ManageEngine
AD360

Identity is the new security perimeter

here's how to protect it

Table of contents

Shifting the focus from traditional security perimeters to identity as a security parameter

Back when organizations were using only on-premises software, all their applications and data were stored and accessed within the confines of their corporate firewall. Organizations therefore focused only on firewalls to protect their networks from external intrusions. With the advent of cloud computing, software as a service (SaaS), mobile devices, and more, organizations have started using applications and storing data outside their corporate networks. These resources are accessed not only by employees, but also partners, vendors, etc. from anywhere, at any time, using multiple devices. This has made the old model of security based on firewalls, network security, and virtual private networks (VPNs) less effective in stopping current security threats.

As the digital identity of a user determines their access to an organization's network and data, identity has become the new perimeter protecting that network, meaning organizations should focus on strongly safeguarding their identities. This can be achieved through an identity-centric security approach using an efficient and granular identity and access management (IAM) solution, which can help organizations control how users access data and applications.

Some key aspects of the IAM process are identification, authentication, and authorization. To gain access to an organization's resources, users first provide their login credentials. Authentication then happens through passwords or multiple factors if multi-factor authentication (MFA) is deployed. Once users are successfully authenticated, the authorization process checks whether they have the required privileges to access the resources.The IAM process should also include regular verification and revision of the list of active users and their access privileges.

Remember, even if you have implemented network and perimeter security solutions, without IAM you may as well be leaving the key to your IT environment in the door for attackers to take advantage of.

The price companies pay for poor identity and access management

A 2019 Data Breach Investigation Report by Verizon[1] reported that 52 percent of all security breaches were due to hacking, and 80 percent of those breaches happened due to compromised credentials. This essentially means nearly one out of two security breaches is due to compromised identities. A Forbes report[2] presented a starker picture: 74 percent of IT decision-makers whose organizations were breached reported privileged account compromise as the reason for the breach.

According to Ponemon Institute's 2019 Cost of a Data Breach Report[3], the global average cost of a data breach has increased by 1.5 percent to $3.92 million in 2019. The cost was the highest for organizations in the US at $8.19 million, more than twice the cost for companies elsewhere in the world. These costs included class action lawsuit settlements, regulatory fines, technological investments after a breach, damage to the organization's reputation, and increased customer turnover. It has also become harder for organizations to recover from data breaches, with the average time taken to identify and thwart a breach up to 279 days in 2019 compared to 266 days last year.

The healthcare sector was the most affected, with companies having to spend $6.45 million on average for a data breach. Sectors like finance, healthcare, technology, and insurance suffered higher costs than average, and also experienced higher customer turnover after a breach. The customer churn rate was seven percent and 5.9 percent in the healthcare and finance sectors, compared to the average churn rate of 3.9 percent.

IAM best practices to protect identities from cyberattacks

Automatically provision and deprovision access privileges

Organizations need to set access privileges for new employees based on their business roles. To make this process foolproof, they can implement a workflow with multiple approval levels. After an employee resigns or is terminated, organizations should revoke all their associated privileges automatically. Often this step is performed manually, and it's possible for admins to forget to revoke these permissions.

Create and enforce complex password policies

As previously mentioned, compromised credentials are a major source of data breaches. Organizations should 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.

Enable MFA-protected single sign-on (SSO)

MFA adds extra layers of security for passwords, making it difficult for hackers to take over an account even if they crack the password. These extra layers can be anything from fingerprints to SMS-based verification codes and push notifications. Most employees require access to multiple applications, but it can be difficult to remember multiple passwords; because of this, employees often use repeated or weak passwords, or write them down, paving the way for security breaches. SSO enables employees to authenticate in multiple applications by logging in to a centralized console just once using trusted MFA methods.

Controls on privileged accounts

Hackers often target privileged accounts as they hold more valuable data and higher access levels. Therefore, organizations must assemble an accurate inventory of their privileged accounts and their access rights, and should also keep track of those accounts' activities. Besides implementing strong password policies, organizations must enforce the principle of least privilege, meaning privileged accounts should only possess the rights needed to perform a task. For example, the head of the marketing department should not have the rights to access payroll data or financial records. Organizations should also implement user behavior analytics (UBA) to quickly detect and proactively thwart anomalous activities by privileged accounts.

Get audit trails on the four Ws of user activities and resource access

It's important to keep track of the who, when, what, and where of logons and logon failures, privileged access, changes to privileged access, etc. Plus, organizations are expected to document these details for regulatory audits.

Identify and remove ghost or unmanaged accounts

Inactive accounts, especially of senior-level employees who leave the organization, could retain access to critical resources like financial documents or intellectual property. Hackers often perform recon on social media and other sources to find senior employees who've moved out of organizations, and target such accounts to remain undetected long after gaining entry to the organization. There should be regular audits to identify and remove these accounts.

What is AD360?

AD360 is an integrated IAM solution that provides many capabilities ranging from user provisioning, self-service password management, and Active Directory (AD) change monitoring, to MFA enabled-SSO for enterprise applications. AD360 makes it easy to report, audit, monitor, manage, and send alerts on AD, Azure AD, Exchange Online, Skype for Business, OneDrive for Business, Microsoft Teams, and other similar cloud services from an easy-to-use interface.

How AD360 can fulfill your IAM requirements

Streamlined user life cycle management

AD360 lets sysadmins configure automations that simplify routine user provisioning and deprovisioning tasks. Sysadmins can simply provide the list of users, and AD360 will help create user accounts and add them to appropriate groups, provision Office 365 licenses, and accomplish even more tasks during account creation. Other important aspects of the user life cycle are role changes and transfers. AD360 helps admins create automations to easily modify user accounts to reflect the changed roles of users, eliminating the possibility of human error.

AD360 helps sysadmins streamline user deprovisioning by automating the removal of employees who are leaving the organization, disabling their accounts, and more. Sysadmins only have to add the list of user accounts to be deprovisioned in a CSV file, and schedule the necessary automations.

MFA and SSO

AD360's MFA capability adds a second factor to authenticate users on their Windows or macOS machines. This second level of authentication can be a combination of the following:

- Security questions and answers
- Email verification
- SMS verification
- Google Authenticator
- Duo Security
- RSA SecurID
- RADIUS Authentication
- Push notification authentication
- Fingerprint authentication
- QR code-based authentication
- Microsoft Authenticator
- TOTP authentication
- AD-based secret questions

AD360 provides MFA during SSO for an additional layer of security. It offers SSO for over 100 applications; sysadmins can also configure any Security Assertion Markup Language (SAML)-based custom application for SSO. Its SSO capability eliminates the need for end users to remember multiple passwords, and prevents them from having to log in multiple times to different applications. Users can securely access all their enterprise applications from a single dashboard.

Password policy enforcer

AD360's password policy enforcer allows sysadmins to enforce custom password policies to strengthen their organization's cybersecurity. Admins can enforce different policies for users with various privileges, such as C-suite executives, IT admins, and non-IT staff. To enhance password complexity, AD360 enables admins to:

- Prevent patterns, palindromes, dictionary words, and such being set as passwords.
- Specify a minimum password length.
- Restrict repeated use of passwords through password history rules.
- Ensure a mix of special characters, upper case and lower case letters, numbers, and more to strengthen passwords.

Automated inactive account cleanup

With AD360, admins can schedule automations to identify and remove inactive accounts at specified intervals. Admins can also set up a review-approve workflow to verify the inactive account cleanup process.

Just-in-time access privileges

Using AD360's time-based permissions for resources, sysadmins can grant users temporary access to critical IT resources, and forget about having to revoke it later. This just-in-time privilege elevation capability ensures that employees have elevated privileges only when necessary and for the least possible time.

Comprehensive auditing capabilities

AD360 provides comprehensive audit trails detailing which users had access to which resources and what was done with those resources. It provides out-of-the-box reports for SOX, HIPAA, GLBA, the GDPR, PCI, and FISMA for comprehensive compliance reporting. Sysadmins can schedule customized audit reports to be generated and sent to their email at a preconfigured time.

User behavior analytics

With its machine learning (ML) driven UBA, AD360 creates a baseline of behavior specific to each user to accurately detect anomalous user behavior and threats.

References

1. enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf
2. forbes.com/sites/louiscolumbus/2019/02/26/74-of-data-breaches-start-with-privileged-credential-abuse/#2df1a4833ce4
3. all-about-security.de/fileadmin/micropages/Fachartikel_28/2019_Cost_of_a_Data_Breach_Report_final.pdf

Our Products

Log360 | ADManager Plus | ADAudit Plus | ADSelfService Plus

Exchange Reporter Plus | RecoveryManager Plus

ManageEngine
AD360

AD360 is an identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. AD360 provides all these functionalities for Windows Active Directory, Exchange Server, and Office 365. With AD360, you can choose the modules you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments—all from a single console.

For more information about AD360, please visit www.manageengine.com/ad360.

$ Get Quote

Download