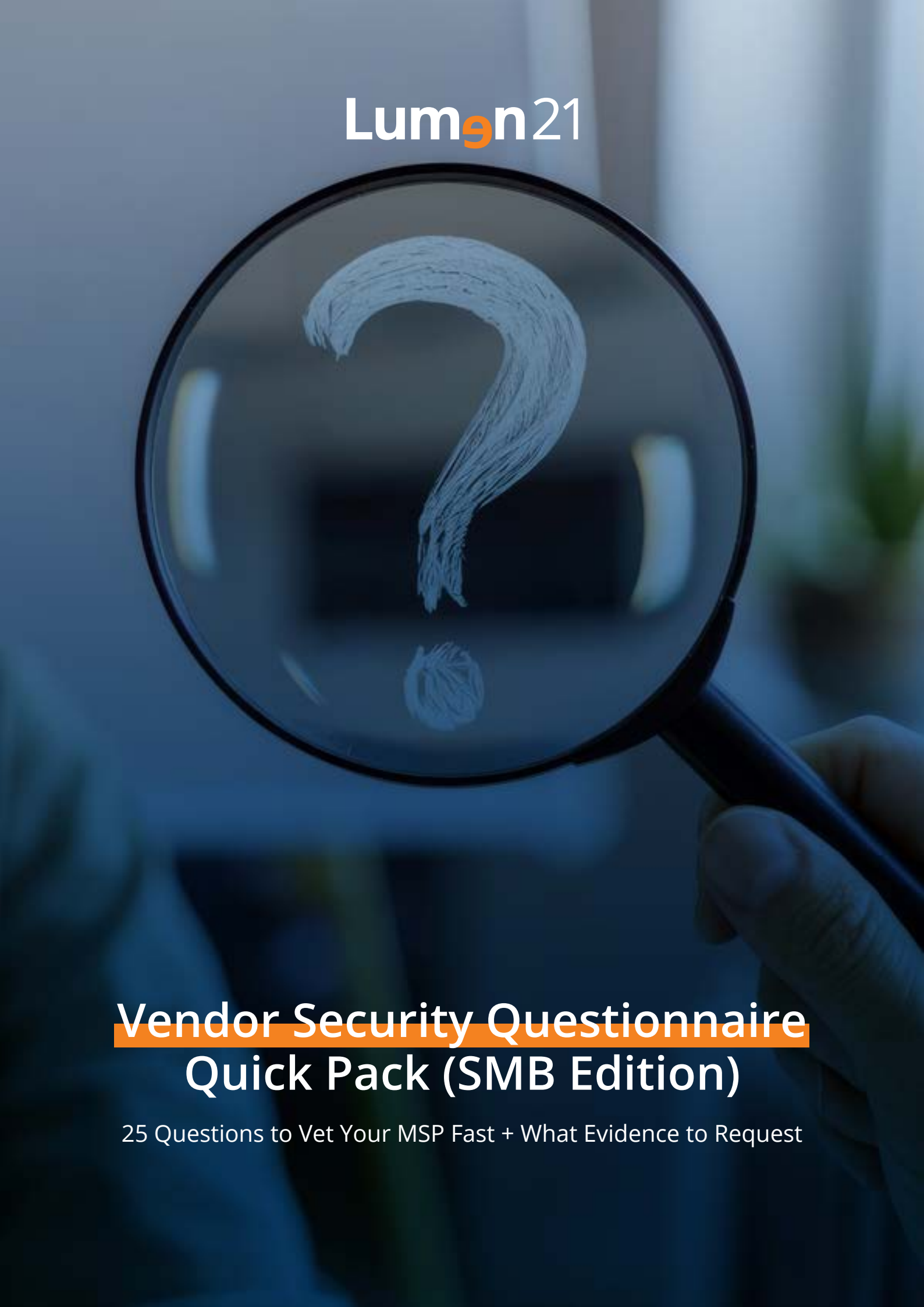
Lumen21



Vendor Security Questionnaire Quick Pack (SMB Edition)

25 Questions to Vet Your MSP Fast + What Evidence to Request

How to use this pack

Use these questions to evaluate a managed service provider (MSP) or security partner quickly—withoutrunning a full enterprise procurement process.

Ask for short, clear answers and evidence where it matters. If a provider is SOC 2 Type II verified, many of these questions should be supported by their audited controls (often shared under NDA).

Quick Vet Questions (25)

Lumen21

Lumen21, Inc. | sales@lumen21.com | www.lumen21.com

Identity & Access Management

1

1. Do you enforce MFA across all critical systems (cloud, PSA/RMM, VPN, admin tools)?
2. Do you use unique named accounts (no shared logins)?
3. Do you apply least privilege and role-based access by job function?
4. Do you perform periodic access reviews (and document them)?
5. What is your offboarding process and timeline (e.g., disable access within 24 hours)?

Endpoint & Server Security

2

6. Do you deploy EDR/MDR on all managed endpoints?
7. How do you handle patch management for OS and key applications?
8. Do you maintain an up-to-date asset inventory for all managed devices?
9. Do you standardize secure baselines/hardening for endpoints and servers?
10. How do you handle privileged access on endpoints (admin rights, elevation)?

Logging, Monitoring & Detection

3

11. Do you centralize logs from endpoints and cloud systems?
12. Do you monitor alerts 24/7 (internally or via an MDR SOC)?
13. How do security alerts turn into tracked incidents (ticketing/workflow)?
14. How do you define severity levels and escalation paths?
15. How long do you retain logs (and how is retention enforced)?

Incident Response (IR)

4

16. Do you have a documented incident response plan?
17. Do you run at least one incident tabletop exercise annually (and document it)?
18. How do you handle ransomware incidents (containment, isolation, recovery)?
19. What is your typical incident response timeline for after-hours events?
20. Do you perform post-incident reviews and track improvements?

Backup, DR & Resilience

5

21. How often are backups run and monitored?

22. Do you test restores (and how often)?

23. What is your RTO/RPO approach for SMB environments?

24. How do you protect backups from ransomware (immutability, segregation, MFA)?

25. Do you document recovery procedures and responsibilities (client vs MSP)?

B

Evidence to Request

(What to Ask For + Why)

Request only what you need. The goal is fast verification, not paperwork overload.

Evidence shortlist (high value)

- MFA policy screenshot / configuration proof
  - *Why: confirms MFA isn't "optional."*
- Access review template + last completed review (redacted)
  - *Why: shows discipline and repeatability.*
- EDR/MDR deployment coverage report
  - *Why: proves endpoint coverage across the fleet.*
- Patch compliance dashboard (sample report)
  - *Why: demonstrates operational execution, not intent.*
- Incident response plan (table of contents is often enough)
  - *Why: proves IR is structured.*
- Tabletop exercise summary (redacted)
  - *Why: shows IR is tested, not theoretical.*
- Backup job success/failure report + restore test proof
  - *Why: validates recoverability.*
- Vendor inventory sample + risk classification approach
  - *Why: confirms third-party risk isn't ignored.*
- SOC 2 Type II report availability under NDA (if applicable)
  - *Why: consolidated third-party validation of controls and evidence.*

Scope & Boundaries Worksheet (5 minutes)

Use this to prevent “grey zones” later.

1. **What systems are in-scope for the MSP?** *(endpoints, M365, network, backups, etc.)*
2. **What is out-of-scope / retained by the client?** *(internal apps, staff actions, etc.)*
3. **Who owns incident decision-making?** *(client vs MSP)*
4. **Who is responsible for user provisioning/offboarding approvals?**
5. **Where does evidence live and who can access it?** *(policies, logs, tickets, reports)*

If you’d like to shorten vendor due diligence and verify controls faster, request supporting evidence (and SOC 2 documentation under NDA where applicable) as part of your MSP evaluation process.

At Lumen21, we know that you want to be a confident owner who protects patient data and empowers your team with technology that just works. To do that, you need an IT partner who understands compliance, communicates clearly, and takes the weight of cybersecurity off your shoulders. The problem is you're stuck with an IT setup that's confusing, unproven, or leaves you wondering if you're truly protected — which makes you feel anxious, exposed, and frustrated when all you really want is to focus on running your practice. We believe healthcare leaders like you shouldn't have to become IT experts just to keep your data safe. We understand how stressful it is to carry the responsibility of compliance and patient protection without knowing if your systems are secure, which is why we've spent nearly two decades supporting clinics like yours — with 24/7 monitoring, HIPAA-aligned systems, and a team that speaks your language.

Start with a free cyber and risk assessment today! Contact us at Lumen21Cyber@lumen21.com or call us at 800-340-0927