



throttnet.com



TODAY'S PRESENTER:

Chris Montgomery

Director of Sales



throttle.net

AGENDA



Microsoft
Active Directory



throttlenet.com

ACTIVE DIRECTORY STATS



AD OUTAGES HAVE A SERIOUS BUSINESS IMPACT.

Almost every respondent (97%) said that AD is mission-critical to significant, severe, or catastrophic.

the business, and 84% said that an AD outage would be



AD RECOVERY FAILURE RATE IS HIGH.

Most respondents (71%) were only somewhat confident, not confident, or unsure about their ability to recover AD to new servers in a timely fashion. Only a tiny portion (3%) said they were “extremely confident.”

Source: Semperis - Recovering Active Directory from Cyber Disasters



AD RECOVERY PROCESSES REMAIN LARGELY UNTESTED.

Exactly one-third of organizations (33%) said they have an AD cyber disaster recovery plan but never tested it, while 21% have no plan in place at all. Out of the entire poll, just 15% of respondents said they had tested their AD recovery plan in the last six months.

Organizations expressed many concerns about AD recovery, with the lack of testing being the number one concern. This includes organizations that have not tested AD recovery at all and those who have tried but failed.

Source: Semperis - Recovering Active Directory from Cyber Disasters

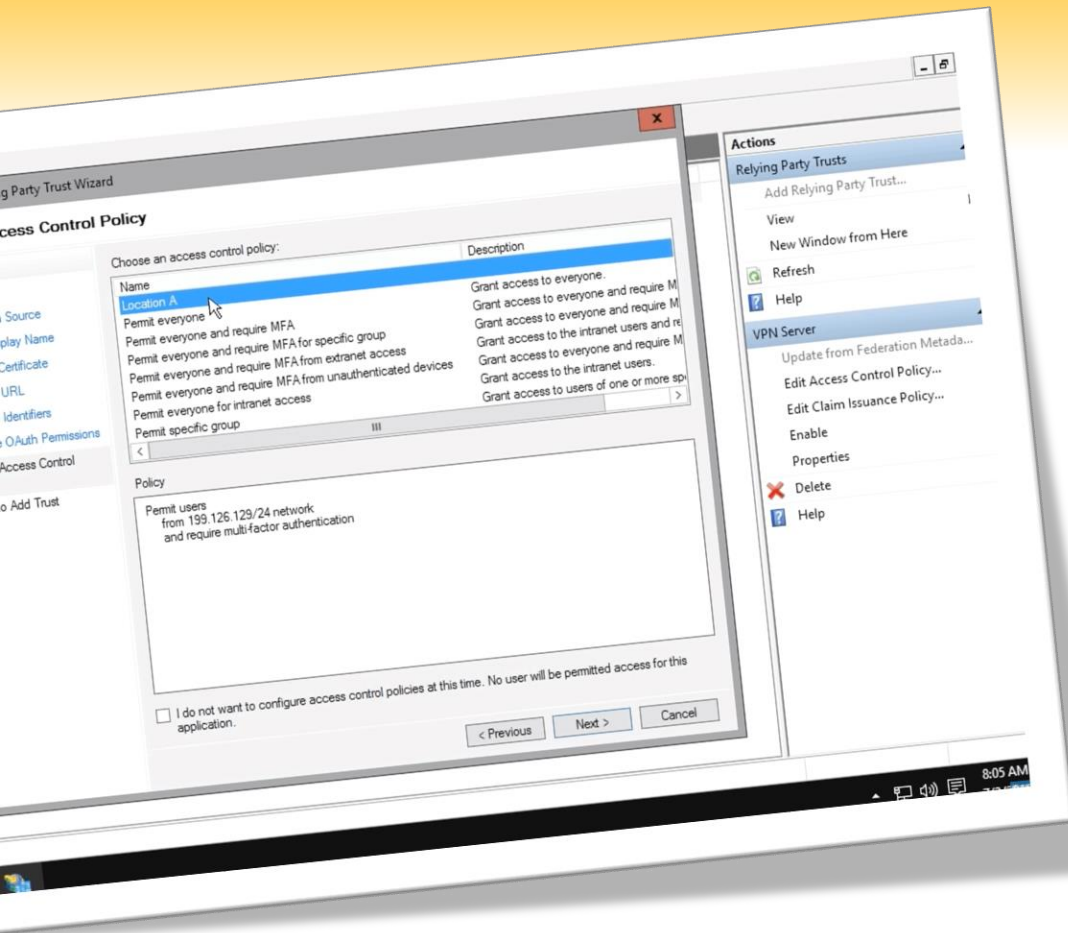


WHAT IS ACTIVE DIRECTORY?

[Active Directory](#) helps you organize your company's users, computer and more. Your IT admin uses AD to organize your company's complete hierarchy from which computers belong on which network, to what your profile picture looks like or which users have access to the storage room.

WHAT DOES AN ACTIVE DIRECTORY DO?

[Active Directory](#) allows network administrators to create and manage domains, users, and objects within a network.



Where is your **AD** housed or

where can it be?



Active Directory services can be housed on a local server or in a hosted environment such as Microsoft Azure. In the case of Azure, this is a standalone offering that doesn't require a fully hosted server environment.



How does **ACTIVE DIRECTORY** benefit your business?



ADMINISTRATIVE CONTROL

Since **Active Directory** grants control of all machines on a network to the administrator, that person can oversee anything that happens on the domain.

This makes it easier to implement specific settings and grant certain rights and privileges to users on the network.



CENTRAL STORAGE

Active Directory domains also provide a centralized storage repository for users' files. By saving files to the central server, other users on the domain can access them if necessary.



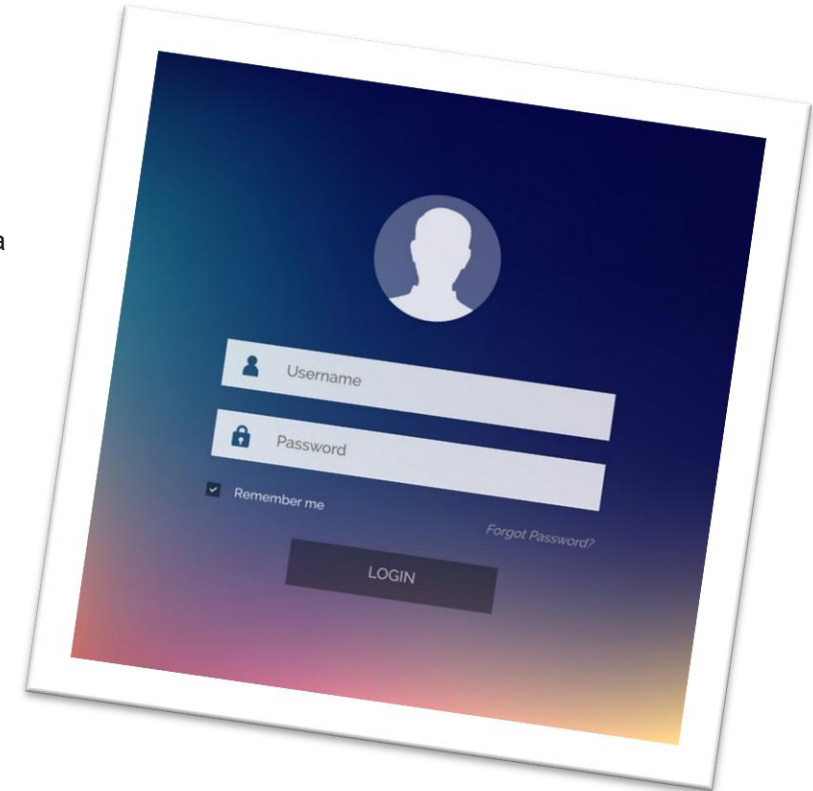
BETTER BACKUPS

Without a central storage domain, users are only able to save their files to their local drives. If a user's machine is infiltrated by a cyberattack, all of the files on that machine may become inaccessible. However, if they were saved to a central storage location, it would be much easier to recover them.



EASY LOGINS

Once Active Directory is in place, logging into your machine becomes easier. Essentially, when you log into a machine on the network, the machine and network communicate back and forth. The network will verify the password and automatically grant rights and privileges to the user, such as logging into Outlook





IMPROVED SECURITY

Since the network administrator has the ability to control whatever happens on the domain, they're able to implement new security measures when necessary. This includes installing a new antivirus software onto each machine or making certain sensitive documents inaccessible so they don't fall into the wrong hands.



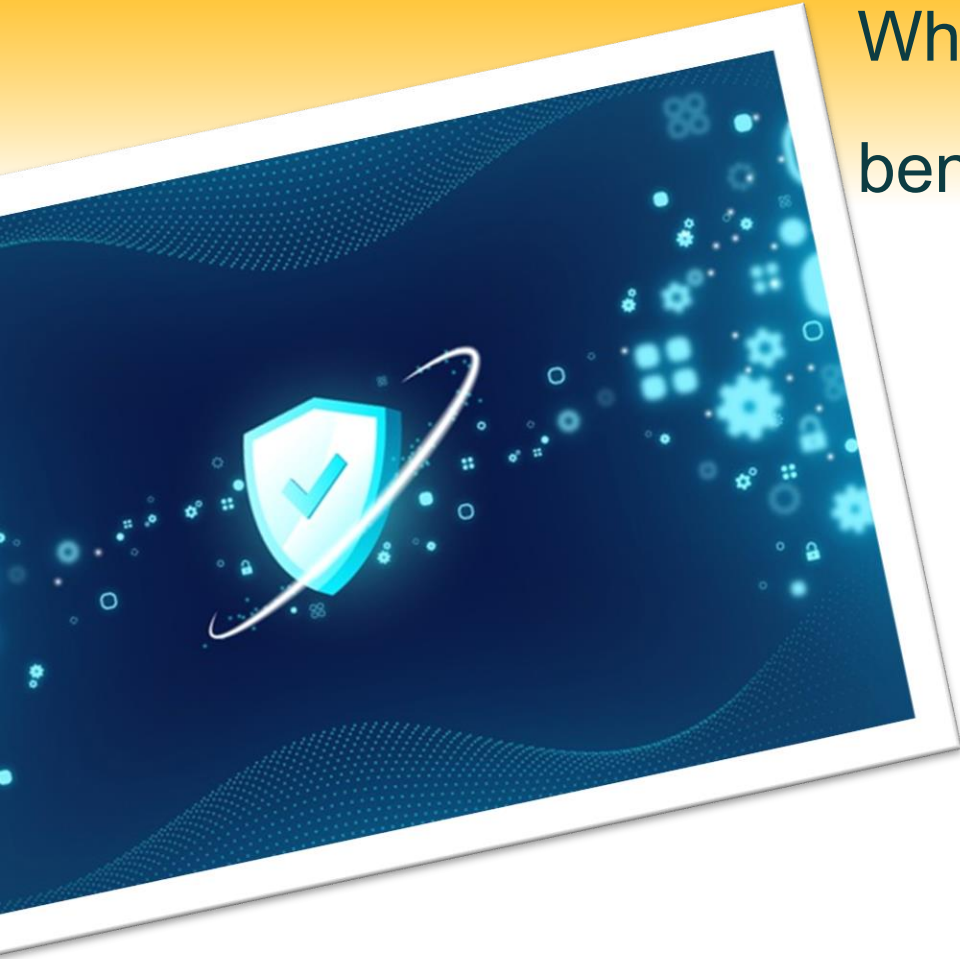
CUT COSTS

All of the above benefits of Active Directory streamline IT operations in a way that drastically reduces IT costs.

Since Active Directory is easier to scale up or down than it is to install in the first place, it's best to implement it as soon as possible. This way, if your business grows, all you must do is add a new machine to the network.



What are the **SECURITY** benefits of **ACTIVE DIRECTORY?**



Active Directory provides a single point from which administrators can manage and secure network resources and their associated security objects. An organization can administer Active Directory based on an organizational model, a business model, or the types of functions being administered.

HOW ARE CYBERCRIMINALS USING ACTIVE DIRECTORY?



Cybercriminals today are targeting [Active Directory \(AD\)](#), performing reconnaissance to discover users, servers and computers in an enterprise network and then move laterally to carry out multi-stage attacks to gain access and abuse organization resources and data.

Threats to the **Active Directory Systems?**



DEFAULT SECURITY SETTINGS

AD has a set of predetermined, default security settings created by Microsoft. These security settings may not be ideal for your organization's needs. Additionally, these default security settings are well-understood by hackers, who will attempt to exploit gaps and vulnerabilities.

INAPPROPRIATE ADMINISTRATIVE USERS AND ACCESS:

PRIVILEGED

Domain user accounts and other administrative users may have full, privileged access to AD. Most employees, even those in IT, do not need high-level or superuser privileges.



INAPPROPRIATE OR BROAD ACCESS FOR ROLES

AND EMPLOYEES:

AD allows administrators to grant access to specific applications and data based on employee roles. Roles are assigned to groups that determine access levels. It's important to only allow the levels of access individuals and roles need to perform their job functions.

UNCOMPLEX PASSWORDS FOR ADMINISTRATIVE ACCOUNTS:

Brute force attacks on AD services often target passwords. Uncomplicated passwords and easily guessable passwords are most at risk.





UNPATCHED VULNERABILITIES ON

Hackers can quickly exploit unpatched servers, giving them a critical first-foothold

LACK OF VISIBILITY AND REPORTING OF UNAUTHORIZED ACCESS ATTEMPTS:



If IT administrators have awareness about unauthorized access attempts, they can more effectively disrupt access attempts in the future.

Thus, a clear Windows audit trail is vital to identify both legitimate and malicious access attempts, and to detect any AD changes that have been made.



How do bad actors compromise the ACTIVE DIRECTORY?



INITIAL BREACH TARGETS

Most information security breaches start with the compromise of small pieces of an organization's infrastructure-often one or two systems at a time. These initial events, or entry points into the network, often exploit vulnerabilities that could have been fixed, but weren't.

Commonly seen vulnerabilities are:



Gaps in antivirus and antimalware deployments



Incomplete patching



Outdated applications and operating systems



Misconfiguration



Open RDP (Remote Desktop Protocol)



PRIVILEGE ELEVATION AND PROPOGATION

Specific accounts, servers, and infrastructure components are usually the primary targets of attacks against Active Directory. These accounts are:



Permanently privileged accounts



VIP accounts



"Privilege-Attached" Active Directory accounts



Domain controllers

Other infrastructure services that affect identity, access, and configuration management, such as public key infrastructure (PKI) servers and systems management servers








ATTRACTIVE ACCOUNTS FOR CREDENTIAL THEFT

Credential theft attacks are those in which

an attacker initially gains privileged access to a computer on a network and then uses freely available tooling to extract credentials from the sessions of other logged-on accounts.

Activities that Increase the Likelihood of Compromise - Because the target of credential theft is usually highly privileged domain accounts and "very important person" (VIP) accounts, it is important for administrators to be conscious of activities that increase the likelihood of a success of a credential-theft attack. These activities are:

-  Logging on to unsecured computers with privileged accounts
-  Browsing the Internet with a highly privileged account
-  Configuring local privileged accounts with the same credentials across systems
-  Overpopulation and overuse of privileged domain groups
-  Insufficient management of the security of domain controllers.

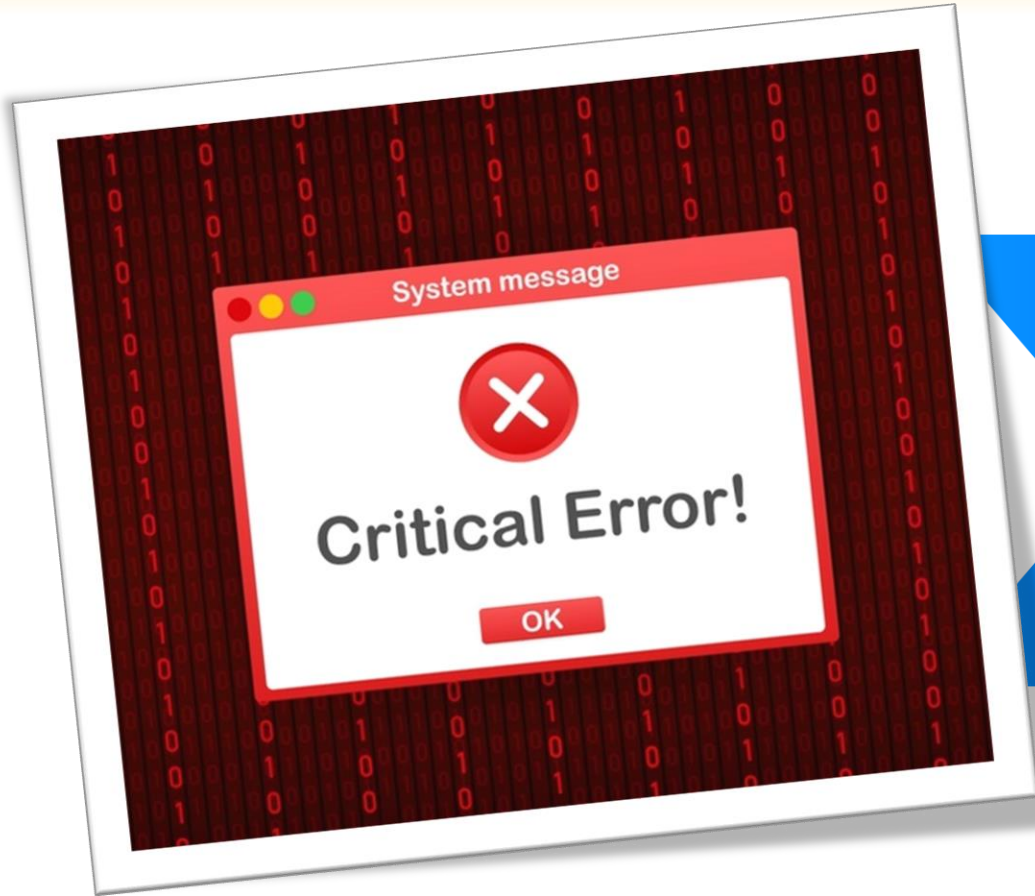
How do these compromises impact the ability to do business?



Since Active Directory is central to authorizing users, access, and applications throughout an organization, it is a prime target for attackers.

Top 5 CONCERNS for recovering after a cyberattack

ACTIVE DIRECTORY



- Have not tested AD recovery process
- No cyber recovery plan for AD
- Backups get encrypted or wiped out
- Can't recover AD quickly
- Responsibility for AD recovery hasn't been defined

What are common best practices to protect the **ACTIVE DIRECTORY** against attacks?



ENSURE all applications and operating systems are up to date on patches

DEPLOYMENT of AV across all systems and monitor for attempts to remove

CREATION of an incident response plan

ISOLATION of legacy systems and applications that may no longer have new security patches

DISABLE users within AD when they leave the company

IMPLEMENT password refresh policies that ensure if a user isn't disabled, that their credentials will expire

What should be included in an **ACTIVE DIRECTORY** recovery plan?



IDENTIFY
the severity of the problem

DETERMINE
how to recover

PERFORM
initial recovery

Why is an image-based backup is AD?

key to restoring



An image-based offsite backup takes a snapshot of the entire server including active directory which means you can restore from an attack quickly by simply restoring the image. Ideally, this should include versioning just in case the most recent version has been compromised.

How does TN help protect against and assist in recovery of **ACTIVE DIRECTORY**



Azure AD Sync



Datto BCDR



Managed Services



Firewalls and Servers

HOW CAN WE

HELP?

866-829-5557



throttlenet.com



throttlenet



throttlenet.com