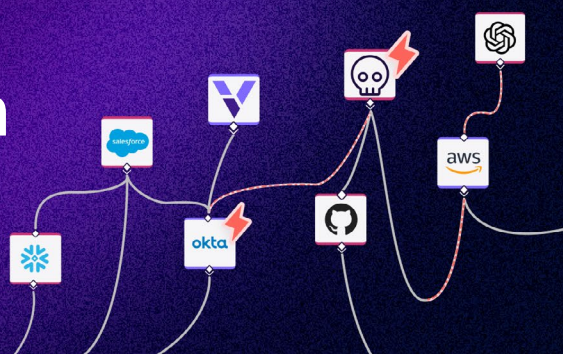
vorlon

SOLUTION BRIEF

Secure your SaaS ecosystem

SaaS moves fast. Vorlon gives you context to move faster.



Finally, an easy way to secure your SaaS ecosystem

Attackers aren't just breaching a single misconfigured SaaS app; they're exploiting the web of integrations, non-human identities, AI automations, and data flows that link these applications together. It's a complex and growing attack surface. It's also largely unmonitored.

Vorlon combines SaaS security posture management (SSPM), NHI security, data flow visibility, and detection and response, so you can see the full picture: what's connected, what's at risk, and what needs immediate action. After an agentless, proxy-free setup, you can monitor sensitive data flows, manage secrets, detect anomalies, and revoke access. With its agentless, patent-pending DataMatrix™ technology, Vorlon builds a live model of your SaaS environment to power fast, AI-driven remediation.

Core capabilities that protect your SaaS ecosystem

Visibility

Map third-party apps, APIs, and downstream services to monitor sensitive data and app-to-app connections.

Threat Detection

Detect unauthorized API activity, abandoned credentials, and unusual data-sharing behaviors that put sensitive data at risk.

Automated Response

Revoke risky credentials and remediate incidents via workflows integrated with SIEM, SOAR, IAM, and threat intel.

Continuous Monitoring

Detect policy drift, misconfigurations, and unauthorized changes in near real-time.

Actionable Alerts

Prioritize security alerts based on business impact—by apps, data flows, and downstream services.

Compliance-ready Reports

Support privacy requirements while providing actionable insights for security teams and application owners.

Vorlon addresses common SaaS ecosystem security challenges

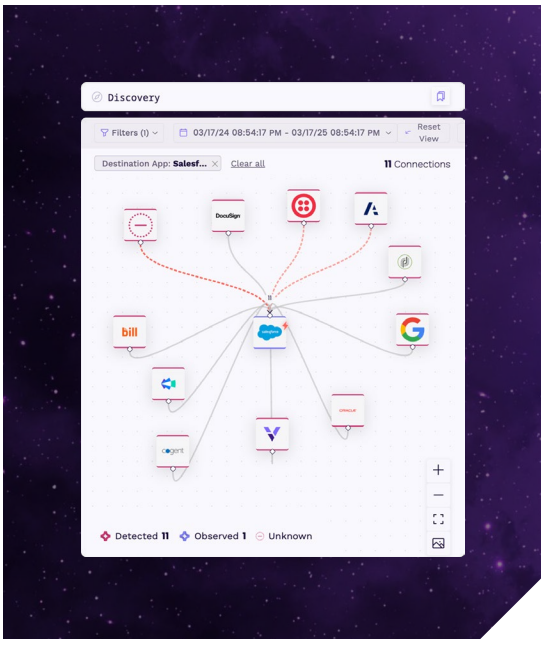
Challenge

- SaaS misconfigurations expose personal and financial data.
- Managing secrets (API keys, credentials, and OAuth tokens) in spreadsheets is a tedious, manual process.
- SaaS vendor breaches expose sensitive data, potentially leading to compliance violations and reputational damage.
- Third-Party Risk Management Programs (TPRM) provide point-in-time external risk assessments.
- HIPAA, HITRUST, HITECH, and PCI compliance require continuous monitoring, strict access controls, and audit-ready reporting.

How Vorlon helps

- Get visibility into APIs, risky misconfigurations, and sensitive data flows.
- Centralize NHI security, manage hygiene, and monitor secrets. Revoke access in two clicks.
- Rapidly assess the impact of a SaaS data breach and prevent further exposure.
- Add security monitoring to your TPRM program to detect policy drift and suspicious behavior.
- Simplify compliance by automatically collecting evidence. Run audit-ready reports for PCI and data privacy mandates.

Secure what others miss: the interactions between apps, identities, and data that power your business.



CarGurus

"Enables us to identify risks and detect SaaS threats faster."

Kelly Haydu
VP, InfoSec, Technology & Enterprise Applications

ThoughtSpot.

"Safeguards the data flowing across our SaaS applications."

Anthony Lee-Masis
CISO & VP IT

dutchie

"Brings third-party APIs out of the shadows."

Eric Richard
SVP, Engineering

splitit

"My SOC is resolving security issues 10 times faster."

Ran Landau
CTO

About Vorlon

Backed by Accel and SOC 2 Type 2 Certified, Vorlon is trusted by Fortune 500 companies and startups. Learn more at vorlon.io.

AICPA SOC

SOC 2 Type II
Certified