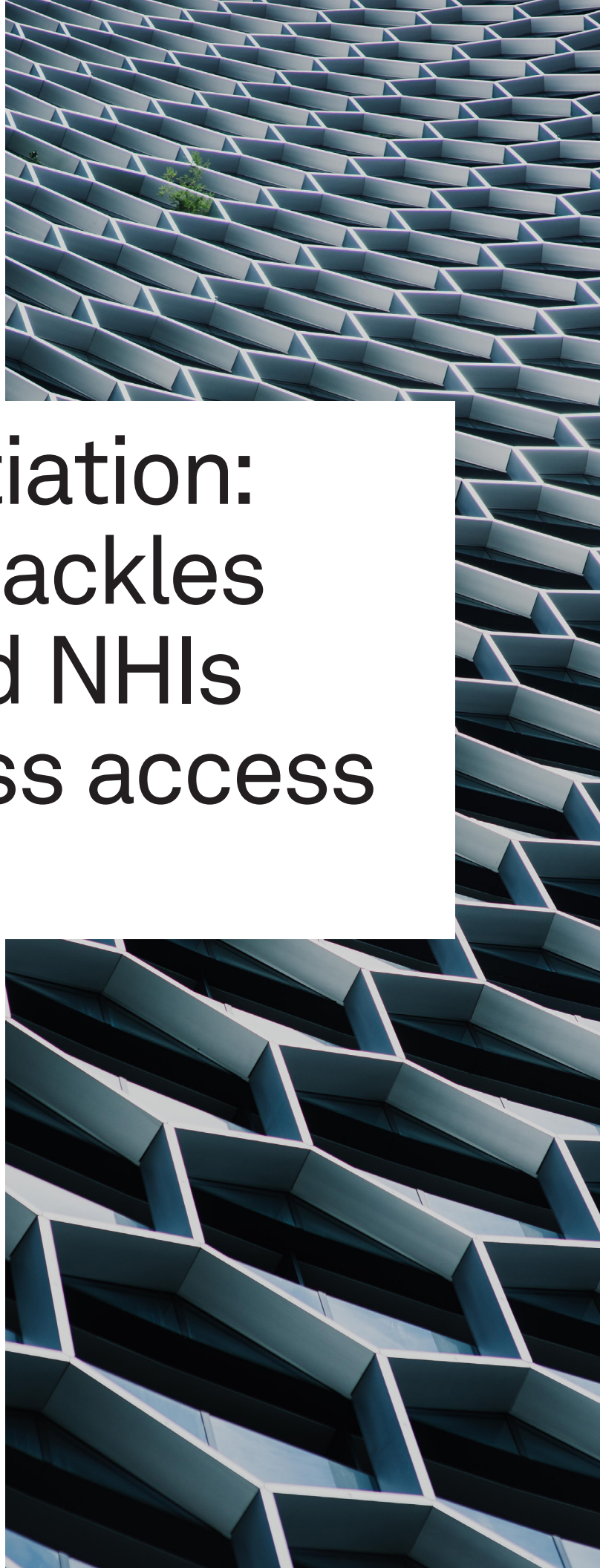
451 Research
by S&P Global



451 Research Market Insight Report Reprint

Coverage Initiation: P0 Security tackles IGA, PAM and NHIs with agentless access platform

May 26, 2026

by Garrett Bekker

Betting that the authorization layer is where modern privilege now lives, the company is attempting to address several emerging key trends in identity and access management with an agentless platform that combines identity governance and administration and privileged access management for both human and nonhuman identities.

This report, licensed to P0 Security, developed and as provided by S&P Global (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

We have recently observed several emerging themes in identity and access management, including the growing convergence of identity governance and administration and privileged access management, the rise of nonhuman identities, and the emergence of agentic identities. P0 Security is attempting to address all three of these trends with an agentless platform that covers IGA and PAM use cases for both human and agentic identities.

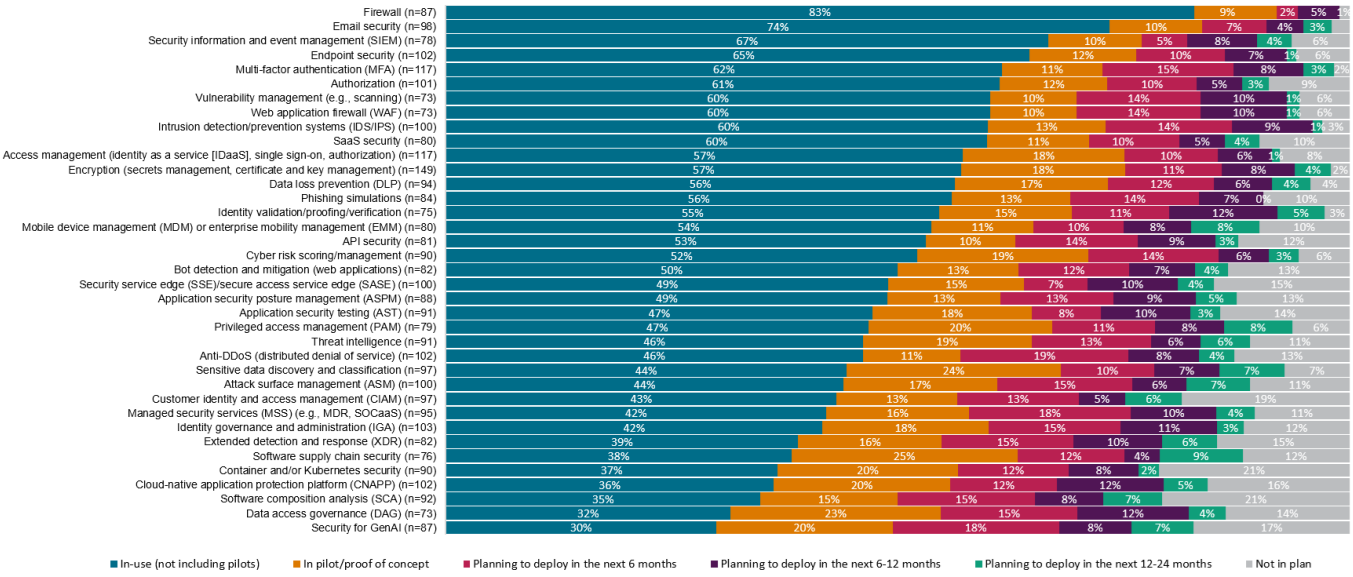
THE TAKE

From a marketing perspective, P0 Security is betting that the authorization layer is where modern privilege now lives. Thus, the company has taken care to differentiate itself from a prior wave of authorization startups by framing its offering around runtime authorization rather than authentication and credential management.

Context

According to 451 Research's Voice of the Enterprise: Information Security, Technology Road Map 2025 survey, managing privileged access and employee access rights consistently rank among the top identity management pain points for enterprise decision-makers, yet both identity governance and administration (IGA) and privileged access management (PAM) deployment rates sit well below 50%. At the same time, the proliferation of cloud resources and the recent explosion of nonhuman identities (NHIs) (service accounts, workload identities, AI agents) have expanded the attack surface far beyond what traditional PAM architectures were designed to protect. P0 Security is positioning itself as an answer with an agentless, API-native architecture that removes a primary barrier to IGA and PAM adoption as well as its unified treatment of human and agentic identities.

Enterprise IGA and PAM adoption remains below 50%



Source: 451 Research from S&P Global Energy Horizons.

Voice of the Enterprise: Information Security, Technology Road Map 2025.

Q. What is your organization's status of implementation for the following information security technologies?

Base: All respondents, abbreviated fielding (n=149).

© 2026 S&P Global.

©Copyright 2026 S&P Global. All Rights Reserved.

San Francisco-based P0 Security was founded in 2022 by three practitioners with deep backgrounds in cloud-native development, cloud security, observability and DevOps: Shashwat Sehgal (CEO), Gergely Danyi (CTO) and Nathan Brahms (VP of Engineering). The company name derives from the term "priority zero," which refers to the highest-urgency classification in engineering, inspired by the founders' frustration with existing (typically lengthy) processes for obtaining secure access to production resources to resolve a critical customer issue. P0 Security has raised $20 million to date, including a $15 million series A round in 2024 led by SYN Ventures, along with Zscaler and Lightspeed. Current headcount stands at roughly 50 employees.

Products

P0 Security offers a unified platform that governs and controls access for both human and agentic identities across cloud, hybrid and on-premises infrastructure. The platform is built on an agentless, API-native architecture, without any proxies, jump hosts or bastion infrastructure to deploy or maintain.

At runtime, when a user or workload requests access to a resource, P0 Security authenticates the requesting identity through the organization's existing Identity provider (IdP; currently Okta, Microsoft Corp. Entra ID, Active Directory, Google Workspace and Ping Identity), enforcing the organization's existing MFA or authentication controls. Once authenticated, P0 dynamically provisions the appropriate role or policy in the target system. The provisioned access is time-bound and expires automatically, in line with recent trends toward zero standing privilege in PAM, which P0 addresses by replacing standing access with just-enough-privilege and just-in-time (JIT) access for all types of identity.

The foundation of the platform is the Access Graph, which provides a continuous mapping of every identity's access paths, entitlements and potential vectors for lateral movement. The graph surfaces posture risks such as unused roles and over-permissioned service accounts to help teams prioritize remediation before potential incidents occur and replace standing permissions with JIT policies directly from the remediation workflow. Identity Inventory is P0 Security's comprehensive integration mesh, which centralizes all identity-related metadata across servers, databases, entitlements, IdPs, clouds, Kubernetes, code and on-premises assets, in order to auto-discover privilege and provide critical context for runtime policy enforcement.

For NHI governance, P0 applies the same discovery, posture, life cycle, JIT access and audit capabilities to NHIs as it does to human users. The platform provides automated discovery of service accounts across multi-cloud environments, maps entitlements and ownership, automates credential rotation and enforces least-privilege access.

P0 Security's most recent capability is its Authorization Control Plane for AI agents. As with humans, P0 replaces persistent agent permissions with time-bound, task-specific authorization evaluated at runtime — ensuring that AI agents can perform only actions aligned with policy and business intent. The platform currently integrates with Claude, AWS Bedrock, Google Vertex AI and Microsoft CoPilot. P0 also offers an MCP Gateway as an enforcement point that sits in front of every MCP server in the customer's environment and enforces tool-level authorization.

Strategy

The year 2025 was primarily focused on building out P0's go-to-market (GTM) strategy, including executive hires across product (Chief Product Officer Neha Duggal), sales (VP of Sales Dan Hoffman) and marketing (Chief Marketing Officer Cari Jaquet). P0's GTM motion targets midsized to large enterprises that have or are in the process of making the transition to cloud, particularly as a supplement to existing PAM tools for on-premises environments. In the past year, P0's strategy has shifted away from authentication-centric messaging focused on establishing "who you are" via credential rotation, vaults and shared accounts, toward authorization and determining "what can you do," and perhaps more importantly, "what did you do?" The company is also targeting smaller organizations facing SOC2, HIPAA or other regulatory requirements that need automated access governance without the complexity or cost of enterprise IGA platforms. P0 Security also has a strategic alliance with Zscaler's ZPA.

©Copyright 2026 S&P Global. All Rights Reserved.

Competition

P0 Security competes primarily in the cloud-native and next-generation PAM space, with some overlap with IGA and NHI governance. Incumbent PAM vendors include BeyondTrust, CyberArk (acquired by Palo Alto Networks Inc.) and Delinea, as well as Segura, ARCON, Devolutions, Manage Engine and Wallix. Emerging vendors with next-generation PAM functionality include StrongDM (acquired by Delinea) and Teleport; Okta Inc. and SailPoint Technologies have also added PAM and identity security capabilities recently. Devolutions is SMB-focused and combines PAM with password management and remote access management.

As noted above, Delinea recently added JIT authorization with the acquisition of StrongDM, along with the ability to span both legacy on-premises and modern cloud-based environments. Teleport's cloud-native infrastructure access platform uses a proxy/gateway model (as does StrongDM). C1 (fka ConductorOne) is a cloud-native IGA specialist that has added PAM capabilities including JIT access.

The competitive landscape for agentic identity spans multiple categories including customer identity and access management vendors like Descope, as well as vendors from IGA (SailPoint), PAM (CyberArk), ITDR (Cayosoft, Silverfort, Sonrai) and even password management (1Password) vendors expanding to cover NHIs. Additionally, AI platform providers with native agent identity tooling, and emerging NHI-focused startups that see agentic AI as an extension of machine and other nonhuman identities are also part of the mix, as are certificate and secrets management vendors such as AppviewX (via the Eos pickup), Comodo, Digicert, Entrust, GitGuardian, Keyfactor and Sectigo.

Emerging startups with agentic identity ambitions include Actual AI, Aembit, Clutch Security, Dedalus Labs, Eve Security, Indent, Metorial, Spirl, Strata, Sym, Teleport, Token Security and Zenity. Aembit has been described as an "Okta for nonhuman identities." Indent (recently acquired by Terraform/HashiCorp parent company) focuses on JIT access provisioning for both human and machine identities.

SWOT Analysis

STRENGTHS	WEAKNESSES
P0 Security has a strong practitioner-led founding team with deep cloud security, DevOps and cloud-native backgrounds backed by established investors (Zscaler, SYN Ventures, Lightspeed). P0 has a unified governance model for human, nonhuman and agentic identities. Its agentless, API-native architecture reduces deployment complexity, which is a primary barrier to PAM adoption.	P0 Security is primarily focused on cloud and hybrid infrastructure, with limited native support for on-premises-only environments that traditional PAM vendors address, as well as workloads that are not callable by APIs. Authorization positioning could rekindle memories of a prior generation of authorization vendors that failed to gain commercial traction.
OPPORTUNITIES	**THREATS**
As enterprises race to deploy AI agents, agentic AI governance represents a substantial emerging market opportunity. P0 Security's agentless architecture could appeal to an underserved market, particularly midmarket and cloud-native organizations that have never deployed legacy IGA or PAM tools.	Well-funded incumbents (CyberArk, Okta, SailPoint) are actively pursuing IGA/PAM convergence and NHI governance through acquisitions and product expansion.

Source: 451 Research.

The author(s) used a proprietary S&P Global AI platform in the production of this report. It was subsequently peer-reviewed, fact-checked and edited before publication.

©Copyright 2026 S&P Global. All Rights Reserved.

CONTACTS

www.spglobal.com
www.spglobal.com/en/enterprise/about/contact-us.html

Copyright © 2026 S&P Global Inc. All rights reserved.

These materials, including any software, data, processing technology, index data, ratings, credit-related analysis, research, model, software or other application or output described herein, or any part thereof (collectively the "**Property**") constitute the proprietary and confidential information of S&P Global Inc its affiliates (each and together "**S&P Global**") and/or its third party provider licensors. S&P Global on behalf of itself and its third-party licensors reserves all rights in and to the Property. These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable.

Any copying, reproduction, reverse-engineering, modification, distribution, transmission or disclosure of the Property, in any form or by any means, is strictly prohibited without the prior written consent of S&P Global. The Property shall not be used for any unauthorized or unlawful purposes. S&P Global's opinions, statements, estimates, projections, 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, and there is no obligation on S&P Global to update the foregoing or any other element of the Property. S&P Global 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. The Property and its composition and content are subject to change without notice.

THE PROPERTY IS PROVIDED ON AN "AS IS" BASIS. NEITHER S&P GLOBAL NOR ANY THIRD PARTY PROVIDERS (TOGETHER, "**S&P GLOBAL PARTIES**") MAKE ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE PROPERTY'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE PROPERTY WILL OPERATE IN ANY SOFTWARE OR HARDWARE CONFIGURATION, NOR ANY WARRANTIES, EXPRESS OR IMPLIED, AS TO ITS ACCURACY, AVAILABILITY, COMPLETENESS OR TIMELINESS, OR TO THE RESULTS TO BE OBTAINED FROM THE USE OF THE PROPERTY. S&P GLOBAL PARTIES SHALL NOT IN ANY WAY BE LIABLE TO ANY RECIPIENT FOR ANY INACCURACIES, ERRORS OR OMISSIONS REGARDLESS OF THE CAUSE. Without limiting the foregoing, S&P Global Parties shall have no liability whatsoever to any recipient, whether in contract, in tort (including negligence), under warranty, under statute or otherwise, in respect of any loss or damage suffered by any recipient as a result of or in connection with the Property, or any course of action determined, by it or any third party, whether or not based on or relating to the Property. In no event shall S&P Global 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 Property even if advised of the possibility of such damages. The Property 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.

The S&P Global logo is a registered trademark of S&P Global, and the trademarks of S&P Global used within this document or materials are protected by international laws. Any other names may be trademarks of their respective owners.

The inclusion of a link to an external website by S&P Global should not be understood to be an endorsement of that website or the website's owners (or their products/services). S&P Global is not responsible for either the content or output of external websites. S&P Global keeps certain activities of its divisions separate from each other in order 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 Ratings' public ratings and analyses are made available on its sites, www.spglobal.com/ratings (free of charge) and www.capitaliq.com (subscription), and may be distributed through other means, including via S&P Global publications and third party redistributors.

Content may be created with the assistance of an AI tool in accordance with our Terms of Use (https://www.spglobal.com/en/terms-of-use).