Underutilization and Misalignment of IAM Tools

In today's cybersecurity landscape, identity is the new perimeter. Organizations are increasingly relying on Identity and Access Management (IAM) tools to protect their digital assets. However, a common challenge persists: while IAM tools such as Multi-Factor Authentication (MFA) and Single Sign-On (SSO) offer robust security features, these capabilities are often underutilized.

Common Challenges

Security Gaps in MFA and SSO: Customers struggle to harden security gaps in MFA and SSO configurations using existing licensed capabilities, such as Conditional Access policies in Microsoft or Okta. Despite having these powerful tools at their disposal, many organizations fail to fully leverage their potential to enhance security.

IAM Tools Owned Outside Security Teams: IAM tools are frequently managed by teams outside the core security function, such as IT or the applications teams. The primary focus of these teams is to enable business operations – facilitating SSO, provisioning access to applications, and streamlining operational workflows. As a result, the rich security features these tools offer often go underutilized.

Indirect Ownership and Communication Barriers: The indirect ownership of IAM tools by non-security teams leads to significant communication barriers. Security teams face difficulties in articulating which features should be deployed, where to deploy them, and understanding the risk mitigation impact. This misalignment often results in only limited security capabilities being implemented within sign-on policies.

Limited Layering of Security Attributes: Without direct control over IAM tools, security teams struggle to layer in the rich security attributes necessary to mitigate risks effectively. This leads to a scenario where, despite having advanced IAM tools, organizations remain vulnerable due to suboptimal security configurations.

Solving the Challenge is within Reach

Reach transforms your security landscape by not only identifying gaps but also helping you effectively navigate the 'last mile' of cybersecurity. With a risk-based approach, Reach provides the context needed to optimize your IAM tooling to get the best security possible from the tools you already own.

Reach

Drive Outcomes with Reach

Make Risk-Based Decisions: Tailor sign-on policies and make full use of advanced IAM features, Reach significantly limits the potential damage in the event of credential compromise, effectively reducing the blast radius of breaches.

Take Confidence in IAM: Reach provides unmatched visibility into how IAM capabilities are being used, allowing security teams to monitor and manage their security posture proactively.

Manage Resources Strategically: With detailed analysis and reporting, Reach empowers teams to measure their utilization of licensed capabilities; to drive informed decisions on whether to consolidate or expand licensing based on quantifiable risk mitigation.

reach.security/connect
415.828.7475
sales@reach.security

Reach Capability	Description
Optimized Utilization of Licensed Capabilities 	Reach conducts a complete analysis of the IAM capabilities that an organization is licensed for and provides actionable recommendations to help justify consolidating or buying more. This includes distinguishing between basic and advanced capabilities, such as P1 vs. P2 in Microsoft's Entra ID, or standard vs. adaptive MFA and SSO in Okta, ensuring the full potential of investments is realized.
Tailored Sign-On Policies 	Reach uses a sophisticated algorithm to design the optimal combination of sign-on policies. It establishes robust baseline security for the entire company and crafts stringent, tailored policies for 'Most Attacked' groups. This includes advanced sign-on policies using risk/contextual-based attributes or custom configurations like geolocation-based enforcement.
One-Click Automation and Deployment Guides 	Reach streamlines the implementation of optimized policies through one-click automation and provides detailed deployment guides and configurators. This enables security teams to efficiently stage and apply changes directly back to the product, ensuring that recommendations are not only suggested but also executed with precision.

Use Reach with:

Microsoft Defender · proofpoint. · /\bnormal · Microsoft Entra ID · okta

Reach Security is revolutionizing the cybersecurity landscape by empowering organizations to maximize the ROI of their existing security products. With a focus on optimizing what organizations already own rather than adding complexity with new tools, Reach Security is committed to simplifying cybersecurity, reducing operational costs, and enhancing protection against evolving threats. Founded by cybersecurity experts with venture-backing from leading investors and cybersecurity luminaries, Reach Security is setting a new standard for cybersecurity efficiency and effectiveness. For more information, visit: **Reach.Security.**

Reach

Get Started!

To join the community of customers enjoying the benefits of Reach and learn more about how it can transform your security posture, visit:

Reach.Security/try-reach

reach.security/connect
415.828.7475
sales@reach.security