



From Chaos to Control: SailPoint Unlocks a Secure Agentic Era with Autonomous Identity Security

October 6, 2026

Expands product innovation across unified platform at Navigate 2026 delivering the industry's first real-time defense to discover, govern and protect all human, machine and AI agent identities

Key Announcement Highlights:

- **Introducing SailPoint Autonomous Agents:** SailPoint debuts three classes of Autonomous Agents that enforce policy, right-size privileges, and protect systems without disrupting legitimate business automation.
- **Autonomous Identity Security Posture Management (A-ISPM):** New A-ISPM uses the live identity context in SailPoint Atlas to continuously uncover critical exposures across all identity types, then closes the loop with real-time remediation.
- **Expanded SailPoint Agentic and Human Fabrics:** SailPoint expands its Agentic Fabric to map the entire AI agent surface area—enabling shadow AI discovery, runtime authorization, and instant 'kill switch' controls—while simultaneously advancing its Human Fabric with next-generation certifications and segmented identity data to give organizations finer-grained access governance.
- **Enhanced Atlas capabilities and Atlas Extensibility framework:** New common services, SaaS plug-ins, and Workflow enhancements, including versioning, execution history, and serial loops of up to 1,000 iterations, make Atlas a more unified and extensible foundation for scaling identity security.
- **Zero Standing Privilege for humans and machines:** New Just-in-Time (JIT) provisioning with conditions, plus effective privilege visibility, replaces always-on access for people, service accounts, and AI agents alike.

AUSTIN, Texas, Oct. 06, 2026 (GLOBE NEWSWIRE) -- Today at Navigate 2026, its annual flagship conference, [SailPoint, Inc.](#) (Nasdaq: [SAIL](#)), a leader in enterprise identity security, announced significant [new capabilities](#) across [SailPoint Agentic Fabric](#)™ (SAF) and [SailPoint Human Fabric](#)™ (SHF), the two purpose-built products of its Identity Security solution, built on SailPoint Atlas. These innovations give enterprises what they need most in the agentic era: full visibility into every hidden AI tool, continuous compliance across human and machine workflows, the replacement of permanent access keys with temporary permissions, and the transformation of identity security from a static compliance check into real-time, automated defense.

According to the latest [SailPoint Horizons of Identity Security report](#), 79% of enterprises are already running AI agents in production, yet only 2% have deployed identity security tools purpose-built to govern and secure them. Meanwhile, enterprises are stuck between static reviews that are outdated the moment they finish and posture dashboards that flag risks but can't fix them.

Introducing SailPoint Autonomous Agents

When AI agents invoke MCP tool calls at machine speed, human review of every action is impossible. SailPoint announced [Autonomous Agents](#), a fleet of specialized AI agents built to govern and protect the agentic ecosystem. Unlike generic tools that simply shut agents down when anomalies occur, Autonomous Agents use identity context to tell legitimate intent from malicious activity, stopping threats while keeping productive agents running. These Autonomous Agents actively govern the agentic lifecycle: continuously monitoring runtime actions, intercepting threats, and right-sizing permissions to enforce zero standing privilege at machine speed.

Matt Mills, President of SailPoint, said:

"Autonomous agents are no longer just experimental copilots; they are becoming the primary execution layer of modern enterprises. Enterprises cannot afford to slow down AI innovation out of fear, nor can they afford ungoverned access chaos. Moving beyond Zero Trust to Autonomous Identity allows organizations to master the converged human-plus-AI workforce, eliminate invisible risk, and innovate with complete confidence."

Chandra Gnanasambandam, EVP of Product and Chief Technology Officer, said:

"The idea that a security admin is going to review and approve access for a group of autonomous agents making 10,000 tool calls a second isn't just outdated—it's a fantasy. The only way to govern autonomous machines is with autonomous machine defense. We've built Autonomous Agents so enterprises can stop the threat, save the good agents, and bring human and non-human identity into real-time. In a near-AGI world, standing privilege is dead."

Autonomous Identity Security Posture Management (A-ISPM) goes beyond the dashboard

Using the live identity context in SailPoint Atlas, [SailPoint's new A-ISPM](#) continuously detects dormant accounts, partially offboarded identities, orphaned access, shadow admins, and privileged outliers hidden deep in access paths. It then closes the loop on each organization's terms, with remediation ranging from one-click fixes, such as revoking access, disabling an identity or AI agent, or assigning an owner, to fully automated policy enforcement.

New automation and global compliance upgrades

SailPoint is advancing global identity security with powerful new updates across its platform. The company introduced new updates to the SailPoint Atlas engine with advanced automation workflows to help enterprises scale security, while also [launching IdentityIQ 9.0](#) to make everyday access governance simpler and more secure for business users. To support this growth, SailPoint is also expanding its global footprint—opening a new data center in South Korea and preparing to meet some of the strictest federal and financial compliance standards, including FedRAMP High, PCI DSS 4.0, and EU Sovereign Cloud.

Delivering four core customer outcomes through new innovations

SailPoint delivers autonomous identity and a host of customer benefits and improved security outcomes across its Identity Security platform. New product innovations showcased at Navigate enable customers to realize these four critical business outcomes:

- **Comprehensive discovery:** Security teams can't govern what they can't see. Every agent, credential, and data store that never reach the identity program becomes access no one owns. New endpoint and browser sensors, SIEM and XDR telemetry, and vault and pipeline NHI discovery bring MCP servers, tools, credentials, and data stores into view. [Data Access Security](#) adds classification integrations with Microsoft Purview and BigID, plus new connectors for Atlassian Confluence, Google BigQuery, and AWS Redshift.
- **Enabling compliance:** Auditors are asking how AI agents are governed, and most organizations can't yet produce the evidence. New [Agent Audit](#) turns agent inventory and governance activity into framework-aligned evidence reports that can be exported in one action, customized, or scheduled, making audit preparation repeatable.
- **Strengthening security posture:** Standing privilege is invisible risk. Every always-on account is an open door for attackers. [Just-in-Time provisioning \(JIT-P\)](#) grants access only when needed, with conditions such as business justification or reauthentication and activation through Slack or ServiceNow. Agentic Fabric delivers prompt monitoring with policy-based redaction and blocking and behavioral risk detection. Human Fabric features a [CrowdStrike Foundry App](#) and SecOps containment actions with a full audit trail.
- **Streamlining operations:** Governance has become too admin-heavy, and manual processes can't keep pace with the volume of human and agent access. Human Fabric will now offer next-generation access requests with an embedded [Harbor Pilot Access Request Agent](#). The upcoming Harbor Pilot Policy Agent lets administrators explain and draft access policies for people and agents in plain language, and Agentic Fabric provides one-click agent lifecycle controls and an agent kill switch.

Platform milestone: SailPoint Agentic Fabric + Entro integration

Also announced during Navigate, the Entro Security integration into SailPoint Agentic Fabric will soon be complete. The integration includes Entro-powered credential lineage, exposed secret discovery, and prompt-intent monitoring into Agentic Fabric, extending governance to secrets and credentials that AI agents and NHIs depend on.

Availability

Capabilities across SailPoint Agentic Fabric, SailPoint Human Fabric, and [SailPoint Atlas](#) are rolling out globally beginning at Navigate 2026. A-ISPM, the Harbor Pilot Policy Agent, and the Proofpoint integration are expected in Q4 FY27.

New Success Acceleration service packages combine expert-led roadmaps, vertical-specific deployment accelerators, AI-driven risk reduction, and continuous compliance support to help customers reach zero standing privilege and realize value faster.

To watch Navigate 2026 keynotes and product demonstrations live or on demand, visit www.sailpoint.com/navigate.

About SailPoint

SailPoint (Nasdaq: SAIL) is defining the new era of adaptive identity security. In a world where non-human identities now significantly outnumber humans, our AI-powered platform unifies identity, security, and data intelligence to protect today's enterprise from advanced identity-based threats. We deliver the identity solution that spans both the breadth of identities and the depth of context needed to drive real-time access with confidence. Built on principles like zero-standing privilege and contextualized risk, our SailPoint platform transforms identity from a point of vulnerability into a powerful security advantage. Trusted by many of the world's leading organizations, SailPoint secures the enterprise with intelligent, autonomous identity security.

Forward-Looking Statements

This press release may contain "forward-looking statements" within the meaning of the Private Securities Litigation Reform Act of 1995, including with respect to SailPoint's expectations regarding announcements made at Navigate. In some cases, you can identify forward-looking statements because they contain words such as "may," "will," "expects," "plans," "anticipates," "could," "would," "plan to," "intend to," "believe," or "goal" or the negative of these words or other similar terms or expressions that concern our expectations, strategy, plans or intentions. These forward-looking statements are not guarantees of future performance, but are based on management's current expectations, assumptions and beliefs concerning future developments and their potential effect on us, which are inherently subject to uncertainties, risks and changes in circumstances that are difficult to predict. Our expectations expressed or implied in these forward-looking statements may not turn out to be correct. The development, release, and timing of any features or functionality described for SailPoint's products that are not currently available remain at SailPoint's sole discretion on a when, and if available, basis, may not be delivered at all and should not be relied on in making a purchasing decision, and could be materially different from our expectations because of various risks.

Important factors, some of which are beyond our control, that could cause actual results to differ materially from our historical results or those expressed or implied by these forward-looking statements include the following: our ability to deepen our

relationships with existing customers; the growth in the market for identity security solutions; our ability to maintain successful relationships with each of our partners; our ability to compete successfully against current and future competitors; the increasing complexity of our operations; our ability to maintain and enhance our brand or reputation as an industry leader and innovator; unfavorable conditions in our industry or the global economy; our ability to successfully introduce, use, and integrate artificial intelligence (AI) with our solutions; breaches in our security, cyber attacks, or other cyber risks; interruptions, outages, or other disruptions affecting the delivery of our SaaS solution or any of the third-party cloud-based systems that we use in our operations; our ability to adapt and respond to rapidly changing technology, industry standards, regulations, or customer needs, requirements, or preferences; real or perceived errors, failures, or disruptions in our platform or solutions; and the ability of our platform and solutions to effectively interoperate with our customers' existing or future IT infrastructures.

More information on these risks and other potential factors that could affect our financial results is included in our reports and other documents filed with the Securities and Exchange Commission including in the "Risk Factors" and "Management's Discussion and Analysis of Financial Condition and Results of Operations" sections in our most recently filed Annual Report on Form 10-K and subsequent Quarterly Reports on Form 10-Q. Any forward-looking statement speaks only as of the date as of which such statement is made, and, except as required by law, we undertake no obligation to update or revise publicly any forward-looking statements, whether because of new information, future events, or otherwise.

The development, release, and timing of any features, functionality, capabilities, or services described for SailPoint's products that are not currently available remain at SailPoint's sole discretion on a when, and if, available basis and may not be delivered at all and must not be relied on in making a purchasing or investing decision.

Media relations for SailPoint

Shannon Paulk

Sr. Manager, Corporate Communications

303-748-2275

shannon.paulk@sailpoint.com