Understanding Active Directory: Structure, Functions, and Security

What is Active Directory?

Active Directory (AD) is a service by Microsoft designed for managing users, computers, and resources on a Windows network. It acts as a phone book but for your network. It stores information about everything on the network, including user accounts in one central database.

In simple words it is a centralized tracker of all the users are, devices they can use, and their access. This helps IT and admin teams in organizations manage the network efficiently and ensures users only access necessary resources. Now that we know what is active directory, let’s look at how it works.

How does Active Directory Work?

Active Directory acts as the boss of the Windows server operating system, that controls operations behind the scenes. The AD database is an organized center point with all the information about users, systems, passwords and more. These resources are organized into domains, each managed by a Domain Controller (DC) responsible for authentication and access control.

Active Directory has a major benefit. One domain controller quickly copies changes to others. This ensures consistency and updates across all controllers.

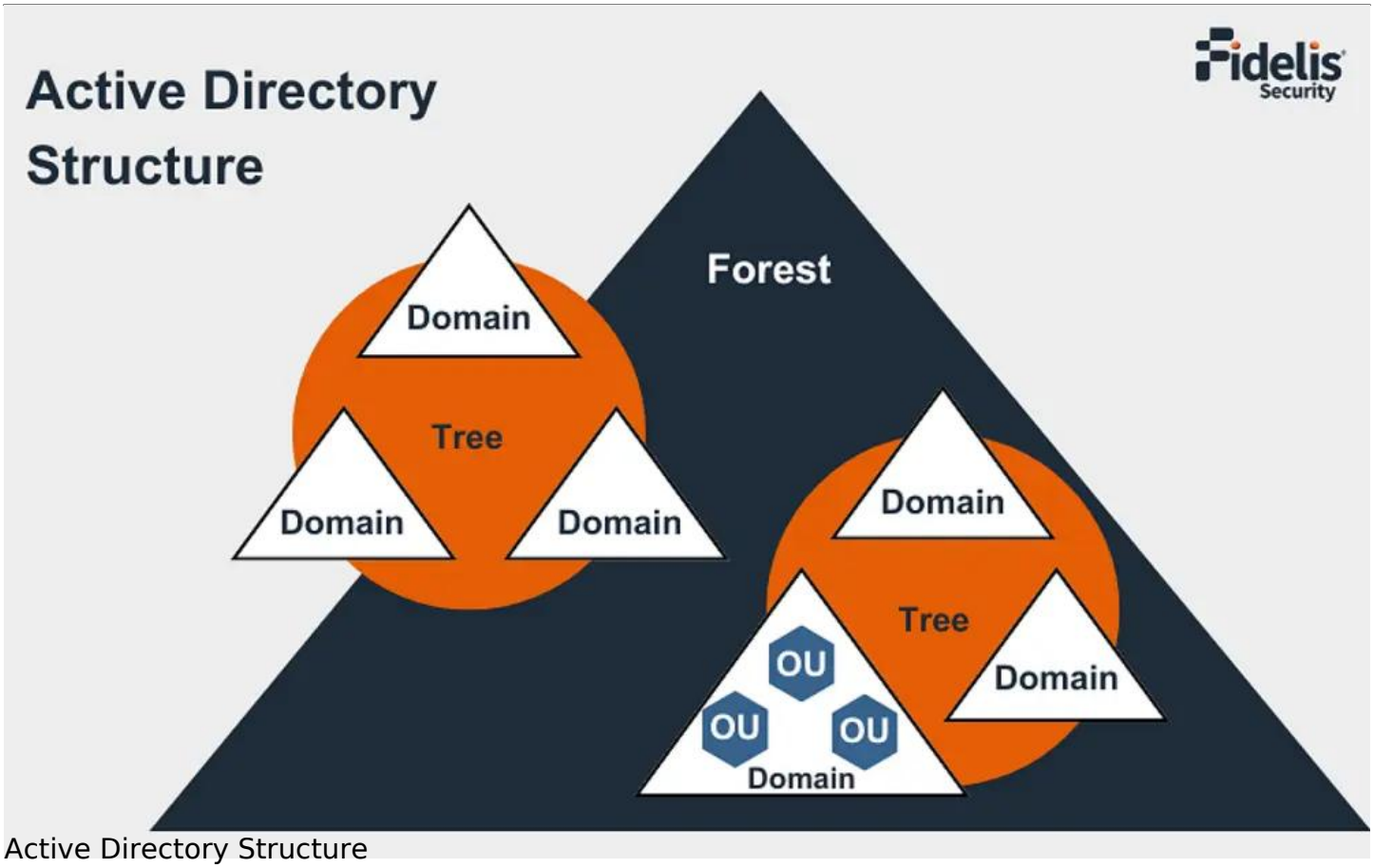
For efficiency, AD lets administrators group users and devices with similar permissions. One policy change for a group can apply to many.

And this is the core of how AD works. Microsoft Active Directory streamlines resource management, authentication, authorization, and policy enforcement in Windows-based networks.

What does the hierarchical structure of data in AD look like?

Active Directory is a layered system for managing users, computers, and resources in Windows networks. Its structure includes:

1. **Forest**: A forest is the top-level container with one or more domains.
2. **Domain**: A domain is a logical partition with user accounts and trust relationships.
3. **Organizational Units (OUs)**: These are containers for organizing objects (e.g., user groups).
4. **Trees:** These are a hierarchical grouping of domains that allow for efficient replication of data within the same namespace.



Active Directory Structure

What are the different types of Directory Services?

Active Directory is a broad umbrella structure. There are different types of AD services, let’s look at some of them.

Active Directory Domain Services (AD DS): This is the most basic and commonly found type of AD service. It acts as the central user which stores data, users, devices, domains and more.

Active Directory Lightweight Directory Services (AD LDS): It is a lightweight version of the common Active Directory. It does not need domain or domain controllers and hence is ideal for smaller networks. It is also a versatile directory service.

Active Directory Federation Services (AD FS): Users can use one login to access multiple apps with AD FS’s single sign-on (SSO) features. By offering online single sign-on (SSO) and secure identity federation, it enables businesses to safely extend their AD identities to outside partners and services.

Azure Active Directory (AAD): This is the cloud-based directory service of Microsoft. It specifically manages identities and access in a cloud environment.

Why do attackers target Active Directories?

As the centralized unit that houses all privileged information, the windows AD becomes a lucrative destination for hackers to attack. It mimics the security vault of a wealthy household which holds all the crown jewels of the family. If they crack AD, they can basically rule the entire network, steal data easily, and move around undetected.

Furthermore, continuous access makes it possible for ransomware to spread, destroy data, and

interfere with corporate operations. AD is a key target for cyber attackers due to its important role in network security. This highlights the significance of having strong security measures in place to guard against these threats.

Most Common AD Risks and Securing Them

Credential Theft and Pass-the-Hash Attacks: With Active Directory security measures organizations can mitigate the risk of credential theft. Pass-the-hash attacks are the ones in which adversaries try to move laterally within the network by using cached password hashes. AD monitoring technologies can be identify and counter these attacks.

Insider Threats and Unauthorized Access: Active Directory's granular access control features enable administrators to define and enforce permissions based on roles and responsibilities, disallowing unauthorized access to critical resources.

Ransomware and Data Breaches: Robust backup and recovery solutions integrated with Active Directory enable organizations to restore systems and data in the event of a successful ransomware attack or data breach.

Active Directory Security

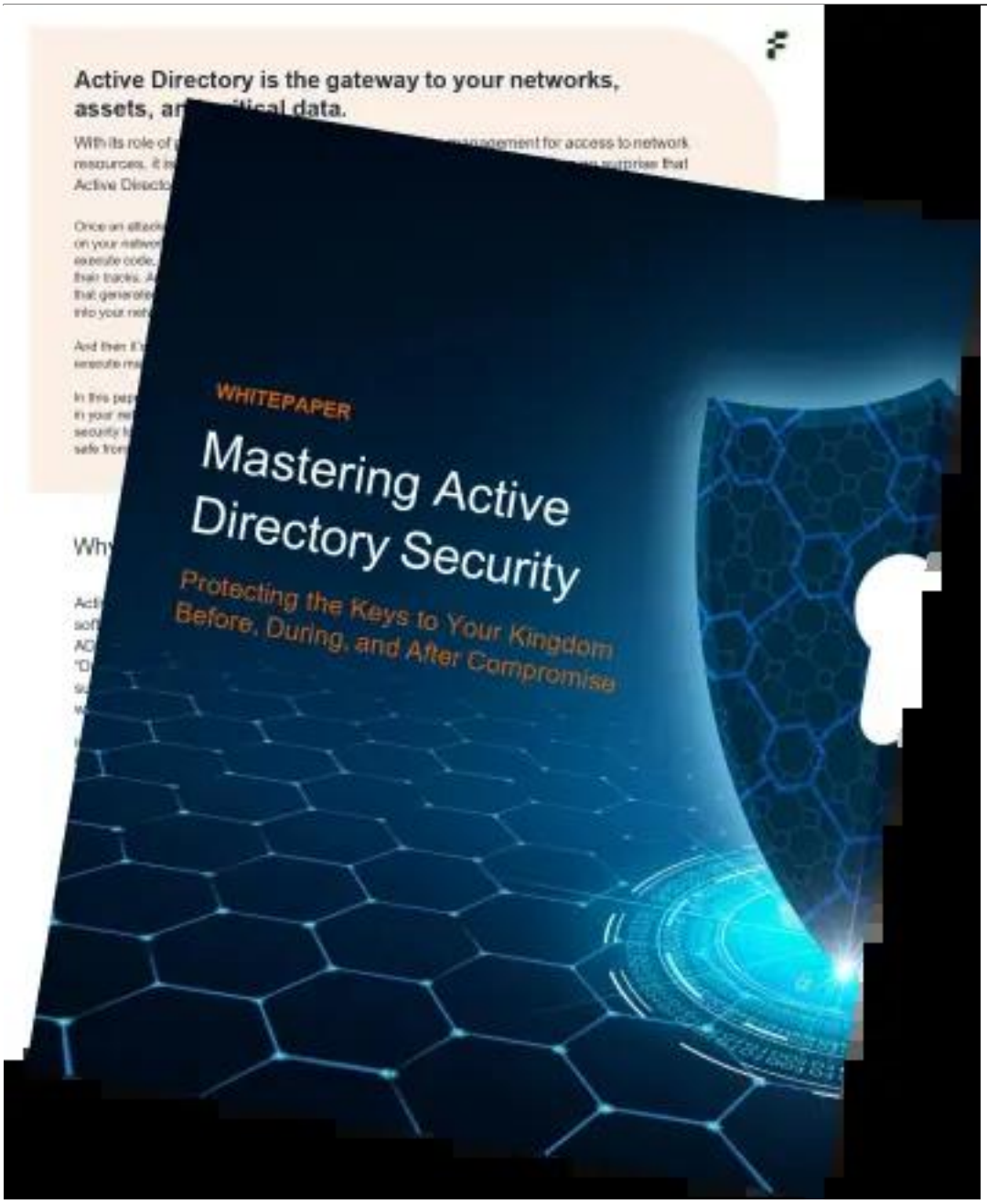
Active Directory security means following the best practices to keep your Windows AD safe from unauthorized access, data leaks, and other security problems. This helps protect the integrity, confidentiality, and availability of resources within a Windows domain network. The importance of a secure active directory includes:

- Centralized Access Control
- Assured Authentication
- Security Policy Enforcement
- Compliance and Auditing

Mastering Active Directory Defense: Proactive Strategies to Thwart Attacks

- Continuous Visibility
- Ensure Compliance Against Misconfiguration
- Proactive AD Defense

Download Whitepaper



Here are some essential points to keep in mind when securing your AD:

- **Regular Updates and Patch Check:** Make sure your AD and associated systems are always up to date with the newest updates to avoid vulnerabilities.
- **Strong Password Policies:** Make in mandatory to create complex strong passwords. You can also promote regular password changes.
- **Watch out for Suspicious Activities:** Keep an eye out for unusual login attempts. Track revisions, logins, and other important occurrences with tools.
- **Implement Multi-factor Authentication:** MFA can act as an extra layer of security for accesses. It requires users to use another method apart from passwords to login.
- **Timely Backups:** Make sure you are regularly creating backups of the data in your AD. This ensures recoverability in case of breach or corruption.
- **Educating Users:** Teach your employees how to securely navigate through the network and avoid phishing attacks.
- **Regular Review of Accounts:** Make it a practice to regularly delete and remove

accounts that are no longer needed. This could mean employees who quit, got laid off or people.
- **Least Privilege Principle:** Give users the bare-minimum access they need to perform functions on applications. Do not allow them to alter structures and other things.

While it is good to implement all these suggestions, it might still not protect your AD a 100%. That's where Fidelis Active Directory Intercept comes in.

Fidelis Active Directory Intercept ™

Fidelis Security's active directory management solution combines AD-aware network detection and response (NDR) and integrated AD deception technology with foundational AD log and event monitoring to not just identify Microsoft Active Directory threats – but to respond swiftly. Fidelis Active Directory Intercept has a unique combination of features like:

- **Active Directory Log and Event Monitoring:** Powered by Active Directory Intercept, you'll gain real-time malicious/suspicious activity detection and response.
- **Integrated Intelligent Deception:** With full terrain mapping and risk profiling, Fidelis Deception® automatically deploys intelligent deception to secure active directory.
- **Intercept and Defeat AD Attacks and Attempts:** With sensors placed strategically across your network and clouds, you'll detect, thwart, and build Microsoft security that other tools cannot.
- **Network Traffic Analysis:** Fidelis Network® provides Deep Session Inspection® that finds threats to AD deep within nested and obfuscated files as they move across the wire.

Multi-layered Defense for Active Directory with Fidelis

- AD-aware Network Traffic Analysis
- Log and Event Monitoring
- Integrated Deception

Download Datasheet

Datasheet

Fidel

Multi-layered Defe

Active Directory (AD) is th
entitlements management
It authenticates and authc
provides for the storage a
deploys services such as
management, and more.
launch point from which
escalate privileges, and
execution, data exfiltrati

Protecting AD is a prime
But many tools fall shor
imminent attack. And o
game over. They can o
network traffic and data
protection tools.

That's where Fidelis A

**See More. Sto
Only with Acti**

Fidelis Active Directc
detection and respor
technology with four
just identify AD thre
Intercept gives you
exactly how, where,
into your network, a
ability to defend ag

Fidelis Active Directory Intercept™

Multi-Layered Active Directory Defense