

From Shadow AI to Strategic Asset How to Secure Your Business in the Age of ChatGPT Webinar-20250828_110153UTC-Meeting Recording

August 28, 2025, 10:00AM

1h 1m 11s



Nsovo Shimange 1:52

Alrighty, good morning everybody and welcome to today's webinar on how to secure your business and the age of ChatGPT. My name is Sawas Mangia. I'm the inbound marketing manager here at Struto and I'll be your host today.

So before we get started, we'll just go through some housekeeping rules. First of all, please feel free to use the chat feature and the Q&A button to submit any questions. This webinar is being recorded, but chat and house rules do apply, so if you feel like asking any.

Questions that are specific to your business. Feel free. We will edit those out when we do publish the video. So what happens here stays here. Basically the webinar will be available on the Struto universe after the session and your feedback is valuable to us. We will be sending out a survey near the end.

So please take a moment to fill that out. It does help us improve on these webinars. And Please note that by joining this webinar, we've opted you into our marketing updates, but you can unsubscribe from that at any time. Next, I'd like to introduce our speakers. I'm joined today.

By my CEO Craig and our CRM and AI administrator Jared. Just give them a moment to formally introduce themselves and then I will move on to the agenda of what we're discussing today.



Craig Wiltshire 3:16

Yeah, I'll go first. I'm Craig, Managing Director at Streeto and founder. Really, I look after the strategy for the company. I'm more and more involved in product these days and developing our product future feature set if you like.



Nsovo Shimange 3:18

OK.



Craig Wiltshire 3:31

Yeah, I'm Jared, CRM and AI administrator here at Struto. You'll typically find me stuck into HubSpot or our own Struto AI doing some configuration. Awesome.



Nsovo Shimange 3:45

Thanks so much guys. Let's move on to the agenda. So I think first of all we'll be discussing what Shadow AI is and then we'll give you a simple plan on how to move away from that. We'll show you how private AI platform will keep your data private, helps all the outputs.

Remain on brand and helps your teams work faster. Next we'll present a demo to you and then we'll give you a sneak peek of what the future could look like and in the end we'll make some time for some Q&A. So I'm going to move aside and let Craig take over. So Craig, would you like to?

Tell us.



Craig Wiltshire 4:23

Yeah, thank you very much, Sorgo. First off, I just wanted to get a feel and this is the elephant in the room really. It's like hands up if you know someone or you are someone who uses AI or public AI in your organization right now. Yeah, absolutely. There's no point in hiding it. It's the truth, right? We have access to these incredibly powerful tools, and we're living in an age of unprecedented technological change. It's the next industrial revolution, right?

And it's going to raise new challenges for us. So let's talk about Shadow AI, that proverbial elephant in the room. And Shadow AI is really any unapproved AI use in an organization where the company data flows to third parties outside of your control.

Right. And the thing with Shadow AI is it happens by mistake. Yeah, people going about doing what they're doing, needing to get things done, lead to data breaches, compliance breaches and non-conformist behavior that threatens the security of.

Of your business data. Simple as that, all right? And then loads of examples of shadow AI and what it looks like. And the most common one is folks using personal GPT Accounts or LLM Accounts for proposals, briefs, customer lists. You just want to have a quick look at something. Yeah, there's no audit trail, there's unknown retention policies.

In place, you don't know. Most users don't know whether their data is being used to train a public LLM or not. Most of the time, if it is a publicly accessible LLM. And remember that most of the LLM providers will provide publicly accessible versions of their products.

And non publicly accessible versions of their products. They provide versions that use your data to train what they do, but always allow you the option to opt out of that. And they provide versions that are very locked down, designed specifically for business use. I think a simple rule of thumb when it comes to publicly accessible LLM's is.

Like with social media, you are the product and your information can become part of the product, right? So it's one to avoid. So we want to give people that the opportunity to work around that. And then there are things like, you know, just last month, we all love Dharmesh at HubSpot for those of you who don't know Dharmesh at HubSpot.

He's the CTO. He has shares in Open AI, and last month he opened up access for ChatGPT to connect directly to your HubSpot portal.

This is a bad idea, right?

If you don't know what you're doing, if you haven't configured your GPT 5 correctly, it will be using your information and your information will be leaving your instance of HubSpot and being processed by the GPT 5 LLM.

In its domain, which may or may not be in the UK, which means that some data is leaving the UK and you've got GDPR problems and various other issues.

In it's very it's that time of the year when it's very, very close to inbound. So there's a bunch of information that we've been given that's obviously under wraps at this point. But watch this space because that LLM access and that those agentic tools are gonna be opened up in tools like HubSpot.

And whilst this is an amazing productivity enhancement, we need to be mindful of the setup and management of these things in order to do it. If you're a partner in the best way for your customers and if you're a company in the best way to protect your company data.

And then there's the good old spreadsheets being uploaded to public A I's for quick analysis. Think about public identifiable information, your pricing forecast, things like this being uploaded, another common one, which is.

Which is harder to manage, but but certainly is manageable, but harder to management is Microsoft copilot. Think about the breadth and scope that this tool

has within an organization, any misconfigurations or under configuration of the tool from a security posture perspective.

Is going to mean information being opened up to the wrong people within an organization. Yeah, so we need to think about how these things are used when these things are turned on. The organizations themselves are not responsible.

For the way you use the technology that's given to you, yeah. So the expectation and the onus is on you as an organization to make sure that information is secured and that data is protected throughout these processes.

So what are the risks? Well, obviously data leakage and IP loss is the is the main main risk with content being logged and used to train third party systems. So when we're out there and we're thinking about what a future state of the system needs to look like, we want to make sure that we're mitigating against something like that.

And then there's obviously the GDPR and contractual risk. For those of you with GDPR being front of mind, we've got to think about where data is being processed, if it's being processed, is it being retained? You know, there are models that and there are situations where we want.

External LLMS to process data, and that's not a bad, not necessarily a bad thing. It's only a bad thing if the retention policies around that information at the LLM side is not being considered and thought of as part of the process.

Yes. So you'll note like companies like, I don't know if some of you might use Click up. Click up has an A I enabled across the platform, but that a I works in such a way that the LLMs have a zero retention policy associated with them. So the LLM can do something but can't retain any information around them.

That so there are ways in which to work with these LLM's in order to make them, um, more compliant.

And then it's questions around the actual user themselves and the way they use the technology, right? So naturally, if they're using publicly accessible LLMS, it's harder to remain on brand. As organizations, we want to be able to control our brand message and any messaging coming from within the organization.

So you know when you use a public available LLM, the risks of it going off brand or hallucinating and just generally providing inconsistent outputs is going to ramp up significantly the way users use the tools.

Especially when it comes to prompting and prompt engineering would mean that you could get very, very different results with people using different publicly available LLMs. And then lastly, there's the decision on decisions based on quality. So

one of the challenges that you have.

With LLMS these things are designed to give you, the customer, the best possible answer, even if it means making up stuff and it's very good at making up stuff, specifically number based stuff when they do their outputs.

So for instance, we use LLMS extensively in order to build our product roadmaps, in order to build product forecasts, these types of things. And the LLMS are very good at telling us what our growth is going to look like off the back of sales and the numbers etcetera associated with it right down to margins.

And revenue projections, gross margins, profitability, you name it, they'll go work all that stuff out. But it's all a thumbs up, right?

Unless you're feeding it base information that it can actually use to do it, it's very, very easy for these things to do the best job they possibly can and give you the best answer, which is often a made-up answer.

So this leaves leaders with generally, like most leaders we find, fall into this binary trap when it comes to making decisions around A I. And they either just ban it, which just stifles innovation and doesn't do anything positive for the business, or they throw their hands up in the air and go, well, I'll just.

You know, accept it, take the risk, manage it. We'll deal with it when it happens and it will happen.

We think there's obviously a better path and that's to govern it, right? So why not centralize on a private audited AI platform that gives you the control that you require, but the tools that give your your customers or your teams?

The chance to move at pace and stay ahead of what's happening in the A I space, evolve with the A I space, stay in touch with the with the speed of progress. And that's why we've chosen the specific platform we have for Studio A I and Studio A I really is an A I assistant platform. Yeah, so there's a couple of.

Terms that are being bandied around at the moment and you'll have heard these terms, AI agents, AI assistants, things like that, right? So just to be clear on where Streeto AI sits, we classify Streeto AI as an assistant, not an agent. Yeah, you'll note our agents in the platform are called agents.

But just for a transparency in terms of the way messaging is going and the way the terms are being applied right now, this is an assistant category, not an agent category. OK, and the difference is pretty simple. The agents are persistent. They're always working for you and able to do things for you on demand.

Demand independently, whereas assistants are usually backed by some kind of

agentic behavior, but they are used by you when you need to use them and they work with you when you engage with them. So we're talking about assistants here. And we think about our Studio IO right really as a private walled garden. And in order to understand how that works, I think, you know, I've mentioned a team of assistants, but think about the security posture. So security posture is very important to me. It's always been important to me.

Those of you, some of you might know that in a previous life I worked with a bunch of guys who built and sold a network security company. Yeah, so security's always front of mind for me. And it's those same guys that I built that company with that we work with today around Street to AI.

I have a cyber security company called ITHQ and we work with them in order to secure customer tenants for the various instances of Street AI. And really what we offer is tenant isolation. So the chance to set up your own instance of the platform that's segmented from other platforms.

Your data is locked in, if you like, within a walled garden, and provide you with sort of enterprise class tools to track and audit the usage and engagement with the tools. This is what's missing from public LLM's, right? You don't know what they've been asked, you don't know what they're being fed, you don't know what they're responding with. And the power is through to AI is really around that audit trail. So it brings it into the business and gives you business tools to manage the engagement with AI assistance.

And then you get all the benefits of things like GDPR compliance. And then in fact, the Studio AI platform is SOC 2 and HIPAA compliant for those folks based in the States. Other things that we look for out of an enterprise class platform is your security tools.

Things.

Like single sign on role based account control, SCIM, SCIM being the ability to integrate the platform with other identity management software in the organization. Many, many organizations use Active Directory if they're a Microsoft House for instance. This allows it to integrate with that, so you're starting to deploy.

The system and the and in a way that IT loves because you're helping them do their job and finance will love, compliance will love because all aspects of the data control being taken into account.

We can also do things like tacky manage the scope of access to systems, yeah. So if we think about going back to the sort of plug GPT5 into HubSpot type scenario,

that's quite an open, broad scope form of access, right?

HubSpot provides MCP servers, Model Context Protocol servers with specific tools that allow you to manage the scope. We think this is a better way to access HubSpot, and we think MCP is probably the future of.

Application access. From an integration perspective, we see a future where we'll be able to spin up our own versions of these MCP servers and set up tools that are unique to us, our intellectual property that allow us.

Based on compliance, based on the job that needs to be done, setting up access to HubSpot for instance, and then allowing users to engage with that information in a controlled way, in a way that's secure and compliant.

We want our our, our private instance of of an assistant to have quota management and alerts, right? Because you know, I've got power users, I've got users that can burn through 20 million.

Tokens a day quite easily, yeah. And tokens being the sort of output function from an LLM, the information we're receiving back, yeah. And they'll go through 20 million, you know, that's like \$100 worth.

\$200 worth sometimes in a day. So you want to be able to set those limits and manage my budgets and so forth accordingly. And then we want to be able to create block lists and flagging systems for people trying to use the A I from inside our organization for the wrong reasons.

We want to be able to flag, block, manage these types of things. Last but not least, we don't want to be tied into any specific LLM provider. We want access to every LLM because every LLM offers something slightly different to the other. They all have a competitive edge in some way, shape or form.

And there's specific use cases where you might want to use them. Also, LLMs are moving at an incredibly fast pace, so as a new one becomes available, we want to be able to roll that out to our users, test, roll out, do the things we need to do in order to provide them with access to that so that they stay in current so that their productivity keeps moving.

Moving with the speed of the LLM. Yeah, the speed and the and the functionality of the LLM is the speed of thought these days, right? So we want to be moving along with that.

The other thing we want to be able to do is centralised knowledge and this is a this one is a complex one because when you talk to companies like HubSpot, you know, especially with some of the the sort of changes that they're going to be making in

advance of inbound this year and the announcements they're going to be making. HubSpot always says they centralize your data for you, but the truth of the matter is that they centralized front office information, right? Customer information that relates to marketing, sales and service. The organization is bigger than marketing, sales and service, and we believe everybody in an organization needs. Access to data, right? So centralizing data to us is not centralizing data about your customer. It's centralizing all data. Yeah, whether it's product development data, whether it's.

Certain forms of financial data that are allowed out of financial systems, whether it's R&D information, anything that's needed, it could be warehouse information and anything that's needed to run the business. Yeah, talking all data.

And we want to be able to centralize accordingly. And we want to be able to centralize all kinds of information, be they PDFs, be they Word documents, you name it, we want to be able to centralize. And then we want to be able to track our retrieval augmented responses.

So for those of you who maybe aren't as aware, but LLMs and assistants work together in order to serve you as a customer by augmenting your information with the information they have. We think about most LLMs, they're trained on a subset of data that's been available.

Hopefully they haven't been trained on your information, right? So we want to be able to come to work alongside what the LLM knows and provide it with information that you provided that it won't ingest but will use in order to answer and.

Reduced outputs for us, and these need to be audited, right? We want to see where the information came from that the LLM used in order to answer a particular question, and we want to see the source of that, and we actually want to see what came out at the same time.

And then the bonus of this version is obviously that with the centralised knowledge piece, the assistance that we deploy learning are learning from a centralised data point and they reindex and reversion everything that's going on. You simply keep updating the knowledge base.

Every agent then has access to the most recent version of any information that you have, and this provides A genuine single source of truth. You'll have heard this term. I'm just looking for a single source of truth so many times, but it means different. Things in different contexts. In a HubSpot context, it means a single source of truth with related to the customer. We're talking about a single source of data across your

organization going beyond the customer.

So what does this mean and why? How or what is important about this? Well, if you're involved in growth, speed is critical to your success, the ability to be agile, flexible, move quickly and agents, absolutely, or agents and assistants.

Absolutely play a part in that. We we're at a point now where we cannot create and deliver the amount of content that we generate without a I. It's simply impossible.

Yeah, we don't. We're we're scaling with agents. We're not scaling with people.

So in order to speed up, you've got to market to make sure that the content and outputs across your organization, whether they be marketing related, product related, research related, finance related, whatever it is, making sure those outputs are consistent, you have to be using that central source of truth.

And then for your IT leaders and the folks that are worried about compliance and the way technology is being used, we're going to provide them with clear DPIADPIADPIA endpoint inputs and really DPIA is about your data impact assessments.

From a GDPR perspective and making sure that they are clear and easily understood and then we provide them with auditability, the data residency and the other things that are required from a compliance perspective.

And last but not least, for our marketing and sales leaders, we give them one place to create accurate on brand content backed by your current internal knowledge. So.

With that, we want to give you a slight overview and give you an intro to the actual platform themselves. Before I dive in, any questions on that so far?



24:34

No.



Craig Wiltshire 24:35

You could go for a tiny.



Tony 24:38

Thanks, Greg. Just zip in right to the beginning and it may not be appropriate perhaps to answer it here, but I was, I was quite surprised to hear about hear the your view on what GPT is taken from us.

Particularly regarding the HubSpot connector, I I was very much under the impression that it didn't do some of the things that you were saying it does do like like see the personal data for instance.



Craig Wiltshire 24:54

But.

It all depends. Yeah, it all depends on how it's set up though, Tony. That's the thing. Yeah, it's a it's a set up question. So if someone doesn't know what they're doing, yeah, that's where you're gonna run into problems, right?



T Tony 25:12

OK.

Like me.

Yeah. No, I I guess so. I guess because I've got an assumption perhaps that that isn't the case. That was really interesting. Thanks, Greg. I'll I'll take that away and I'll dig a little bit deeper on it.



Craig Wiltshire 25:29

No, no, no worries.

There was someone else with a question.



T Tony 25:39

I think you're me, Betty.



Craig Wiltshire 25:39

There might be.

I think you're on mute.

Do the top. Give you a sec to type it in.

Once it come through.

Tom, is there a question there?



Tamryn Waters 27:01

Yes, it's just popped up here. Uh, what is the difference between Struto and ChatGPT Enterprise?



Craig Wiltshire 27:09

So when you use something like ChatGPT Enterprise, you're tied to ChatGPT.

So it does provide a lot of those protections that I've mentioned because you've got

an environment that you can narrow down and provide the security access control and so forth. So it's a really good option. But what you don't get is the ability to connect all your other LLM's and use the same interface. So you're tied into the. That's the difference. So we provide the same functionality, but any vendor's LLM can be used and we use them all. So at the moment, I mean we use Open AI, Anthropic Grok from Elon's crew.

You know, we use them all and Gemini extensively as well.

And then we'll use different versions of those also, depending on who's doing what so.

Oh.

It's gonna share my other screen.

T specs.

It.

I want to just go to the kitchen then.

OK, I'm sharing a back end dashboard here. This is the back end of the Street AI platform. So I just wanted to give you a nip around within this just so that you could understand a few of the concepts so that when you see.

Jared do the demo, you'll understand a little bit more and you'll have the context around what he's showing you. So a couple of things that we're going to find, we're going to see in the dashboard, we're going to be able to see things like, you know, an overview of my token usage and so forth.

Across the business, we're going to get an idea or quick access to the various functionality. We've got an API key set up where we set up the APIs to the various providers that we're going to use. This is where the secret sauce is really is sitting around in those APIs because that allows us to configure or control.

The nature of the API's input and control the LLM's functionality in a more centralized way. And the way we do that for customers is via ITHQ. They provide the access to all the LLM's and they lock down the LLM functionality and provide that back.

Through to our customers secure in the knowledge that it's being secured in the right way. What you also get because of that approach is the ability to scale your rate limits beyond what you would be able to do if you went and signed up for these APIs in the.

So when you go and sign up for an LLM and you go start using them, they constrict your rate limits until you pay more, pay more, pay more in order to increase the rate

limits and the access to tokens and various other features, whereas by consolidating that all behind one account we get a scale.

Hailing that happens that gives everyone access to the higher rate limits.

And then the AI agents as they called in this platform, but bear in mind their assistance and really what we're looking at is a way to create very specific little walk workhorses if you like. So most of you will have been watching videos on AI I'm sure you've been looking at videos on.

Um, prompt engineering and things like this. Well, a lot of the overhead of prompt engineering is taken care of by the assistants because the assistant is set up if I go into one.

We'll just use Jared's web demo. Webinar demo agent allows us to set up the roles of the specific agent in the system instructions, allows us to provide training files to the actual agents themselves. And when we think about data management, we're thinking about training files, we're thinking.

About separating information that the assistant needs to process consistently all the time. That's persistent versus information that it needs to go and access only when it gets asked to do so, I E in a rag environment, right? So when it's doing a retrieval based process.

So a training file is information, and Jared's doing a demo on tone of voice, where in this particular instance, this assistant has the tone of voice documents loaded into its memory and it'll process the system instruction, then it'll process the tone of voice, then it'll go and have a look at RAG and things like that in order to find.

Out how else it's going to go and answer a question. And then there's governance around how this particular agent can access our centralized knowledge base. So in this instance and in all instances, we use tags in order to separate and control which agents can see what.

So a document loaded into the knowledge base with the tag demo will be accessible from this agent. If it doesn't have the tag demo, it ain't going to go and see it. OK, there are various other bits and bobs in there that you can play with, but I'll do a private demo.

Demo for you if you need to see that. Then we've got tools that enhance the functionality of the actual agents themselves, so giving them access to MCP servers for instance. So here's a ClickUp MCP server, GitHub MCP server, HubSpot MCP server. This effectively allows us to communicate with those.

Pieces of software retrieve information from those pieces of software, or force an

update to those pieces of software.

The models are essentially the place where we manage the different LLMs and the access or who has access or sorry, which which LLMs our people have access to and you'll see the full gamut of available models in the back here. And this is because we have obviously you'll see the.

LLMs that way you've provided API keys, right? And the beauty of this is as soon as a new LLM comes out, we can enable and control access to it in the back end. Now you want to be able to control access to it in the back end because you might have some assistance that have been set up using a specific version of an LLM with.

One specific functionality that if you go and change the LLM might change the output, right? So one of the things we're always concerned about is getting consistent outputs for our customers and the ways we do that, one of them is by making sure that there's control around these kind of subsets of information around the LLM.

Has been used others around the prompt library and setting up specific prompts that users use in order to generate specific responses and that ensures A consistency across the platform. Just like out there in the real world, these agents or assistants can work together.

They can work in prompt chains and we can call one agent to do one job, another agent to do an editing job, another agent to do a publication job or something like that. And last but not least, the actual knowledge base.

And the knowledge base is where we store information, right? And all the information stored in our knowledge base, we have a look at something like this is tagged. So here we can see like for instance as an organization we use scaling up as our management methodology. So it's tagged with scaling up and I know that that information.

It's accessible to the assistant who does scaling up. It's also available to our product marketing and our street marketing in this particular instance. So a great way to manage that. Jared's actually got a confidential document in here which he's going to use to demonstrate something a little bit later. It's been loaded into the knowledge base.

Then the other things you're going to be interested in, and I'm not going to go deep into this because I don't want to show too much because this is obviously some of this is private information, but audit logs, who's accessing what and chat logs. This is going to be super important. This is every conversation that happens within the

platform.

Write down to the model when it happened, which assistance they used, if they used one and so on. We can go in there, we can see what was asked.

We can see the outputs.

We're doing some code here.

And so on and so on. So fully audited in the in the back end.

I think from an overview perspective, just from contextual, it's probably enough to for you to understand the nature of it obviously. Oh, one other thing, obviously users, important users, role based access control, you know, so you can set up.

Specific roles like a prompt manager, a content editor, this or that, and you can give them specific permissions with access to specific functions.

OK.

Jared, yeah.

Cool. So we've been talking about Craig's showing you through the the kind of back end of Street to AI, but I think it's time to have a look at the front end as well. Before we do, I just want to make note that.

I'm going to be talking about the knowledge base and training files here a bit as well. So just to go over that one more time, your knowledge base is your larger repository of data where you tag things and that allows agents to access it and your training files are you use a cache augmented generation.

Which essentially means that every time I load up a chat with a specific agent in that has specific training files, it's going to load those training files in every single time. So it's always, always, always in your chats.

First of all, I want to just kind of demonstrate how you can use assistance to govern your your your brand voice and your tone of voice in any kind of content that you might be generating.

So here we have an example.

Where I've just prompted an LLM that doesn't have any kind of knowledge of the tone of voice I want it to be speaking with or anything like that. And I've essentially said write me a blog about French Bulldogs and the challenges that one might face when owning one.

What we kind of get, just to read out the first paragraph, is they're everywhere, aren't they? Aren't they? Those adorable, batted, snorting little clowns trotting down the High Street, peeking out of tote bags and flooding your Instagram feed. The French Bulldog has well and truly captured the UKS heart, and it's easy to see why with their

comical.

Expressions and affectionate, playful nature, they can seem like the perfect pint sized companion. That's just the first paragraph from something that doesn't have any kind of governance around how it's being output and how it's supposed to sound when it's being output. It sounds like a cheeky monkey. Exactly.

If we now look here at the same prompt, but we're using the Struto AI webinar demo agent, which Craig showed you, has a tone of voice document loaded into it to kind of govern how we kind of want that output to sound and that tone of voice document, by the way.

Um was generated based on. I essentially just fed the Um assistant a couple of HubSpot's different blogs and how they sound and I said generate me a tone of voice document based on these blogs, so that's what it's using.

And what we get now instead is the same prompt, but our response is.

Here I'll just again read out the first paragraph. So you're thinking about welcoming a French bulldog into your life. We can't blame you with their comical expressions, bat like ears, and incredibly affectionate nature. It's easy to fall head over heels for these little characters.

You get that different kind of sound and I'll just go in a bit more here as well. It's tackling. So mind you, the the prompt is trying to the main kind of focus of the prompt is the challenges that one might face when owning a French Bulldog. I think this.

With this tone of voice document, we get that more kind of face on look and it tackles the challenges, but also provides you with solutions or kind of remediations. I think the word is for how you can kind of tackle these challenges.

Yeah, a lot more positive, kind of less dismissive tone of voice.

Any any kind of questions on this initial piece of loading in the tone of voice document into your training files and getting your your assistants to kind of give that kind of an output?

Not seeing anything, I will continue.

So.

The bit bit I'd like to look at next is the kind of knowledge base aspect. How, how can we leverage Struto A I to actually surface tagged data or tagged documents in our prompts and provide that additional context on.

Our own kind of personal domain knowledge that we want surfaced.

First, I want to look at a scenario where we've done this, where it's successfully gone

and retrieved specific documents from our knowledge base.

In this prompt, we're using again the Struto AI webinar demo agent and we saw that this agent was tagged with demo and there is a knowledge based document that's also tagged with demo that it's pulling. And this document essentially talks about Project Nightingale, which is done by Aura Dynamics Limited.

What we can see here is actually it's successfully retrieved this document and generated us a summary of this document. So Project Nightingale is a is the code name for Aura Dynamic Limited's secret development of next generation biometric authentication.

In this scenario, it's been prompted, gone and fetched the the specific tag document from the knowledge brace, brought it back, augmented our prompt with that additional context from that document.

And then generated a response based on that.

If we now look at a scenario where I've just prompted the LLM, it doesn't have access and hasn't been tagged with any kind of explicit access to that confidential document. What we get is the LLM trying its best to search the Internet and search its own internal.

Like training data on anything related to a Project Nightingale and it comes up with Project Nightingale was the code name for a partnership initiated in 2018 between Google and this. It's completely unrelated and it can't access the document.

Without having that explicit kind of access to her.

Craig, is there anything you want to add to any? I think the thing with that particular piece of the demo is that the document you loaded into the knowledge base could be anything right in future if you think about the amount of information available in your company.

Any of that information can be loaded into that knowledge base. People based on their specific roles, with access to specific agents that are tagged in the right way, would be able to access any information they need in order to do a job.

Essentially whether they know how to do some of that or not, right? And I'll give you a good example is we're busy developing product at the moment. That means that people like Consolvo and Tam, whilst we're always trying to keep them up to speed, they're often having to work ahead of the curve, right? They have to deploy content. Ahead of the actual final outputs being done. What we do is we load our product documentation and product information into the knowledge base, provide them with an AI assistant that has access to that knowledge base, which allows them to then go

and generate information confidently.

On the on the specific products off the back of that information, yeah, they don't have to be trained to the Nth degree on it. We can set up other agents to go and review any outputs that they create to check the the work, make sure that it's.

Compliant and then approve that and we can approve that work and then deploy it. So the knowledge base for me is the kind of secret sauce. It's that thing that enables your business to move forward.

Awesome. And back over to you then to finish up with.

What's next? Oh.

Cool. Let me stop sharing there.

OK.

So I wanted to talk a little bit just about where this is going, and to do that, I'll tell you what I'm going to do.

And then I'm gonna break from script here a little bit.

Share.

It's this one.

It's probably the.

26.

Cool.

So I just want to give you a little bit of a taste of what's to come, and there's a couple of terms that that you're going to hear being deployed soon if you haven't heard a couple of these terms already.

There's two OS.

Acronyms that look quite similar but mean different things. Yeah, we think about where we are with a I agents, with a I assistance, and we think of the world being opened up off the back of centralized.

Information and knowledge. We're going to get to a point where the AI agents, I E those entities that are working for us persistently in the background to do things for us, start becoming more and more powerful.

We're going to see a time where.

Certainly within the integration space, there's a coming together of a number of integration methodologies and the convergence is likely to happen.

In a context where A I is playing a massive part in all of that, right? And a lot of you, well, some of you all know that integration is our our second biggest area of focus within the business. It is an incredibly painful place to be.

Yeah, integrating platforms or integrating technology is painful. Managing the data, managing where the data is, setting up and making sure you're compliant, making sure data's in the right format that it turns up in the right place at the right time is difficult.

Yeah. And the the pain in the *** for me is that the business leaders that we engage with, they don't care about that difficult thing that you're trying to do. They're only interested in the outcome. Yeah.

And the truth is that the world of a I is moving to a place where outcomes are all that are going to be important. Yeah, how we get there is going to be less of the point of interest and the end point is going to be.

What everyone's interested in.

So in that, in that particular arena, there's a term called outcome as an agentic solution that you're going to start hearing more and more about. So think about within an integration space where technology comes together.

Platform like HubSpot has various agents within it, has various workflows, has various data points that are changing that can trigger activities within a system. Think about other business platforms that also have automation.

Yeah, that will also have agents within them. Think about a middle ground, a world where agents conduct and orchestrate those processes with between those systems and manage the data flow within it.

These particular agents will effectively be able to run your processes end to end across a business function. Think about a quote to cash scenario. Yeah, that's a long process. Some of it happens within a platform like HubSpot. Some of it might have to take place.

Within warehouse technology, some of it might need to take place within an ERP.

Yeah, all of it uses data. If we centralize the data, if we put the right agents in the middle, if we have technology.

That orchestrates those processes, we will effectively be able to run the processes end to end, yeah.

This is a a term or a service that's called will be known as BOAT. Yeah, business orchestration and automation technology. So we've been working with the last year or so.

Now, well, it's actually we've been working on this for three years, but with AI for the last year in order to figure out how we move to a world where we'll be able to do this. Yeah, so we'll be able to run services in an end to end capacity.

Where customers don't have to worry about the technology and only worry about the outcome and that's what we're interested in. So our focus is around this and that's going to turn up a new software service subscription model.

A SaaS model. Now you know SaaS, SaaS, software as a service. We believe that's gonna be turned around on its head in favor of a services as software model. Yeah, I told you that business leaders don't care about the plumbing that connects one system to.

Another system anymore. They just want the outcome, right? They don't want to be hassled by the technology that sits in the middle. So by us building a platform that's a layered agentic computational platform with an orchestration layer, we take on the technology aspect.

We become the provider of technology. What the technology is doesn't matter to the end user customer. And it shouldn't matter because this technology is moving so fast and will change so often that there's absolutely no point in them going to go get it themselves, right?

Because you're just gonna be changing it.

So you leave that up to us, we take that on and we start building out automated services for customers in the future. So you're going to see this being launched soon in the foundational customer program where we're looking for folks to work with on this.

People that want to take the integration to the next level, we're trying to build something that's super flexible that enables traditional connectivity as well as agentic connectivity in future. It's going to look something like this from a.

From a launch perspective.

This is where we're going effectively to a world where people stop buying software, they stop buying services done by people and they buy outcomes instead. And what we do is we work with people in an automated way to deliver end to end services.

Using traditional integration and AI working together. So we'll see this launching with us within the next week or so. So hopefully by the weekend a little taste of things to come, something to watch out for. I think this is.

Genuinely where the future lies from an integration perspective, I think it's important that we enable our customers now with things like assistance and so forth to get used to agents.

To start engaging with the technology in a Safeway, to start feeding in basic access to things like MCP service for HubSpot and whatnot, so that you're building up a

foundational sense of knowledge as to what's possible.

And then launching the platform in future in such a way that we've got people who understand what's going on, people who want to engage with it, people who are going to be able to make use of it for their customers or themselves.

So that's where we're headed. That's me. Thank you very much for for listening. I really appreciate it.



Nsovo Shimange 54:56

All right. Thank you so much, Craig. Thank you, Jared. I'd just like to open up the floor quickly. I think we only have 5 minutes. Are there any questions that anyone would like to ask on this?



T Tony 55:10

I'll just ask quickly. Well done, Jared. I'm being very old and assuming that as you appear a bit young to my jaded eye, I thought you did a lovely job with the presentation. I just wanted to say well, well done.



Craig Wiltshire 55:26

Thank you very much.



T Tony 55:27

Maybe see and maybe miss it way to the mark, but well done anyway. Craig, it appears the your big USP on this product will be the governance perspective. Is that is that the way that you're seeing it as well yet?



Craig Wiltshire 55:40

100 percent, 100%, you know you you can get a lot of this functionality everywhere, right?



T Tony 55:43

So I can buy.

Yeah, I was going to say, yeah, yeah.



Craig Wiltshire 55:48

That's the thing and and it's, you know, just like with the plugging ChatGPT and

something, I take the most secure posture in anything. I don't trust anyone basically, but and then you go, well, why should I trust you? And I go look.

 **Tony** 55:59
Yeah.

 **Craig Wiltshire** 56:05
The guys I work with at ITHQ, I've worked with for 25 years. Number one, we've built a security company in the past. It's their passion. Security is what they do day in, day out. They are ISO 27001 compliant.
They're the right people to manage the tenant for you within this context, right? Because that's what they're good at. That's what they do, and they secure to a stricter security posture than most.

 **Tony** 56:28
Mm.

 **Craig Wiltshire** 56:36
And I appreciate that. That's what I'm looking for.

 **Tony** 56:41
So do you would you see I I've got two more questions related. Do you see the the target market really then as enterprise rather than no?

 **Craig Wiltshire** 56:43
Hello.
No.
This is from the ground up. It's very accessible from a pricing perspective. So you know it, it doesn't, it's not out of reach for a smaller business. You know if if you're doing a half a million or more, I think you should be good to go with the platform. So it's dog letting himself in.

 **Tony** 57:06
Yeah, I I I just kind of, yeah, don't worry my my pup, I got a puppy. So I'm just thinking because sometimes, you know those smaller businesses speaking as a small

business, we're a bit more of a cowboy in our approach perhaps than we should be, you know, and ISO 27, 27,001 or 9001 or.



Craig Wiltshire 57:11

It.
Yeah.



Tony 57:26

Sock two or whatever. They're, you know, they we dream big about those things, but but maybe they're not quite so important.



Craig Wiltshire 57:30

Yeah, I think 100%. But I believe these things should be accessible to any size business. One of the thing that grates me is that SSO is usually an enterprise function on technology. That's a sin, right? That's just wrong.



Tony 57:41

Yeah, yeah, yeah, yeah, completely agree as well. Last question, speaking as a HubSpot partner, will we, you know, in our relationship with Struto, I should say speaking as a Struto partner.



Craig Wiltshire 57:48

Yep.



Tony 57:57

Will we have the opportunity to sell that on your behalf? Are you looking at going with a product? Yeah, so it OK.



Craig Wiltshire 57:57

Yes.
Yep. Yeah, yeah, yeah. You can set it. Yep, Yep.



Tony 58:06

Oh, interesting. Really interesting.



Craig Wiltshire 58:06

Yeah.



T Tony 58:09

Thank you very much.



Craig Wiltshire 58:09

Delani, have you got a question?

Sorry man, you're you're muted. The your microphone is just not working.

If you want to type it in there.



T Tony 58:26

We're watching him type. This is awesome.



Craig Wiltshire 58:27

Yeah, no pressure.



T Tony 58:31

I base making all the mistakes, going back and correcting the spelling and everything, but making sure.



Craig Wiltshire 58:35

You can always have AI generate your response.



T Tony 58:40

Get, get, get a move on. We're waiting. We're waiting. Go faster. Type faster.

See, this better be worth it.

The bigger question. That's absolutely right. Yeah. Sorry, Craig, go on.



Craig Wiltshire 59:15

About \$7000 upfront for the software itself. It's usually it's an annual upfront on the software element, and then there's a nominal amount that's paid monthly in advance on the tokens in order to have access to the actual LLM tokens and so forth.

Underneath that, there's also a support piece that we need to wrap around that. So

whilst you can with training, build your own agents and so forth, and we would absolutely encourage that, yeah, getting you up and running all the rest of it. It's going to be a nominal amount of service in order to get you up and running and then support you as you go. You should have support purely because the technology is changing and shifting all the time. So in order to stay abreast of things you need someone to work with. Just to keep you moving in the right direction.

 **Tony** 1:00:11
No.

 **Craig Wiltshire** 1:00:11
Maximize the ROI from the platform, so to speak.

 **Delali Kukah** 1:00:16
Thank you.

 **Craig Wiltshire** 1:00:17
OK.

 **Nsovo Shimange** 1:00:19
Alrighty, I think that's it from our side. That's all right. Terren Terren has sent out a survey. Please could you just take a moment to fill that out for us and then from our side if.

 **Craig Wiltshire** 1:00:25
That's a wrap.
OK.

 **Nsovo Shimange** 1:00:36
You didn't ask questions and you want further information, please feel free to contact us and we will be in touch. We'll send you the video and we will send you further communications around this topic and keep you informed about our next webinar next month. Yeah, thank you all for attending. Enjoy the rest of your day.



Delali Kukah 1:00:41

OK.

Thank you.



Craig Wiltshire 1:00:50

Awesome. Thanks very much. Thanks for coming to him as well. Thanks to Ladi.
Cheers. Bye. Thanks. Bye.



Tamryn Waters 1:00:53

Wonderful. Thanks. Bye.



Timur Musaev 1:00:55

Thank you all. Thanks a lot, guys. Cheers.



stopped transcription