vorlon

SOLUTION BRIEF

Vorlon Third-Party Application Detection and Response (TADR)

Stop unauthorized PHI access before it spreads.

Modern healthcare runs on a complex ecosystem of third-party applications, APIs, and cloud platforms, making patient records more vulnerable than ever.

Vorlon TADR delivers proactive security coverage for this complex ecosystem. After an agentless, proxy-free setup, you can monitor sensitive data flows, manage secrets, detect anomalies, and revoke access. Powered by patent-pending DataMatrix® technology, Vorlon creates an algorithmic model of your applications and connected services for faster, AI-driven remediation.

Protect your healthcare app ecosystem and beyond

Visibility

Map third-party apps, APIs, and sensitive data flows containing PHI and billing data.

Threat Detection

Detect unauthorized API activity, abandoned credentials, and unusual data-sharing behaviors that put PHI 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 and access violations to maintain HIPAA, HITECH, and HITRUST compliance.

Actionable Alerts

Prioritize security alerts based on business impact—by third-party 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 healthcare IT security challenges

Challenge

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

How Vorlon helps

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

Other solutions solve a different challenge

Cloud Security (CNAPP and DSPM)

- Protects your public cloud, K8s, and static data stores...
- ...not SaaS and app-to-app sensitive data flows.

XDR

- Covers your endpoints, network, email, and cloud...
- ...not your third-party app ecosystem.

API Security

- Secures the APIs you publish...
- ...not the ones you consume.

SaaS Security (SSPM)

- Focuses on access risks...
- ...not the sensitive data flowing between SaaS apps.

DLP

- Targets endpoints, networks, and corporate data stores...
- ...not sensitive data flowing across applications.

Non-Human Identity Security

- Manages secrets for the apps you control...
- ...but lacks the context to understand deeper risks.

About Vorlon

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

AICPA SOC

SOC 2 Type II Certified