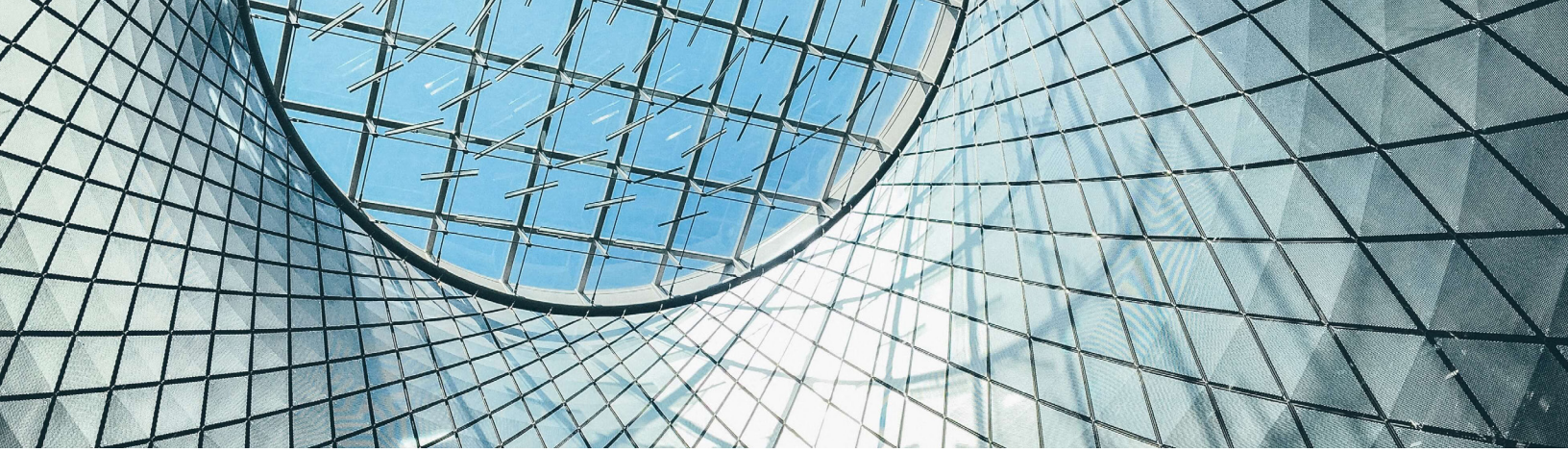


451 Research Market Insight Report Reprint

Coverage Initiation: Solvo tackles CNAPP with adaptive cloud security and deep application analysis

November 6, 2023

by Garrett Bekker

Israel-based Solvo combines elements of CIEM and CSPM into a broader cloud-native application protection platform. The company provides “adaptive remediation” capabilities that enable application of least-privilege access policies and secure configuration to cloud-native applications.

S&P Global
Market Intelligence

Introduction

Israel-based Solvo is a vendor that combines elements of cloud security posture management (CSPM) and cloud infrastructure entitlement management (CIEM) into a broader CNAPP (cloud-native application protection platform) offering. It provides "adaptive remediation" capabilities that enable the application of least-privilege access policies and secure configuration to cloud-native applications via its patented application analysis technology.

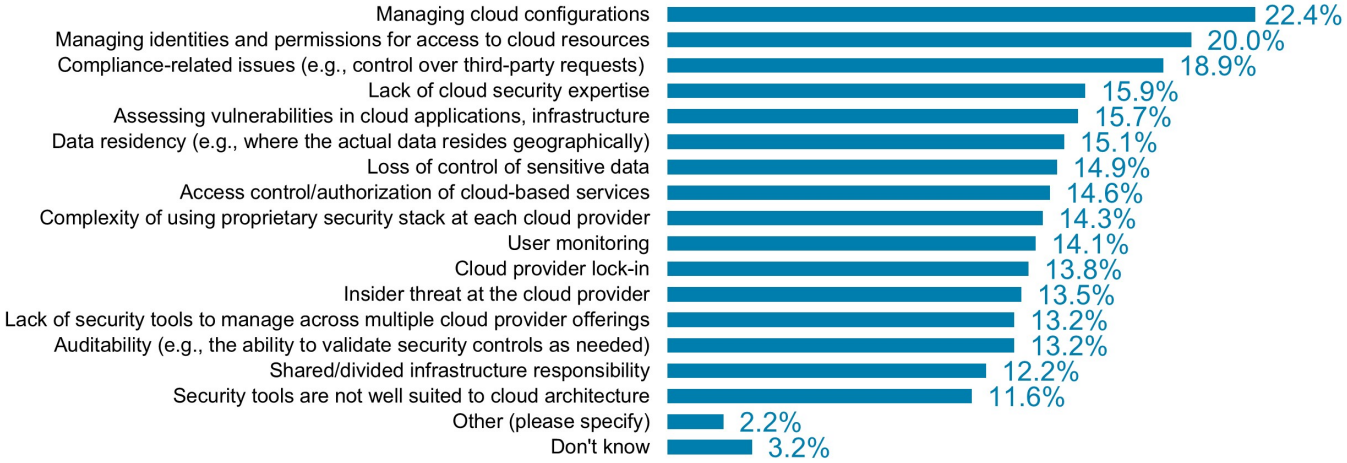
THE TAKE

Solvo's pedigree reflects management's background in the Israeli Defense Forces, as well as work with cloud security pioneer Dome9. Solvo's runtime application analysis and ability to create policies automatically could help it stand out in a crowded field, along with its automated remediation and new data security features. However, both CIEM and CSPM have arguably become features of the broader CNAPP market, which implies Solvo will compete with both well-heeled CNAPP startups like Wiz, Orca and Aqua, as well as established veterans like Palo Alto Networks Inc. and Zscaler Inc. Adding cloud workload protection, as other CIEM vendors have, would be a logical extension for Solvo. However, like many cloud security startups, Solvo could be an acquisition target for a larger CNAPP or cloud security vendor, or established vendors in privileged access management (PAM), identity governance and administration, or identity threat detection and response that are looking to add CNAPP capabilities.

Context

According to 451 Research's Information Security, Cloud Security 2022 survey, enterprises now devote roughly one-third of their overall spending on security tools to cloud security. Furthermore, some of the most pressing security pain points include managing configurations, identities and permissions in cloud resources (see figure). In recent years, the CSPM and CIEM segments have emerged to address these challenges, as we have chronicled in reports on Sonrai, Ermetic and others.

Managing configurations, identities and permissions are top cloud security pain points



Source: 451 Research's Voice of the Enterprise: Information Security, Cloud Security 2022.
Q. What are the top pain points with securing your organization's cloud infrastructure (e.g., IaaS or PaaS)? Please select up to three.
Base: All respondents (n=370).

Tel Aviv-based Solvo was founded in April 2020 by CEO Shira Shamban and CTO David Hendri. Both gained experience in cloud security while at CSPM provider Dome9, and served in the Israeli Intelligence Corps. When we last spoke with Solvo, the company had roughly 30 employees, with R&D in Israel and the rest in the US (virtual/remote). Solvo claims over 65 customers worldwide (mostly in North America and Latin America) in healthcare, banking and IT. The company has raised a total of $11 million in venture funding, with investors including lead TLV Partners, along with Surround Ventures, Magenta Venture Partners, and startup funding from AWS and Intel Corp.'s Ignite.

Products

At its most basic level, Solvo scans and discovers misconfigurations, excessive permissions, admin-level access and third-party access to applications running in the public cloud (AWS, Azure and GCP coming). In that sense, it combines features of both CSPM and CIEM offerings. Solvo claims to be agnostic, and can work with all public cloud workloads including containers and serverless functions.

The company offers five separate products. The core product is IAMagnifier, which discovers all an organization's public cloud inventory and creates a visual map of how the components are connected. For example, it can show how a container is connected to an S3 bucket or to a bastion server. It can also show what roles and policies are in place and who is allowed access to specific resources, including to demonstrate compliance to auditors. IAMagnifier can be used to uncover unnecessary connections and highlight them so they can be identified as a potential attack path.

Policy Manager analyzes the behavior of cloud apps, and automatically creates a granular least-privilege access policy that only grants the specific access needed for a given user or machine. For example, if a container needs to read an item in an S3 bucket, it does not need access to the whole S3 bucket, or all S3 buckets, but only to specific buckets/partitions/file types. Solvo can also add specific conditions for access to cloud resources. However, unlike other cloud security vendors that rely on static analysis of cloud access logs, Solvo uses a patented technique that performs runtime analysis of applications running on the public cloud, to understand their context and help automatically craft a least privilege access policy from scratch.

Data Posture Manager is a newer product that was built to respond to customers looking for help managing and securing sensitive data. Data Posture Manager helps organizations understand the risk of their sensitive data, and how to mitigate that risk by discovering and monitoring it, providing risk scores and remediation. This product is now included as a feature of Solvo's overall security posture management, and can be applied to a wider range of resources than just data.

Compliance Manager provides preconfigured rules and predefined frameworks for compliance with mandates such as HIPAA, PCI-DSS, GDPR, CCPA, SOC2, ISO 27001 and others. Compliance Manager provides a dashboard to show violations (which entities are violating specific rules, etc.) along with detailed access logs and insight on potential breaches. Alerts can be sent via Slack, Jira, SNS, Webhooks or other standard tools or frameworks. A new addition to the compliance manager is remediation code scripts, which are adapted for each issue and each account to help security and DevOps teams assist governance, risk and compliance teams.

Security Genie started as an app that automatically generates a simple health-check report that surfaces the top dozen or so issues that need attention, mainly those that need more advanced security measures. Security Genie is now offered as an AI-based chatbot that can answer basic questions, like "Am I PCI compliant?" or "Do I have any S3 buckets configured for public access?"

Strategy

Solvo initially took a shift-left approach, and earlier in the development process focused mainly on developers and tackling cloud security issues. It now believes (rightly) that security posture has become a commodity, and that fixing security issues remains the biggest challenge for organizations. As such, its current focus is on remediation.

In contrast to other cloud security products, which provide remediation by giving specific instructions for the organization to follow (e.g., do steps one, two and three), Solvo provides actual code fixes that address infrastructure configuration for each unique security issue. However, the company falls short of providing auto-remediation, which it believes most organizations are not yet ready for. Instead, Solvo provides a detailed set of guardrails to guide customers through the remediation process without full automation.

The Solvo console is deployed as a SaaS app, and is priced based on the total number of compute and storage assets in the account. In terms of go-to-market focus, it mainly targets smaller enterprises with shorter sales cycles in verticals including financial services and fintech, software, retail, and the cloud. The company has also focused on machine identities more than human identities, although it plans to partner with identity providers like Microsoft Corp. (Entra), Okta Inc. and Ping Identity.

Competition

Although Solvo is most likely to compete with vendors that offer CIEM and CSPM functionality, the bulk of the latter have expanded beyond their roots and into new areas. Authomize, for example, has added identity threat detection and response capabilities, while Ermetic (recently acquired by Tenable) and Sonrai have added CSPM and cloud workload protection and are now squarely in the CNAPP camp, as is Horangi (recently acquired by BitDefender).

Sonrai also has data security capabilities. Britive has CIEM features, but has positioned itself as more of a cloud-native PAM vendor. Identity governance and administration vendors like Sailpoint Technologies and Saviynt, and PAM vendors like BeyondTrust, CyberArk and Senhasegura have also added CIEM features. Solvo could encounter Microsoft's Entra Permissions Management (from the CloudKnox acquisition) in CIEM deals. In the broader CNAPP space, competitors include pure plays such as Wiz, Orca, Aqua, Lacework and Sysdig, as well as incumbent security providers like Crowdstrike Holdings Inc., Palo Alto Networks, Tenable Networks (Ermetic), Trend Micro Inc. and Zscaler.

SWOT Analysis

STRENGTHS	WEAKNESSES
The company offers the ability to create policies automatically, as well as a combination of CIEM and CSPM, data security posture features, and patented application analysis. Adaptive remediation is a key differentiator.	CIEM and CSPM are now CNAPP features. Solvo lacks other CNAPP capabilities, such as cloud workload protection.
OPPORTUNITIES	**THREATS**
Dealing with configurations, identities and permissions are top pain points for cloud security. As such, enterprises now devote roughly one-third of their overall security budgets to cloud security.	Solvo will need to take on both well-heeled cloud security startups and incumbents.

CONTACTS

The Americas
+1 877 863 1306
market.intelligence@spglobal.com

Europe, Middle East & Africa
+44 20 7176 1234
market.intelligence@spglobal.com

Asia-Pacific
+852 2533 3565
market.intelligence@spglobal.com

www.spglobal.com/marketintelligence