vorlon

Unifying SaaS and AI Security

Why your SaaS data protection strategy must cover AI tools and agentic systems, and how Vorlon delivers

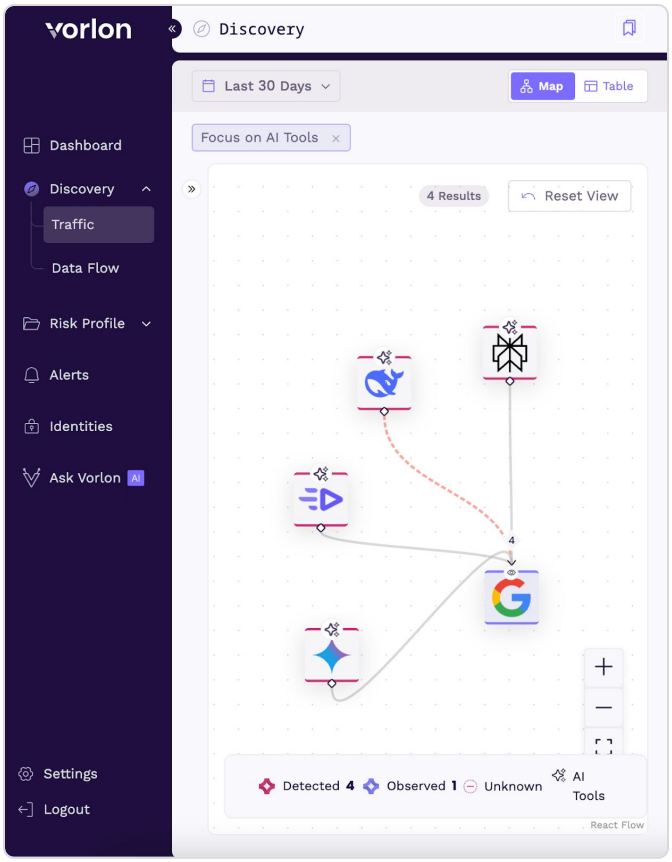
Unifying SaaS and AI Security

Why your SaaS data protection strategy must cover AI tools and agentic systems, and how Vorlon delivers

Executive Summary

AI agents and copilots are the newest members of your SaaS ecosystem. Their ability to automate work, analyze content, and connect disparate apps transforms how enterprises operate and how they're targeted. Yet, most security programs still treat SaaS and AI as separate domains, leaving dangerous blind spots where sensitive data can move undetected.

Enterprise security and compliance teams need a unified security platform with deep visibility and control across all apps, identities, and their sensitive data flows, including AI. Vorlon was built for this reality, closing the gap between SaaS security and AI governance with a single, unified approach.



The Converging Risk Surface: SaaS and AI are Now One Ecosystem

AI agents don't just live in a vacuum; they are deeply entwined with your SaaS environment, interacting with sensitive data, triggering workflows, and leveraging the same APIs, secrets, and permissions as any user or app. This convergence introduces a new spectrum of risk:

Risk Vector	SaaS Security	AI Security	Unified Risk
Access Control	User permissions, API keys, OAuth tokens	AI agents inherit broad app/API privileges	Overshared access and privilege drift
Data Movement	File sharing, SaaS-to-SaaS integrations	AI models and copilots moving data between apps and services	Unmonitored data exfiltration
Shadow IT	Unsanctioned (Shadow) apps, unknown connections	Shadow AI tools, agents, and plugins	Blind spots in SaaS and AI usage
Compliance Monitoring	Activity logging, user-based alerting	AI-driven actions often lack granular, explainable logs	Gaps in audit and forensic readiness
Non-Human Identity Risk	Bots, service accounts, machine credentials	AI agents act as non-human identities, blending with automation traffic	Difficult-to-track, high-impact incidents

Why a Unified Platform is Essential

Siloed approaches leave organizations exposed. Only a platform that treats AI tools as first-class citizens within the SaaS ecosystem can:

- **Discover shadow AI usage** — surface unauthorized or hidden AI agents, copilots, and integrations.
- **Map data sharing to models** — trace where and how sensitive SaaS data is accessed, processed, or exported by AI tools.
- **Monitor AI-to-SaaS connectivity** — visualize how AI agents and automations are plugged into your core data stack.
- **Detect and investigate anomalies** — flag and explain unusual data flows, excessive access, or suspicious API calls—no matter the source.
- **Contextualize and prioritize response** — use risk intelligence to focus security efforts on the most impactful threats, whether human or machine-driven.

Key Risk Factors Unique to AI in SaaS Ecosystems

Risk Factor	Description	Example
Shadow AI Usage	Unauthorized, hidden, or “rogue” AI tools operating across SaaS apps	Employee connects DeepSeek to Google Drive via Zapier
Excessive Permissions	AI agents inherit broad/scoped access far beyond what’s necessary	Copilot with admin rights in M365 has access to sensitive HR data in Workday
Opaque Data Sharing	Sensitive data shared with AI/LLM models, sometimes outside regulatory boundaries	PII sent to a third-party LLM via an MCP Server (Model Context Protocol)
Complex Integrations	AI tools connect indirectly via APIs, bots, or third-party automation platforms	Slack bot retrieves Salesforce records for summarization
Difficult-to-Detect	AI-driven, API-based activity mimics legitimate service/user behavior, masking exfiltration or misuse	AI agent uploads confidential docs to an external endpoint

Vorlon's Unified SaaS and AI Security Capabilities

Vorlon's approach is rooted in the belief that SaaS and AI security are inseparable. The platform delivers advanced technical capabilities designed to provide enterprise-scale visibility, control, and compliance across both domains:

Technical Capability	How It Works	Value
Shadow AI Discovery	Continuous scanning for AI agents, copilots, and scripts across SaaS environment	Surfaces unknown AI usage, AI add-ons, MCP Servers, and integrations
Sensitive Data Mapping for AI	Data classification engine inspects all flows involving AI tools—PII, credentials, admin, and financial data	Identifies where sensitive data is exposed to AI
AI-to-SaaS Integration Monitoring	Tracks every API call, secret usage, and service account linking AI to business apps	Observes how AI apps connect back to your data
Behavioral Analytics for AI Agents	Applies UEBA/UAM to both human and non-human identities, scoring risk by data type, frequency, and anomalies	Detects unusual, risky, or excessive AI behaviors
Real-Time Alerting and Automated Response	Flags suspicious AI-driven access, terminated user secrets, or unauthorized data exports; enables instant remediation	Minimizes dwell time and reduces incident impact
Data Map and Explainability	Visualizes all data flows and connections involving AI, with full audit logs	Delivers auditability and forensic readiness
Leveraging AI for better security outcomes via remote MPC (Model Context Protocol Server)	Connective tissue between LLMs and SaaS data queries and orchestration (leverages DataMatrix™ modeling)	Natural language prompts to automate complex investigations, threat hunting, and reporting tasks
Compliance Tagging and Policy Enforcement	Tag fields as "compliance-critical"; triggers alerts and blocks for policy violations involving AI	Supports SOX, HIPAA, PCI, GDPR, and custom tagging

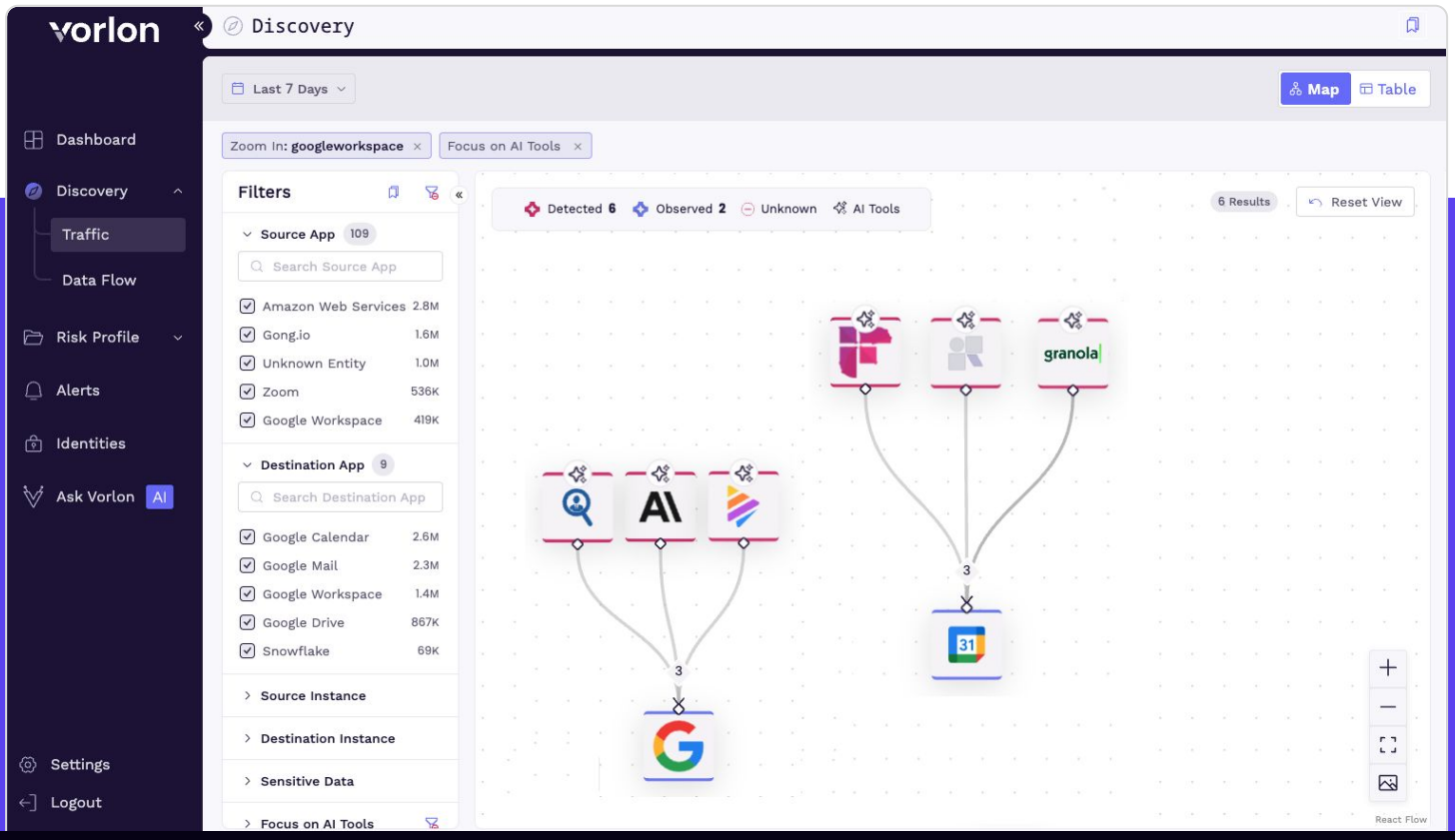
Example: Technical Workflow Table

Scenario	Vorlon Detection and Response
New AI agent connects to Salesforce	1. Detect via API monitoring 2. Assign a high risk score based on elevated permissions and sensitive data access 3. Fire and Alert (for unusual field exports) with steps to remediate 4. Kick off automated remediation (e.g. via SOAR) or route remediation steps to the Salesforce admin via email, Slack, or ITSM (e.g. Jira, ServiceNow) 5. Capture evidence for AI governance and compliance
AI model accesses compliance data	1. Tag sensitive data fields (PII, GDPR, PCI, HIPAA, etc.) 2. Alert if accessed/exported by an AI agent 3. Depending on policy, initiate block or escalation workflow
Excessive downloads by AI copilot	1. Detect anomaly vs. baseline 2. Trigger behavioral alert 3. Log activity and remediation for audit/compliance evidence
Terminated user's AI script active	1. Flag stale secret/service account 2. Revoke the secret in two clicks 3. Access Vorlon Flight Recorder to conduct a forensic investigation

Why Vorlon's Approach Stands Apart

By treating AI agents as core participants in your SaaS ecosystem, not as afterthoughts, Vorlon provides:

- **Unified discovery:** One inventory for all users, apps, and AI tools and agents
- **Consistent data classification:** Sensitive data detection and classification across every data flow, human or machine
- **Alert prioritization:** Based on the app, sensitive data access, and permission levels for humans, non-human identities (NHI), and Agentic AI systems
- **Actionable, explainable alerts:** Near real-time, context-rich notifications, routed to the right owner, to drive fast and effective remediation
- **Cloud scale:** MCP Server integrated with live SaaS ecosystem enables context-aware automation at a scale and speed legacy SSPMs can't match
- **Compliance and forensics support:** Automated evidence collection, mapping, and reporting for regulatory frameworks and forensic investigations



Conclusion

AI agents are now as integral to your SaaS environment as any employee or app. Protecting your business means seeing the entire ecosystem, every connection, every data flow, every action, regardless of whether it's initiated by a person, a bot, or an AI agent.

By bridging the gap between enterprise data and AI-driven workflows, Vorlon empowers security teams to defend the entire SaaS+AI ecosystem with unprecedented speed and precision.

Only a unified approach delivers real visibility and control. Vorlon gives security and compliance teams the platform they need to secure the future, where SaaS and AI security are finally one and the same.

Contact Vorlon to see how unified SaaS and AI security can close your organization's most urgent gaps, before they become tomorrow's headlines.

About Vorlon

SaaS and AI data move fast — Vorlon's SaaS ecosystem security platform gives enterprises the context to move faster. By combining data flow visibility, posture and secrets management, and detection and response, Vorlon helps you see what's connected, what's at risk, and what to do next. With its agentless, patent-pending DataMatrix™ technology, Vorlon builds a live model of your SaaS environment, including AI systems. Backed by Accel and SOC 2 Type 2 Certified, Vorlon is trusted by Fortune 500 companies to secure what others miss: the interactions between apps, identities, and data that power modern business. Learn more at vorlon.io.

SOC 2 Type II
Certified