CionSystems

Next Generation Enterprise Identity Management (EIM)™

THE SECRETS OF HARDENING ACTIVE DIRECTORY

eBook

by Zubair Ansari, ADGuru & CEO

CionSystems, Inc.

www.cionsystems.com

Contents

Introduction

Every enterprise, small and large, REQUIRES Directory Services (Microsoft AD, Novell E-directory, Sun, Oracle, etc.).

Over 90% of all businesses have chosen to deploy Active Directory. It is difficult to give restricted access to enterprise resources in the Cloud.

Provisioning and de-provisioning of Users and Access to mission-critical enterprise applications is extremely complex.

Lack of easy, auditable change management and reporting for identity, access, and authentication of users and applications leave too many open doors for hackers.

Since 2020, Active Directory became the #1 target of exploitation so that hackers and cybercriminals could gain access to privileged accounts for lateral movement, planting backdoors, deploying ransomware, and taking over computer networks, remotely.

Managing Enterprise Active Directory (AD) is STRESSFUL!

In this ebook, we will cover the major vulnerabilities and methods hackers and cybercriminals use to exploit Active Directory.

Then, we'll go over the best practices to dramatically reduce this risk by "Battleship" hardening your Active Directory servers.

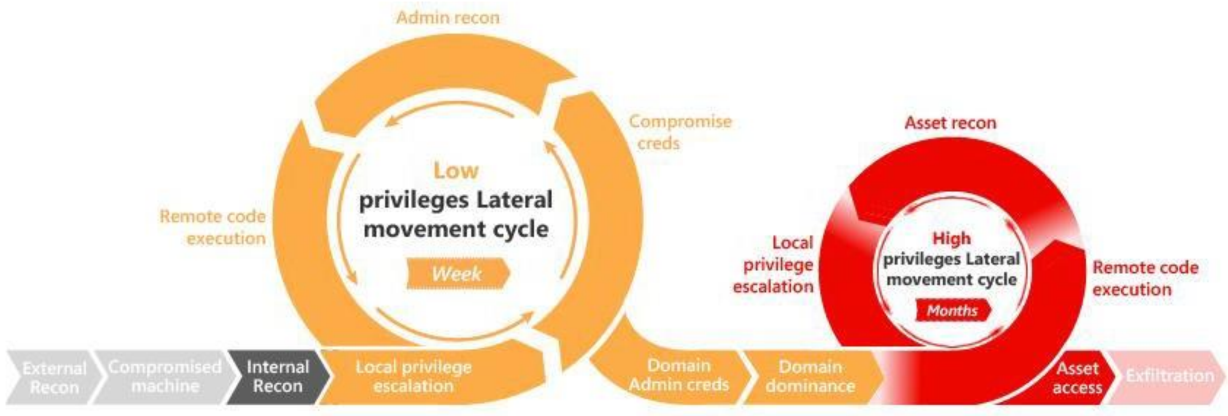
Let's get started…

Exploiting Active Directory Weaknesses

Like most hacking methodologies, attacking Active Directory is done in the following manner:

1. Reconnaissance
2. Domain Enumeration
3. Local Privilege Escalation
4. Local Account Stealing
5. Monitor Potential Incoming Account
6. Local Account Stealing
7. Admin Reconnaissance
8. Lateral Movement
9. Remote Administration
10. Domain Admin Privileges
11. Cross Trust Attacks
12. Persistence and Exfiltration

The Active Directory Kill-Chain looks like this:



While it might take a hacker a week or more to break in, escalate privileges and move around an organization, remotely, exploring usernames, permissions, profiles, file sharing, group policies and much more, this happens all the time now and is usually unseen by the IT Staff, until it is too late. The average detection time of a breach is usually many months, not days or hours or minutes or what it should be – seconds. While I don't want to provide techniques to hack, I do want you to understand how easily these tools are accessed and how powerful the exploits against Active Directory can be, so as you look at the following list and consider clicking through to the GITHUB repository for more information on these attack methods, I only recommend you see them and use them for professional or legal purposes, with integrity. This will help you understand how weak and vulnerable Active Directory can be, based on misconfigurations, poor password and group policies and lack of frequent audits and system hardening. Do not use this information for criminal or illegal purposes and always get permission to perform penetration testing from the owner of the assets.

Active Directory Hacking Cheat Sheet:

- /A - Recon
- /B - Domain Enum
- /C - Local Privilege Escalation
- /D - User Hunting
- /E - Monitor Potential Incoming Account
- /F - BloodHound
- /G - Lateral Movement
- /H - Persistence
- /I - Domain Admin Privileges
- /J - Cross Trust Attacks
- /K - Database Hunting
- /L - Security Downgrade
- /M - Privileged Accounts and Groups in Active Directory
- /N - Data Exfiltration
- /O - Looting
- /P - .NetPayload
- /X - Reverse PSShell FUD
- /Y - UL-DL-EXEC Skills
- /Z - Tool Box

Example: Reconnaisance Tools and Techniques

POWERSHELL SCAN

PORT SCAN

```
Import-Module Invoke-Portscan.ps1
<#
Invoke-Portscan  -Hosts  "websrv.domain.local,wsus.domain.local,apps.domain.local"  -
TopPorts 50
echo websrv.domain.local | Invoke-Portscan -oG test.gnmap -f -ports "80,443,8080"
Invoke-Portscan -Hosts 172.16.0.0/24 -T 4 -TopPorts 25 -oA localnet
#>
```

AD MODULE WITHOUT RSAT

The secret to being able to run AD enumeration commands from the AD Powershell module on a system without RSAT installed, is the DLL located in **C:\Windows\Microsoft.NET\assembly\GAC_64\Microsoft.ActiveDirectory.Management** on a system that has the RSAT installed.

Set up your AD VM, install RSAT, extract the dll and drop it to the target system used to enumerate the active directory.

```
Import-Module .\Microsoft.ActiveDirectory.Management.dll
Get-Command get-adcom*
```

GENERAL FUNCTIONS OF POWERVIEW

Misc Functions:

```
Export-PowerViewCSV             #  thread-safe CSV append
Set-MacAttribute                  # Sets MAC attributes for a file based on another
file or input (from Powersploit)
Copy-ClonedFile                 # copies a local file to a remote location, matching
MAC properties
Get-IPAddress                   #  resolves a hostname to an IP
Test-Server                     #  tests connectivity to a specified server
Convert-NameToSid                  # converts a given user/group name to a security
identifier (SID)
Convert-SidToName              #  converts a security identifier (SID) to a group/user
name
Convert-NT4toCanonical           # converts a user/group NT4 name (i.e. dev/john) to
canonical format
Get-Proxy                       #  enumerates local proxy settings
```

```
Get-PathAcl                     # get the ACLs for a local/remote file path with
optional group recursion
Get-UserProperty               # returns all properties specified for users, or a
set of user:prop names
Get-ComputerProperty           #  returns all properties specified for computers, or
a set of computer:prop names
Find-InterestingFile          #  search a local or remote path for files with specific
terms in the name
Invoke-CheckLocalAdminAccess      #   check  if  the  current  user  context  has  local
administrator access to a specified host
Get-DomainSearcher              # builds a proper ADSI searcher object for a given
domain
Get-ObjectAcl                  # returns the ACLs associated with a specific active
directory object
Add-ObjectAcl                  # adds an ACL to a specified active directory object
Get-LastLoggedOn               # return the last logged on user for a target host
Get-CachedRDPConnection        # queries all saved RDP connection entries on a target
host
Invoke-ACLScanner                 # enumerate -1000+ modifable ACLs on a specified
domain
Get-GUIDMap                      # returns a hash table of current GUIDs -> display
names
Get-DomainSID                  #  return the SID for the specified domain
Invoke-ThreadedFunction          # helper that wraps threaded invocation for other
functions
```

net * Functions:

```
Get-NetDomain                  #  gets the name of the current user's domain
Get-NetForest                  #  gets the forest associated with the current user's
domain
Get-NetForestDomain            #  gets all domains for the current forest
Get-NetDomainController            #   gets  the  domain  controllers  for  the  current
computer's domain
Get-NetUser                      # returns all user objects, or the user specified
(wildcard specifiable)
Add-NetUser                    #  adds a local or domain user
Get-NetComputer                #  gets a list of all current servers in the domain
Get-NetPrinter                  #  gets an array of all current computers objects in
a domain
Get-NetOU                      #  gets data for domain organization units
Get-NetSite                    #  gets current sites in a domain
Get-NetSubnet                  #  gets registered subnets for a domain
Get-NetGroup                   #  gets a list of all current groups in a domain
Get-NetGroupMember               # gets a list of all current users in a specified
domain group
Get-NetLocalGroup               # gets the members of a localgroup on a remote host
or hosts
Add-NetGroupUser                 # adds a local or domain user to a local or domain
group
Get-NetFileServer               # get a list of file servers used by current domain
users
Get-DFSshare                  #  gets a list of all distribute file system shares on
a domain
```

```
Get-NetShare                    #  gets share information for a specified server
Get-NetLoggedon                 #  gets users actively logged onto a specified server
Get-NetSession                  #  gets active sessions on a specified server
Get-NetRDPSession                 # gets active RDP sessions for a specified server
(like qwinsta)
Get-NetProcess                   # gets the remote processes and owners on a remote
server
Get-UserEvent                   #  returns logon or TGT events from the event log for
a specified host
Get-ADObject                    # takes a domain SID and returns the user, group, or
computer object associated with it
Set-ADObject                     #  takes a SID, name, or SamAccountName to query for
a specified domain object, and then sets a pecified 'PropertyName' to a specified
'PropertyValue'
```

GPO functions:

```
Get-GptTmpl                     #  parses a GptTmpl.inf to a custom object
Get-NetGPO                      #  gets all current GPOs for a given domain
Get-NetGPOGroup                   # gets all GPOs in a domain that set "Restricted
Groups" on on target machines
Find-GPOLocation                  # takes a user/group and makes machines they have
effectiverights over through GPO enumeration and correlation
Find-GPOComputerAdmin          # takes a computer and determines who has admin rights
over itthrough GPO enumeration
Get-DomainPolicy                #  returns the default domain or DC policy
```

User-Hunting Functions:

```
Invoke-UserHunter               # finds machines on the local domain where specified
users are logged into, and can optionally check if the current user has local admin
access to found machines
Invoke-StealthUserHunter             #  finds all file servers utilizes in user
HomeDirectories, and checks the sessions one each file server, hunting for particular
users
Invoke-ProcessHunter             # hunts for processes with a specific name or owned
by a specific user on domain machines
Invoke-UserEventHunter            # hunts for user logon events in domain controller
event logs
```

Domain Trust Functions:

```
Get-NetDomainTrust              #  gets all trusts for the current user's domain
Get-NetForestTrust              # gets all trusts for the forest associated with the
current user's domain
Find-ForeignUser               #  enumerates users who are in groups outside of their
principal domain
Find-ForeignGroup              #  enumerates all the members of a domain's groups and
finds users that are outside of the queried domain
Invoke-MapDomainTrust             # try to build a relational mapping of all domain
trusts
```

MetaFunctions:

```
Invoke-ShareFinder               # finds (non-standard) shares on hosts in the local
domain
Invoke-FileFinder                # finds potentially sensitive files on hosts in the
local domain
Find-LocalAdminAccess           # finds machines on the domain that the current user
has local admin access to
Find-ManagedSecurityGroups      #  searches for active directory security groups which
are managed and identify users who have write access to
                                #   those groups (i.e. the ability to add or remove
members)
Find-UserField                  # searches a user field for a particular term
Find-ComputerField              #  searches a computer field for a particular term
Get-ExploitableSystem           # finds systems likely vulnerable to common exploits
Invoke-EnumerateLocalAdmin       #   enumerates members of the local Administrators
groups across all machines in the domain
```

As you can see, starting with a POWERSHELL and a PORTSCAN, you can begin recon to discover much information about the Active Directory environment you wish to conquer or exploit.

In the next section, I will begin to teach you the best practices for hardening Active Directory against exploitation.

There are new tools on the market, to buy you much needed time to tune up, harden and protect your Active Directory environment and they are called Active Directory deception technologies.

They create “honeypots” whereby the hackers and cybercriminals think they are exploiting weak and vulnerable AD servers and nearby systems and users accounts, using lateral movement, when they are really trapped in a virtual deception environment, allowing the IT staff much needed time to detect and stop the exploiters, while also hardening their real infrastructure.

Contact us at CionSystems and we’ll happily put you in touch with our friends in the Deception technology market sector who we would trust and recommend for your Active Directory Deployment.

In the meantime, let’s get started at making our existing infrastructure a bit harder to exploit, shall we?

Best Practices for Hardening Active Directory

You’re probably wondering why it’s so important to harden your Active Directory environment. Yes, you heard that the SolarWinds exploit allowed the cybercriminals to gain privileged account access but maybe you are not running SolarWinds, so “why me?” Right? Wrong! Here is the real problem:

- Globally, over 90% of Businesses, Run Active Directory (AD)
- AD Mismanagement Exposes 90% of Businesses to Breaches
- Cyber Attack Targets 95 Million AD Accounts Daily
- Penetration Testers Breach AD Nearly 100% of The Time
- 80% of All Breaches Involved Access to A Privileged Account

Active Directory is now the #1 target of cybercriminals as their pivot or hopping off point for stealing credentials, attacking other parts of your network, exfiltrating confidential data and making what could have been a tiny risk of a breach into a long-term, massive breach.

When you finally found out they exploited your AD servers to initiate the breach, it will be too late and your company will probably be in the news with the big risks of going out of business, having a tarnished brand, being sued by customers and/or investors and much more.

Your cyber insurance carrier, if you have one, might not honor your breach claims in cyber insurance because they might forensically see that you did not practice due care and due diligence on a regular basis in hardening your most critical asset, your Active Directory environment.

Before we get started, you should understand what Common Vulnerabilities and Exposures (CVEs) are, how to find them and how to fix them as part of your configuration, patch and vulnerability management process. Learn more at https://nvd.nist.gov

In addition, your DNS servers should be secure and your firewalls should be properly configured – especially to limit remote access to your critical cloud services and servers.

So, given the tremendous risk to your organization, let's get started at hardening your Active Directory servers. I have a list of at least 12 critical steps you should take immediately, and they are:

1. Use a Secure Admin Workstation
2. Lock Down Service Accounts and Disable SMB v1
3. Use a Local Administrator Password Solution
4. Use Multifactor Authentication for Remote Access and Strong Passwords
5. Clean up the Domain Admins Group
6. Secure the Domain Administrator account
7. Disable the Local Administrator Account on all Computers
8. Enable Audit policy Settings with Group Policy
9. Monitor Active Directory Events for Signs of Compromise
10. Use Descriptive Security Group Names
11. Cleanup Old Active Directory User & Computer Accounts
12. Continues Patch Management & Vulnerability Scanning

Let's take a look at each one of these steps in more detail:

Use a Secure Admin Workstation

Your secure admin workstation is a dedicated system that should only be used to perform administrative tasks with your privileged account.

Consider installing the least amount of software and services, never use it to brose the internet, check email, do social media posting or reading. It should have state of the art malware protection, firewall and all the latest patches and security updates.

You should vulnerability scan and harden it, regularly. From this system, you should feel more comfortable that you've reduced risk of exploitation while you are performing AD administration, Group Policy modifications and any other tasks requiring admin level privileges.

Microsoft has some useful resources on how to do this at https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/privileged-access-workstations

Lock Down Service Accounts and Disable SMB v1

Much overlooked are service accounts. These are accounts that run an executable, task or service or Active Directory authentication, for example. These are frequently used with passwords set to never expire. These accounts usually have tremendous permissions, beyond what they really need.

Setup a strong password that you change on a regular schedule for these accounts. Give them access only to the resources they really need to function properly. Try to avoid giving them local administrator rights, denying local logins and login as a batch and demand of your software vendors that they make their software function without requiring domain admin rights, if possible.

Remember the world's first Ransomworm? Wannacry? It was the first piece of ransomware that wormed its way very quickly through networks by taking advantage of Active Directory servers that were still running the weak and easily exploitable Server Message Block (SMB) version 1 protocol. SMB v1 is 30 years old and Microsoft has been saying for a very long time to stop using and upgrade to SMB v2 and preferably SMB v3.

You can either disable SMB v1 under Programs and Features, by Turn Windows features on or off – you would scroll the list and uncheck "SMB 1.0/CIFS File Sharing Support" and then you will be prompted to restart the operating system. Alternatively, you can disable the feature in the registry. Navigate to the key:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters

Then, right click the parameters key and choose New > DWORD (32-bit) value. Then name the new value SMB1. It should be set to a value of 9 by default, to ensure it's disabled. You can disable it across all windows computers by creating a group policy registry preference and set it to disabled by default.

Use a Local Administrator Password Solution

The Local Administrator Password Solution (LAPS) is a popular tool to handle the local admin password on all computers. The LAPS is a Microsoft tool that provides management of local account password of domain joined computers. It will set a unique password for every local administrator account and store it in Active Directory for easy access. This is one of the best free options for mitigation against pass the hash attacks and lateral movement from computer to computer.

While it is very common that organizations deploy Windows using an image-based system for rapid deployment, this also means the local administrator account will be the same on every computer. Since the local Administrator account has full rights to everything on the computer, all it takes is for one of them to get compromised, then the hacker can gain access to all the systems. Because the LAPS is built upon the Active Directory infrastructure so there is no need to install additional servers. This solution uses the group policy client-side extension to perform all the management tasks on the workstations. If you need to use the local admin account on a computer, you would retrieve the password from AD and it would be unique to that single computer. To learn more on LAPS and how to install it, see: https://systemcenterdudes.com/how-to-install-local-administrator-password-solution-laps/

Use Multifactor Authentication for Remote Access and Strong Passwords

One of the best ways for you to protect against the risk of compromised accounts is to use at least two factor authentication, also known as multifactor authentication or MFA. This will also help against password cracking and admin account hijacking.

Belief it or not, compromised accounts are now the most common exploitation, which ends up providing attackers with remote access to your systems, network and online resource.

You should check your ADFS (and Office 365) logs and see how many login attempts are coming from outside – even other countries like China and Russia, to name a few.

Phishing attacks are the most popular so if your users are not well trained, they can easily be compromised and install malware including remote access trojans and ransomware, by accident. However, if the said user has two factor enabled, this could prevent access even though the account has been compromised. The cybercriminal would need the second set of credentials to login.

Clean up the Domain Admins Group

The Domain Admins (DA) group is the most powerful group. Members of this group have the most powerful local admin rights on every domain joined systems from laptops to workstations to servers. This is exactly what the cybercriminals are looking to gain access to as they initiate exploitation against you.

Cleaning up the DA group is an important step to harden your Active Directory servers. Be very cautious in removing accounts from the DA group because you may break some software or app in the process. So, before you start removing accounts from the DA, document each account in detail and review each one with your IT team. Then, you can slowly begin removing accounts one at a time until something breaks, then figure out why and fix it.

Secure the Domain Administrator account

The built in Administrator account should only be used for the domain setup and disaster recovery such as restoring Active Directory. Because every domain includes an Administrator account, this account by default is a member of the Domain Admins group, it is an important high risk account. In fact, it's too risky to give access to this account to anyone on the team. It should have an incredibly strong password and multifactor authentication enabled. If someone needs admin permission to access their servers, services or AD, they should do so from their own, individual account.

No one should know the Domain Administrator account password. You should set a really long 21+ characters password and lock it in a vault, giving the only set of keys to the CEO and CFO with instructions on the importance. Remember, the only time this is needed is for recovery purposes. In addition, you should follow Microsoft’s top recommendations for securing the DA account. This includes: deny remote access, deny logon as a service, deny logon through remote desktop protocol (RDP) and even enable smart card for interactive login.

Disable the Local Administrator Account on all Computers

The local administrator account is a high target of hackers and this account is not needed. It is best to use an individual account that has the necessary rights to complete tasks, instead of the default local administrator account. If for some reason, you cannot disable this account, then please follow the top security recommendations from Microsoft and look into using the LAPS tool.

Enable Audit policy Settings with Group Policy

Cybercriminals love to attack laptops, desktops, workstations, and servers. If you are not frequently monitoring all these systems, you will miss the early signs of a successful attack. It is so important you ensure your Audit Policy settings are configured in group policy and applied to all computers and servers. You will need to set Account Login auditing is enabled, Account Management, Policy Change, System, Object Access, Policy Change and Detailed Tracking auditing is enabled, and Login/Logoff auditing is also enabled, in most cases set to “Success and Failure” so that you can track all these critical events.

Monitor Active Directory Events for Signs of Compromise

It is so important to monitor high risk and critical AD events to detect a compromise from abnormal behavior on your network. Some of the most important events you should monitor include a high volume ‘spike’ in bad password attempts, account lockout attempts, logon and logoff events, use of local administrator accounts, disable or removal of firewalls, antivirus software, vulnerability scanning agents and EDR solutions being disabled on endpoints as well as changes to privileged groups such as Domain Admins. You should collect all these logs on a centralized log management or analyzing system. With a good log analyzer, you will be able to quickly pinpoint suspicious activity in your AD environment.

Use Descriptive Security Group Names

When creating security groups, use descriptive names to help you identify exactly what they are used for and what they are meant to do. For example, if you have a security group for the IT team that manages the helpdesk, you might also let them do password resets so you could name the group IT-HelpDesk-Password-Resets-AD. Whereas, if you wanted a security group for the HR department to work on shared folders for an employee handbook, you could name that group HR-Employee-Handbook-Folder. Feel free to come up with your own, creative naming convention that helps you manage access by having very descriptive names.

Cleanup Old Active Directory User & Computer Accounts

It is important to create and implement a policy to detect unused, old and inactive user and computer accounts in AD. Hackers love to find these accounts and exploit them for lateral movement. While automation tools are so helpful here, you can manually use the following two attributes to find old accounts – the first is “Last logon time” and the second is “Computer password age”. Powershell can help you get this information quickly. The command you would use is as follows:

```
get-adcomputer -filter * -properties passwordlastset | select name, passwordlastset | sort passwordlastset
```

Once you run it, this command will display all the computers by name and password last set date. Export the results to CSV, load into Excel and sort by Last Password Set date and time. Look for those that haven’t been reset in the last 90 days or longer and you’ll have your initial cleanup list.

Continues Patch Management & Vulnerability Scanning

Patch management is a critical component of system hardening. Vendors produce weak and vulnerable software all the time, including Microsoft. When this is discovered, they will usually send out a patch to update their software and remove their holes or weakness. However, in many cases, you should enable automation in patch management and there is some risk that something will break. Make sure as you automate your updates, you can quickly roll-back if there is a problem. Vulnerability management is a continuous process of identifying, prioritizing, remediating, and reporting on security vulnerabilities in systems and the software that runs on them. When you find a hole, there may be an upcoming patch to fix it or there will be configuration changes that you can make to remove the hole. The more automation on fixing and hardening systems, the less risk they can be easily exploited by attacks against common vulnerabilities and exposures (CVEs). Learn more about this at https://cve.mitre.org and https://nvd.nist.gov.

Conclusion

Your Active Directory servers have now become a major target for exploiters. It is not if it will happen to you, it’s when will it happen and how will you respond. Getting your shields up is more than just a secure DNS server and well configured firewall. It’s about constantly monitoring any issues that might arise with your AD servers and being able to proactively harden them from passwords to user accounts and group policies. Strong configuration, patch and vulnerability management take time and energy. Generating deep audits and insights into your AD servers status need to become a regular process.

Don’t Go It Alone

At CionSystems, Inc., we’ve been working on these AD problems as well as Office 365 and Azure for years. Utlizing our expertise, we provide the most comprehensive Active Directory security, assessment and hardening enterprise class solution to automate most of these challenging tasks, freeing up thousands of work hours so you can focus on helping yourcompany grow, while more easily defending your AD environment.

We offer:

ADGuardian | ADSploit the **‘Active Directory Mechanic and Defender’**

Single Pane of Glass for Enterprise Identity Management, Security, Compliance, Reporting and Automation for Active Directory Servers

Over 80% of all breaches involve Access to a Privileged Account. The mass migration to Remote Workforce enterprise operations has created more Security Gaps and Risks than ever before. ADGuardian is an “out of the box” solution to dramatically Harden, Simplify, and Secure enterprise Active Directory deployments – NO SCRIPTS OR CODE required. ADGuardian enables swift transition of Active Directory to handle large Remote Workforces, with Real-Time Tracking of ALL changes with Defined Notifications.

And our latest Enterprise add-on for ADGuardian called ADGuardian+ and ADGuardianCloud. Together, they are the Complete Suite for increasing productivity, security, and compliance while simplifying the management and synchronization of onpremise Active Directory, Microsoft Office 365 Cloud, OpenLDAP, and Azure AD with Realtime change alerts, remediation, backup and recovery.

Simplifies Office365, OpenLDAP and Azure AD management, access control, security, compliance and disaster protection.

Do it all in the fastest, easiest, most efficient, and secure way with ADGuardian+ bundled togetherwith ADGuardianCloud

Learn more, here: https://cionsystems.com/enterprise-identity-manager/

and consider scheduling a demonstration, here: https://cionsystems.com/register/

Call us at: 1-425-605-5325 or email us at sales@cionsystems.com | info@cionsystems.com

CionSystems

CionSystems, Inc.
6640 185th Ave NE
Redmond, WA 98052