

**S&P Global**

Market Intelligence

**451 Research Market  
Insight Report Reprint**

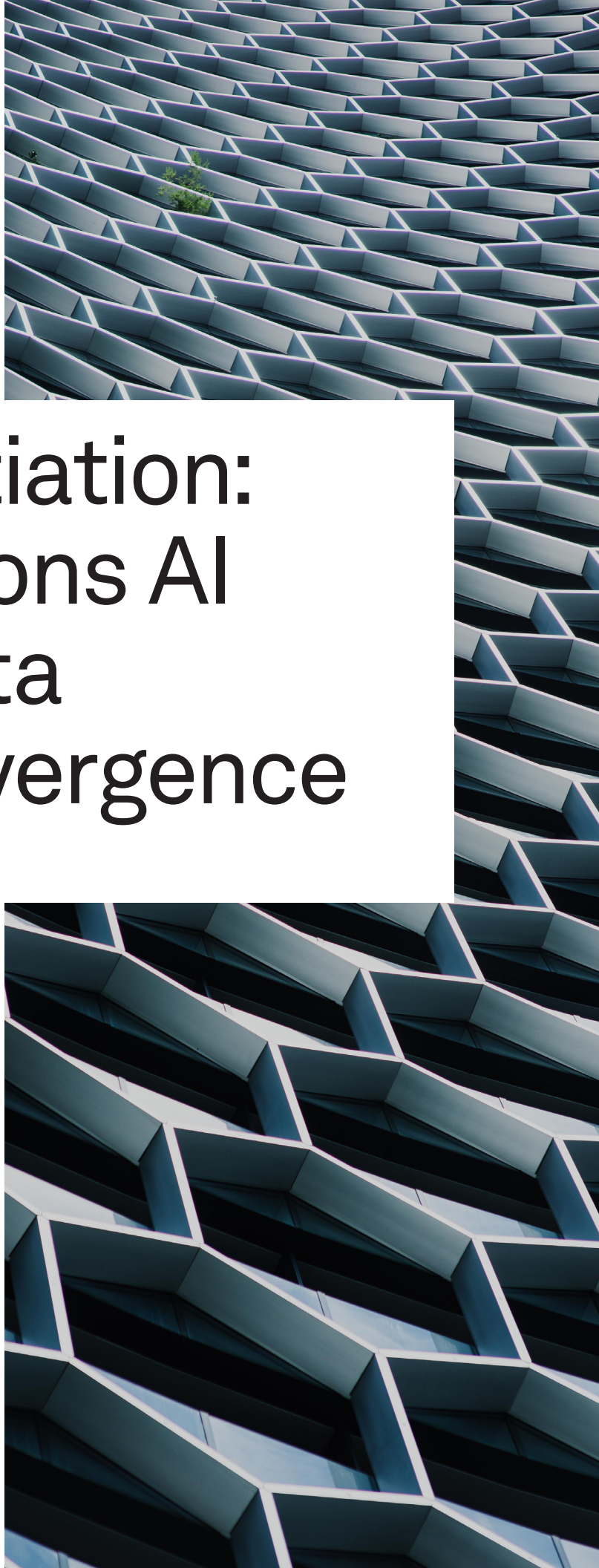
# Coverage Initiation: Vorlon envisions AI and SaaS data security convergence

December 19, 2025

**by Justin Lam**

The company has emerged to help enterprises secure their sensitive data as they adopt, integrate and operate SaaS and AI solutions. Vorlon believes in the convergence of AI and SaaS, and considers them a joint data security issue to address.

This report, licensed to Vorlon, developed and as provided by S&P Global Market Intelligence (S&P), was published as part of S&P's syndicated market insight subscription service. It shall be owned in its entirety by S&P. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from S&P.



## Introduction

Among SaaS companies, the question is no longer to what extent AI is used, but to what extent it is incorporated into products or transforms underlying business models. In functional SaaS categories such as content collaboration or customer relationship management, AI enhances a range of business outcomes. Whether they are looking to reduce toil via better automation or launch new products, existing and emerging SaaS vendors are eyeing larger opportunities. Vorlon has emerged to help enterprises secure their sensitive data as they adopt, integrate and operate SaaS and AI. The vendor believes in the convergence of AI and SaaS, and considers them a joint data security issue to address.

### THE TAKE

The distinctions between AI, SaaS and data security are converging, and Vorlon is looking to leverage this convergence to establish a more consistent framework and platform that an enterprise's third-party SaaS and AI tools now house and move on its behalf. With the proliferation of third- and fourth-party associations, SaaS providers and their customers will have mutual goals of secure and fast adoption, integration and operation.

Some SaaS vendors require additional licenses for security features, while others have different or custom data constructs. Vorlon is attempting to unify understanding of all interconnected services, agents, identities and data flows, and offer a common method for security operators to onboard SaaS and AI more efficiently. For the company, integrating with existing SaaS providers to furnish SaaS security posture management (SSPM) controls is one challenge, while motivating them to help drive distribution in a mutually beneficial way is another. As a newer market entrant, Vorlon will need to lead from the front.

---

## Context

Founded in 2022 by CEO Amir Khayat and CTO Amichay Spivak, Vorlon has raised almost \$16 million in funding from Accel Partners and Shield Capital, according to S&P Capital IQ Pro. Prior to founding Vorlon, Khayat and Spivak respectively held senior go-to-market and technology leadership roles at Palo Alto Networks Inc. They joined Palo Alto as key members of Demisto, which the company acquired in 2019 for \$560 million. Demisto's offerings are now foundational to Palo Alto's Cortex XSOAR product. Headquartered in Mountain View, California, Vorlon has approximately 30 employees spread throughout the US, UK and Israel.

## Services and technology

Vorlon is deployed as an agentless SaaS platform to protect and secure sensitive data that an enterprise's third-party app (e.g., SaaS and AI tools) vendors house and move. Vorlon roughly fits into the profile of SSPM but it exhaustively examines third- and fourth-party SaaS and AI providers that an enterprise has, enabling identification of both direct and indirect sensitive data deployment. For instance, while many organizations have sensitive customer personally identifiable information stored in their CRM as a system of record, they might also use adjacent services such as customer outreach or loyalty that operate against the CRM data. Understanding the flows of sensitive data and contextualizing assessed risk among different SaaS and AI suppliers is critical to security.

SaaS security faces potentially faster attacks. As a result, SaaS environments have shorter attack paths for adversaries to follow. Recent attack techniques used by adversarial groups like ShinyHunters worked by taking an OAuth token and hijacking sessions into SaaS environments. While many data breaches have featured more persistent threats with significantly longer dwell times, recent breaches into SaaS environments have exfiltrated data in minutes and hours rather than residing on corporate networks or endpoints for weeks or months. Monitoring for unusual activities or behaviors is also critical to remediating fast-moving attacks.

Vorlon converges SaaS posture management, data and identity security. Much of the access to sensitive data is not governed by permissions assigned to the data itself but rather to the identities entitled to that data. Moreover, API access and other nonhuman identities (NHIs) are also frequently “bearer” identities. What frequently determines an API call from one SaaS environment to another are the secrets, tokens or certificates that the API bears or has direct access to. Especially in SaaS environments, data access is remediated by changes in the properties of identities.

The inclusion of AI promises greater automation but also increases security dependencies and complexities. Agentic interfaces operating on behalf of other processes might not correctly honor the original user’s permissions or entitlements. For example, if one SaaS user relies on an agent or AI process to augment data generation with retrieved content, there must be assurances that the agent has the same levels of authority as the original SaaS user. Individual staff members automating their performance reviews in a human resources management system should not be able to easily jailbreak AI to offer full company payroll information.

Against this backdrop, Vorlon is seeking to establish the full chain of both direct and indirect consumption, whether by users, NHIs or AI agents. By understanding enterprise data within SaaS and all subsequent dependencies, the vendor is aiming to both enhance alert fidelity and add greater confidence to remediation efficacy.

## Strategy

SSPM providers have varied their approach to the depths of integration with SaaS specialists. Some SaaS offerings have extensive built-in security controls, such as Salesforce Shield. ServiceNow Inc.’s recent purchase of Veza is another example. Other SSPM vendors integrate deeply with just a few SaaS tools, while others add dozens of new integrations every quarter.

Vorlon believes that there is merit to both approaches. Fundamental to its strategy is bringing common understanding to security risks across an enterprise’s SaaS ecosystem. While the company integrates with dozens of SaaS tools, it can also observe or detect hundreds more. It asserts that it is not just the aggregate number of SaaS integrations available that is important, but also the continuous ability to normalize the relationships across multiple SaaS tools. Matching the third- and fourth-party risks has benefits for operators, as each service can be securely onboarded consistently.

As such, Vorlon has found initial success among technology-savvy organizations that incorporate SaaS services while building or offering their own SaaS services. These advanced customers have dual pressures — onboarding SaaS securely to incorporate into their own stacks becomes a time-to-market issue as well as a compliance and governance matter. Given the dynamic nature of its customers’ SaaS environments, Vorlon argues that security assessment is better understood over time rather than at a single point in time. Enterprises must demonstrate not only that they have securely onboarded a given SaaS, but also that they continue to operate it safely.

For Vorlon and its customers and technology partners, it sees a converged destiny where all parties share the same desired outcome — successful and secure operation and adoption of their respective technologies. Previous 451 Research reports on SSPM have described the notion of converged destiny. Compliance automation has also enabled thousands of SaaS companies to achieve design compliance, highlighting how SaaS vendors from all verticals and functional use cases are embracing security to increase customer trust.

## Competition

Vorlon operates in a crowded data security space. AI security providers such as HiddenLayer and Knostic are but two examples of vendors looking to police models, model composition, and prompt inputs and outputs. Other data security players are leaning heavily into AI security initiatives — in some cases, all prompts in chat interfaces are inspected for data loss, while in other cases, data classification prevents retrieval for augmented generation.

Cyera, Varonis Systems Inc., Proofpoint, Thales SA, IBM Corp., Fortra, CrowdStrike Holdings Inc., Palo Alto, Cyberhaven and Netskope Inc. have all augmented their data security suites to combine data security observation and remediation. Newer vendors like Teleskope have embraced this combined approach from their inception. Blurring the lines, SSPM providers such as Valence Security, Reco, Wing Security, Material Security, AppOmni, Obsidian, Nudge Security and DoControl have embedded data security controls into their SaaS offerings.

Major SaaS platform developers have incorporated their own data security features. ServiceNow's reach for Veza both enriches the company's entire IT service management suite as well as provides an intriguing upsell. Salesforce Inc., Google and Microsoft Corp. are additional examples of vendors with built-in controls. In the long term, it is conceivable that frontier models from Anthropic or OpenAI will include data security features in their models.

## SWOT Analysis

<p><b>STRENGTHS</b></p> <p>By leaning into its platform-first approach, Vorlon is aiming to provide a consistent method for security teams to onboard new SaaS vendors. The consistency and flexibility of this process will better help enterprises respond to third- and fourth-party risks while operating various SaaS and AI tools.</p>	<p><b>WEAKNESSES</b></p> <p>Distribution could be a challenge. Although it shares a common vision and believes in a converged destiny with other major SaaS providers, Vorlon must demonstrate to the SaaS incumbents how this will be accomplished. It will have to do most of the heavy lifting and lead from the front by winning one major joint customer to build momentum.</p>
<p><b>OPPORTUNITIES</b></p> <p>Interest in GenAI and in securing GenAI are peak initiatives, and both have grown in tandem. Conveying how both interests are inclusive of each other should unlock value for Vorlon. Heightened adoption of AI and SaaS creates an opportunity for more mature security adoption.</p>	<p><b>THREATS</b></p> <p>Rivalry is immense in multiple converging categories of data, SaaS and AI security. In addition to deciding which of these categories to focus on, the threat of lost time is also immense. As Vorlon matures from its product-market-fit stages to go-to-market-fit stages, it must crystalize the customer profile that makes it a "must have." Pursuing deals without compelling events is a competitive risk.</p>

## CONTACTS

**Americas:** +1 800 447 2273

**Japan:** +81 3 6262 1887

**Asia-Pacific:** +60 4 291 3600

**Europe, Middle East, Africa:** +44 (0) 134 432 8300

[www.spglobal.com/marketintelligence](http://www.spglobal.com/marketintelligence)

[www.spglobal.com/en/enterprise/about/contact-us.html](http://www.spglobal.com/en/enterprise/about/contact-us.html)

Copyright © 2026 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global keeps certain activities of its divisions separate from each other to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain nonpublic information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its websites, [www.standardandpoors.com](http://www.standardandpoors.com) (free of charge) and [www.ratingsdirect.com](http://www.ratingsdirect.com) (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at [www.standardandpoors.com/usratingsfees](http://www.standardandpoors.com/usratingsfees).