Command your data and AI from a single platform

Why we recommend Securiti for data security, privacy, governance and safe AI adoption

Data now lives everywhere: public cloud, SaaS applications, data warehouses and on-premises systems. AI is being adopted faster than most organisations can secure it. The usual answer is a shelf of disconnected tools, each with its own view of the estate. Coverage gaps appear between them, costs stack up, and it becomes hard to answer a simple question: where is our sensitive data, and who can reach it?

Securiti takes a different approach. Its DataAI Command Platform is built on a knowledge graph that maps data and AI assets across connected systems, along with their sensitivity, ownership, access paths and regulatory obligations. Security, privacy, governance and AI teams can then work from a shared view. Following its acquisition by Veeam, Securiti also carries the backing of an established data-resilience vendor.

1,000+	No. 1	Modular	Veeam
prebuilt integrations across cloud, SaaS & data platforms	in GigaOm's DSPM rating, three years running (2024 to 2026)	deploy the modules that fit, and add others later	enterprise backing following the 2025 acquisition

WHAT THE PLATFORM OFFERS

A modular set of capabilities

Clients deploy the modules that fit their use cases and can add others as needs grow. Where these overlap with tools already in place, there may be scope to consolidate, which we would confirm against your existing products and requirements.

Data security posture management

Discovers data assets across connected systems, including shadow and forgotten stores. Flags misconfigurations and toxic risk combinations, and supports least-privilege access.

AI security & governance

Helps locate models, copilots and agents in use. LLM firewalls screen prompts, retrievals and responses. Agent Commander is an early-access capability for detecting agentic AI risk; where the relevant Veeam recovery integration and a protected environment are in place, it can also help reverse unintended agent actions.

Privacy automation

Automates much of the privacy lifecycle: subject access requests, data mapping and RoPA, consent for web and mobile, assessments and breach notification, across GDPR, POPIA, CPRA, LGPD and other regimes.

Governance, catalog & quality

A searchable catalog helps people find and trust data. Lineage traces how information moves, quality checks validate it, and ROT minimisation retires obsolete data to reduce cost and risk.

Gencore AI: build safe AI systems

Connects enterprise data to AI pipelines: extracting content from complex files, sanitising it, syncing to vector databases, and applying entitlements so copilots draw only on data a user is permitted to see.

Compliance & breach management

Assessment against security frameworks and global regulations, with evidence collected automatically. Breach impact analysis helps identify affected individuals and supports notification.

WORKING WITH FOOTPRINT AFRICA

We suggest starting with a tightly scoped proof of value. In a well-prepared environment, initial findings can surface quickly, though timing depends on credentials, connectivity, security approvals, repository size and agreed scope. Footprint Africa Business Solutions works alongside your team through scoping, rollout, enablement and support, and would arrange a session with your security and compliance stakeholders.

CLASSIFICATION AND DLP

How it identifies sensitive data

The platform's controls draw on a shared classification engine. Securiti discovers data across structured and unstructured stores in connected systems, then works out what is sensitive using several techniques together rather than pattern matching alone, which is why results hold up where regex-based tools produce noise.

Machine learning & NLP
Auto-classifies datasets and applies labels; for structured stores, multiple AI/ML signals are fused to classify each column.

Pattern matching
Identifies sensitive document types such as consent forms and financial statements, and groups files by business category.

Contextual analysis
Reads surrounding text and structure, so an identifier is recognised by its context, not only its shape.

Metadata & attributes
File type, location, owner and age inform the decision, so files in an HR store can inherit a confidential rating.

Exact Data Match
Fingerprints your own records, designed to eliminate false positives; fingerprints stay in your cloud or on-premises environment.

Labelling & tagging
Applies sensitivity labels automatically, imports labels from Microsoft's security centre, and adds privacy metadata tags.

Where this leaves your existing DLP. Securiti is not an endpoint, email or network DLP and does not replace one. Instead it enforces at the data layer, through dynamic masking, access restriction, encryption of exposed stores and remediation of misconfigurations, then feeds classification back into the DLP, SIEM and IAM tools you already run. Available actions depend on the modules deployed and the permissions granted. Because many legacy tools classify with regex, higher-quality classification can improve their accuracy.

THE COMMERCIAL CASE

Where the value comes from

Securiti is a premium platform. The argument is not that any single module is the lowest-priced option, but that consolidating overlapping tools onto one platform may reduce duplicated technology, integration effort and operational complexity. Whether that produces a net saving in your case is something we would establish together, through a tool-consolidation and total-cost-of-ownership review.

Potential to consolidate
Where the platform replaces overlapping tools, you may reduce duplicated licences, integration work and day-to-day overhead.

Supports risk reduction
Clear visibility of sensitive data and access is one important element of a wider defence-in-depth programme.

Helps unblock AI initiatives
Guardrails, classification and entitlement controls can address common blockers; final approval for production remains your decision.

Independently recognised
Recognised by industry analysts across DSPM and privacy management, and by customer reviews on Gartner Peer Insights.

RECOGNITION · GigaOm DSPM Leader 2024 to 2026 · Frost & Sullivan Most Innovative DSPM Leader · Forrester Wave Leader, Privacy Management · IDC MarketScape Worldwide Leader, Privacy Management · RSA Conference 2020 Innovation Sandbox ‘Most Innovative Startup’ · Gartner Peer Insights Customers’ Choice

Gartner Peer Insights Customers’ Choice recognitions reflect the subjective opinions of individual reviewers; they do not represent the views of, or an endorsement by, Gartner or its affiliates.

Regulatory context: Zimbabwe. For organisations in Zimbabwe, the platform's discovery, data mapping, access intelligence, assessment and breach-management capabilities can support activities relevant to the Cyber and Data Protection Act [Chapter 12:07], such as understanding what personal data is held and where, how it flows, and who can access it. For regulated financial institutions, the same capabilities can help evidence practices addressed in the Reserve Bank of Zimbabwe's Cybersecurity and Resilience Guideline, including asset inventories, data flows, access rights and least privilege, and audit evidence. These capabilities support compliance activities; they do not, on their own, guarantee compliance, which remains the organisation's responsibility.