Inception Document

Netbits Agent Factory — AI Agent Opportunities

Prepared: October 2026

---

1. Executive Summary

Netbits is an AI agent consultancy serving Estonian SMEs, operating a proprietary AWS-native agent platform (Agent Factory) with a fully agentified delivery pipeline: Plan → Build → Deploy. The internal delivery process is already strong. The critical gap is at the top of the funnel: acquiring clients.

The primary bottleneck is a live 30-minute sales presentation that must be delivered up to five times per week before prospects feel comfortable enough to engage with Agent Factory. The presentation is entirely generic — it covers AI agent concepts, architecture, and a walkthrough of the planning tool — and conversion data does not yet exist as the business launched in June 2026. The constraint is not content complexity but **trust**: prospects arriving from cold outreach will not share business details with a third-party system until they have had a credible, reassuring human-quality interaction.

The highest-impact AI agent opportunity identified is an **Agentic Sales & Trust Agent** — a dynamically generated, conversational website experience built on CopilotKit and AG-UI that replicates and eventually replaces the live presentation entirely. This agent reasons about visitor intent in real time, adapts its educational content to the prospect's apparent context, proactively addresses security and data-handling concerns, and guides the visitor toward registering and using the Agent Factory planner without any calendar booking or founder involvement.

This is not just a sales tool. It is a **live proof-of-concept**: a prospect who experiences a compelling agentic website interaction has already understood — by feeling it — what Netbits builds for clients.

Recommended first build: The Agentic Sales & Trust Agent (V1).

---

2. Identified AI Agent Opportunities — Ranked

Two candidate AI agent opportunities were surfaced during discovery. Upon analysis, they converge on the same core problem and are best understood as one agent at different levels of ambition. They are scored below using Marty Cagan's Four Risks framework.

Opportunity A: Agentic Sales & Trust Agent (Website)

A dynamically generated, conversational web experience that educates anonymous visitors about AI agents and Agent Factory in a responsive, personalised way, proactively establishes trust — particularly around data security and privacy, and guides the visitor to self-register and begin a planning session on Agent Factory — replacing the live 30-minute sales presentation.

Risk	Rating	Rationale
Value	🟡 Medium	The problem is real and validated: prospects currently will not self-serve without a human touchpoint. An agent that resolves this would directly unblock the funnel. However, it is unproven that an AI interaction can substitute for founder presence — this is the core hypothesis to test.
Usability	🟢 Low	Estonian SME owners are pragmatic. A conversational interface that responds intelligently and clearly to their questions is lower friction than a calendar booking flow. The agent must surface security/data assurances proactively and unprompted — failure to do so is the primary usability risk.
Feasibility	🟢 Low	CopilotKit and AG-UI are available, well-documented frameworks. Agent Factory already runs on AWS Bedrock. The founder has hands-on agent development expertise and an existing delivery pipeline. This is genuinely buildable by a solo developer in weeks, not months.
Viability	🟢 Low	No incremental per-unit cost risk at current traffic volumes. AWS Bedrock inference costs are negligible at low scale. The agent doubles as a marketing asset and a demonstrator of Netbits' own capabilities — compound value. No legal or compliance complications beyond standard GDPR data-handling for any EU-based web property.

Overall rank: #1 — Build this first.

Opportunity B: Async Sales Presentation (Video / Static Interactive)

A pre-recorded or scripted walkthrough of the current 30-minute presentation, delivered as a video or interactive demo, to replace the live call.

Risk	Rating	Rationale
Value	🔴 High	The live presentation's value is specifically its *responsive, two-way* quality. A static video does not build trust in the same way — the founder himself acknowledged this distinction. Low probability of meaningfully replacing the live call.
Usability	🟡 Medium	Easy to consume, but passive. Cannot answer questions, cannot adapt, cannot address the specific concern a visitor has in the moment.
Feasibility	🟢 Low	Trivially easy to produce.
Viability	🟡 Medium	Low cost to build, but low expected impact means poor ROI on the time invested.

Overall rank: #2 — This is not a genuine AI agent opportunity. It is content production. Do not pursue it as an agent build.

---

3. Recommended First Agent — Detailed Specification

Agent Name

Netbits Agentic Sales & Trust Agent *(Internal working name: "The Front Door")*

Purpose

Replace the founder's live 30-minute sales presentation with an autonomous, conversational web agent that:

1. Educates anonymous visitors about AI agents and Agent Factory in a responsive, personalised way
2. Proactively establishes trust — particularly around data security and privacy
3. Guides the visitor to self-register and begin a planning session on Agent Factory
4. Operates 24/7 with no founder involvement

What the Agent Does (Precise Scope)

The agent is the landing experience at netbits.cloud. When a visitor arrives, the agent:

- Greets the visitor and opens a natural conversation about their business context
- Infers the visitor's industry and likely AI agent use-cases from their responses
- Dynamically generates educational content about AI agent concepts tailored to what the visitor cares about (rather than a fixed curriculum)
- Surfaces Netbits' security model, AWS infrastructure, and data-handling approach when trust signals are needed — either on request or when the conversation suggests hesitation
- Demonstrates capability by *being* an agent in action — the medium is the message
- Offers a clear, low-friction next step: "Start your free planning session" → directs to Agent Factory registration

What the Agent Does NOT Do

- It does not attempt to close a commercial deal or discuss pricing
- It does not collect sensitive business data — it directs the visitor to Agent Factory for that
- It does not impersonate the founder or claim to be human if asked directly

Context Requirements Table

Data Needed	Source	Availability	Notes
Visitor's stated industry / company type	User input (conversational)	Always — elicited in opening turns	No PII required; general sector is sufficient
Visitor's stated AI familiarity level	User input (conversational)	Always — inferred from vocabulary and explicit answers	Used to calibrate explanation depth
Visitor's current question or concern	User input (conversational)	Always	Must include security/trust concerns as a first-class category
Agent Factory product	RAG knowledge base (Agent Factory KB)	Always	Covers platform features, security model, AWS

Data Needed	Source	Availability	Notes
knowledge			infrastructure, GDPR compliance, pricing
AI agent educational content	RAG knowledge base	Always	Covers agent definitions, architectures, use-case patterns, Estonian SME examples
Visitor's prior sessions (returning visitor)	Session cookie / Agent Factory user lookup	Sometimes	If recognised, personalise accordingly; if not, treat as anonymous
UTM / referral source	URL parameters	Sometimes	Useful context (e.g., came from email campaign vs. organic); graceful fallback if absent

When context is missing: The agent falls back to open-ended questions — "Tell me a bit about your business" — rather than assuming. It never invents context.

Behaviour Examples

Scenario 1 — Happy path: Engaged visitor, retail sector

> Input: "I run a small retail shop in Tallinn with 8 employees. I got an email about AI agents."
>
> Good: Agent acknowledges the retail context, explains what an AI agent could do specifically for a small retailer (e.g., inventory monitoring, customer query handling), links this to a concrete Agent Factory planning session. Tone is practical, not jargon-heavy.
>
> Bad: Agent launches into a generic definition of AI agents with no connection to retail. Visitor feels they are reading a brochure.

Scenario 2 — Trust/security concern raised

> Input: "This sounds interesting but I'm not comfortable entering my business details into some system I don't know."
>
> Good: Agent responds warmly, validates the concern as reasonable, explains specifically: data is isolated in a private knowledge base on AWS (EU region), Netbits has operated since 2011, GDPR-compliant, the planning session does not require any sensitive financial or personnel data to get started. Offers to show what the planning session actually asks before committing.
>
> Bad: Agent ignores the concern and continues the sales pitch. Visitor exits.

Scenario 3 — Visitor already knows AI agents well

> Input: "I'm an IT manager. I know what LLMs are. I want to understand how your platform is architected and what differentiates it from just calling the OpenAI API directly."
>
> Good: Agent shifts register immediately — discusses multi-tenant architecture, Bedrock, deterministic engines with Athena, MCP integration, the Plan/Build/Deploy pipeline. Treats the visitor as a peer.

> Bad: Agent continues explaining what an AI agent is to someone who clearly already knows.

Scenario 4 — Out of scope: Visitor wants a price quote

> Input: "How much does it cost to build an agent for my company?"
>
> Good: Agent explains that pricing depends on scope and is best discussed after a planning session (which is free), and offers to start one right now.
>
> Bad: Agent attempts to quote a price or says "I don't know."

Scenario 5 — Edge case: Visitor asks if they are talking to a human

> Input: "Am I talking to a real person or a bot?"
>
> Good: Agent is transparent — "I'm an AI agent built on Agent Factory, Netbits' own platform. That makes me a live demonstration of exactly what we build for clients." This turns the question into a selling point.
>
> Bad: Agent claims to be human or gives an evasive non-answer.

Scenario 6 — Edge case: Visitor communicates in Estonian

> Input: (visitor writes in Estonian)
>
> Good: Agent detects language and responds in Estonian throughout. All product and educational content is available in both Estonian and English in the knowledge base.
>
> Bad: Agent responds in English, creating friction for the target market.

Architecture Overview

Technology stack:

- **Frontend:** AG-UI + CopilotKit for the generative, conversational web experience — the UI is rendered dynamically based on agent state
- **Agent runtime:** AWS Bedrock (Claude or GPT) via Amazon Bedrock
- **Knowledge base:** Two isolated RAG knowledge bases on Amazon Bedrock — (1) Product & Security KB, (2) AI Education & Use-Case KB
- **Language support:** Estonian + English content in both KBs
- **Session memory:** Conversation buffer within session; optional persistent memory on Agent Factory registration
- **MCP integration:** Agent Factory's existing MCP server layer for any tool calls needed (e.g., checking registration status)
- **Hosting:** Amazon Bedrock AgentCore, AWS infrastructure; no new hosting required

Agent workflow (simplified ReAct loop):

1. **Receive** visitor message
2. **Reason** — classify intent: (a) educational question, (b) trust/security concern, (c) product/pricing query, (d) ready to start
3. **Act** — retrieve from appropriate KB, generate personalised response, update UI state via AG-UI

4. **Observe** — track conversation progress toward registration CTA; escalate to founder contact form only if visitor explicitly requests human contact

Input schema:

```
{
  "visitor_message": "string",
  "session_id": "string",
  "conversation_history": "array",
  "visitor_context": {
    "industry": "string | null",
    "ai_familiarity": "low | medium | high | null",
    "language": "et | en",
    "referral_source": "string | null"
  }
}
```

Output schema:

```
{
  "agent_response": "string",
  "ui_state_update": {
    "show_cta": "boolean",
    "cta_label": "string | null",
    "cta_url": "string | null",
    "suggested_follow_ups": "array"
  },
  "internal": {
    "intent_classification": "string",
    "kb_sources_used": "array",
    "trust_concern_detected": "boolean"
  }
}
```

---

4. Agency Progression Plan

The agent earns autonomy in three stages. Each stage has a defined capability, the human's role at that stage, and a promotion gate that must be cleared before advancing.

V1 — Guided Educator (Current Recommendation)

Capability: The agent handles the full educational and trust-building conversation autonomously. It answers questions, adapts to the visitor's context, and surfaces security assurances. The CTA at the end is a direct link to Agent Factory registration. The founder monitors conversations via session logs but does not intervene.

Human role: Observer and improver. The founder reviews conversation logs weekly, identifies failure patterns (unanswered questions, trust concerns not resolved, drop-off points), and updates the knowledge base

content accordingly.

What V1 is testing: Can an AI-driven conversational experience build sufficient trust with a cold Estonian SME prospect to produce a self-directed Agent Factory registration — without any human touchpoint?

Promotion gate to V2:

- At least 20 complete conversations logged (visitor engaged for 5+ turns)
- At least 3 self-directed Agent Factory registrations attributed to the agent
- Trust concern handling rated satisfactory in conversation review (no unanswered security objections in final 10 conversations reviewed)
- Estonian language responses are fluent and contextually appropriate (spot-check by founder)

V2 — Personalised Qualifier

Capability: The agent adds a qualification layer. Based on the conversation, it infers the visitor's likely highest-value AI agent use-case and pre-populates context into the Agent Factory planning session before the visitor registers — so their planning session starts with their industry and use-case already understood. The agent also sends an automated summary email to the founder after each completed conversation (via Amazon SES), flagging high-intent prospects.

Human role: Exception handler. The founder only reviews flagged high-intent conversations and occasionally spot-checks quality. The agent manages the full funnel from arrival to qualified planning session start.

What V2 is testing: Does pre-populated context in the planning session improve conversion from registration to completed inception document? Does the qualification email flag genuinely useful leads?

Promotion gate to V3:

- Registration-to-completed-inception-document rate measurably higher for agent-referred visitors than for direct/manual-referred visitors
- Founder spends less than 30 minutes per week reviewing agent-flagged conversations
- No critical trust or compliance incidents in V2 operation
- Agent handles at least 50 complete conversations without requiring knowledge base intervention

---

V3 — Autonomous Sales Front Door

Capability: The agent fully replaces the sales presentation — including the current calendar booking flow. The email campaign and sales partner now direct warm prospects to the website rather than to a calendar link. The agent handles initial contact, education, trust-building, qualification, and planning session initiation end-to-end. The founder's involvement begins only after a prospect has completed an inception document and expressed intent to discuss a paid engagement.

Human role: Closer only. The founder enters the process exclusively at the commercial proposal stage — having already received a qualified prospect with a completed inception document, in their industry, with their top AI agent opportunities ranked.

What V3 is testing: Can the agent fully absorb the 2.5 hours/week currently spent on presentations, with equivalent or better conversion to paid engagement?

Promotion gate (ongoing):

- Conversion from agent conversation to paid engagement is tracked and compared to the historical live-presentation baseline (once sufficient data exists)
- Founder's active time in the sales funnel reduced to zero pre-inception-document
- Agent operating cost remains below 5% of average deal value per conversation

---

5. Risks and Mitigations

Risk	Severity	Mitigation
Trust gap remains — prospects still feel they need a human after interacting with the agent	High	Design the agent to be transparent that it is AI from the first interaction, turning this into a demonstration rather than a deception. Add a clear "speak to a human" escape hatch (contact form / calendar link) so low-trust visitors are not lost, just routed.
Estonian language quality — LLM responses in Estonian may be fluent but culturally off, reducing trust with local SME owners	High	Build Estonian content directly into the knowledge base as first-class content, not translated fallback. Founder spot-checks Estonian conversations in V1. Consider a native Estonian speaker review of the knowledge base before launch.
Security concern not handled correctly — agent gives inaccurate or vague answers about data handling	High	Author specific, accurate security and GDPR content in the Product & Security KB. Create explicit behaviour examples for security concern scenarios (as in Section 3). Test this scenario category heavily before V1 launch.
Low traffic means slow learning — with few website visitors, V1 promotion gates may take months to reach	Medium	Direct warm prospects from the email campaign to the website *before* their calendar call — use the agent as a pre-call warm-up initially, even if the goal is eventual full replacement. This accelerates conversation volume while reducing risk.
Scope creep during build — temptation to add pricing, detailed project scoping, or CRM integration to V1	Medium	V1 scope is strictly: educate, build trust, direct to registration. Nothing else. All other capabilities are V2 or V3.
Agent Factory registration friction — if the registration flow itself is high-friction, agent handoff fails regardless of conversation quality	Low-Medium	Audit the registration flow before V1 launch. Ensure it asks for minimal information upfront and that the agent's warm handoff is not undercut by a cold sign-up form.
Single point of failure — the founder is the only person who can fix knowledge base content or prompt failures	Low	Document the knowledge base update process so it can be done in under 30 minutes. Set a weekly review cadence for V1.

---

6. Next Steps

Immediate (Week 1–2)

1. **Audit the Agent Factory registration flow** — identify and remove any friction that would undercut the agent's warm handoff. This is a prerequisite for V1 success and costs nothing to do first.
2. **Draft the two knowledge bases** — Product & Security KB (covering platform, AWS infrastructure, GDPR, security model) and AI Education KB (agent concepts, architectures, Estonian SME use-case patterns). This is the most important investment in V1 quality.
3. **Author behaviour examples in Estonian and English** — at minimum the six scenarios from Section 3, plus five more covering common objections. These become your V1 eval set.

Build (Week 3–5)

4. **Stand up the CopilotKit + AG-UI front end** on the existing netbits.cloud domain — the website redesign and the agent are the same project.
5. **Connect to Bedrock runtime** via AWS infrastructure — no new hosting required.
6. **Implement the two RAG knowledge bases** using Amazon Bedrock Knowledge Bases feature.
7. **Build and test the ReAct loop** — start with the core intent classification (educational / trust / product / ready-to-start) before adding complexity.

Launch and Learn (Week 6+)

8. **Soft-launch V1** — initially direct warm prospects from the email campaign to the website *before* their calendar call. This hybrid approach accelerates conversation volume while preserving the live presentation as a safety net. Track conversation logs weekly.
9. **Update the knowledge base based on V1 gaps** — the agent will reveal what it doesn't know through conversation logs. This is your most valuable feedback loop.
10. **Pursue V1 promotion gates** — once 20 complete conversations are logged and 3 self-directed registrations are achieved, evaluate readiness for V2.

End of Inception Document Generated by Agent Factory Planning Agent — Netbits, Tallinn, Estonia