5 best practices for finding and securing sensitive data

With more data to manage in more places, knowing what data is where—and protecting it the right way—is a key step in optimizing your data risk posture. Follow these 5 best practices for finding and securing your sensitive data.

1. Discover all data, including secondary data

Use AI-based classification to detect data across your IT estate, including files, backups, archives, and cloud environments. This proactive visibility will help prevent surprises by revealing hidden copies and unknown repositories.

Why this matters:

Blind spots in backups, archives, or snapshots can hide sensitive data and increase damage in the event of a breach.

Benefit to you:

Gaining full visibility helps you reduce data exposure and avoid compliance gaps—before an attack.

2. Enable automated, high-accuracy classification

Use AI-based pattern matching to help you reduce false positives (where non-sensitive data is mistakenly classified as sensitive) and more accurately identify context-aware sensitive data across PII, PHI, PCI, intellectual property, and other critical categories.

Why this matters:

Automated classification ensures scalability and consistency across expanding datasets.

Benefit to you:

You'll save time, improve accuracy, and scale data protection without adding manual overhead.

3. Tag data with contextual metadata

Enrich your sensitive data with metadata—such as classification labels, location tags, and ownership details—to enable faster sorting and a more effective response when potential breaches arise.

Why this matters:

Automatically tagging both existing and new data with metadata improves the speed and accuracy of risk assessment.

Benefit to you:

You can act quickly and confidently when incidents occur, with clearer insight into what's at risk.

4. Prioritize high-risk data by degree of exposure and sensitivity

Flag sensitive items that are especially exposed (e.g., shared folders, object storage buckets, unsecured backup copies) or critical to compliance. Focus your protection efforts on the highest risk areas.

Why this matters:

Since not all data poses the same risk, you shouldn't protect it all the same way. Treat your data like it's currency. Some data is like a single dollar, while other data is like a $100 bill.

Benefit to you:

When you've focused your protection efforts, you'll reduce time spent on incident response.

5. Integrate classification with incident response

When an incident or breach occurs, immediately use classification insights to pinpoint what sensitive data was impacted and support regulatory obligations.

Why this matters:

Knowing what sensitive data was impacted enables faster forensics, more accurate risk assessments, and better compliance reporting.

Benefit to you:

You can assess potential damage during a cyberattack and streamline regulatory reporting with confidence.

Follow these 5 best practices for finding and classifying sensitive data, and you'll be well on your way to optimizing your data risk posture.

Ready to take your data classification further with API-powered integrations? Read the blog, New DSPM integration with Cyera shows the power of open APIs.

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

9100086-001-EN 6-2025