3

step action plan to

ensure critical data protection and compliance

ManageEngine

AD360

Table of contents

Introduction to data protection and privacy

The stakes involved in protecting personal data of customers and employees has never been higher. With governments tightening regulatory requirements and increasing fines for failing to ensure critical data integrity, ensuring data privacy is becoming increasingly challenging. A resilient approach to data protection can help businesses avoid legal troubles and steer clear of monetary penalties.

Data protection fundamentals

Ensuring data security is a two-fold process: both the physical and technological access to stored data should be restricted, monitored, and governed. When it comes to the restriction of user access, adequate security measures such as maintaining password hygiene, monitoring security events continuous to spot intrusions, and limiting who has access to data, is required to ensure data integrity.

Recent developments in data protection laws

Recent revisions to the European Union data protection regulations have effectively rendered data processors and controllers responsible for data protection. This means that organizations that hold and process critical data are responsible for its integrity. Regulatory bodies are coming up with new compliance mandates that emphasizes data privacy and provides more control to the users whose data are being stored and processed. For instance, we have the GDPR and CCPA that instructs companies to:

1. Establish security measures to instantly detect data breaches and report them within 72 hours (GDPR) to concerned authorities
2. Oblige to user requests to delete the data and let them know if there had been any modifications made to their personal information.

   These compliance requirements are exhaustive and companies are scrambling to update and re-strategize their security policies to comply with these regulatory mandates.

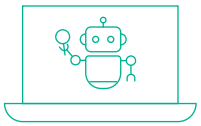
2.

Implementing multi-factor authentication

1.

Implementing a Zero-Trust environment

3.



Leveraging user behavior analytics to spot data breaches

Formulating an action plan to **ensure data protection and compliance**

Given the stakes of protecting customer data and complying with all applicable privacy laws is at an all-time high, it is imperative for organizations to implement a data protection policy that meets all applicable jurisdiction laws.

One of the crucial steps in protecting sensitive data would be to impose the principle of least privilege (POLP). Access control by least privilege assures that all the users in the network only have the bare minimum permission required to complete their job. POLP implementation is supported by establishing a zero-trust environment.

Zero-Trust architecture
An introduction

The zero-trust approach to an organization's security was proposed by the analyst firm Forrester Research nearly a decade ago. Zero-trust is a security concept centered on the belief that organizations should not automatically trust anything inside or outside its environment, and must instead verify all endpoints and users before granting access to its resources.

The rapid cloud adoption and implementation of internet of things (IoT) have extended the traditional network boundaries. The zero-trust POLP, and multi-factor authentication (MFA) are the keys to safeguarding the critical data of an organization. Zero-Trust architecture functions on 5 basic guidelines.

The five tenets that Zero-Trust relies on are listed below:

- The network is always assumed to be hostile.
- External and internal threats exist on the network at all times.
- The physical location of the network should not be a determining factor for deciding trust in a network.
- Every device, user, and network flow is to be authenticated and authorized.
- Access control policies must be dynamic and calculated from as many sources of data as possible.

Challenges that zero-trust architecture can address

Insider threat

The obvious reason insider threats cause more harm than external threats is that a malicious insider knows more about the network, might already have the necessary permissions and privileges to access critical data, and has knowledge on existing vulnerabilities. Even if the insider does not have the necessary privileges to access the critical resource, they move laterally within the network network elevating their privilege until they attain their goal. This lateral movement of insiders can be thwarted by applying the principles of Zero-Trust. Since only the least privilege is granted to an user, if the intruder does manage to take hold of an user account, they cannot escalate privileges as all user actions are assumed to be hostile. Instead, the intruder has to face various rounds of authentication and authorization.

But ensuring authentication and authorization is easier said than done. For starters, most databases that house critical data do not have the capability to monitor and restrict data access. Since some legacy systems, like packet filtering firewalls and flat file databases, can't align well with the zero-trust approach, they can cause security gaps leading to potential breaches.

Network visibility

In an ideal zero-trust environment, all network traffic is logged, inspected, and analyzed to identify and respond to network attacks. Implementing this gives network administrators a clear picture of who accesses what in the network.

However, in real-life, traffic from productivity suites like Google Workspace and Microsoft365 can only be monitored from their respective dashboards. These siloed applications force administrators to toggle across multiple consoles to monitor network traffic. Hence, third-party solutions that lets administrators keep tabs on their network, all from a central console, becomes essential.

Vulnerable endpoints

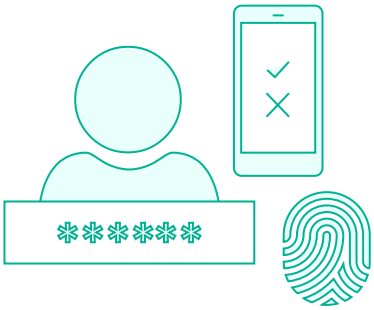
With every organization having to keep an eye on multiple endpoints like servers, workstations, desktops, laptops, tablets, and mobile devices, ensuring network security can quickly get out of hand. To harden the security posture and implement zero-trust, endpoint protection and firewall solutions have to work hand-in-hand. It is imperative that, if and when a workstation is under attack, the endpoint protection solution should execute the incident response and also should signal the firewall to cut off network access to the workstation to prevent the threat from propagating into the network.

Implementing a zero-trust environment with AD360

Implementing a zero-trust environment is a laborious exercise. However, it does not require replacing existing infrastructure or security frameworks. If you are looking to implement a Zero Trust architecture in your environment, consider a third-party tool like ManageEngine AD360. Here's how AD360 can help you implement Zero-Trust architecture and, in turn, ensure critical data integrity.

Migrating to a Zero-Trust architecture also means revamping the way users are provisioned and modified. The most commonly committed mistakes while provisioning and modifying users are:

1. Granting excessive permissions to users
2. Failing to clean up stale accounts
3. Failing to monitor a user's gradual accumulation of unnecessary access privileges (privilege creep)
4. User management delegation without boundaries



1.

Implementing a Zero-Trust environment

Tackling excessive privileges

Any user receiving excessive permission than they actually need to get their job done—like permissions to view, modify, or delete sensitive files—is a security loophole that can lead to data loss, breaches, incorrect modifications, and more. A Zero Trust architecture dictates employing POLP.

AD360 helps administrators and IT technicians granularly assign permissions to users and groups. Doing this with the help of native tools involves writing complex PowerShell scripts to query Active Directory (AD), which can be time consuming.

AD360 provides reports on access permissions of all NT file system (NTFS) folders, as well as files and their properties for Windows file servers and NetApp server. This helps IT administrators quickly view and analyze file-level security settings in their environments. To ensure that users are not placed in the wrong groups and provisioned with excess privileges, IT administrators easily generate preconfigured reports that show which groups each user, group, contact, and computer belong to.

Cleaning up stale accounts

When an employee leaves an organization, their account should be stripped of its privileges, then deprovisioned. Malicious insiders could leverage stale accounts to access your organization's resources. Software licenses don't come cheap, so your organization should take action promptly.

AD360 can generate actionable reports to identify stale accounts, and strip them of their group memberships, revoke all their permissions, remove Microsoft 365 licenses, and delete or disable the unnecessary accounts. This ensures greater system security, and saves your organization money and valuable IT support team time.

Monitoring privilege creep

Over time, some users might accumulate access to certain sensitive files, even if they no longer need it.

With AD360, administrators can grant time-bound access rights to important file servers for a limited time, after which the permissions will be automatically revoked. AD360 helps generate actionable reports in regular intervals to help zero in on users who have excessive permissions, and strip them of unnecessary permissions.

User management delegation without boundaries

Delegating tasks to IT technicians can be beneficial when you are hard-pressed for time. However, technicians with excess privileges can cause more harm than good.
With AD360, delegate IT technicians to work on tasks without elevating their native AD permissions.

1. Set boundaries on what technicians can and cannot do.
2. View all the permissions assigned to, or revoked from, help desk technicians.
3. Establish an audit trail to identify administrators performing changes on help desk technicians, and see which roles were modified.

2. Implementing multi-factor authentication

Since the traditional login method authenticates users with only a username-password combination, any person with these credentials can gain access to critical resources. A major drawback with this method is that, if the credentials are stolen or compromised, then the entire network security is at stake. To avoid this, we need an additional layer of security that authenticates the users with two or more independent credentials.

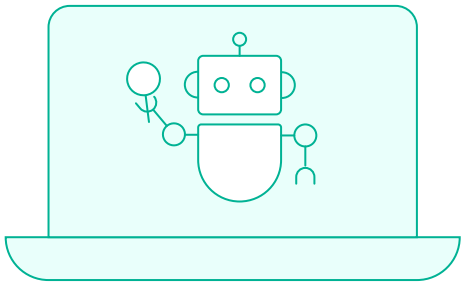
Double up on security with AD360

By enabling organization-wide MFA, you can tackle all credential-based cyberattacks, including brute force, password spray, and dictionary attacks. With AD360, administrators can secure both local and remote login attempts to servers and workstations.

AD360 offers MFA for Windows, macOS, and Linux endpoint logins. With endpoint MFA in place, users are first authenticated through AD domain credentials, and next through one of the supported authentication techniques such as SMS codes, security questions, OTPs, YubiKey authenticator, fingerprint, and FaceID authentication.

Even if the intruder has obtained user credentials, with MFA enabled they will not be able to access the network without the other identity factors, which is something unique to the user.

Additionally, AD360's password management module also offers password self-service, password expiration reminders, a self-service directory updater, a multi-platform password synchronizer, and single sign-on (SSO) for cloud applications.



3.

Leveraging user behavior analytics to spot data breaches

Many organizations are depending on the machine-learning based user behavior analytics (UBA) to accurately detect advanced persistent threats (APTs), and internal and external attacks. . UBA solutions can spot what a traditional rule-based incident detection tools can't by looking for strange behavior of the user, referred to as anomalies, that can indicate a pending attack. They apply statistical analytics and machine learning principles that creates a baseline of normal behavior specific to each user and alerts about deviations from this norm, something that is impossible to do if logs are analyzed manually.

The following is a list of events that are tell-tale signs of a cyber criminal trying to gain access to your network.

1. Multiple logon failures followed by a successful logon and a high volume of activity
2. Unusual logon time followed by activities like security group membership changes/critical file changes/user account changes/GPO changes
3. Dormant admin account becoming active
4. Unusual volumes of file activity
5. High frequency of account lockouts

Manually keeping track of such events is next to impossible, and can quickly get out of hand.

UBA solutions first collect information on what users across the organization typically perform over an extended period of time. They then create a baseline of "normal" activities specific to every single user. Whenever there is a deviation from that norm, the solution flags it and notifies the administrator.

Part of what makes UBA solution highly efficient is that human behavior is hard to mimic. So, even when an intruder does manage to break into a network, it's going to be hard for them to duplicate another person's daily behavior.

User behavior analytics capabilities:

1. Monitor user behavior continuously to spot anomalous activities and get instant alerts in case of malicious behavior.
2. To address compliance concerns, keep track of all file and folder access and permission changes made by the user.
3. To spot threats, correlate unusual activity volume and time.
4. Get details on user idle time and productivity by tracking user logon/logoff, startup/shutdown, and screensaver invokes/dismissals.

AD360's UBA engine for tackling real-life security issues

By looking at how UBA solutions detect common breach scenarios that fly below the radar, we gain a better understanding of UBA. The following breach scenarios cover the entire threat spectrum: from an insider gone rogue, to an attacker who has just gained foothold within the network using compromised credentials, to an all-out external threat.

UBA versus rogue insiders

A disgruntled employee departing from the organization decides to exfiltrate data.

Indicator of compromise: *Unusual file activity count*

How AD360 helps

Because of the low volume of file activity, this breach would go undetected if not for a UBA solution. AD360, though, knows how many files the user usually accesses at that particular time of day based on their past behavior, thanks to the baseline it has computed. IT administrators are notified when a deviation from this baseline is detected. AD360 can also instantly send an alert when users access files that they've never accessed before.

UBA versus compromised accounts

An attacker with stolen credentials wants to elevate his privileges within the network, so he targets other systems using remote desktop protocol (RDP) to gain remote access to other hosts on the network.

Indicator of compromise: *Unusual logon activity—First time remote access on host network*

How AD360 helps

AD360 can spot and raise an alert because hosts on the network were accessed for the first time by a remote logon. This can again be owed to the baseline that was generated for every single user. When a deviation from the baseline is observed, an alert is triggered.

UBA versus external threats

When a user in the organization clicks on a malicious link, that automatically downloads a malware, such as ransomware, which encrypts their data and starts spreading across the network.

Indicator of compromise: *Unusual process—New process on host network*

How AD360 helps

While existing security solutions can detect ransomware infestations once data encryption starts, AD360 detects ransomware attacks before files are even encrypted. Immediately after the malicious program is downloaded, AD360 detects a new process on the host and triggers an alert.

If you're looking to revisit your data protection strategy, ManageEngine AD360 can help. Our identity and access management (IAM) and cybersecurity consultants will work with your team to formulate or revamp your data protection policy and strategy.

About 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.
AD360 provides all these functionalities for Windows Active Directory, Exchange Servers, and Microsoft365. With AD360, you can choose the modules you need and start addressing IAM challenges across on-premises, cloud, and hybrid environments from within a single console.

To learn how you can implement AD360 for your organization's data protection needs, schedule a demo with our product experts, and dramatically improve how IT supports your diverse business needs. Whether it's on-premises, cloud-based, or hybrid, by leveraging the capabilities of AD360 you can make your IT environment more secure and easy to manage.

$ Get Quote Download