Prevent Active Directory password attacks: Steps and Tools

Presented by,
Jay Reddy | ManageEngine
Sr. Cybersecurity Strategist & IAM expert

ManageEngine IAM & Cybersecurity series
LIVE WEBINAR & SHOP TALK

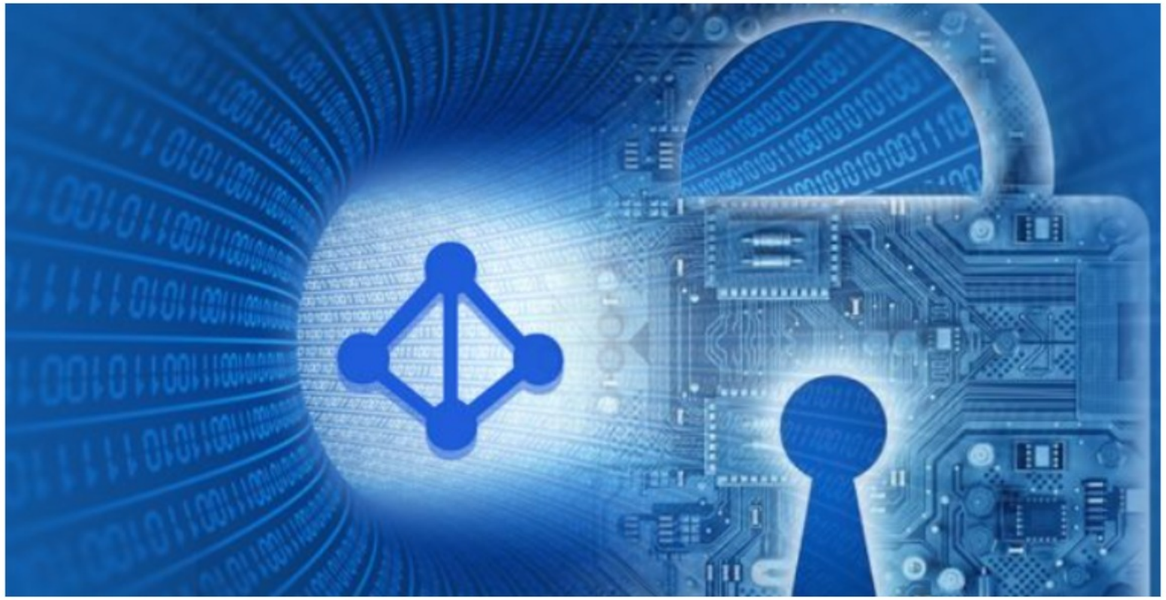
ManageEngine
AD360

Agenda

- Why focus on Active Directory (AD)?
- Aftermaths of a password breach
- Understanding why passwords are still threat actors' favorite target
- Two major passwords-related AD misconfigurations that are abused
- Attacks that exploit weak passwords
- Steps to protect passwords from the attacks
- How AD360 can help

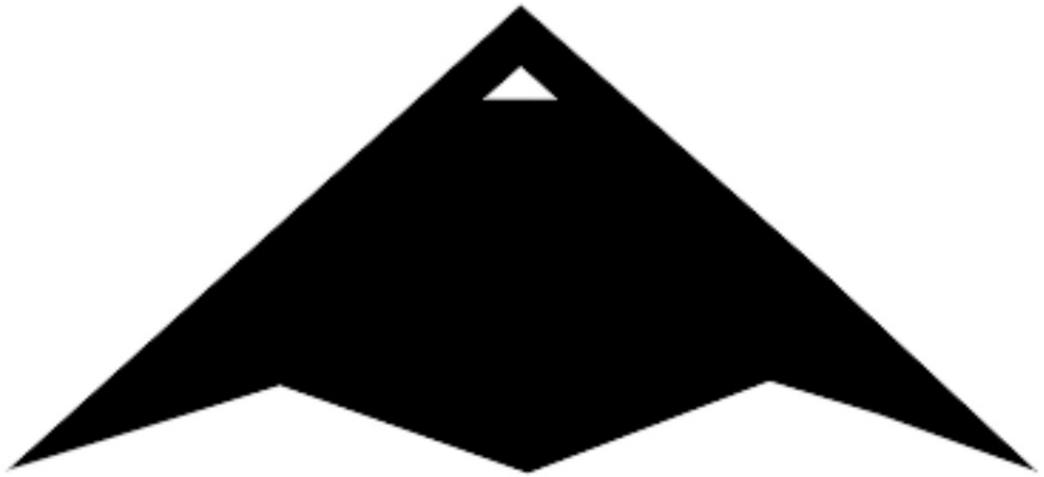
Why focus on Active Directory (AD)?

- Active Directory (AD) is widely used by organizations to manage their identities.
- Identity security has become synonymous with cybersecurity since the work-from-home environment became common place
- Once an attacker has access to your org's active directory, it’s game over.



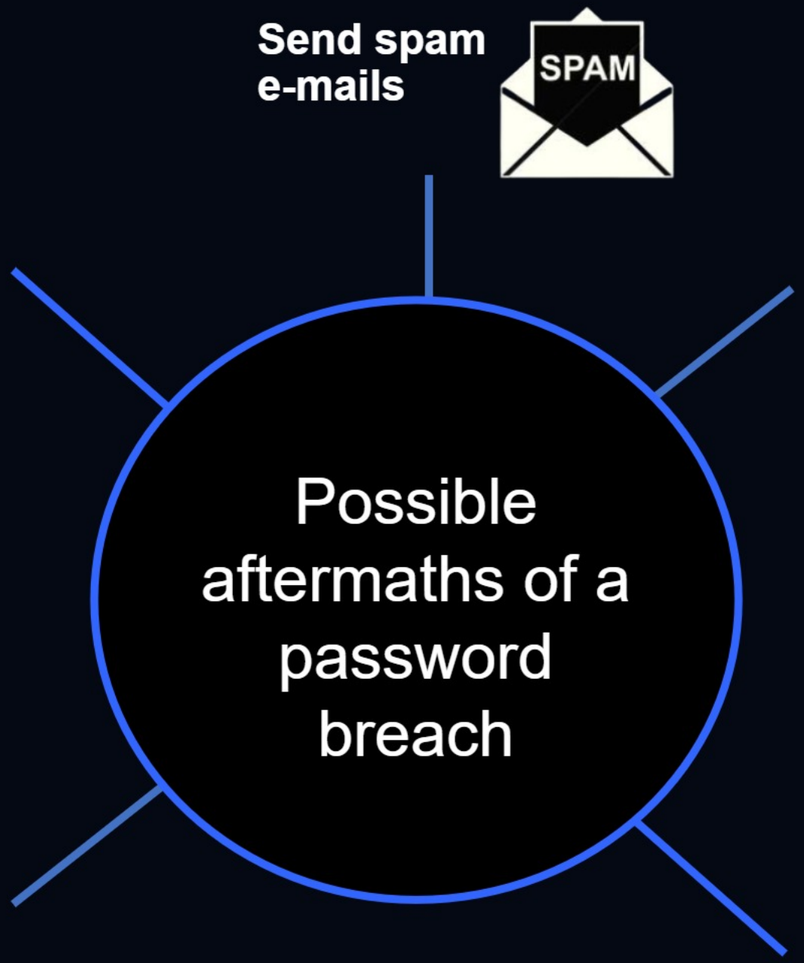
It’s not just about data exfiltration!

Once threat attackers gain access to AD, they tend to stay long to exploit all the loopholes within that particular AD infrastructure

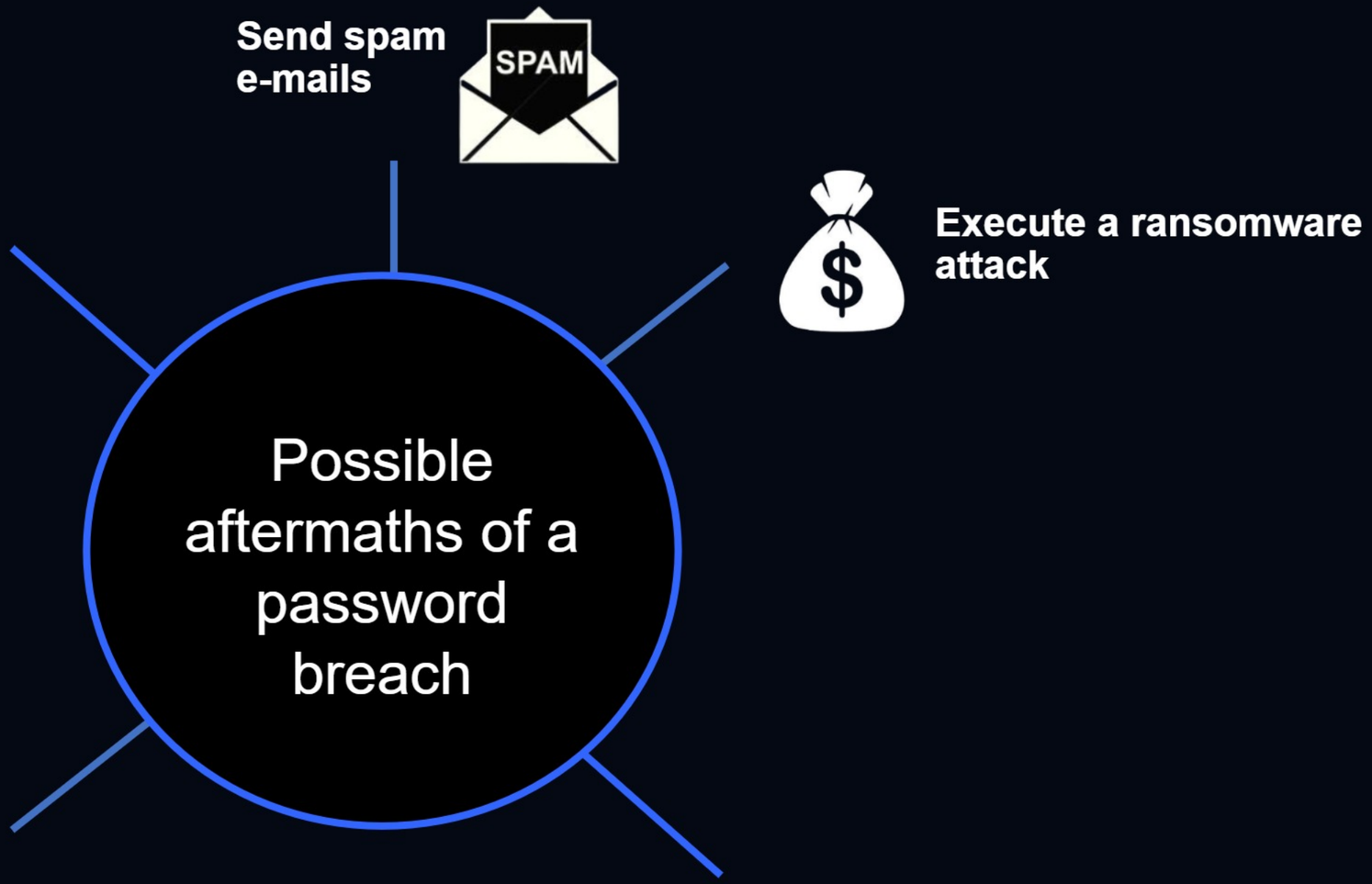


For instance, in 2018, attackers used a phishing attack to introduce Cobalt Strike Beacon, a malware, into an employee’s system. The same day they compromised a domain admin’s credentials and it used it for 63 days, the entire duration the malware campaign lasted.

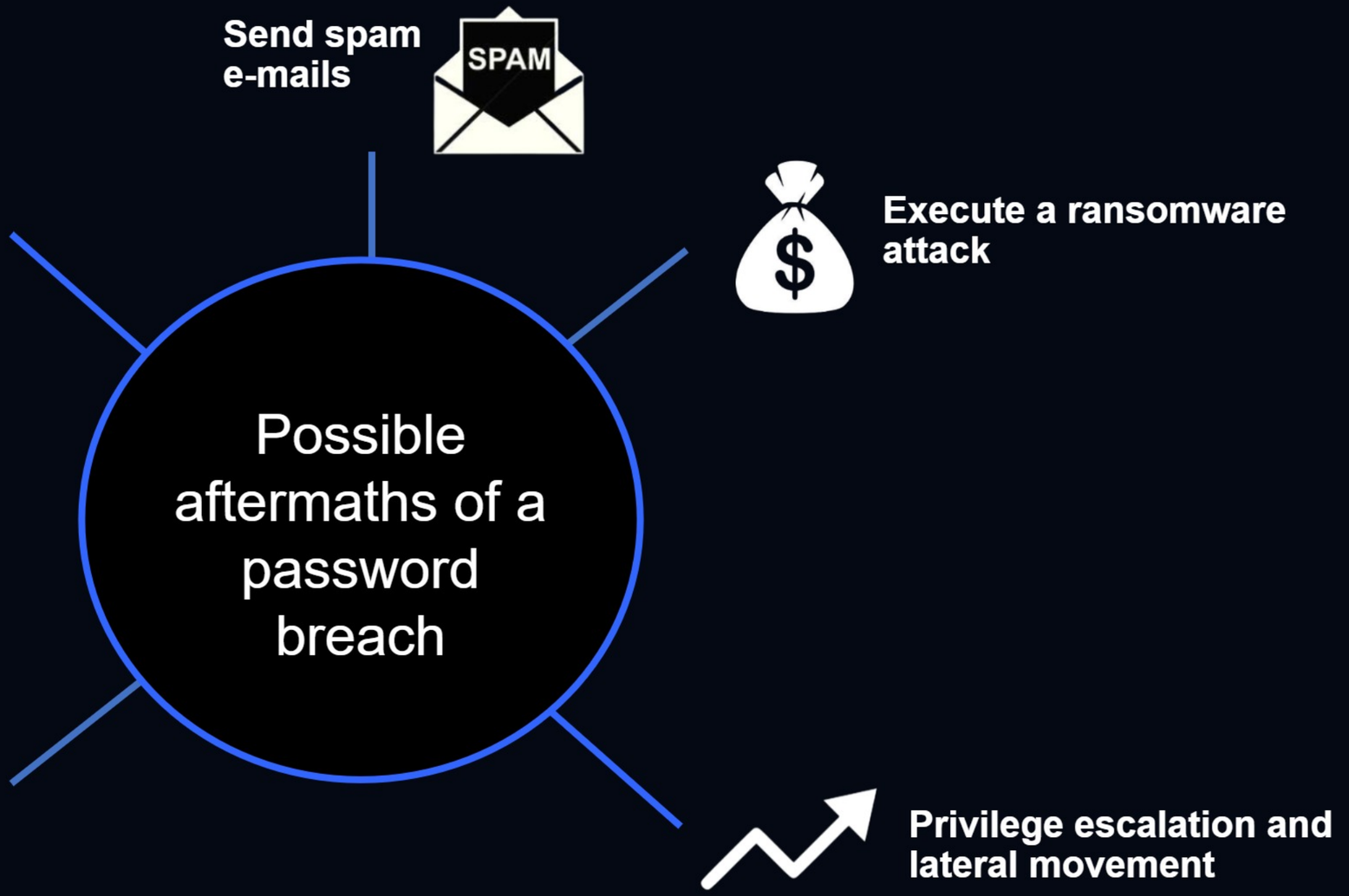
Endless possibilities



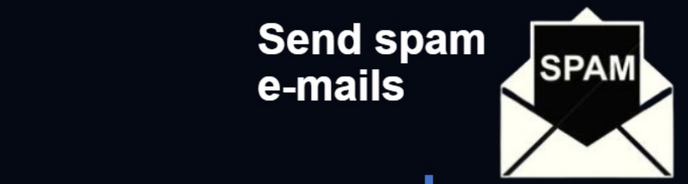
Endless possibilities



Endless possibilities



Endless possibilities



Send spam e-mails

Execute a ransomware attack

Possible aftermaths of a password breach

Compromise additional systems with malware

Privilege escalation and lateral movement

Endless possibilities

Possible aftermaths of a password breach

Send spam e-mails

Create backdoors for future check-ins

Execute a ransomware attack

Compromise additional systems with malware

Privilege escalation and lateral movement

Understanding why passwords are still threat actors' favorite target

1. Password reuse is rampant in organizations

65% of people reuse passwords for multiple or all accounts

Source: 2019 Google Security Survey

Dropbox employee's password reuse led to theft of 60M+ user credentials

Kate Conger, Matthew Lynley / 7:47 AM GMT+5:30 • August 31, 2016 Comment

CPO CPO Magazine

Breach of Dating App Mobifriends Highlights the Ongoing Problem of Password Reuse

3.68 million Mobifriends users have had just about all of the information associated with their accounts, including their passwords, leaked to the ...

18-May-2020

8/19/2020
10:00 AM

Stolen Data: The Gift That Keeps on Giving

Users regularly reuse logins and passwords, and data thieves are leveraging that reality to breach multiple accounts.

Understanding why passwords are still threat actors' favorite target

2. Looks like weak passwords are here to stay

81% of all data breaches were caused to weak or stolen credentials

Source: Verizon's 2020 Data Breach Investigation Report

2020's top 10 most common passwords include 123456, 123456789, picture1, password, and so on

Source: NordPass' top 200 list of common passwords, 2020

Understanding why passwords are still threat actors' favorite target

3. Password fatigue perpetuates use of weak passwords and password reuse

A person has to remember over 90 passwords!

Source: Study by Dashlane

Two major password-related Active Directory misconfigurations that are abused

1. Local administrator accounts

USES

Offers extensive control over files, folders, and services in that select local computer and also enable management of rights and permissions to users

Are the only way in, when network authentication fails i.e. when the device is unable to communicate with the DC

Two major password-related Active Directory misconfigurations that are abused

1. Local administrator accounts

USES

Offers extensive control over files, folders, and services in that select local computer and also enable management of rights and permissions to users

Are the only way in, when network authentication fails i.e. when the device is unable to communicate with the DC

PITFALLS

Many organizations tend to have one common password for all local admin accounts across the organization

In most AD attacks, lateral movement originate from compromised local admin accounts

Two major password-related Active Directory misconfigurations that are abused

2. Service accounts

USES

Highly-privileged local or domain accounts that aren't related to a human identity and are used to run applications that interact with the operating system.

Used to run applications, virtual machine instances, and support the smooth operation of various processes.

Two major password-related Active Directory misconfigurations that are abused

2. Service accounts

USES	PITFALLS
Highly-privileged local or domain accounts that aren't related to a human identity and are used to run applications that interact with the operating system.	Most service accounts are configured with weak and non-expiring passwords.
Used to run applications, virtual machine instances, and support the smooth operation of various processes.	Temporary service accounts that are created for installing a particular software are often left unchecked, sometimes even with default passwords.

Three attacks that exploit weak passwords

- Remote Desktop Protocol brute force attacks
- Cracking passwords of domain users using password spray attack
- Spear-phishing campaigns to get hold of AD passwords

Brute force attacks

- A guessing attack in which attackers try out either just passwords or combinations of usernames and passwords until the target account is compromised
- A go-to attack for threat actors as it's low-cost and requires very basic technological know-how.
- Threat actors often use automated tools to execute brute force attacks. Mostly they are purchased from the darkweb. Those looking to carry out sophisticated attack build their own tools.

Types of brute force attacks

Dictionary attacks

A combination of words and phrases are supplied as guesses. Previously, only words taken from a dictionary along with some numbers were used, but today it also includes data from leaked breaches.

Simple brute force attack

Uses automation and scripts to crack passwords. Simple passwords with made of upper and lower case letters can be cracked in few mins

Hybrid attacks

A combination of dictionary and simple brute force attack. Guesses are made of words and numbers. Usually the word part is initially kept constant, while the numbers in the password are automated to rotate.

Credential stuffing attacks

Stolen login credentials available in the dark web are used to carry out attacks. Success rate is high as many reuse passwords across platforms

Password Spraying

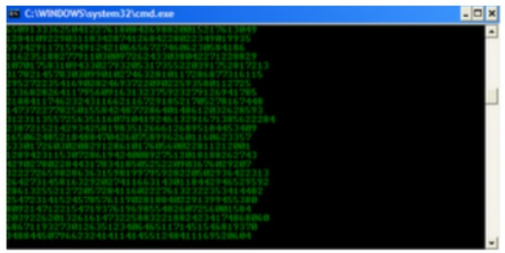
Exact opposite to the traditional brute force attack that tries out multiple passwords for a single account. Here, one password is tried against multiple accounts.

1. The RDP brute force attack

- One of the most common methods used to attack windows systems and infect them with malware.
- System’s weak passwords and RDP ports left open to the internet are exploited in the attack.
- The method is so successful that there are ransomware groups like SamSam and Dharma (aka Crysis) that solely use the RDP open ports to spread ransomware.

Anatomy of a RDP brute force attack

Attackers use scanning tools such as Nmap and Massscan to identify open RDP ports (port 3389).

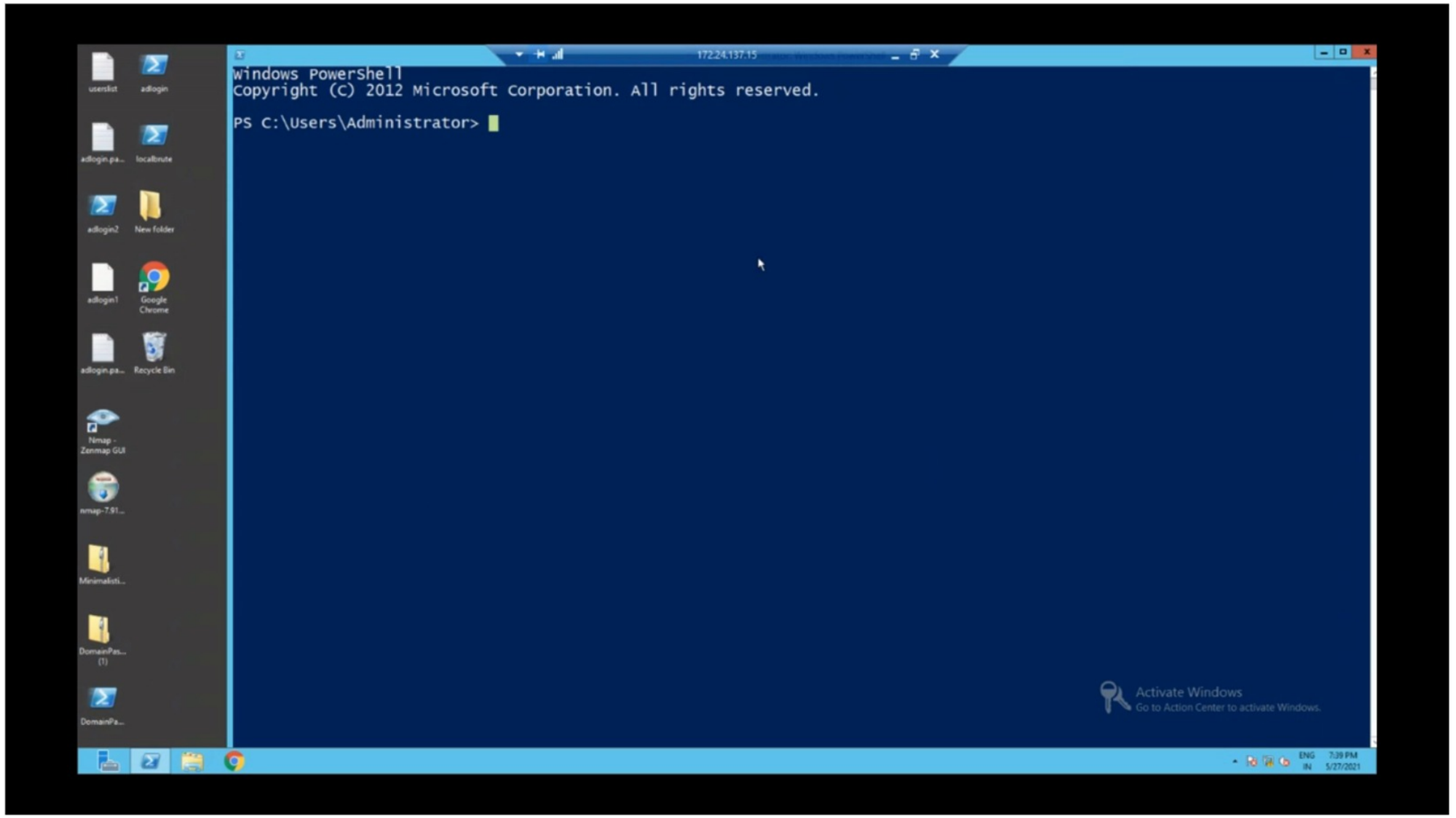


Weak credentials are cracked through a brute force technique. Tools used: Crowbar, eampd5pass, or known_hosts_bruteforcer.

After gaining access to the system, it's infected with ransomware or other malware.

Brute force attack demo

Now that we've seen how threat actors exploit open RDP let's look at a brute force attack demo



2. Cracking passwords of domain users using a password spray attack

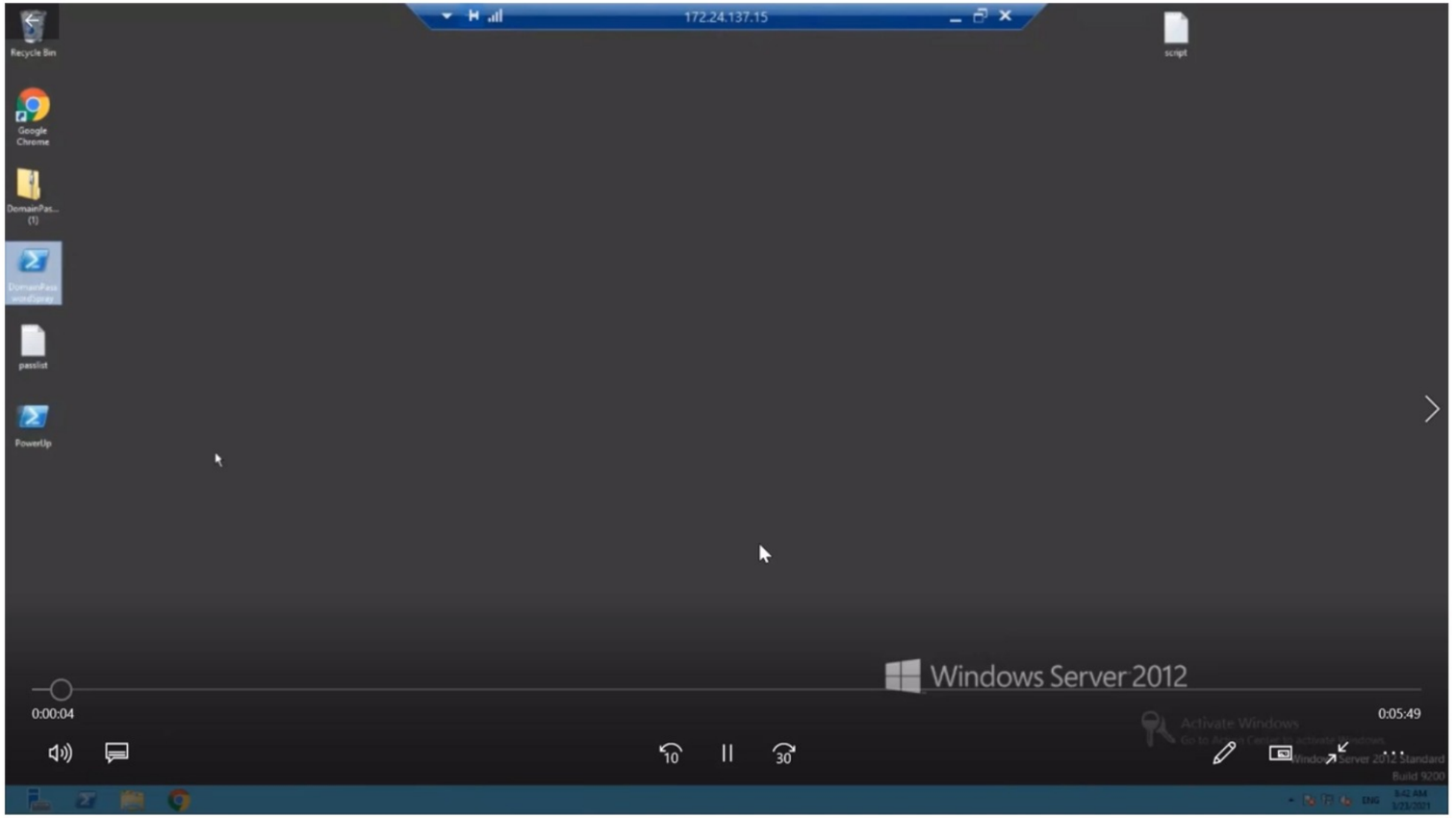
- Even passwords that satisfy the length and complexity criteria can be cracked using password spraying as often they are predictable. Most tend to have numbers towards the end, or their birth year or common keyboard patterns as past of their passwords.

- Password spray attacks slip under the radar because during an attack they are unlikely to disturb lockout policy and logon attempts restrictions in place.

- Common password spray tools: domainpasswordspray.ps1, BurpSuite, spray.sh, Crackmapexec, Hydra and Metasploit: SMB Login

2. Cracking passwords of domain users using a password spray attack

- Password spray demo



3. The Spear Phishing campaign that validates credentials in real-time using Active Directory

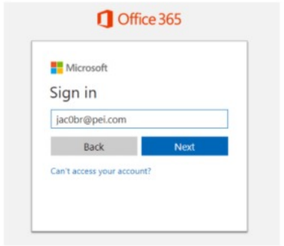
- Spear phishing attacks are nothing but granular phishing attacks with personalized messages targeted at a small recipient group. Though they contain a malicious link, they are hard to discard as spam as they are filled with details like the names, places, or terms that the recipient is extremely familiar with.

- Attackers leverage information available on the target's social media accounts and other public sites such as a company website, to create personalized messages.

3. The Spear Phishing campaign that validates credentials in real-time using Active Directory

Researchers at Armorblox discovered a unique phishing attack that cross-verified O365 credentials entered on the phishing page against the organization's Azure AD infrastructure.

Attackers sent a phishing email containing fake payment remittance report through Amazon simple email service.



On opening the mail, recipients were taken to a O365 look-alike page with a message, "Because you're accessing sensitive info, you need to verify your password" and their email ids were already filled in.

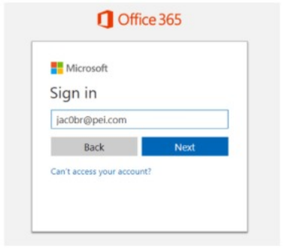
When the user entered a password, an O365 API call was triggered to instantly verify the login credentials with the organization's Azure AD infrastructure.

If successful, the user was redirected to zoom.com, to create a diversion.

If unsuccessful, the user was redirected to login.microsoftonline.com to mask the phishing attempt as failed login

3. The Spear Phishing campaign that validates credentials in real-time using Active Directory

Attackers sent a phishing email containing a fake payment remittance report through Amazon simple email service



On opening the mail, recipients were taken to a O365 look-alike page with a message, “Because you're accessing sensitive info, you need to verify your password” and their email ids were already filled in

When the user entered a password, an O365 API call was triggered to instantly verify the login credentials with the organization’s Azure AD infrastructure

If successful, the user was redirected to zoom.com, to create a diversion

If unsuccessful, the user was redirected to login.microsoftonline.com to mask the phishing attempt as a failed login

Why it’s a unique attack: Since attackers could get their hands on the valid credentials instantaneously, they can compromise the account even before the victim becomes aware of a breach.

Steps to protect your passwords from these attacks

For brute force attacks:

- Disable access after multiple failed login attempts.
- Set password refresh cycles (30 or 90 days) depending on organization needs.
- Prevent use of dictionary and breached passwords.
- Enforce setting up of passphrases instead of increasing complexity if length is too long.
- Deploy MFA.
- Monitor number of failed logon attempts.
- Configure conditional access for highly privileged accounts, especially IT admins.

For password spray attacks:

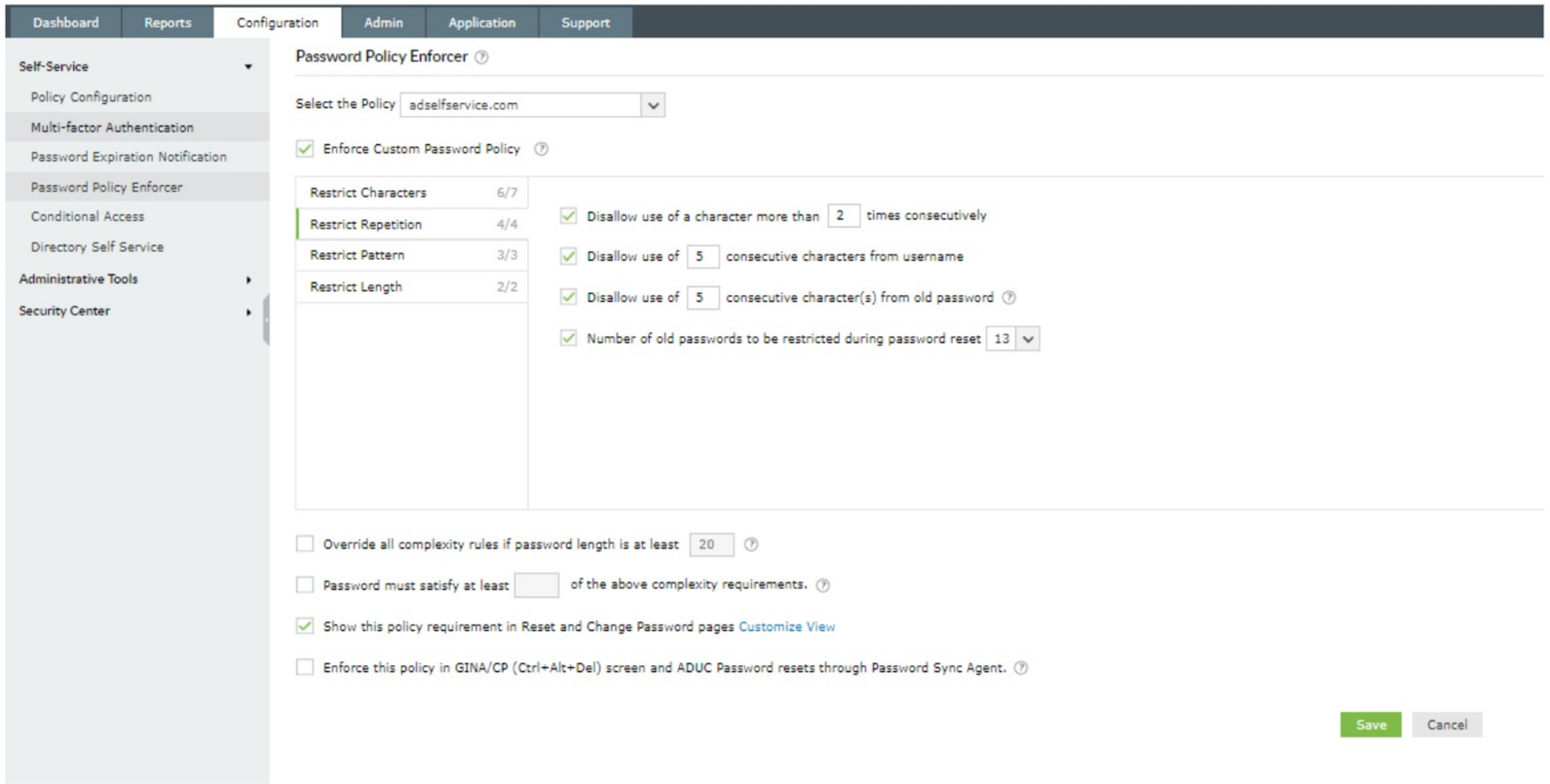
- Prevent users from setting up predictable passwords including keyboard sequences and palindromes.
- Set stringent password policies.
- Prevent password reuse
- Deploy MFA.
- Configure conditional access for highly privileged accounts, especially IT admins.

For phishing attacks:

- Deploy MFA.
- Train employees such that they don't impulsively click on links that urge them to take a rapid action.
- Implement e-mail filters that leverage machine learning and natural language processing to flag high-risk emails.
- Patch all remote services and VPNs.
- Configure conditional access for highly privileged accounts, especially IT admins.

How AD360 can help you implement the recommendations

Restrict users from reusing old passwords during password reset

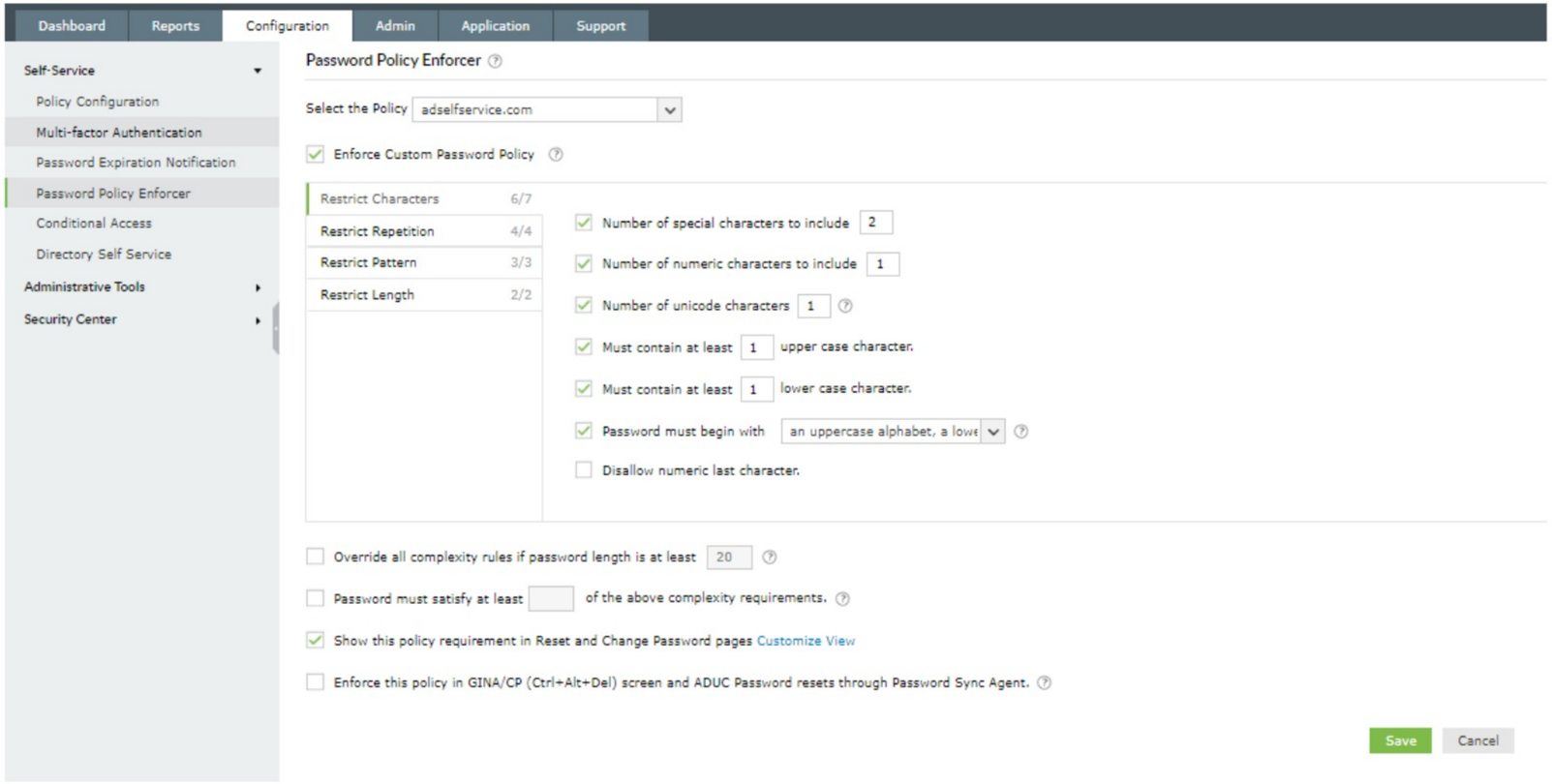


How AD360 can help you implement the recommendations

Enforce strong custom password policies

IT admins can ensure one or more of these rules are followed when the password is set:

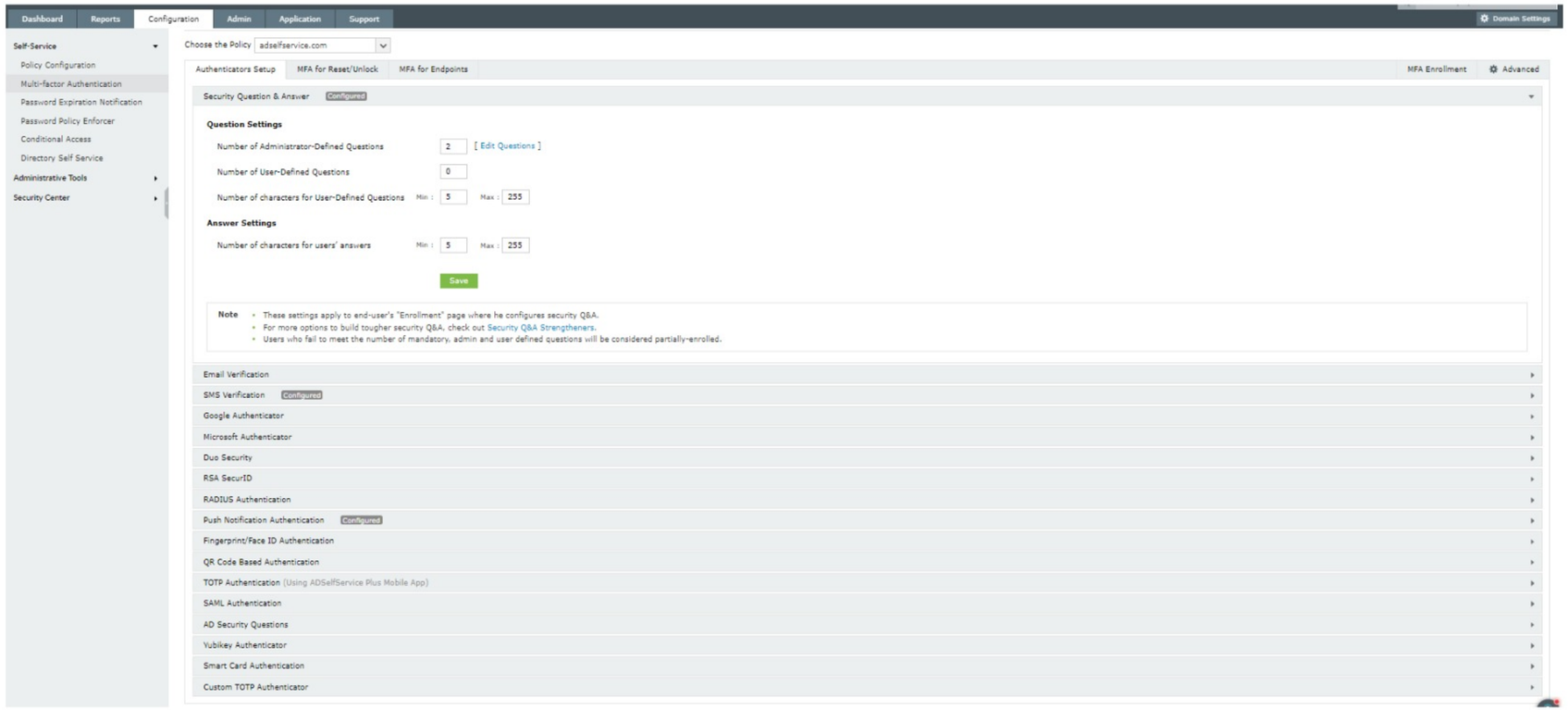
- Meets a minimum length
- Includes both upper and lower case letters
- Includes special characters
- Includes numbers
- Requires that the password begin with either a letter, a number, or a special character
- **Blocks dictionary words, or patterns** that are easy to crack
- **Creates a custom list of weak passwords** which new password resets will be checked against
- **Prevents the use of breached passwords through an integration with the "Have I been Pwned?" service** that checks passwords against a continuously updated list of compromised passwords



How AD360 can help you implement the recommendations

Enable MFA for workstations, applications, and self-service features

- Support for over 15 authentication techniques, including YubiKey authentication, biometrics, and RSA SecurID
- Secure local and remote access of your organization's Windows, Mac, and Linux endpoints
- Safeguard access to SSO-enabled applications
- Ensure users can use the self-service password reset or account unlock features only after their identity is verified.



How AD360 can help you implement the recommendations

Enable risk-based conditional access based on IP address, device type, and login times and geolocation

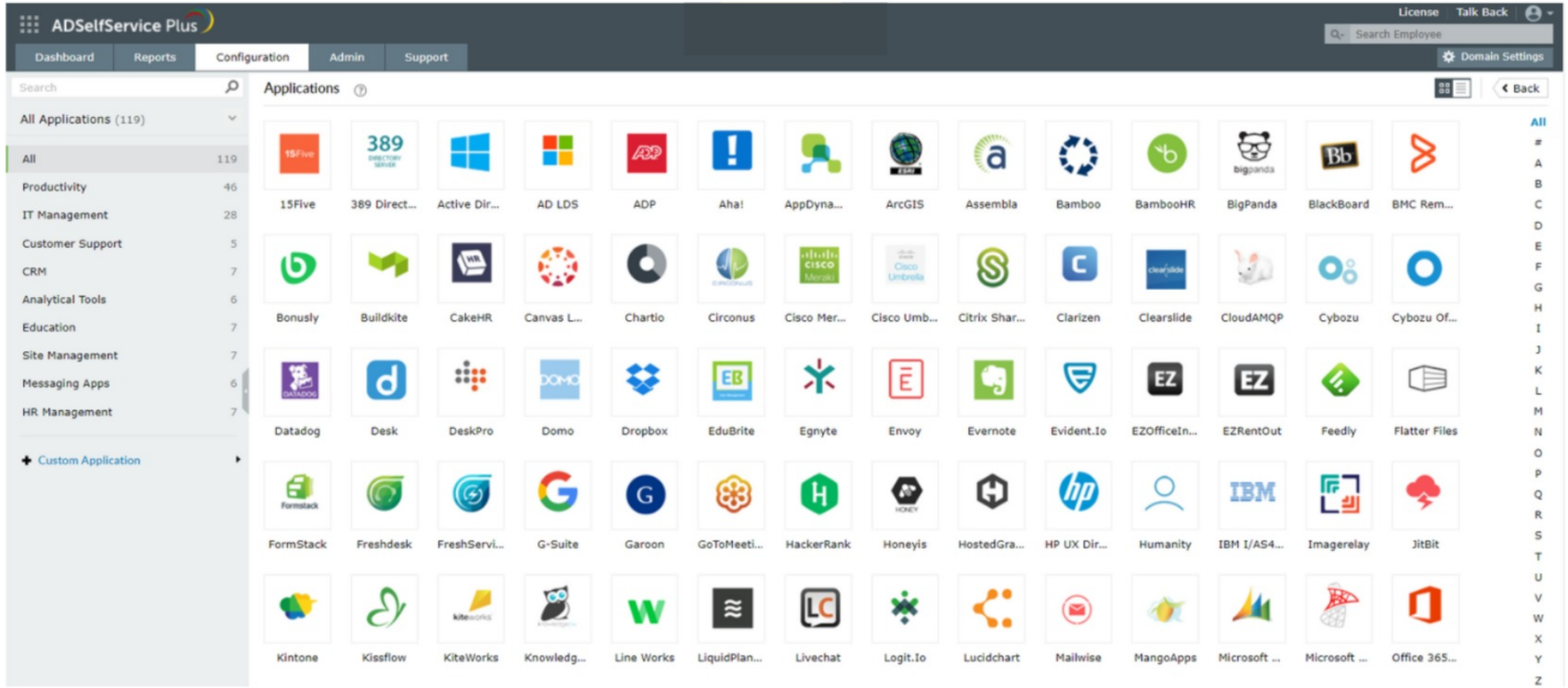
Scenarios

- Mandating biometric authentication during **IT admin logins.**
- **Allowing access from authorized machines only** to important applications through single sign-on (SSO).
- **Enforcing three levels of authentication for password reset requests from untrusted IPs,** or from computers that are not joined to the domain.

How AD360 can help you implement the recommendations

Set up SSO for your applications

- Manage access to all applications with one click from a single dashboard
- Secure access with MFA
- Create application access policies based on AD organizational units (OUs) and groups.



How AD360 can help you implement the recommendations

Prevent and mitigate security threats with User Behavior Analytics (UBA)

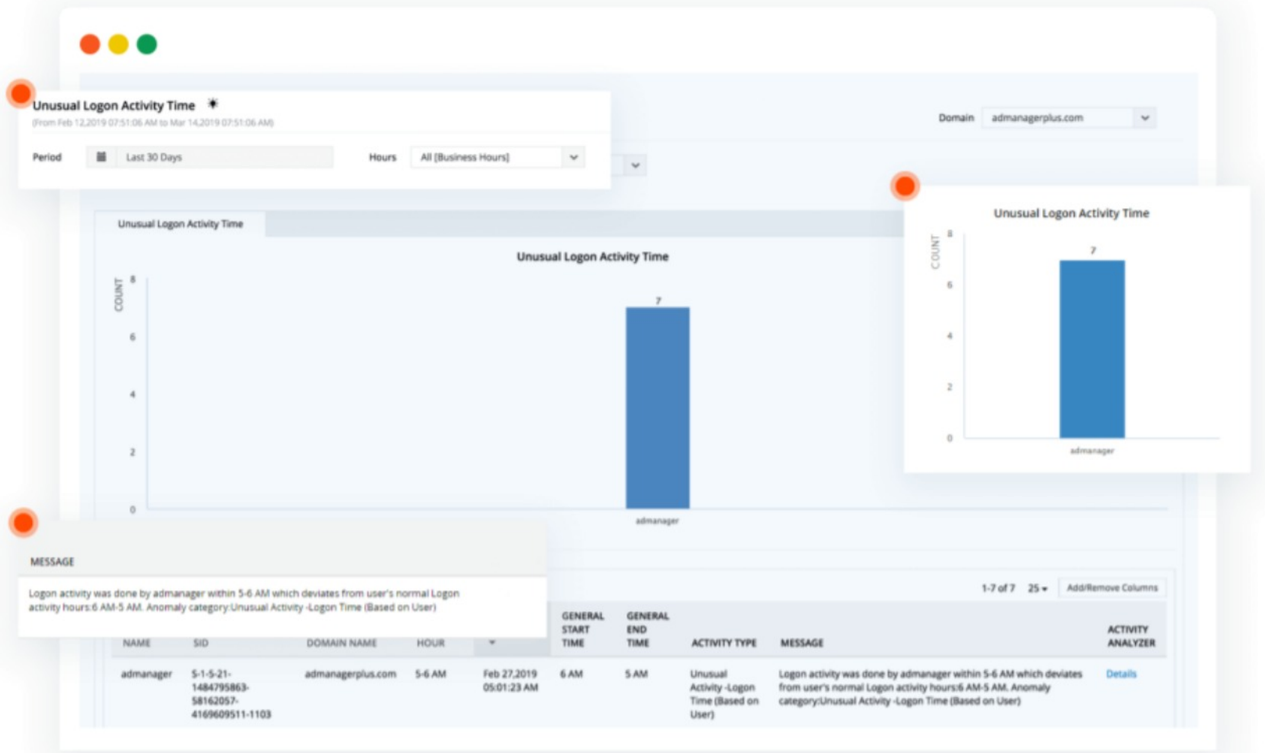
Applying machine learning, AD360 creates a baseline of normal behavior specific to each user and alerts about deviations from this norm.

Type of alerts

- **Unusual Count:** If a user's activity or file activity count exceeds a dynamic threshold.
- **Unusual Time:** Any activity occurs after the calculated normal activity hours.
- **New resource access:** If a new resource was accessed. E.g., a new user access on a computer, new remote to a server from a client, or a new process ran on a server.

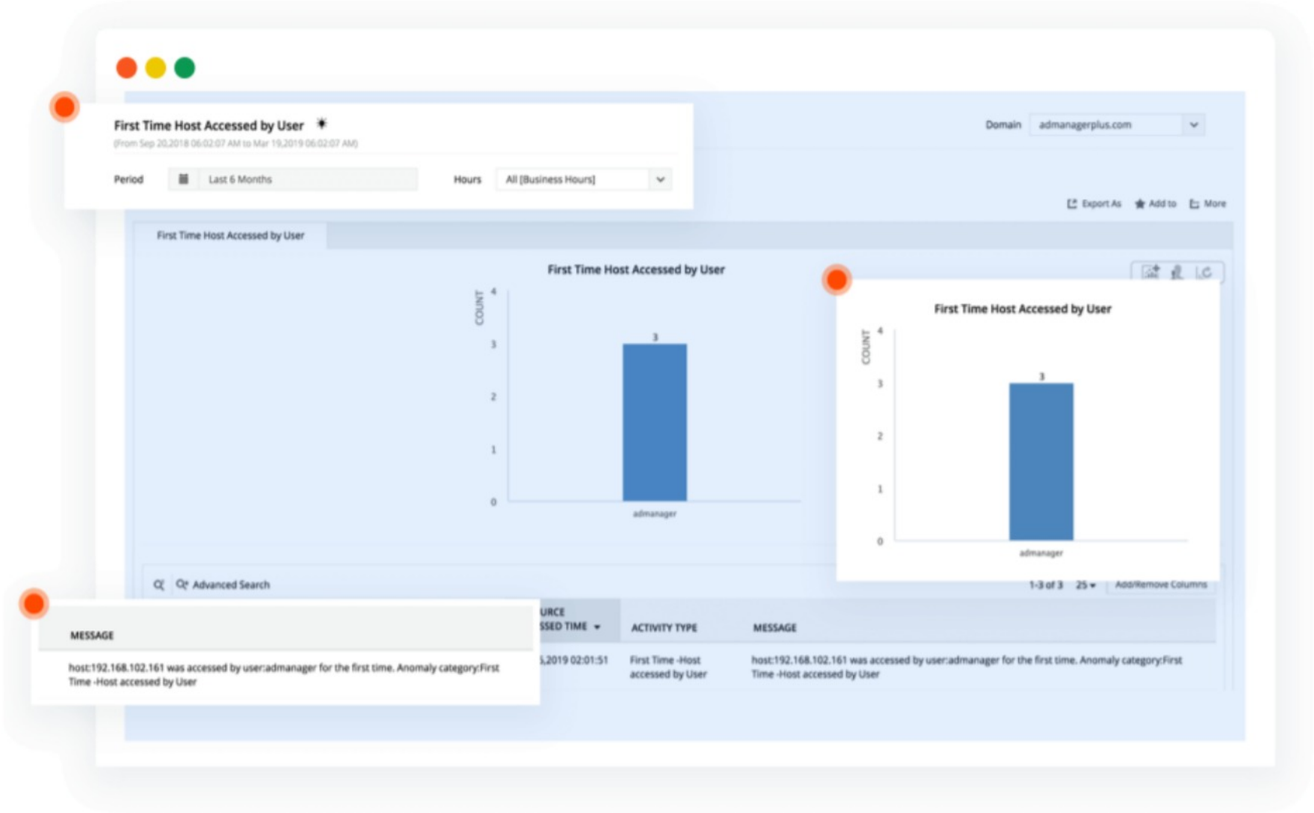
How AD360 can help you implement the recommendations

Unusual logon activity



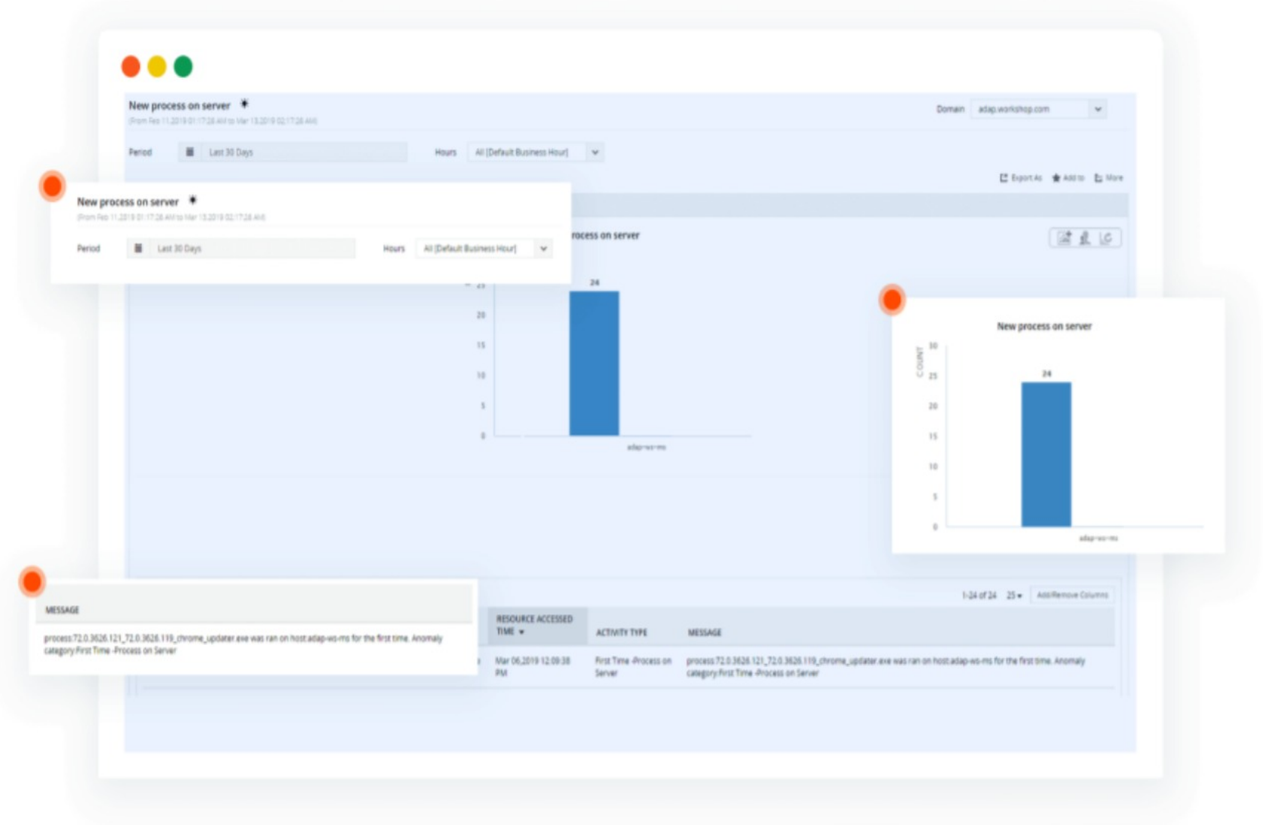
How AD360 can help you implement the recommendations

Detect lateral movement



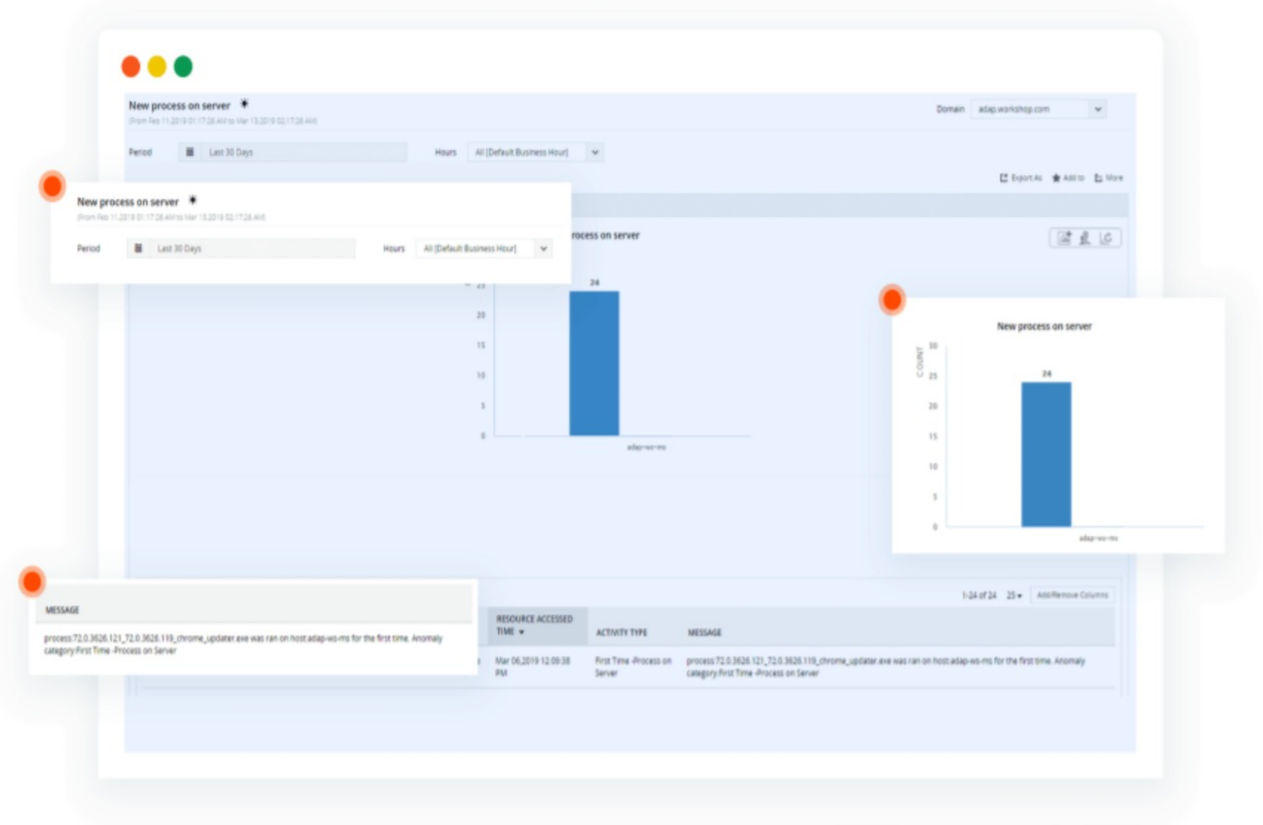
How AD360 can help you implement the recommendations

Thwart malware attacks

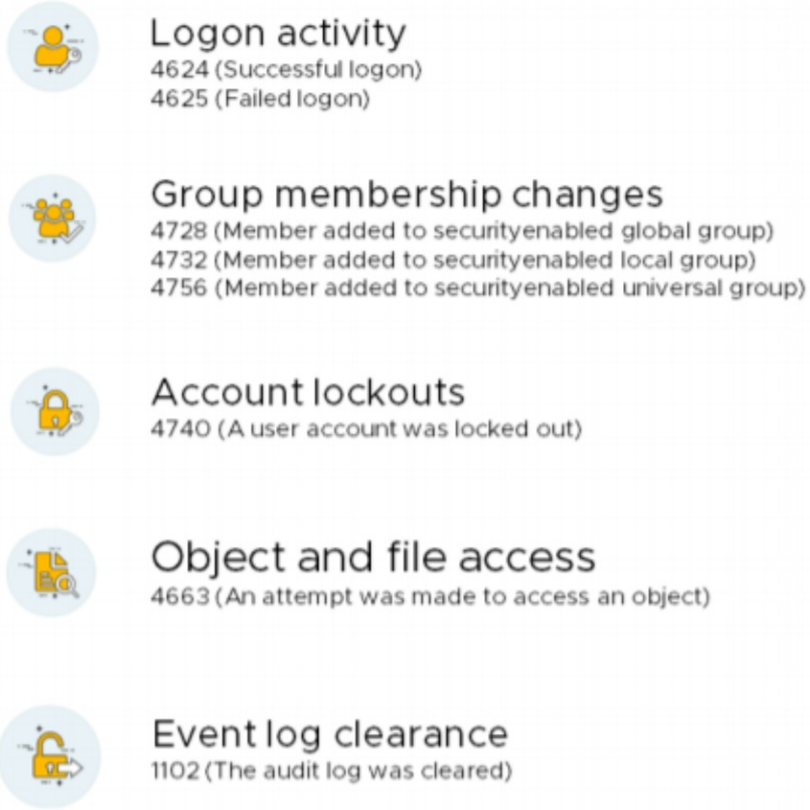


How AD360 can help you implement the recommendations

Track privilege abuse



How AD360 can help you implement the recommendations



Track and report key AD events in your network

Thank you.

Write to me for the resources

jayreddy@manageengine.com

ManageEngine

www.manageengine.com