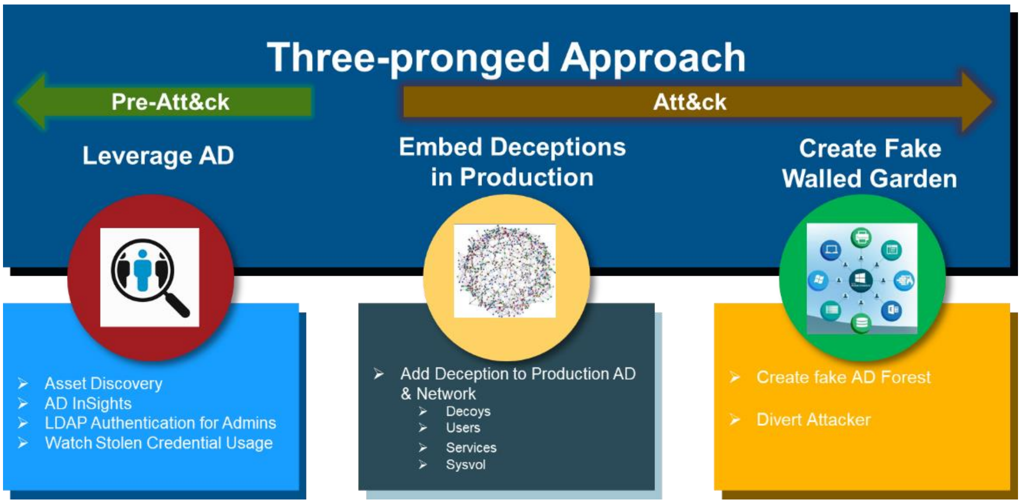
ShadowPlex: Active Directory Protection

Active Directory (AD) is one of the most important assets in an enterprise, given that it is at the heart of most networks and is a repository of rich network data. Tools like *dsquery*, *net command*, and the more prevalent *BloodHound* are used by the attackers to assess the lay-of-the-land and find the shortest path to the key assets in the enterprise.

Acalvio ShadowPlex weaves in blended deceptions into the enterprise Active Directory, covering all entity types and relationships. Using Deceptions combined with AI provides a strong layer of protection in detecting recon, lateral movement, credential access and other malicious activities against the enterprise AD. ShadowPlex provides comprehensive AD protection, by both hardening AD Security and using deception in multiple ways to detect and redirect any AD attacks.



Three-pronged Approach

Pre-Att&ck

Att&ck

Leverage AD

- Asset Discovery
- AD InSights
- LDAP Authentication for Admins
- Watch Stolen Credential Usage

Embed Deceptions in Production

- Add Deception to Production AD & Network
  - Decoys
  - Users
  - Services
  - Sysvol

Create Fake Walled Garden

- Create fake AD Forest
- Divert Attacker

Figure 1: Comprehensive AD Protection

1 Attack Surface for Active Directory

1.1 AD Insights

ShadowPlex uses asset discovery data from the AD for reducing the attack surface area as well. The asset data is processed through AI algorithms to surface rich Insights for the Enterprise. ShadowPlex can discover and surface various AD misconfigurations and vulnerabilities, such as shadow administrators, privileged users with access to assets, inactive users in super active groups, users recently added to privileged groups, over-permissioned delegation, risky users with no password expiration etc.

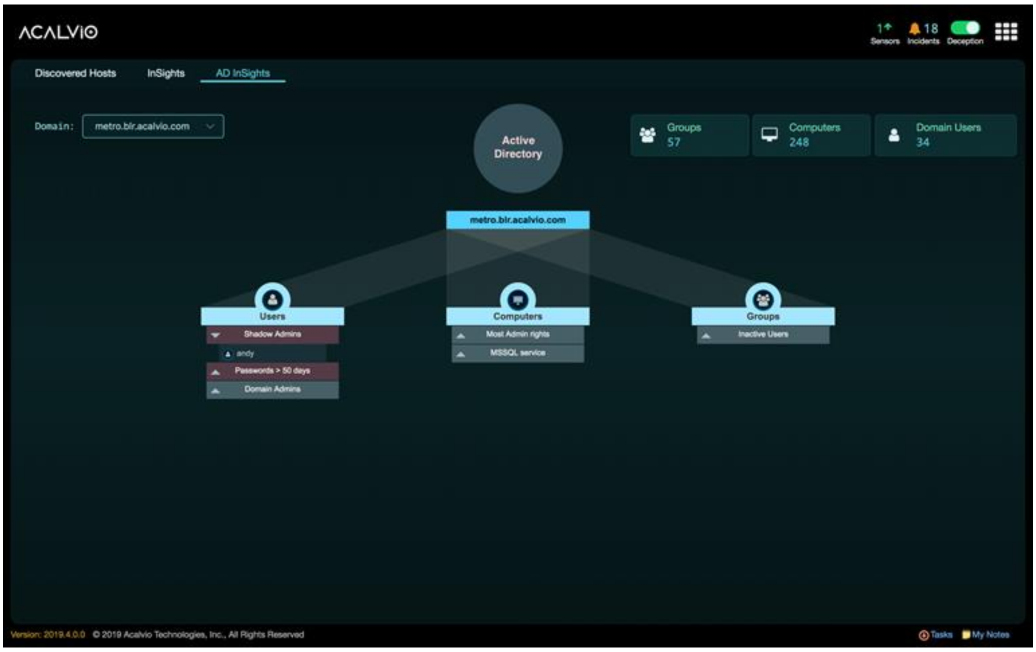


Figure 2: Active Directory Insights

Figure 2 shows the AD Insights screen listing the Shadow Admins (users who have gained an extra administrative privilege through an ACL but are not a part of the Administrative group).

2 Active Directory Deception

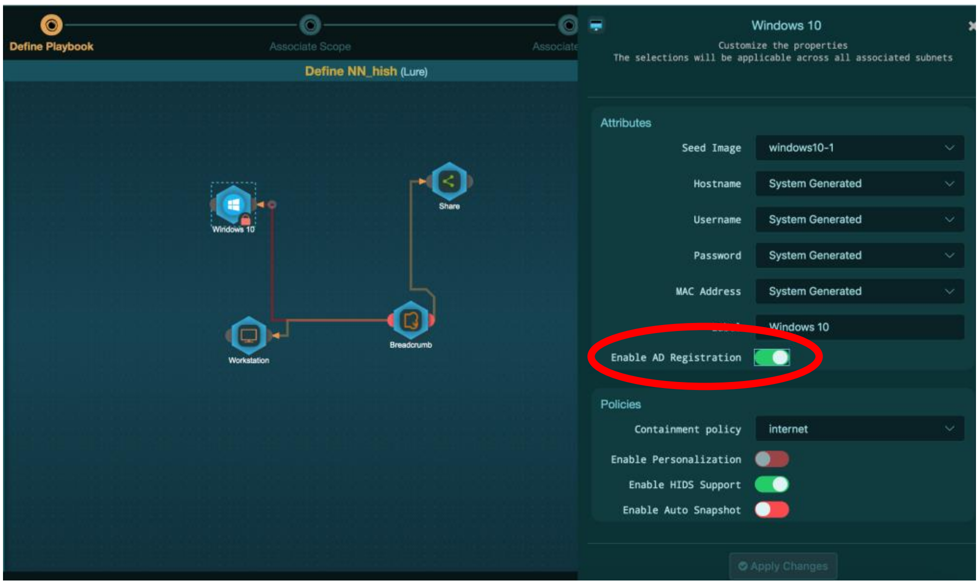
AD Deception is one of the significant ways to detect attacks and redirect them to the decoys. AD is a critical asset and enterprises tend to have different AD policies. ShadowPlex provides comprehensive AD deception with several flexible options to address different requirements.

- Decoys in the enterprise AD
- Decoy AD forest
- Decoys can also be created without joining them to an AD

Breadcrumbs corresponding to the decoy hosts, services and decoy AD are placed on the enterprise hosts, for all options. ShadowPlex also provides the option to watch the Key Distribution Centre (KDC) logs for failed attempts to authenticate decoy credentials.

2.1 Decoys (Users, Computers, SPNs) in the Enterprise AD

Decoys can be configured to join the enterprise AD. The decoys show up just as regular hosts and services in the AD to any attacker using AD to discover targets for lateral movement or exploitation.



Windows 10

Customize the properties
The selections will be applicable across all associated subnets

Attributes

Seed Image: windows10-1
Hostname: System Generated
Username: System Generated
Password: System Generated
MAC Address: System Generated
Windows 10
Enable AD Registration: on

Policies

Containment policy: internet
Enable Personalization: off
Enable HIDS Support: on
Enable Auto Snapshot: off

Figure 3: Adding Decoys to Enterprise AD

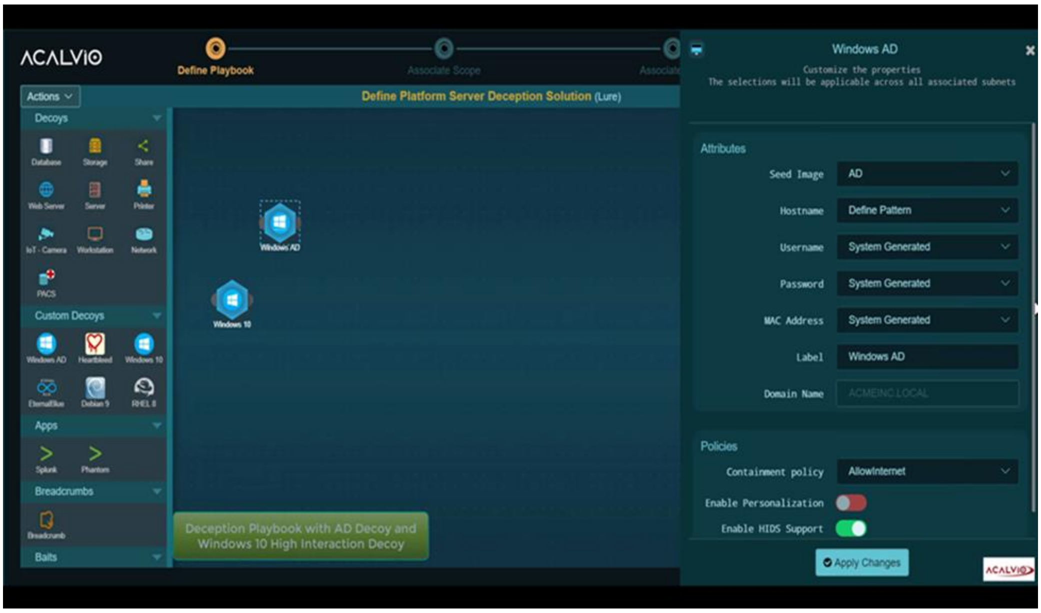
Deception playbooks allow defining each decoy properties. Figure 4 shows configuring a decoy to be part of the enterprise AD. The corresponding credentials are automatically created and used for breadcrumbs.

ShadowPlex registers Decoy Computers, Users and SPNs in AD. These enable the Enterprise to get early detection into AD specific attacks (Reconnaissance such as SPN Scans, Lateral Movement Attempts).

2.2 Decoy AD Forest (with Optional One-Way Trust to Production AD)

ShadowPlex allows creation of a decoy AD forest. Decoy hosts, services and users are joined to this decoy AD forest, instead of the enterprise AD, thereby keeping the decoy entries separate from the enterprise assets. The decoy AD forest can be created as completely walled from the enterprise AD, or optionally made a subdomain in the enterprise AD.

The Decoy AD can have a One-Way Trust set up with the Production AD. This provides an ability to divert the attacker away from the Production Domain and to the Decoy Domain.



Deception Playbook with AD Decoy and Windows 10 High Interaction Decoy

Windows AD

Customize the properties
The selections will be applicable across all associated subnets

Attributes

Seed Image: AD
Hostname: Define Pattern
Username: System Generated
Password: System Generated
MAC Address: System Generated
Label: Windows AD
Domain Name: ACMEINC.LOCAL

Policies

Containment policy: AllowInternet
Enable Personalization: off
Enable HIDS Support: on

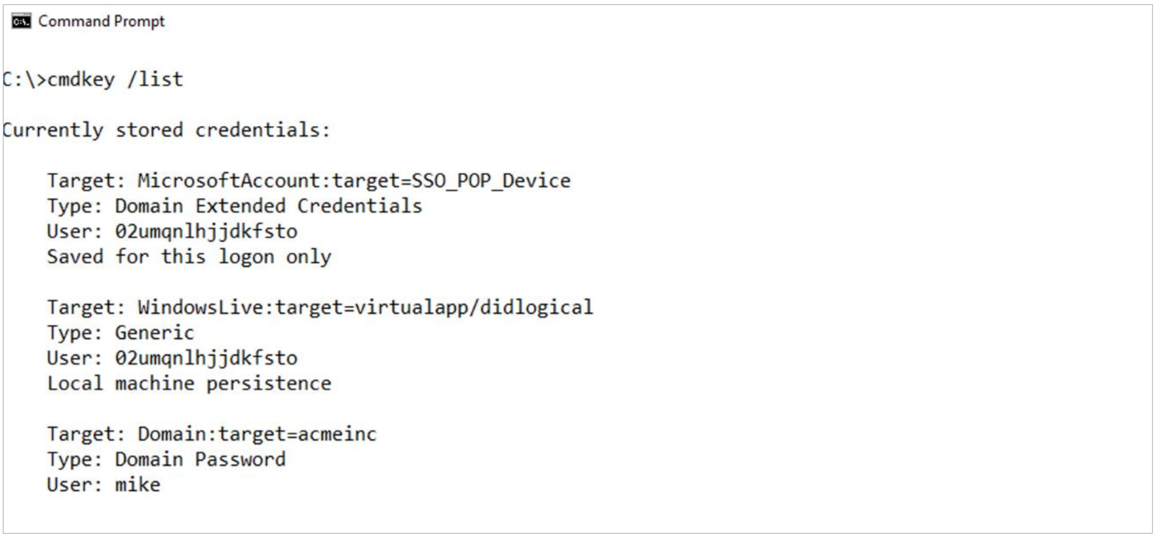
Figure 4: Decoy AD Forest

2.3 Breadcrumbs/Baits on Production endpoints/Servers

Breadcrumbs and Baits can be placed on production endpoints/Servers that enable early Detection of AD Reconnaissance and host compromise. Breadcrumbs/Baits can also lead the attacker to the Decoy and away from Production Assets.

The breadcrumbs include Deceptive credentials (passwords, hashes), connection strings, Application profiles.

ShadowPlex breadcrumbs and baits are deployed using an agentless deployment architecture. This ensures that no additional Attack Surface is created and also avoids maintenance/operational overheads for the Enterprise.



```
Command Prompt

C:\>cmdkey /list

Currently stored credentials:

    Target: MicrosoftAccount:target=SSO_POP_Device
    Type: Domain Extended Credentials
    User: 02umqnlhjjdkfsto
    Saved for this logon only

    Target: WindowsLive:target=virtualapp/didlogical
    Type: Generic
    User: 02umqnlhjjdkfsto
    Local machine persistence

    Target: Domain:target=acmeinc
    Type: Domain Password
    User: mike
```

Figure 5: Breadcrumbs: Credential Manager Profiles that Enable Attackers to be Diverted to Decoy AD Domain

2.4 Detection of Advanced AD Attacks (Kerberos Protocol Attacks, Domain Trust/Delegation related Attacks)

ShadowPlex Deceptions can be used to detect Advanced AD Attacks – such as Kerberoasting, AS REP Roasting, Unconstrained Delegation attacks.

ShadowPlex Deceptions can be registered to detect Advanced AD Attacks. The combination of the Deceptions with the Observation and Monitoring capability in ShadowPlex can be used to generate High Fidelity Incidents.

3 Summary

ShadowPlex provides a multi-pronged approach to AD protection (figure 1), to both harden AD security posture and detect and divert AD attacks. Using flexible and configurable options, ShadowPlex builds a complete AD deception solution.

Appendix: Ineffective Agent-based Approach to AD Deception

An alternate approach followed by some deception vendors involves deploying and agent onto every endpoint in an attempt to hide the enterprise Active Directory from the attacks. Agent-based approach suffers from multiple challenges, besides introducing security and stability risks.

Complete Hiding of AD is Impossible

Windows environments have multiple caches. For example,

- LOGONSERVER environment variable
- Registry entries such as HKLM:\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\DomainControllerName
- Commands such as
    - nltest /dclist:<Domain>
    - nslookup -type=SRV _ldap._tcp.mydomain.com
- Entries in the SYSVOL share

An agent-based approach can never completely modify the results in all the caches, since manipulating the stored caches across all these locations will result in system malfunction.

Windows also provides multiple interfaces through which one can query AD and an agent cannot cover all possible interfaces. Attackers can run two simple commands – comparing the results from *nslookup* and the *LOGONSERVER* environment variable and can trivially fingerprint the Deceptions.

The agent-based approach also does not work with devices where an agent cannot be deployed – such as a printer that is joined to a domain. Attackers can perform AD Recon from the Printer – and see all the Real AD Data.

Ineffective Deception

Agent-based approach is ineffective since the deception is trivially fingerprintable. As agent-based approach cannot cover all caches and all interfaces, queries accessing different caches return different results. The results also differ between a system with an agent installed and from a system where an agent cannot be installed (e.g. domain-joined printer).

Attackers can trivially bypass the agent on the endpoint by rebooting the endpoint, booting up in Safe mode and disabling the agent. Once the endpoint boots up, attackers can now perform Recon activity and will see the Real Domain Controller.

An advanced attacker can now easily compare the inconsistent results and identify all the Deceptions in a single action – this makes the Deception completely ineffective.

Security and Stability Risks

An agent-based solution adds risk to an Enterprise environment.

1. Agents run with high privileges on an endpoint. This increases the Attack Surface on the endpoint as it provides a target for Privilege Escalation to an attacker.
2. Agents have significant maintenance and operational challenges – each OS upgrade and Security patch can cause compatibility issues for the Agent.
3. Active Directory Overhead – the agents keep accessing the Active Directory repeatedly to keep the results current and consistent across all the endpoints. This results in a significant amount of traffic to the Enterprise Active Directory and may cause instability.