ManageEngine
AD360

Deliver outstanding

patient care

with a comprehensive

IT compliance solution

Introduction

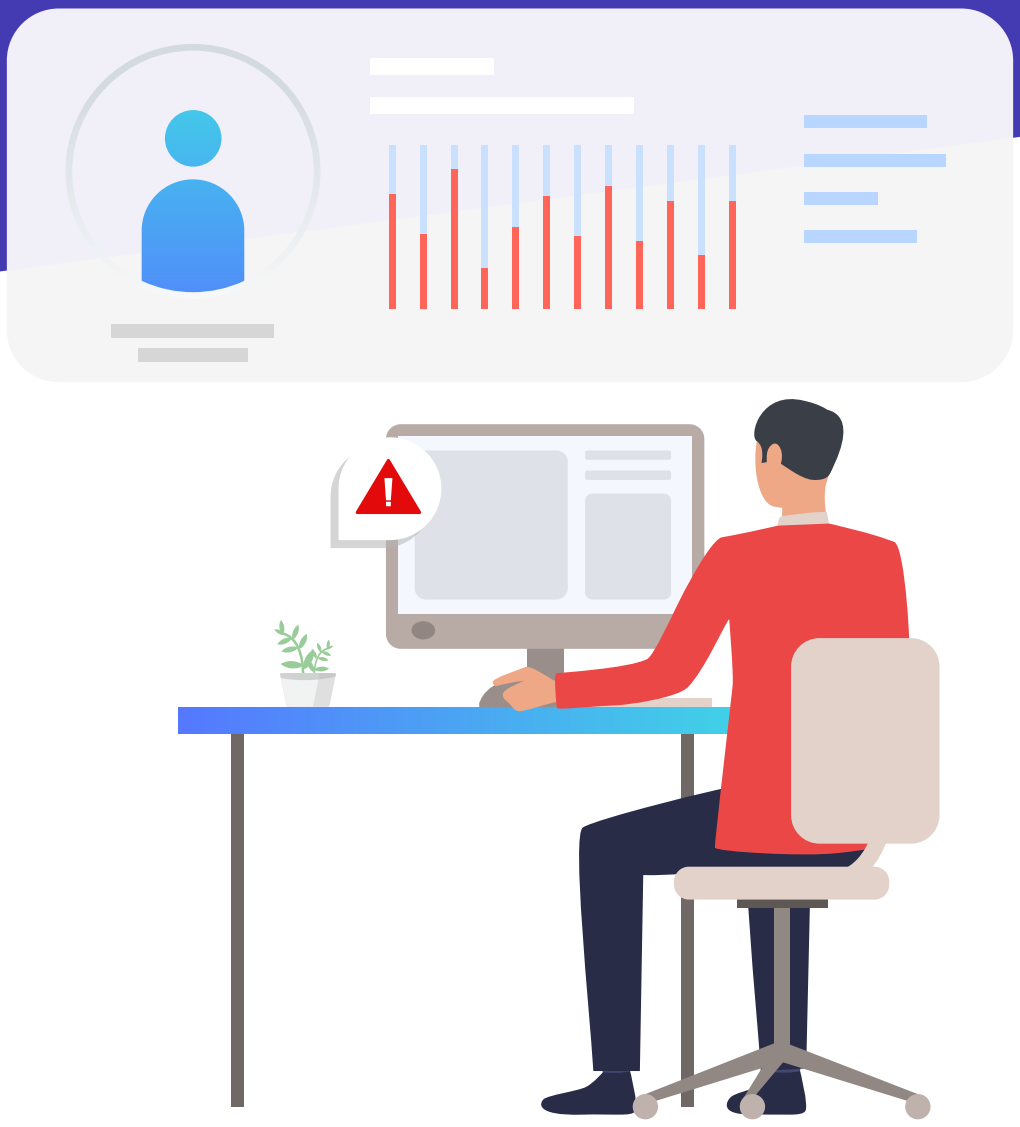
Healthcare organizations face various challenges while navigating their distributed IT environments. Ensuring patient data integrity, establishing compliance controls, and mitigating insider threats are all critical to the success of an organization.

ManageEngine AD360 helps healthcare organizations protect patient privacy, prove compliance, fend off attackers, improve operational efficiencies, and confront healthcare IT challenges.

ManageEngine
AD360

What you should be doing to

protect vulnerable healthcare data from security attacks



1

Fortify and secure electronic health records

Electronic health records (EHRs) contain protected health information (PHI) that makes them a lucrative target for cybercriminals. Servers containing EHRs need to be monitored closely to spot unauthorized access and potential data breaches. All file modifications and movements have to be monitored and audited to preserve data integrity.

How AD360 can help

Leverage AD360's real-time change monitoring function, and take proactive measures to keep patient information private.

Audit access to systems containing PHI

- Track the who, what, when, and where behind every successful and failed attempt to access a file across your Windows Server, NetApp, and EMC environments.
- Detect USB devices plugged into domain controllers, servers, or workstations, and receive alerts when files are copied to them.
- Thwart PHI exfiltration by identifying where the data in your organization is traveling, and set boundaries on how far it can go.

Review and respond to security incidents

- Save crucial time with automated responses to security incidents, such as running custom scripts to shut down devices once an alert is triggered.
- The Alerts dashboard gives administrators a clear view of how many alerts have been triggered and neatly organizes them based on their severity.
- Get real-time email or SMS alerts delivered directly to your inbox or mobile phone.

Gain visibility on AD and GPO changes

- See who made what change, when, and where with AD360's AD change auditor.
- Monitor and log changes made to all Active Directory objects, including users, computers, GPOs, passwords, and more.
- Keep tabs on administrative group membership changes, and get instant alerts on critical membership changes.
- Get a consolidated audit trail of changes made to users, computers, and Group Policy Objects (GPOs) within a given time frame.

Ensure HIPAA password requirements are met

- Enforce fine-grained password policies, and implement password requirements such as minimum password length, password complexity, and password expiration.
- Prevent users from setting passwords that are dictionary words, using phrases that are blacklisted, or following easy-to-crack patterns.
- Administer granular password policies for OUs and groups, and implement a stringent password policy for privileged users who have access to PHI.
- Enforce multi-factor authentication (MFA), and use different sets of authentication techniques for different users based on domain, OU, and group memberships all while ensuring a seamless login experience.

2

Mitigate privilege misuse and insider threats

Employees with access to sensitive data in your network are one of the biggest security threats. Privileged users with control over your Active Directory environment, GPOs, and servers pose privilege misuse and insider threat risks. For effective security, a Zero Trust environment needs to be established so that insider threats are kept at bay.

How AD360 can help

Combat insider threats by leveraging AD360's machine-learning powered user behavior analytics (UBA) capability.

Mitigate insider threats with UBA

- Apply machine learning algorithms to create a baseline of normal behavior specific to each user, and get notified about deviations from this norm.
- Configure automatic actions to be performed, such as running scripts or executing batch files, when an anomalous event occurs, and instantly respond to these incidents.

Detecting privilege abuse

- Identify and get alerts on tell-tale signs of privilege abuse, such as unusually large volumes of file modifications and attempts to access critical files.
- Spot privilege escalation attacks by monitoring and auditing changes made to security groups.

Gain visibility into your IT environment

- With over 200 preconfigured reports, monitor critical changes such as unauthorized modification of a security group, high volumes of failed attempts to access a critical database, remote logins, and much more.
- Establish a Zero Trust policy: monitor file creation, deletion, modification, and permission changes made by healthcare staff to ensure that permissions are granted on a need-only basis.

3

Meet healthcare regulations

Healthcare IT staff are tasked with protecting healthcare information against security threats and risks. Electronic protected health information (e-PHI) is constantly in the crosshairs of hackers and malicious insiders. HIPAA mandates healthcare organizations implement policies and protective procedures that restrict access to PHI based on employees' roles. The regulation also mandates that healthcare organizations limit PHI disclosure to the minimum number of employees necessary.

How AD360 can help

Easily meet HIPAA and HITECH compliance with out-of-the-box reports.

Making HIPAA compliance easier

- With preconfigured file integrity auditing reports that are tailored to meet HIPAA compliance, proving compliance is a breeze.
- Continuously audit changes made to your Active Directory, Exchange, and Office365 environments, and get notified of any anomalous behavior.
- Generate actionable and intuitive reports, and keep records on who has access to sensitive PHI.

ManageEngine
AD360

Healthcare delivery made more secure

Audit access to files containing PHI, monitor privileged user activity, enable user behavior analytics, meet healthcare regulations, and fortify patient data from unauthorized access, all from a single console. AD360 helps improve your cybersecurity posture and lets you concentrate on what is important—delivering elevated patient care.

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