vorlon

WHITE PAPER

Agentless Data Loss Prevention for SaaS Ecosystems

Why SaaS ecosystems demand agentless, risk-based data loss prevention, and how Vorlon delivers

Agentless Data Loss Prevention for SaaS Ecosystems

Why SaaS ecosystems demand agentless, risk-based data loss prevention, and how Vorlon delivers

Executive Summary

The average enterprise now runs over 300 SaaS applications, creating a sprawling, interconnected ecosystem that moves sensitive data far beyond traditional security perimeters.

Legacy Data Loss Prevention (DLP) solutions leveraged agents and deep packet inspection in order to provide visibility into endpoints, networks, and on-premises data stores. First-generation DLP for SaaS solutions followed suit, inheriting many of these more invasive deployment requirements. However, today's SaaS-first world demands a new approach: one that is quick to deploy, broad in coverage, yet still capable of near real-time detection and response.

Vorlon delivers DLP for SaaS that's right-sized for today's sprawling SaaS ecosystems, which contain hundreds of SaaS applications and thousands of connected services. Our agentless approach leverages API endpoints for visibility and data classification, and continuous behavioral monitoring with rich context to detect and prioritize unauthorized and suspicious activity. This powerful combination provides much broader coverage than agent-based DLP for SaaS solutions. It also empowers security leaders to detect, investigate, and prevent data loss, whether caused by insiders, external attackers, or automated integrations.

The New DLP Imperative: Visibility Across the SaaS Ecosystem

Why old-school DLP fails in the SaaS era

Classic DLP tools were designed for environments you owned and controlled, relying on deep packet inspection, endpoint agents, and on-premises file scanning. In the SaaS era:

- Sensitive data flows between hundreds of apps, APIs, and third-party integrations, with little to no logging or oversight by default.
- Threats move laterally: Attackers exploit OAuth tokens, stale API keys, and machine identities to exfiltrate data beyond the reach of legacy controls.
- Employees, contractors, and bots interact with data from anywhere, on any device, often outside the corporate network.

You Can’t Prevent What You Can’t See.

To deliver effective DLP for SaaS, you must discover all connected SaaS applications and data flows, monitor every API interaction, every integration, and every human and non-human identity.

Adaptive, Risk-Based DLP: The Modern Standard for DLP for SaaS

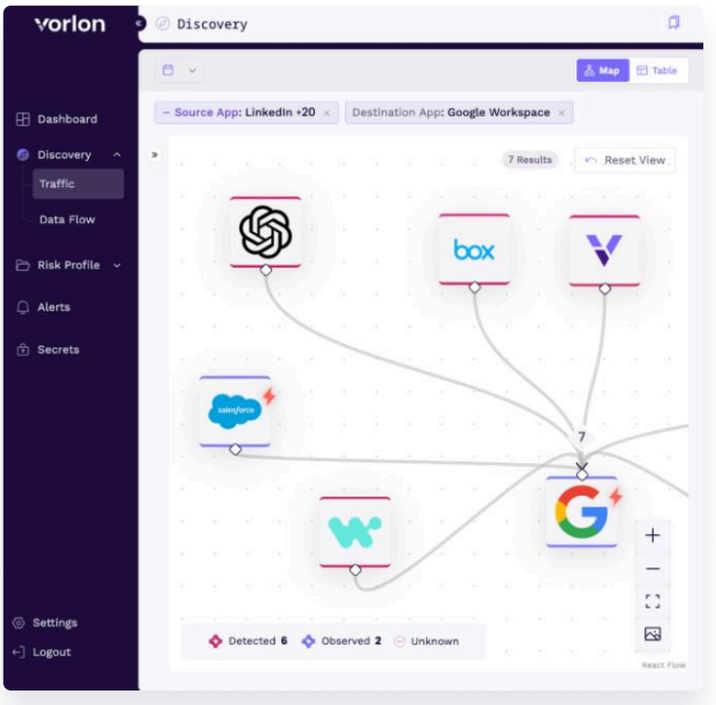
From Gartner 2025 Market Guide for Data Loss Prevention:

According to Gartner, “Solutions with adaptive risk-based DLP often leverage user and entity behavior analytics (UEBA) and user activity monitoring (UAM) to supplement or replace data detection. These solutions can analyze user activities, communication patterns and other contextual information derived from user activity to detect anomalous deviations from normal behavior and establish user intent. This allows for early detection of risky user behavior, enabling SRM leaders to deter malicious insiders, educate careless users and monitor departing employees.”

— Gartner Market Guide for Data Loss Prevention, 9 April 2025. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

How Vorlon delivers adaptive, risk-based DLP for SaaS

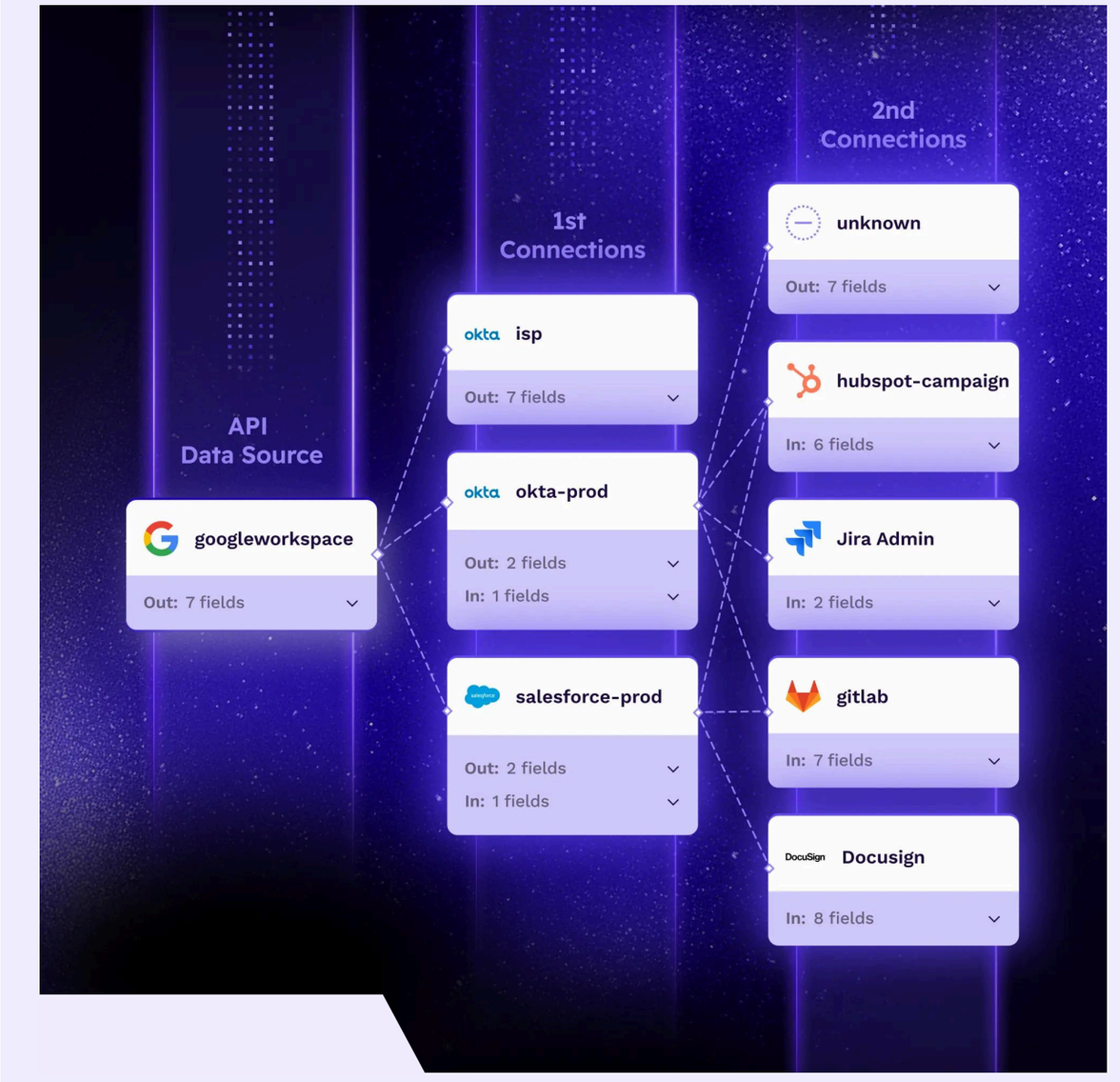
- **Agentless, API-based monitoring:** no endpoint agents or proxies needed, making deployment feasible across hundreds of SaaS apps and connected services.
- **Continuous behavioral analytics:** Vorlon monitors user and machine activity across all connected apps, building behavioral baselines and detecting deviations in near real-time.
- **Rich context for every alert:** Each alert is enriched with information about the data type, user risk profile, app risk score, and behavioral anomalies, allowing teams to focus on what matters most.
- **Proactive detection:** Vorlon surfaces not just "data in motion" but intent, flagging suspicious behaviors before they become incidents (e.g., a departing employee accessing sensitive reports days before resignation).
- **AI discovery and posture management:** Vorlon shows AI tools in use (sanctioned and unsanctioned), what observed applications are connected, exchanging data, and helps manage permissions/access to third-party apps.



Vorlon Data Classification via API Endpoint Analysis: The Missing Link for Effective SaaS DLP

Given the nature of SaaS APIs and the limitations of traditional content inspection done out-of-band, Vorlon approaches sensitive data identification by analyzing the API endpoints in near real time and determining which APIs are designed to handle which sensitive data types (PII, credentials, financial data, secrets, etc.).

- **Out-of-the-box classification:** Vorlon identifies and categorizes API endpoints based on their potential to expose sensitive data, drawing from our extensive analysis of SaaS API documentation and common design patterns. In this way, we can infer:
  - **PII:** Names, emails, DOB, social security numbers, passports, UK national insurance, etc.
  - **Secrets:** API keys, tokens, client IDs, private/public keys, refresh tokens.
  - **Credentials:** Passwords, admin functionality, permissions/scopes, credential fields.
  - **Financial data:** Credit card numbers, postal addresses, and more.
- **Customer extensibility:** You can map, add, or edit sensitive data fields per application, ensuring classification keeps pace as new APIs, fields, or business needs emerge.
- **Context-aware classification:** PII is flagged based on static analysis of API endpoints as well as dynamic analysis of traffic data.



This approach lets Vorlon perform DLP across apps, even when field names or structures differ, mapping everything back to a single, actionable source of truth.

Risk Scoring: Prioritizing What Matters Most

Vorlon assigns dynamic risk scores to every SaaS application and integration, providing crucial context for DLP decision-making and response:

- **Sensitive data risk:** Does the API expose PII, credentials, or secrets?
- **PII risk:** Does the app or API allow access to personally identifiable information?
- **Credentials risk:** Can credentials be listed, created, updated, or deleted via the API?
- **Secrets risk:** Does the API provide access to secrets (API keys, tokens, etc.) that allow further access or privilege escalation?

Risk scores are additive: The more sensitive the data or privileges exposed, the higher the risk score. These scores help security teams:

- Focus on the highest-risk apps and connections.
- Prioritize responses during incident investigations.
- Continuously monitor for risk drift as new data fields or integrations are discovered.

In-Depth Features: DLP for the Modern SaaS Stack

Detect newly accessed API endpoints containing sensitive data

- Vorlon automatically flags newly active API connections that our analysis shows could expose sensitive information, along with details about who or what accessed them
- Users can opt to receive multi-channel notifications and can review details, enabling timely action and prompt updates to DLP rules and compliance policies.

User risk profile

- Provides granular visibility into which applications and data each user (or non-human identity) accesses.
- Supports investigation into insider threats, privilege abuse, or compromised accounts, crucial for forensic readiness and compliance.

Labeling and alerting on compliance-related data access

- Tag specific API endpoints or applications as handling compliance-related data (e.g., SOX, HIPAA, GDPR, PCI).
- Receive instant alerts if access to those tagged interfaces occurs from unauthorized IP addresses, geolocations, or apps.

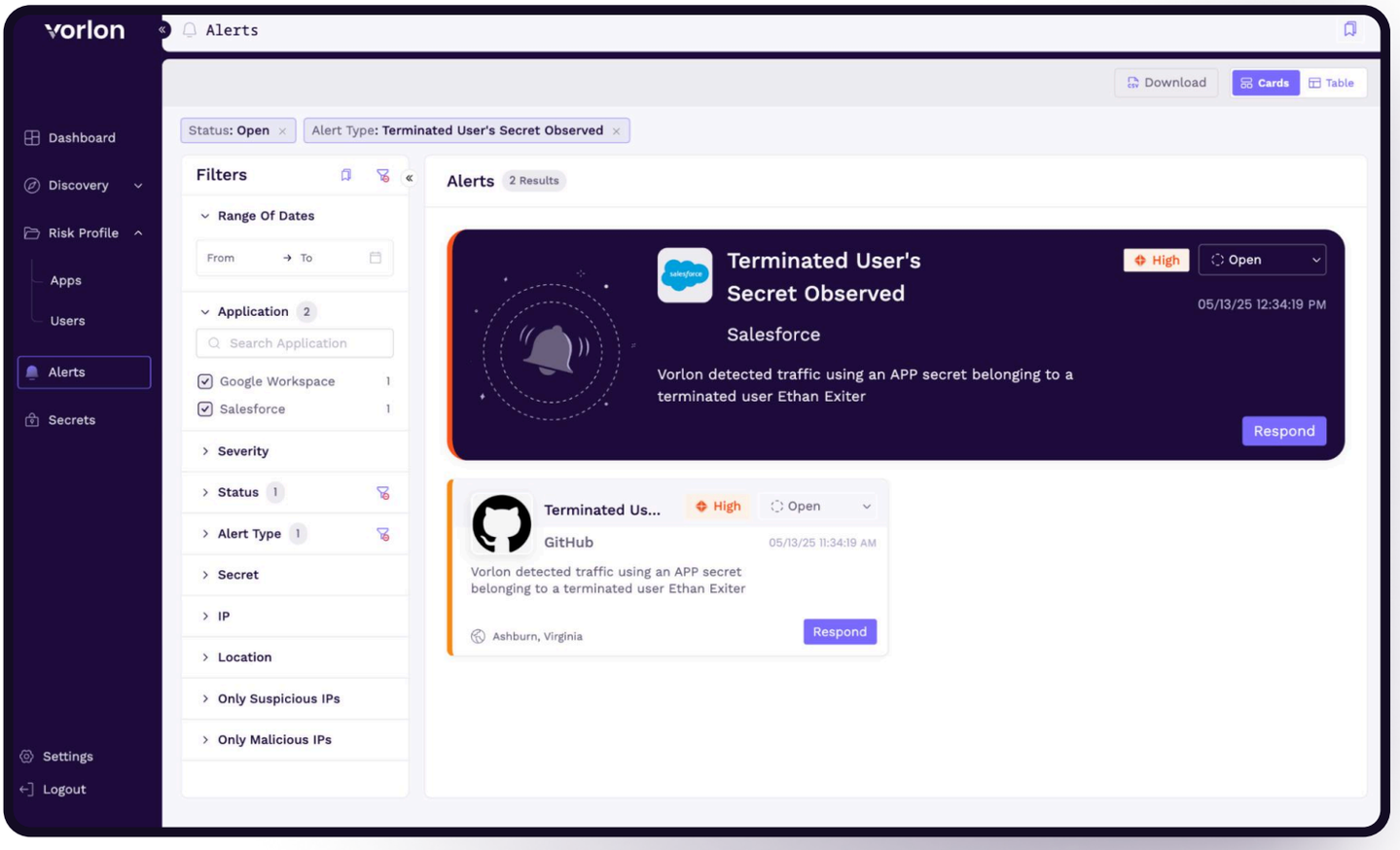
Data map

- Vorlon's intuitive data map visualizes where potentially sensitive data is being transferred between SaaS apps, APIs, and third-party integrations.
- Helps security, GRC, and audit teams immediately spot risky data flows and shadow integrations.

DLP-Type Alerts

Vorlon's DLP alerting framework provides actionable, real-time notifications for critical SaaS scenarios, including:

- **Sensitive data access:** Traffic from an IP address, app, or service to a new API endpoint that may contain sensitive data.
- **Terminated user's secret observed (High Severity):** Traffic using a high-privilege secret belonging to a terminated user, accessing sensitive endpoints.
- **Terminated user's secret observed (Medium Severity):** Similar activity with lower privileges, but still accessing endpoints with potential sensitive data.



Why Vorlon's Approach is the Right Fit for SaaS

- **Scalable and lightweight:** No agents, proxies, or invasive data inspection, which is perfect for large, fast-changing SaaS environments.
- **Adaptive and contextual:** Goes beyond basic data matching to incorporate behavioral analytics, risk scoring, and real-time context for every action.
- **Ecosystem-centric:** Designed to secure the entire SaaS ecosystem, not just individual apps or endpoints.
- **Compliance-ready:** Vorlon supports continuous monitoring requirements for compliance frameworks (SOX, HIPAA, PCI, GDPR) by providing audit evidence of access attempts to API interfaces identified as potentially handling regulated data. This delivers crucial visibility into who accessed what type of sensitive data endpoint, when, and from where.

Traditional DLP can't keep up with today's complex, ever-changing SaaS ecosystems. Vorlon is built for the way SaaS really works, delivering true data loss prevention, context, and control for the SaaS era.

Conclusion

Modern DLP isn't just about blocking data exfiltration; it's about understanding, detecting, and managing risk across a dynamic, interconnected SaaS ecosystem. Vorlon's agentless, adaptive, and risk-based approach redefines what's possible for DLP for SaaS, empowering security teams to see, control, and protect sensitive data no matter where it flows

About Vorlon

SaaS data moves 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 creates a live model of your SaaS environment to power fast, AI-driven remediation. 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.

AICPA SOC **SOC 2 Type II** Certified