Techstrong Research

PulseMeter

Sponsored by orca security

Data is all over the place, and it's getting worse. Resulting from COVID-driven remote work, SaaS use has exploded, as well as the rapid movement of workloads to public cloud platforms. This data migration means sensitive data most likely resides on someone else's platform. If not now, the data will be on a cloud platform soon enough. Any organization with regulatory oversight or sensitive intellectual property should ensure they know where the data is, how it's used, and what options they have to protect it.

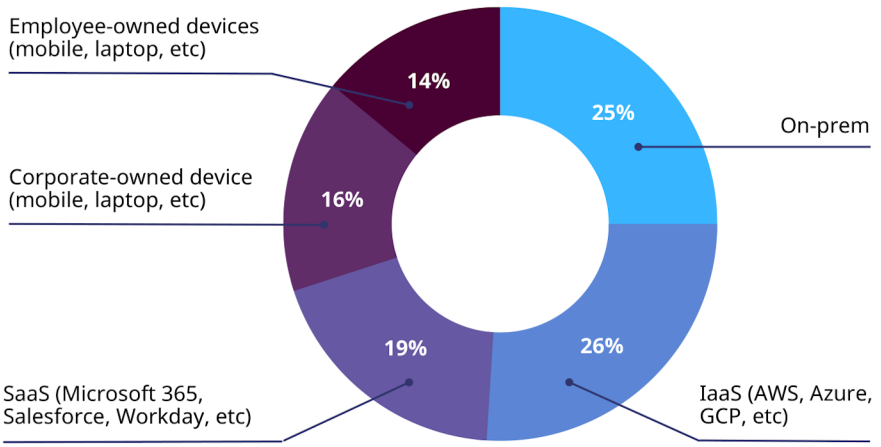
In late 2022, Techstrong Research polled our community of DevOps, cloud-native, cybersecurity and digital transformation readers and viewers to take their pulse on data security posture management (DSPM). Respondents indicated that more sensitive data is in the cloud (45%) than on-prem (25%), which will only grow over time. These organizations don't know where their sensitive data is, as almost 50% do less frequent or no discovery, which is concerning.

Despite the current sub-optimal data security posture, emerging solutions may offer the ability to gain better visibility and control as data movement to the cloud accelerates.

Discovery of Sensitive Cloud Data is Lagging

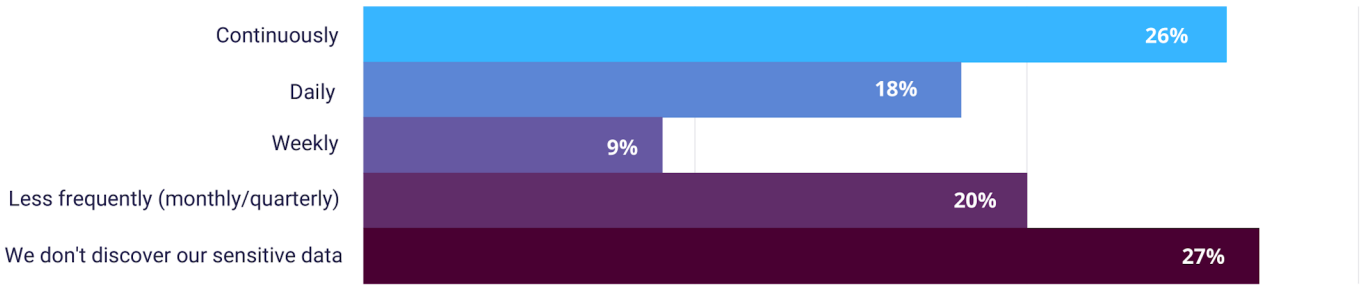
Whatever reluctance to put sensitive data in the cloud is gone. More sensitive data now resides in the cloud between IaaS (26%) and SaaS (19%).

Where is your sensitive (protected/regulated/proprietary) data located?



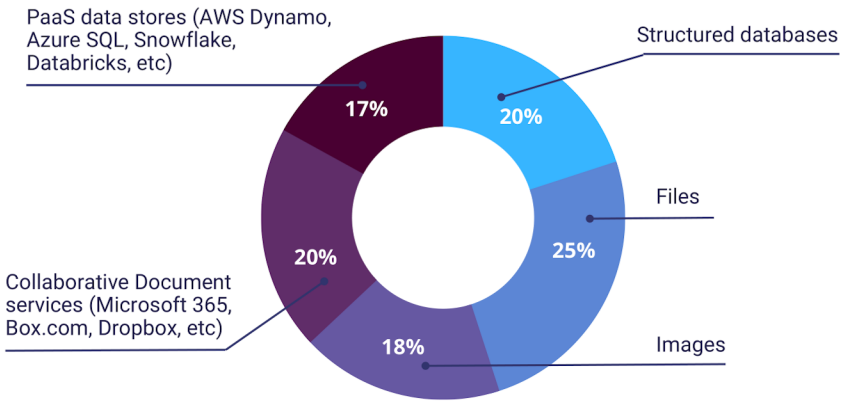
How often do you scan cloud data repositories for sensitive data (discovery)?

Too many organizations don't know the location of their sensitive data, with 27% doing no discovery and another 20% doing monthly or quarterly scans.



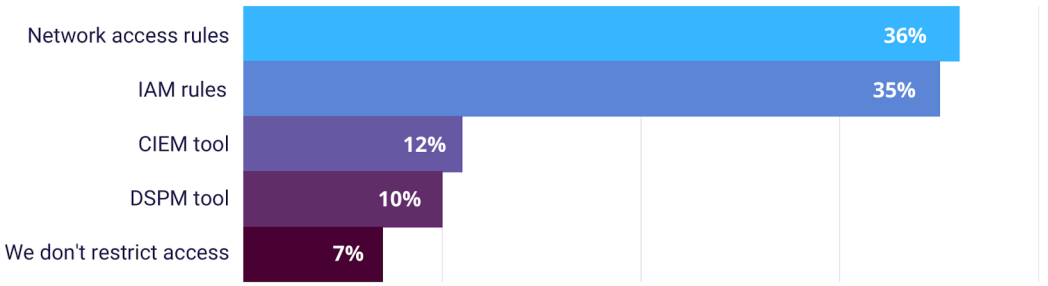
Do you scan the following data types for sensitive information? (Select all that apply)

For those that do scan for sensitive data, files garner the most activity (25%), closely followed by collaboration services (20%) and structured databases (20%), as these data stores have more plentiful options for scanning.



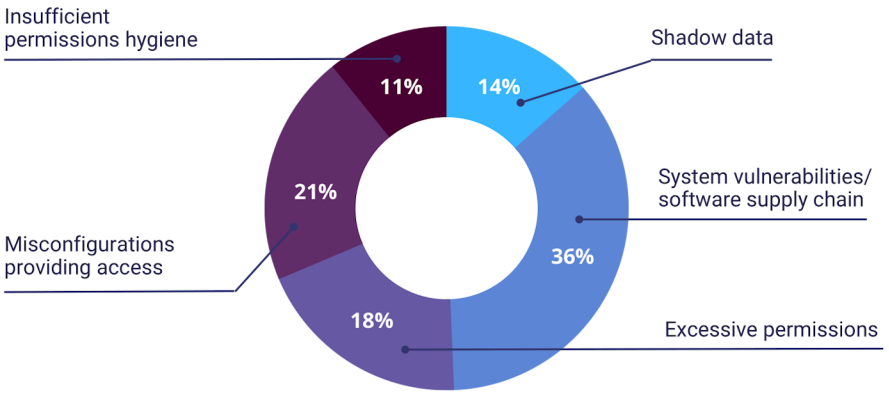
Cloud Security Solutions Should Protect Sensitive Data

How do you restrict access to sensitive data? (Select all that apply)



Data access controls are mixed between old school (network access rules - 36%) and new school (IAM rules - 35%). Thankfully only 7% don't bother restricting access.

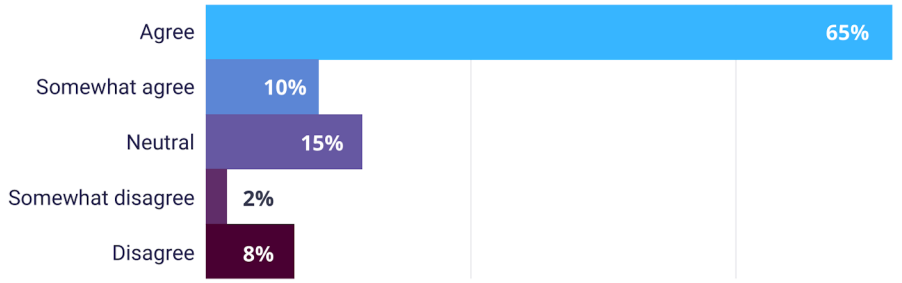
There isn't a lot of trust in the underlying infrastructure and applications, as 36% of respondents are most concerned with system vulnerabilities or software supply chain exposures. Shadow data is still in the shadows, with only 13% of respondents worried about it.



What risk to your data is the most concerning?

Looking at potential solutions, it's clear that respondents expect their cloud security platform to provide DSPM capabilities, with 65% agreeing and another 11% somewhat agreeing.

Do you view cloud data security as an integral part of your overall cloud security management, meaning it should be integrated into cloud security platforms?



Techstrong Research Analyst View

Although not surprising, the poor state of discovery and protection of sensitive cloud data should be ringing alarm bells. At this point, more sensitive data is on cloud platforms than on-prem. Yet almost 50% of the respondents scan for sensitive data less frequently (monthly/quarterly) or not at all. We're confident that organizations burying their heads in the sand won't make the problem disappear. Although many solutions can scan files, especially in object storage and collaboration services like Microsoft 365 and Google Workspace, maintaining visibility becomes more challenging as data increasingly moves into data lakes and other PaaS services.

Regarding the perceived risks to sensitive data, 37% of the respondents are most concerned about system vulnerabilities and software supply chain exposures. Another 19% are worried about excessive permissions. Yet, when you ask the respondents how they protect sensitive data, they mostly use access control rules on the network (36%) or IAM (35%).

This would seem inconsistent, as these controls manage permissions but do not address system vulnerabilities or the supply chain. A significant majority of respondents (65%) believe data security should be integrated into a central cloud security platform, which addresses system vulnerabilities, misconfigurations and the software that runs in the cloud.

The bottom line is that a majority of sensitive data will be in the cloud sooner rather than later. Organizations need to ensure they can locate and scan for sensitive data, preferably continuously, and be able to enforce proper access control and hygiene for the systems accessing and storing the data. A central cloud security platform will be able to provide the full contextual insights needed to understand which data risks are the most critical and need to be fixed first.