Protecting Against Data Breaches

Identity is the critical missing piece in the fight against breaches

Executive Summary

We have entered an era where massive data breaches are a regular occurrence. Not surprisingly, protecting against breaches has become a top priority for modern businesses. Breaches continue to occur in spite of our best efforts; increased spending, long hours and constant vigilance. The fight is made harder due to escalating technological and landscape realities.

But there is hope. While specifics vary from breach to breach, nearly every incident can be traced back to a common cause—compromised credentials. Identity is the common thread that links those credential compromises together.

By taking control of identity, we can turn the tide in the battle against data breaches by centralizing and hardening access, reducing the attack surface and improving our ability to react faster to emerging threats.

The Challenge: Compromised Credentials

Looking across high profile data breaches in the industry, it becomes clear that compromised credentials is the root cause in nearly every one. As an industry, we have found that users, long touted as the weakest link in the security value chain, struggle to practice good password hygiene.

Research supports this:

- **81%** of breaches involve stolen or weak credentials[1]
- **91%** of attacks target credentials[2]
- **73%** of passwords are duplicates[3]

Despite best industry efforts towards education, users continue to deploy and use weak credentials. Part of this is due to a fundamental flaw in passwords themselves. We expect users to use long and complex passwords, but tell them not to reuse them across 30 or 40 different services or to write them down.

This request is unreasonable and well beyond reasonable limits on the human brain. Tools like password managers offer some relief, but in practice are not used nearly often enough and are at times misconfigured and misused.

It is no surprise that credential harvesting presents a lucrative opportunity to an increasingly sophisticated set of threat actors.

Stolen and recycled passwords continue to pose an important security issue

Poor access control management leaves people with access to everything

Authentication strategies haven’t evolved in 15+ years

To make matters worse, sensitive data resides in far more places than it used to. Cloud services like Office 365, Salesforce.com and Box provide incredible agility and business value to modern organizations. But they also increase the attack surface exponentially. And since password duplication and reuse is so common, an adversary only needs to compromise the credential once—often in the softest target—to use it everywhere.

Even looking inside organizational firewalls, users often have access to far more than they should. With the rapid rate of onboarding, attrition and change in today’s climate, it is just too hard to keep pace.

For better or worse, “default allow” becomes the path of least resistance, and can keep the business running smoothly and ticket queue low. But the convenience comes at a steep cost, allowing for attack propagation and access to high value information through more easily compromised accounts.

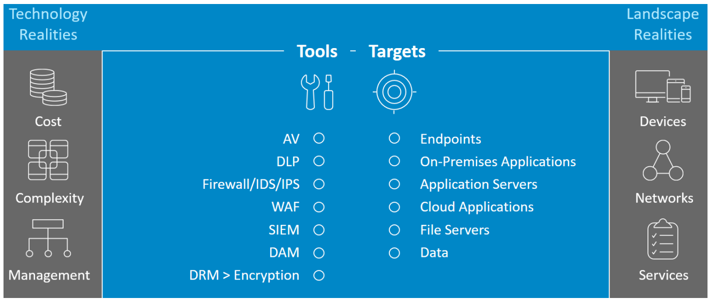
Yesterday’s Tools vs. Tomorrow’s Threats

As access control requirements have gotten far more complex, many approaches to access management have not kept pace. As a result, businesses often rely on manual approaches—error prone checklists, manual onboarding and change management processes and expecting the unreasonable from our users.

Due to fragmentation and proliferation of services, each with unique access requirements and credentials specifications, we often fail to take advantage of improvements. Multi-factor authentication provides

[1] 2017 Verizon Data Breach Investigations Report
[2] 2016 Verizon Data Breach Investigations Report
[3] TeleSign 2016 Consumer Account Security Report

additional protection, yet is implemented far less often than it should. And password reuse is far more common than it should be, mostly because users are not using tools like password managers.



Our defenses are squeezed between technological and landscape realities

But the fundamental problem is that much of today's security infrastructure, while necessary, is not sufficient in the fight against breaches. Management consoles like SIEMs are often overloaded with noise from firewalls, intrusion detection and prevention systems, anti-virus solutions trying to monitor an exponentially increasing number of attack vectors and services.

In addition, a number of technological and landscape realities impede our ability to get value from our investments.

- Technological realities include the cost, complexity and oversight requirements of our modern technology stack. Budgets are stretched thin, and expertise is in short supply. It is difficult to hire enough skilled resources to manage it all.
- Landscape realities include the proliferation of devices, networks and cloud services. People require more connectivity and access to more information than ever. The attack service is just too big to keep up with.

But there is hope. Across all of these challenges and realities, the common thread is identity. If we can take control of identity, we can turn the tides against data breaches.

Controlling Identity: The Missing Link

Identity is the missing piece. In order to be successful in turning the tides, a modern identity strategy needs to do four key things:

1. Extend governance across the entire attack surface—from cloud to mobile to on-premise
2. Prevent insider threats and safeguard against all forms of account compromise
3. Reduce silos to improve identity assurance
4. Improve security posture by working with the rest of the technological environment

By centralizing identity and access control by single sign-on, a large amount of human error is taken out of the attack surface. Less reliance on users remembering passwords mean better authentication practices and less chance for compromise.

Strong authentication is difficult to manage in a manual environment, but once an organization has taken control of identity it becomes far easier. Organizations can ensure that strong authentication is the default, and that all services require it. This makes it far more difficult to compromise accounts and credentials.

Automated provisioning and deprovisioning reduces the attack surface by making it far easier to follow the principle of least privilege. This ensures that users do not have more access than they need to, and makes it harder for the adversary to reach additional high value targets when they do compromise an account.

Finally, a strong identity strategy enables faster visibility and response to credential compromises and account takeovers. Through integrations, security teams get more value from existing investments, and are empowered to react faster and better contain a breach in progress.

Why Okta?

Okta's modern approach to identity management is uniquely positioned to help businesses take control of identity to reduce breaches across the four pillars of value.

1 Centralize identify and access control via single sign-on

2 Ensure strong authentication across all services, everywhere

3 Reduce your attack surface through automated provisioning and deprovisioning

4 Enable visibility and response to credential compromise and account takeover attacks

Centralizing identity

- Reduces account management complexity
- Unifies access for users to eliminate passwords while simplifying access
- Mitigates risk and reduce identity sprawl by restricting access to services via intelligent SAML connections

Enabling strong authentication everywhere

- Helps enable multi-factor authentication (MFA) "everywhere" quickly and easily with 5,000 out of the box connections on the Okta application network
- Helps extend coverage to on-premises applications via support for RADIUS, RDP, ADFS and LDAP
- Facilitates intelligent, contextual access decisions based on device and connection attributes

Reducing the attack surface

- Automated provisioning and deprovisioning accelerates consistent onboarding, while eliminating orphan accounts
- Extensible for custom applications via SCIM, SDK and Okta's API
- Complete lifecycle management ensures the right level of access to the right applications with access request workflows

Enable rapid response to compromise

- Centralized view into all authentication data across cloud, mobile and on-premises applications
- Identify unusual and suspicious behaviors
- Enrich and enhance your cybersecurity ecosystem investments via Okta's System Log API, including: Splunk, ArcSight, IBM QRadar, Palo Alto Networks, F5 Networks and more

Roadmap to Identity Success

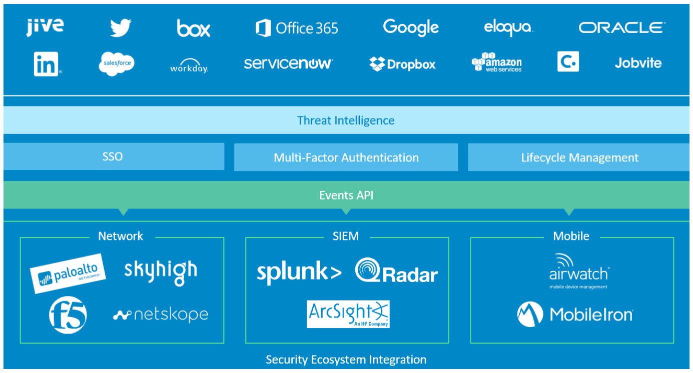
To recap, a modern, automated approach to identity helps take control of credentials to drastically reduce the risk of a data breach. Where should organizations start?

We recommend you focus on these key milestones:

1. Eliminate passwords wherever possible
2. Enable strong, unique passwords everywhere else
3. Harden critical applications with step-up authentication
4. Apply unifies policy to on-premises, cloud, and mobile applications
5. Automate provisioning with accurate entitlements
6. Deprovision at scale, and enable visibility and reporting
7. Roll out centralized, real-time reporting for all authentication events
8. Integrate your identity management strategy with existing security tools

We are Here to Help

Okta provides an end-to-end suite for modern identity management. We connect with complex service infrastructures, enrich context by providing threat intelligence to deploy single sign-on, multi-factor authentication and automate lifecycle management. We do all of that by working with your existing security infrastructure to provide value.



The Okta Identity Cloud Security Platform

About Okta

Okta is the foundation for secure connections between people and technology. Our IT products uniquely use identity information to grant people access to applications on any device at any time, while still enforcing strong security protections. Our platform securely connects companies to their customers and partners. Today, thousands of organizations trust Okta to help them fulfill their missions as quickly as possible.