okta

# Checklist:

## 12 Key Steps for Protection Against Data Breaches

**Okta Inc.**
301 Brannan Street, Suite 300
San Francisco, CA 94107

**info@okta.com**
**1-888-722-7871**

# Checklist: 12 Key Steps for Protection Against Data Breaches

Today, organizations face the challenge of protecting data in more places including the cloud, mobile, emerging platforms, and legacy on-premises applications. At an increasing volume and velocity, protecting this data is not easy. Compounding this challenge is the fact that organizations of all sizes, and in all industries, are being hit with data breaches. In fact, Ponemon reports the average total cost of a data breach rose from $3.62 to $3.86M, an increase of 6.4 percent.

While you're fortifying your defenses, it's vital to realize that many of these data breaches are identity-based attacks; in fact, 81% of data breaches involve stolen/weak credentials, according to the 2017 Verizon Data Breach Investigations Report. Now is the time to take proactive steps to combat data breaches, and ensure that the steps you are taking are protecting against one of the primary threat vectors.

We developed this checklist to provide strategic and tactical tips that can help you protect against one of the top causes of data breaches—identity-based attacks.

## Centralize Identity

Organizations have thousands of applications—each with an account and password. Managing so many accounts and passwords is a growing challenge. Many of your employees use the same, and often weak, passwords with multiple accounts. The top 10 most used passwords include Password123, and Football. This increases the chances of threat actors gaining access (often to multiple accounts) by guessing or stealing credentials.

- ❑ Centralize your accounts and access with single sign-on.
  This provides ease of management for both users and administrators.
- ❑ Consider eliminating passwords where possible. This helps reduce risks due to password weakness.
- ❑ Enable strong, unique passwords everywhere else.
  This reduces risks from identity-based attacks like credential stuffing and password spraying.

## Implement Strong Authentication

Even if you have strong passwords, they can still be phished and stolen. Strong authentication helps harden and fortify access to your organization's most important asset: data.

- ❑ Harden authentication everywhere you can. This prevents an attacker from gaining access with a stolen identity and using privilege escalation to target other accounts in the network.
- ❑ Implement Multi Factor Authentication (MFA) across all applications. Using MFA helps prevent unauthorized access—even if credentials are stolen.
- ❑ Enable a MFA solution with adaptive capability. This technology can help make intelligent, contextual access decisions based on a variety of attributes like user, device, and location context. Overall, this increases usability by reducing end-user burden and maintains high security standards so users are prompted for step-up authentication only when necessary.

## Reduce Attack Surface Area

Users leaving your organization can result in "zombie" accounts (unused accounts that have not been deprovisioned), which can leave open attack surface areas. Your enterprise may also have many users/employees changing roles, which can accidentally result in excess privileges. For example, an employee who moves from Payroll to HR may still have access to sensitive W2 information—leaving that person's account open as an opportunity for attackers.

- ❑ Automate provisioning and deprovisioning when possible. When you automate the onboarding and off-boarding process, you don't have to remember to update roles/permissions or deactivate accounts.
- ❑ Enable reporting so you can see who and what groups have access to which applications. This can help provide visibility and is also helpful for auditing purposes.
- ❑ Periodically review user group access to applications. It's important to make sure the right people have the right level of access for their role.

## Enable Visibility and Agile Response

While you may not be able to cover all security gaps, you can be proactive in tightening your security grid as much as possible. Increasing your visibility and control helps create a complete picture of security within your organization, enabling quicker security response times.

- ❑ Use identity data to augment visibility. This can help you determine who was impacted by a breach and what applications or accounts were accessed, and helps you get more out of your existing security investments. For example, if you're getting several failed authentications from a specific IP address, this can be flagged for investigation.
- ❑ Correlate identity data with other security logs and data for more complete picture. For example, correlation with network logs can show how and where an attacker moved within the network.
- ❑ Enable faster response with identity. For example, identity and access management solutions can prompt for step-up authentication, or even remove user access to applications in case of suspicious events or incidents.

## Time to Check Off All the Boxes

The proliferation of data breaches and credential-based attacks is quickly ushering in a new age of security—but most organizations haven't caught up yet. Historically, security solutions had to be complex for users and admins to be complex for hackers, and this is where a lot of organizations are stuck. It's now possible to have intelligent security solutions that are user- and admin-friendly. Okta delivers security solutions that are simple and intelligent that include Adaptive MFA, Single Sign-On, and Lifecycle Management. These solutions secure access to applications on-premises and in the cloud. Okta enables organizations fulfill their missions by making it safe and easy to use the technologies they need to do their most significant work.

For more information about how Okta can help keep your organization secure, visit our Protect Against Data Breaches page.