Welcome everyone.

Today I am really thrilled to be chatting with Daniel Lai.

He's the managing director

of Aus AR nine is the ticket code here.

It's a global software company focusing on secure

data centric collaboration.

Basically, what does that mean?

Well, let's, uh, governments, military,

corporates secure sensitive information lets people control

who sees what, when they see it, all of that kind of stuff.

So you want to think here about clients

that include the Australian Department of Defense,

major law firms, defense contractors,

these kinds of players.

The company's origins go all the way back to 2006.

And really at that stage, Daniel might clarify this for me,

but I, I believe it was more of a consulting kind

of business that in-house developed some pretty cool kit.

And in 2018, they took that to the market with a focus of,

of commercializing that kit.

And from a standing start,

really on the revenue front in terms of the software, uh, as

of last year, it's about $10 million in revenue.

Um, so the company is really focused on

international expansion.

Uh, we've just raised a bit of cash there

to sort of accelerate that.

We've had a few strategic acquisitions along the way just

to bulk up the software and the offering.

So it's in a really exciting
and pivotal time for the business.
And, and today we're just really trying
to find out a bit more about it, peer underneath the hood,
and, and really who's, who better to speak
to than, than Daniel.
Um, before I welcome Daniel.
Just remember none of this is financial advice.
If you do have any questions, you've got a Slido link,
please value yourself of that.
And I'll, I'll put them to Daniel when we get the chance.
Uh, all of that is said and done.
Daniel, thanks for your time today.
Thanks very much. Pleasure to be here.
So let's, I said to you off air, we,
we want the big picture kind of stuff here,
and we're gonna have people watching this
who have been following the journey since the get go,
and we'll have people who are brand new to it.
So, just to make sure that we're sort of,
we're all on the same page here.
What's the, what's your elevator pitch
to the business when you are, you know,
meeting people in social settings
and they say, Daniel, what do you, what do you do?
And you go, I work, you know, actors.
And they go, what the hell is that?
What's your, what's your reply?

Well, you've already done that job for me.
You've done it through the introduction.
What we solve is that difficulty of sharing information
and collaborating on that information.
Because if we can't share it
and get it to the right person at the right time, really we,
there's no value in it.
Mm-hmm. Now, the opposite side of that value story is
what if it's sensitive?
What if it's classified?
What if we need to protect that value
and make sure that it's going to only the people we need
to share it with, with a need to know.
And that's the difficult conundrum that we sit in
that middle of that conundrum, where how do we do that?
Now, we do that at the data layer
because, um, essentially the network boundaries now
compromised or considered contested.
And we've just seen with Qantas, you know, if all of
that data in each one of those rows
and columns had been secured,
it wouldn't have mattered whether they were hacked.
Right, right, right. Yeah. Right.
So they've gotten in there somehow through the boundary
and through whatever with the social network, whatever.
And, and so, so we, we do that essentially.
Yep. Yep. That must be great
marketing for you, by the way.
Oh, I, I must admit, I did get,

I was traveling at the time.
So one, I was traveling with bloody Qantas.
Two, Two, I rang, I, I immediately went to, um,
Jerry Foley, our, our service, uh, senior sales guy here,
and general manager for the APAC business,
and said, do you know someone at Qantas?
Right. Pick up now. So yes, of course we do that.
And, and particularly when, you know,
as I've just summarized that story Yep.
They had been protecting their data.
This would've be, had a,
a far less impact on their reputation.
Yep. No, I guess they would
say, well, we are protecting it.
We had password protections and that,
but I guess if I'm, if I'm understanding
you, I would that work for you.
So that's, that's right. But
You know, that that's what Optus is, that's
what all of those guys say.
And, and obviously, um, you know, that's why, um,
what we do is the fastest growing area
of cybersecurity. Yep.
Okay. Let, let's dig into that a little bit here.
So, so what is it that companies are doing now
or previously, and what is it that's, that's new or, or,
or unique or differentiated about
what Aus is doing to solve that problem?

Yeah, look, that, that's an excellent question.

So, traditionally,

and up until probably, you know, a couple of years ago

we've been doing what's called boundary security

or enterprise security.

When you hear those words, enterprise security,

boundary security, network security,

what does all of that mean?

It means that I'm buying a firewall. I'm buying antivirus.

I've put in a, a secure operation center,

which has got a secure information management,

enterprise management system.

It's looking at the data coming in and out of the boundary.

Yeah. It's looking for anomalies.

It's trying to find, um, phishing attacks.

It's trying to find viruses.

It's trying to make sure that only trusted stuff is

coming in and out of the boundary.

Yeah. That's not your data. Your data is naked. Yep.

Your data's sitting in databases and email accounts

and all this sort of stuff

where a generic password gets me in

and once I'm in, there's nothing protecting the data.

Yeah. Now that's,

that's typically what's been happening over the years.

The other point to make is just

because I've got a firewall, how does it

and what is its relationship to the network control

and its relationship to the router

and its relationship to the application

and its relationship to the database.

Yeah. These things are actually unrelated.

Each one of those security controls is managed differently.

And if they're not managed consecutively

and in within a context, that's

where the vulnerabilities happen.

Interesting. There's no dependency, uh,

between those controls.

Yes. Now, we fast forward after all of these attacks

and, you know, the, the, the issues

that have happened in the US and Australia

and defense and all of these things.

And what they started to realize was, well, I can't

fix my network quickly

and the vulnerabilities in my network,

I can do the top eight.

Great. Mm-hmm.

How well have, how successful have most organizations

been put in there?

They've been saying they've been putting it in,

but their level of maturity is still really low.

Yeah. So it's just too hard. Yeah.

So everyone has gone, well, what is everyone

after they're after my data?

Mm-hmm. How do I protect my data and secure my data first?

Mm-hmm. As I said,

because if I get in, how do I make sure that,

and the second thing is how do I use my data outside of it?
We've got this huge productivity issue
around the globe stagnation and all of this other thing.
The one way out of all of this is increase in productivity.
The great promise of AI
and all of these other technologies is they're going
to increase productivity Mm.
And uplift global productivity
and global economics, um, activity.
Now, to do that, we need to share a,
a digital transformation of the supply chain,
the manufacturing, pharmaceuticals, all
of these things in the economy with that, that promise
that the digitization on the digital transformation,
which is what they're calling Industry 4.0,
is gonna accelerate all of that.
So we've gotta move data around, which means it needs
to be able to be activated
and consumed through that supply chain, which means it needs
to go beyond the boundary.
Mm-hmm. Not just gonna let everybody in.
So how do we make that happen?
And really the key to all of that is the data itself.
So that's what's called data centric security.
It's very easy with these kind of conversations,
for me in particular, to get way over
my head very, very quickly.
'cause I'm, I'm not a, I'm not a coder.
I'm not a programmer. I'm not a a a cryptographer.

But what's the, what's the simple layman's, uh, description
of how you achieve what you're talking about?
Really simple. It's called attribute based access control.
So what does that mean?
So we take attributes about you, yourself, you know, Andrew.
So who is Andrew? What's, what credentials does he have
that says, I am Andrew.
Okay, what other things do we know about Andrew?
What's his nationality? Does he have a security clearance?
What up to what classification of security can he see?
What devices, environmental attributes do we need?
Is his device secure And up to what level of classification?
What networks does it come across? Is that network trusted?
Is he coming across a secure network which
the corporation owns?
Or is he coming across the McDonald's wifi at a cafe
and he's sitting inside having a coffee?
Right. We take all of these attributes
and we form on the data, we bind those attributes,
and those attributes might say
that this document's cigarette, it's authored by Daniel.
Um, it, you know, it, it, it has to have these sorts
of roles before them to access.
So if it's financial information only,
the finance people can access it.
If it's personal information, they might see my name
and address, but they don't see my financial details.
So we can split these things up based upon these attributes,

and we put a policy in between which says,

Andrew can see secret information.

If he's on this device across this network, if he not on

that device, he can't see it.

Or maybe he can see less classified information at

McDonald's than he can in the building.

So we changed dynamically.

The view of all of this,

and this is all, comes from what's called zero trust.

Now, you would've heard of zero Trust secure. Yeah.

Really simply, what does that mean?

Trust nothing, validate everything. Right.

Now, what are we validating

through attribute based access control, we can validate

who you are, what your nationality are,

that you're coming in on your phone

and you're coming in across an untrusted network,

and we can set a policy to the data,

which says he can only see unclassified information.

Now you walk into the office building

and you get onto your corporate laptop,

and we go, okay, he's coming from a,

a land network connected directly, which we own,

and we trust up to secret.

He can see all the secret information he wants. Yep.

We haven't done anything except moved your context. Yep.

And it does it automatically.

So that's a very powerful tool.

That's interesting. Um, yeah,

I take that information
and you send it to somebody else,
those policies travel with it.
So now you send it to, to Ryan who's on the screen,
and Ryan tries to open it.
He can't open it because the policy
doesn't allow him to open.
It stays encrypted.
Right. But John, who's on the call is part of
that community of interest that we've allowed to,
and John can open it
Interesting. But John can't
send it to Ryan and Ryan open it.
So all of a sudden we're, we're putting security in
where people, it's almost invisible to the end user
and they're forced to, to meet the terms
and conditions of whoever sets it.
Yep. Yep. That sounds super powerful.
Um, I guess the, the next question is,
and this is, this is a, um, a positive
and a negative if I'm framing it up correctly, which is
we come across, um, various software companies
and they've got this really cool tech.
But one of the challenges is it's like you've got
to convince a customer to throw out their legacy, uh,
software, or they've gotta go
through some costly implementation.
And that's a negative 'cause

it's sort of a hurdle to get over.
It is also a positive though,
because once you've sort of made that transition, it tends
to be rather sticky.
Now, um, I guess where I'm going with this is, is
that what's the integration look like if someone comes
and knocks on the door and says, Hey, we are interested,
we've obviously got Qantas knocks on the door
and says, we've obviously got a problem.
We need, we need to fix this up.
How quickly can you implement this
and what, what kind of needs to change? Yeah.
Brilliant, brilliant question. Absolutely love it.
We, we deal with large defense organizations.
Now, they're not known for having, you know, the latest tech
that, well, actually that's not true.
Well, they have the latest tech
and tech that's not available to everybody else.
And then they have corporate systems, which are slow
to change, right.
Legacy systems they use still, you know, mainframes
and they might have a bit of Windows 10 in there
and some still Windows nines and running on Al and CC plus
and all this, all sort of stuff.
Yeah. So they have a whole mixture of all of these things.
Yep. You said it's, it could be a negative
and it can be a positive trick
is to be able to service both.
Right. And then you turn it all into a positive. Yeah.

So what we did most recently was acquire a
company called Directive.
Yes. Now, that directive platform enables us
to integrate with legacy systems as well as new systems.
So new systems which are potentially attribute based enabled
and have some form of data centric security.
And I can name a couple of areas there.
So let's say Cloud dira, which is a data analytics tool,
and it uses a product called Ranger, which has some
of these capabilities for the databases.
It pulls that information out of mm-hmm.
Now, directive can have a central policy management area
where I put my policies in
and just move the policy to Ranger
and use that as the enforcement point.
But it gives the organization still a central point
to manage all their policies.
But I might have a Neo four J database
for geographical data, which I'm looking at maps
and where I put pins on that data for, you know, enemy
or friends or whatever, or satellites,
or geez, all those trucks are lined up at that, uh,
nuclear facility we're gonna bomb
and what's being moved out.
Um, all of that sort of stuff.
Um, it can't do attribute based access control.
So the platform can consume that data
and enrich it with attributes and control it

and make that legacy system data centric, security enabled.
That's gotta be pretty compelling, right?
If it, that's an extremely powerful story. Yeah.
And I've just come back from, I mean, I, I, I've,
we've recently had conversations here about this product,
uh, that we've sold it to NEC
for them, Japanese Ministry of Defense.
I've just come back from the Japanese Ministry of Defense.
Um, I've met with the UK Ministry of Defense the last week.
Everyone is telling the same story.
Some of these, the, these type of capabilities, uh,
are being looked at in, in, in Talisman Saber.
Um, yeah. This is a really critical problem to solve.
Now let me explain why,
what's driving the adoption of this technology?
And there's two, two key points.
The first point is the geopolitical shift in
an uncertain world.
And when you go
and read the United States, um, security,
national security strategy,
it clearly articulates the importance of alliances.
Yep. And using that connectability
and integration with those alliances to deter aggression
and the shift in power and slow that shift in power.
And that's all circ, you know, all about Taiwan and,
and the Middle East and, and everywhere else.
So how do they do joint force integration,
not only strategy policy, um, how do we actually

pick something upon an Australian sensor, send
that targeting information to an ally
and have a third party fire something at it?
Mm. Do that quickly. Mm. Export joint force integration.
Yeah. Right. Uh, nato, same problem.
How do they use all, how do they combine as a force to,
to be greater than what they are individually Yeah.
And share those resources. That's a big problem. Yeah.
Right. That's where this type of technology becomes
absolutely critical.
That's the first story about why the world's looking at this
type of data centric security.
Yep. The acknowledgement of these organizations
and governments to shift
to data centric security is already known
and they've mandated zero trust architectures
and adoption per spy 2027 for these frameworks to be
and capabilities to be put into place.
Mm-hmm. Mm-hmm. And that's being driven by
that geopolitical concern.
Yep. Now that's what's driving this entire business model,
and it's driving the uplift in security spending globally.
Yeah. And so part of that is, well,
how do we use it smarter?
We need to share information.
How do we solve that information sharing problem? Yeah.
Yeah. It, it definitely seems like a pretty good tailwind.
Um, there's, there's not many silver linings to

that scenario, but I suppose that

that is definitely why Well,

Actually there is. Yeah.

If you ha have strong deterrents,

you don't have to go to war.

That that's a good point. That's a really good point. Yes.

That's, that's the whole, that's the whole policy.

People miss this. They all always, yeah.

Inevitably that means this is dark, we're gonna war. No.

What we want is to build up a strong enough deterrence

that we even up the balance of powers.

So we are forced to negotiate.

I, I think I heard Macron say this week,

you might have heard it, he said, for France to be safe,

we need to be feared,

or something like that, which seems

to be along the same lines as what you're saying.

Well, that's right. You know, um, it, it, it, it, it,

it is a great issue

and it's gonna be a very different, you know, we,

we've all grown up in relative security

and that's, you know, obviously

not the whole world has always been geographically secure.

We, we can't say that,

but in Australia we've grown up with relative security.

The question is how do we maintain that? Yeah.

Go in that way. And they're doing their

best to work out all of that out.

The fundamental problem they must solve for that to happen

is that sharing of information securely.

Yeah. And that's the niche that we're in.

Just to finish off on that, that prior point,

and I know it's, the answer is gonna be,

it depends on the customer and the requirements

and the rest of it, but just for our, our members, what,

what would you say a typical integration looks like?

Is this something that, you know, from signing

of the contract that they're up

and running in six weeks, six months or longer?

Or what, what, what's the

general ballpark sort of answer to that? Well,

It's all dependent upon the different organizations,

the skill sets that are inherent there

and the product that they choose to procure.

Right. So, where we are heading,

obviously I've talked about, uh, you know,

trusted data integration

and that effectively that directive product

and why we acquired it,

because it's a, a major component of that.

Yeah. Um, we have three products, trusted data integration,

which is that structured data, unstructured data platform,

and can do all those really cool integration things.

Yeah. Um, then there's the, um, NC Protect suite,

which does it for the Microsoft business application.

So if I want to build strong collaboration information,

sharings managing documents and PowerPoints and slides

and PDFs and CAD drawings, that's where we go to.

Yeah. That's if I want build it using teams and, and, and,

and those, those Microsoft products, as I said.

Then we've got another platform there,

which is called cogency, which is our original product.

Mm-hmm. And each one of these products, uh,

so pro Cogency could take a data implement

and it sits on any technology platform.

If you wanna bring your own team on it

in your environment, fine.

We'll build it on that. Um, if you want it in the cloud

as a SaaS service, you can consume it.

Which, which cloud do you want?

Do you want it on Azure or do you want it on Google?

It's, it's agnostic.

And this comes from, you know, your introduction,

ARCTA stands for architected trusted Information sharing.

We were a bunch of architects that came together

to solve this problem and ended up producing products

because they didn't exist in the marketplace.

Yeah. So we, we went through a transition from a, uh,

consultants to, to system integrators to,

uh, a product company.

So we've been on that journey because we know what we need

and what, we're not a technology company,

it's the business problem of trust

and sharing those, that, that stuff.

How do I share information? What's the constraints on that?

And how do I trust someone to, to do the right thing

with my technology that's driving our product development.
Yeah. How unlike most companies out there, which are,
I've got AI a back, woo-hoo.
Well, how did you get that? What's it do?
How does it solve the problem?
We are coming up from the problem
and the business value Yeah.
And out from there.
And I think that that's a real powerful story, having all
of those years of experience building product. Yeah.
My, my bells are going off in my brain.
There's, there's a few examples I can think of,
uh, on the A SX.
The companies have got a product which was really built
for them internally, and then they just thought, wait a sec.
Um, which is a great story. Um, well, think about
The Israeli market.
I mean, all often all of those products are coming out
of the military and then they're being commercialized.
Right. So, so it, it is not that different.
We, we are doing the same thing here in Australia.
We're, we're doing cutting edge difficult problems,
which gives us a competitive advantage,
and then we're productizing them and you
and applying them to different use cases as they become
required in the commercial sector.
Yeah. So, look, to answer your such question,
which I haven't, how long does it take?

Um, well, it takes a few hours to run up.
NC Protect, it takes a few a day for a cogency,
but director's a little bit different
because it does sit as a middleware layer Yeah.
In the environment. And it can do so many things
that it depends upon the use case.
So it could be a, a, a week's implementation
to, to whatever it is.
Yep. Um, sorry, a couple more naive questions, but,
but hopefully they, they're sort of sort
of helpful in building the foundation here.
Um, Daniel, if I'm reading you right, I don't need
to be an artist customer of anything to do with you guys
to participate in your TE technology.
If the counterparty that I'm dealing with is a, is a member,
so that's, that's, I think that's
what you're saying. That's correct. Right.
Well, essentially as an end user, you may
or may not be using our technology and you wouldn't know.
Right. The only experience difference in your experience is
that you are only gonna see the documents
that you're allowed to see
Or, uh, or are allowed. Yeah. Yeah.
Right. So, so, so, so all
of a sudden you don't know any different,
it doesn't change your experience with Word
or, or PowerPoint.
Yeah. It just says you are only allowed to use,
you are only allowed to edit these documents.

Okay. So I can only edit these documents. Okay.

Documents, I can't edit. Okay.

These documents, you know, um, so, so it it,

it does that for you.

Yeah. So your user experience is seamless.

I, it's, it's why I wanted to ask it just to order,

clarify that, because that's, that's a, that's a big deal.

The other thing that's always super interesting, it seems

to be far more common in, in the software space, is

that you have the potential for network effects.

You know, just the fancy way of saying

that the more people using it,

the more valuable the, the product is.

Is, is there a network effect dimension to,

to the software tech stack that you've got?

Well, there's a huge network effect.

And, and that's, so look, I, I guess per our, the people

who have been on the journey and the shareholders

and investors that have been on the journey, um, you know,

part of that journey is, you know, understanding

that this company is a very strategic company.

Yep. We're not, this is not consumer growth.

This is business to business growth. Yep.

Um, so they are really enterprise sales. Yep.

But what we are doing there is that we have chosen two areas

where, one, we've got a niche technology,

it's got a high value proposition,

and if we win it, there's a network growth effect.

So, and that is the, obviously the military.
Now, let me start with an example of
that network growth effect in the military,
and then I'll go on to the network growth from a defense
industry capability, um, a defense industry base,
industrial base, which services that defense organization.
So they're the two key markets that we focus on exploiting.
The first one is obviously defense
with classified information
and sensitive information gives us a unique value
proposition on a high value problem to solve.
And we've talked about that information sharing problem.
The, the classified information means
that there's not many players that will go to
that extra mile to build their products to the level
of accreditation that is warranted for these organizations
to be able to adopt them.
That's why we have a relationship with Microsoft.
That's why they use our product,
because we do that extra 10% that they don't invest in,
because it's not commercially applicable to all the,
the other organizations yet to, to niche for them.
Too. Niche. Yeah. So they, they partner with us to do that.
Um, and the directed product platform is the same.
There's, you know, MuleSoft out there and other platforms,
but they don't do security.
So we sold that extra 10%, which actually means
that these products are viable in the defense space
and national intelligence space.

Now, obviously I got, the reason that I met with JO is
because we get introductions from our customer who say,
we already trust this, this already works for us.
This is what we are doing about data centric security.
And they are asked how are they managing
that from solving that problem?
A good example of that was nato.
NATO asked the Australian Department of Defense,
what were they doing on data centric security?
And we became the first Australian sponsored advisor to NATO
to talk to them about their data
centric security architectures.
Uh, the introduction to the UK MOD was a direct introduction
from the Australian Department of Defense.
Yep. Introduction to the us.
DOD was an introduction, um, from another partner company.
Um, NEC was an introduction by Microsoft.
So you can start to see this trusted network
of people creates this ecosystem where you, you are getting,
um, referenced referenceability.
And that's really, really important. Why?
Because it's, the importance of solving this between the US
and Australia is as important as solving between Australia
and the UK and New Zealand.
And you, you have in existence these communities
already, which talk to each other.
That's the first thing. Then there's also
the internal referenceability.

So we've sold it to Army who then adopts it
for all deployed space.
Yeah. So that introduces you to Navy, which introduce you.
And so all of a sudden you get elevated and you Yeah.
And you've gotta consider, each department
of defense is a marketplace.
Yes. Multiple deals
to be done in each of these environments.
Yeah. It's, yeah.
That, and a good example of that is U-S-D-O-D
with the a thousand licenses that we sold
to the US marketplace, if that gets adopted
in this Microsoft 3, 6, 5 environment,
not only does it scale to
however many users are in that environment,
and you know, we, there's no secret we've put out
to the marketplace that, that,
that we've already given pricing for up to 150,000 users.
Uh, but there's a total 450,000 users just from
that one agency in the U-S-D-O-D.
But that agency services up to, well,
it services every other area
of the us DOD including marines, uh, special operations,
uh, department of Defense, um, Navy, you name it.
So the, the network growth effect there,
once it gets adopted for scaling up the user
numbers is huge.
Yeah. Let's take network growth effect two.
There are seven Microsoft DOD environments.

So if it gets accredited in this one Yeah.
It becomes a pattern for those other seven. Yeah.
Then there's the coalition forces using those systems, and
therefore Microsoft, and they also use Microsoft in 3 6 5.
So there's a network growth of the US setting the standard
for the level of security that you must have
and that pattern being replicated around the globe.
Yeah. That's,
that's a pretty strong network growth effect story.
Yeah. Uh, look, um, that's really interesting.
Um, the reason I ask it is, is
because we, we encounter this a lot where
naively you might assume
that actually it's all just about the technology.
And obviously the technology's found foundational,
but it's kind of moot entirely if you can't
convince anyone to use it.
But what's always super fascinating to me, Daniel,
is we see it again and again
and again, is that it's the, it's my favorite.
I think saying at the moment, the overnight success
that's 10 years in the making.
Yeah. And, and whether it's a human being
or whether it's a large military organization, social proof
is a super powerful thing.
And the old saying is, no one ever got fired for hiring IBM.
So Aus rocks up and goes, Hey, we've got some cool kit.
It's like, great, who else is using it?

Well, no one, but you could be the first.
That's hard when you can say, well, actually they use it.
They use it, they use it.
And actually you've probably already used it indirectly.
It, it, it, it, it doesn't have that aura of objectivity
that you might otherwise assume.
But it is super, super, super powerful
and you tend to see a lot of momentum that be, that
that built, once you start getting those key reference
sites, uh, it, we all, we all tend
to think growth just in general is very linear.
And it, it just strikes me that when these kinds of things,
and, and please tell me if I'm,
if I'm barking up the wrong tree here,
but it tends to be far more
of an s-curve adoption than anything else gradually than,
than, than sort of suddenly Well,
That's why it takes 10 years, right? Yeah.
Yeah. Exactly. It takes 10 years
to become the overnight success.
I mean, you know, um, that, that creating
that referenceability is extremely difficult because
So hard You go
through this thing called crossing the
chasm with new products.
Yep. Um, and it's a well known story.
You, you start with these early
adopters who have a unique problem.
They, they can't, no one else can solve it.

So you create something to solve it. Yeah.
Then you have, um, an innovator which says,
oh, I like what you're doing.
And they, they get, and what we define a marketplace
is those people with a common problem
and common set of needs which reference each other.
Yeah. 'cause it's the referenceability which grow, give,
grows through word of mouth
before it becomes a common thing.
And when it's a common thing, that's your inflection point.
Yep. Right.
So you've gotta get across that ca
and great, there's
so many great technologies which have died.
Yep. Cham, right? Yep.
Our job is to nurture this product,
to hit that inflection point.
Yep. And as you've heard, so we started here in Australia.
That's the referenceability that we required
that's opened those doors for us,
but we had, it took us a long time to prove that
and get that confidence.
Yeah. Particularly in a new area of, uh, of technology such
as data centric security,
because everyone else out there is a network guy.
Yeah. So, but, and,
and so it's helped that it's started to be mandated.
Yeah. Now, what we are seeing is whole networks being

replaced by data-centric security,
and that's what they're planning for in the fire lines.
So, so we're only the start of this journey.
That's why it's growing at a compound annual
growth rate of 34%.
Yeah. Why we see this as the future.
And that's what we have been hanging in there to execute
and while defending our position.
Um, now that's really important
because that, as I said,
that defense story is gonna get mandated to
that defense industrial base and they are multinationals.
Yeah. And there's a new network growth effect. Yeah. Right.
And then there's that supply chain,
because we're talking about orus now and,
and stock my Virginia class submarine
over in the UK and in Australia.
And, and so all
of a sudden this integrated supply chain
becomes critical as well.
And then you can see the vertical adoptions there
for manufacturing, pharmaceuticals, um, energy
where, where I, I also need to start
to protect these is a growth map for us,
but today we're very highly focused in this space
because that's where the activity is.
And that's what's the fastest growing market.
So you're right. We've done all the hard yards, um,
and god bless all of our shareholders who've stuck with us,

because you know, that's really hard for them to understand
that it takes that long Yeah.
To get to that pivotal point.
But then what do are you end, what do you end up
with a high growth, sustainable company that's embedded
for a long term with its client base?
Yep. Yep. Right. And the rest is history.
So you've, what we need
to focus on right now is executing the opportunities in
front of us to become the dominant player in the,
in the market that we've chosen and keep our customers happy
and to get them on that journey across that chasm with them.
And that's what we are highly, highly focused on doing.
And you don't do that alone.
You do that through an ecosystem of strategic partners Yeah.
Alliances. You people do business with people you Yes.
That trust you deliver for them, you service them, you know,
over and above anything, nothing's a problem.
But to do that, you need a team in place
that can do it quickly.
And, and yeah. And,
and this is, the quality has to be just right.
If you, if we, if we get an event
that's catastrophic when you're a security company.
Yeah. So you, you, you, you know, you wanna make sure
that you're getting the quality right as you do this.
Yeah. That, that burns dollars. Yeah. And it takes time.
And so, like I said, the 10 years is

that real investment? Yeah.

Yeah. I believe it. Oh man.

I've got so many questions, but I, I really,

I really don't want to do what I often

do, which is run out of time.

And there, there are, there are some, uh, viewer questions,

but I will ask one more

'cause it just leads so nicely on, on from what,

what you've been talking about, which is this,

I was gonna say, problem of scaling. Let,

Let me just quickly one thing.

Yeah. We don't run out there

to think we've got another 10 years to go.

We haven't. We've been Sure,

Yes, Yes. Doing

this for a long, we believe we're obviously with

that deal in the US and, and,

and the, what we've done

represented the globe last few global deals that we've done,

that we are actually at that point

of pivoting into that inflection point.

Absolutely. I mean, that's really what I was getting at.

I didn't, I didn't wanna suggest otherwise

because it's just, it's such, the more I've been doing this,

it is more a familiar story. Yeah.

I hear investors going, oh God,

they're gonna take another 10 years.

Investors have already been on the journey with us for,

you know, quite some time since you

Know, two. It just takes
time. It really does.
And it, it sounds a bit old fashioned, but it's like,
and if you kind of solve a problem
and you do it well, it's kind of, it's, it,
it goes a long way.
Um, but I do wanna ask you on this,
and then I'll go to the, some of your questions here.
And I said, I framed this up originally as like the,
the problem of scaling.
And it's not really a problem 'cause Well, it's a challenge,
but it's the best of problems to have.
You're only scaling up if there's more
and more customer demand.
So let's say for the sake of argument,
you're at this inflection point.
You know, things has really start, you've,
you've done the hard yards.
Most of the tech is in place,
the team is in place, the word is out there.
You've got some good reference science sites
and all of a sudden things just explode Being software.
I assume that you've got a capacity to scale much, much
to a much greater degree than, than,
than than other companies.
But what level
of revenue do you think you could support at this point in
time with the resourcing that you have now?

Or that's just one way of asking.

It may answer that in any way you think is appropriate.

Well, the, the trick here is to make sure that you are,

I, I have three mantras in the business.

Repeatable, profitable, and growth. Right. Right.

Now that's, that's the objective. Yep.

Make sure that everything in the company is repeatable.

If it's repeatable, it will be profitable. Yep. Right.

And I don't just mean profitability in terms of dollars,

I mean in terms of increasing capacity,

increasing knowledge, increasing all

of those other things as well as dollars.

Yeah. But obviously all our shareholders want us

to be profitable growth.

What you don't want to be able, what you don't want is

that all your dependencies

and infrastructure in the business have

to scale at the same rate as you,

you scale in terms of your growth.

What you want it to do is to hit a ceiling. Yep.

So we are not here to be a mega company. We wanna be global.

We want to be a mega company,

but we don't want the infrastructure cost, the cost

of goods should decrease is,

and particularly in the software service business, where,

you know, you really want to hit margins of about 80

to 85% in terms of profitability in growth profit.

So that's, that's the key to the model. Yeah. Right.

And that's the beauty of,

of software businesses when they get it right.
Yeah. As I said to you
before, we're a very strategic business.
We are obviously looking at all of those metrics
as we build the business out.
We've just obviously done a raise.
The reason we we've done that raise is
because, you know, there's, there's probably for us, um,
three key areas that we need to invest in to take,
make the most of this network growth opportunity
that I talked about with the U-S-D-O-D.
You know, obviously I've got three people in,
in the US at the moment because I didn't wanna over invest
until we had a milestone.
Um, deal.
We, well, it looks like we, you know, we're working towards
that milestone deal, so that's fantastic.
So now I need to expand my presence in the us Why the US
$2.7 trillion spent on defense globally,
they spend approximately 38%
or close to 40% of that total global expenditure.
Yeah. They're the largest market in the world.
If we're gonna make that network growth effect work,
we need to invest in that.
That Yeah. Is, I mean, it's a no brainer. Yeah.
Um, so we need to excel out our revenue, we need
to put people in there, we need to get ready for that.
We need to service that. They need 24 hour

support, all of those things.

But how much do we need, and can we do that smart

and make sure that that digital transformation is work

and productivity gains are working for us as well?

Absolutely. Yep. We're focused on that.

Yep. That, that makes perfect sense.

Alright, I'm gonna go, go to some viewer questions.

Oh, sorry. Do you have one more thing? I was just

Gonna say the other two there is grow

that strategic global relationship.

Yeah. And the last one is to make sure we get, continue

to get that product in the right place.

So they're, they're the three areas

that we need to invest in.

Yeah. Awesome. Awesome.

Um, I'm just gonna go top to bottom, everyone.

So remember you can vote these things up or down.

Um, Ryan, I think your first question,

Daniel's already answered, so I'll skip to the next one.

Um, can you expand on your total addressable

market expectations?

It's my understanding that not everyone in militaries have

secret and top secret access requirements,

But everyone has a classification.

Okay. Right.

Every everyone has a security clearance up

to a certain level and all information is classified,

whether it's unclassified official, so,

so irrespective the, the,

the attributes apply to them. Right.

Right. Okay. That's, that's so, so, uh,

yes, that answers it.

Well, uh, tus revenue is prob is approximately 50 50

licenses versus services, the systems integration.

Makes sense. Can you expand on

what the security consulting aspect is?

Yes, certainly. So look, a a good example of

that was I'm on a call with a customer today.

They, they have to look

after their, um, the information that they,

they are servicing here is an organization, uh,

that services defense,

but they've also got businesses in the us So they've asked

us to talk to them about how and what information

and compliance regulations do they need

to put into place into the US

and how do our products solve that.

So that's a, that's an example

of a security consulting type service.

Right? Yeah. We definitely outsource that to,

to other companies, strategic partners.

But we, we also have obviously a deep knowledge

of it ourselves and where we can assist our customers

to make decisions around buying our products for that

and how that could work for them.

Obviously, we're gonna do that.

The truth is, last year was really 50 50, uh, you know,

50% revenue on services.
We are moving away very much from services.
So this year I would expect that, you know, uh, it won't be
as reflective in the business.
The services that we did over the last two years,
which was substantial in contributing to our revenue base,
was about positioning our data centric security products in
those organizations.
So it was, now what we wanna see is
that convert to licenses.
Yeah. So we've started to see that this year
with a $2.4 million deal in enterprise deal in Q1
with the Australian Department of Defense.
We saw a renewal
and uplift for, um, $1.4 million for cogency, uh,
in Department of Defense, uh, in Q3.
So we are starting to see that,
but we would, we do expect that revenue will dip
because what the metrics we're focusing on quite clearly are
licensing a RR and gross margin. Yeah.
Not many people will, will intentionally, um,
engineer a revenue dip.
And, and that's one of the, I I'm, let me, let me has
to add, Daniel, I'm, I'm, I'm, I, I'm actually, I'm,
I'm not being critical here at all.
I I actually think it's that short-termism
and market pressure from people like us that, that dissuade
that kind of thinking, whereas it's completely the wrong
thing to do if that's the, if

that makes a lot more sense longer term. Well,
We had last year a deal,
which was worth 4.2 million for services.
Right. And it was to work with the Australian Department
of Defense to move from a centralized record management
system to a decentralized records management system.
And obviously they needed data centric security to do that,
but we were working actually only one 10,
about 10% of the solution for that.
So we did the review for them. Yeah.
We didn't, we we killed it
because it wasn't called business.
We're not a records management company. Yeah. Yeah.
And, and I don't want to get distracted from the, the focus
that we need to succeed.
You don't wanna win the battle and lose the war.
Pretty simple, isn't it? Yeah.
And, and you've gotta be brave
and courageous to do those things,
but to start a business like this,
you've gotta be brave and courageous anyway.
Yeah. And, and you know, we get a lot
of advice from a lot of people.
The only people who really know our business are the people
that are working in the business. Yeah.
Yeah. Enough of the helpful backseat drivers.
No, I'm, I'm always prepared to listen
and I do listen to everything and Sure.

And know that, and I, I, I,

I've got a very much an open door policy,

but my job's to run the business.

Yeah. Yeah. And you know what?

There is a real danger strategically in, in just, uh, again,

just speaking from observational experience, the company

that tries to be everything to everyone

generally doesn't go well.

But, and that sounds obvious,

but especially when you are scrappy and small

and trying to scale, it's a very difficult temptation.

You know? And a customer, potentially a big customer says,

well, we're kind of interested, but we need you to do this.

And you think, well, gosh, I guess we should do that.

And it's, it's very, very, very hard to say. No.

So I'll ask, it's more of a comment than a question.

Um, other than just,

You know, company that tries to be everything

to everyone ends up being nothing.

Nothing to, to everyone. Yes. Um,

Like I said, we're very strategic, we are very focused.

We know what, what where we want succeed.

Um, important. We don't apologize for that.

No, you shouldn't. You shouldn't.

Um, I've got a good one here actually. Where did it go?

Um, oh, it's just gone off my screen.

But it was along the lines of with competitors, um,

and, uh, uh, the, the zero knowledge aspect of it,

aren't others doing this?

Surely when you look at something like this, I,

I guess it's, it seems like an

obvious out outside of question.

It's like, well, if it's so obvious,

why isn't anyone else doing it?

Look, you want competition.

'cause if you don't have competitions

and companies popping up who are trying to do exactly this,

you don't have a market.

Right.

No one's doing it because it's not a good idea. You must

Be very lonely. Yes. Or

doing really, really, really well.

So, so it's one or the other. We won.

So that's a good thing. Let's talk about

the big players though.

Your Palo Altos, your Ciscos, your, your z scalers,

you know, your Varonis

and all of these big companies,

they all are marketing this right now.

Mm. Want to be these things.

They're aspiring to be these things. Mm.

Where are they in reality, including Microsoft? Yeah.

They're network bound, they're application bound. Mm.

They go to the application layer

because they started off as cloud access security brokers.

So whatever you put in the cloud, we'll look

after we're DLP we, this, that,

the other we're device we're this. But you're not data.

Right. And that's the difference. Yeah.

So actually they come to us when, um, Palo Alto

and VMware, were talking about how they apply zero trust.

What's the relationship between your network label

and the application label and the data label?

Mm. We don't have one, but we produce a network label.

Right. We'll fill in the rest for you.

Yeah. Yeah. That creates real genuine opportunities.

Why wouldn't we, as a company, we can go up and look,

and this is part of the conversations we have internally.

Do we want to build the company up

and compete head on against these guys?

Or do we wanna be the OEMed product, which gives them

that competitive advantage?

Let's be smart about this.

Which one's faster time to market?

Which one's faster to do accelerate this, which one's,

how do we get this dominance and defensible position

and who do we, and that's where

that strategic alliance comes in.

Mm-hmm. It's, it's, we invest, we're investing in that.

And so, you know, you know, I've asked Kurt to, to,

to really focus on that strategic alliance

because it becomes critical, uh,

at this point in time in the market, at

that inflection point for

how you carve out your market share.

Super interesting. Um, let's talk about the dollars

for users of NC Protect within, uh,
this US Department of Defense.
What type of contract
for enterprise agreements are possible?
Well, the huge amounts
of enterprise agreements are possible,
but look, it's, um, again, what, how this typically works
inside of defense organizations is you'll win a space,
whether it's Army, air Force, Navy, you need to be accepted,
adopted by multiple areas.
And when you start to do that,
eventually the corporate notices
and says, why aren't we doing a whole
of defense blanket enterprise agreement here instead
of all these small enterprise agreements that we're doing?
You can start to see that.
I mean, Pete, we have got definitely presented
to our investors slides on how we are trying to achieve
that, in which spaces, and
that we've mapped this against activities and where we are
and, and who we're targeting in each of those areas.
And, and we do that quite deliberately, um,
because where we wanna be is at that whole
of defense licensing capability.
Now, if people are gonna go out there
and extrapolate that U-S-D-O-D, for example, 38,000
for a thousand users, they'll say 150,000,
you'll be somewhere around 6 million.

Um, but you've got possibly 450 then a means.

And they go, but you gonna,

that's gonna get capped somewhere along the line.

Yeah. There's gonna be volume discounts for these licenses.

Yeah. They're not gonna be, you know, 50, 180%

or whatever that is, but they are gonna

get capped at a certain point.

Yeah, but you want that.

Yeah. Right. So look, where do we want be?

Our job is to get this company

to a hundred million valuation to 150 million to 200 million

to two 50, and just see where we end up.

Yeah. And when we are generating significant revenue

and profit to spin off, where are the other verticals,

which we think we can dominate

because we have banking customers, we have energy customers,

we have logistic management companies, we as customers,

we have, you know, shipbuilding companies as customers.

So, you know, we need to make sure that we're planning for

that next vertical expansion into which industries.

But each one of those is another journey.

And it's, and it is quite nuanced.

And again, it's building up the trust

and the referenceability and you go again.

Yeah. Yeah. Gosh, we're fast running out of time,

so apologies everyone,

I'm not gonna get through your question.

So, um, let me just see here.

Um, I have to ask, I have to ask Austin's question

because it is the new black Daniel, um,

and you're the first CEO we've spoken to in a long time

who hasn't led with this.

So congratulations on that.

Um, but ai, AI is just like everywhere at the moment.

Uh, how does that work in a zero trust

data centric environment?

That's a great question and really important.

One of the reasons we bought the directive product

and built TDI, there was, um, there was a little data spill

with a company, small company, uh, called ViaSat.

Right. And it's

where a software developer put his software

into AI to check it.

It just happened to be, have important, um,

information in there which got publicly published.

Okay. GPT publishes everything.

What we've done is we used directive to run up a container,

which runs AI and to, for each individual

and says where it can publish the results

and where it can source its information to give a response.

Interesting. So how, the real question here is

how do I secure AI in a classified environment

and still get the productivity gains?

And that's what we're focused on. Interesting.

So for example, we've got an ai, a small AI module inside

of our, of TDI, which says I've, we have a graphic interface

where we select the policy

and here's how I've written the policy, and it looks at it
and it comes back and it tells, the AI tells you what,
what works, what doesn't work,
and what your, what your policy means in plain English so
that a soldier who's out in the field who has
to change this can go, oh yeah, that, that, that works.
That's what I intended. Sure. Publish.
So we are looking at it from both senses.
How do we help the organizations adopt ai, ai securely,
and how do we use AI to improve the product?
We're gonna have to do this again maybe next year
or something, because there's just,
there's just too much to cover.
Um, but it's been really illuminating.
I guess I'll just end by saying, oh, asking Daniel,
you know, you speak to all kinds of stakeholders, um,
including investors.
What's the one or two questions that you just,
you don't get asked that often,
but you find odd that you don't get asked that often?
I I, I, I, I, I, I actually don't ask
that question of myself
Because I I I've asked, I mean, look,
there's an old saying there's no stupid questions.
Right? And, and maybe there's stupid answers,
but there's no stupid questions.
Good. I've built a career on that. So,
So, so look, I I, I entertain all sorts
of different questions and because I do talk

to such varying people, the level of understanding is,

is varies dramatically.

Yeah. The, I think the key is to be able

to answer any question in a language

that somebody can comprehend is that, you know,

how do you tell teach a a, a kindergarten kid something?

If you can't explain it to that level, you, you know,

you're lost in the first instance.

Yep. So look, I guess what really,

Or you, or you don't understand

it yourself more to the point Well

If you Yeah. You know,

if you can't teach it, you don't know it. Exactly.

Yeah. It, it, it's one of those things.

So I look, there's probably no questions

that I haven't come across that I thought,

why hasn't someone asked me that?

Yeah. 'cause, um,

but so I can't really answer your question.

Okay. Well, let, let me, lemme try this one then.

What's, you know, 'cause there's so many different, uh,

ways to, to go with this.

But what's, what's the one take home message if,

if someone was to take one message from you from this

discussion, what, what would it be?

Look, I, I, I would hope what they took away from this

today is that there,

there's somebody out there doing some really smart things,

but they're deeply thinking about

how they execute it. Right.

Like that. And,

and that's what I think is what you should invest in Smart

people executing their opportunity really well

and that they've got a niche market, high value proposition

and a defensible position

to make a high growth company sustainable.

You could build an investment strategy around that. Yeah.

I'm a bit of a Warren Buffet fan, I've got to tell you.

So, you know, yep. Do those things right.

The rest will look after itself.

I've got nothing to add except strong agree.

So, um, listen, Daniel, it's been really, really valuable.

Really appreciated the chat.

It's given us a lot of food for thought.

And as I said, we'd love to catch up again in 2026 at some

stage and, and check in on things.

Thank you very much for having me,

and thanks for the audience for spending the time to listen.

Awesome. Okay. Thank you. Cheers.