SailPoint Identity Outliers

Challenges

In today's highly interconnected digital world, organizations face increasing cybersecurity threats. Protecting sensitive data and essential business resources is now more critical than ever.

One of the critical challenges in ensuring robust identity security and governance is managing identities that have access to resources that are not normal or appear anomalous. These outliers may exhibit behavior that puts security at risk, such as unauthorized access to sensitive data or accounts with excessive permissions. The difficulty lies in identifying these outliers, making it taxing for traditional tools to detect anomalies effectively. SailPoint Identity Security Cloud delivers the ability to proactively identify these risks by leveraging machine learning and analytics to examine large datasets for patterns and deviations, ensuring that potential identity outliers are recognized early.

Another significant challenge is addressing the complexity of managing outliers without disrupting legitimate business operations. While it's critical to address potential security risks posed by outliers, organizations must balance this with ensuring that the right users have the access they need to perform their roles effectively. This challenge can be a nuanced process that requires continuous monitoring and the use of automation to quickly respond to potential threats without affecting productivity. By using identity analytics and automated decision-making in Identity Security Cloud, you can empower your organizations to implement a more proactive and intelligent approach to managing outliers, helping to ensure a secure and efficient environment.

Identity Outliers

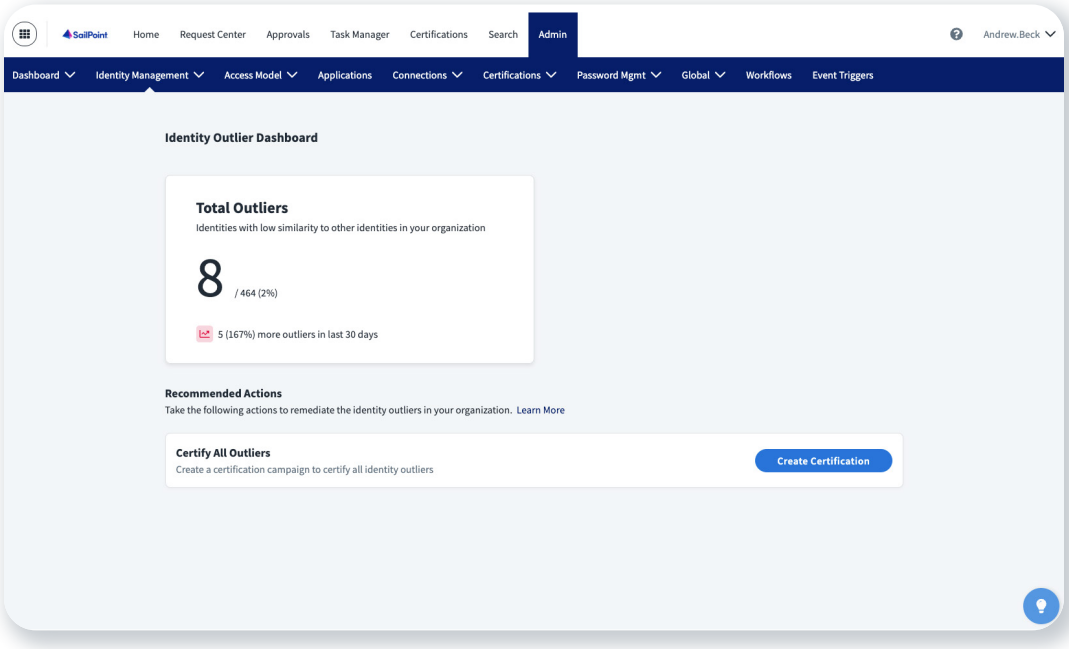
Outliers refer to the digital identities in an enterprise that exhibit abnormal access patterns. Outliers are identities that are not similar to peers and present patterns that deviate significantly outside the norm. Outliers can be an indicator of risky access or in some cases an indication of a set of unique roles or job function within the enterprise. Not all outliers are necessarily bad. An outlier could be an executive, a super admin or privileged user. The trick is being able to distinguish between risky outliers and legitimate users with elevated or unique privileges. Without technologies like AI and ML powering your identity security program, risky outliers can go undetected and at worst, wreak havoc to your IT infrastructure, critical resources and applications.

> **"We are using SailPoint's AI capabilities to identify outliers, users that have more access privileges than they should as compared to others. We're using it as a basis for cleaning up and auditing our access privileges and tightening our identity governance structure.**
>
> **Nickisha Bennett-Burton**
> Identity and Access Manager
> ECU Health

How it works

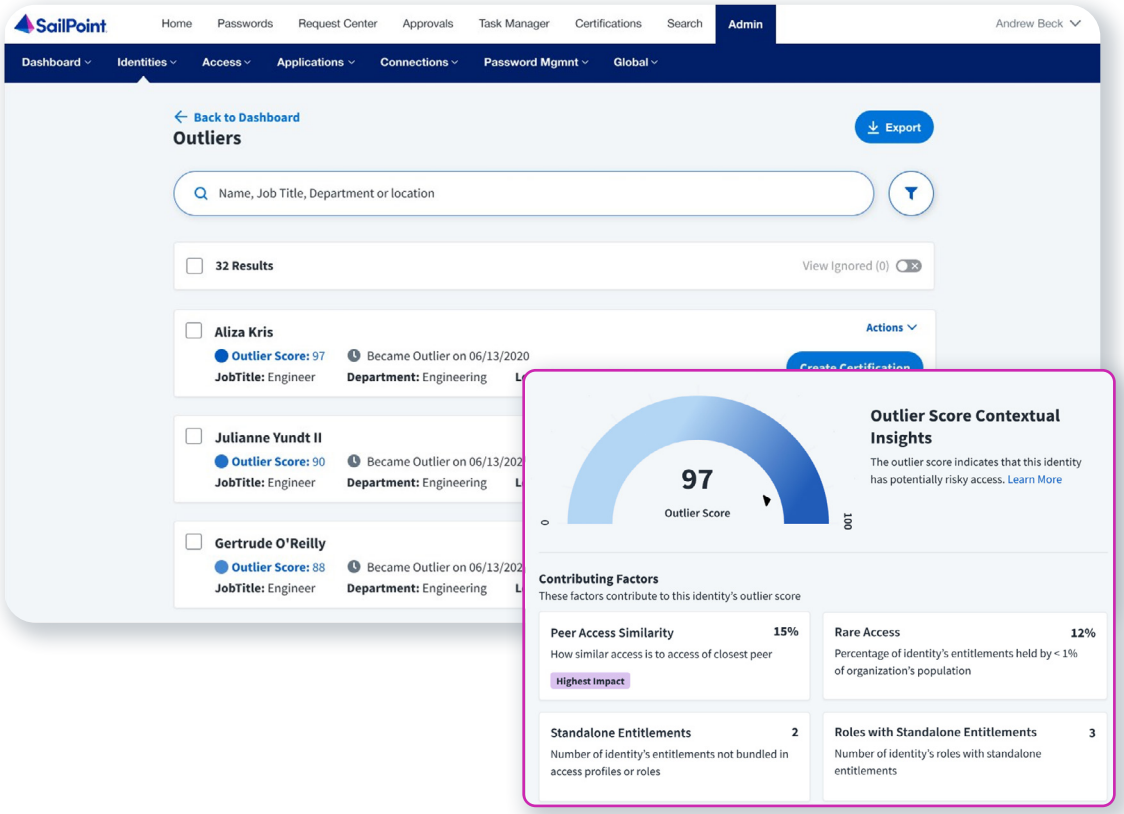
SailPoint identity outliers is a feature designed to enhance identity security by identifying anomalous or potentially risky behaviors within an organization's identity data. It leverages advanced machine learning to analyze an organization's identity access relationships and flags anomalous access for review and remediation. Outliers could display unusual access permissions or unexpected changes in roles or access levels. By automatically flagging these anomalies, outliers help identity teams quickly pinpoint potential security risks or compliance violations, enabling faster response and reducing the threat surface. This proactive approach helps organizations maintain stronger security postures while helping to ensure compliance with internal policies and regulatory standards.

Identity Security Cloud provides visibility into identity data and outliers in the form of a dashboard, showing trends and patterns and can help predict future risks. The anomalous identities are assigned a risk score to help normalize the measurement of access anomalies and risk across the enterprise. The outlier risk score can be given a threshold that if an outlier exceeds it, an automated workflow can be triggered to perform an appropriate, pre-set remediation, such as kicking off a micro-certification, or prompting further investigation. Conversely, the detection of an outlier can be ignored if upon investigation, a legitimate reason for unusual access is determined, providing context and improving decision-making.



With SailPoint Identity Security Cloud monitoring outliers, the solution has the additional benefit of helping to keep the access model updated. By monitoring outliers, identity security teams can gain valuable insights into abnormal patterns and deviations delivering the ability to remediate access and make access model adjustments to align with the needs of the business.

Outliers provide risk scores and contextual insights, including factors that influence scores, such as peer access similarity, identities with standalone entitlements, rare access- % of entitlements held by less than 1% of users, or roles with standalone entitlements.



Benefits

- Predict, monitor, detect and eliminate identity threats before they escalate
- Accelerate the discovery of potential risk like dormant or orphaned accounts
- Support audit accuracy and help prove compliance
- Identify and remediate your most unique, over-entitled, and risky users
- Reduce manual workload, streamline processes and deliver actionable insights
- Target the highest risk outliers first through direct remediation and focused micro-certifications for quick and efficient mitigation actions
- Improve the efficiency of your Identity Security program via customized dashboards
- Help maintain an optimized access model by evolving in response to changing user behaviors and organizational needs

Solution Brief
SailPoint Identity Outliers

Improve the effectiveness of your Identity Security program with Identity Outliers

AI and ML is quickly becoming a necessity in managing and operationalizing your identity security program. Leverage Identity Outliers in Identity Security Cloud to identify subtle patterns with speed and accuracy to deliver early detection of risky and anomalous access for swift and automated remediation for an improved security posture.

To learn more visit **www.sailpoint.com.**

SailPoint

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.