Re(AI)magine Conversations

Persistent Podcast | Episode 15

The New Data Security Reality in the Age of AI

Dilipkumar Panjwani and Ani Chaudhuri

Dilipkumar Panjwani: Hi everybody. This is Dilip Panjwani. I head the Global Security Practice at Persistent. Welcome to Re(AI)magine Conversations. Today's theme is Data Security Posture Management (DSPM), AI and the Future of Trust. And with me, I have Ani from Netskope. Ani, why don't you introduce yourself today?

Ani Chaudhuri: Hey Dilip, good to be here. I am the VP of Product Management at Netskope and we are super excited to bring you exciting stuff that we are doing and how it impacts your security board.

Dilipkumar Panjwani: So, let's go ahead with the discussion for today. So Ani, the topic being DSPM, could you help us understand what is DSPM and why is it becoming so central to modern data collection studies today?

Ani Chaudhuri: It's a very interesting question because I came to Netskope through an acquisition which was called Dasera, which was a D-S-P-M company that Netskope then acquired.

And our journey started in about 2019. At that point in time, there was no DSPM. We were trying to just figure out visibility and classification. That's all that we were doing. We were very close to what catalogs used to do, except it would be automatic, right?

Dilipkumar Panjwani: Okay.

Ani Chaudhuri: Uh, then about two years after that, Gartner came up with the term DSPM, and I think it mirrors their CSPM thing.

First, they had Cloud Security Posture Management (CSPM), then it was DSPM. What also happened is that initially when we asked Gartner, like they made a list of DSPM players and we asked them what the criteria was. They had a bunch of catalog companies there as well, because that's how they were thinking about it. Wherever you put, you know, data about data that would be DSPM.

Eventually what happened is because the velocity that this picked up, we were in the middle of a perfect storm, right? So, there was regulatory pressure, there was data sprawl happening. And so, all of these companies evolved and it became DSPM. Unfortunately, DSPM is kind of an incomplete story.

DSPM is primarily visibility and classification. But if you think about data security as a whole, it is many things you are to find, you have to flag, you have to fix. And unless you take DSPM and you combine it with SSPM and CSB, inline and CS-BAPI, which is retired, rest and data in motion, it doesn't complete it.

So, it's an important call to action. When you say DSPM, what you mean is not actually DSP, but everything to do with end-to-end security of your data. To me, it's a good place to start a conversation, but a very bad place to end your conversation.

Dilipkumar Panjwani: I couldn't agree more. And it does look like it's a very complex topic itself because when we look at data today, it's everywhere.

The way we are using AI, AI resides or works on data and eventually that means the data which is being used has to be sanitized, has to be correct, has to be used in the right manner or accessed by the right people to ensure its right usage. So when we talk about this data, we also hear a lot of talks about sensitive data.

Now, what kind of sensitive data is most at risk today? Because when we talk about security, there is some risk that is there to the organizations for this so-called sensitive data. And how do you think that DSPM can help organizations discover and protect it?

Ani Chaudhuri: It is a great question. You know, a lot of times when you talk to people, they'll say, I am in a regulated industry, right?

The thing is every industry is regulated today. Some are more regulated than others, right? So, the way to think about it, and I think this is, there's also been a very proactive approach. Previously it was like, okay, this is compliance-driven. And so, people would basically check boxes. Now it's very, very proactive.

So, if you think about it, there are the basic PIA right information about a person that can identify the person. So that's like, table stakes anywhere and should have been there in the first place. Right? The second one is industry specific. For example, in the US in the healthcare, you've got HIPAA, like similarly, you've got FINRA, then you've got international regulations.

Like in the case of India, there is D-P-D-P-A, there is GDPR. There are even state level ones. Like in California, you, we have got CPRA. And so, all of these have different responsibilities, but interestingly, it is all about similar kinds of data.

Dilipkumar Panjwani: So, it's different names. It is similar kinds of data. Now, how does DSPM help in this space?

Ani Chaudhuri: I think about DSPM in two different buckets. One bucket is the SaaS bucket where your data is sitting somewhere else, right?

Dilipkumar Panjwani: Mm-hmm.

Ani Chaudhuri: The second one is. Data stores, data lakes and data warehouses, right? When you combine the two, one is you're trying to make sure that sensitive data is not uploaded to a second party site, or I would call it a third-party site, and no one creates sensitive data there.

So for example, what could happen is you could put a person's name and let's say their other card number or their SSN inside a file and somebody uploads it into a place that they should not be uploading. So that's one problem. The second problem is somebody took a call and actually just typed it in there.

Dilipkumar Panjwani: Right.

Ani Chaudhuri: Right. And so, the way, the place, the data is sitting is still the same, but how it gets there is different. So, you have to kind of think about it slightly differently. When you think about databases, data lake, data warehouses, there the challenges are very, very dense data, which is already mostly structured.

What DSPM allows you to do is it allows you to firstly discover all of your assets. Second, all the data that is sitting there, and by data that is sitting there is the classification. Third, who has access to it? And fourth, how are they using it? This is the role of DSPM four questions. Where is my data? What data do I have? Who has access to it and how are they using it?

Dilipkumar Panjwani: I think it could not be more correct, Ani. Eventually, whatever we are doing today, whether it's going to be sensitive or more private data, or PHI data or PI data, all of them have the common theme. It is data, which needs to be understood.

Where is it? How is it being used? Who are accessing it? And eventually how to protect it at all times. The regulations, the business requirements and the need for the business to use or dispose of it.

Ani Chaudhuri: So Dilip, you interact with a lot of companies as somebody they trust, that is your role to lead that practice.

What are some of the common misconceptions around data visibility and control in the cloud environment? Like what have you seen that you can share with us without taking any names?

Dilipkumar Panjwani: In our experience, Ani, one of the biggest myths that I see today across customers, is this belief that since we're in the cloud, we are modern and secure.

Cloud makes you faster. It doesn't make you disciplined. That's the first thing that we need to all understand. And most exposures come from over permissions, scale sharing, misconfigurations and shadow usage. I believe cloud didn't remove the data problem, it actually industrialized it. And forgive me Ani, if I'm sounding a little bit blunt today, but it's because the facts are blunt, right? Most organizations don't have a cyber problem. They have a data reality problem. Data is everywhere.

Ani Chaudhuri: Hundred percent.

Dilipkumar Panjwani: It's cloud endpoints, and now it's flying into AI prompts and agents at scale. So, the future of trust isn't about saying we're secure. It's about proving continuously where sensitive data is, who can touch it and what they're doing with it.

That's why I totally agree with you when you said that DSPM is becoming foundational and that is why AI makes our conversation today so much more urgent.

Ani Chaudhuri: Yeah, and in fact, you know, we did an internal check within our systems of about 1500ish customers. What we realized was quite shocking, and the shock is this, that on an average in a company of moderately large size, there are 60 different AI tools being used. Six, zero!

Dilipkumar Panjwani: Wow.

Ani Chaudhuri: 50 of them are shadow IT.

Dilipkumar Panjwani: Yeah.

Ani Chaudhuri: So, it's like five is to one from a perspective of shadow IT to authorized it, right? Additionally, the other thing that we realized is when you go through all of the practices of these AI providers that you're connecting with, 90% of them are rated as poor.

From a data leakage perspective, their terms of use, who owns the data. So, it is not just like leakage, but you're even working with operators who are very loose around the boundaries and the trust angle.

Dilipkumar Panjwani: I agree. Ani. And we've been talking about shadow IT, then moved to Shadow Cloud, now it's becoming shadow AI. Tell me, Ani, how is the rise of AI and GenAI actually challenging the cybersecurity landscape?

Ani Chaudhuri: It's a question that everybody from the CEO to the panwalla is talking about AI, right? Um, why that is important is that means every stratum of our economic and social ladder is using this, which means more data is getting in.

People are trading their privacy for value that they get, right? And some of it is known, and some of it is on unknown, but as a company, you have to think about AI as three different pieces. The first piece is data, like somehow it all comes down to the data, right? The second piece is what I call the pipeline, which is how is the data getting to the application that is doing your work?

And the third one is identity. At Netskope, we have two very, very big pieces, right? We have data security and we have secure access. So, what data security does for us is, think about it like a prism. You remember the cover of Pink Floyd's, "Dark Side of the Moon?" Here is the prism. There is a ray coming in and a rainbow coming out on the other side.

So, we think of ourselves like that prism, where anytime there is a call into the prism, which is what we call NewEdge, which is our network security, our zero trust engine, which sits inside of that is able to see what data is going to who and what the permissions are. And that kind of creates the triumvirate of data pipelines and identity.

And if we can get a good handle on these three, I think companies risk profile will go down, tremendously! And that's where the focus should be.

Dilipkumar Panjwani: The AI wave didn't create a new data problem at all. It actually exposed the old one. If I had to summarize, we've always had the data sprawl for years. Now we are just feeding it into faster systems.

Ani Chaudhuri: Right, and that is true. That actually is a great segue into one of the questions that I had for you.

Are there any real world examples of cyber-attacks or large scale data misuse that you have seen? So that our listeners can, kind of, be aware of ex-additional patterns that they can look for.

Dilipkumar Panjwani: So, since we're talking on data and we just got up the segment on AI, let's take some real examples around that space.

Ani Chaudhuri: Mm-hmm.

Dilipkumar Panjwani: For example, the Hong Kong police described a case. A finance employee transferred around $25 million after a video call with what looked like the CFO and his colleagues. And it turned out that the people on the call were all defects. That's where trust is being attacked.

Ani Chaudhuri: Wow! And this was the police?

Dilipkumar Panjwani: Yes.

Ani Chaudhuri: Wow.

Dilipkumar Panjwani: So this was the Hong Kong police who had done investigation on a case. It's an organization where the employee was on a video call with the CFO. So, he recognized the CFO by face.

He recognizes colleagues on the call by face, but they were all deep fakes. He was not aware of that, so he trusted it by the video feeds itself coming to him. We have also seen generative AI being used to level up the entire game of business. Email compromises the BCs as we call them. I read somewhere in one of the articles from reporting where tools like BoomGPT are being used to create hyper realistic and convincing phishing and BC style emails.

Better grammar, better tone, very much realistic to your specific style of writing and unbelievable social engineering in that space. It's very hard to really make sense, whether it's going to be me who has the AI, who's writing in that sense. And then when I look at the other aspect, one of the most common employees-based sensitive data into generative AI today because it is convenient.

It's not malicious, but it's the path of this resistance, right? That's why government has to build around these workflows because most breaches aren't break-ins anymore by hackers. They're actually logins or bad permissions or exploits.

Ani Chaudhuri: No, that is exactly right. So, one of the things that I have been thinking about is this. See, GenAI is not going anywhere because it delivers tremendous value. I'm not saying that it is. Like, there's always going to be that debate, like, can it do true creativity? The point is, let's say it cannot do true creativity, but what it can do, it can lift the mundane to a place where it is faster and better, right?

Dilipkumar Panjwani: Yes!

Ani Chaudhuri: So, it's delivering value. Now, how does a company balance this value with security

Dilipkumar Panjwani: From a Gen perspective, Ani, one thing which I talk to my customers very often is stop the false choice between block AI and embrace chaos. I think the winning model is safe enablement. Know what data is sensitive, where it lives, and what policies apply to protect it as you rightly called out initially.

And then, allow AI to be used with the right guardrails. And that's exactly why we need the solutions like these, where DSPM matters today. Something that gives you the inventory exposure, access, context you need. It helps you with realistic rules around them to guard rail. Yeah?

Ani Chaudhuri: Makes sense. Makes sense. So, one more question is, before we move into the zero trust thing, right?

Is given that you're talking to customers, what is the number of tools that they're using and where do you see the most proliferation of GenAI? In what functions do you see it the most?

Dilipkumar Panjwani: So traditionally speaking, if you look at, all the surveys done across the various analyst advisors today. Any organization on an average from a security standpoint would have anywhere between 35 to 70 odd tools.

And that keeps on increasing, right? So, every tool will have its AI component and after the guardrails around that, AI and so on. But when we look at how they are using AI in that respect to security space today, so there are two aspects of AI. AI for tech and AI for business. Tech is a space where you are looking for AI, for cybersecurity and supporting all the use cases to enhance your cybersecurity maturity.

Your preventive and detective control your responses and your knowledge base to constantly stay up on the game. And AI for business is where you secure the AI used by the business so that you provide the right guardrails and allow them to experiment, learn, adopt, and scale. Using AI and not left behind in competition.

Ani Chaudhuri: Yeah, that makes total sense. Sometimes I feel we are in Florence at the time of Renaissance. Like every day you find something new. Some of it is risky. I'm sure it was when Renaissance happened that new ideas scare people. New ideas will initially also be misused, but eventually things settle down and the world becomes a better place.

So with that, why don't we move on to Zero Trust?

Dilipkumar Panjwani: Sure. Sounds good. You talk about Zero Trust, Ani. What are some of the biggest challenges organizations face when trying to adopt Zero Trust model according to you?

Ani Chaudhuri: That's a loaded question. I think the way I think about it is, Zero Trust, if you think about it, can only be implemented when you're able to inspect, right? Inspection. All of us have been through airport security. You know, your bank goes one way, you go one way and then they will stop you.

Certain things will take longer. They'll manually check, right? So, the trade-off is always between good security and performance. Like how do you make an airport efficient is how you make security efficient, right?

Dilipkumar Panjwani: Mm-hmm.

Ani Chaudhuri: And so again, the way we have been doing this is using a combination of secure access and data security. We have something called NewEdge, which is our own network, and this network is the 12th Most Used Network in the world. It actually sits two places above Netflix.

Dilipkumar Panjwani: Okay.

Ani Chaudhuri: The reason why we built our own network was that as you are calling for data over the internet, it takes some time. Right now, if I add on top of that time to inspect what is going up and down, it's going to slow it down further.

Which is what happens in most companies, which are data security companies. Like, it just takes more time. So, what Netskope did was that it built its own internet inside the internet. It's like a intranet for all of our customers. So, they enter at the closest point and then they can access whatever data they want, and then, the data is delivered to them.

This is called NewEdge. It's very, very simple. Now because it's a very efficient network, we use the gain that we get to do the inspection and there is still speed leftover. So, what we did was instead of just thinking about data security, we thought about performant data security. And it took us down to first principles thinking like if we were to do it from scratch, how would we do it?

And that's what we have been working on. So that is one angle, which is performance security. The second one is from an operator's perspective. Now, if you think about it, you have got endpoint, you have got your private apps, you have got your SaaS solutions, you have got on-prem data. You've got email that needs to be inspected, right?

From an operator's perspective, this is a very, very complex world and it's easy for one to say, okay, this is best-in-class, and that is optimizing for the local maxima. So, the trade-off then becomes, do I create a bunch of best-in-class, which on paper looks great, or do I go with a platform that is actually optimized, right?

And so, the second trade off to me is that you should think about a platform that understands where your data is, who your people are, what are they trying to do, and is able to deliver that efficiently. So those are basically, I feel when you can do both, which is create an efficient system and have all the pieces talking to each other like a functional body should, like my left hand should know what my right hand is doing.

Then you actually get closer to the utopia of security. You know, eventually it is, we are all still managing risk. It'll never be a hundred percent because it's a cat and mouse game. But how can you reduce the defender's dilemma by doing less but actually gaining more. The outcome is better though you are doing less.

Dilipkumar Panjwani: Interesting. So, coming to the next segment on the same thread, Ani, now we are seeing that every organization is moving beyond the IT world and also into IoT and there are also manufacturing organizations now not being spared from cyber-attacks. And that's a hundred percent the OT side of the world is also coming onto.

Integrated OT IT environment. How can organizations ensure data security in environments where OT and IT systems are increasingly getting interconnected? Because it was a different story. At a point of time, your plant was very isolated. You only had one desktop sitting there, which was giving you visibility.

But today with Data and AI trying to talk to the plants, it is just getting more and more interconnected, and the risk are increasing to allow attacks to flow from one segment to the other and vice versa.

Ani Chaudhuri: You probably will know the stats better on this in terms of the ratio of people to machines, but my suspicion is that the machines outnumber people in a very big way, right?

And so, every machine. And by machine, I don't just mean like a physical machine, it everybody should have permissions. Everybody. There should always be at least on the agent side, something called decision trace. Like how did they make a decision? What data did they pull so that if there are anomalies, you can understand those anomalies.

Like where, where did those come from? It's a lot of root cost analysis, but I think the key goes down to, again, the three elements, which is like data, pipeline, which is how are they accessing it and the identity. I'm going to flip this around a little bit.

Dilipkumar Panjwani: Mm-hmm.

Ani Chaudhuri: Like, companies have had also to step up.

Right? And their step up has been that they used to live in a world where AI wasn't there, and then there was a little bit of it, which made its way through. Machine Learning and then it became mainstream AI. How do you see these transitions happen? How should they manage it? Like what should be the things that they keep in mind?

Dilipkumar Panjwani: A successful transition when you're looking at such projects or, engagements? Looks like you need to have something, which is going to be with fewer assumptions and more measurements. You start with visibility from a data perspective. Similarly, as you mentioned earlier, then you prioritize the risk around it, and finally you automate the remediation.

So, it makes security continue to mitigate risks and not just a quarterly point in time. Compliance audit exercise. I think looking at even the design, when you're looking at any transitions or

transformation engagements, they also need to work in a similar manner. Do not keep security as an afterthought.

Do not think about data and your pipelines as an afterthought. Put it right at the center stage, right at the design phase itself. Get it into the whole planning. And then, identify all the risk and then start putting guard rails around it right from day one.

Ani Chaudhuri: So that is a phenomenal thing that go back to design-thinking and bring all of the elements in when you are kind of still at the blueprint stage so you can make the corrections and of course it's going to be iterative process.

As we come to a close of today's discussion, are there any last thoughts that come to your mind that you would like to share with the audience?

Dilipkumar Panjwani: So, keeping the theme in mind, Ani, my closing thought would be simple. Trust in the AI era is a data problem before it's anything else. The organizations that win won't be the ones with the most tools.

They'll be the ones with the clearest visibility of data, their understanding of the posture and the fastest path from insight to remediation. I could flip it off back to you and just ask your closing remarks to understand what would you give as a takeaway to our reader and listeners today?

Ani Chaudhuri: I do agree with you.

I think it's a combination of three things. The first thing is the skill level of the operators, and it is impossible for any practitioner to have all of the skills. So having a very, very good partner like Persistent would be a good starting point, because before you buy the tool, somebody who is seeing what is happening globally as a benchmark is able to give you that tribal knowledge.

Like in one engagement, right? The second one is the basic tools. And by basic tools, I mean, do I use the word basic? What it means is, okay, here is the technology, here are the configurations and benchmarks. So, these are kind of the tools, right? That is the second piece that's foundational.

And the third one is the partnership. And the partnership then becomes a combination of the customer, the partner who's helping them, and the vendor, the technology or security vendor. So, number one is knowing, number two is the tooling, and number three is the partnership. With these, we will get much closer to where we need to be.

Dilipkumar Panjwani: Awesome. Thank you so much, Ani. I think, with this, we are coming to the close of our discussion. Thank you so much for your time today and look forward to speaking to you again.

Ani Chaudhuri: It's always a pleasure spending time with you, exploring new ideas and thank you for having us over.

Dilipkumar Panjwani: And thank you to our listeners and viewers for tuning in today for the podcast where we engaged with Ani from Netskope to discuss about DSPM, AI and Zero Trust.

This has been fun. Again, I'm Dilipkumar Panjwani, Global Head of Cybersecurity at Persistent. And you are part of Re(AI)magine Conversations. Stay curious, stay inspired. Thank you.

Re(AI)magining™ the World

About Persistent

Persistent Systems (BSE: 533179 and NSE: PERSISTENT) is a global services and solutions company delivering AI-led, platform driven Digital Engineering and Enterprise Modernization to businesses across industries. With over 26,500 employees located in 18 countries, the Company is committed to innovation and client success. Persistent offers a comprehensive suite of services, including software engineering, product development, data and analytics, CX transformation, cloud computing, and intelligent automation. The Company is part of the MSCI India Index and is included in key indices of the National Stock Exchange of India, including the Nifty Midcap 50, Nifty IT, and Nifty MidCap Liquid 15, as well as several on the BSE such as the S&P BSE 100 and S&P BSE SENSEX Next 50. Persistent is also a constituent of the Dow Jones Sustainability World Index. The Company has achieved carbon neutrality, reinforcing its commitment to sustainability and responsible business practices. Persistent has also been named one of America's Greatest Workplaces for Inclusion & Diversity 2025 by Newsweek and Plant A Insights Group. As a participant of the United Nations Global Compact, the Company is committed to aligning strategies and operations with universal principles on human rights, labor, environment, and anti-corruption, as well as take actions that advance societal goals. With 468% growth in brand value since 2020, Persistent is the fastest-growing IT services brand in 'Brand Finance India 100' 2025 Report.

USA
Persistent Systems, Inc.
2055 Laurelwood Road, Suite 210
Santa Clara, CA 95054
Tel: +1 (408) 216 7010
Fax: +1 (408) 451 9177
Email: info@persistent.com

India
Persistent Systems Limited
Bhageerath, 402
Senapati Bapat Road
Pune 411016
Tel: +91 (20) 6703 0000
Fax: +91 (20) 6703 0008

Persistent
Re(AI)magining the World

www.persistent.com