ManageEngine
AD360

5 essentials for your **hybrid identity management and security.**

www.manageengine.com/active-directory-360

Introduction

Active Directory (AD) is used by IT administrators to consolidate an organization's information into a central repository, and facilitate identity and access management. With digital transformation ushering in cloud-based technologies with greater capabilities, many organizations view legacy systems as a burden that inhibits productivity.

The boundaries around today's workplace are shifting, and employees increasingly request access to sensitive resources to carry out their day-to-day tasks. On top of this, the number of software-as-a-service (SaaS) applications used by employees is expanding rapidly; combined with the increasing number of mobile devices, temporary accounts, and more, managing all this from a central on-premises identity solution becomes a major challenge.

Organizations are trying to adapt to these changes by modernizing their IT infrastructure, but moving over entirely to the cloud isn't easy or cheap. This is why organizations often opt for a hybrid approach to help them implement a flexible yet comprehensive identity and access management system to gain the capabilities offered by the latest technologies. With this approach, organizations can extend their existing on-premises identities to the connected devices and cloud apps.

According to Gartner, 90 percent of organizations will adopt hybrid infrastructure management capabilities by 2020. While organizations adopt hybrid environments, there are concerns about data protection, security, and compliance. In this e-book, we'll discuss the five most common challenges businesses face in managing a hybrid environment and ways sysadmins can leverage AD360 to overcome these challenges.

Challenges

Manual provisioning and deprovisioning

Often after implementing a hybrid environment, organizations manage their on-premises and cloud environments in silos. Using PowerShell scripts to manually perform repetitive tasks like user creation across both environments delays the provisioning process. Additionally, IT administrators need to know the requirements each employee has before provisioning, or they run the risk of providing employees with more or less access than required. Apart from the time and effort it takes, manual provisioning can be error-prone and pave the way for serious security issues.

Another challenge is to ensure the correct permissions for employees moving in and out of departments. Sysadmins need to ensure they are regularly assigning or revoking permissions as required by the users' current roles. Most organizations have workflow-based processes that require a manager's approval. Often after employee transfers, these processes get delayed because the user attributes are not updated on time.

Many organizations have temporary staff such as partners, third-party vendors, contract employees, and more. These users often have accounts that required regular provisioning and deprovisioning. However, sysadmins often forget to revoke access rights from the accounts of these temporary employees, potentially exposing their organizations to serious security breaches.

Distributed applications and password struggles

Many organizations use a number of different applications for day-to-day business processes; the challenge for IT administrators is providing a seamless user experience to all users regardless of where they're located.

With so many cloud-based, business-critical applications to access, it can be difficult for employees to remember every password for every application. When users forget these passwords, they're often left without access to the applications and resources they need, and contact the IT staff for help. These password reset calls absorb a huge amount of the IT team's time and drive up help desk costs.

Complying with IT regulations

Privacy and data protection have become vital to end users, resulting in new, strict regulations that organizations are required to comply with. Moreover, the responsibility of meeting these compliance standards falls on IT admins.

Admins are expected to keep track of who has what permissions, logons and logon failures, privileged access along with changes to privileged access, etc. Plus, they're expected to document these details for regulatory audits. Microsoft's native tools don't provide any prebuilt reports for this purpose, making it a challenge for sysadmins to get the audit information they need.

Lack of total visibility

Organizations using native tools for managing their hybrid environment do not have good visibility into their hybrid infrastructure as these tools operate in silos. It's difficult for sysadmins to keep track of what configuration changes were made and when. Native tools can accumulate enormous amounts of logs on the various activities carried out in on-premises and cloud environments, but these logs do not provide immediate, actionable insights to admins.

A Ponemon Institute survey has revealed that it takes 187 days on average to identify a data breach. However, AD's native tools have a maximum retention period of 90-days for activity logs. On top of this, a maximum of 50,000 log entries can be downloaded from a single log search, meaning sysadmins need to put in a fair bit of extra effort to find the insights they need.

Organizations sync the existing identities in their on-premises environment to the cloud when they transition to a hybrid environment. Without proper vetting of their existing accounts (especially the privileged and admin accounts), this practice can be dangerous, because if an on-premises AD account is compromised, the hacker will also have access to any synced cloud services.

Recent surveys by Varonis find that nearly 65 percent of companies have over 1,000 stale user accounts in their environments, and 41 percent of organizations have over 1,000 unprotected sensitive files. This means that attackers have a large surface area to attack and can access a substantial amount of information once an attack is successful. The limitations of native auditing tools leave sysadmins unaware of these dangers.

Ensuring data security

In many organizations, employees, third-party vendors, contractors, partners, and others all have access to the organization's data. IT admins often struggle with knowing who has access to confidential business data and which devices are used to access it.

On top of this, with large amounts of data getting stored on cloud environments, it can be a challenge for sysadmins to keep an eye on suspicious access to confidential data in their environment. Even if sysadmins set alerts, the overwhelming volume of alerts makes it difficult for sysadmins to pinpoint threats in their environment correctly.

What is AD360?

AD360 is an integrated identity and access management (IAM) solution that provides capabilities ranging from user provisioning, self-service password management, and Active Directory change monitoring, to single sign-on (SSO) for enterprise applications, and more. 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 a simple, easy-to-use interface.

AD360 provides preconfigured reports that consolidate data from your hybrid environment, giving you complete visibility into your Office 365 setup. You can monitor your hybrid environment in real time, and receive instant email notifications about service outages. It also simplifies compliance auditing with built-in compliance reports and offers advanced machine learning-based analytics and alerting to keep your hybrid environment secure.

How AD360 can solve your hybrid identity challenges

AD360 is a comprehensive hybrid IAM and security tool that offers the following capabilities to overcome the routine challenges sysadmins face:

Streamlined user life cycle management

AD360 lets sysadmins configure event-driven automation policies that simplify routine user provisioning and deprovisioning tasks. Sysadmins can simply provide the list of users, and AD360 will create user accounts, assign licenses, enable mailboxes, configure multi-factor authentication (MFA), add users to appropriate groups as required by their roles, and more.

Using time-based permissions for resources lets sysadmins essentially set it and forget it; they can set the time for which users will gain temporary access, and forget about having to revoke it later without putting the organization at risk.

AD360 helps sysadmins streamline user deprovisioning by automating the removal of employees who are leaving the organization from all groups, deleting or removing their licenses, forwarding their emails to another employee or converting their mailboxes to shared mailboxes, removing their mobile devices, 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 at required frequencies.

SSO and self-service password management

AD360's single sign-on (SSO) capability eliminates the need for end users to remember multiple passwords and prevents them from logging in multiple times to different applications. Users can securely access all their enterprise applications from a single dashboard. AD360 even provides multi-factor authentication during single sign-on for an additional layer of security. AD360 offers SSO for over 100 applications; sysadmins can also configure any SAML-based custom application for SSO as well.

Moreover, end users gain access to a self-service portal where they can reset passwords and unlock accounts irrespective of their location. This enables end users to reset their AD passwords through a VPN connection without relying on their IT help desk, even when they're not in the office.

With features like these, end users will always have access to the applications they need, regardless of whether they're in the office or on the go. These features also enable the IT help desk staff to focus on more critical tasks that truly require their expertise rather than attend to mundane password reset calls from frustrated users.

Pre-built compliance reports

AD360 provides comprehensive compliance reporting capabilities with its out-of-the-box reports for SOX, HIPAA, PCI DSS, FISMA, and GLBA. Sysadmins can schedule customized audit reports to be sent to their email at a preconfigured time.

In AD360, audit logs are placed in an archive indefinitely, providing long-term access to audit information, helping sysadmins adhere to compliance regulations that require several years' worth of data.

Total visibility on AD, Azure AD, and file servers

AD360 provides insights into all the changes happening in AD, Office 365, Windows Server, and Exchange Server. It tracks user logon activities including the originating IP address; changes made to AD objects like OUs, groups, computers, schema, DNS, GPOs, etc.; file and folder activities like file-read access (including failed attempts); folder permission changes; file/folder deletions; files copied-and-pasted; and more.

AD360 also keeps track of all the mobile devices that are configured to synchronize with users' Office 365 mailboxes. It provides information such as user name, device name, device type, device ID, first sync, and device international mobile equipment identity (IMEI) number to help sysadmins identify any unauthorized device connected to their environment.

Intelligent threat alerts

Using AD360, sysadmins can configure alert profiles to send customized messages to administrators when selected actions happen inside your Office 365 setup. They can also include information on the severity of the action that triggered the alert, who performed the action, the time it occurred, and more, making it easy to prioritize and act on alerts. With its user behavior analytics capability, AD360 uses machine learning to create a baseline of typical user behavior specific to each user to accurately detect anomalous user behavior and threats.

ManageEngine
AD360

AD360 is an integrated identity and access management (IAM) solution for managing user identities, governing access to resources, enforcing security, and ensuring compliance. From user provisioning, self-service password management, and Active Directory change monitoring, to single sign-on (SSO) for enterprise applications, AD360 helps you perform all your IAM tasks with a simple, easy-to-use interface. With AD360, you can just choose the components you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments from within a single console.

$ Get Quote

Download