Resilience), at a minimum ensure every endpoint has reputable anti-malware protection and that disk encryption is enabled on all mobile devices/laptops. Full-disk encryption (e.g., BitLocker) protects data in case of device loss or theft – a simple but important resilience measure. Also consider [dark web credential monitoring services](#) to get alerts if the company's emails/passwords are exposed in breaches. This can preemptively warn of increased risk (for example, if an employee's password was leaked, you can force a reset).

- ▲ **Strong identity and access management:** Enforce strong password policies and deploy multi-factor authentication (MFA) on all critical systems, especially email and remote access. Consider providing a password management tool (like [N-able™ Passportal](#) or equivalent) for the client's users to encourage use of complex, unique passwords. MFA is a must-have for email, VPNs, and any remote access, as it dramatically reduces the chance that a leaked or guessed password leads to a breach.
- ▲ **Security awareness training:** The human element is often the weakest link. Implement regular security awareness training for all end users. This might be a monthly phishing simulation, quarterly mini-courses, or at least an annual training program. Educate staff on phishing, safe Internet use, and incident reporting. A well-trained workforce is part of a resilient business. Many attacks (phishing, social engineering) can be thwarted if employees recognize the threat and act cautiously. Make training an ongoing service in your program instead of a one-time event.
- ▲ **Regular health check and risk review:** Conduct a quarterly (or at least periodic) risk assessment and review with the client. Update them on new threats, check compliance with policies, and plan improvements. This can be part of a Quarterly Business Review (QBR). The idea is to continuously improve their security posture—resilience is not “set and forget.” Use these reviews to adjust the preventive measures as the client's business or the threat landscape evolves.

By implementing the above, you shrink the attack surface. You're closing the doors and windows that hackers could slip through.

**Outcome of the Endpoint Resilience pillar for the client:** A strong Endpoint Resilience strategy is delivers three key outcomes:

- ▲ **Fewer security incidents overall,** as attacks are less likely to succeed in the first place due to the preventative measures in place.
- ▲ **Reduced frequency and severity of events.** Even if something does happen, it's likely to be a less severe incident because you eliminated the easy exploits and pathways. Effective cyber hygiene here means your client is dodging bullets daily, without them even knowing, and your limited response resources can be reserved for truly sophisticated threats that do manage to get through.
- ▲ **Greater confidence** that basic issues won't cause downtime and disrupt business productivity. Their systems are hardened and maintained in a secure state, reducing overall business risk. They avoid the operational and financial pain of preventable incidents (example: reduction of breaches caused by an unpatched server or an employee falling for an obvious phish).

## Pillar 2: Security Resilience – DURING an attack



## Pillar 2: Security Resilience – DURING an attack

**Reality check:** no matter how strong your preventative measures are, some attacks will slip through. No defense is 100%. What matters is how quickly you can detect and contain an attack when it happens.

Security Resilience is about what happens during an incident—the tools and processes to detect, contain, and neutralize threats in real time—so that a security event doesn't turn into a business disaster.

Here, the focus is on early detection and rapid response to minimize damage.

### Key components of Security Resilience

- Endpoint Detection & Response (EDR):** Deploy a next-generation EDR agent on all endpoints (workstations and servers). Unlike traditional antivirus, EDR uses behavioral analysis to catch suspicious activities (unknown malware, fileless attacks, etc.). For example, N-able offers SentinelOne EDR, which can automatically kill and quarantine malware and even rollback ransomware encryption on the fly. This capability is critical for resilience: if ransomware starts encrypting files, the EDR can stop it within minutes and revert changes, dramatically reducing recovery time and data loss.

**Action:** Install EDR on every client device and configure it for alerts and autonomous response. Make sure your team—or Security Operations Center (SOC) provider—is monitoring the EDR console.

- 24/7 threat monitoring and SOC services (MDR):** Implement a Security Information and Event Management (SIEM) system combined with active monitoring, often delivered as a Managed Detection & Response (MDR) service. This extends visibility beyond just endpoints to the entire network and cloud environment. For instance, [N-able Adlumin MDR](#) provides a SIEM platform with an integrated 24x7 SOC team. The SIEM aggregates logs and security events from firewalls, servers, cloud services, identity systems, etc., correlating them to spot signs of attack (e.g., unusual logins, network scans, privilege escalations). The MDR service means human analysts are watching those alerts around the clock and can respond immediately, either by guiding you or executing automated countermeasures (SOAR: Security Orchestration Automation and Response).

**Action:** If you're not building your own 24/7 SOC, partner with an MDR provider. Feed your endpoints, network devices, and cloud logs into a unified monitoring system. This way, if a breach occurs at 3 AM on a Saturday, someone is on it.

- Incident detection and automated response:** Set up automated containment actions for certain triggers. For example, if the EDR detects ransomware behavior, it should automatically isolate that endpoint from the network (containment) and alert the SOC. If the SIEM sees a new device on the network communicating with a known malicious IP, it could automatically block it at the firewall. These automated responses buy you time and often neutralize threats before they escalate. Many EDR/MDR solutions allow playbooks or automatic quarantines, so use them. Fast isolation is key to limiting an attacker's lateral movement.
- Unified threat visibility:** Ensure you have "single pane of glass" visibility into the client's security posture. EDR and SIEM dashboards should be regularly checked. During an active incident, unified visibility means you can quickly trace how the attacker got in and what systems are affected. With a combined EDR+MDR approach, you get a clear storyline of an attack in progress. This is crucial for fast decision-making under pressure.
- Active threat hunting and continuous posture checks:** Security Resilience isn't just reactive. It's also proactive threat hunting. Many MDR services include threat hunting, where analysts look for stealthy signs of threats that automated tools might miss. Additionally, continuously assess the security posture (e.g., are all endpoints still running the EDR agent? Is logging from all devices flowing to the SIEM?). These checks help ensure your "during attack" defenses remain robust over time.
- Incident response (IR) plan and skills:** Even with the best tools, your team needs an IR plan for what to do when an alert indicates a likely incident. As part of your service, have a documented procedure: who gets notified, what steps to contain and investigate, at what point you should involve law enforcement or cyber insurance, etc. Practice this plan (through tabletop exercises or drills) so that when an incident happens, your team and the client know how to react calmly and effectively. Note: As part of the ResilienceReady offering, you might include a certain level of IR service, but large-scale incident remediation (weeks of effort) may be outside scope and handled as a separate billable service. Be clear in your agreement on the extent of IR coverage you will provide as part of the monthly fee.

**Why EDR and MDR BOTH matter.** This is not an either/or decision. Both EDR and MDR are essential components of a comprehensive ResilienceReady Program because they work together: EDR protects the endpoints, while MDR covers everything else.

As a partnership, EDR and MDR working together will:

- ▲ Reduce dwell time
- ▲ Prevent lateral movement
- ▲ Limit the blast radius

**Outcome of the Security Resilience pillar for the client:** If an attack occurs, it is detected and thwarted quickly. Instead of an attacker dwelling in the network for months (very common when there's no security monitoring), your monitoring might catch them within minutes or hours. For example, if a user opens a malicious file, EDR might detect it within seconds and kill the process. If a hacker tries to create a new admin account or exfiltrate data, your SIEM/MDR will catch the anomalous behavior and alert the SOC for immediate action. The incident is contained: a few machines may be infected, but with your Security Resilience pillar in place, it doesn't spread to all servers.

From a **business perspective**, the client experiences **minimal disruption** during the incident versus an unchecked attack that could down the entire network for days or weeks. They maintain operations while the issue is handled in the background. Put simply: "The burglar might get in, but the alarm blares, and the security team apprehends them before anything major is stolen."

Security Resilience gives the client a fighting chance during an attack, helping ensure that one breach doesn't become a widespread outage or data loss event. It's a critical part of delivering on the promise of resilience.

### Pillar 3: Data Resilience – AFTER an attack

**Hard truth:** Organizations don't fail because they get breached. They fail because they can't recover fast enough.

Despite the best prevention and detection measures, you must assume worst-case scenarios will happen. Data Resilience is about the aftermath: having robust systems to recover data and restore operations when something does get through. It's essentially your client's safety net. In the context of the **ResilienceReady Program**, Data Resilience primarily means Backup and Disaster Recovery (BDR) done in a modern, "resilience-first" way.

## Key components of Endpoint Resilience



- ▲ **Comprehensive data protection strategy:** Ensure all critical data and systems are backed up regularly—no exceptions. This includes server data, databases, critical workstations if any, and SaaS data (like Microsoft 365 emails, SharePoint, etc., which are often overlooked). Ensure no device, user, and data set is left out. Determine appropriate backup frequency and retention based on the client's business needs or Recovery Point Objective (RPO). For instance, if they say they can't lose more than one hour of data, you need hourly backups at least. Have that frank conversation: "How much data could you afford to lose?" Most will say, "As little as possible," which helps justify robust backups (and the associated cost).
- ▲ **Cloud-first, immutable backups:** Use a backup solution with cloud storage and immutability to protect against modern threats that target backups. For example, [N-able Cove Data Protection](#) is a cloud-first backup with encrypted, immutable storage. Immutability means once a backup is taken, it cannot be altered or deleted, even by an admin or attacker. This is extremely important because ransomware attackers now try to destroy backups first. Storing backups off the production network (in an isolated cloud repository) and making them tamper-proof ensure you always have a clean restore point. Make sure your backup strategy includes off-site copies (cloud or at least offline) that ransomware cannot reach.

- ▲ **Anomaly detection and early warning in backup systems:** Modern backup software can also serve as an early breach detector. For instance, Cove now has an anomaly/honeypot system. It deploys decoy files or systems to attract attackers and monitors unusual backup patterns (like a sudden surge in changed files, which might indicate encryption by ransomware). If ransomware attempts to encrypt or delete backups, it triggers an alert before the actual data is compromised.

**Action:** Enable anomaly detection features in your backup platform. This adds an extra layer of security by helping detect an attack in progress (complimenting the Security Resilience measures). It gives you a chance to respond before the client even realizes they're under attack, preserving the backups and production data.

- ▲ **Flexible recovery options (RTO):** Plan and provide for multiple recovery strategies to meet the client's recovery time objective (RTO), or how quickly they need to be back up.

For example:

- ▲ Quick file restores for minor issues
- ▲ Full system restore to new hardware or virtual machine (VM) for major server failures
- ▲ Virtual standby images or continuous recovery: having a cloud VM ready to spin up (Cove offers standby image) for near-instant failover
- ▲ Option for secure, staged recovery (restoring into an isolated sandbox to check for malware before reintroducing to production)
- ▲ Discuss with the client: "If your main server catches fire (or gets ransomware), do we need you running again in an hour? A day?"
- ▲ If they have low tolerance for downtime, you might implement a hot standby solution. If they can tolerate a bit longer, regular restore from backup might suffice.
- ▲ The **ResilienceReady Program** can scale to those needs, possibly as add-ons (e.g., an option for instant cloud recovery at a premium). The key is your program ensures there is a way to get them running in the timeframe they expect, and that might involve different tools or approaches for different clients.
- ▲ **Regular recovery testing:** Arguably the most important part: test the restores regularly. A backup is only as good as your ability to restore it. Incorporate scheduled disaster recovery tests into the service (e.g., quarterly test restores of a server, an annual full disaster simulation). Show the client that you can meet the RTO/RPO promises. Testing builds confidence and hones your team's recovery skills. It turns recovery from a theoretical capability into a practiced routine. Keith Young, Cove Specialist at N-able, has an apt quote he uses in his technical sales presentations: "We don't rise to our backup strategy; we fall to the level of our recovery practice." Meaning, in a crisis, you perform as you've practiced, not just according to your plan. So, practice, practice, practice. Use automated backup verification features and manual drills.

- ▲ **Maintain a business continuity plan (BCP):** Beyond IT recovery, ensure the client has a basic BCP. This includes knowing how they would operate if systems were down, e.g., if they can do certain tasks manually, how they will communicate with customers, and so on. It might not be formally part of your service deliverables, but advising them on having contingencies (even if it's just a phone tree and a manual invoicing process) can make a big difference in a crisis. This positions you as a trusted advisor taking a holistic view of resilience, not just the IT bits.

**Outcome of the Data Resilience pillar for the client:** Slow recovery is NOT recovery. It simply extends the painful downtime experience. With the Data Resilience Pillar in place, it ensures that when the worst happens—say, ransomware does encrypt data, or a server is destroyed—the client won't have to pay the ransom or suffer extended downtime. You can recover their data and systems quickly from backups, with minimal data loss. Business operations can resume perhaps within hours instead of weeks.

For example, if a server is down at 9 AM, you might spin up the last backup as a VM and have them running by 10 AM. If an entire site is flooded, you have cloud backups to restore to new hardware at a temporary location, getting critical services online the next day.

From the client's perspective, this can be the difference between a minor inconvenience and a business-threatening catastrophe. With effective Data Resilience:

**Fewer security incidents overall**, as attacks are less likely to succeed in the first place due to the preventative measures in place.

- ▲ They avoid huge financial losses brought about by prolonged downtime
- ▲ They preserve their reputation and customer trust because they can say, "We had an incident, but we're back up, and all data is safe"
- ▲ They may also get more favorable treatment from cyber insurers or regulators because they can demonstrate having had strong recovery controls (and they can recover without paying ransom, which even law enforcement recommends against)

In short, Data Resilience helps ensure your client's business survives the disaster and continues moving forward. **This is the ultimate promise of the ResilienceReady Program: even if the worst case happens, you can help them rebuild.**

## Summary of ResilienceReady components

The three pillars—Endpoint, Security, and Data Resilience—work together to deliver full-spectrum, end-to-end business protection for your most at-risk customers.



By covering all three stages—before, during, and after an incident—you can deliver a comprehensive resilience solution. It's not just monitoring, EDR, MDR, or backup, but an **integrated** program. This is a major differentiating selling point: many competitors may only offer pieces (e.g., just backup or a VCISO security project), but your MSP is packaging a complete end-to-end program that ensures that the client's business stays up, running, and protected through any incident.

While each pillar delivers significant value on its own, the real power lies in the combination. And all three of these components work together to cover the full threat lifecycle, enabling you to deliver true business resilience to your customers. Because this isn't about just preventing incidents for your customers. Yes, prevention does matters—but it's about being able to operate during the chaos and successfully recover afterwards, so your customer doesn't face any type of extinction event. Good cyber hygiene shrinks the blast radius, while data resilience drives operational recovery, and proper endpoint resilience keeps your customer's environment stable enough to withstand it all.

It's a layered safety net. If one layer fails, the next catches the issue. This is the same approach large enterprises use, and now, SMBs can get it through the **ResilienceReady program**.

# Packaging and delivering the ResilienceReady Program

Beyond the core technical components, the ResilienceReady Program should be packaged with additional services and practices that add value and ensure its success.

These include consulting, reporting, and support elements that round out the offering:

- ▲ **Regular Executive Business Reviews (EBRs):** As part of the program, schedule quarterly (or at least semiannual) meetings with the client's leadership in a vCIO-style meeting. In these EBRs, the focus shouldn't be on patch counts or technical metrics, but on these strategic items:
  - ▲ Review their **security posture and compliance status** (example: "This quarter, we improved your phishing test pass rate to 90%, and here are the compliance gaps we should address")
  - ▲ Discuss **business changes** (new employees, new offices, software changes) and how they might introduce new risks or require changes in the IT strategy
  - ▲ Go over an **asset lifecycle plan**. Identify if equipment is aging or due for refresh, so they can budget proactively.

Ultimately, show them the **business value delivered** by the program (example: "No incidents this quarter," "We neutralized X threats," or "You passed your audit because of these controls"), and plan ahead to keep improving. This keeps the relationship consultative rather than just transactional and helps to build pipelines and improve revenue.

- ▲ **Monthly reports:** Provide monthly summary reports that give the client high-level insights into their environment's health and resilience. For example:
  - ▲ **Security report:** number of threats blocked, training participation, patch compliance percentage
  - ▲ **Backup report:** backup success rates, any anomalies detected (with reassurance they were handled)

These reports reinforce the ongoing value they're getting ("Look at all the bad stuff we stopped," or "Here's proof your backups are working"). They also help maintain transparency and trust.

- ▲ **Compliance insights:** If your toolset (like the MDR) provides compliance-related summaries (example: a score or report against frameworks like HIPAA, PCI, etc.), include that in your deliverables. Many SMBs in regulated industries will appreciate a regular compliance check-ins, and this becomes another value-add of your program (helping them stay compliant, which is part of resilience, and avoid legal trouble).

- Scope of support services:** Clearly define what day-to-day IT support is included with the program. Typically, general helpdesk support (for general IT issues) is part of their overall managed service, which likely continues with this program. Ensure clients know that reactive support (like user password resets, minor fixes) is covered, as well as vendor management (dealing with third-party software support on their behalf).

However, you should also clarify that major incident response/remediation beyond the automated stuff is limited. For instance, if, despite everything, a big breach happens that requires hundreds of hours to fully remediate, that might be handled as a separate project or under an IR retainer. This protects your MSP from open-ended labor in extreme cases. Many MSPs exclude full incident recovery from flat fee plans or offer a separate retainer for it. You can position that honestly to set clear expectations: “Our program drastically lowers your risk of a big incident. In the unlikely worst case, our team will be there for you, but those efforts would fall under a separate incident response agreement.”

- Standardization and no exceptions:** A side effect of offering a comprehensive program like the **ResilienceReady Program** is that you will insist on standardizing the client’s environment to meet your stack requirements. This is good for both you and them. Let the client know every device in their org will be covered. This “no exceptions” stance (all endpoints must be in the program) makes them safer and your job easier with fewer unknown variables. It also can increase your revenue (more endpoints under management). Emphasize that standardization is part of ensuring the promised outcomes (one weak link can break the chain, so there can be none). Most forward-thinking clients will accept that logic, especially if tied to things like compliance: “If an unmanaged PC causes a breach, you will be noncompliant and at fault, so let’s avoid that by enrolling ALL your PCs in the program.”

**In summary, deliver the ResilienceReady Program as a complete package: technology + consulting + support.**

You become their virtual CIO for resilience, not just an IT fixer. Bundle in quarterly reviews and strategic guidance, as these reinforce your value and help you build pipelines by identifying upsell projects (like if a risk assessment reveals something outside your base package, you can propose a project to fix it). The goal is to form a partnership where you are actively managing their risk and stability, not just reacting to tickets.



# Pricing the ResilienceReady Program

One of the most common questions is, “What do I charge for all this?” Selling a comprehensive package like this is typically done at a premium price point, given the extensive value and tools included.

Here are some suggestions on how to approach pricing, based on industry best practices (note that all amounts are in US dollars):

- ▲ **Aim for outcome-based, per-user pricing:** It's best to price the program as a **per-user per-month (PUPM) fee**, which, internally, is derived from all the per-device and labor costs. This makes it easier for the client to understand and budget (“It's \$X per employee for comprehensive protection”). Usually, MSPs charge within the range of \$225–\$250+ PUPM for a package like this. In some markets or with more inclusions, it can even go above \$300 PUPM.
- ▲ **Ensure healthy gross margin (~50%–70%):** At ~\$250/user and with efficient costing, you should see about 50%–60% gross margin on the service. Many MSPs target even higher (60%–70% margin) for advanced security and compliance packages because of the high value delivered. The key is to calculate all your costs per user: the cost of all software/tools (EDR, backup, etc.), plus the labor time you'll spend for maintenance, support, reviews, and so on. Within N-able U, the N-able education and training portal for N-able customers, there is a “Costing Calculator” that can be used to tally these costs. If you have access to that or a similar spreadsheet, use it. Input your costs for licenses (list all the tools in the stack) and your fully burdened labor rate, and don't forget to include labor for those quarterly reviews and any “unexpected” work. Once you know total cost, apply your desired markup to achieve, say, 60% margin, and that's your price.

## Pricing caveats and considerations:

- ▲ The \$225–\$250/user pricing **assumes you are including most or all of the services** described (managed EDR, managed cloud backup, etc.) and using standard pricing for those tools. If you use different tools or have special deals, it could affect cost, but not drastically. Always price to the value, not just cost-plus.
- ▲ If you're using a different stack (e.g., different EDR vendor) adjust accordingly, but **don't let clients “opt out” of parts of the program to save money**. The program is a package.



- ▲ **Labor costs:** The model assumes about a \$50/hour fully burdened tech rate. If your labor is costlier (or cheaper), adjust. Notably, because this program leverages automation and outsourced SOC, it's designed so that your internal labor isn't huge, which is good. If you tried to do 24/7 SOC monitoring yourself, your labor costs would skyrocket.

- ▲ **What's included vs. not:** Make sure your price and contract clearly define what is covered. The intention is for this to be comprehensive, so it includes a lot—security tools, monitoring, regular maintenance, user support, and more. But as mentioned, you may exclude lengthy incident recovery labor, or projects like major upgrades. Those could be billed separately. Some MSPs include a small block of hours for remediation or give a discounted hourly rate for incident work as part of the package (example: “If something big happens, we'll handle it at \$Y/hour,” or “Includes up to Z hours of incident recovery—beyond that, it's billable”). Decide on that and make it clear.
- ▲ **No good/better/best—this is a best-only offering:** This kind of resilience program is usually your top-tier service and the recommended plan for anyone serious about compliance and security. Many MSPs choose to offer it as the only option going forward for their highest-risk customers and those that operate in regulated markets. Some may still have a basic plan for very small or lower-risk clients (see the [N-able Playbook “Defend & Prosper”](#) that includes examples of such programs like the “Identity Protection Program”).
- ▲ **Justifying the price:** At first glance, \$250 PUPM might sound high to a prospect who's used to paying maybe \$100 for basic IT support. This is where all the outcome selling and risk discussions come in (next section on objection handling). Explain that the monthly cost of the program will be far less than the cost they will pay to recover from an incident, and they are receiving comprehensive protection. Also point out that this program rolls in multiple services into one: it's their security, backup infrastructure, monitoring, user training, vCIO consulting, etc. all rolled into one predictable monthly price. If they tried to piece these out, it might even cost more (and certainly wouldn't be as effective).
- ▲ **Use the cost of inaction:** For example, if a client has 20 users, \$250/user is \$5,000/month. That's \$60K/year. That might seem big, until you compare it to the **cost of one significant incident**, which can easily reach six figures, or even routine downtime costs (if their revenue is, say, \$2M/year, \$60K is worth it to protect that \$2M). Frame it as **insurance and assurance**—a fixed, predictable cost to prevent massive unpredictable losses.
- ▲ **Flexible pricing models:** You might build the cost differently for different environments (since server-heavy clients cost more than cloud-based ones, etc.), but ultimately, presenting a per-user price is simplest for the client.

**In short, don't undervalue this offering.** It's not “IT support with a few add-ons.” You are selling a comprehensive business resilience service that bundles in multiple layers of protection, designed to reduce catastrophic risk. You are selling outcomes, not software licenses, so price it profitably.

While cheaper options may exist, they simply won't deliver the same set of outcomes. Clients who truly understand the value (or who have lived through a disaster) will pay for it.

Some MSPs find that if a prospect truly won't budget for it, that prospect might not be an ideal client. It's okay to walk away or refuse to downgrade in those cases (more on affirmative defense later).

Next, we'll cover how to handle common objections to the price and effectively communicate the value to close the deal.

## Handling sales objections: “It’s too expensive!”

When you present a premium offering like the ResilienceReady Program, you may get reactions such as, “Wow, that costs way more than we expected. We can’t afford that,” or “We’ve been fine so far, why invest so much now?” This is where your sales skills and reframing come into play.

Here are key strategies and example responses to help prospects see the value of your program:



- 1 **Reframe price as risk (cost of inaction):** Shift the conversation from the **price of the program** to the **potential cost of not having it**. Get the prospect to quantify what an incident could cost their business. For example:

**Response:** “I hear you. Any dollar amount can sound high until you compare it to the costs of a serious outage or breach. Let me ask: what would one hour of downtime cost your business? What about a full day?” Then, gently share industry data: “Many SMBs report thousands of dollars per hour lost. [A single cyber incident for an SMB now averages between \\$120K and \\$200K](#) to remediate. And that’s just the direct costs. Would your business survive that hit?”

(To make this example punchier, it would be best to draw on real stories that your own customers or a local business has experienced to make it more relevant to the prospect you are speaking with: “This actually happened to one of our new customers we just recently took on. Their clinic lost hundreds of thousands by not investing in proper resilience. This program would cost a fraction of that.”)

**Why it works:** This changes their mindset from “\$X per month is expensive” to “a breach or prolonged downtime would be far more expensive.” It introduces cost-of-inaction thinking. Most businesses greatly underestimate downtime costs. By doing this, you’re helping them do the math and realize the program is a small investment to avoid massive losses. Essentially, no CFO would spend \$0 to protect against a potential \$200K loss if they truly understood the risk probabilities.

- 2 Emphasize outcomes, not tools:** Make sure they understand they are not buying a pile of software subscriptions. Instead, **they are buying assured outcomes**. Many objections come when the client thinks they're paying for "stuff" rather than results.

**Response:** "Let me clarify. You're not paying for antivirus or backup software here. **You're investing in guaranteed outcomes:** that your data stays protected, your operations keep running, and you can recover from anything thrown at you. The **ResilienceReady Program** isn't a product; it's **insurance for your ability to stay in business.**"

**Why it works:** It steers them away from line-item thinking (comparing the cost of, say, EDR if they bought it themselves) and toward the value of the solution. Framing it as insurance/investment solidifies that this is about preserving their business, which is priceless if you think about it. This response also subtly positions cheaper competitors as incomplete: "Sure, someone might offer AV for cheaper, but are they assuring you that you'll stay in business through a disaster? Probably not."

- 3 Break it down into the three business benefits:** Clients often get sticker shock because they have not yet grasped everything they're getting. Refer to the three pillars of the program—prevention, detection, and recovery—and reinforce the breadth of coverage.

**Response:** "Remember, you're essentially buying three services in one:

1. **Prevention:** reducing the chance of a costly breach or outage happening
2. **Detection:** catching threats early before they paralyze your business
3. **Recovery:** if something does happen, getting you back up fast, so you don't lose customers or revenue.

Together, these three will protect your revenue, employee productivity, and customer's trust."

**Why it works:** It simplifies the value into digestible chunks and ties them directly to business outcomes (revenue, productivity, trust). It helps the prospect see the "why" behind the components rather than feeling overwhelmed by a big nebulous package. It also reminds them that cheaper offerings might only cover one of these pillars, not all three.

- 4 Use a real-world incident comparison:** Quantify the risk with a known statistic or example to make it real:

**Response:** “Recent data shows that most SMB breaches cost around \$150K (within a range of \$120K–\$200K) to clean up. That includes emergency IT work, downtime, lost sales, maybe legal penalties. For **less than 1% of that cost annually**, this program dramatically reduces your risk of ever facing such a catastrophe. In other words, the program isn’t expensive. **An incident is.**”

**Why it works:** Putting a concrete dollar figure on breach costs (\$150K) and comparing it to the program cost highlights the value. It’s basically the same logic as the first point but with a statistic to back it up, which many business owners find persuasive. It shows that this isn’t just your opinion, but industry reality.

(If you have a case study of a client who avoided a big loss due to the program, or a reference where something happened, but they were saved by these measures, share that story too.)

- 5 Align with their stated priorities:** During your earlier discovery, you should have asked what matters most to their business (ex., “Our e-commerce site can’t go down,” or “We must protect patient data,” etc.). Use their own words to justify the investment:

**Response:** “Earlier, you mentioned that maintaining client trust and keeping uptime were critical for you. Everything in our **ResilienceReady Program** is designed to protect exactly those priorities. Let’s make sure your **budget matches the things you said are most important**. Cutting corners on this would be at odds with the goals you’ve set for the business.”

**Why it works:** It gently calls out any inconsistency between their goals and their spending willingness. People may challenge your price, but they can’t really argue with their stated business priorities. This tactic (sometimes called the “**reflective alignment**”) refocuses the conversation on value vs. cost. If uptime, data integrity, etc. are truly vital, then investing in them is necessary. It helps the prospect realize “Yes, I did say those things matter ... so I need to back that up.”

**6 Highlight predictable cost vs. unpredictable loss:** Stress the budgeting benefit of your program:

**Response:** “One key reason our clients love this program is it turns unpredictable, potentially huge costs into a fixed, predictable operating expense. Without a program like this, you’re basically gambling. You might be fine this year, or you might get hit and suddenly owe tens of thousands in emergency recovery, fines, or ransom. With our **ResilienceReady Program**, you’re choosing to pay a known amount to significantly reduce and cover that risk. It’s smoothing out the ride—no budget surprises.”

**Why it works:** Executives and owners appreciate cost predictability and risk mitigation. You are framing your service to **avoid nasty financial surprises**. This also aligns with how insurance is sold. It’s an appeal to their desire for stability in budgeting and operations.

**7 “Who owns the risk?”:** If price haggling continues (like, “Can we remove something to make it cheaper?”), pose this crucial question:

**Response:** “I understand the need to control costs. Let me ask: if we reduce the price by scaling back protections, who will be taking on the extra risk that those missing pieces would have covered? The risk won’t disappear. It would fall back on you. Are you comfortable owning that risk?”

**Why it works:** This is a reality check. Often, cutting costs means transferring risk back to the client. If you remove, for instance, the MDR service to save money, no one will be watching the network at 2 AM. Is the client willing to accept the risk of a breach not being caught? By making them explicitly acknowledge, “If not us, then you,” it often makes them reconsider skimping. They usually realize they don’t want to carry that risk.

Using a combination of these strategies, you can navigate the price objection and help prospects see your ResilienceReady Program as a necessary investment, not a burdensome expense. The key is to stay consultative: keep tying it back to their business survival and success. Also, stand firm on value. If you discount too quickly or apologize for the price, you risk undermining the credibility of the program.

If, after all this, a prospect absolutely refuses to invest in proper resilience, consider whether you want them as a client. It’s okay to walk away from deals that don’t make sense.

Remember your **affirmative defense**. You don't want to take on a client who isn't willing to be safe because if they get hit badly, your business could suffer (reputation or even liability wise). As mentioned previously, not every prospect will be a fit for this program, and that's fine. It's better to have fewer, well-protected clients than many under-protected ones who might become firefighting nightmares.

In fact, you might say to a reluctant prospect: "I understand your concerns. Thank you for sharing them with me. But we only onboard new clients under this resilience program. It's for both your protection and ours. We have seen too many businesses get hurt without these measures, and we don't want that for you. If you like, I can refer you to another MSP who doesn't enforce the same set of cybersecurity and resilience standards that I do?"

This confident stance can sometimes even turn the tide (the prospect realizes you're serious and perhaps reconsiders), but if not, you part ways amicably.

Next, let's discuss how positioning such a program becomes a competitive differentiator for your MSP and how it even protects your MSP business, reinforcing why you shouldn't compromise on its components.

## Competitive differentiator and affirmative defense for your MSP

Adopting the ResilienceReady Program as your flagship offering does more than protect your clients. It significantly strengthens your market position and provides an affirmative defense for your MSP:

- ▲ **"Blue Ocean" differentiation:** Most MSPs are still selling piecemeal IT services or basic security. By pivoting to selling **business resilience outcomes**, you're creating a differentiated space for yourself—effectively a "blue ocean" where you stand out with a unique value proposition. You're no longer just another MSP offering antivirus and backups; you're offering to be a strategic partner who safeguards the client's entire business continuity. This is compelling to savvy SMB owners. It becomes your **competitive advantage** and primary differentiator when bidding against others. For example, if a prospect is comparing three MSP proposals, with two being standard break-fix or basic managed services, while yours is talking about ensuring their business never faces an extinction-level IT event, your proposal will resonate more with what the business owner cares about.
- ▲ **Value over price:** As we've hammered home, you're moving the conversation to value. Competing MSPs who only talk technology will often resort to cutting prices. But with your approach, **you compete on value, not on being the cheapest**. Many clients will pay more for confidence and peace of mind. By educating prospects on why resilience matters, you also subtly highlight competitors who don't mention these things as behind the times or not looking out for the client's best interest. That builds trust in you.

- ▲ **Affirmative defense – protecting yourself:** There's a concept in the industry of building an "affirmative defense" for your MSP. This means having documentation and measures that show you did everything reasonably expected to protect a client. If a client refuses certain critical services, some MSPs have used liability waivers. However, as the masterclass has taught, **don't rely on waivers or allow clients to opt out of basics**. Instead, make the program mandatory or walk away. This way, in the event of a breach, you can demonstrate that your client was following best practices (which also likely limits any damage). You won't be in a position where the client (or an insurance subrogation lawyer) can say, "The MSP failed to do X and caused this." You will have **standardized security across your client base**, closing those gaps that could be seen as negligence if left open.
- ▲ **No more exceptions = cleaner operations:** Selling this program as designed means **you set a high baseline standard for every client**. You'll no longer keep risky clients who refuse security measures just for the revenue. This improves your overall client portfolio health. It also simplifies your operations because everyone has roughly the same stack (which is easier to manage and support). Your technicians aren't juggling different levels of service for different clients; every **ResilienceReady** client has EDR, secure backups, and more—a unified approach. Standardization drives efficiency and reduces support headaches (leading to better margins too).
- ▲ **Building client trust and stickiness:** When you position yourself as the vCIO guiding them through not just IT but business risk management, you **elevate the client relationship**, which leads to higher client retention. They see you as irreplaceable because you understand their business deeply and are constantly helping them avoid trouble and succeed. It's much harder to switch away from an MSP who provides that kind of strategic value. So, while the immediate goal is to win new clients, the long-term benefit is **creating stickier, long-term partnerships**.
- ▲ **Marketing advantage:** You can market success stories of how your program saved clients from incidents or how clients feel more secure. Use testimonials: "Since enrolling in XYZ MSP's **ResilienceReady Program**, I sleep easier. We had a server failure and were back up in an hour with no data loss. It could have been a nightmare without them." These stories make for powerful marketing content (webinars, blogs, etc.) that draw in more prospects looking for something beyond break-fix IT.
- ▲ **Focusing on the right clients:** This approach naturally attracts clients in higher-risk, compliance-focused industries (healthcare, finance, legal, manufacturing with IP), which are often **willing to pay more** and value the service more. It also filters out very small or very cost-sensitive prospects that might not be profitable or stable for you. That's a good thing. This program is ideal for your **medium to highest-risk customers, operating in regulated industries** (finance, healthcare, legal, etc., where they must take cybersecurity and compliance seriously). By targeting them with a robust solution, you can carve a niche in those verticals.
- ▲ **Positive impact on insurance and compliance:** Clients in the program will likely fare better in cyber insurance assessments and compliance audits. You can use that as another selling point: "This package could help lower your cyber insurance premiums or at least ensure you qualify for coverage." And if something happens, being able to show all these measures were in place can reduce liability (some insurers might even require certain things that your program covers, like MFA, EDR, etc., so your clients won't be caught off guard or have claims denied due to lack of controls).

Making the **ResilienceReady Program** your standard offering sets a high bar that elevates your MSP's profile in the market.

You become known as the MSP who talks business outcomes and resilience, not just servers and PCs. This thought leadership can open doors, perhaps invitations to speak at local business events about cybersecurity resilience and more. It's a virtuous cycle: offering a genuinely valuable service leads to client success stories, which drive more credibility and sales.

## Protecting your MSP

From a pure business risk perspective, if all your clients have this level of protection, the likelihood of a devastating incident on your watch is greatly reduced. You won't have many, if any, panicked 3 AM calls about total data loss or massive breaches, and if you do, you have a well-oiled process to handle it. This protects your MSP's reputation. The last thing you want is for one of your clients to suffer an ugly, public incident that could make headlines and tarnish your record. By being proactive and even turning away those who won't take action at times, you preserve your brand as the MSP whose clients "don't make the news." And in the rare case something still happens, you can point to the documentation, reviews, and recommendations and show you did everything possible. That is the





N-able protects businesses from evolving cyberthreats. Our AI-powered cybersecurity platform delivers business resilience to more than 500,000 organizations worldwide, leveraging advanced end-to-end capabilities, simplified workflows, market-leading integrations, and flexible deployment options to improve efficiency and drive critical security outcomes. Our partner-first approach pairs our technology with experts, training, and peer-led events that empower customers to be secure, resilient, and successful. [n-able.com](https://n-able.com)

---

This document is provided for informational purposes only and should not be relied upon as legal advice. N-able makes no warranty, express or implied, or assumes any legal liability or responsibility for the information contained herein, including for the accuracy, completeness, or usefulness of any information contained herein.

The N-able trademarks, service marks, and logos are the exclusive property of N-able Solutions ULC and N-able Technologies Ltd. All other trademarks are the property of their respective owners.

© 2026 N-able Solutions ULC and N-able Technologies Ltd. All rights reserved.