sentra

Jason Chan's DSPM Buyer's Guide

A security leader's advice to successfully navigate DSPM

Former VP Infosec at **Netflix**

July 2023

Table of Contents

03 Preface

04 Who Needs a DSPM?

05 Data Platform Diversity and Movement Matter More than Volume

06 Understanding the ‘Must Haves’ of DSPM

07 Integrating DSPM with Your Security Stack

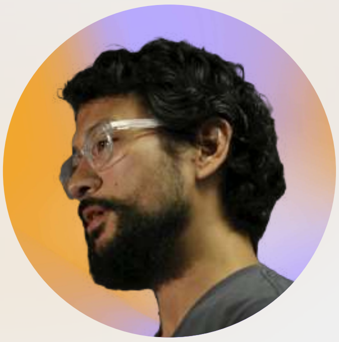
09 Platform Ownership: Who Manages the DSPM?

10 What CISOs Should Ask from their DSPM Reports

12 Making the Budget Case for DSPM

13 Evaluating Your DSPM Implementation - How to Know if it’s Working

14 About Sentra



Jason Chan

Former VP Infosec at **Netflix**

Preface

Any security solution – no matter how innovative or groundbreaking – is only as good as it is understandable, implementable and deployable.

This means that no matter how much your colleagues talk about the latest and greatest thing during the RSA Conference, you've still got to understand whether it's the right fit for you, your organization, and your ecosystem. This is one of the primary challenges of running a cybersecurity organization – not only choosing the right tools, but building the proper procedures so that you're getting the most out of these solutions.

That applies to Data Security Posture Management (DSPM) as well. This guide is meant to help prospective and current users of DSPM understand what the 'must haves' of a DSPM are, how to implement it in your organization, and what you need to be measuring to understand whether your DSPM implementation was a success.

Who Needs a DSPM?

I don’t consider DSPM to be about industry or how much data you have.

It’s about where your organization is on its cloud journey.
For example, if you’re doing a large cloud migration or you are in the middle of a digital transformation project, then you’d want to be looking into a way to understand where your data is and how it’s secured.

Another good example would be highly regulated industries like finance, healthcare, insurance, and banking. Data can easily become noncompliant with regulations like PCI-DSS and HIPAA, and this is an excellent example of where a data centric approach to security can help.

Finance

Healthcare

Insurance

Banking

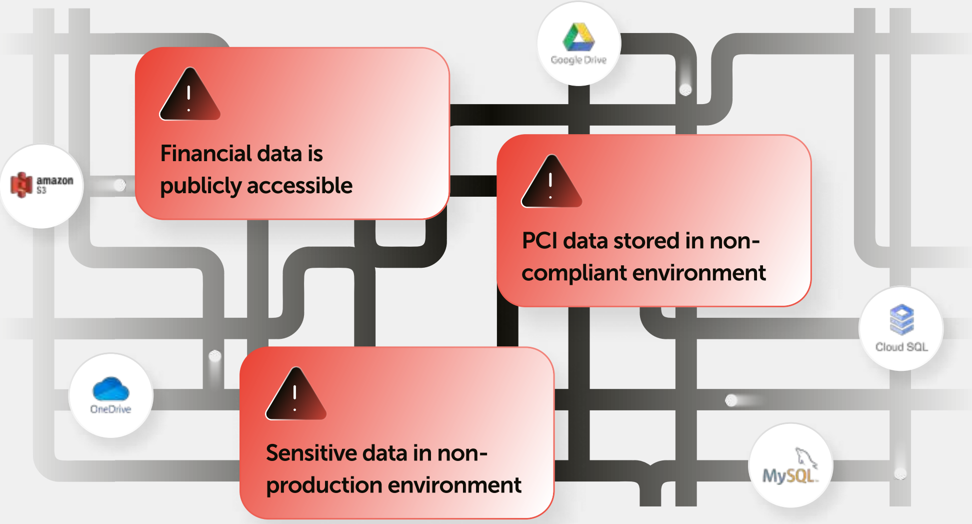
Highly regulated industries with sensitive data are natural fit for DSPM solutions

The final organization type that could benefit from DSPM is one with a strong developer first culture which embraces distributed technology management. In those cases you're adopting these approaches for their speed, and I think having a DSPM as a guardrail, allowing for speed but protecting against recklessness, makes a lot of sense.

Data Platform Diversity and Movement Matter More than Volume

DSPM adoption shouldn't necessarily be driven by quantity. I don't think you can really say "Oh, once I hit 100 TB or a PB of data, it's time to go look for a DSPM."

It's more about the diversity of your data platforms and the amount of data stores. Organizations have data moving between lots of different data sources - S3 Buckets, Cloud SQL, Google Drive, etc.


Google Drive
amazon S3
Financial data is publicly accessible
PCI data stored in non-compliant environment
Cloud SQL
OneDrive
Sensitive data in non-production environment
MySQL

If you're getting to the point where your sensitive data is spread out and being moved, extracted, duplicated, then it makes sense to start considering your options.

Understanding the 'Must Haves' of DSPM

There are a few things I'd consider base requirements when looking at any security tool. Of course, integrations are key - it needs to support the platforms that my team and I live in day to day. I don't want a standalone solution - it should have an API and be designed to integrate as part of a broader portfolio.

Ease of deployment is another big one for me. A DSPM should be agentless, with a quick time to value- you should be able to see results before you're at 100% adoption. Setting up should be measured in hours, not days.

- ✓ **APIs for integrations**
- ✓ **Robust data discovery capabilities**
- ✓ **Agentless**
- ✓ **Serves functions outside of security**

These are things I want in all tools, but when it comes to DSPM specifically, I think the discovery mechanism is the most important component and should be extremely robust. The value of a DSPM - fixing weaknesses in your data's security posture- all flows from accurate data discovery and classification. If it misses something, the rest of the platform loses security impact.

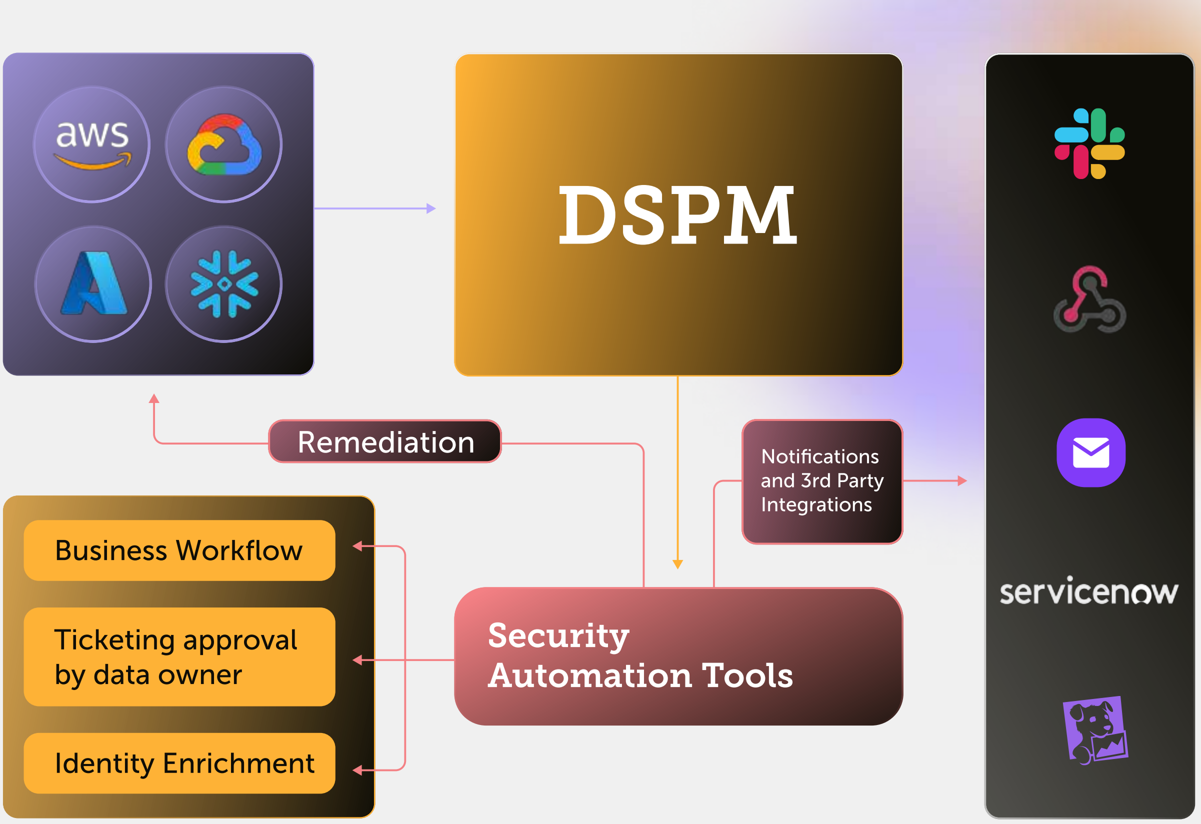
> Good tools are useful to multiple audiences

The final thing I'd say here is 'how can it serve adjacent functions?'. Is this tool only for security, or can other teams like CloudOps, Compliance, and Finance use it and find value as well? Will it help us stay compliant with global regulations? Can it reduce cloud spend by finding and eliminating shadow data? These are all considerations beyond security which should be taken into account when looking at a DSPM.

Integrating DSPM with Your Security Stack

Folks looking for DSPM already have (or they should have) an existing operational security capability.

When a DSPM finds an issue, I want it to integrate with my ticketing system like JIRA, my Cloud SIEM, my SOAR platform, and common productivity tools. **Essentially, I want to add to my existing operational workflow, not create an entirely new one.**
You don't want any tool that requires new capabilities or teams just to manage.


aws
DSPM
Remediation
Notifications and 3rd Party Integrations
Business Workflow
Ticketing approval by data owner
Identity Enrichment
Security Automation Tools
servicenow

I also think it's really important first to understand when rolling out a DSPM - who should care about the findings? Who needs to be involved? And if other teams are involved, how are findings going to be accessible to them on the tools that they use?

For example, I've already mentioned how a DSPM should be used to help multiple teams. But if the compliance team works over email, and the security team works on JIRA, and the ops team is on Slack mostly, it's important results get to where they need to go, in the format those teams actually use.

Platform Ownership: Who Manages the DSPM?

I think to answer this question a typical RACI chart makes sense - who's paying for this, who's maintaining it, who handles the output, etc. My instinct is that even with its broad applicability across cloud enterprises, security will own and run it.

Whether that's the cloud security team or a dedicated data protection team would depend on the size and structure of your organization. Regardless, the key partners from all the other teams I've mentioned need to be involved, especially when it comes to findings that they will need to remediate.

When it comes to remediation and actually fixing the issues found by the DSPM, that's based on your own security philosophy and how the security team operates.

DSPM RACI Chart

DSPM Platform	Data Security Manager	Cloud Security Architect	Cloud Security Architect
Planning	A	R	C
Deployment	A	R	C
Maintenance	A	R	I
Usage	A	R	R

For some organizations, the security team is primarily for identifying issues and trying to find the right teams to fix them, while other security teams will take on more of the burden of fixing. Personally, I always prefer the latter approach, because I want each part of the organization to focus on what it does best.

With DSPM, there's going to be different types of remediation. It might be as simple as taking a decision as an organization that 'this type of data platform can't be used for personal information' or 'let's change the settings to make this data store non-public'. That's pretty straightforward, but on the other hand, you could have potentially more complicated issues, for example if we need to say "hey, we're storing data in a platform that doesn't support the controls we need, and we need to begin a migration." In this case we're now talking about a project, not a task, and I think then you'll have to make a choice for your organization about who leads that - is it the data platform owners, security, business users, etc.

What CISOs Should Ask from their DSPM Reports

I always want to look at trends and see that numbers are headed in the right direction. So for DSPM that might include:

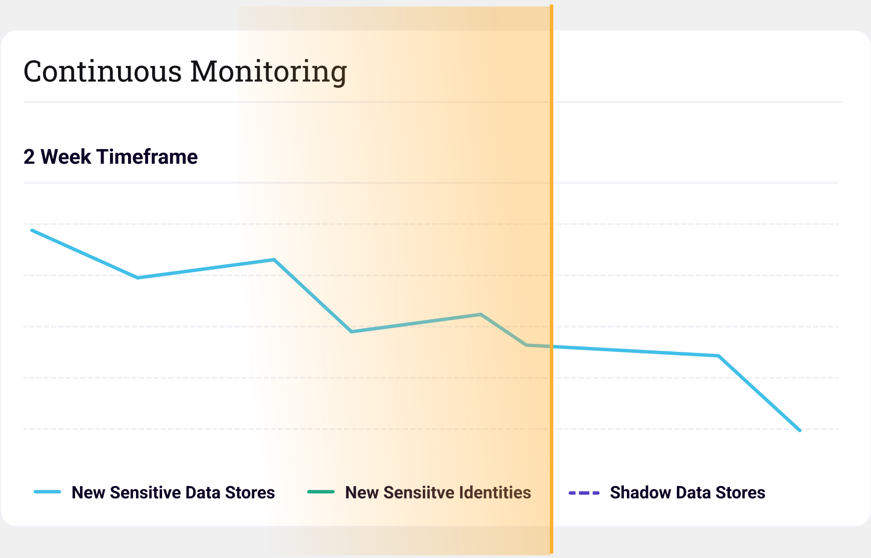
1. Is the amount of **noncompliant data stores decreasing**? For example if we discovered 4 data stores with non compliant PCI-DSS data, have we resolved that by either moving them somewhere compliant or deleting them?
2. How much **shadow data** is being discovered between scans

3. Is our most **sensitive data** - PII, Source Code, HR records, being protected properly? Are the **right access and security controls** in place?

4. Is the number of unmanaged data stores decreasing

> **Ultimately, I want to see less red and more green on my reports, that more data is being protected across all environments.**

These are the types of metrics I'd check out on a regular basis, but there are also projects that I would want to use DSPM to assist with, such as a cost reduction project where we use it to find and delete data, or a data regulation project. Ultimately, I want to see less red and more green on my reports, that more data is being protected across all environments.



Making the Budget Case for DSPM

You need to make the case that not only is DSPM a core part of our security capabilities, but it's going to have a positive impact on both compliance and costs.

If you suspect you have huge amounts of shadow data or other non compliant data stores, the ROI case can clearly be made on reduced cloud costs and mitigating the risk of a data fine.

Cloud Cost Reduction

Developer Freedom

Agility

But really, if you're a company that really values business agility and developer freedom, there are clear operational benefits from DSPM - it really opens engineering teams up to do interesting things with the data, and that's one of the reasons you made this huge investment in the cloud to begin with.

Evaluating Your DSPM Implementation - How to Know if it's Working

In addition to the trends I mentioned when talking about results, what I really want to know is have we meaningfully changed the way we manage data.

1. **Are our cloud costs decreasing?**
2. **Are the big issues found by the DSPM in the process of being addressed?**
3. **Do we have less shadow data?**
4. **Are the controls we need in place on our most sensitive data enabled?**

There's a long tradition of security teams getting tools that they don't then fully implement. DSPM is too valuable to be one of them, which is another reason why integrations are so important - when you're working in the platforms you're used to, you are much more likely to get the most out of a new tool.

About Sentra

Sentra is a data security platform that helps organizations discover and remediate the top data security risks in their public environments. Sentra automatically detects if sensitive data is vulnerable due to misconfigurations, over-permissions, unauthorized access, data duplication or other security issues. The company was founded in 2021 and is co-headquartered in New York City and Tel Aviv.

For more information, please visit www.sentra.io.

sentra