SailPoint

Leveraging activity data to maximize the potential of identity security

Risk reduction and robust applications across the identity security spectrum

Table of contents

Introduction 3

Fundamentals of activity data 4

A three-stage productivity model 4

- Stage #1: Display of data 5
- Stage #2: Introduction of thresholds and recommendations 5
- Stage #3: True AI-driven decision-making 5

Applying robust activity insights and AI integration to role management 6

- Use case #1: Streamlining Access Certifications 7
- Use case #2: Updating roles based on usage patterns 8

Behavioral analysis and activity monitoring 9

A more automated approach 10

SailPoint Activity Insights 11

- Features of Activity Insights 11

Conclusion: A more secure, dynamic future for enterprise 12

Introduction

Identity governance and administration (IGA) as a security discipline is a requirement in today's future-focused enterprise. Its stated aim is to efficiently manage user identities and access across the organization–including customers, partners, employees, and machines. The right solution improves visibility into identities and access privileges and helps identity security and broader IT teams implement the necessary controls to manage access, mitigate risk, and comply with regulations.

Until now, identity security has lacked the requisite comprehensive activity data to maximize the efficiency and effectiveness of security-focused processes. Current solutions only address components of the problem–namely, managing access. New features intended to address common issues require time and resources most teams do not have, hogging bandwidth while roles continue to go unoptimized.

In this paper, we highlight that existing methods address immediate issues but fail to provide longer-term, scalable solutions for identity security challenges, nor can they realize the full promise of Artificial Intelligence (AI).

Fundamentals of activity data

Despite customers struggling to stay afloat in the realm of identity security, the market continues to introduce new features intended to resolve customer issues. However, these innovations demand additional time and resources. Fundamental aspects like role optimization remain unaddressed, partly because customers are preoccupied with addressing immediate identity security crises, such as certification campaigns, segregation of duty (SOD) violations, and data access governance. While solutions such as certifications and access requests temporarily address immediate problems, they do not facilitate long-term, strategic handling of these issues.

Activity data refers to a collection of records related to specific actions, interactions, and behaviors of identities within an organization's IT ecosystem. It's precisely this data that will significantly aid in our broader decision-making processes, as well as allow us to imagine a future where concepts such as manual access requests, frequent certifications, and role updates become a relic of the past. Rapid advancements in AI technologies, plus the strategic integration of rich activity data sets, make this future not just possible but imminent. Activity Insights from SailPoint Identity Security Cloud makes this capability as real as it is powerful.

But we're not just talking about automating access requests. We're talking about leveraging data at the decision-maker and policy level to facilitate faster and more accurate decision-making processes across identity security. At SailPoint, we propose a thoughtful approach to robust activity data integration and AI automation.

A three-stage productivity model

We advocate for a graduated approach to enhancing productivity through activity data utilization encapsulated in a three-stage model:

Stage 1: Display of activity data model

Stage 2: Introduction of thresholds and recommendations

Stage 3: True AI-driven decision-making

Through this progressive three-stage approach, we envision a transformation in the landscape of identity governance. The synergy between human insight and identity security capabilities will foster a more secure, efficient, and intelligent access management ecosystem.

Stage 1: Display of activity data

It's crucial to present activity data early and directly to the decision-makers. By displaying activity data prior to processes or AI incorporating the data itself, you allow users to become more familiar with leveraging these metrics in their day-to-day activities while also enhancing the speed and accuracy of their current decisions. This also allows users to skip the time-consuming and often inaccurate step of soliciting individuals of activity-based information such as "Do you still use XYZ application?"

Although this stage of the model aids significantly in decision-making, stopping at this stage will still demand analytical thinking to determine how the data presented will impact decisions.

Stage 2: Introduction of thresholds and recommendations

Many of the decisions we make on a day-to-day basis could be automated based on policy-based decisions incorporating activity data. Allowing thresholds to be put in place and automated policy-based decision-making will allow most day-to-day decisions to be automated. Additionally, by leveraging activity data and past decision-making, we can provide decision-makers with recommendations on many decisions, whether during access request reviews, certifications, etc. Here is where we offer likely outcomes based on the analyzed data, diminishing the cognitive load on the decision-maker and streamlining the process. Again, completing this stage is helpful; the presence of edge cases, particularly in access management, necessitates a degree of verification and oversight. Recommendations and thresholds can only take identity security so far.

Stage 3: True AI-driven decision-making

Our model culminates in this third stage, where AI assumes *much of the* responsibility for decision-making based on human decisions and input. In an *ideal* scenario, automation would eliminate the need for human intervention but, a more realistic expectation is the elimination of the need to manually address up to **80%** of decisions, adhering to the Pareto principle.

This substantial reduction in manual decision-making not only enhances efficiency but it also allows identity access managers to focus their expertise on more complex, nuanced cases that AI may not yet fully comprehend beyond mere edge cases.

Applying robust activity insights and AI integration to role management

Integrating activity data through artificial intelligence harbors immense potential to enhance decision-making capabilities. While seemingly simple on the surface, thoughtful automation of applicable tasks plays a pivotal role in securely and efficiently managing digital identities. Integrating this productivity model into identity governance frameworks helps maintain robust security measures while promoting efficiency and flexibility–underscoring the importance of holistic identity governance automation.

Roles fundamentally serve as the foundation of an organization's access structure. You can think of this foundation as akin to allocating keys to specific floors and subsequent rooms in an office building. Ideally, upon the beginning of a new role within an organization, an individual should be granted access (keys) exclusively to the resources necessary for their immediate job responsibilities.

Unfortunately, organizations can deviate from this ideal. The prevailing approach to defining roles and assigning access rights is based on assumptions about the needs of a team, rather than empirical evidence of individual requirements. While this is the best approach we can take today, it is comparable to simply asking "Which keys should this new employee have for the building?" This method often leads to overprovisioning of access, undermining the principle of least privilege.

More concerning, new employees often inherit the access privileges of their predecessors who, over years of service, have accumulated access to a broad spectrum of resources–including some that have remained unused for extended periods. This scenario is analogous to being handed a master key without a clear understanding of which doors it opens

The risk here is two-fold:

1. **There's a lack of oversight on which access rights are essential for a user**
2. **Should this "key" fall into the wrong hands, a breach might go undetected due to the surplus of unused access rights**

This analogy highlights the critical philosophy behind role management: to ensure that each identity within an organization is equipped with the minimum necessary access to fulfill their current job responsibilities. As these responsibilities and day-to-day processes evolve, so should their access rights, in a manner that is both responsive and proportionate to changing landscapes. Currently, the absence of detailed activity data presents us with a significant challenge in this regard.

Some of the more straightforward use cases include streamlining access certifications for identities or dynamically updating roles based on usage patterns. Automating access certification and role management not only saves considerable time for those responsible for maintaining security protocols; automation of these capabilities also significantly enhances the whole organization's ability to adapt to changing access needs swiftly.

IGA question	Today's answer	Tomorrow's answer with activity insights
Should I add this entitlement to this role?	Well, the identities all have it, so yes	The entitlement is popular, but no one has used it in 90 days, so no
Does this person still need this access?	Well, their peers all have it, so yes	They haven't used this entitlement in 90 days, so no
Should I grant access to this entitlement for this identity?	Well, their peers all have it, so yes	Their peers do have access to this entitlement, but no one is using it, let me reach out and ask why

Use case #1: Streamlining access certifications

Access certifications are an essential security measure that ensures individuals only retain access to resources they genuinely require. In traditional setups, this involves access certifiers painstakingly reviewing every access privilege granted to an identity, confirming its necessity. Done by a human, this task sprawls into a thankless series of tedious tasks. The scope of access certification becomes apparent when one considers the staggering multitude of access points each individual in an organization might possess. By integrating robust activity data, we can significantly streamline this process.

For example, if an individual has not utilized a particular access right within a predetermined period (e.g. 90 or 180 days), the system can automatically revoke this privilege. Conversely, if access has been utilized within this timeframe, we can automatically validate the certification. This reduces the administrative burden on certifiers, promptly removes unnecessary access rights, and enhances the overall security posture. This improved agility is crucial in a digital landscape where access requirements can evolve rapidly.

Use case #2: Updating roles based on usage patterns

Leveraging AI's analytical prowess and activity data can also greatly assist with updating roles. By examining activity data over specific time intervals (again, e.g. 90 or 180 days), AI algorithms can adjust roles to reflect actual activity access patterns.

This process allows us to revoke seldom-used access rights and automatically–yet securely–incorporate access rights for roles that require them more frequently. This dynamic role management not only ensures that identities have access to the tools and information they need but also minimizes the risk associated with excessive privileges.

IGA question	Today's answer	Tomorrow's answer with activity insights
How can I update this role and its entitlements?	Well, the entitlement is still popular, so I can't make any changes	The usage of these entitlements has stopped so I should remove these, and these are new entitlements that are being used more often now which I'll add
Should I be concerned with this identity's access?	Well, I asked and they need the role just in case	They are using this source 5x more than anyone else, I should investigate that

Behavioral analysis and activity monitoring

Identity security concerns not only the allocation and revocation of access rights but the intricacies of how these rights are utilized. Current systems may adeptly monitor who accesses what, but they fail to interpret the nuances of whether such access aligns with actual need.

The fundamental concern isn't just who has access to what but who takes what actions with what access to what ends. Did the store manager appropriately remove money from the cash register for a bank deposit? Or did they simply take the money? Who has a key to the register doesn't matter nearly as much as whether you can trust that no one will steal its contents. This makes behavioral analysis a profoundly critical component of identity security. As it pertains to IGA, behavioral analysis discerns the intent and legitimacy of actions conducted within the scope of granted access. Effective behavioral analysis requires a dual understanding: recognizing the access and the appropriateness of the actions taken within the context of one's role. These insights seek to bridge a gap in traditional IGA frameworks, which cannot typically contextualize access utilization within the broader narrative of an individual's role and responsibilities.

Not all breaches are the result of sophisticated coordinated attacks or hacks from bad actors to gain access inside a system. The misuse of legitimately granted access rights can be all it takes to cause a breach. This means organizations remain vulnerable at all times, and effective behavioral analysis helps alleviate that vulnerability.

A more automated approach

To fully secure an organization's access, identity security requires a more sophisticated approach that goes beyond managing who should have what and focuses on the how. "How are identities using their access". Leveraging a sophisticated approach that employs behavioral intelligence and identity data to discern and mitigate potential threats–before they culminate in actual harm.

Imagine a system imbued with AI capabilities, designed to continuously monitor and analyze access and activity patterns against the backdrop of an individual's role. Upon detecting an initial deviation from expected behavior, the system would log the activity and initiate a cascading series of responses tailored to the deviation's severity.

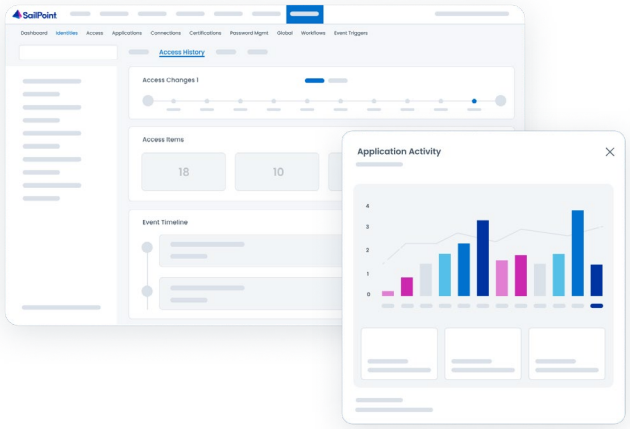
The envisioned AI-driven system would operate on a principle of progressive escalation, starting with internal notifications to direct supervisors for immediate review and acknowledgment. Should the unusual behavior persist, indicating a pattern rather than an isolated incident, the system would escalate its response, ultimately involving Information Security for a decisive evaluation. This could include temporary suspension of access rights pending a thorough investigation, thereby limiting the potential for damage.

An effective behavioral intelligence system can serve as a critical check against the unauthorized dissemination of sensitive information. Identifying and reacting to early signs of aberrant behavior enables organizations to proactively safeguard against threats–especially those incurred via properly granted access rights. Remember, it's not just what identities have which access–it's what those identities do with that access.

Behavioral analysis, leveraging identity and activity data, can help organizations check activity against the appropriateness of access for a predefined role. Leveraging AI to do this on a perpetual basis, flagging suspicious activity, and even dynamically adjusting roles and access to respond–all without the need for human involvement–helps further improve security posture. All these capabilities help close the current gaps in proactive behavior monitoring and appropriate security response. This approach also embeds a dynamic, adaptive layer within the access management framework, ensuring access rights are continually aligned with legitimate operational needs.

SailPoint Activity Insights

SailPoint Identity Security Cloud pulls in activity data in the form of events like user logins, password changes, and content updates within the application. You can view an identity's activity data within an application to discover trends for that user.



You can use this activity data to determine whether a user has used an application, calculate how often a user uses an application, and inform decision-making in certifications.

Features of Activity Insights

To get started, you'll set up the activity insights sources. After Identity Security Cloud has gathered account and activity data, you can then view activity insights in the following features:

- **Access History** - Users can view the number of times that identities logged in to an application and compare these numbers to the company's average.
- **Access Modeling** – Users can view the percentage of identities that engaged with an entitlement's source during the past 90 days. Selecting a specific identity displays their source activity to help users make more accurate role assignments.
- **Certifications** - Users can view the number of days an identity was active for 90 or 180 days. This information can be used to determine if an identity should retain access to an entitlement.
- **Access Request Reviews** – Approvers of an access request are provided with critical activity data, including access popularity and usage metrics at the source level to improve decision making

After setting up a connector, Activity Insights provides information about usage patterns and activity trends for SaaS applications and sources, including Atlassian Suite, Box, Dropbox, Duo, GitHub, Google, Salesforce, Slack, Workday, Zendesk, or Zoom. You can then view activity data in Identity Security Cloud.

Conclusion: A more secure, dynamic future for enterprises

Integrating robust activity data and artificial intelligence in Identity Governance & Administration marks a pivotal shift in enterprise security. As organizations face increasingly complex threats and regulatory landscapes, the need for dynamic, intelligent access management has never been greater.

These advancements not only improve an organization's security posture but also drive operational efficiencies, reducing the burden on identity, IT, and security teams. As identity security solutions evolve to incorporate these capabilities, organizations will be better equipped to enforce the principle of least privilege more effectively, respond swiftly to changing access needs, mitigate risks associated with over-privileged accounts, and ensure compliance with regulatory requirements.

The future of identity security lies in intelligent, data-driven solutions that can adapt to the dynamic nature of modern enterprises. By embracing these technologies, organizations can create a more secure, efficient, and responsive identity governance framework, better prepared to meet the challenges of an ever-evolving digital landscape.

About SailPoint

SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data through the lens of identity – at speed and scale. As a category leader, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency. SailPoint helps many of the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.

sailpoint.com

SP2460-2408