A New Mandate for IAM with Multifactor Authentication

SPONSORED BY:

Cyberbreaches aren't just in the news—they are the news. Yet headlines rarely mention the No. 1 source of those breaches: weak or stolen passwords. Whether they involve malware, hacking, phishing, or social engineering, the vast majority of breaches begin with account compromise and credential theft, followed by dormant lateral network movement and data exfiltration. In fact, weak or stolen passwords account for a staggering 81% of breaches, according to the Verizon 2017 Data Breach Investigations Report.

Not surprisingly, a new Okta-sponsored IDG survey finds that identity access management (IAM) is a top priority for nearly three-quarters (74%) of IT and security leaders. Yet the same survey uncovers widespread concern that their current IAM implementations are falling short. Just one worrisome example: Fewer than one-third (30%) of respondents report a good or better ability to detect a compromise of credentials.

The following report explores the gap between respondents' aspirations for IAM and current capabilities, the risk factors that most worry them, and how they plan to respond over the next 12 months.

New Mandate—but Lots of Work to Do

The Okta/IDG survey leaves little doubt that there is a growing mandate for IAM with multifactor authentication. An overwhelming majority (74%) consider it either a high or critical priority in their cyberdefense strategy. Remarkably, that number rises to 92% among leaders with a title of VP or higher.

However, most respondents say their current IAM solutions fall well short of their ideals, whether in preventing breaches or responding quickly and effectively when they do occur. For example:

- Fewer than one-third (30%) report a good or better ability to detect a compromise of credentials.
- Only 36% report a good or better ability to detect the sources of compromises.
- Only 41% report a good or better ability to provide the kind of meaningful IAM data about breaches to security operations to drive effective and holistic threat visibility.

The good news is, respondents aren't sitting idly by. Within the next 12 months, nearly half (46%) will either plan for or deploy new IAM solutions with multifactor authentication, or replace existing solutions.

Assessing Gaps and Risk Factors

However, it is vital to understand specific challenges before taking action. The Okta/IDG survey finds three key areas where, according to respondents, current IAM solutions are stretched to the breaking point.

❶ Sprawling attack surfaces.

As the number and type of users, devices, and app environments multiply, so do the potential attack surfaces respondents must secure.

- **Expanding access to users outside the enterprise.** From customers to consultants, credentialed access is constantly expanding, with each user or user type requiring a discrete set of access rights. Managing this expanding user base is a top concern for 59% of respondents.
- **App environment sprawl.** As organizations increasingly adopt both cloud-based and on-premises apps, 61% of respondents are concerned about managing identity across disparate app environments.
- **Security sprawl.** As companies implement disparate security solutions, integration between security and IAM solutions grows more complex. And this makes it hard to achieve holistic threat visibility—a top challenge for 35% of respondents. For 29%, shadow IT is also top concern, since it creates new security use cases to manage.
- **Device sprawl.** Every new device extends the potential attack surface, and 33% say managing access across devices (laptops, tablets, mobile, etc.) is a top challenge.

❷ Poor password hygiene driven by poor usability.

When users find it hard to log in—whether because processes are slow or involve multiple passwords—they tend to find risk-prone work-arounds. As a result, inconvenient authentication controls are a top concern for 43% of respondents. Inconvenient processes and worrisome practices, such as credential sharing and the use and reuse of passwords across work and personal boundaries, are top concerns of 33% and 29% of respondents, respectively.

Beyond systems that promote noncompliant behavior, 18% also consider weak credentials and/or access requirements a top concern. In addition, 29% worry about time-consuming credential provisioning and deprovisioning—and the associated risk of orphan accounts from deactivated users vulnerable to outsider threats.

❸ Current IAM solutions failing to meet evolving threats.

Bad actors are constantly evolving new tactics, making it vital to detect compromises, and prevent and/or limit damage when they do occur. To do so effectively requires the sharing of meaningful IAM data with security operations to better meet both current and evolving threats.

Yet many respondents fear their IAM solutions just aren't keeping up. For example:

- Only 41% report a good or better ability to feed information about breaches back into the security operations center.
- 35% are not satisfied with their ability to collect and report on user access information and patterns.
- 16% are concerned they cannot respond with new IAM policies quickly or at scale as risks evolve.

Fighting Back with IAM and Multifactor Authentication

As this assessment of gaps and risks reminds us, a few things are certain. The number of credentialed users and devices will expand. Systems requiring safeguarding will grow more complex. And risks will evolve right along with security technologies.

Since bad actors will exploit the narrowest of opportunities, how do you ensure that your IAM implementation effectively addresses all these gaps and risk factors? Look for solutions that are:

- **Simple enough to scale quickly, while massively shrinking attack surfaces.** An IAM solution should integrate easily with third-party cloud apps, VPNs, and hybrid security technologies. Only in this way can you can scale while maintaining accurate, systematic entitlement across systems—including rapid provisioning and deprovisioning.
- **Easy enough to encourage adoption and compliance.** A single, integrated, easy-to-use solution eliminates multiple passwords, driving down credential sharing, reuse of personal passwords, and other noncompliant user behavior.
- **Strong enough to defend against today's threats.** With adaptive, risk-based multifactor authentication, you can maintain a simple user experience while adding vital new layers of defense to ensure the right person accesses the right information at the right time.
- **Intelligent enough to stay a step ahead tomorrow's threats.** Look for a solution that gathers comprehensive access data and shares meaningful IAM data to other security solutions and security operations generally. This enables you to drive more secure risk-based multifactor authentication, detect abnormal activity faster, and improve both real-time responses and long-term defense strategies.

When 81% of breaches depend on weak or stolen passwords, IAM with multifactor authentication isn't merely an option—it's a must. If IT managers implement an integrated and intelligent solution that can rapidly scale to their own evolving operations, they stand a fighting chance.

To learn more, visit **Okta's site**