ManageEngine
AD360

# 3 Major identity security failures of the last decade.

www.manageengine.com/active-directory-360

# Introduction

Digital transformation has made today's organizations more flexible and efficient, enabling employees to work from anywhere, any time, using any device they own. With this development, traditional methods of protecting on-premises IT networks are no longer sufficient to safeguard users' identities. Employees, vendors, partners, and other stakeholders must be given access to an organization's network only after verifying their identity—and they should have access only to the resources they need.

Traditional authentication methods for verifying users' identities include passwords, hardware tokens, smart cards, and more. However, with today's complex IT environments facing heightened levels of security threats, organizations require capabilities like biometric verification, machine learning (ML) techniques, contextual authentication, and other security measures to protect their users' identities. Further, in today's workplaces, employees use numerous applications daily, and tend to use a single, easy-to-remember password to access all of them. If an attacker gets hold of this password, they can gain access to the applications, too.

Understanding every user's behavior within a network, i.e., who is accessing what information, at what time, from which location, and using what device, is essential for network security. Organizations should have advanced analytics capabilities to learn the normal behavior of every user, and trigger alarms upon detecting anomalous behavior for timely threat detection and response.

To achieve this, organizations must adopt a strong identity and access management (IAM) framework that helps prevent privilege escalation and unauthorized access to sensitive applications, comply with IT regulatory mandates, conduct in-depth security audits and forensics, and much more. In this e-book, we'll discover how a few organizations with some of the strongest cybersecurity systems fell prey to devastating data breaches due to poor IAM practices.

# Three cases of poor IAM

**Deloitte,** one of the "big four" accountancy firms in the world, fell prey to a cybersecurity attack in 2017. As one of the largest consultancy firms in the US, the company provided cybersecurity advice to powerful government agencies, financial institutions, and multinational companies, and had access to a large amount of sensitive financial and personal data.

With a revenue of $37 billion in 2017, Deloitte had all the resources it needed to implement a robust security system. However, all it took the hackers to bypass it was a simple password breach. So, how did the hackers do it?

The hackers breached Deloitte's global email server via an administrator account. This admin account had unrestricted access to the entire network, and was only guarded by a single password. By failing to implement multi-factor authentication (MFA), an important IAM best practice, Deloitte left the account wide open for hackers to exploit it. According to reports[1], the hackers had access to Deloitte's systems for about six months, from emails to a range of sensitive information including passwords, business architectural diagrams, IP addresses, and more.

Ironically, Deloitte was ranked number one in cybersecurity consulting for five years in a row by Gartner before the incident.

**eBay,** a popular online shopping platform, suffered a breach in 2014. Between late February and early March of that year, hackers compromised the login credentials of a small number of eBay employees, and gained entry into its corporate network.

The hackers were successfully able to siphon gigabytes of data, including encrypted passwords and personal information, and remained undetected inside eBay's corporate network for over seven months. Though the stolen passwords were encrypted, eBay advised its 145 million active customers to change their passwords as a precautionary measure.

Despite no financial information being exposed in the data breach, the information the attackers obtained could potentially create much bigger problems. With the names, email addresses, phone numbers, dates of birth, and registered addresses of 145 million people, attackers could devise numerous attacks like spear phishing, social engineering, and more.

**Home Depot**, the largest home improvement retailer in the US, was a victim of a major data breach in 2014. Initially, it was reported that the breach affected 56 million credit card holders, but it was later revealed that the scope of the breach included 53 million emails as well. So, how did such a huge data breach happen?

Home Depot's network was initially breached due to a compromised third-party vendor's account, which could have been avoided using MFA. The hacked account then had its privileges escalated and custom-built malware was injected into the system, all without arousing any suspicion. On top of all this, the data was siphoned out of the system effortlessly under the radar. Without the capability to capture event information and perform analytics and reporting, Home Depot was unable to spot this malicious activity in time to stop it.

Home Depot reported that the data breach would cost an estimated $62 million. Later, the costs were found to be much higher, and included a lawsuit it settled for $25 million two years later.

# How AD360 helps implement **IAM best practices**

AD360 is an identity governance and administration solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. From user provisioning, self-service password management, and Active Directory (AD) change monitoring to single sign-on (SSO) for enterprise applications, AD360 helps perform all IAM tasks with a simple, easy-to-use interface.

AD360 provides all these functionalities for Windows AD, Exchange Servers, and Office 365 platforms. With AD360, you can choose the modules you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments from a single console.

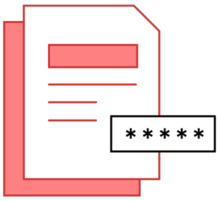
## 1 Automating provisioning and deprovisioning access privileges

Set access privileges automatically for new employees based on their business roles, and implement approval-based workflow for even more reliability. Automatically revoke the access privileges of terminated employees to eliminate the possibility of human error.

With AD360, you can configure automations that simplify routine user provisioning and deprovisioning tasks. Simply provide a list of users, and AD360 will help create user accounts and add them to appropriate groups, provision Office 365 licenses, and more during account creation.

2

## Creating and enforcing complex password policies



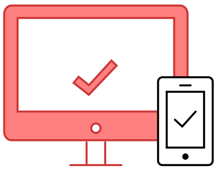
Prevent employees from using weak passwords by enforcing policies that increase password complexity. Passwords with a healthy mix of special characters, numbers, and letters are difficult for hackers to brute-force and crack.

AD360's Password Policy Enforcer enables you to enforce custom password policies to strengthen your organization's cybersecurity. Different policies can be enforced for different users with various privileges, such as C-suite executives, IT admins, and non-IT staff. To enhance password complexity, AD360 enables you to:

- Prevent palindromes, dictionary words, etc. from being used as passwords.
- Ensure that users don't use compromised passwords during password change and reset operations by leveraging the tool's integration with the Have I Been Pwned API service.
- Set organizational unit (OU) and group-specific password policies, with the flexibility to set stringent policies for privileged users.
- Prevent patterns such as consecutive characters from an old password or username, repetition of a character twice in a row, consecutive numbers in a row, and more.

3

## Enabling multi-factor authentication



MFA adds an additional layer of security, making it difficult for hackers to take over an account even if they crack the password. These additional layers can be anything from fingerprints to SMS-based verification codes and push notifications. Enterprises can protect single sign-on (SSO) with these trusted MFA methods to enable employees to securely authenticate in multiple applications.

AD360's MFA capability adds a second factor to authenticate users on their Windows, Linux, or macOS machines. It provides MFA during SSO for over 100 applications, and you can also configure any Security Assertion Markup Language (SAML)-based custom application for SSO. With this feature, users can securely access all their enterprise applications from a single dashboard.

## 4 Controls on privileged accounts

With access to critical resources and data within a network, privileged accounts are usually prime targets for hackers. Organizations should accurately inventory their privileged accounts and their access rights, and also keep track of those accounts' activities. By implementing user behavior analytics (UBA), organizations can quickly detect and proactively thwart anomalous activities performed by privileged accounts.

With its ML-driven UBA, AD360 creates a baseline behavior specific to each user to accurately detect any anomalies and insider threats.

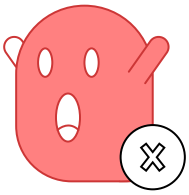
## 5 Auditing user activities

It's important to keep track of the who, when, what, and where of logons and logon failures, privileged accesses, changes to privileged access, etc. Organizations are expected to document these details in order to prove their adherence to regulatory audits.

AD360 provides comprehensive audit trails detailing which users had access to which resources, and what was done to those resources. It provides out-of-the-box, audit-ready report templates for SOX, HIPAA, GLBA, the GDPR, PCI DSS, and FISMA. You can also schedule customized audit reports to be generated and sent to your email.

6

## Identifying and removing ghost or unmanaged accounts



Inactive accounts, especially of senior-level employees who leave the organization, can cause unauthorized access to critical resources like financial documents or intellectual property. Hackers often perform reconnaissance on social media and other sources to find senior employees who've moved out of organizations, and target these accounts to remain undetected long after gaining entry to the organization.

AD360 empowers you to schedule automations to identify and remove inactive accounts at specified intervals. You can also set up a review-approve workflow to verify the inactive account cleanup process.