



Frequently Asked Questions.

This document addresses the questions risk, operations, technology, and procurement teams ask most often when evaluating Quantum Defense, the composable fraud detection platform for SMB lending.

Need fuller architecture detail?

For utility specifications, integration patterns, and fraud-assessment timelines, refer to the Quantum Defense Solution Brief. **Replies within 48 business hours.**

DOCUMENT	SECTIONS	LAST UPDATED	AUDIENCE
QD-FAQ V1	10 · 52 questions	August 2026	Evaluation committee

CONTENTS

01 / 10	About Quantum Defense	6 Questions
02 / 10	The Three Utilities	5 Questions
03 / 10	How It Works With Your Existing Stack	5 Questions
04 / 10	Data, Privacy & Security	6 Questions
05 / 10	Integration & Deployment	6 Questions
06 / 10	The Analyst Experience	6 Questions
07 / 10	Outputs & Evidence	5 Questions
08 / 10	Customers & Use Cases	4 Questions
09 / 10	Commercial & Getting Started	5 Questions
10 / 10	About Quantum Lending Solutions	4 Questions

01

SECTION 01 OF 10

About Quantum Defense.

What Quantum Defense is, who it is for, how it differs from generic fraud tools, and where it sits next to credit decisioning.

Q
01

What is Quantum Defense?

Quantum Defense is a fraud detection platform purpose-built for small-business lending. It is composed of three composable utilities, Quantum Sentinel (AI scoring), Quantum Proximity (graph-based identity linking), and Quantum Workflow (fraud operations), that work together to detect, link, and act on fraud signals across the application-to-portfolio lifecycle.

- 01 **Quantum Sentinel:** AI scoring layer that reads open-web and physical-presence signals.
- 02 **Quantum Proximity:** graph-based identity linking across fifteen years of SMB applications.
- 03 **Quantum Workflow:** analyst-facing operations layer with case routing, override, and audit.

Q
02

Who is Quantum Defense for?

Risk, operations, and technology leaders at banks, credit unions, fintechs, embedded-finance platforms, and non-bank lenders running SMB lending programs.

Q
03

How is Quantum Defense different from generic fraud tools?

Generic fraud tools are calibrated on card-transaction or consumer-identity data. SMB fraud does not behave like consumer fraud: synthetic businesses, shell entities, address fronts, and fraud rings that recycle PII across applications are the dominant patterns. Quantum Defense is calibrated on Quantum's own SMB lending loss experience and linked across fifteen years of SMB applications.

BUILT FOR SMB FRAUD PATTERNS

ABOUT QUANTUM DEFENSE · continued

Q
04

Does Quantum Defense replace my bureau, ID verification, or bank-account verification vendor?

No. Quantum Defense is additive. It reads the open-web, physical-presence, and entity-relationship signals the bureau stack cannot see. Your existing vendors stay where they are. Quantum Defense plugs in as an API layer between application intake and credit decisioning and fills the gaps the existing stack leaves open.

ADDITIVE TO YOUR STACK

Q
05

Is Quantum Defense the same as Quantum Decisioning?

No. Quantum Defense is fraud detection. Quantum Decisioning (the Gen 5 Credit Model) is credit decisioning. They are separate products under the Quantum Lending Solutions platform, designed to work together when partners want both, but sold and deployed independently.

Q
06

Is Quantum Defense generally available?

Yes. Quantum Defense is generally available to partner institutions in the Quantum Lending Solutions ecosystem and to qualified prospective partners.

GENERALLY AVAILABLE

02

SECTION 02 OF 10

The Three Utilities.

What Sentinel, Proximity, and Workflow each do, how the three compose, and which combinations partners deploy in practice.

Q
07

What does Quantum Sentinel do?

Quantum Sentinel is the AI scoring layer. It reads publicly available signals about the business and the principal guarantor, web presence, social media, Secretary-of-State filings, aggregator and review sites, domain registration data, public maps, and adverse media, and returns a real-time risk score with an explainable evidence bundle on every application.

Q
08

What does Quantum Proximity do?

Quantum Proximity is the graph-based identity-linking engine. It links every incoming application against fifteen years of SMB lending history using PII and BII data, name, date of birth, legal name, DBA, EIN, addresses, phones, email, and IP, and returns first- and second-order matches across the application graph, highlighting prior applications that were confirmed fraudulent.

Q
09

What does Quantum Workflow do?

Quantum Workflow is the analyst-facing operations layer. It connects screening, scoring, case routing, override controls, and audit trail into your fraud workflow. It is the reviewer console your team operates in, or the API surface your own case-management system consumes.

Q
10

Can I deploy just one utility?

Yes. The three utilities are composable. Most partners start with Sentinel and Proximity together, AI scoring with network context, and add Workflow when they want their team operating in the Quantum console. Some partners deploy a single utility.

COMPOSABLE DEPLOYMENTQ
11

How do the three utilities work together?

Every incoming application runs through Sentinel and Proximity in parallel. Sentinel produces a risk score and recommendation; Proximity produces a network match graph. Workflow takes the combined output and routes the case to the right queue: clean applications proceed to decisioning, flagged applications open in the analyst console with the full evidence bundle.

03

SECTION 03 OF 10

How It Works With Your Existing Stack.

Where Quantum Defense sits in the origination workflow, what it does to your current vendor relationships, and how output flows downstream.

Q
12

Will Quantum Defense disrupt my origination workflow?

No. Quantum Defense deploys as an API layer between application intake and credit decisioning. Application data goes in; risk score, recommendation, and evidence bundle come out. Your underwriting flow consumes the output through your existing policy engine.

SITS BETWEEN INTAKE AND DECISIONING

Q
13

What if my bureau or IDV vendor already flags something Quantum Defense flags?

That is useful, not redundant. Quantum Defense gives you a second, independent read on the application using signals your bureau and IDV cannot see. When the layers agree, you have stronger evidence to act. When they disagree, you have a case worth a closer look.

Q
14

Do you require me to give up any existing vendor relationships?

No. Quantum Defense is designed to be additive to whatever fraud stack you operate today.

HOW IT WORKS WITH YOUR EXISTING STACK · continued

Q
15**How does Quantum Defense fit into our case management workflow?**

Three options. Output can flow directly into your existing case management system, cases can route into Quantum Workflow, or you can run a hybrid setup where clean applications proceed through your existing flow and flagged applications open in Quantum Workflow for deeper investigation.

- A Webhook into your existing case management system.
 - B Cases route into Quantum Workflow, our analyst console.
 - C Hybrid: clean cases stay in your flow, flagged cases open in Workflow.
-

Q
16**Can Quantum Defense feed our decisioning engine directly?**

Yes. The risk score, recommendation, and evidence bundle are returned as structured output, consumable directly by your policy engine or decisioning platform.

04

SECTION 04 OF 10

Data, Privacy and Security.

Which data Quantum Defense consumes, what leaves your environment, how training works in consortium and in-tenant deployments, and the encryption baseline.

Q
17

What data does Quantum Defense use?

Quantum Sentinel uses publicly available data only: social media, Secretary-of-State filings, aggregator and review sites, public maps, WHOIS data, and public news and court filings. Quantum Proximity uses no purchased data; it draws from our internal application corpus and fifteen years of SMB lending history. The only data you provide is the application data you already collect.

Q
18

Do you use purchased bureau or IDV data feeds?

No. Quantum Defense's AI scoring layer does not consume purchased bureau, IDV, or other third-party data feeds. Those feeds remain in your existing origination workflow and are not duplicated in Quantum Defense. That is a deliberate design choice: it removes per-call data costs and makes the product deployable in environments where data egress is restricted.

NO PURCHASED DATA FEEDSQ
19

Does my application data leave my environment?

In consortium mode, application data is transmitted to Quantum Defense via encrypted API connection. In in-tenant mode, Quantum Defense capabilities run inside your environment and no application data leaves your perimeter. The deployment mode is chosen during program scoping based on your data-governance posture.

DATA, PRIVACY AND SECURITY · continued

Q
20 Will my data be used to train models that benefit other partners?

In consortium mode, your participation strengthens the Quantum Proximity network, and the network strengthens your fraud detection in return. Network value compounds with participation. In in-tenant mode, your data does not leave your environment and is not used to train shared models.

Q
21 Is data encrypted in transit and at rest?

Yes. All data in transit is encrypted using TLS 1.2 or higher. Data at rest is encrypted with industry-standard ciphers. Detailed security documentation is provided as part of vendor due diligence.

TLS 1.2+ IN TRANSIT · INDUSTRY-STANDARD AT REST

Q
22 Do I need to provide historical fraud labels to start?

No. Sentinel uses unsupervised methods and does not require labeled fraud history to begin producing signals. Proximity surfaces network matches regardless of whether you have prior tagged fraud. As you provide feedback on confirmed fraud outcomes, the system improves on your specific loss patterns.

05

SECTION 05 OF 10

Integration and Deployment.

How Quantum Defense connects to your origination system, how long it takes to deploy, what consortium and in-tenant deployments look like, and where latency lands.

Q
23**How does Quantum Defense integrate with my origination system?**

REST API with OAuth 2.0 authentication. Application payload in; risk score, recommendation, network match graph, and evidence bundle out. The API surface is designed for direct consumption by your origination platform's policy engine. Webhooks are available for asynchronous status updates.

Q
24**How long does integration take?**

Sandbox in days. First production verification in weeks. Standard partner programs run 45–90 days from contract to first live transaction.

45–90 DAYS · CONTRACT TO LIVE

Q
25**What is the difference between consortium mode and in-tenant mode?**

Consortium mode is the standard deployment: you send application data via API and we return scoring and network matches. Network value compounds across participating partners. In-tenant mode is for institutions where data egress is restricted by policy or regulation; the capability is the same, but Quantum Defense runs inside your environment and no application data leaves your perimeter.

INTEGRATION AND DEPLOYMENT · continued

Q
26

Which mode should I choose?

Consortium mode is the right answer for most partners: it is faster to deploy, lower-overhead operationally, and gives you the full benefit of the network. In-tenant mode is the right answer when your data-governance policies prohibit application data from leaving your environment. The choice is made during program scoping.

Q
27

What is the latency on a verification?

Sub-second for the API response in standard configurations. The full verification cycle, including the Proximity match graph and the Sentinel evidence bundle, completes in roughly a minute, versus the 20 to 40 minutes the same review takes by hand.

SLA API response Sub-second	SLA Full verification cycle ~1 min	SLA Same review by hand 20–40 min
-----------------------------------	--	---

Q
28

Which origination platforms does Quantum Defense work with?

Quantum Defense is platform-agnostic. The REST API is consumable by any modern origination platform. Specific integration patterns are scoped during program scoping. If you operate on an unusual or proprietary platform, our solutions engineering team works with your integration team during onboarding.

PLATFORM-AGNOSTIC REST API

06

SECTION 06 OF 10

The Analyst Experience.

How analysts work inside Quantum Defense: the explainability model, the override path, false-positive tuning, and the console at go-live.

Q
29

Is Quantum Defense a black-box auto-decisioner?

No. Every score is explainable. Every signal in the evidence bundle is auditable. Your analyst sees what Sentinel saw, what Proximity matched, and why the score landed where it did. The model is a co-pilot, not a decisioner.

CO-PILOT, NOT A DECISIONER

Q
30

Can our analysts override the system?

Yes. Quantum Defense is designed around analyst-in-the-loop operation. The analyst is in charge on every decision. Every override is captured with the analyst's rationale, timestamped, and preserved alongside the verification record.

ANALYST-IN-THE-LOOP

Q
31

What happens when an analyst overrides?

Every override becomes a labeled training example that flows back into Sentinel. The model improves on your specific loss patterns over time, not on generic data.

THE ANALYST EXPERIENCE · continued

Q
32 **How do we tune for false positives?**

Threshold configuration. Sensitivity is configurable by product, channel, partner, or any other dimension your business runs on. Every flag includes explainable reason codes, so review teams can clear false positives quickly.

Q
33 **What does the analyst console look like?**

One screen per verification. A step rail showing each signal with a pass / fail / hold marker. An evidence panel with the actual artifacts: screenshots, WHOIS rows, search snippets, the Proximity match graph. Override controls on any step. The verification record is preserved automatically.

01 **Step rail:** every signal with a pass / fail / hold marker.

02 **Evidence panel:** actual artifacts, not summaries.

03 **Proximity match graph:** first- and second-order links.

04 **Override controls:** captured with rationale on every step.

Q
34 **Do we need to train our analysts on the console?**

A working session at go-live, plus a written operating guide. Most analysts are productive in their first review session.

07

SECTION 07 OF 10

Outputs and Evidence.

What Quantum Defense returns on every verification, what the evidence record contains, and how records flow to regulators, auditors, and bank partners.

Q
35

What do I get back on every verification?

A risk score from 0 to 100. A recommendation: approve, reject, or hold. A network match graph from Quantum Proximity. An evidence bundle with every signal that contributed to the score, attached to the verification record.

- 01 Risk score from 0 to 100.
- 02 Recommendation: approve, reject, or hold.
- 03 Network match graph from Quantum Proximity.
- 04 Evidence bundle with every contributing signal.

Q
36

What does an evidence record contain?

Everything that justified the verification. Every Sentinel signal with its source artifact, every Proximity match with the identity elements that drove it, the AI's written assessment, and any analyst override with its rationale. All timestamped, all linkable, all attachable to credit memos.

Q
37

Can I share evidence records with regulators, auditors, or bank partners?

Yes. The records are designed for exactly that use. Permanent, evidence-backed, and audit-ready by default.

AUDIT-READY BY DEFAULT

Q
38

Are records stored permanently?

Yes, within your retention policy. Verification records are designed to be retrievable a year out, useful when an application needs revisitation or a portfolio loss needs investigation.

Q
39

Can I export records to my own systems?

Yes. Records export in structured formats for archival, audit, or integration with your existing case management system.

08

SECTION 08 OF 10

Customers and Use Cases.

Who runs Quantum Defense today, what reference access looks like, the minimum deployment threshold, and the post-funding portfolio-monitoring story.

Q
40

Who uses Quantum Defense today?

SMB lenders across three categories: banks and credit unions, SaaS platforms and fintechs running embedded lending, and non-bank lenders running specialty programs. 250+ active partners across the QLS ecosystem.

- A Banks and credit unions.
- B SaaS platforms and fintechs running embedded lending.
- C Non-bank lenders running specialty programs.

Q
41

Can I see a customer reference?

Customer references are available under NDA following discovery and the fraud assessment phase.

Q
42

What is the smallest program you will deploy with?

Quantum Defense is designed to scale up and down. The cost-effective deployment threshold is determined during program scoping based on your origination volume, deployment mode, and utility selection.

Q
43

Can Quantum Defense help with portfolio fraud, not just application fraud?

Yes. Ongoing portfolio monitoring is one of the four capability pillars. After funding, Quantum Defense continues running: new applications are matched back to your existing book, so a fraud actor identified later in time still lights up earlier exposures on your portfolio.

[APPLICATION + PORTFOLIO COVERAGE](#)

09

SECTION 09 OF 10

Commercial and Getting Started.

How Quantum Defense is priced, what the evaluation path looks like end-to-end, and how to open a discovery call with the solutions team.

Q
44

How is Quantum Defense priced?

Pricing is aligned with the way lenders already buy bureau and identity signals. Specific commercial terms are scoped during program scoping, based on volume, deployment mode, and utility selection.

Q
45

What does the evaluation path look like?

Five stages, sequenced from discovery to first live transaction. Total elapsed time is typically 45 to 90 days from contract.

- 01 **Discovery:** week 1.
- 02 **Fraud Assessment:** weeks 1–4.
- 03 **Program Scoping:** weeks 3–5.
- 04 **Integration:** weeks 4–10.
- 05 **Live:** 45–90 days from contract.

Q
46

What is a Fraud Assessment?

You send us a sample of historical SMB applications, including any that were later confirmed as fraud. We back-test Quantum Defense against that sample and walk you through what it caught that your current stack missed. Typical timing: two to four weeks from receipt of the sample data.

TWO TO FOUR WEEKS · BACK-TESTED ON YOUR DATA

COMMERCIAL AND GETTING STARTED · continued

Q
47

Can I take a discovery call without committing to a fraud assessment?

Yes. A 60- to 90-minute discovery working session is available: we walk your team through Quantum Defense live, look at one or two fraud scenarios from your own program, and answer questions. No commitment.

NO COMMITMENT REQUIRED

Q
48

Who do I contact to get started?

partnerships@quantumlends.com. The solutions team replies within 48 business hours.

10

SECTION 10 OF 10

About Quantum Lending Solutions.

The company behind Quantum Defense: operating history, the size of the partner network and application corpus, and the wider product family.

Q
49

Who is Quantum Lending Solutions?

Quantum Lending Solutions (QLS) is the lending infrastructure provider behind Quantum Defense. QLS delivers origination, decisioning, compliance, servicing, and portfolio management infrastructure to community banks, regional banks, credit unions, fintech lenders, and non-bank lenders running SMB lending programs.

Q
50

How long has QLS been operating?

Fifteen years operating SMB lending, not just building software around it. The same team that runs origination, decisioning, and portfolio management for partner institutions built Quantum Defense, because the off-the-shelf options did not match the way SMB fraud actually shows up.

15 YEARS OPERATING SMB LENDING

Q
51

How big is the QLS partner network?

\$7B+ in originations across the partner ecosystem. 250+ active partners. Fifteen years of SMB lending application history. The corpus Quantum Proximity links against is the largest dedicated SMB lending application corpus in the market.

SLA

Originations across the network

\$7B+

SLA

Active partners

250+

SLA

SMB application history

15 yrs

Q
52

What other Quantum products are there?

Quantum Core (origination infrastructure), Quantum Flex (modular lending capabilities), Quantum Ignite (managed program services), Quantum Defense (this product), and Quantum Decisioning (the Gen 5 credit model). Each is independently deployable; partners can adopt one or several depending on the program they are running.

NEXT STEP IN EVALUATION

Schedule a Fraud Assessment.

Send us a sample of historical SMB applications, including any later confirmed as fraud. We back-test Quantum Defense against the sample and walk your team through what it caught that your current stack missed.

Schedule Fraud Assessment

HAVE A QUESTION WE DID NOT COVER? EMAIL:

partnerships@quantumlends.com

The solutions team replies within 48 business hours.

*Quantum Defense is a fraud detection platform; it is not a credit decisioning system and does not approve, decline, or price credit. Commercial terms, deployment scope, and utility selection are negotiated and documented in the Master Partnership Agreement. Past fraud-detection performance does not guarantee future results.

*SMB fraud detection products are configured per-partner during program scoping. Detection coverage, deployment mode, and utility availability vary by jurisdiction and partner posture. Quantum Lending Solutions is not a bank. **Quantum LS LLC** · NMLS ID 1587491.