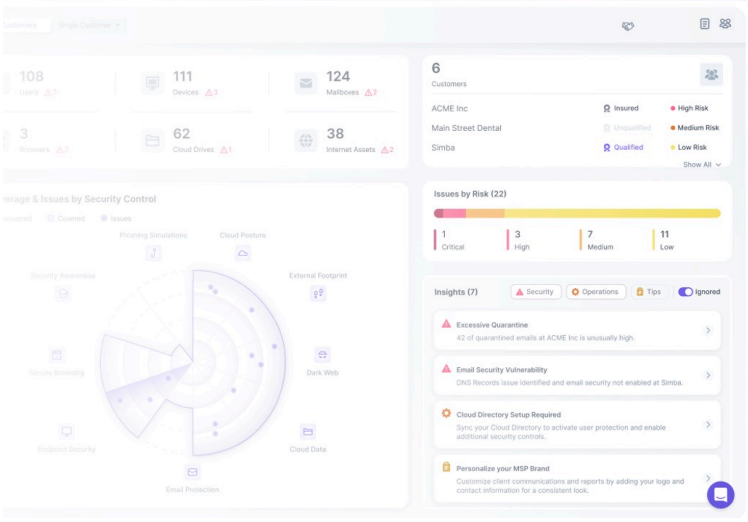
EDAO Guard – MSP to SMB Sales Kit

Sep 2025

For more information For more information, please visit https://edaogroup.io or contact us at info@edaogroup.io

Ref. No: EDAO-Guard-MSP1/25/0921



EDAO Group LLC

Elevator Pitch (MSPs to SMBs)

Short & Conversational

We provide small and mid-sized businesses with complete cybersecurity protection, acting as your dedicated security team. We protect your computers, emails, and data 24/7, while also helping you minimise risk by advising on technology policies and training your staff to avoid cyber threats. This way, you can focus on running your business worry-free.

Sales-Driven Version

Our managed cybersecurity service delivers enterprise-grade protection to your business through a unified platform, all handled by our expert team. We secure your endpoints, email, identities, and data with monitoring and automated threat detection. By leveraging EDAO Guard, an advanced AI-powered platform behind the scenes, we stop cyber threats in their tracks and even train your employees to recognise phishing and other risks – providing peace of mind that your company is safe from hackers while you concentrate on growth.

Discovery Questions for MSPs selling Cybersecurity Services

Engagement Phase 1 – Discovery

Connection Questions (optional)

- "Out of curiosity, what prompted you to start exploring cybersecurity solutions now?"
- "When you think about your company's data and systems, what worries you the most?"

Situation / Engagement Questions

- "What cybersecurity solutions are you currently using? Since when? Why did you choose them?"
- "How well do you feel those protections are working for you?"
- "If one of your employees clicked on a malicious link tomorrow, who would know and who would respond?"
- "How much time do you or your IT team spend dealing with security tools, updates, or alerts?"
- "Have your employees ever had training to recognise phishing attempts?"

👉 *Curious tone, no rushing. Always go deeper with follow-ups.*

Engagement Phase 2 – Problem Awareness

Core Question: "Are you 100% satisfied with your current cybersecurity/network solutions"

If they say YES (satisfied):

- "That makes sense. Just out of curiosity, what do you like most about your current solution?"
- "Is there anything you'd change about it if you could?"
- "Would you be against exploring additional solutions that may uncover and protect against additional threats and vulnerabilities?"

If they say NO (not satisfied):

- "What's not enough about your current setup?"
- "Have you experienced any security incidents or close calls?"
- "What impact did those have?"

👉 *Use labelling/mirroring here: "It seems like you're not completely confident...," "Not enough?"*

Engagement Phase 3 – Consequences (Loss Aversion)

- "Have you thought about what could happen if nothing changes and your company stays vulnerable?"
- "What would it mean financially and operationally if your systems were locked by ransomware?"
- "How would your customers react if their data was exposed?"
- "Would it be riskier to invest in prevention now, or to face the costs and downtime of recovery later?"

👉 *Tone shift to concerned. Focus on **risk of inaction**. Make them imagine the loss.*

Transition Question:

- "Now that we've uncovered these challenges, would you like to see how our platform addresses them directly?"

Presentation Phase

- Keep it short, 5–10 minutes.
- Focus **only** on what they mentioned as pain points.
- Tie each feature → directly back to their own words.

Example:

- "You mentioned being worried about phishing emails. Let me show you how EDAO Guard detects and blocks those before they ever reach your employees."

- "You said password security was a concern. Here's how we stop stolen credentials from being reused."

👉 *No irrelevant features, no long demos. Just connect solutions to problems.*

Commitment Phase

- **Option 1 (soft close):**
  "Based on what we've discussed, do you feel these solutions could address your main cybersecurity challenges?"
  → Follow-up: "Which ones in particular? How do you think they'd help you?"

- **Option 2 (forward close):**
  "Would you be against discussing next steps for implementation?"

If not ready to decide:
Always close the next step (e.g., a second call, demo, proposal review).
Never just send the proposal by email.

Objection Handling for MSPs Selling EDAO Guard to SMBs

Alternative Objection Handling Framework:

1. **Acknowledge the frame** (accept their reality without resistance).

2. **De-frame** (subtly loosen their belief by questioning or challenging).

3. **Reframe** (guide them toward a more results-oriented, risk/loss-aversion perspective).

4. **Advance** to pull them into your frame and move the sale forward.

1. “We already have antivirus.”

- Acknowledge:
  “Of course, most companies already use antivirus.”

- De-frame with questions:
  “Let me ask you — do you feel antivirus alone can stop threats like phishing , ransomware, leaked credential theft and cloud apps threats?”
  “How confident are you that it would catch an attacker who already got inside your network?”

- Reframe:
  Antivirus is a good start, but it only protects one layer, the device itself. Most threats today arrive through email, cloud apps, and compromised accounts. Wouldn’t it make sense to see if there are gaps your antivirus doesn’t cover?”

2. “This sounds expensive.”

- Acknowledge:
  “I understand — strong security can sound like a big investment.”

- De-frame with questions:
  “Expensive compared to what?”
  “What would you compare the cost of protection against — recovery, downtime, fines, or something else?”

- Reframe:
  “Often, the real expense is what happens if nothing is in place. Would it be riskier to invest now, or to gamble that you won’t be attacked while so many small businesses are being hit every day?”

3. “We haven’t had a problem so far.”

- Acknowledge:
  “That’s great — you’ve been fortunate up until now.”

- De-frame with questions:
  “Do you think that’s because attackers aren’t targeting you, or because they just haven’t tried yet?”
  “How long do you feel that run of luck can last in today’s environment especially with AI helping even ameteurs generate multiple attacks to create significant damage?”

- Reframe:

  “You would surprised to know that cybercriminals target businesses like yours, since they assume smaller companies aren’t actively protecting themselves. Wouldn’t it be smarter to strengthen security while things are calm, instead of waiting until the damage is done?”

4. "We're a small team, we don't need this."

- Acknowledge:
  "Absolutely — small teams have different priorities than large enterprises."

- De-frame with questions:
  "But let me ask you — why do you think hackers go after smaller teams more often?"
  "What would happen to your operations if even one account was taken over?"

- Reframe:
  "Whether you're five people or fifty, one incident, a ransomware attack, or stolen credentials can cause real damage. Doesn't that make protection even more critical for you?"

5. "We've been burned before."

- Acknowledge:
  "I can see why you'd be cautious — a bad experience makes it hard to trust again."

- De-frame with questions:
  "What happened last time that made you feel burned?"
  "What would you need to see this time to feel confident it's different?"

- Reframe:
  "A lot of our clients start small, focusing on their most critical systems first, then expand once they feel secure. Would that be a safer way for you to move forward this time?"

6. "How do I know your team is qualified?" - Directly advance to offer free trial

- Acknowledge:
  "That's a fair question — qualifications matter."

- De-frame with questions:
  "What level of proof would give you confidence?"
  "Would certifications, case studies, or live demonstrations help?"

- Reframe:
  "Our team has decades of combined experience securing SMB networks globally. But more important than what I say — wouldn't it make sense for you to judge based on how well our solution addresses the exact threats you're worried about?"

- Advance: "Let's install our solution in your network, free of charge for a 2 week period so you can observe first hand our services and its capabilities.

7. "I don't want something complicated."

- Acknowledge:
  "That makes sense — the last thing you want is another system adding stress (we are well aware of how many overwhelming security solutions are out there in the market)."

- De-frame with questions:
  "What does 'complicated' look like to you?"

"Do you feel tools should work silently in the background, or do you want more hands-on control?"

- Reframe:
  "EDAO Guard is designed to be invisible day-to-day — it reduces noise instead of adding more. Would it help if I showed you how it simplifies, instead of complicates, security?"

8. "We're in the middle of other projects."

- Acknowledge:
  "Of course — projects always demand focus."

- De-frame with questions:
  "What would happen to those projects if a cyber incident forced everything to stop?"
  "Do you think it's less disruptive to add protection now, or after something damages your progress?"

- Reframe:
  "Security is what keeps your other projects safe to complete. Would it make sense to secure them before finishing, so they don't get damaged/disrupted by a breach?"

9. "We're already using some security tools."

- Acknowledge:
  "That's good — you're already investing in protection."

- De-frame with questions:
  "How confident are you that those tools cover insider threats, phishing, and cloud vulnerabilities?"
  "What blind spots do you think still exist in your current setup?"

- Reframe:
  "EDAO Guard doesn't replace your existing tools — it fills in the gaps. Would you be open to seeing where your current security leaves off, and where attackers often slip in?"

10. "Isn't this just for big companies?" - (optional)

- Acknowledge:
  "I hear that a lot — many think security is only for enterprises."

- De-frame with questions:
  "But why do you think attackers go after small businesses even more often than big ones?"
  "What would happen if a single breach wiped out months of revenue for a smaller company?"

- Reframe:
  "Big companies can survive an attack — small ones often can't. Doesn't that make protection even more critical for businesses like yours?"

Value Propositioning

Value Proposition: Why Choose a Managed Security Service?

Small businesses are increasingly targeted by cybercriminals, yet most are not prepared for modern threats. Limited IT resources and budget constraints make it hard for an SMB to deploy the kind of complex, expensive security tools that large enterprises use.
That's where we come in. We offer a comprehensive cybersecurity service designed specifically for small and mid-size companies. Rather than you having to juggle multiple security products or worry about constant threats, we handle everything as your managed security partner.
Our team leverages a unified, multi-layered security platform (powered by EDAO Guard) to protect all aspects of your IT, from devices and email to cloud apps and user accounts, under one service. We continuously monitor your environment, preventing attacks before they cause damage, and responding instantly if an issue arises. The service is delivered with simplicity and outcomes in mind. You get enterprise-grade protection without the enterprise complexity. There's no hardware to maintain or complicated software for you to manage – we take care of setup, monitoring, updates, and incident response.
The result for you is peace of mind: your business stays secure and compliant, your employees stay educated about cyber risks, and you can focus on your core business knowing an expert team is watching over your security. In short, our managed cybersecurity service lets you operate confidently, free from cyber worries.

Value Proposition: Why choose our Managed Services?

Choosing our managed cybersecurity service yields tangible benefits for your business. We don't just sell tools – we deliver outcomes and peace of mind as a service.

Here are the key advantages of partnering with us for your security needs:

- **Comprehensive Protection, No Gaps**: Because we cover everything from endpoints to email to user training, you get holistic security coverage. All your critical assets and attack vectors are protected under one umbrella, eliminating the gaps that hackers could slip through when using piecemeal solutions.
- **Expertise on Your Side**: When you sign on, you essentially gain a virtual cybersecurity department. Our certified security experts monitor your systems 24/7 and respond to incidents immediately. You get enterprise-level expertise and oversight, which most SMBs couldn't otherwise afford in-house.
- **Simplicity and Peace of Mind**: Security becomes one less thing you have to worry about day-to-day. We run the tools, manage the updates, and handle any issues. You can focus on your business, knowing we're handling all the cyber defenses in the background. It's a hassle-free solution – no need for you to become a cybersecurity expert or manage multiple point products.
- **Cost-Effective & Predictable**: Our service is provided for a flat, predictable monthly fee. This approach is often far more cost-effective than purchasing several separate security tools (and certainly cheaper than the cost of even a single serious breach). You're essentially getting an all-in-one security stack plus a team to run it, at a price designed for small business budgets.

- **Regulatory Compliance**: We help you implement security best practices that protect you and help with compliance. By having us manage your cybersecurity, you'll be better aligned with any compliance requirements and eligible for cyber insurance because you can demonstrate strong security controls.

In short, our managed service provides business outcomes you can trust – a secure, resilient operation, rather than just technology. You get the benefit of top-tier cybersecurity without the burden of doing it yourself, which means peace of mind for you and trust from your customers.

Value Proposition: By the main security controls

EDAO Guard all-in-one service is a robust platform that integrates multiple layers of protection, allowing us to manage and optimize your security from a single point. You benefit from a seamlessly coordinated defense, without the hassle of dealing with multiple vendors or systems.
Here are the key components we provide as part of our managed cybersecurity offering:

- **Endpoint Protection**: We deploy advanced security on your computers and servers to block malware, ransomware, and other attacks. Every device in your business is continuously protected and kept updated, ensuring viruses or malicious software are stopped before they can cause harm.

- **Email Security**: We guard your business email (e.g., Office 365, Gmail) against phishing, spoofing, and malicious attachments. Suspicious emails are filtered or quarantined automatically, drastically reducing the risk of email-borne attacks, which are among the most common threats to SMBs.

- **Identity & Credential Monitoring**: Our service monitors the dark web and other data breach sources to see if your company's user accounts or passwords have been compromised. If employee login credentials or other sensitive identity information leaks online, we get alerted immediately. This proactive monitoring means we can promptly reset passwords or tighten access if we discover any sign of compromise, keeping criminals out of your accounts.

- **Phishing Simulations**: We conduct periodic phishing simulation campaigns to bolster your human defenses. This means we send your staff safe test emails that mimic real phishing attacks to see who might click. Employees who fall for the bait are gently alerted and coached. These simulations help employees learn to spot scams in a no-risk environment, making themselves less likely to be tricked by real phishing emails.

- **Security Awareness Training**: We provide ongoing cybersecurity awareness training for your team as part of the service. Through brief interactive courses and tips, your employees learn best practices – how to create strong passwords, recognize social engineering, securely work from home, and more. Regular training and quizzes keep security top of mind. An informed workforce means fewer mistakes and a significantly lower chance of a breach caused by human error.

Next Steps and Closing the Sale

After communicating your value and addressing questions, the final step is to guide the prospect toward action. Here are the recommended next steps to close the conversation on a positive, service-focused note:

- **Offer a Security Assessment**: Invite the prospect to a free or low-cost cybersecurity assessment or audit of their current environment. Explain that you can identify vulnerabilities or gaps in their IT safety and provide them with a report. This not only delivers immediate value (they learn something about their risk exposure) but also naturally highlights where your managed service would fill in those gaps. *(EDAO Guard's platform allows you to run a prospecting report quickly, which you can leverage for this step.)*

- **Customize the Solution**: Reiterate that your service is scalable and tailored. You can start with core protections and easily scale up as their business grows or as threats evolve. This flexibility often reassures clients that they can start at a comfortable level. Emphasize that because it's a managed service, they can add or adjust coverage without the headache – you handle the details.

- **Trial/Proof of Concept**: If the client is still hesitant, consider offering a short trial period or pilot. With EDAO Guard, you can create a 14-day free trial for any prospect. Seeing your service in action demonstrates the value firsthand. At the end of the trial, provide the prospect with a more comprehensive security business review report. Many small businesses appreciate this "try before you buy" approach, especially when dealing with a newer concept like fully managed security.

- **Close with Reassurance**: End the meeting or call by summarizing the main outcome they can expect: *"With our team taking care of your cybersecurity, you will have one less major worry. You'll know that an expert watches over your systems day and night, using the best tools available to keep your business safe. It's a partnership – we succeed when you're secure and thriving."* Thank them for their time and express excitement about the possibility of helping protect their business. A confident, positive closing reinforces our professionalism and approachable style, leaving a strong final impression.

- **Set Regular Follow-Ups**: Sales is about nurturing relationships and building trust. Set automated reminders to follow up promptly and consistently. Additionally, enroll prospects in email campaigns with valuable content and marketing materials to reinforce your messaging and keep them engaged.

By following these steps, you'll position the decision as low-risk and high-reward. Your goal is to make it as easy as possible for them to say "yes" to better security and peace of mind. Position yourself not just as a vendor, but as a long-term security partner committed to their success.