carahsoft

secuvyai

When DSPM Isn't Enough

Thank you for your interest in exploring this content.

Carahsoft is the **Trusted Government IT Solutions Provider**® supporting a broad portfolio of industry-leading technologies through NASA SEWP V and E&I Carahsoft Cloud Solutions & Services Distributor Contract and a wide range of other contract vehicles.

As the **Master Government Aggregator**®, Carahsoft connects government agencies, industry partners, and technology providers to deliver innovative, mission-focused solutions.

In partnership with Secuvy, we provide technology solutions that drive modernization, strengthen operations, and ensure compliance with evolving government standards.

To learn more about how Carahsoft can support your technology needs, please visit carahsoft.com

Explore More Resources:
carah.io/learn

Join Events & Webinars:
carah.io/events

Discover Technology Solutions:
carah.io/secuvy

Learn About Procurement:
carah.io/secuvycontracts

Connect With Our Team:
Secuvy@carahsoft.com
(703) 230-7597

secuvyai

When DSPM Isn't Enough

The AI-native discovery and classification platform for when **accuracy matters**. Secuvy doesn't just find sensitive data — it classifies any data by value and purpose, so your AI pipelines are filled with only the right, appropriate content. Secuvy reaches **up to 99% classification accuracy**, while legacy, pattern-based tools stall in the low 80s and drop far lower on the unstructured content that now dominates the enterprise.

Modern data doesn't follow a template. It sprawls across clouds, on-prem systems, and SaaS apps — and roughly **80% of it is unstructured**: free text, documents, chats, and AI-generated content. And "sensitive" no longer means just PII or security data. It means company intellectual property — the **source code, designs, strategies, and trade secrets** that define your competitive edge — and, in regulated environments, classified or controlled data that carries no traditional pattern at all. Traditional DSPM leans on **regex, keyword dictionaries, and pre-trained models** that only find what they were explicitly programmed to see — leaving valuable "dark data" undiscovered. In an AI world, the ability to classify not just sensitive data but all data by its true value and purpose is the whole game.

> "Regex-only classification scored just 52.7% — versus 95% for AI."
>
> — Independent regex vs. AI data-classification benchmark, 2026

Four capabilities that set Secuvy apart

Auto-Classification Engine

Automatically builds a sensitive-data bill of materials across structured and unstructured sources, classifying data by type and purpose with no hand-written rules. Classification runs at onboarding and then continuously re-analyzes data as it changes — new files, edits, moves, new data types — so your inventory is always current, never a stale point-in-time scan.

AI-Based, Self-Learning Discovery, Classification and Recommendations

Unsupervised self-learning trained on your environment, not a generic label set. It gets smarter the more data it sees, adapts to schema and data drift on its own with no retraining cycles, and recommends data you may have missed — surfacing what could also be sensitive. Accuracy compounds over time instead of degrading.

Non-Pattern Data Recognition

Find what rules can't. Regex and pre-trained models only catch predictable formats and break the moment data deviates, flooding teams with false positives. Secuvy reads data by its meaning, surfacing the IP, unpatterned regulated data, and "dark data" legacy tools leave undiscovered — no rule-writing, no retraining.

Contextual Linkage

Understand data in relationship, not isolation. Pattern matching can't tell an SSN from a test value or a product ID. Secuvy's contextual AI links and groups related data into a single, accurate view of an identity, record, or asset across clouds, on-prem, and SaaS — turning raw matches into trustworthy classification at petabyte scale.

The bottom line: pattern-based tools answer "does this look like sensitive data?" Secuvy answers "is this sensitive data, and how does it relate to everything else?" — the difference between chasing false positives and acting on trustworthy results.

Why Accuracy Decides Everything in the AI World

Feed an LLM or analytics pipeline mislabeled or missed data and you inherit its mistakes at scale — exposed secrets, compliance gaps, and poisoned models. Accuracy isn't a vanity metric; it's what determines whether you can safely put your data to work. Here's how Secuvy compares to legacy pattern-based and pre-trained approaches.

Up to 99%
Secuvy classification accuracy

~53%
Regex-only accuracy vs. 95% for AI

50-70%
Data legacy tools typically find

Up to 90%
Lower cost & manual effort

Dimension	Legacy pattern-based & pre-trained DSPM	Secuvy AI-native
Classification accuracy	Low 80s for some structured data; falls to ~50% on unstructured / regex-matched content	**Up to 99% across structured & unstructured**
Data discovered	Often only 50–70% of the estate	**Comprehensive, petabyte-scale coverage**
Non-pattern data (symptoms, quasi-IDs, free text)	Missed — no rule or label exists	**Discovered via contextual, self-learning AI**
Setup	Manual rules & labeled training data	**Self-learning on your environment; no labels**
Maintenance	Constant tuning, retraining & redeployment	**Adapts to schema & data drift automatically**
Result	False-positive noise, analyst fatigue	**Trustworthy results teams can act on**

Built for AI, not retrofitted for it. Because Secuvy understands data by meaning and context, it's uniquely suited to govern the data flowing into LLMs and AI pipelines — ensuring only the right, correctly classified data powers your AI, at up to 4x faster time-to-value than competing platforms.

From Capabilities to Business Impact

Ship AI faster — Trustworthy data classification in days, not months of setup and tuning.
Protect what matters most — Catch the IP, trade secrets, and regulated "dark data" legacy tools miss — cutting breach and compliance exposure.
Stay audit-ready, always — Continuous re-analysis keeps your data inventory current – provable.
Spend less to get it right — Self-learning retires rule-writing, retraining, and false-positive triage — up to 90% less effort.
Free teams for real risk — Up to 99% accuracy replaces false-positive noise, so teams act on real findings, not ghosts.
See your whole data picture — Petabyte-scale coverage closes the 30–50% blind spot left by tools that find half the estate.

About Secuvy

Secuvy is an AI-powered data intelligence platform that automatically discovers, classifies, filters, and governs enterprise data at scale — ensuring only clean, policy-compliant data ever reaches an AI pipeline, model, or agent. As the governance layer purpose-built for the AI era, Secuvy fills the critical gap that infrastructure and security tools alone can't solve: knowing exactly what data you have, where it lives, and whether it's safe to use. Backed by Dell Technologies Capital, Westwave Capital, and Z5 Capital. SOC 2 Type II certified.

Sources: Secuvy (secuvy.ai/overview, secuvy.ai/dspm) — up to 99% accuracy, 4x faster time-to-value, competitors find only 50–70% of data, up to 90% lower cost. Independent regex vs. AI classification benchmark (arXiv 2605.20368) — regex 52.7% vs. 95.0% for AI/LLM classification; ~80% of enterprise data is unstructured (industry DSPM research). Figures are vendor and third-party claims provided for comparison.