ManageEngine
AD360

RANSOMWARE

How attackers weaponize Active Directory, and what defense measures can stop them

www.manageengine.com/active-directory-360/

Table of contents

The continued rise of ransomware

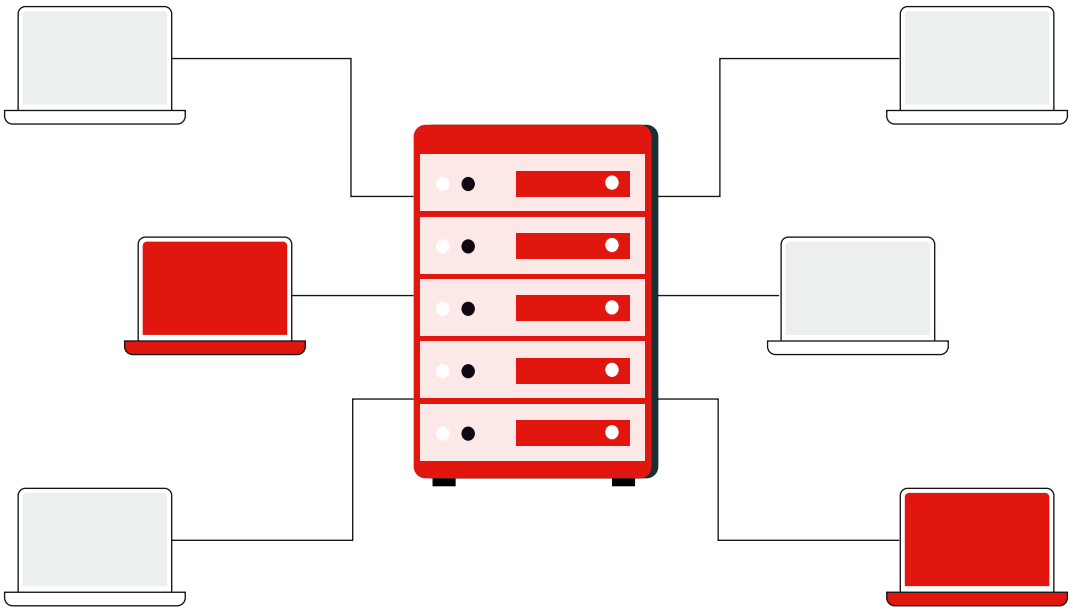
Ransomware attacks have exploded since the COVID-19 pandemic began, with 2020 witnessing 485% more ransomware incidents than 2019.[1] The surge has only continued in 2021, and predictions for the future of ransomware are even more alarming: By 2031, a new organization is expected to fall prey to a ransomware attack every two seconds.[2] The increase in the number of ransomware variants in operation, the success of the Ransomware-as-a-Service (RaaS) model, and organizations' willingness to pay the ransom demanded in exchange for the decryption key are crucial reasons why ransomware attacks have become enormously successful. The average ransomware payment today has touched a staggering $570,000, which is 80% more than the average ransom demanded in 2020.[3]

In this guide, we'll explore how ransomware attacks exploit Active Directory (AD), and discuss steps that will help organizations prevent ransomware gangs from taking over their AD infrastructure. We'll also walk you through how ManageEngine's identity and access management offering, AD360, can help you defend AD against today's most prominent cyber threat.

AD a prime target in ransomware attacks

Despite AD being two decades old now, it is the technology that most organizations continue to build their IT infrastructure around. Since AD enables organizations to store an ever-increasing amount of information and also helps with controlling and organizing who has access to this data, it is an integral part of most IT environments. AD is used to store crucial identity-related information, including user permissions and passwords, and information about all the various entities in the network, such as servers, workstations, and applications. It's this high-value information stored within AD that makes the platform a key target for attackers.

In many of today's ransomware attacks, threat actors are exploiting AD to accomplish various objectives. They are leveraging AD to understand the target network's configuration, discover and take over domain admin accounts and non-admin accounts with excess privileges, laterally move within the network to compromise more systems without being detected, push ransomware to all devices in the network in one go, and much more. Here's a look at how AD was abused in two recent ransomware attacks.

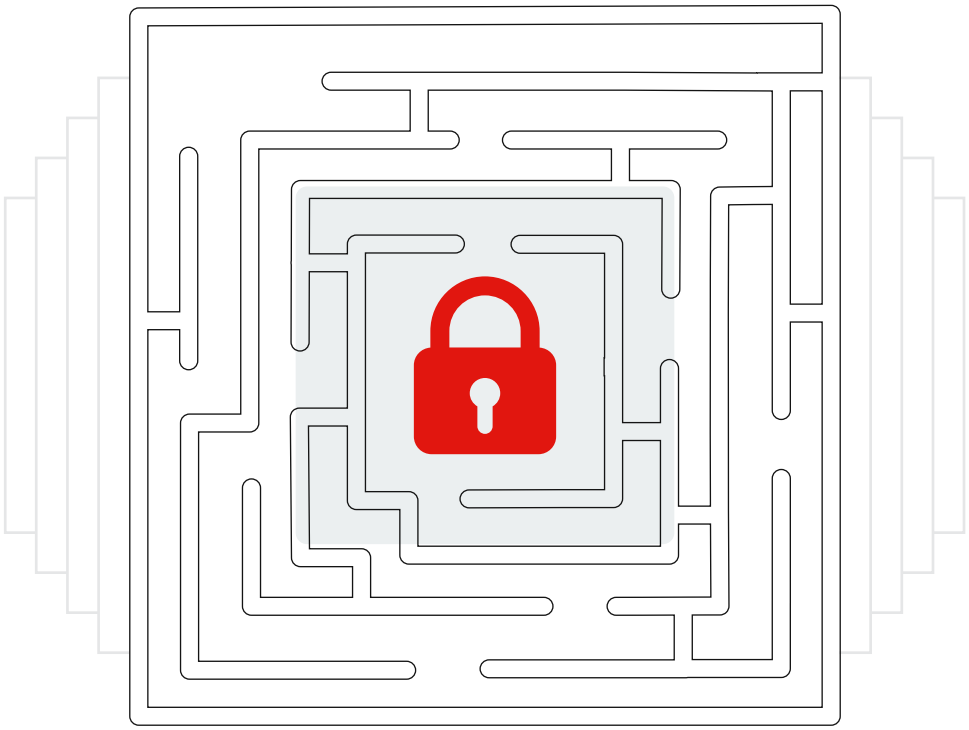


SaveTheQueen ransomware

In early 2020, security firm Varonis discovered a new strain of SaveTheQueen ransomware that leveraged AD domain controllers (DCs) to spread across the network. The DC is the server that not only authenticates users in the network but also stores crucial information related to users and devices, such as group policies. This particular strain of SaveTheQueen was found propagating through the SYSVOL share stored in DCs. The SYSVOL is a folder that is present in every DC. It's the vehicle through which group policies and login scripts are delivered to every domain-joined workstation. The contents present in SYSVOL in one DC are replicated across all other DCs with the help of the File Replication Service to ensure data across SYSVOL folders is synchronized.

In the case of SaveTheQueen, two types of files were created inside the SYSVOL folder: log files and a file called hourly, which was a scheduled task that executed the malware on the devices.

While all authenticated users in a domain have read access to the SYSVOL folder, only those with admin privileges have write access, showing that the ransomware attack wouldn't have progressed if threat actors couldn't get their hands on an account with admin privileges.



Maze ransomware

Maze ransomware was actively deployed by threat actors in late 2019. Maze ransomware attacks gained notoriety for their departure from usual ransomware attacks—in most Maze attacks, in addition to data being encrypted, it was also exfiltrated. The group behind Maze threatened to release the stolen data on its website on the dark web if victims didn't agree to pay the ransom.

Attacks involving Maze weren't carried out by a single group. Instead, it followed the RaaS model, where the original developers of the malware partnered with affiliates who would distribute it. Affiliates received a package containing the tools necessary to execute the attack. After a successful attack, the parties involved would get a commission on the ransom extorted from the victim.

While threat actors initially relied on phishing campaigns and exploit kits to spread Maze, they later started using virtual private network (VPN) connections and Remote Desktop Services as their primary mode of infection.

In most Maze attacks, the attackers leveraged tools like Mimikatz and BloodHound to harvest credentials that would enable them to take over privileged accounts. Often, they also used BloodHound to profile an organization's AD configuration and discover the privileged accounts within it. Security researches found that Maze attacks also use SharpHound, a data collector program that BloodHound leverages to collect AD data. When SharpHound is run on a compromised domain-joined workstation, it can fetch a plethora of AD details, including the group membership, domain trust relationships, local admin accounts, and RDP users.

When the collected data is fed to BloodHound, the tool offers a range of prebuilt scripts to analyze the data. It includes queries such as "Find Computers where Domain Users are Local Admins" and "Find Servers where Domain Users can RDP." The attacker can even run a query to identify the shortest path through which they can gain domain admin status from a domain user account they have compromised.

At the end of 2020, the Maze ransomware group announced that they were shutting down. However, security experts thought this was likely a re-branding exercise and that organizations should be on the lookout for attacks similar to ones carried out by the group.

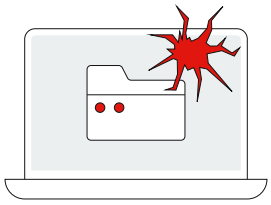
Key stages in a ransomware attack

There are plenty of ransomware strains in circulation, and new ones continue to emerge. While not all ransomware attacks follow the same rule book, most of them have common stages in their attacks. MITRE, a nonprofit organization involved in cybersecurity, developed the ATT&CK framework, which is a repository of adversary tactics and techniques used in real-world cyberattacks. It was developed to help organizations understand the various stages in a cyberattack and enable them to thwart attacks, even if they're in progress. Based on the MITRE ATT&CK framework, here's a high-level overview of the various stages in a ransomware attack.

1.

Initial access

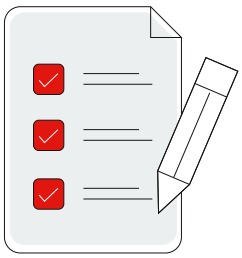
This is the first step in any cyberattack, irrespective of whether the end goal is to deploy ransomware or any other form of malware. There are plenty of ways threat actors gain an initial foothold in a network, ranging from a supply-chain compromise to exploiting a vulnerability in an internet-facing application. However, since the switch to remote work, ransomware groups have predominantly used phishing campaigns and RDP attacks as initial entry points into internal networks.



2.

Tools checklist

Threat actors require a variety of tools to carry out an attack. They either enter with malware containing a package of all the tools necessary for the attack, or, after intrusion, they download the required tools by establishing communication with a command-and-control (C2) server. The most common types of tools used include:



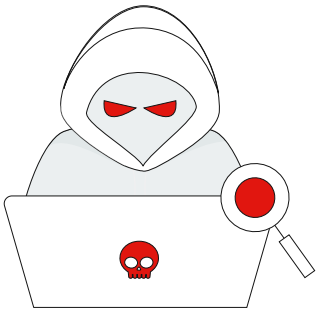
- Reconnaissance tools that help the attacker understand where they are in the network and what accounts can be targeted further.
  - **Examples:** Nmap, Process Hacker, and BloodHound

- Credential dumping tools that help compromise the login credentials of other privileged accounts, which the attacker can use to move laterally within the network.
  - **Examples:** Mimikatz and ProcDump

- Built-in programs such as PowerShell, Windows Management Instrumentation (WMI), and PsExec. Take, for instance, attacks involving DarkSide ransomware. Security researchers found that WMI and PSExec commands were being used to delete local backup copies, and PowerShell was being used to create malicious backdoors.

3.

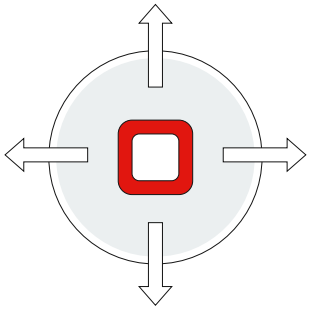
Network reconnaissance



Here, attackers put to use their reconnaissance tools. They discover open ports, check if the compromised system is connected to AD, and perform a series of other checks to get a complete overview of the internal network.

4.

Lateral movement

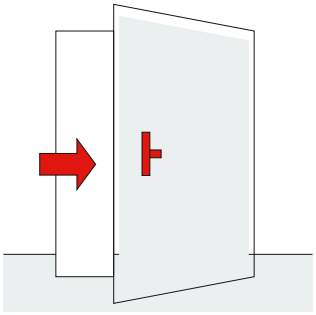


Threat actors move laterally within the network to find vulnerable privileged accounts. One of the most common techniques observed in ransomware attacks is the exploitation of local admin accounts; this behavior has been seen in PARINACOTA and Clop, two ransomware strains that have been active since early 2020. Local administrator accounts are key targets because organizations tend to have one common password for all their local admin accounts.

5.

Establishment of backdoors

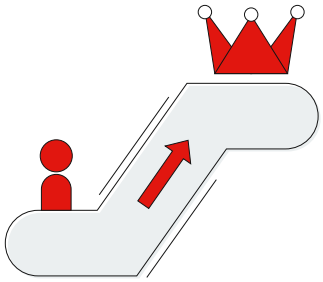
Malicious programs that enable attackers to bypass any security controls in place and maintain unauthorized access to the internal network are called backdoors. In the case of WannaCry ransomware, DoublePulsar was the backdoor used. DarkSide ransomware, the strain that recently crippled the Colonial Pipeline, is known to establish backdoors in two ways: the creation of attacker-controlled domain accounts, and the deployment of the Cobalt Strike Beacon, a payload that can establish communication with a C2 server over HTTP, HTTPS, or DNS. Threat actors rely on backdoors to maintain persistence in a network, download any utilities they'll need for an attack, and, in some cases, exfiltrate data to a remote location.



6.

Privilege escalation

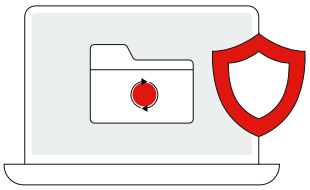
This is the stage in which AD is abused the most. Access to a DC, which usually domain admins have, is invaluable to threat actors, especially in a ransomware attack because this access will enable them to release malware to all the systems in the network in one shot. Threat actors have a range of tactics for gaining domain admin rights, including techniques like Kerberoasting, pash-the-hash attacks, and stealing passwords stored in the SYSVOL folder.



7.

Destruction of backups and disablement of security products

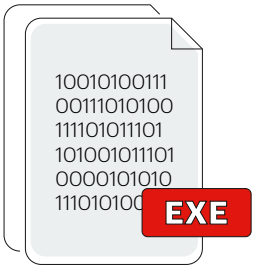
To ensure victim organizations can't easily recover data from their backups, most ransomware attacks involve the destruction of backups. As organizations tend to have backups both in local systems, also known as shadow copies, as well in a central location, threat actors usually try and erase both forms of backups. They often have greater success in erasing shadow copies. In instances where they are unable to tamper with the backup data in the central location, they tend to encrypt all data files for a long period. Attackers usually leverage PowerShell and WMI to erase the shadow copies. VSSADMIN.EXE and WMIC.EXE are system utilities that attackers leverage to delete the shadow copies.



Disabling security products is usually the penultimate step before the ransomware encryption of files begins. While attackers use tools like PCHunter or Process Hacker to go after any antivirus solutions in place, they rely on accounts with domain admin privileges to try and turn off any other security tools, such as endpoint security systems. Existing Windows services are also halted to ensure that the data that is part of those services can also be encrypted. For instance, Dharma ransomware attacks are known to terminate database services such as sqlwriter, mssqlserver, and sqlserveradhelper to ensure data files that are being processed by these services are also encrypted.

8.

Encryption and the ransom note



The encryption of files takes place only towards the end of an attack. The type of algorithm used to encrypt data varies from one ransomware group to another.

For instance, Ryuk ransomware uses a combination of symmetric (AE-256) and asymmetric (RSA-4096) encryption algorithms, while DarkSide uses a combination of a stream cipher (Salsa20) and RSA-1024, which is an asymmetric algorithm. The ransomware payload is usually delivered using logon scripts via a Group Policy Object (GPO) or by leveraging WMI. Once the encryption is complete, a ransom note is left with an email address that the victim can contact.

As you can see, AD is involved throughout the various stages of a ransomware attack, and it's predominantly abused during privilege escalation and lateral movement. In the next section, we'll look at defense strategies you should adopt to secure AD from ransomware attacks.

6 defense measures to stop ransomware attacks from taking over your AD infrastructure

1.a

Enforce strong custom password policies

It isn't always easy to get users to follow password best practices, like setting long, complex passwords, skipping passwords that are common dictionary words, and avoiding already compromised passwords. Also, native AD tools can enforce only extremely basic password restrictions, so much so that organizations can still set passwords like Admin12$ for an account.

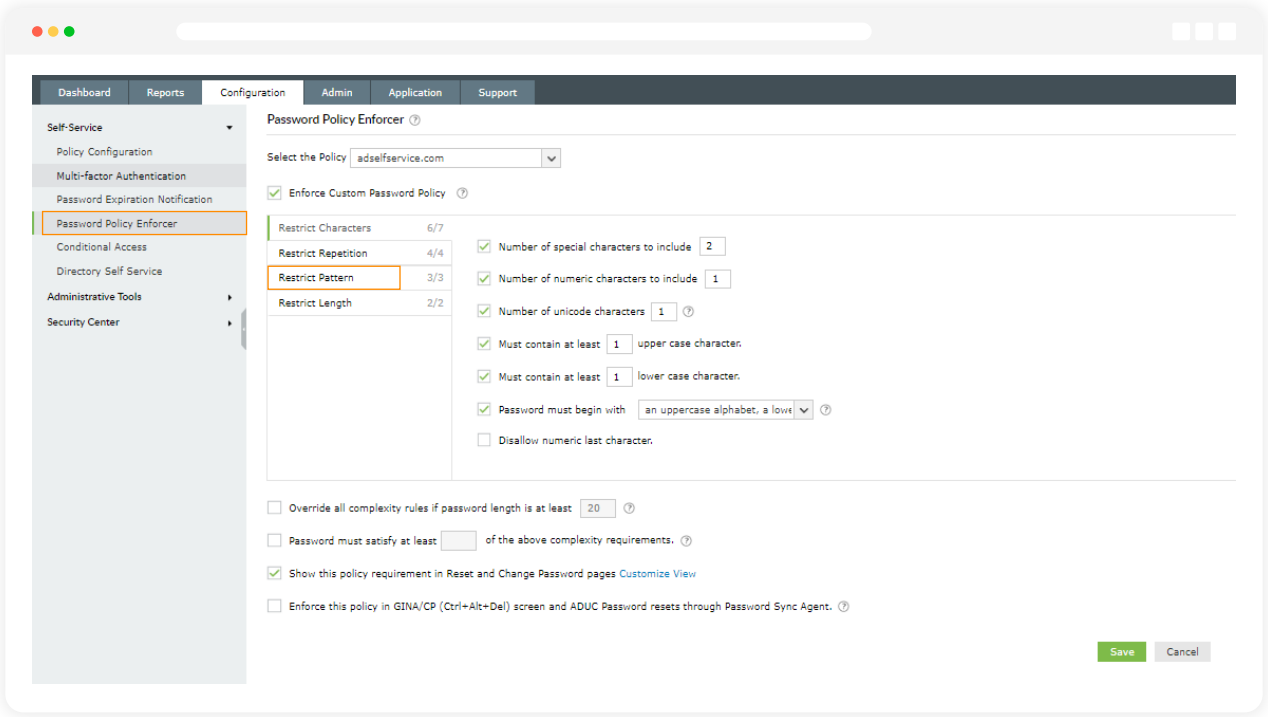
However, weak account credentials are the primary reason why an AD takeover is possible in a ransomware attack.

With ManageEngine AD360's password policy enforcer, IT admins can ensure users set passwords which comply with either one or all of these rules:

- Meets a minimum length
- Includes both uppercase and lowercase letters
- Includes special characters
- Includes numbers
- Requires that the password begin with either a letter, number, or special character

Even if a user's password meets all these rules, the solution checks the password and won't allow the user to set the password if it:

- Is a dictionary word, or patterns which is easy to crack
- Is found in the organization's custom list of weak passwords
- Belongs to the list of already breached passwords. This is achieved through an integration with the "Have I Been Pwned?" service that checks passwords against a continuously updated list of compromised passwords

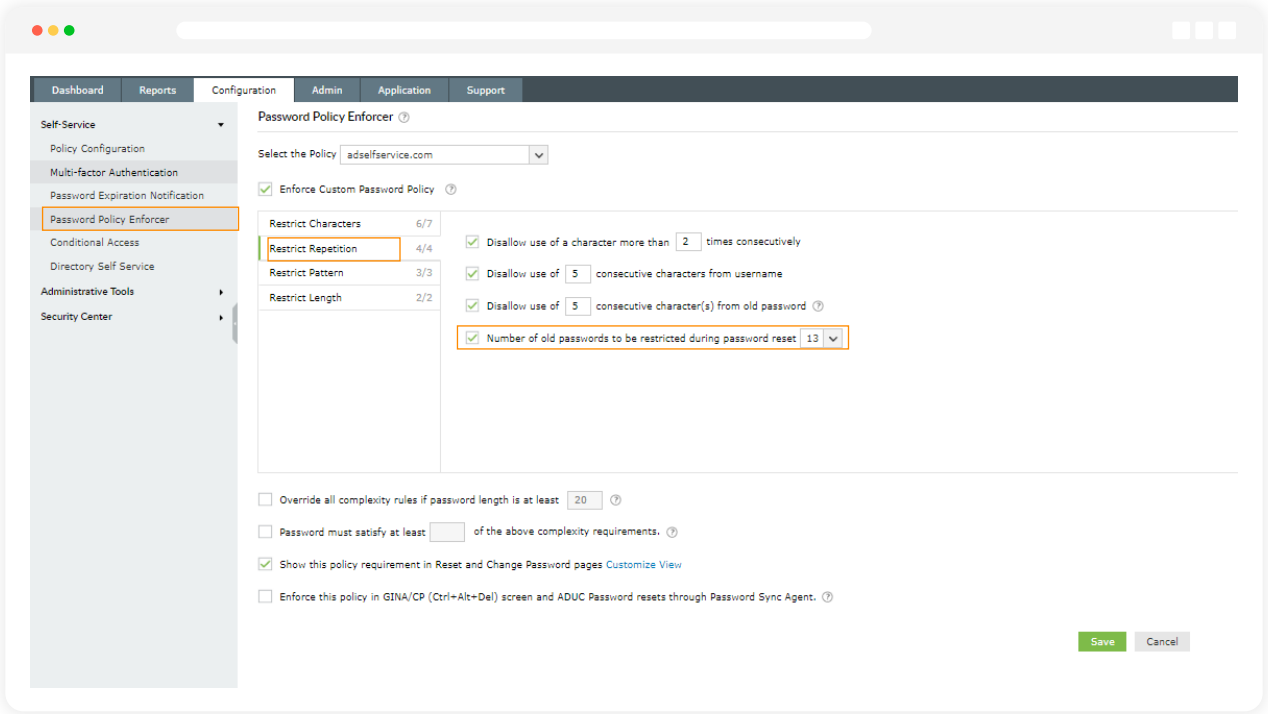


1.b

Restrict users from reusing old passwords

Fifty-four percent of all employees reuse passwords for many of their work accounts, a recent survey by hardware authentication device manufacturer Yubico revealed.4 Thanks to password reuse by a majority of users, attackers need to compromise only one pair of corporate credentials to sneak into your network.

With AD360's password history check feature, IT admins can ensure that users can't reuse any of their past 24 AD passwords.



2.

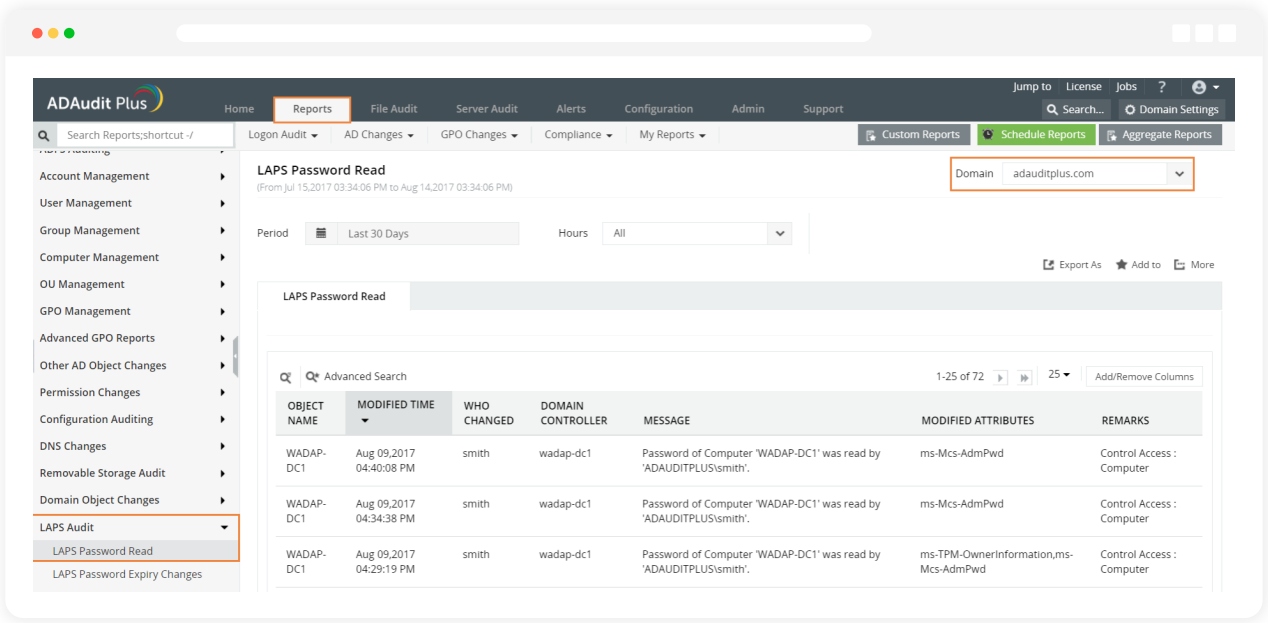
Ensure all local administrator accounts don't have the same password

Threat actors have leveraged local admin credentials in multiple ransomware attacks to accomplish privilege escalation or lateral movement. Since manual management of local admin credentials is time-consuming, it's best for organizations to use tools like Microsoft's Local Administrator Password Solution (LAPS) to manage them. LAPS leverages AD to store, control, and randomize the local admin passwords of all domain-joined Windows computers. You can learn more about LAPS here.

A problem that's likely to arise when organizations start using LAPS is finding a way to audit changes made to the tool. LAPS requires administrators to manually perform a lengthy list of steps on each workstation to view password changes in LAPS.

With AD360, organizations can generate reports on:

- Users who have viewed passwords.
- Users who have modified a password's expiration date and time.



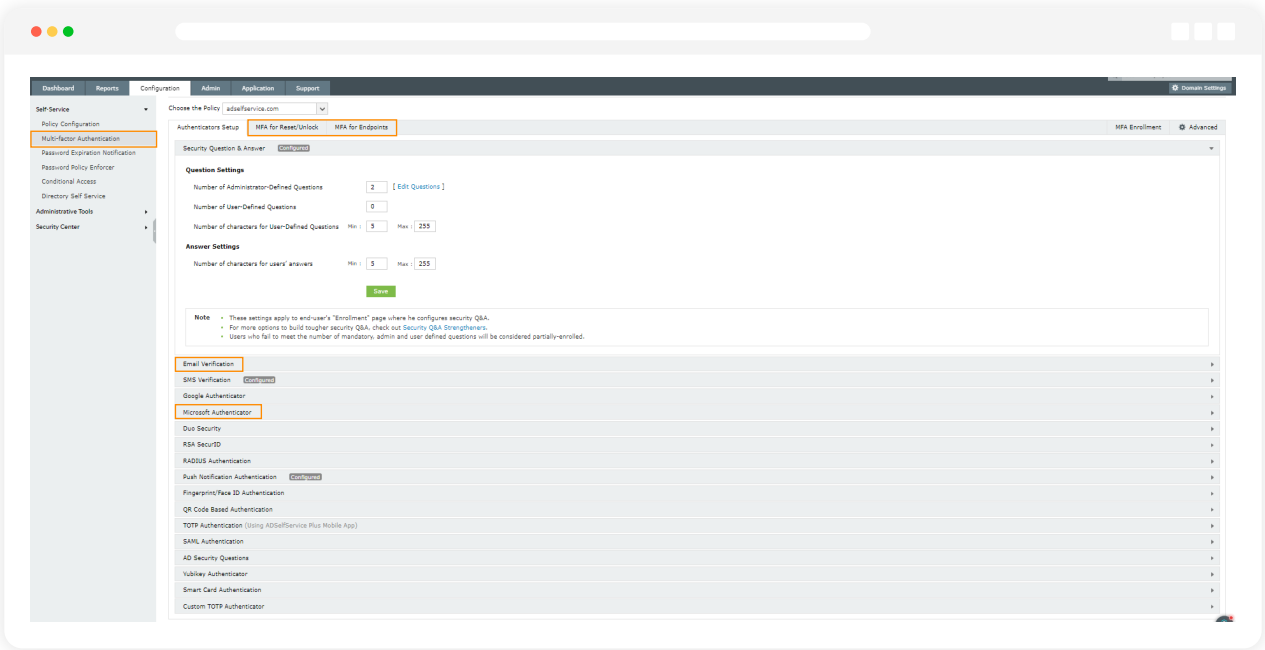
3.

Enable MFA for VPN logins, workstations, and applications

Passwords, the most common authentication factor used to verify identity, are the most vulnerable one too because users tend to set easy-to-remember passwords and are likely to use the same weak password for other devices and services. MFA provides an extra layer of security as it involves verification of an additional factor that the user owns, like a smartphone, or a factor proving who the user is, like a fingerprint or any other biometric attribute. With MFA enabled for all domain users, and specifically admin accounts, even if the password is compromised, the attacker can't complete the heist because they don't have access to the additional factor. MFA is a MITRE-recommended mitigation strategy for various adversary techniques that affect initial access, lateral movement, and privilege escalation to domain admin.

Also, one of the best ways to protect your RDP connection is to grant RDP access only through a VPN and further strengthen security by securing the VPN access with MFA. Other steps to take are to ensure unnecessary open RDP ports are locked down, periodically reevaluate users who can log in to the network using RDP, and keep the Network Level Authentication of your RDP server always on.

AD360 supports over 15 authentication techniques, including YubiKey authentication, biometrics, and RSA SecurID. With AD360's MFA options, IT admins can secure VPN connections as well as Windows, macOS, and Linux endpoints; safeguard access to SSO-enabled applications; and ensure users can use the self-service password reset or account unlock features only after their identity is verified.



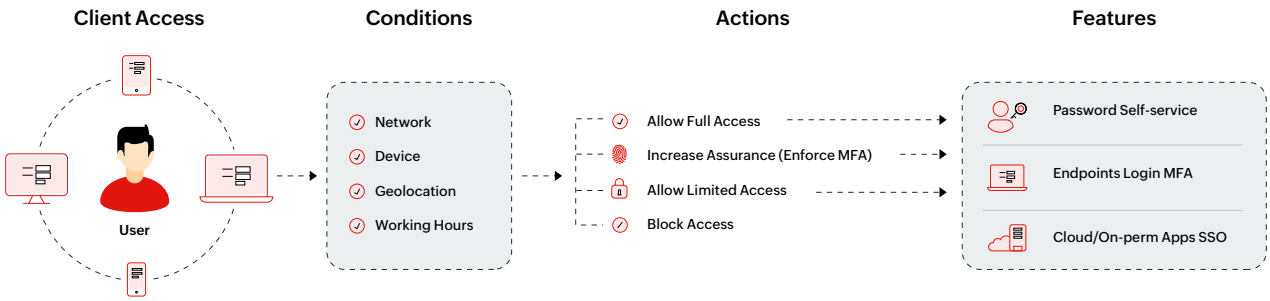
4.

Enhance security with contextual authentication

In today's remote-first organizational setup, the likelihood of a cyberattack is enormous. The context behind any login attempt, especially ones after failed attempts or from an unknown location or device, should be examined, and access should be provided only for those who don't pose any security threat to the organization.

For example, in many RDP attacks, threat researchers found the RDP server under attack received a barrage of authentication requests either from IP addresses that never connected to the network before or from locations that the company didn't have employees in. Had there been a mechanism to block such authentication requests, the attacks wouldn't have made it even to the second stage.

With AD360, organizations can analyze various risk factors, such as IP address, time of access, and device and user's geolocation, and configure conditional access policies based on them. IT admins can also create policies that check either one or all of the factors. Based on the risk, a user can be asked to prove their identity by submitting an additional authentication factor, be granted full or partial access, or be denied access.



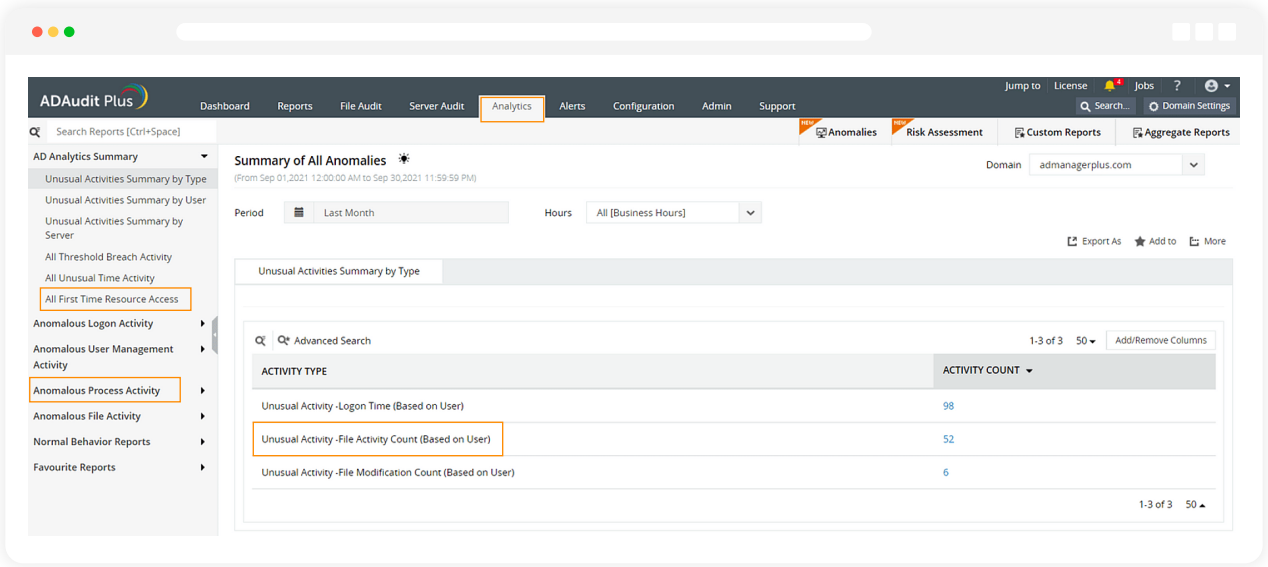
5.

Continuously monitor AD

When it comes to ransomware attacks, we know that threat actors will either download additional tools required for the attack after intrusion or introduce all the necessary tools as one single malware package. Once the malware is activated, it will certainly spring up new processes in the affected systems. Additionally, in attacks involving ransomware strains similar to Maze, data exfiltration attempts are also likely to happen. Such security threats can't be mitigated unless an organization continuously monitors their AD environment.

With AD360's AI-powered user behavior analytics, organizations can create a dynamic baseline for each user's activity and monitor any deviations that are abnormal for that particular user. Real-time alerts can be issued for various security threats, including:

- Malicious logins that are detected when a critical server is accessed for the first time or there is an unusual number of failed login attempts from an account.
- Privilege escalation attempts, such as a user exercising a privilege for the first time.
- Privilege abuse instances where a user has downloaded an unusually high amount of data.
- Attempts of data exfiltration or deletion.
- Discovery of unusual processes on a system in the network.



6.

Monitor privileged accounts, periodically review user access permissions, and revoke unnecessary privileges

Without access to privileged users, a ransomware attack cannot progress. That's why securing privileged users such as admins should be an organization's top priority when it comes to ransomware mitigation. Organizations should also ensure all users are granted access to resources only based on a least-privilege model. This type of model ensures that users don't accumulate unwanted privileges over time, a phenomenon that's common in most organizations today.

With AD360, organizations can:

- Audit all administrator activity, including changes to the AD schema, groups, and GPOs.
- Discover and manage permissions for all user accounts in the environment, and ensure temporary permissions are revoked automatically after a set period.

Footnotes

[1] 2020 Consumer Threat Landscape Report, Bitfender

[2] "Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031," Cybercrime Magazine

[3] Ransomware Threat Report 2021, Unit 42

[4] Cybersecurity in the Work From Anywhere Era, Yubico

About 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.

Download $ Get a quote