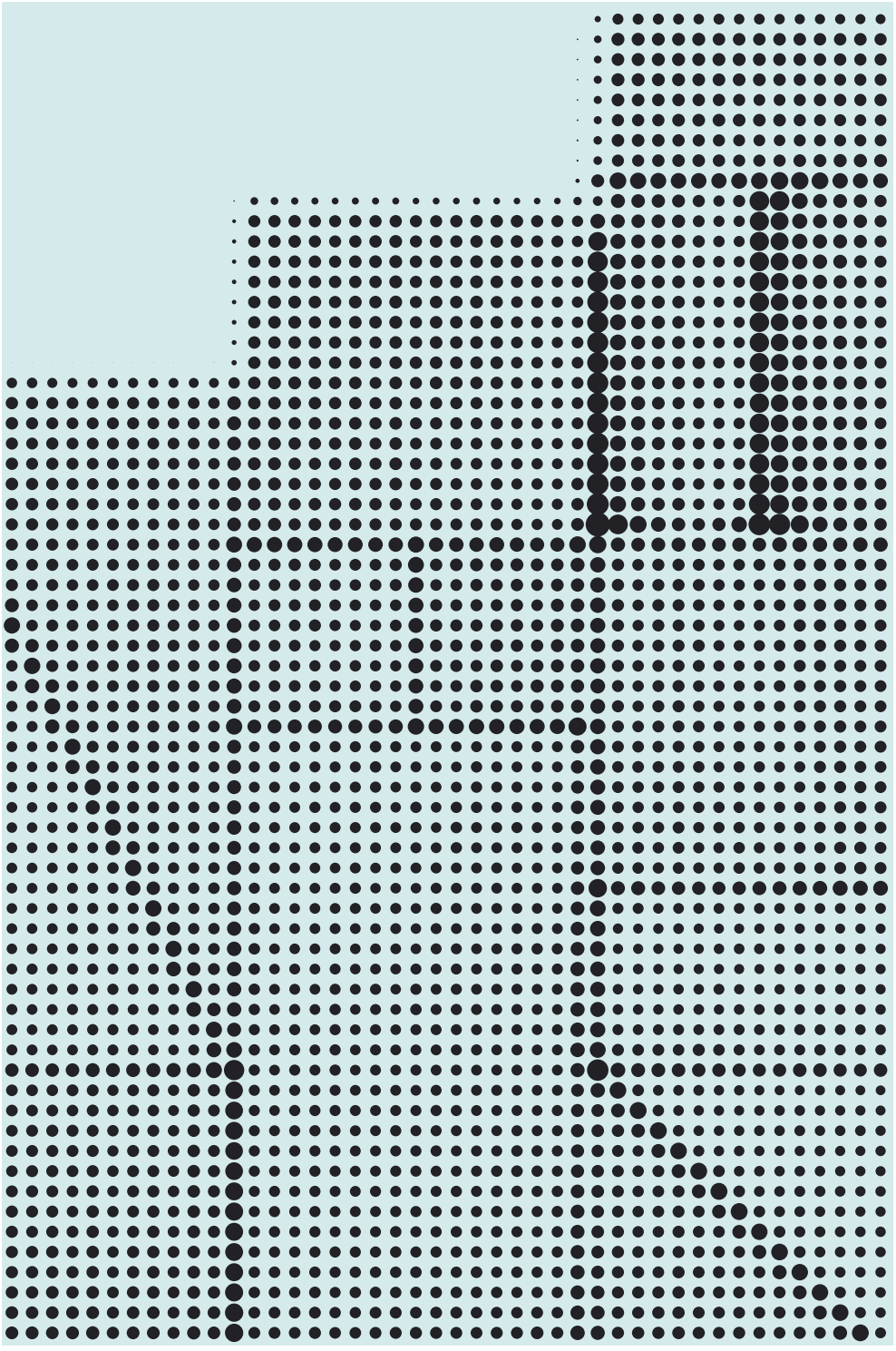
Whitepaper

June 2021

5 Reasons You Should Start with Identity to Protect Against Account Takeover

Okta Inc.
100 First Street
San Francisco, CA 94105
info@okta.com
1-888-722-7871



okta

Introduction

For employees, contractors, and consumers, a new era of digital business has begun. The lasting shift into remote work means more and more business is being done on personal devices—from the comfort of home, coworking spaces, or the local coffee shop. Eighty percent of company leaders plan to allow remote work at least part of the time for the long term, and 47% are enabling permanent work from home environments.

Alongside the rise in remote work, there's been a staggering rise in security threats, in particular account takeover (ATO) attacks, increasing at an alarming **282% between Q2 2019 and Q2 2020**. This is a trend we've continued to observe in 2021. An ATO can impact anyone who has online accounts, login credentials, and access to infrastructure or applications—and today, that's nearly everyone.

But, what is an ATO attack, and how does it work?

ATO occurs when a bad actor illegally accesses a user's account and steals the "stored values" in this account—including personal information, financial information, and any credit the user has with a business. When these cybercriminals have infiltrated the account, they can do major damage, such as posting spam or moving laterally through the organization to target other systems and data.

Typically, fraudsters stake their success on the tendency for users to choose weak passwords, opening themselves up to brute force attacks such as credential stuffing and password spray. This also allows them to attempt ATO attacks at scale using automated bots. However, these attacks can also be human-driven, and begin with a data breach or phishing attack that steals a legitimate user's login credentials.

In a global survey by IDG, commissioned by Okta, 80% of IT, security, and developer leaders say that weak passwords, phishing attempts, and credential sharing have impacted their security posture, with four in ten saying that it has greatly affected it. That comes as no surprise, considering even minor incidents can threaten monetary loss, increased chargebacks, regulatory fines, and reputation loss.

Many organizations see the looming threat that ATO attacks pose to their business, but they don't understand the most important place to start to prevent these attacks: **identity security**.

Identity is the foundation of good security

Identity is not only critical for security—it is security. With strong authentication, centralized user management, and automated provisioning and deprovisioning, identity minimizes the attack surface available to threat actors. It also provides the insight and analytics admins need to recognize risks and compromises immediately, and respond accordingly.

There are many challenges that make ATO attacks possible: the number of apps and services users rely on have proliferated, as have the passwords that protect them. This is combined with a lack of centralized visibility and control over which users have access to certain resources, creating vulnerabilities in an organization. In the past, it was assumed that only critical apps needed harder access policies; cyber criminals have long since disproved that, making their way to important data and intellectual priority after breaching a single weak point.

At present, the majority of enterprises have limited experience in detecting and preventing ATO-related incidents, managing user-flows for logins, and restoring compromised accounts, and that's largely because identity has not been a core focus of their security stack. Prioritizing a comprehensive identity solution can reduce the risk of an ATO attack for many reasons. Here are five of them.

#1. Identity enables passwordless authentication

Passwords are a known issue, causing a lot of problems for enterprises and their end users. Employees and customers constantly forget them, creating an unsustainable burden for IT and a headache for everyone. But the inconvenience for users and admins is nothing compared to the risks to the business.

On average, a credential stuffing attack targets **1,041 accounts**, making it increasingly likely that organizations that rely on passwords will suffer a breach. In 2019, Akamai recorded a credential stuffing attack that resulted in over 55 million malicious login attempts against a single US financial institution. And it's not just weak or stolen passwords that are the issue; hackers can take advantage of password and account reset flows, as well as insecure reset channels and social engineering, to seize access to accounts.

By eliminating passwords from the authentication experience, credential attacks such as password spraying, credential stuffing, and man-in-the-middle attacks can be prevented, curtailing attempted ATO. For many enterprises, passwords have been the default login method for so long, the thought of passwordless authentication seems unfathomable.

Yet, it's surprisingly simple. Passwords can be replaced with more secure authentication practices such as email credential links, factor sequencing, or enabling biometric-based logins through WebAuthn, the latest web standard published by

the World Wide Web Consortium (W3C), allowing admins to deliver seamless biometric authentications.

It's important to take a standards-driven approach to authentication that's backward compatible with roaming authenticators. That's why a comprehensive approach to identity is so critical to modern security, and company leaders are catching on.

#2. Identity enforces second factor authentication for users to validate identity

One of the simplest ways to reduce the risk of an account takeover is to enforce a second authentication factor so that access doesn't depend exclusively on passwords, even if users still have them. A bad actor who manages to steal a username and password will be stopped by something like a mobile one-time password (OTP)—or even better, physical OTP tokens and push notifications are the aforementioned biometrics.

It's for this reason that multi-factor authentication (MFA) is becoming a standard practice for many enterprises. But despite the fact that it's an easy way to prevent ATO attacks, deploying MFA comes with its own challenges. Organizations often have custom-built solutions and that may be hosted on-premises, with legacy infrastructure that's complex to manage and costly to maintain. This can make it onerous to deploy and adopt, presenting obstacles on the path towards robust security.

That's why using a modern, cloud-based MFA solution is necessary to ensure security that is reliable and scalable. An adaptive MFA solution will further improve an organization's security posture with context awareness, taking into account whether a particular user is typically associated with a specific device, network, or location, and proactively flagging unusual activity.

#3. Identity allows for increased verification based on the context of the user

IT and security admins may question whether context-aware adaptive MFA may become more of a hindrance than a help. After all, distributed workforces are requesting access to business applications from outside the network perimeter, often using personal devices or public networks. Stepping up authentication in all of these cases could prove burdensome and reduce productivity.

But the truth is, adaptive MFA enables them to succeed. With a context-aware approach, admins can set granular policies around the situations when users will be prompted for secondary factors, and what levels of access they will be granted. So, when a cyber criminal tries to take over a user's account, adaptive MFA policies will come into play to evaluate whether the login request is coming from a recognized network, location, or device. Any noticeable changes will prompt an additional factor—like biometric authentication—that the bad actor does not have access to.

Not only does this simplify IT workflows and user experience by reducing the challenge of passwords and the cumbersome reset flows that accompany them, it also supports employee, partner, contractor, and customer ecosystems that are constantly in flux.

#4. Identity increases visibility and insight to help identify suspicious behavior

With end users sharing or recycling credentials across multiple sites, it's no wonder that credential stuffing attacks—whether conducted manually or automated with bots—are of particular concern for security professionals. This is why it's so important for them to be able to detect both typical and atypical behavior patterns. There's a strong possibility that these could indicate bots or bad actors hitting end-points as they attempt ATO fraud.

This is yet another instance where the most powerful defence is identity. The best solutions on the market include robust analytics that monitor and recognize high risk login patterns, such as authentication volume and failure rate using ML, to stop credential stuffing attacks. They also take into account high-risk regions, and can implement effective IP and network zone restrictions.

In the best-case scenario, third-party identity partners also have threat detection teams dedicated to watching for anomalous activity across its customer and application networks, adding another layer of security. With these protective measures in place, organizations benefit from a reduced attack time, since they can spot and block fraud attempts earlier across the organization.

#5. Centralized identity management means accounts are accounted for

Organizations have invested far too much in several point security solutions that do not solve the core problems related to ATO attacks. As a result, costs are high, ROI is low, and fraud attempts are still happening. However, by focusing on authentication and authorization, and intelligently monitoring login activity, identity succeeds where traditional security solutions have failed.

A unified identity solution lets admins manage users and credentials at scale, while providing security logs to understand the end-to-end authentication journey. This ensures they have the insights necessary to inform all their identity decisions, and all their previously disjointed point security solutions become part of a strategic, coordinated, and in-depth defense.

Centralized identity blocks out the noise from third party point solutions so that admins can focus on what matters. In this manner, they can aggregate and unify inputs from the solutions that are still relevant, and retire the solutions that are no longer effective for today's integrated, cloud-first environments. Identity provides a holistic approach that eliminates blindspots and enhances the overall security posture.

Start with identity to prevent ATO security threats

Account takeover attacks happen when identity is compromised. Organizations can proactively work to stop these threats (and restore trust in those accounts) by ensuring that's exactly where they start—with identity security.

In the new perimeter-less network, identity is the building block to a modern security strategy. This includes:

- Strong authentication
- Centralizing identity for ease of management and elimination of passwords when possible
- Reduce attack surface for threat actors through proper user management
- Providing data towards holistic security visibility and enabling response in the event of a compromise

Ideally, there should be one best-in-class platform to manage the entire identity lifecycle, from registration and onboarding, to sign-on and beyond. This allows IT and security teams to keep track of unique user and device identities across the organization, along with their credentials, behaviors, contexts, sessions, and application actions, so that they can take an informed and proactive approach to preventing ATO attacks.

The scalability, reliability, and agility of a cloud identity solution should be a priority, along with the ability to connect the entire technology stack from cloud to ground; that way, you can ensure robust security that's always on across the organization. Furthermore, an independent identity provider helps prevent vendor lock-in to any particulate infrastructure or application stack.

Finally, there are specific features to look for to strengthen the security posture and mitigate the threat posed by fraudulent actors. Risk-based authentication and behavioral authentication solutions give admins greater control over granting the right users the right level of access to the right resources in the right circumstances. Centralized credential management and risk APIs also allow security teams to stay ahead of potential threats, rather than responding to them after. Lastly, a wide range of integrations is crucial, so that the identity platform can serve as a single nexus for all the security applications an organization relies on.

The risks of account takeover attacks may be on the rise, but the tools to guard against them are readily available. It starts with the understanding that today, identity is no longer separate from security. Data breaches begin at the login screen when criminals get their hands on compromised credentials. In a world of decentralized workforces, passwordless authentication, context-aware MFA, effective user management, and comprehensive visibility are the best defense.

Learn about how Okta can help you build security with identity by reading **our customer stories.**

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 7,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 10,000 organizations, including JetBlue, Nordstrom, Slack, Teach for America, and Twilio, trust Okta to help protect the identities of their workforces and customers. For more information, go to https://okta.com