SAVVY

The Visibility Challenge: Uncovering Gaps in SSO and MFA

Whitepaper

The Year of Identity -Related Breaches

2024 underscored the critical importance of identity security, as even the most prepared organizations faced challenges with identity-related breaches. High-profile incidents demonstrated that while investments in IAM tools like Single Sign-On (SSO), Multi-Factor Authentication (MFA), and even Identity Governance and Administration (IGA) are helpful, they are not sufficient to address today's challenges. These tools' inherent technology limitations mean that blind spots can still emerge, and attackers are adept at finding and exploiting their gaps. The challenge isn't a failure of these solutions; it's a call to enhance visibility and close gaps that these tools weren't designed to address.

SSO and MFA in the Spotlight:

Breaches That Made Headlines

Snowflake Data Breach via EPAM Systems (2024):

Hackers compromised an EPAM Systems employee's credentials, which were stored without encryption, to access Snowflake accounts lacking MFA. This breach affected clients like Ticketmaster, Santander, and Lending Tree, leading to the theft of financial and personal data. The incident highlighted the risks of inadequate MFA enforcement and poor credential management.

Okta Authentication Bypass (2024):

A vulnerability in Okta's authentication system allowed users to log in without a password if the username exceeded 52 characters. This flaw, present from July to October 2024, was particularly exploitable in environments where MFA was not enforced, underscoring the importance of robust authentication mechanisms.

Change Healthcare (2023):

Attackers exploited a vulnerability in a key application that did not have MFA enabled. The breach exposed sensitive patient data and highlighted the consequences of failing to enforce MFA on critical systems. This incident underscored the necessity of comprehensive MFA implementation across all applications, not just select ones.

MGM Resorts Breach (2024):

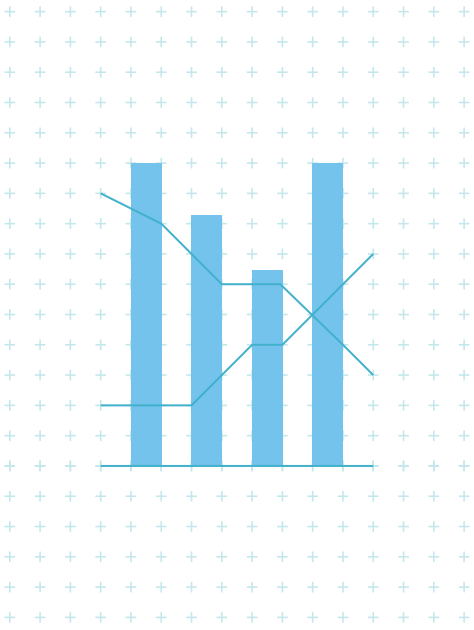
Hackers used social engineering to bypass MFA by impersonating an employee and exploiting weaknesses in the account recovery process, which did not require MFA. This led to unauthorized access to systems and significant operational disruptions, highlighting the need for comprehensive MFA implementation beyond just login processes.

Uber Breach via MFA Fatigue Attack (2022):

In a high-profile attack, a hacker used an MFA fatigue tactic to bombard an employee with push notifications until they approved a fraudulent request. This allowed the attacker to bypass Uber's MFA protection and gain access to internal systems. The breach exposed sensitive employee and customer data and disrupted operations, emphasizing the need for user education and advanced MFA mechanisms resistant to social engineering.

These incidents demonstrate that while SSO and MFA are critical components of identity security, their misconfiguration or improper enforcement can lead to significant vulnerabilities. Organizations must ensure these tools are correctly implemented, regularly audited, and supplemented with user guidance to effectively mitigate risks.

The Hidden Flaws:
What You Need to Know About SSO and MFA Gaps



While SSO and MFA are touted as essential pillars of modern identity security, their implementation often falls short of full coverage. SSO adoption is surprisingly limited, leaving many corporate applications outside the safety net. Meanwhile, local accounts and misconfigurations in MFA create vulnerabilities that attackers eagerly exploit.

These gaps are not just theoretical; they're directly linked to some of the most common identity-related breaches. For organizations relying on these tools without fully understanding their limitations, the risks are significant—and growing.

To understand the magnitude of these issues, let's explore key statistics and trends that paint a troubling picture of the current state of identity security:

SSO Adoption Gaps

- Only **35% of corporate applications** are fully onboarded to SSO. (Gartner, 2024)
- The average enterprise uses **1,295 cloud services**, yet fewer than 30% are integrated with centralized IAM tools. (McAfee, 2023)

MFA Adoption Gaps

- Only **26% of organizations** enforce MFA across all their users and applications. (Cisco, 2024)
- **80% of data breaches** stem from weak or stolen credentials, despite MFA being a widely recommended countermeasure. (Verizon DBIR, 2024)

Visibility Issues

- **63% of IT leaders** cite "lack of visibility into app configurations" as a top barrier to fully enforcing SSO. (Okta State of IAM Report, 2024)
- **90% of security incidents** involving SaaS apps are due to misconfigurations, such as SSO or MFA not being enforced. (CSA SaaS Security Survey, 2024)

Specific Risks Highlighted

Local Accounts

- **15%-20% of SaaS applications** allow local accounts to remain active even when SSO is configured, creating a bypass route for attackers. (CyberArk, 2023)
- Local accounts were involved in **40% of identity-based breaches** in 2023 due to weak passwords and lack of MFA. (IBM Cost of a Data Breach Report, 2024)

App-to-App Integration Risks

- **25% of SaaS breaches** exploit app-to-app tokens or API integrations that lack proper authentication safeguards. (Forrester, 2023)
- Only **12% of organizations** actively monitor app-to-app connections for security risks. (CSA SaaS Security Report, 2024)

Push Notification Spamming (MFA Fatigue)

- MFA fatigue attacks account for **18% of MFA bypass incidents**, with **65% of users** unaware of how to handle repeated fraudulent push notifications. (Microsoft Security, 2023)

Additional Notable Trends

Shadow IT's Role

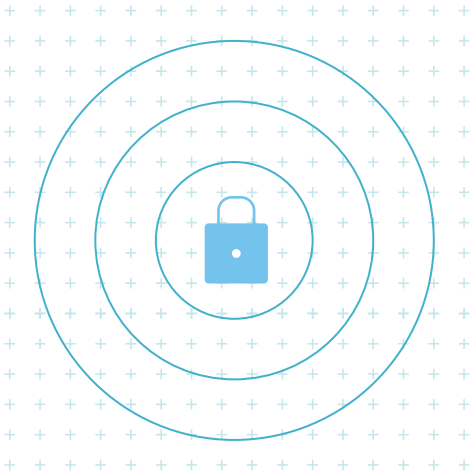
Shadow IT accounts for **30%-50% of SaaS** apps in use at any given organization, often completely bypassing SSO and MFA configurations. (McKinsey, 2024)

On average, **72% of SaaS apps** accessed by employees are unsanctioned by IT, leaving significant security gaps. (Varonis, 2024)

Compliance and Regulatory Risks

45% of enterprises failed compliance audits in 2023 due to poor SSO enforcement and MFA misconfigurations. (ISACA, 2024)

GDPR penalties increased by **42%** in 2024, with identity mismanagement cited as a major contributing factor. (European Data Protection Board, 2024)



Industry-Specific Data

Healthcare

73% of healthcare organizations experience SSO or MFA gaps due to reliance on legacy systems. (HIMSS, 2024)

Healthcare breaches cost **$10.93M per incident** on average, with identity misconfigurations cited as a root cause in **65% of cases**. (IBM Cost of a Data Breach, 2024)

Financial Services

Financial institutions face a **2.5x higher risk** of SSO bypass attacks compared to other industries due to the extensive use of legacy systems. (PwC, 2024)

54% of financial institutions struggle to enforce MFA across all critical systems due to complex app ecosystems. (ISACA, 2024)

Additional Insights

Automation Challenges: Automating the onboarding of apps to SSO is difficult for **62% of organizations**, leading to critical apps being missed. (Forrester, 2024)

Credential Sprawl: On average, employees manage **191 passwords** across work and personal accounts, increasing the likelihood of reused or weak credentials. (Dashlane, 2023)

Role of AI: 39% of attackers now use AI to exploit misconfigurations in IAM tools, including bypassing SSO and MFA. (Cybersecurity Ventures, 2024)

These insights make it clear that while SSO and MFA are essential components of identity security, their effectiveness depends on addressing visibility gaps, properly configuring tools, and mitigating risks associated with local accounts, shadow IT, and app integrations.

The Reality of SSO and MFA

SSO Origins

Single Sign-On (SSO) was designed to streamline access management, enabling users to authenticate once and gain access to multiple apps. This approach reduces password fatigue and enhances user convenience. However, centralizing access under a single set of credentials also creates a single point of failure. If an attacker compromises those credentials, they can gain access to all connected systems.

MFA Origins

Multi-Factor Authentication (MFA) emerged as a solution to bolster access security. By requiring users to verify their identity through multiple factors, such as a password and a mobile device, MFA adds a layer of protection against unauthorized access. Despite its effectiveness, poor implementation or user behavior can undermine its benefits, leaving organizations vulnerable.

Why SSO and MFA Are Commonly Linked

SSO and MFA are often paired to create a balance between convenience and security. SSO streamlines the user experience by reducing the need to manage multiple credentials, making it easier for employees to access the tools they need without sacrificing productivity. Meanwhile, MFA strengthens the security of centralized access by requiring an additional layer of verification, such as a one-time passcode or biometric authentication. Together, they form a powerful combination that enhances both usability and protection, at least in theory.

The effectiveness of this pairing, however, hinges on consistent enforcement and robust monitoring, two areas where many organizations fall short. A significant risk arises from not being able to determine whether SSO and MFA are being used as intended. Are all critical applications onboarded to SSO? Are users bypassing SSO and logging in directly to apps, effectively nullifying MFA enforcement? Without clear answers to these questions, organizations are left with blind spots that attackers can exploit.

Consider the scenario where users bypass SSO to log in directly to SaaS applications. In this case, MFA configurations tied to SSO are no longer applied, leaving these apps exposed to attacks that could have been prevented. Similarly, apps that aren't onboarded to SSO or platform-wide account-based MFA leave significant vulnerabilities, as attackers can target these entry points with credential-based attacks. These gaps are rarely visible through traditional IAM tools, making it difficult for organizations to detect and address them in real time.

The inability to verify whether these tools are being properly used is more than technical oversight which is a critical risk. Without continuous validation of SSO adoption and MFA enforcement, organizations cannot trust that their IAM strategies are functioning as intended. This lack of assurance undermines the very security these tools are designed to provide, turning them into unguarded doors rather than fortified entry points.

To truly benefit from SSO and MFA, organizations must have the visibility to monitor their usage and the enforcement mechanisms to ensure compliance. Without these capabilities, even the most advanced IAM solutions are rendered incomplete, leaving organizations vulnerable to preventable breaches.

Why SSO and MFA Gaps Happen

Legacy Systems and Shadow IT

Many organizations still rely on legacy systems that were not designed to integrate with modern IAM tools. This disconnect creates vulnerabilities where SSO and MFA cannot be enforced. The #1 reason is the presence of local accounts that remain enabled, even in apps integrated with SSO. These accounts bypass SSO and MFA security controls entirely, creating significant vulnerabilities. Additionally:

SSO is enforced at the application level, and implementations vary widely.

In over 15% of apps, local accounts remain active, bypassing centralized SSO and MFA controls.

SSO can only manage what it can see, leading to critical visibility gaps.

Organizations face challenges onboarding every application:

Approximately 35% of corporate apps are onboarded to SSO.

An average of 180 sensitive apps operate outside SSO.

Partner apps, social apps, and SSO tax apps are major contributors to this gap.

Compounding these issues is the rise of shadow IT—unsanctioned applications adopted by employees without IT approval. These apps often bypass security protocols entirely, introducing unmanaged risks.

Dormant and Orphaned Accounts

A major challenge in identity management is handling accounts that outlive their intended use. Dormant accounts, left active after employees depart, and orphaned accounts, tied to individuals who no longer have ties to the organization, are prime targets for attackers. These accounts often retain access to sensitive systems, providing an easy entry point for breaches.

Human Behavior

Even the most robust IAM tools cannot compensate for poor user behavior. Credential reuse, weak passwords, and MFA fatigue—where users approve fraudulent requests without scrutiny—all contribute to the erosion of identity security. Attackers exploit these human vulnerabilities to bypass otherwise strong defenses.

App-to-App Connections

Modern SaaS environments rely heavily on app-to-app integrations for data sharing and workflow automation. While these connections enhance productivity, they also create hidden vulnerabilities. If one app in the chain is compromised, attackers can exploit the connection to access others, often without triggering traditional IAM defenses.

SSO and MFA: Hidden Vulnerabilities

1. SSO Bypass and Local Accounts

Many SaaS applications allow local accounts to remain active even after SSO is configured. These accounts often bypass MFA policies tied to SSO, creating hidden backdoors for attackers.

Solution:

Organizations need continuous visibility into app configurations to detect and disable local accounts promptly.

2. MFA Misconfigurations and MFA Fatigue

Inadequate MFA policies—such as inconsistent enforcement across users and apps—expose critical assets. Meanwhile, MFA fatigue attacks exploit user behavior, where users unknowingly approve fraudulent push notifications.

Solution:

Behavioral monitoring and policies to detect and block suspicious login attempts can mitigate these risks.

3. App-to-App Risks

API tokens and app-to-app integrations, often overlooked in IAM strategies, are increasingly exploited by attackers. These connections may lack proper authentication or monitoring, enabling attackers to move laterally within the network once initial access is gained.

Solution:

Regular audits and security controls for app-to-app integrations are essential to prevent exploitation.

4. Shadow IT and Incomplete SSO Integration

Shadow IT represents one of the largest blind spots for SSO and MFA enforcement. On average, 72% of SaaS apps used by employees are unsanctioned by IT, meaning they completely bypass IAM controls.

Solution:

Automated discovery and onboarding processes are critical to ensure security policies cover the entire SaaS ecosystem.

The Truth About Identity Gaps

Industry Insights from Savvy Research

Savvy's research, derived from deep engagement with customers and in-depth Proof of Value (POV) assessments, highlights pervasive and alarming trends in how organizations implement and manage SSO and MFA. By analyzing real-world environments, we've uncovered critical gaps that challenge the perceived effectiveness of these essential tools.

A widespread misconception is that SSO automatically enforces MFA for all apps. However, the reality is far different. Many users bypass SSO altogether, logging directly into SaaS apps where MFA configurations are not enforced, leaving these applications exposed. The visibility problem compounds this issue. **Only 35% of corporate apps are onboarded to SSO, leaving a majority of the application landscape unprotected. Even among onboarded apps, SSO is bypassed 15% of the time—an average of over 50 apps per organization.**

MFA enforcement fares no better. **For apps outside SSO, MFA is rarely applied, creating additional vulnerabilities. This lack of consistent enforcement results in widespread credential hygiene issues, with 70% of users violating best practices, such as reusing weak passwords or failing to update credentials**. Moreover, 100% of organizations in our assessments had hundreds of sensitive, **dormant app-to-app integrations that remained unmonitored and vulnerable.**

The consequences of these gaps are stark and unavoidable. These findings underscore a chilling reality: **organizations are often just one password away from a breach that could cascade across multiple apps**. Addressing these risks requires more than just implementing IAM tools—it demands visibility, enforcement, and continuous validation to ensure these investments are being used as intended and delivering on their promise.

The Consequences of SSO and MFA Gaps

Operational Impact

When SSO and MFA gaps are exploited, the immediate operational impact can be severe. Breaches disrupt workflows, delay critical projects, and force IT teams to divert resources toward containment and remediation. This additional strain compounds existing pressures on overburdened IT departments.

Financial Fallout

The financial repercussions of identity-related breaches are staggering. Organizations face legal fees, regulatory fines, and lost revenue, not to mention the cost of post-breach recovery efforts. For many businesses, these expenses can be crippling.

Security Gaps

Attackers exploit the blind spots created by SSO and MFA gaps, using overlooked apps, hygiene violations, and dormant integrations to infiltrate systems. These gaps represent a failure to secure the very identities that IAM tools are meant to protect.

Operational Costs

The operational cost includes hours spent identifying, isolating, and resolving vulnerabilities, as well as potential overtime pay for IT staff and lost productivity across the organization. These hidden costs often escalate quickly, adding to the overall burden of managing identity-related breaches.

Reputational Damage

A breach not only compromises sensitive data but also erodes customer trust. High-profile incidents can tarnish a company's reputation for years, resulting in long-term damage to brand credibility and customer loyalty.

The Distance from a Breach

Without visibility and enforcement, organizations remain dangerously close to a breach. When SSO and MFA are circumvented, the path to unauthorized access becomes alarmingly short.

Close SSO and MFA Gaps with a 3-Part Framework

Step 1: Gain Visibility

To address identity risks, organizations must first achieve comprehensive visibility. This means identifying all apps and identities in use, including shadow IT and orphaned accounts. Browser-level insights provide a detailed view of app usage, identities, and app-to-app connections, enabling organizations to uncover hidden vulnerabilities.

Step 2: Understand the Risks

Visibility is only the first step. Organizations need actionable intelligence to prioritize remediation efforts. This involves identifying the most toxic accounts, such as those with SSO bypass risks, MFA misconfigurations, and poor credential hygiene. By focusing on the greatest risks, organizations can allocate resources more effectively.

Step 3: Take Action

Once risks are understood, swift action is required. Automated playbooks can streamline the process of fixing credential hygiene issues, enforcing MFA policies, and securing app-to-app integrations. Real-time guidance ensures that users remediate compromised credentials and follow best practices for identity security.

The Savvy Advantage

Savvy's approach addresses the visibility problem head-on. By providing x-ray level insights into identity risks, Savvy enables organizations to uncover and close gaps in their IAM landscape. Real-time remediation workflows ensure that MFA is consistently enforced and SSO is used as intended, while continuous monitoring simplifies compliance and strengthens overall identity hygiene. With Savvy, organizations can proactively defend against breaches by addressing vulnerabilities before they escalate.

The Stakes Are High

Every organization is one password away from a breach—or a solution.

Identity gaps are a ticking time bomb. Reactive measures are no longer sufficient to protect against increasingly sophisticated attacks.

To secure their IAM environment, organizations must prioritize visibility, intelligence, and actionability. By addressing SSO bypass and MFA gaps, they can build a resilient defense against identity-related threats.

Don't wait for a breach to expose your vulnerabilities.

How secure is your identity perimeter?

SAVVY

Attackers don't break in—they log in.
Are your identity controls actually protecting you, or are hidden risks leaving your organization exposed?

Find out in seconds with our Identity Risk Score tool. To get a real-time assessment,

visit https://risk.savvy.security/